# Acer Altos® NAS 700 Solution Guide

# Basic Setup

This solution guide will show you how to set up and configure the Acer Altos NAS 700 appliance.

**Abstract**

Acer Altos NAS 700 is a Solution based on Acer Storage Center (ASC) Software Version 4.0. ASC provides vital storage services—virtualization, mirroring, capacity expansion, scalability, TimeMark/TimeView, and more--through a software-optimized solution that runs on existing industry standard hardware.

The Acer Altos NAS 700 appliance offers:

NAS capability for file sharing with quota management.

SAN/IP connection for database/application servers

Storage Virtualization

Capacity consolidation & scalability

Mirroring

TimeMark/TimeView

Centralized Backup.

**CONTENTS**

## INTRODUCTION

This solution guide discusses the installation, configuration, management troubleshooting and the benefits provided by the Acer Altos NAS 700 appliance. The Altos NAS 700 appliance is a highly flexible and scalable Network Attached Storage solution.

It improves storage utilization compared to D.A.S (direct attached storage).

It offers storage centralized management and reduces the Total cost of Ownership.

### Who should read this Guide

This configuration guide is intended for:

- Acer field site engineers who are installing and configuring Altos NAS 700 Appliances.
- Acer resellers who are providing technical solutions to customers.
- Customers who are implementing these storage systems in their environment.

### Contents of this Guide

This guide's chapters contain the following information:

1. **ACER ASC Express Basics** – presents an overview of ASC Software suite.

2. **System Specification**—presents the detailed specification of Altos NAS700 as well as Qlogic 23xx Fibre Channel HBA controller.

3. **Installation and Configuration**—presents step-by-step installation and configuration instructions for Altos NAS700 including the basic Linux 7.3 installation, the ASC software suite including the ASC server, the Management console and the ASC SAN clients.

4. **Configure ASC SAN resources** —presents the procedures to create, expand, delete and assign the different resources to be used by your SAN/IP clients.

5. **Manage ASC SAN clients**—presents the procedures for adding, installing and managing ASC SAN clients on Microsoft Windows, Red Hat Linux and Novell NetWare O.S.

6. **Manage the ASC Server**—presents the procedures to start, stop and log into the ASC Server.

7. **Configure ASC NAS resources** present the procedures to create and assign the different resources to be used by your SAN/IP clients.

8. **Troubleshooting**—presents the procedures to help you through some common issues you may encounter when you set up and run the ASC storage network.

## Course Goals

Enable engineers and partners to fully implement an ACER Altos NAS 700 Appliance.

## Prerequisites

Learners should meet the following prerequisites before installing a NAS 700 appliance (or equivalent experience):

- Acer Server Product Training (or knowledge about the current Acer Server product range and technology)

- Acer RAID Workshop (or work experience with Server RAID Adapter and RAID technology)

- Fibre Channel technology basics

- Linux basic knowledge or experience (Installation and configuration)

## Overview of the ACER Altos NAS 700 Appliance

The ACER Altos NAS 700 Appliance is based on the Altos G710 server which comes with two 36Gb U320 SCSI hard drives. ACER recommends that you configure a RAID1 in order to offer redundancy for the Operating System. Final users can use up to 6 additional internal hard disks for their data when using the second SCSI cage, without requiring external enclosure. So this configuration can offer a RAID 5 volume up to 730 GB of internal storage.

ACER Altos NAS 700 Appliance prevents soft-errors by using it's snapshot and TimeMark features. It increases storage utilization and provides both file and block level access. It also offers 2 different backup solutions 1. standard Tape backup and 2. High performing Disk to Disk (D2D) backup for your NAS shares and SANDisks.

## ACER
## ASC EXPRESS BASICS

## What is ACER ASC Express ?

The explosion of data in today's networked computing environments stresses the abilities of many Information Technology groups while the demand to store and access data doubles each year.

Since information, and the storage infrastructure that holds it, are critical to a company's success, the management of the storage becomes a serious issue, where reliability, availability and improved disaster recovery are all key factors. Documents, databases, web pages, and other sorts of media each have their own rules for accessibility, retention and backup. Estimates of the cost to manage storage range from 5 to 10 times the actual cost of the storage hardware itself.

The Storage Area Network (SAN) is a dedicated network devoted to data storage and is a solution that meets the storage requirements of many businesses today. SANs address many of the reliability and availability issues for data storage. Essentially, SANs apply networking methodologies to the problems of storage, expanding the management possibilities for storage

ASC (Acer Storage Centre) is the award-winning storage networking infrastructure software suite that simplifies storage management by delivering SAN and NAS and enterprise class storage services under a unified management umbrella across Fibre Channel and IP.

Developed by a team of world-class network and storage management experts, ASC provides vital storage services through a software-only solution that runs on top of the ALTOS NAS 700 Appliance.

ASC is a software suite that virtualizes the 'disk' hardware into a storage pool, no matter if they are SCSI, Fibre Channel or iSCSI. ASC provides companies with immediate total freedom of choice in connectivity and storage hardware platform.

You can add physical or logical drives or even entire enclosures in this storage pool. Then ASC allocates storage capacity from this pool by creating arbitrary virtual drives. These 'virtual drives' appear exactly like a real SCSI drive, each having their own SCSI ID or world-wide-name. The size can be anything you want and the actual storage space can span across different physical disks. For example you can create a 100GB virtual drive, with 50GB from an ACER S300 SCSI enclosure, another 25GB from an ACER S205F Fibre Channel enclosure and the rest from an X SCSI enclosure.

With this sophisticated storage farm, the provision of the storage back to our servers is done through SAN/IP protocol or iSCSI/IP target mode.

Target Mode is used when a SCSI initiator requests operations to be performed by a HBA target device.

At the same time, we also offer CIFS and NFS protocols.

This is how ASC achieves both Block (SAN) level and File (NAS) level connectivity all under a single infrastructure.

ASC offers enterprises an easy way to purchase, implement, and support new or existing enterprise SANs, while containing the costs associated with the ownership and management of storage solutions. Building an ASC storage network puts enterprise class storage services at your fingertips, allowing you to do more with less.

Provides total freedom in storage connectivity: Fibre Channel, IP/iSCSI, SCSI, JBOD, RAID, and tape/library. Because ASC scales easily and encompasses all protocols and standards (current and upcoming), it is not just a tool, but an entire future-proof system.

- Reduces management costs by leveraging existing IT infrastructures.

- Cuts capital investment by consolidating storage resources for maximized utilization and efficiency.

- Dramatically lowers storage administration overhead through centralized, simplified storage management.

- Eliminates requirement for multiple software licenses and individual management of storage software for each server.

- Maximizes performance for high bandwidth applications.

- Provides total storage security with key-based authentication.

These benefits are all integrated into the ASC Server, an intelligent storage processor capable of supporting high performance storage I/O in a complex data management environment. The ASC solution delivers cost-effective, easy-to-use, flexible, rapidly deployable solutions for storing, managing, and migrating data.

ASC also enables service provider businesses, including Internet Service Providers (ISPs,) Application Service Providers (ASPs,) and Storage Service Providers (SSPs), to grow and manage their storage resources more easily.

## What is an ASC Network

The ASC Storage Network can be either a dedicated storage network, just like traditional Fibre Channel SANs, or it can be embedded into the existing LAN for small or low impact applications. Acer recommends that a separate network segment be dedicated to the Storage Network; this flexibility allows the building and testing of different topologies, the scaling of the Storage Network, and the sharing of networking resources to suit the varied requirements of different computing environment.
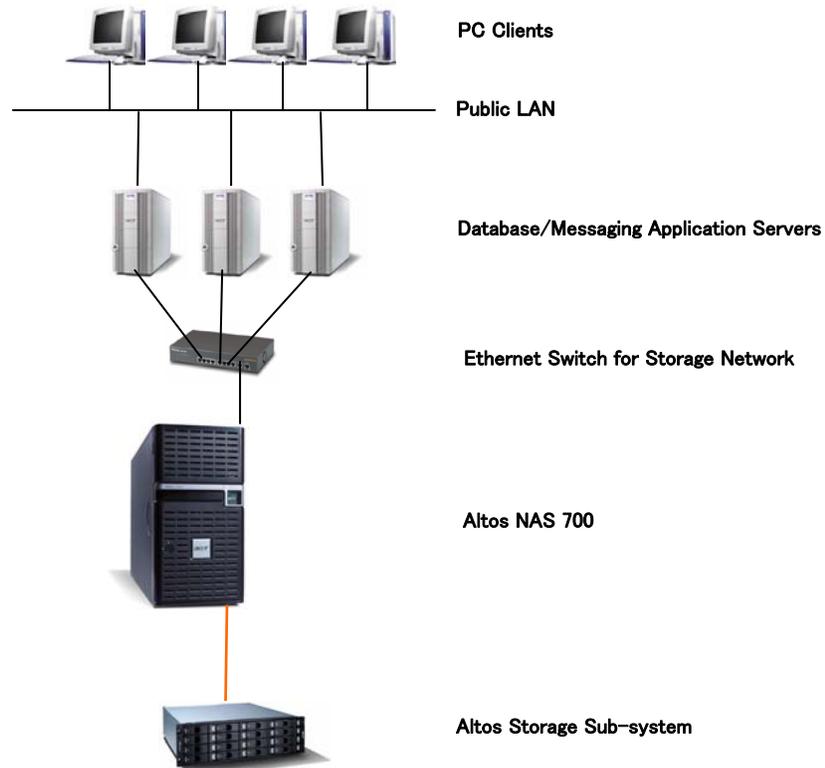


ASC uses in-Band design.
In-Band is using a group of dedicated appliance boxes located between the Storage and the Host servers to manage the storage. It uses at least 2 Ports – One as "Target" to Hosts, and One as Initiator to Arrays. When setting up ASC ports, Hosts are mapped to Target Ports and Arrays are mapped to Initiator Ports.

ASC utilizes SCSI, the standard for server class storage devices. ASC supports all types of SCSI devices, including those running the fastest Ultra 320 SCSI specification.

SCSI is the standard for server class storage because it is fast, intelligent (operations can occur independently of activity on the bus,) and expandable

(depending upon specific configurations, typically up to 16 devices per bus).

For maximum throughput, ASC supports multiple SCSI busses and/or adapters.

For SAN/IP Clients (non-Fibre Channel Clients), ASC packages the storage requests into IP packets using Acer's SAN/IP™ protocol. Requests made to the client's virtual adapters are converted to SAN/IP packets. The ASC Server receives the SAN/IP packets and converts them to SCSI commands. The ASC Server then responds with the storage data, again packaged as SAN/IP packets.

Acer's SAN/IP handles the entire process with minimal overhead so that the SCSI devices are operating at maximum throughput, even over the storage network.

An advantage of packaging the storage data into SAN/IP packets is that the data can be carried over trunked adapters, effectively multiplying the potential throughput for single and multiple device accesses. This is not possible on bus-based interfaces because all of the data must be transmitted on the same bus; data cannot be split over multiple busses.

## ASC Components

The primary components of the ASC Storage Network are the ASC Server, ASC Console, ASC SAN Clients and the ASC NAS Clients.
These components all sit on the same network segment, the *storage network*.

### ASC Server

The ASC Server is a dedicated network storage server. The ASC Server is attached to the physical SCSI and/or Fibre Channel storage devices on one or more SCSI or Fibre Channel busses.
The job of the ASC Server is to communicate data requests between the clients and the logical (SAN and NAS) resources (logically mapped storage devices on the storage network) via Fibre Channel or IP.

### ASC Management Console

The ASC Management Console is the administration tool for the ASC storage network. It is a Java application that can be used on a variety of platforms and allows ASC administrators to create, configure, manage, and monitor the storage resources and services on the ASC storage network.

### ASC SAN Clients

ASC SAN Clients are the actual file and application servers. Acer calls them ASC SAN Clients because they utilize the storage resources via the ASC Server.
There are two types of SAN Clients, SAN/IP and iSCSI and you can have both on your storage network.

These SAN Clients access their storage resources via software-emulated virtual adapters for SAN/IP.  The storage resources appear as locally attached devices to the SAN Clients' operating systems (Windows NT, Windows 2000, Linux, etc.) even though the SCSI devices are actually located at the ASC Server.

### ASC NAS Clients

NAS Clients are the Windows/Unix users and groups that access data and storage (if authorized) on the storage network via standard operating system network mapping protocols.

*Warning:*
*Do not confuse ASC NAS clients with a NAS server.*
*NAS Clients are Users and Groups and not physical server or NAS appliances!*

## SYSTEM SPECIFICATION

In this part, it will cover the detailed specification summary of all important components that make up the Acer Altos NAS 700 Appliance.

### ACER Altos NAS700 Appliance Features

High density computing in a competitive world calls for a server that can keep up and still stay cool in a rack. It's your life in the business fast lane that insists on reliability, performance, and space to move.
The Altos NAS 700 appliance is based on the ACER ALTOS G710 server that offers excellent storage scalability with its 8 slots. For applications needing high performance and high availability, the Altos NAS 700 Appliance uses an Intel Xeon processor. High capacity and high-speed network enabled, this is an appliance to be reckoned with. With the two on board Gigabit LAN adapters it is also the perfect choice as a network file server.

- Provides high level of business continuity through a set of high availability and fault tolerance. The Altos NAS 700 snapshot copy and TimeMark® protects where data from "soft-errors" such as accidental deletion, file corruptions, and virus attacks. The Altos NAS 700 snapshot copy creates scheduled or on-demand point-in-time snapshot copies of data volumes-"TimeMark®". TimeMarks contain only data changes and therefore do not take up a significant amount of disk storage space. Up to 4 TimeMarks can be maintained and used for fast backup and data recovery.

- Reduced storage TCO (total cost of ownership) through increased server/storage resources utilization and simplified storage management. Through providing simultaneous access to both file and block-level applications, Acer Altos NAS 700 enables a consolidated storage platform that can serve storage to any application servers from database, messaging applications (Microsoft® Exchange, Oracle ®, Lotus® Notes, Sybase® IBM® DB2, SQL servers to web servers and file servers under a central console. As storage is consolidated and centralized, the capacity can easily be shared and reallocated among applications servers, minimizing the amount of unused capacity and the management of the storage resources is greatly simplified.

- Lower TCO simplified and accelerates backups.
Altos NAS allows existing 3rd party backup software to backup remote server's disk over IP or FC at speeds up to 2 gigabits per second. Application servers' performance is increased through the elimination of overhead associated with backup/restore operation and any additional processor load on the application server because all data movements and backup command are controlled by the Acer Altos NAS with no impact on the application servers. Furthermore, since only one copy of backup software is

necessary, at the Altos NAS, this centralizes and therefore simplifies the backup management. It is also cost-effective as there is no need for backup agent on each application server.

- Tower or 5HE rackable chassis to slip into a rack.

- 8x DIMM slots offer up to 16 GB of registered ECC DDR333 RAM.

- Up to two Intel® 2.8 GHz Xeon™ Processors at 533 MHz FSB with Hyper-Threading technology for blistering processing power.

- 1+1 redundant, hot-swappable 550 Watts power supplies.

- 2x PCI-Express x4 slots.

- 3x 64-bit PCI-X 100 MHz + 1 PCI 32 bits PCI slots.

- 3 external 5.25 bays.

- Integrated dual U320 Channel LSI1030 controllers.

- LSI MegaRAID 320-1 U320 PCI RAID controller (add on card)

- Dual-channel gigabit-LAN for high-speed connectivity.

- Altos EasyDiagnostic LEDs indicate that you can trust your Altos to keep on going.

- OS Supports: Red Hat Linux 7.3 with 2.4.21-ipstor kernel.

- Warranty Services: 3 years on-site services next business day response time.



Altos NAS 700 Appliance

## ACER ASC Express Features

- Up to 730 GB internal storage / Up to 2 TB with external storage enclosure.

- Mirroring: Protects against device/cabinet/frame level failure for any Acer Altos NAS 700 managed disk

- Snapshot/Timemark: Max 4 times of incremental backup scheduled through the day that provide easy data restoration without having to access tape, with limited utilization of time and space .

- NAS: Provides storage via CIFS and NFS to Microsoft Windows, Linux, UNIX and Mac* clients, allowing folders and files to be shared by users regardless of the operating system.

- 5 SAN/IP clients max.

- Max 15 Virtual Resources / 4 TimeMarks per Acer Altos NAS 700 Appliance.

- Snapshot Copy and Synchronous Mirroring capability.

- iSCSI capabilities: Storage for database and messaging application (such as SQL, Exchange, Oracle) can also be created from a common storage pool via a common network such as Ethernet.

- Supported platforms for the iSCSI clients are:
    Windows XP SP1,
    Windows 2000 SP3 and higher,
    Windows 2003 Standard & Enterprise.

- Storage Management: Centralized storage services at a single console, including storage configuration, capacity management, storage provisioning, reporting and diagnostics.

- Quota Management:
  Manages the capacity usage, allows the administrator to set the capacity limit of each share folder.
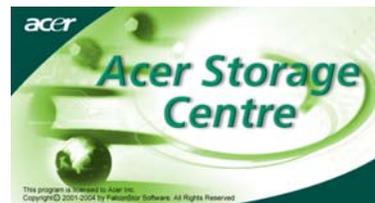
## Qlogic 2340 (Optional Fibre Channel HBA Controller)

The Qlogic QLA234x controllers bring the latest in Fibre Channel 2 (FC2) technology, doubling speeds from 1Gbps to 2Gbps.
The Controller provides multipath and failover capability (when using QLA 2340 or two QLA 2342 Controllers). Each Controller provides an LC cable connector to easily connect to Fibre channel Switches or directly to the Altos S700F or S205F Storage.

- Single-integrated Fibre Channel controller (LC connector) for added reliability and optimum performance
- Auto negotiation of Fibre Channel speed bit rate (1 Gbps or 2 Gbps).
- 200 Mbps at half-duplex / 400 Mbps at full-duplex.
- 1 multimode short wave laser LC port.
- Automatic topology detection.
- Concurrent support for SCSI and IP protocols
- Simultaneous initiator and target mode support
- 64bits/133MHz PCI-X specification. (3,3V and 5V bus supported).
- HBA and LUN level failover
- Persistent binding
- LUN Masking
- Local and remote Management
- Load balancing for optimized performance
- Supports Microsoft Cluster Service.
- OS supports:
  Windows Server 2003 (32-bit and 64-bit),
  Windows NT,
  Windows 2000,
  Windows XP,
  Solaris SPARC,
  Linux (32-bit and 64-bit),
  Novell NetWare.



QLA2340

## INSTALLATION AND CONFIGURATION

### General Installation Sequence

1) Install the HBA in your ALTOS NAS 700 appliance

2) Connect your ASC NAS 700 appliance to your storage network

3) Linux 7.3 installation through a:

   a. Recovery image

   b. Manual installation

4) ASC Server installation

5) ASC Management Console installation

6) ASC SAN Client installation

7) Configure ASC SAN Resources

8) Assign a SAN Resource to one or more client.

### Installing HBA into the Altos NAS 700

Before you can start with setting up the ASC Software you may need to add additional Controllers into your Altos NAS 700. If you are using a Qlogic Fibre Channel HBA you need to add, open the housing and add the Controller. Also make sure that your LSI RAID Controller 320-1 is installed correct and the SCSI Cable from the backplane board is connected to this Controller. There should be up to 2 x 36GB and 6 x 146 GB Hot Swap Hard Disk installed and the Backplane is connected to the LSI 320-1 RAID controller.

### Setting up RAID Array and LUNs

On the first start of the Altos Server G710 press Ctrl-M to get into the MegaRAID set up utility and create a new Array.

1. Select **Configure -> New Configuration** (Note: Choosing "New Configuration" will erase any former configuration, do **not** select this option if you simply want to add a new Array group to an existing configuration)

2. You will see a list of Drives available for your RAID Array, use the arrow keys to move between them

3. You must select 2 disks with the spacebar key to create one Array and a logical drive with 8000MB for operating system.

4. Press **Enter** when you are done with the selection.

5. Finish your physical Array selection and press **F10** to create a Logical

Drive.

6. Choose the **RAID Level** (in this case **RAID 1**) and select the size of your first LUN. We recommend to create a LUN with the size of 8000 MB. You can also select the full size for your O.S mirror.
Confirm the Logical Drive by using the **Enter** key

7. Please select now the remaining disk and create a RAID5 logical drive for your ACER altos NAS 700 Data storage.

8. After you are done do not forget **to initialise** the **Logical Drives**. If you select the Initialise option in the Controller menu it will destroy any existing data on the Array. This is wanted on the first installation, but be careful with this on already installed systems.

## A) Red Hat Linux 7.3 installation using the Recovery Image

**Introduction**

ACER provides on the ASC 4.0 Express cdrom, a Norton Ghost image to restore the Linux 7.3 operating systems necessary to install later ASC 4.0 server on the ACER Altos NAS 700 Appliance. ACER recommends our solution partners to use this image to install the Linux Operating system.

The file can be found in the IMAGE folder of the cdrom and is called: "linux.GHO".

**Supported platform**

Altos Server G710 (with LSI MegaRAID 320-1/320-2 SCSI RAID Controller)
ACER Recommends to use two 36GB hard drives as a RAID-1
Monitor supporting a resolution of 1024*768

**How to restore the image**

 Create a LUN (size is 8000 MB) under MegaRAID BIOS with the initialization done.

Boot from ASC 4.0 CD.

Type "cd image"

Type "ghostro.exe" to launch the ACER Backup Tool.

Select "Local", "Disk", "From Image",

Then select the file "LINUX.GHO".

 In the Destination Drive Details, make sure the New Size for Part 1 & 2 should be the same as those in Old Size (Part 3 could be different).

 Then press "Yes" to proceed with disk restore.

**Important Notes:**
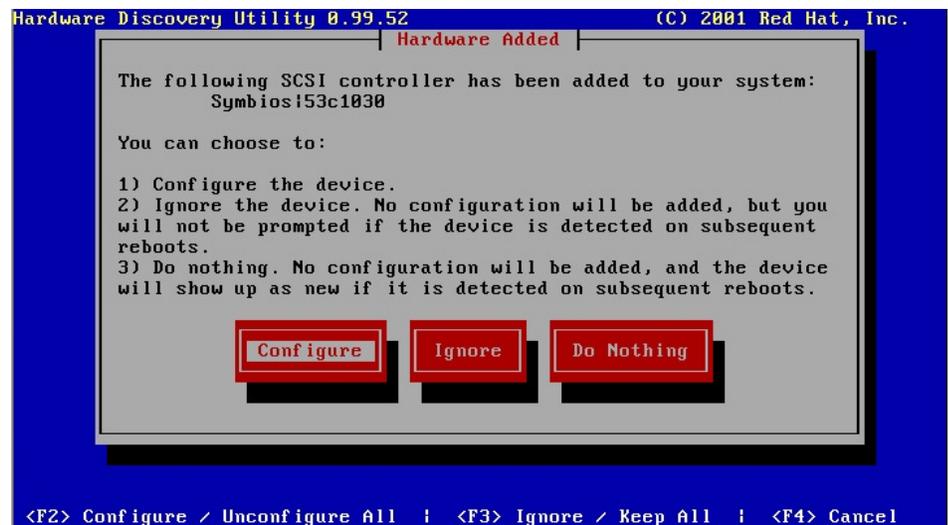
When you reboot the server Linux starts the Hardware Configuration Utility called KUDZU. It will detect the Hardware configuration of your server and will install the correct drivers for them. You might see messages where it says that a device is being removed etc but this is because of a change in the configuration between the ALTOS G710 server used to create the image and your configuration.

So just click on the REMOVE CONFIGURATION button to remove a device.

```
Hardware Discovery Utility 0.99.52                (C) 2001 Red Hat, Inc.
                        | Hardware Removed |

      The following SCSI controller has been removed from
      your system:
              Symbios:53c1030

      You can choose to:

      1) Remove any existing configuration for the device.
      2) Keep the existing configuration. You will not be
      prompted again if the device seems to be missing.
      3) Do nothing. The configuration will not be removed,
      but if the device is found missing on subsequent
      reboots, you will be prompted again.


       Remove Configuration      Keep Configuration      Do Nothing



 <F2> Configure / Unconfigure All  |  <F3> Ignore / Keep All  |  <F4> Cancel
```

Then click on the CONFIGURE button to add a newly detected device.

```
Hardware Discovery Utility 0.99.52                (C) 2001 Red Hat, Inc.
                        | Hardware Added |

      The following SCSI controller has been added to your system:
              Symbios:53c1030

      You can choose to:

      1) Configure the device.
      2) Ignore the device. No configuration will be added, but you
      will not be prompted if the device is detected on subsequent
      reboots.
      3) Do nothing. No configuration will be added, and the device
      will show up as new if it is detected on subsequent reboots.

              Configure      Ignore      Do Nothing



 <F2> Configure / Unconfigure All  |  <F3> Ignore / Keep All  |  <F4> Cancel
```

There're some specific tasks to do when you add the ATI Rage XL (graphics adapter):

- Select your Monitor specs (automatic if your monitor is Plug and Play)

- Select the Video Memory: the ATI Rage XL has 8 MB

- Select "No clockchip settings (recommended)"

- Click OK to test your Graphics configuration under X Window.

- If you see a message displayed on screen, just click YES.

Then, select the automatic startup of X Window when asked by the system.

The default password for Linux 7.3 account "root" is "000000" (six zeros). Please change it with the proper one according to your requirement later.

The Time Zone is default set to Taipei. After restoring, please change to the proper "Time Zone" with the correct "Zone".
To do that, on the G.U.I, click Program / System then Date/Time Properties.

## B) Red Hat Linux 7.3 manual installation

This section is for information only

1.    Boot from the RedHat Linux CD and hit <Enter> to begin the installation.

2.    On the welcome screen, click NEXT to go to the next step.



3.    Select the installation language and click NEXT.

4.    On this page, select your keyboard language and click NEXT.

5.    Select your mouse configuration and click NEXT

6.    Select CUSTOM as installation Type and click NEXT.
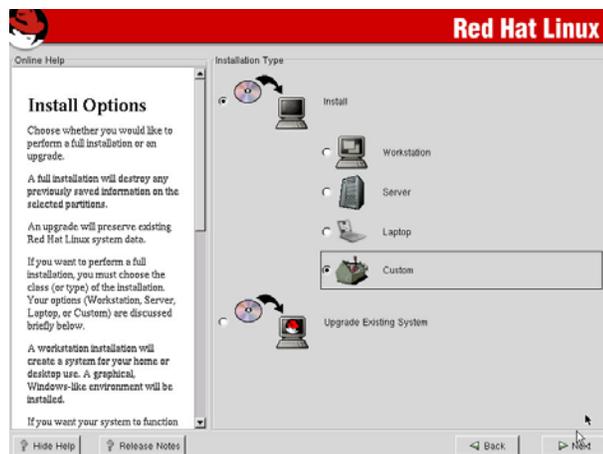
7. Disk Partitioning Setup: Select "Have the installer automatically partition for you" and click NEXT.
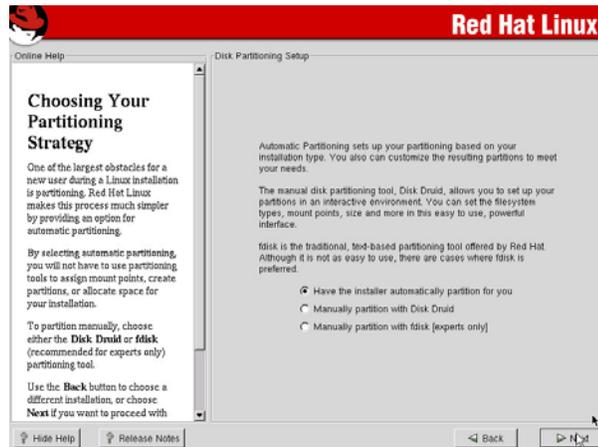


8. Disk Setup.
Verify that the swap partition is smaller than 2000 MB. (Max size for Linux 2.4 kernel). If it's larger than 2000MB, Select the Swap partition, press "EDIT" to reduce the value and then click NEXT.
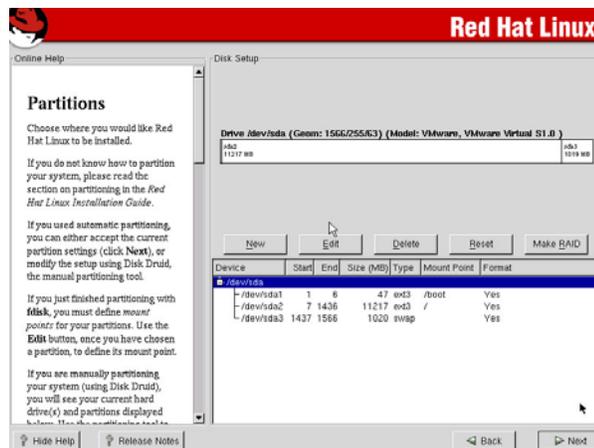


9.

Use GRUB as the boot loader (default setting) and click NEXT to continue.

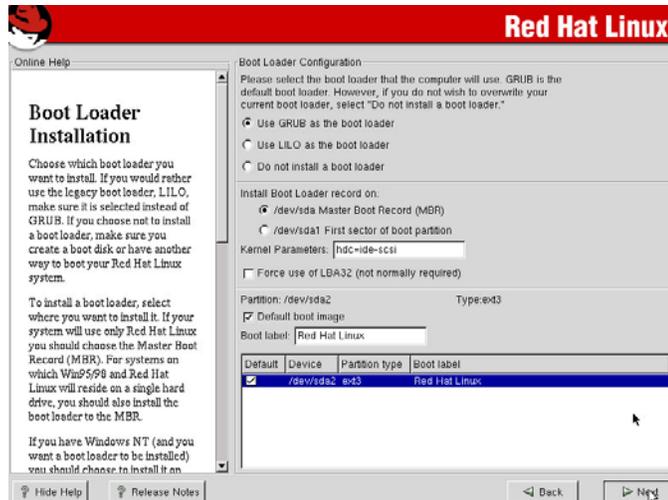10. The GRUB password is not mandatory. Leave the field blank if you don't want to protect the access to your boot loader. Click NEXT to continue the installation.

11. On this page you can configure the TCPIP parameters for your 2 built-in network cards.
ACER recommends to configure and activate on boot only the first network card called eth0.
You can select to manually enter a static IP address or you can choose to use a dynamic IP addressing scheme if you already have a DHCP server installed and running on your network.
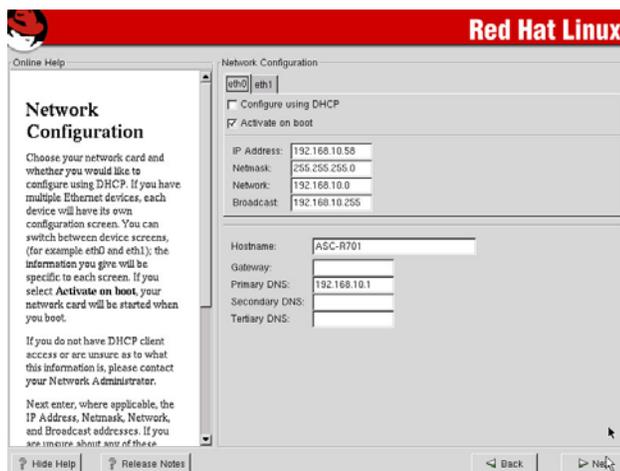


12. Firewall Configuration.

On this page, select No Firewall and click NEXT.
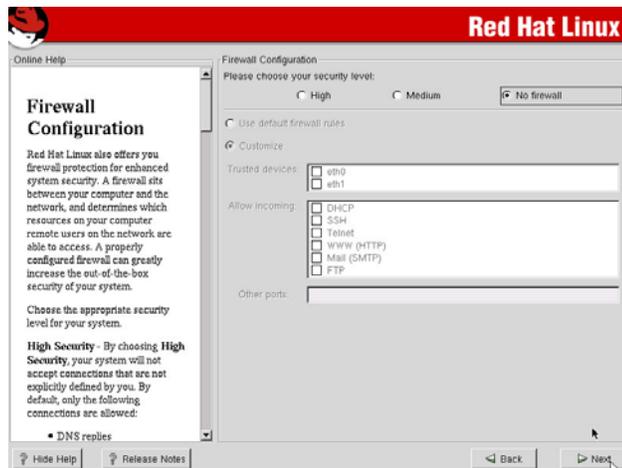


13. Additional Language Support Selection.
    Here you can select an additional language support for your Linux
    Graphical interface.
    ACER recommends to use only English. Click NEXT to continue.

14. Time Zone Selection: select the proper location (instead of UTC offset).
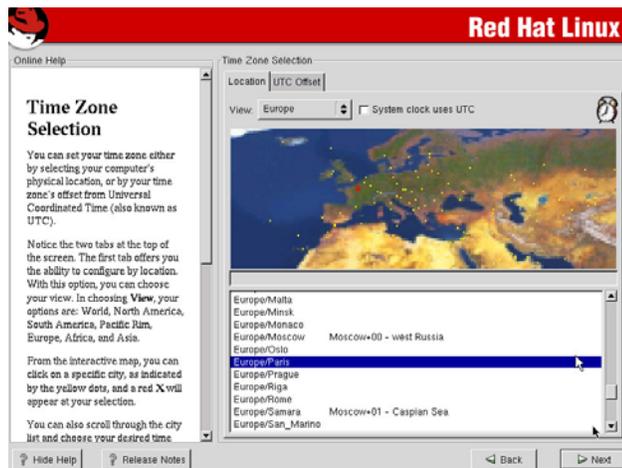


15. Account Configuration.
    Setup the root password on this page and you can also add other users.

16. Authentication Configuration.
    Just leave the default settings and click NEXT to continue.

17. The 8 following packages (total installed size: 1028 MB) are mandatory to
    run an ASC Server.

X Windows system
GNOME
Network Support
NFS File Server
Anonymous FTP Server
Web Server
Networked Managed Workstation
Utilities



Check the "Select individual packages" icon and then click NEXT.
Select Flat view to have a look at the full listing of packages that will be installed on your server.
In this listing, please verify that the following packages are selected:

Netscape-common
Netscape-communicator
Netscape-navigator

18.  In the Video Configuration page, select ATI Rage XL and click NEXT.
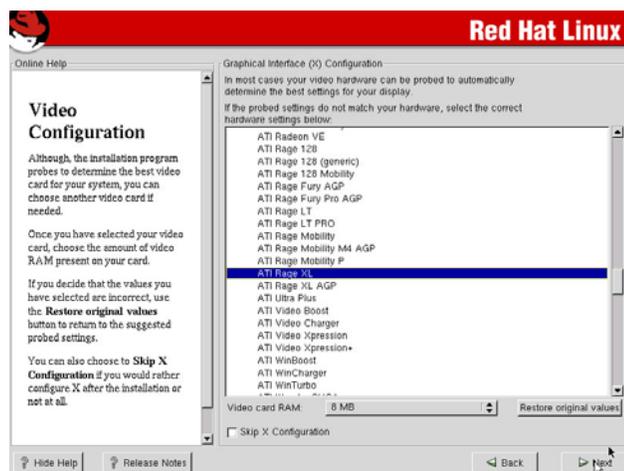


19.  Press NEXT to start the installation.

20. On this screen, you can see the installation of the different packages on your system.
The installer will ask you to insert the second and third CD of your Linux Red Hat distribution.
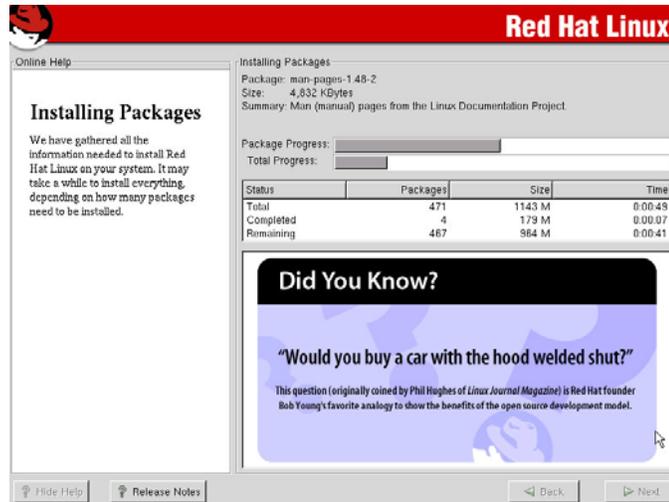


21. On the "Boot Disk Creation" mark the Skip boot creation box and click NEXT to continue the installation.



22. Select your monitor in the manufacturer list or select "Unprobeb Monitor" if not found. Then click Next.

23. Custom X configuration.
   On this screen, configure a standard graphic resolution such as
   1024*768 * 16 bits (65536) colors. Click NEXT.
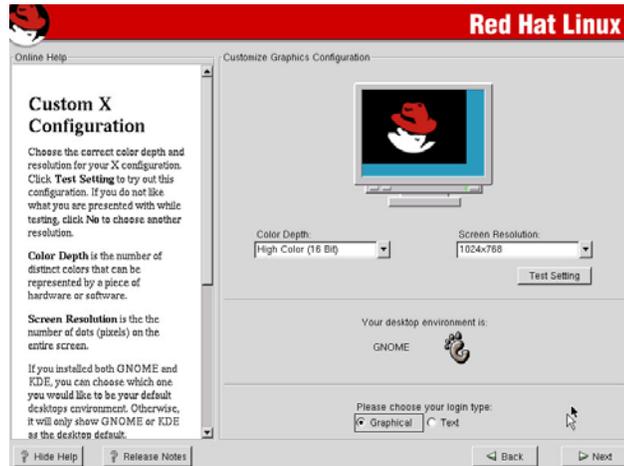


24. Congratulations Screen.
   When you reach this screen, the Linux installation is finished.
   Click on EXIT to reboot your Server and start Linux 7.3
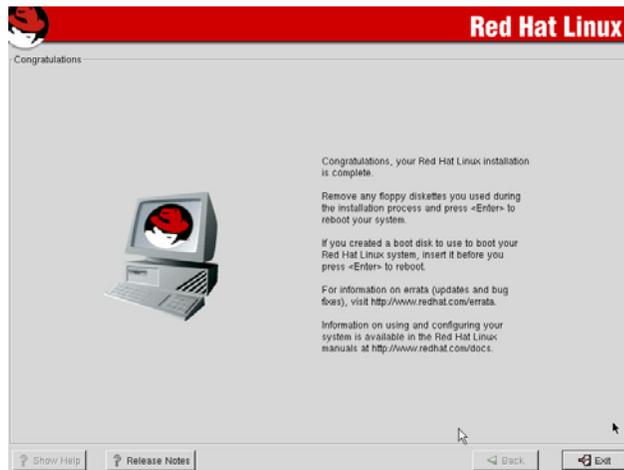
## ASC Server installation

1. After the Linux installation, you must enter into the BIOS by pressing F2 and check that your boot order is configured as shown in the picture below:
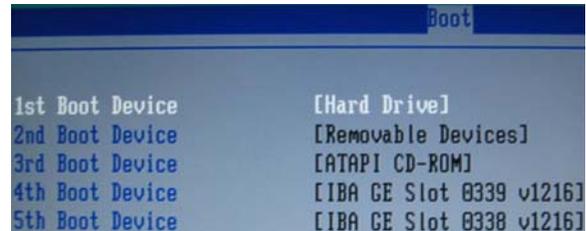


We recommend to have the Hard Drive selected as 1<sup>st</sup> Boot Device on your Altos NAS 700.

2. Select "Red Hat Linux (2.4.18-3smp)" to boot Linux.
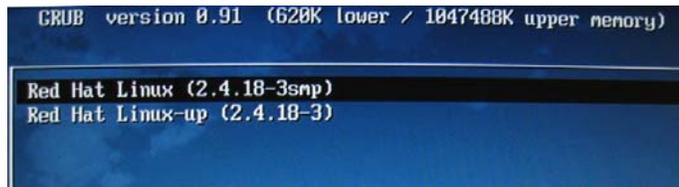


3. Enter your login and password for your ROOT account
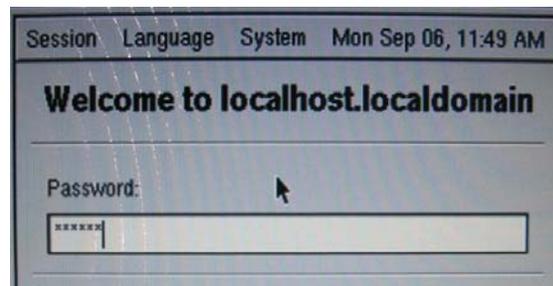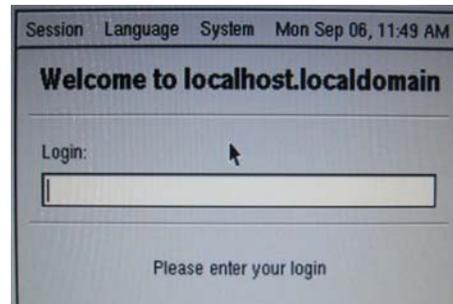




Please Note: If login with the ROOT account, you'll receive a warning message telling you it's risky to log onto an X environment with the full administrative privileges. Just click on the OK button.

4. Close the START HERE window. Right-click on the desktop and select NEW TERMINAL.

5. In this Terminal window, please type the following command to mount your ASC cdrom:

```
[root@ASC root]# mount /dev/cdrom /mnt/cdrom
```

A Nautilus window appears listing the content of the ASC 4.0 CD. Just close it.

6. In the terminal window, type the following command to run the script that will perform the required updates to your Linux operating system and launch the ASC 4.0 installer:

```
[root@ASC root]# cd /mnt/cdrom
[root@ASC cdrom]# ./ascinstall
```

The script will modify the following information:
2.4.18 kernel will be updated by the 2.4.21 –ipstor kernel.
Intel onboard NIC drivers will be installed.
Network configuration.
HBA Drivers installation.

7. When you see the first installation page, Press Y to continue the installation.

```
ascinstall v4.1
========================================

  Important Pre-install notes:

 - This scripts supports new installations of ASC 4.0 and
   specific upgrades to 4.0. Refer to the ascinstall.txt
   file for specific build verions supported.

 - If porting an existing ASC configuration (ex. from another
   server or after reinstalling the RedHat operating system) then
   exit this script now and restore the /usr/local/asc/etc
   directory first before installing ASC using this script.

 - Hardware installed on server must be supported by ASC.

 - RedHat v7.3 must be installed with the GRUB boot loader.

 - This script generates an installation log file and an x-ray
   in the /usr/local/asc-archive directory.

Would you like to continue (Y or N)?
```

8. The script checks to see if ASC is already installed on your machine. Press Y to continue the ASC installation.

```
ascinstall v4.1
========================================

          ---   ASC IS NOT INSTALLED   ---

This script will perform the following tasks:

    1. Prompt for configuration parameters
    2. Update Linux kernel and operating system files
    3. Reboot the Linux server
    4. Install the ASC Server component software
    5. Install the ASC Console optional component software
    6. Start the ASC server component

    Would you like to continue (Y or N)? █
```

9. Type your company name and press <ENTER>

```
ascinstall v4.1                              Question: 1
========================================

What is the name of the company?
  Company: █
```

10. Enter the server name eg. NAS700 and press <ENTER>

```
ascinstall v4.1                              Question: 2
========================================

Configure Hostname
------------------
Current hostname is localhost.localdomain

Press <Enter> to keep the current hostname or enter a
a new hostname and press <Enter>.

Enter new hostname:NAS700_
```

11. ACER recommends to install the ASC Management Console on the ASC server. Type Y and press <ENTER>

```
ascinstall v4.1                              Question: 3
========================================

Do you want to install the ASC Console on this appliance (Y or N)?
```

12. On this page, the cards located in the ASC Server must be selected to run the installation of the drivers.

```
ascinstall v4.1                              Question: 4
========================================

Configure Internal Hardware
---------------------------
Select all the cards that are in the ASC appliance.
Select one item at a time by entering its number
An '*' will appear next to the item(s) that are selected.
Selecting an item multiple times will toggle the selection on and off.

              «« RAID Controllers »»
      1) Compaq SmartArray 640x,64x,5i,5300 Controller(s)
  *   2) MegaRAID Controller(s)
              «« SCSI Cards »»
      3) Adaptec Ultra 160 SCSI card(s)
      4) Adaptec Ultra 320 SCSI card(s)
              «« FC HBA Cards »»
      5) LSI HBA(s)
  *   6) Qlogic HBA(s)
              «« Network Cards »»
  *   7) Broadcom BCM5700 series Ethernet Adapter(s)
      8) Intel PRO/1000 Ethernet Adapter(s)

Select a card (use F to finish): f_
```

Select 2, 6 and 7.
When the selection is finished, press the F key to continue the installation.

13. If Qlogic HBA is selected on the prvious step, please press 2 and F to continue the installation.
    If not, press 6 and F to continue the installation.

```
ascinstall v4.1                              Question: 6
========================================

Configure Target Mode HBA Support
---------------------------------
ASC server supports the following target mode HBAs
NOTE: ASC server only supports one target mode HBA at a time

      1) QLogic 2200 series HBA
  *   2) QLogic 2300 series HBA
      3) MPIO QLogic 2200 series HBA
      4) MPIO QLogic 2300 series HBA
      5) LSI HBA
      6) No Fibre Channel target mode support

Select HBA class (use F to finish): F
```

14. Linux supports multiple LUNs on the same SCSI ID. In this menu, select the number of LUNs you want to use.
The default value is 32.

```
ascinstall v4.1                              Question: 7
=======================================

Configure Multiple LUN Support
-------------------------------
max_scsi_luns setting is not set in /etc/modules.conf.

Press <Enter> to accept the default value 32 or
enter a value and press <Enter>.

options scsi_mod max_scsi_luns=█
```

15. Now, you can setup the maximum number of disks you want to scan. Acer recommends to use the default settings and press <ENTER>

```
ascinstall v4.1                              Question: 8
=======================================

Configure Maximum SCSI Disk Scan
--------------------------------

The max_scsi_disk_fs parameter will force the Linux operating system to
scan a fixed number of SCSI devices on boot-up. This parameter should be
used to scan only those SCSI devices used by Linux to boot the operating
system.

The max_scsi_disks_fs setting is not set in /etc/modules.conf. The value
below shows the recommended value based on the number of Linux SCSI disks
detected after scanning the system.

          options sd_mod max_scsi_disks_fs=1.

Press <Enter> to accept the recommended value or enter a new value and press
<Enter>.

New Value:█
```

16. The installer offers you the possibility to install several network services such as Telnet, FTP and NTP.
These components are all enabled by default.
Please deselect "NTP (Network Time Protocol)" by typing 3 and F. Then press <ENTER>

```
ascinstall v4.1                          Question: 9
====================================

Enable / Disable Network Services
--------------------------------
Enable or disable a network service by entering its associated number.
"Service not installed" indicates rpm package for that service is currently
not installed.

              Service                          Setting
  1) Telnet (SSH is enabled by default)        Enable

  2) FTP (File Transfer Protocol)              Enable

  3) NTP (Network Time Protocol)               Disable

  Select a service (use 'F' to finish): F
```

17. The next screen shows a summary of the configuration that has been selected before.
Press Y to accept the current configuration.

```
ascinstall v4.1      Configuration Summary
===============================================================
Company: ACER
Hostname: NAS700
Server Installation Type: New          Install Console: Yes

------------------ Hardware selected -----------------------
  MegaRAID Controller(s)
  Qlogic HBA(s)
  Broadcom BCM5700 series Ethernet Adapter(s)
-----------------------------------------------------------
Qlogic Target Mode HBA Support: QLogic 2300 series HBA
options scsi_mod max_scsi_luns=32
options scsi_mod max_scsi_disks_fs=1

------------Enable / Disable Network Services ------------------
Telnet: Enable      FTP: Enable      NTP: Disable
Time Server Specified: n/a

Enter 'Y' to accept configuration or enter 'N' to change configuration: y
```

18. A message appears asking the user to wait for a moment during the automatic installation. No user interaction is required now until installation is complete.
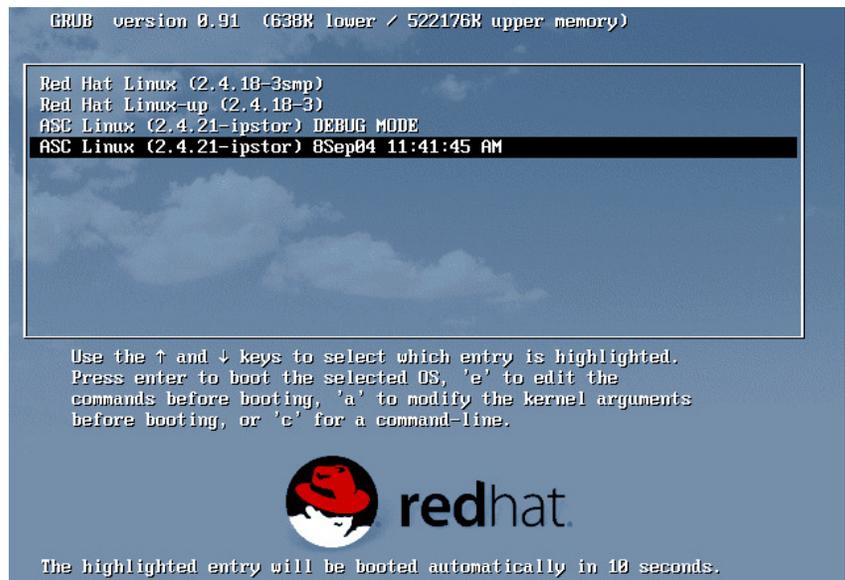


19. When the script has finished updating the Linux kernel, it reboots your ASC server and a new boot option is added in your GRUB boot loader.

20. When the server boots, the Hardware discovery utility named KUDZU starts. Press <ENTER> to go to the next screen.

21. KUDZU has detected new installed devices in your ASC server and asks if you want to configure the new devices or simply ignore them. Here we can see it has detected a Broadcom BCM5700 network card. Click on the "CONFIGURE" button.



```
Hardware Discovery Utility 0.99.52              (C) 2001 Red Hat, Inc.
                            ┤ Hardware Added ├

      The following SCSI controller has been added to your system:
             Symbios:53c1030

      You can choose to:

      1) Configure the device.
      2) Ignore the device. No configuration will be added, but you
      will not be prompted if the device is detected on subsequent
      reboots.
      3) Do nothing. No configuration will be added, and the device
      will show up as new if it is detected on subsequent reboots.


            Configure          Ignore          Do Nothing



   <F2> Configure / Unconfigure All  ┊  <F3> Ignore / Keep All  ┊  <F4> Cancel
```

22. On the next screen, click on "YES" to configure the first network card.

*Note:* *Configure and setup the first network adapter called ETH0. Configure the second network adapter ETH1 but do not setup it at this moment. This configuration works for teaming and non teaming solution.*

23. On this page, you must enter the TCPIP information for the new detected network card. You can select between a dynamic (if you already have a DHCP server running on your network) and a static IP configuration. For the latter case, you must manually enter all the information such as :

- IP address of the ASC server,

- Subnet Mask of the ASC server,

- Network Default Gateway,

- IP address of the DNS server
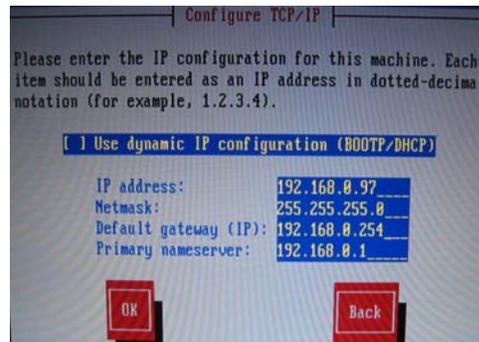


24. After this last configuration step, the script automatically finishes configuring your machine and starts all the ASC services.

*Note: Please make sure you have the CD still in the CD-ROM Drive at this time to allow the setup process to complete.*

**Congratulations.**

You have successfully completed the installation of ASC Server. You can now install the ASC Management Console on your Workstation to manage and configure the ASC server remotely. Please refer to the User Guide chapter 2 for the installation instructions for the ASC Console.

## ASC Management Console installation

The ASC Management Console is the administrative tool that allows ASC administrators to create, configure, manage, and monitor the storage resources on the ASC storage network.

The ASC Management Console is a Java application that can be run on many Windows, Linux, and Solaris platforms that support the Java 2 Runtime Environment (JRE).

Pre-Requisite.
The computer that runs the Console needs connectivity to the Storage Network segment. This is because it communicates directly with the server and clients to administer and monitor their behavior. The Console may be installed on any number of machines, including the clients themselves, provided that they have a Graphical User Interface.

**Installation on Microsoft Windows NT, 2000, XP and 2003.**

The installation CD includes a setup program for installation on Windows computers. On Windows NT and 2000, you must be a Power User or Administrator to install the Console.

- Insert the ASC installation CD into your CD-ROM drive.

- Select *Install Products --> Install ASC Console*.

- If the CD Browser does not launch, navigate to the \Console\Windows directory and run *ISinstall.exe* to launch the ASC Management Console install program.

- To launch the Console, select *Start --> Programs --> Acer ASC --> ASC Console*.

**Installation on Linux.**

For Linux, you will need to manually install the ASC Console.

To install the Console software, log into your system as the root user.

Mount the ASC installation CD to an available or newly created directory and copy the files from the /Console/Linux directory on the CD to a temporary directory.

Type the following command to install the Console software:

```
[root@ASC root]# rpm -i asconsole-4.00-0.883.i386.rpm
```

The Console will be installed in the following location: /user/local/ascconsole

```
[root@ASC local]# cd /usr/local/ascconsole
[root@ASC ascconsole]# ./ascconsole_
```

## ASC SAN Client installation

ASC SAN Clients access their storage resources via software-emulated virtual adapters (for SAN/IP). The storage resources appear as locally attached devices to the SAN Clients' operating systems (Windows NT, Windows 2000, Linux, etc.) even though the SCSI devices are actually located at the ASC Server.
There're 3 types of SAN clients:

- SAN/IP SAN Client

- iSCSI SAN Client

- Fibre Channel SAN Client (not supported by ACER ASC Express version)

### SAN/IP protocol definition

SAN/IP is a protocol specially developed for ASC in order to access SAN Storage over IP.

### iSCSI protocol definition

ACER recommends to use the SAN/IP protocol instead of iSCSI. It's an industry evolving standard storage protocol, recently ratified by the Internet Engineering Task Force (IETF) that is designed to transport block-level storage traffic over IP networks.

iSCSI employs Ethernet as the transport for data from servers to storage devices or SANs. The protocol takes standard SCSI commands into TCP and sends them over standard Ethernet, a venerable technology familiar to most IT shops. To create an iSCSI-based SAN, network designers bring together servers equipped with an iSCSI host bus adapter (HBA) or network interface card (NIC), disk arrays and tape libraries.

It's not widely used today due to a limited number of supported platforms

## Pre-installation checklist

ASC provides client software for many platforms and protocols. Please check the following lists for the versions and the patch levels (if applicable) that are currently supported. While this information is accurate as of the date of its release, you should check the certification matrix on the Acer website for any updates.

### Notes:

- The ASC Client should not be installed onto a networked drive.
- Client software requires network connectivity to the ASC Server, preferably on a separate, ASC-only network. This means that normal LAN traffic does not occur on the adapter(s) dedicated to the ASC storage network.

The ASC Server grants storage access to the client. In order for a client to be able to access storage, you must establish a trusted relationship between the client and server. This prevents other computers from masquerading as the client and accessing storage that it does not have rights to. In order to establish a trusted relationship, you must do two things:

- Add the client in the Console and assign storage resources to the client.
- Add the server to the client from the Client Monitor.
  For more information, refer to 'Add/configure an ASC SAN Client' in the "Manage ASC SAN Clients" chapter.

## ASC SAN Clients Supported Platform

### SAN/IP Client

The following platforms are supported for SAN/IP clients:

| Platform | Supported version |
|---|---|
| Windows NT | 4.0 Enterprise Edition with Service Pack 6a. |
| Windows 2003 | Standard Server and Enterprise Server |
| Windows 2000 | - Professional, Server, Advanced Server, and Datacenter, including Service Pack 2, 3, or 4.<br>- Supports Windows 2000 Clustering |
| Red Hat Linux Advanced Server v2.1 | - Kernel 2.4.9-e.9smp<br>- Kernel 2.4.9-e.12smp<br>- Kernel 2.4.9-e.16smp<br>- Kernel 2.4.9-e.25smp |
| Red Hat Linux v7.3 | - Kernel version 2.4.18-5<br>- Kernel version 2.4.18-5smp |
| Red Hat Linux v7.2 | - Kernel version 2.4.7-10<br>- Kernel version 2.4.7-10smp<br>- Kernel version 2.4.7-10enterprise<br>- Kernel version 2.4.9-31<br>- Kernel version 2.4.9-31smp<br>- Kernel version 2.4.9-31enterprise |
| Red Hat Linux v7.1 | - Kernel version 2.4.2-2<br>- Kernel version 2.4.2-2smp<br>- Kernel version 2.4.2-2enterprise |

| | |
|---|---|
| NetWare | NetWare 5.1 with Service Pack 6. Make sure NSS is running. |
| | NetWare 6.0 with Service Pack 3. Make sure NSS is running. |
| | You must have a separate Ethernet adapter for storage that is placed on a dedicated subnet. Although it is OK to use a 10/100 NIC, it is preferable to use a gigabit NIC. |

**iSCSI client**

The following platforms are supported for SAN/IP clients:

| Platform | Supported version |
|---|---|
| Windows 2003 | Standard Server and Enterprise Server. |
| Windows XP | With Service Pack 1 or higher. |
| Windows 2000 | With Service Pack 3 or higher. |

You should not install any ASC client software on an iSCSI client because it requires the Microsoft iSCSI initiator which can be downloaded from Microsoft's website
(http:/www.microsoft.com/windowsserversystem/storage/iscsi.mspx).
The Microsoft iSCSI Software Initiator package includes both the Microsoft iSCSI Initiator service and the Microsoft iSCSI Initiator software driver.

**SAN/IP Client installation on Windows NT, 2000 and 2003.**

You must be an administrator or have administrator privileges in order to install the client.

- Insert the ASC installation CD into your CD-ROM drive.

- Select *Install Products --> Install ASC SAN Client*.

- If the CD browser does not launch, navigate to the \Client\Windows directory and run *ISinstall.exe* to launch the client install program.

- Note: During the installation, the Microsoft "Digital Signature Warning" window will appear to indicate that the software has not been certified by Microsoft.  Click *YES* to continue the installation process.

- After accepting the license agreement, indicate the type of client you are installing, Fibre Channel or SAN/IP.

- When done, click *Finish*.

Note: The client installs a device driver.  Therefore a Windows NT computer must be rebooted before the client can use storage resources. (It is not necessary to reboot a Windows 2000 computer.)

**SAN/IP Client installation on Linux**

Note: You should not install the Linux client on an ASC Server machine.  The ASC Server installation includes a local Linux Client to service NAS Resources.  If the Linux Client were to be installed on an existing ASC Server, all access to NAS Resources would be lost.

Prior to installing the ASC SAN Client for Linux, assign SAN Resources to the client machine.  To do this, use the *Assign a SAN Resource Wizard* in the Console.  When you are asked to select the SAN Client, click the *Add* button and type in the name of the Linux machine.
The name must match the output of "uname –n" from the client machine.

For more information, refer to 'Assign a SAN Resource to one or more clients'.

- To install the client software, log into your system as the root user.

- Mount the ASC installation CD and copy the files from the CD to a temporary directory on the machine.

- The software packages are located in the /client/linux/ directory off the CD.

- Type the following command to install the client software:

```
rpm -i /mnt/cdrom/Client/Linux/sanclient-4.00-0.883.i386.rpm
```

- The client will be installed to the following location:  /usr/local/sanclient

- Log into the client machine as the root user again so that the changes in the user profile will take effect.

- Add the ASC Servers that this client will connect to for storage resources by typing the following command from /usr/local/sanclient/bin:

```
[root@ASC/]# ./sanclient monitor
```

- Indicate what type of client this is, Fibre Channel or SAN/IP.

- Select *Add an ASC Server* from the menu and enter the ASC Server name, login ID and password.

- After this server is added, you can continue adding additional servers.

- To start the Linux client, type the following command from the /usr/local/sanclient/bin directory:

```
[root@ASC /]# ./sanclient start
```

**SAN/IP Client installation on NetWare.**

Installation of the ASC's NetWare client is done on a Windows NT 4.0 or Windows 2000 machine running Novell's client for NetWare.

Before you install the SAN client on the NetWare server, you must log in to the server and map a drive to SYS:\SYSTEM.

- Run *setup.exe* to launch the client install program.

- Indicate the type of client you are installing, Fibre Channel or SAN/IP.

- When done, click *Finish*.

- To authenticate the NetWare client to the ASC Server, type *SANON* on the NetWare console screen.

- Run the command below to add the ASC Server to the ASC Client.

  - ISCMD AddServer server=*serverIPAddress*

- When prompted, enter your username and password.

- After using the ASC Management Console to assign devices to the client, you can start the client by typing the following command from the NetWare console screen:

- **ISCMD Start Server=***serverIPAddress*

- When prompted, enter your username and password.

- Type the following to scan and discover the ASC disk:

  `[root@ASC /]# list devices`

- If you have not done so before, use NWCONFIG (NetWare 5.1), ConsoleOne or web portal (NetWare 6.0) to create a NetWare volume on the ASC SAN/IP device.

- If you have already created a NetWare volume, type the following to mount the volume:

  `[root@ASC /]# mount all`

## ASC MANAGEMENT CONSOLE

The ASC Console is the administration tool for the ASC storage network.  It is a Java application that can be used on a variety of platforms and allows ASC administrators to create, configure, manage, and monitor the storage resources and services on the ASC storage network as well as run/view reports, enter licensing information, and add/delete ASC administrators.

### Start the ASC Management Console

On Windows, select *Start --> Programs --> Acer ASC --> ASC Console*.

On Linux and other UNIX environments, execute the following:

```
[root@ASC local]# cd /usr/local/ascconsole
[root@ASC ascconsole]# ./ascconsole_
```

Discover all ASC servers on your storage subnet by selecting *Tools --> Discover ASC Servers*.

You can connect to an existing ASC Server, by right-clicking on it and selecting *Connect.*.

If you want to connect to a server that is not listed, right-click on the *ASC Servers* object and select *Add*, enter the name of the server, the root user's ID and password.

When you connect to a server, you may see a dialog box notifying you of new devices attached to the server.  Here, you will see all devices that are either unassigned or reserved devices. At this point you can either prepare the device (reserve it for a virtual, direct, or service enabled device) and/or create a logical resource.

Note: Multiple administrators can access a server at the same time.  Changes to the server's configuration are saved on a first-come, first-served basis.

The ASC Management Console remembers the ASC Servers to which the Console has successfully connected. If you close and restart the Console, the ASC Servers will still be displayed in the tree but you will not be connected to them.

If this is the first time you are using the ASC Management Console after installation, you should add at least one administrator account.

Right-click on the server name and select *Administrators* to add ASC administrators.

## ASC Management Console User interface

The ASC Management Console displays the configuration for the ASC Servers on your storage network. The information is organized in a familiar Explorer-like tree view.
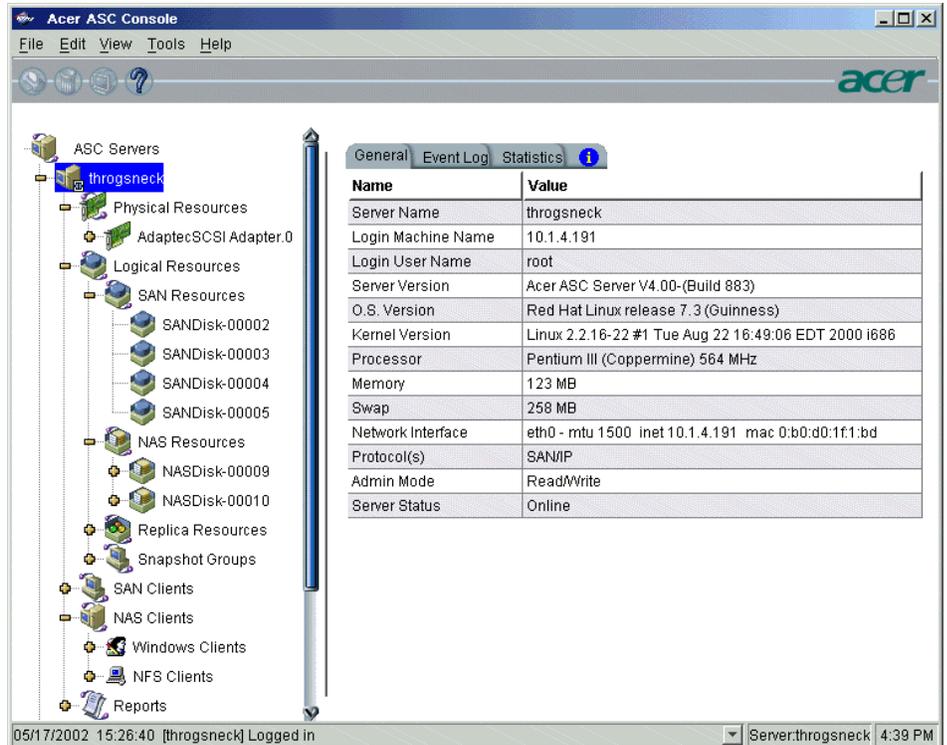


The tree allows you to navigate the various ASC Servers and their configuration objects. You can expand or collapse the display to show only the information that you wish to view.

- To expand an item that is collapsed, you can click on the symbol.

- To collapse an item, click on the symbol next to the item. Double-clicking on the item will also toggle the expanded/collapsed view of the item.

You need to connect to a server before you can expand it.

When you highlight any object in the tree, the right-hand pane contains detailed information about the object. You can select one of the tabs for more information.

The Console log located at the bottom of the window displays information about the local version of the Console. The log features a drop-down box that allows you to see activity from this Console session.

ASC Management Console information displays each object on the ASC Console's configuration tree has a corresponding informational display. These displays show the current configuration of the object and can also show health and performance statistics.

## ASC Server
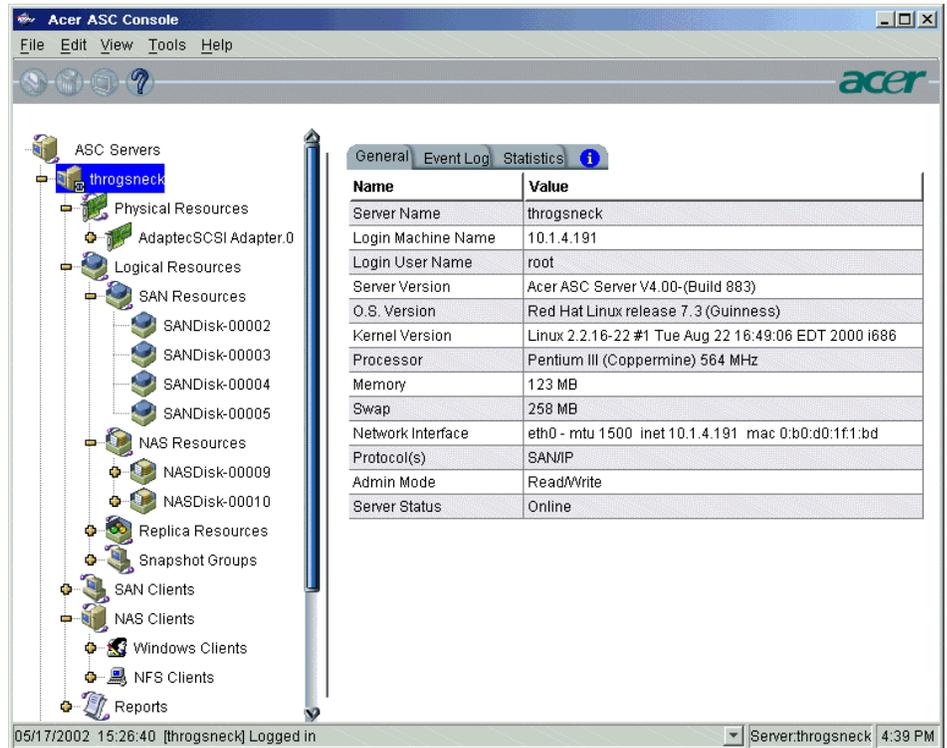


This display shows the configuration and status of the ASC Server. Configuration information includes the version of the ASC Server software and base operating system, the type and number of processors, amount of physical and swappable memory, supported protocols, and network adapter information.
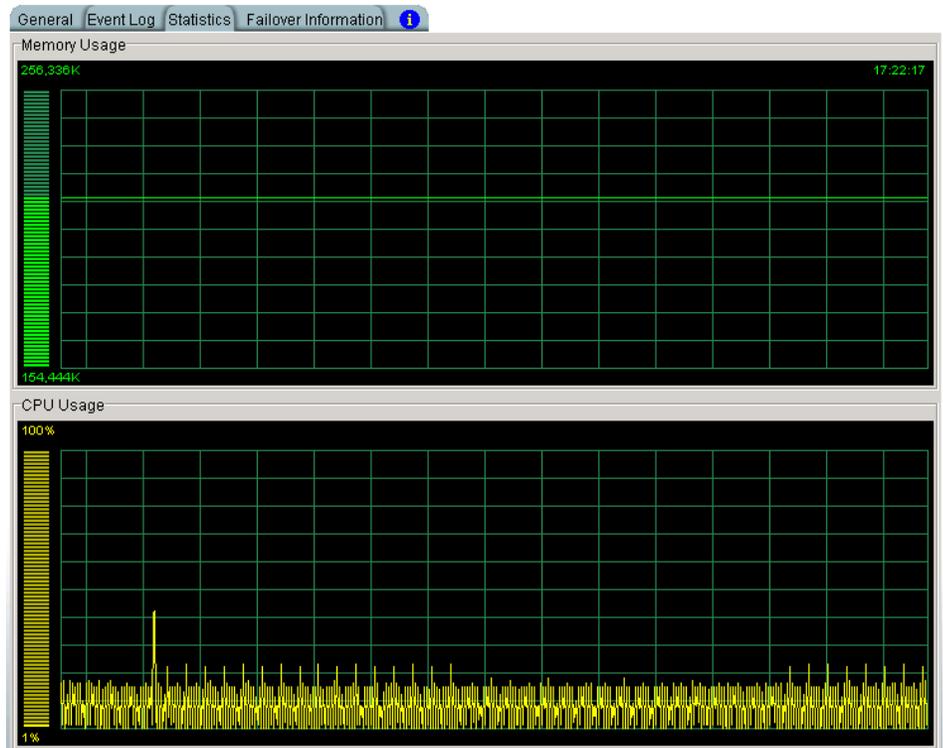
## Discovery ASC Servers

ASC can automatically discover all ASC Servers on your storage subnet.

- Select Tools --> Discover ASC
- Servers.
- Enter your network criteria.

## Server statistics

To display memory and CPU usage for a server, select the *Statistics* tab.



You can turn the statistics on/off by right-clicking on the server and selecting either *Statistics* --> *Start* or *Stop*.

- Open Tools

- Select prompted.

## Save & Restore an ASC Server configuration

ASC provides a convenient way to protect your ASC configuration. This is useful for disaster recovery purposes, such as when an ASC Server is down but you have the storage disks and want to use them to build a new ASC Server.

In this case, after importing all disks from the original server, you would restore your ASC configuration, including SAN and NAS client information and the names of your resources.

### Save configuration

You should save the configuration any time you change your configuration from the Console, including any time you add/change/delete a client or resource, assign a client, or make any changes to your mirroring configuration. If you add a server to a client from the Client Monitor (or via command line for Unix clients), you should also re-save your configuration.

To do this:

- Highlight an ASC Server in the tree.
- Select *File* menu --> *Save Configuration.*
- Select a filename and location.

**Restore configuration**

You can restore an ASC Server configuration from a file that was created using the *Save Configuration* option. This is for disaster recovery purposes and should not be used in day-to-day operation of the server. Changes made since the configuration was last saved will not be included in this restored configuration.

Warning: Restoring a configuration will overwrite existing virtual device and client configurations for that server. ASC partition information will not be restored. This feature should only be used if your configuration is lost or corrupted, as lost virtual devices can result in lost data for the clients using those virtual devices.

To restore the configuration:

- Import the disk(s) that were recovered from the damaged ASC Server to your new ASC Server.

- Refer to Import a disk for more information.

- Highlight the new ASC Server in the tree.
  Note: Do not make any changes to the server before restoring the configuration. For example, do not enable NAS before restoring, even if this server previously used NAS.

- Select *File* menu --> *Restore Configuration.*

- Confirm and locate the file that was saved.

- The ASC Server will be restarted.

## Licensing

When you first install ASC, you are given a 45-day live trial period. After that period, you must purchase ASC and its options to continue using the product. To license ASC:

- Obtain your ASC keycode(s) from Acer or its representatives.

- In the Console, right-click on the server and select *License*.
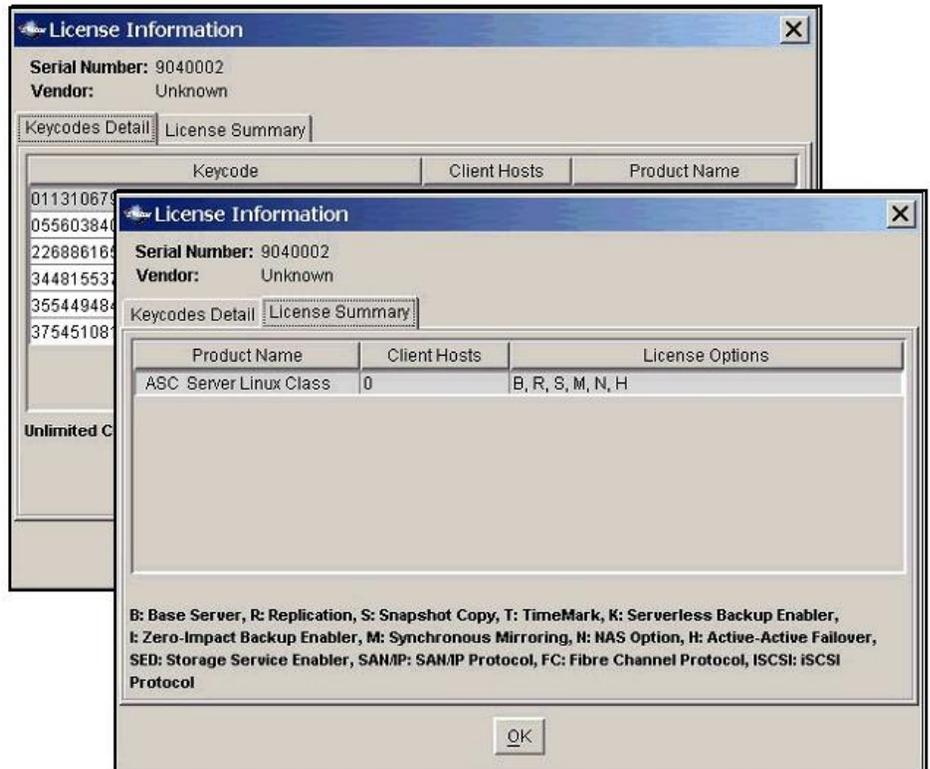


- The *License Summary* window is informational only and displays a list of the options supported for this server. You can enter keycodes for your purchased options on the *Keycode Detail* window.

- Press the *Add* button on the Keycodes Detail window to enter each keycode.

## Set Server Properties

To set properties for a specific server:

- Right-click on the server and select *Properties*.
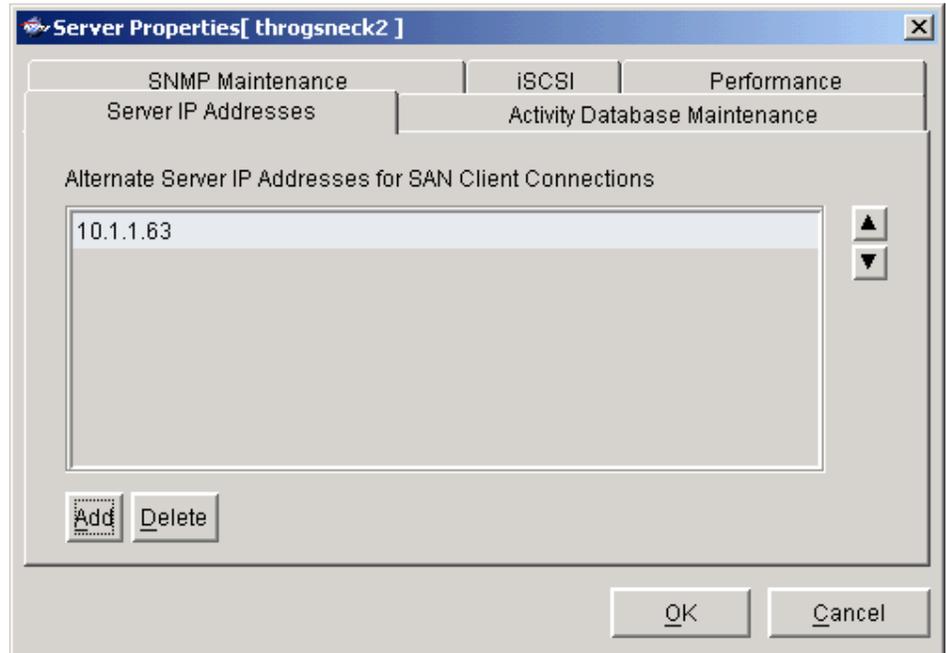


The tabs you see will depend upon your ASC configuration.

- If you have multiple NICs (network interface cards) in your server, enter the IP addresses using the *Server IP Addresses* tab. If the first IP address stops responding, the ASC clients will attempt to communicate with the server using the other IP addresses you have entered in the order they are listed.

Notes:
- In order for the clients to successfully use an alternate IP address, your subnet must be set properly so that the subnet itself can redirect traffic to the proper alternate adapter.

You <u>cannot assign two or more NICs within the same subnet</u>.

- The client becomes aware of the multiple IP addresses when it initially connects to the server. Therefore, if you add additional IP addresses in the Console while the client is running, you must rescan devices (Windows clients) or restart the client (Linux/Unix clients) to make the client aware of these IP addresses.

- On the *Activity Database Maintenance* tab, indicate how often the SAN data should be purged.
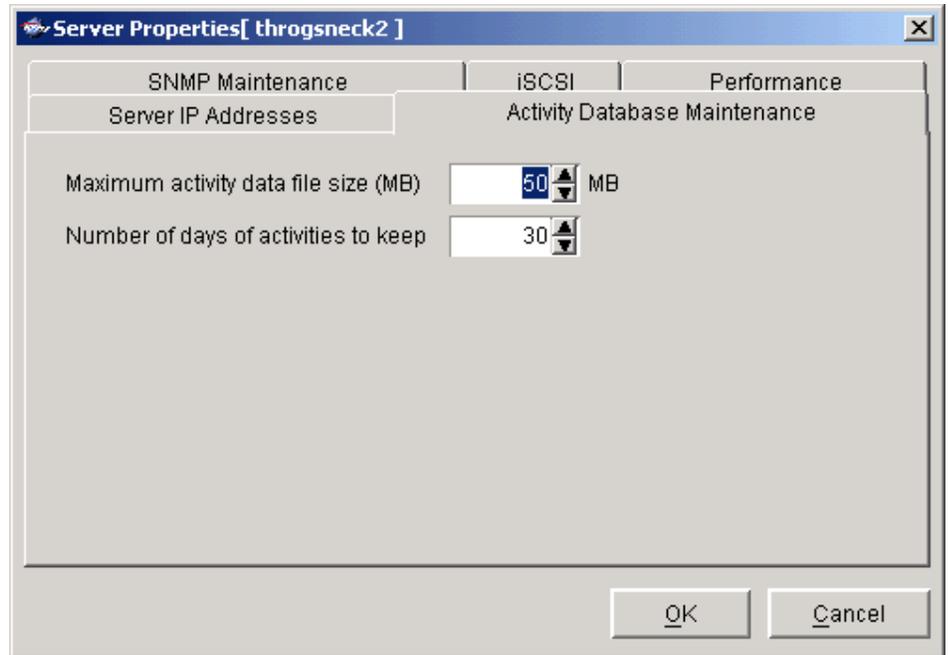


The Activity Log is a database that tracks all system activity, including all data read, data written, number of read commands, write commands, number of errors etc. This information is used to generate SAN information for the ASC reports.

To set limits for NAS information, right-click on *Windows Clients* and select *Properties*.

- On the *SNMP Maintenance* tab, indicate which types of messages should be sent as traps to your SNMP manager
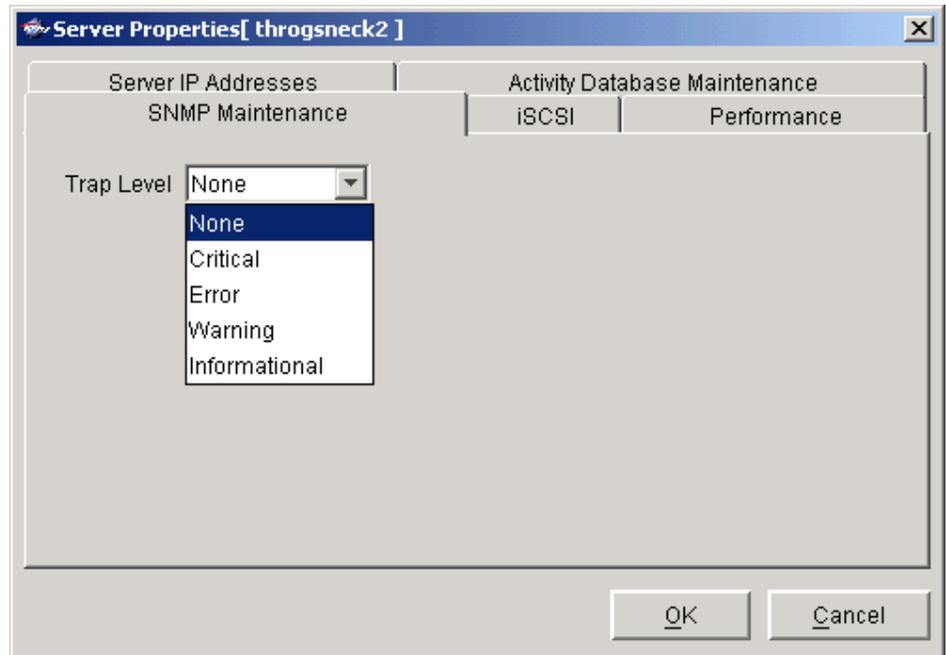


Five levels are available:

- o None – (Default) No messages will be sent.

- o Critical - Only critical errors that stop the system from operating properly will be sent.

- o Error – Errors (failure such as a resource is not available or an operation has failed) and critical errors will be sent.

- o Warning – Warnings (something occurred that may require maintenance or corrective action), errors, and critical errors will be sent.

- o Informational – Informational messages, errors, warnings, and critical error messages will be sent.

- On the *iSCSI* tab, iSCSI users can change the port number.
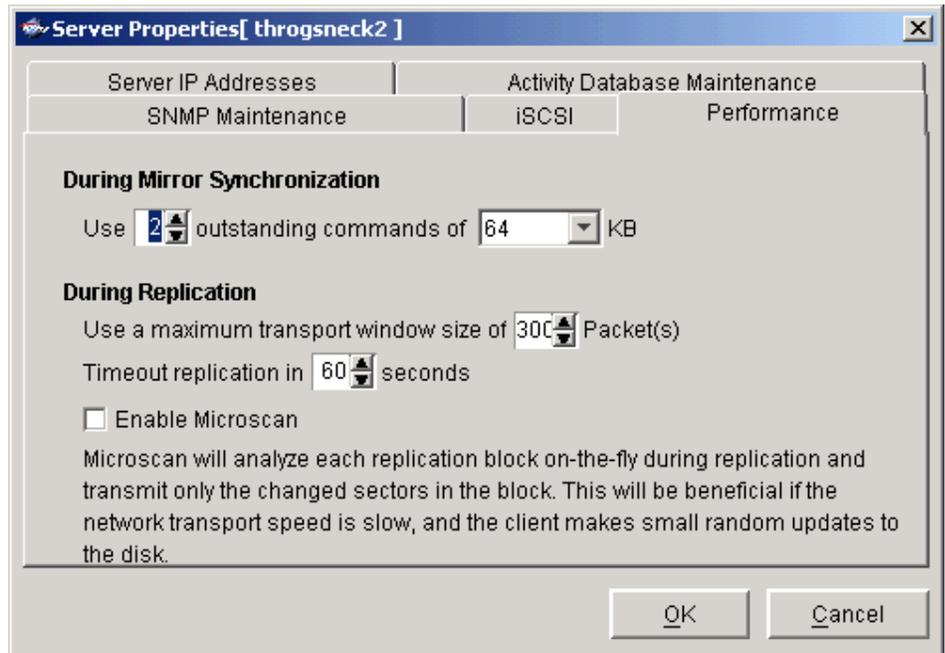


The settings on this tab affect system performance during mirror resynchronization and replication. The defaults should be optimal for most configurations. You should only need to change the settings for special situations, such as if your mirror is remotely located.

*During mirror resynchronization: Use [2] outstanding commands of [64] KB* - The number of commands being processed at one time and the I/O size. This must be a multiple of the sector size.

*Use a maximum transport window size of [ 300] packets* - Maximum transport window size.

*Timeout replication in [60] seconds* – indicates when timeout occurs.

*Enable Microscan* - Microscan analyzes each replication block on-the-fly during replication and transmits only the changed sectors in the block. This is beneficial if the network transport speed is slow and the client makes small random updates to the disk.
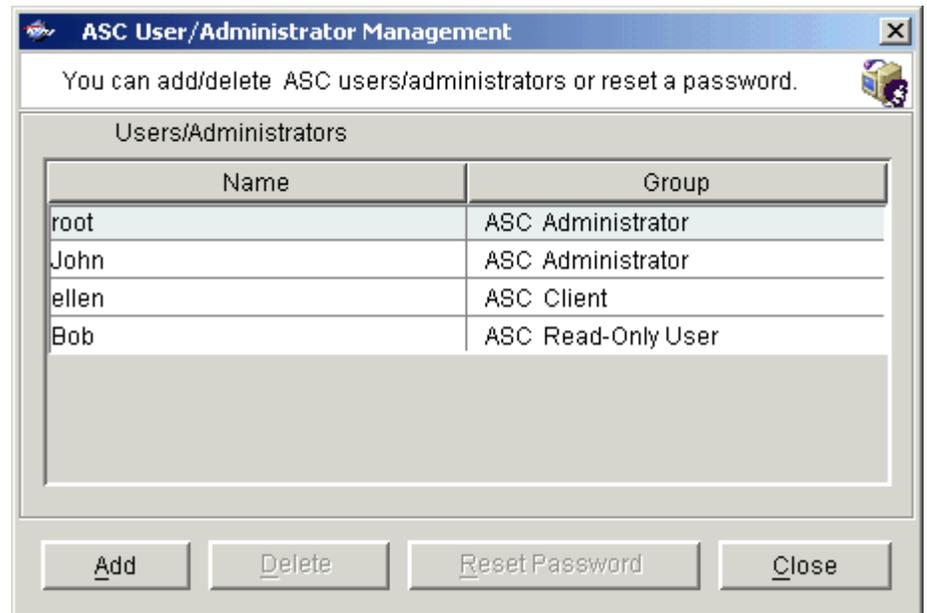
**Note:** *replication is not supported under ASC 4.0 Express.*

## Manage Administrators accounts & Password

**Manage accounts**

To set properties for a specific server:

- Only the root user can add or delete an ASC administrator or change an administrator's password.

- Right-click on the server and select *Administrators*.



There are several types of administrators:

- *ASC Administrators* are authorized for ASC client authentication and Console access.

- *ASC Clients* are authorized for ASC client authentication only. They do not have Console access. For ASC client authentication, the *Administrator Name* field must match the host name of the client. For example, if the client's hostname is ABC, the *Administrator Name* field must be ABC.

- *ASC Read-Only Users* are only permitted to view information in the Console. They are not authorized to make changes and they are not authorized for ASC client authentication.

- *ASC iSCSI Users* are used for iSCSI protocol login authentication (from iSCSI initiator machines). They do not have Console access.

Select the appropriate option.

When you add an administrator, the name must adhere to the naming convention of the operating system running on your ASC Server. Refer to your operating system's documentation for naming restrictions.

You cannot delete the root user or change the root user's password from this screen.  Use the *Change Password* option below.

**Change your administrator password**

This option lets you change your own ASC password if you are currently connected to a server.

- Right-click on the server and select *Change Password*

- Enter your old password, the new one, and then re-enter it to confirm.

## System Maintenance

The ASC Management Console gives you a convenient way to perform system maintenance for your ASC Server.

Note: The system maintenance options are hardware-dependent. Refer to your hardware documentation for specific information.

Deactivate system partition
Right-click on a server and select *System Maintenance --> Deactivate System Partition* to deactivate the system partition. You might want to do this if your existing partition is too small and you want to recreate it. After deactivating the system partition, the server will be restarted.

### Network configuration

- Right-click on a server and select *System Maintenance --> Network Configuration*.
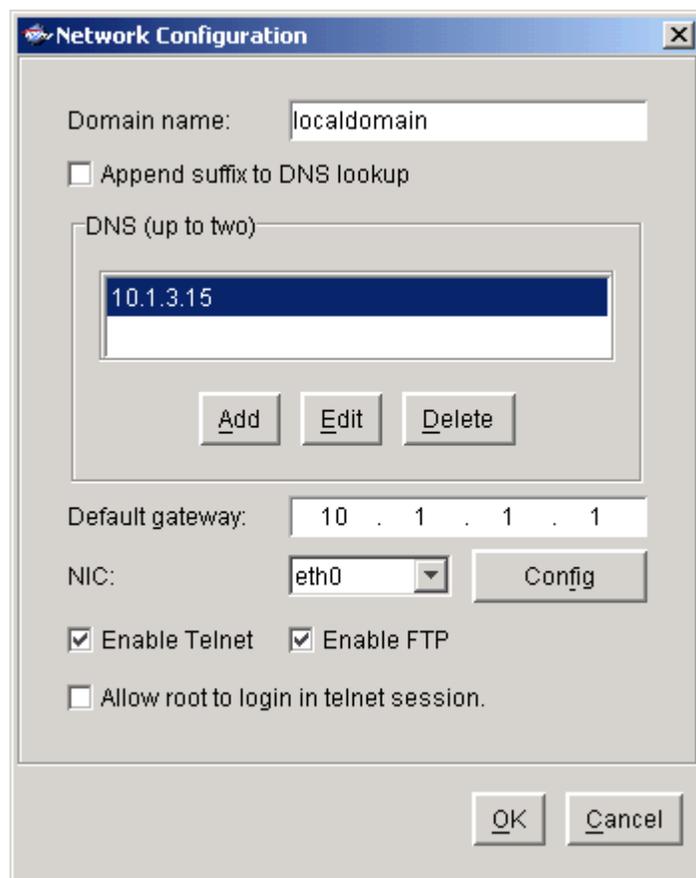
*Domain name* - Internal domain name.

*Append suffix to DNS lookup* - If a domain name is entered, it will be appended to the machine name for name resolution.

*DNS* - IP address of your DNS server.

*Default gateway* - IP address of your default gateway.

*NIC* - List of Ethernet cards in the server.

*Enable Telnet* - Enable/disable the ability to Telnet into the server.

*Enable FTP* - Enable/disable the ability to FTP into the server.

*Allow root to log in to telnet session* - Log in to your telnet session using root.

Click *Config* to configure each Ethernet card.



If you select Static, you must add addresses and net masks. Acer recommends using the Static IP address setting for NAS 700.

*MTU* - Set the maximum transfer unit of each IP packet.  If your card supports it, set this value to 9000 for jumbo frames.

Jumbo Frame Definition

In 1998, Alteon Networks, Inc. promoted an initiative to increase the maximum size of the MAC Client Data field from 1500-bytes to 9000-bytes.
Larger frames would provide a more efficient use of the network bandwidth while reducing the number of frames that have to be processed.

Software update

Right-click on a server and select *System Maintenance* --> *Software Update* to locate a software package that you can update.  This option is only valid for ASC embedded appliances.

Set hostname

Right-click on a server and select *System Maintenance* --> *Set Hostname* to change your hostname.  You must restart the server if you change the hostname.

Restart ASC

Right-click on a server and select *System Maintenance* --> *Restart ASC* to restart the Server processes.

Restart network

Right-click on a server and select *System Maintenance* --> *Restart Network* to restart your local network configuration.
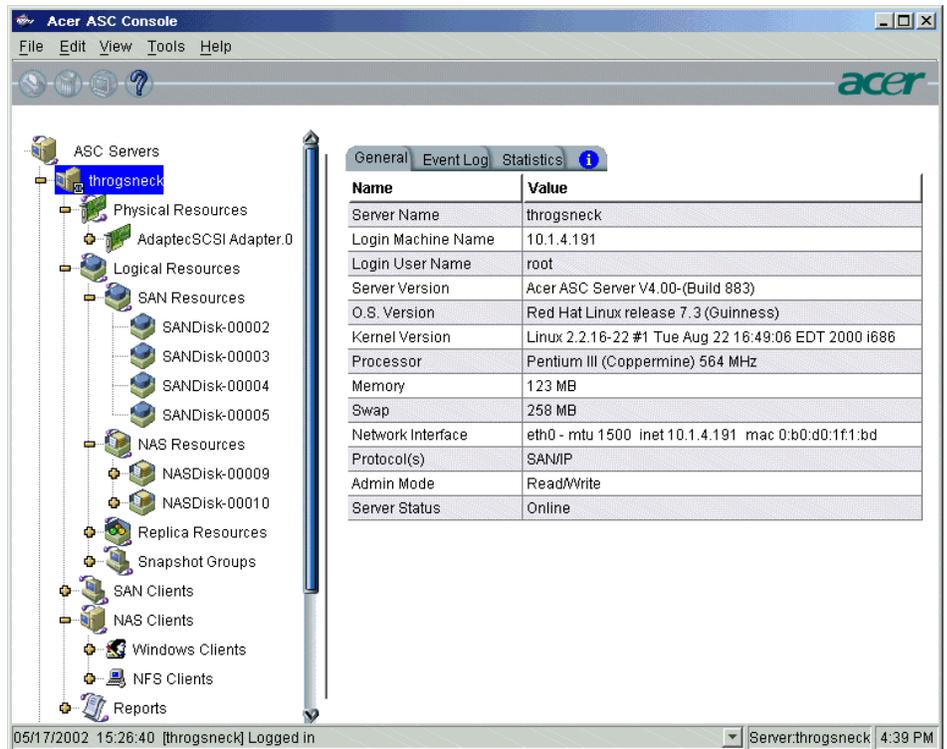
Reboot

Right-click on a server and select *System Maintenance* --> *Reboot* to reboot your server.

Halt

Right-click on a server and select *System Maintenance* --> *Halt* to turn off the server without restarting it.

## Physical resource



When you highlight *Physical Resources*, the right-hand pane displays the SCSI addresses (comprised of adapter number, channel number, SCSI ID, LUN) of your devices. The *SCSI adapters* tab displays the adapters attached to this server and the *SCSI Devices* tab displays the actual SCSI devices attached to this server. These devices can include hard disks, tape drives, device libraries, JBOD and RAID cabinets.

Note that some multi-channel SCSI adapters may appear as multiple adapters. In addition, depending upon how many paths there are to a device, it is possible to see the same device listed multiple times before it is virtualized. Once the device is virtualized, ASC will discover the aliases and will display the device only once.

When you highlight a physical device, the *Category* field in the right-hand pane describes how the device is being used.  Possible values are:

Reserved for virtual device - A hard disk that has not yet been assigned to a SAN/NAS Resource or Snapshot area.

Used by virtual device(s) - A hard disk that is being used by one or more SAN/NAS Resources or Snapshot areas.

Reserved for direct device - A SCSI device, such as a hard disk, tape drive or library that has not yet been assigned as a SAN Resource.

Used in direct device - A directly mapped SCSI device, such as a hard disk, tape drive or library, that is being used as a direct device SAN Resource.

Reserved for service enabled device - A hard disk with existing data that has not yet been assigned to a SAN/NAS Resource.

Used by service enabled device - A hard disk with existing data that has been assigned to a SAN/NAS Resource.

Unassigned - A physical resource that has not been reserved yet.

Not available for ASC - A miscellaneous SCSI device that is not used by ASC (such as a scanner or CD-ROM).

System - A hard disk where system partitions exist and are mounted (i.e. swap file, file system installed, etc.).

Reserved for Striped Set - Used in a disk striping configuration.

## Prepare devices to become logical resources

You can use one of ASC's disk preparation options to change the category of a device.  This is important to do if you want to create a logical resource using a device that is currently *unassigned*.

The ASC Server detects new devices when you connect to it. When they are detected you will see a dialog box notifying you of the new devices.  At this point you can highlight a device and press the *Prepare Disk* button to prepare it.

At any time, you can prepare a single unassigned device by doing the following: Highlight the device, right-click, select *Properties* and select the device category. (You can find all unassigned devices under the *Physical Resources/Adapters* node of the tree view.)

For multiple unassigned devices, highlight *Physical Resources*, right-click and select *Prepare Disks*. This launches a wizard that allows you to virtualize, unassign, or import multiple devices at the same time.

## SCSI aliasing

With ASC, you can eliminate a potential point of failure in your storage network by providing multiple paths to your storage devices using multiple Fibre Channel switches and/or multiple adapters and/or storage devices with multiple controllers. In a multiple path configuration, ASC automatically detects all paths to the storage devices. If one path fails, ASC automatically switches to another.

If you have multiple paths to your Fibre Channel hardware, you can use the *Alias* feature to select the primary path and the order for using the other paths. This can be useful for load balancing purposes as well.

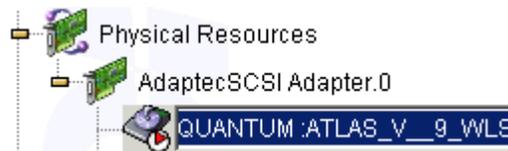Right-click on a physical device and select *Alias*.

The device must be virtualized and you must have rescanned physical devices at some point to discover the aliases.

Use the up and down arrows to put the devices in the order you want to use them.

The secondary paths will only be used in the event of a storage path failure.
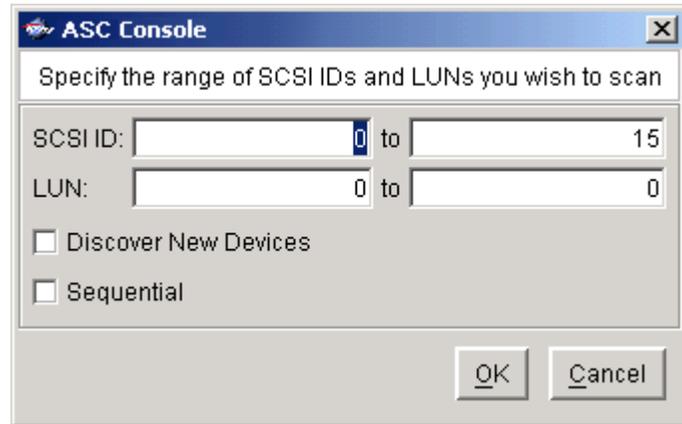
## Rename a SCSI device

You can rename a SCSI device, by right-clicking on the device and selecting *Rename*.



Type the new name and press *Enter*.

## Rescan adapters

To rescan all adapters and search for new devices, right-click on *Physical Resources* and select *Rescan*.



(Linux only) If you only want to scan a specific adapter, right-click on that adapter and select *Rescan*.

Set the range of SCSI IDs and LUNs that you want to scan.

For Linux, the *Sequential* option works in conjunction with the LUN range. You should only use it if all of your devices are numbered sequentially, because scanning will stop once the last sequential device is found. If you do not select *Sequential*, ASC will continue scanning to the ending LUN number specified.

Determine if you want to discover new devices.

If you want ASC to discover new devices as well as rescan existing devices, be sure to select the *Discover New Devices* option. If selected, you should enter a SCSI ID range. It is not needed if you are only rescanning existing devices.

## Import a disk

You can import a 'foreign' disk into an ASC Server. A foreign disk is a virtualized physical device containing ASC logical resources previously set up on a different ASC server. You might need to do this if an ASC Server is damaged and you want to import the server's disks to another ASC Server.

When you right-click on a disk that ASC recognizes as 'foreign' and select the *Import* option, ASC scans the disk's partition table. ASC then tries to reconstruct the virtual drive out of all of the segments.

If the virtual drive was constructed from multiple disks, you can highlight *Physical Resources*, right-click and select *Prepare Disks*. This launches a wizard that allows you to import multiple disks at the same time.

As each drive is imported, ASC marks the drive 'offline' because it has not yet found all of the segments. Once all of the disks that were part of the virtual drive have been imported, ASC re-constructs the virtual drive and marks it 'online'.

Importing a disk preserves the data that was on the disk but does not preserve the client assignments. Therefore, after importing, you must either reassign clients to the resource or use the <u>Restore configuration</u> option.

Note: The GUID (Global Unique Identifier) is the permanent identifier for each virtual device. When you import a disk, the virtual ID, such as *SANDisk-00002*, may be different from the original server. Therefore, you should use the GUID to identify the disk.
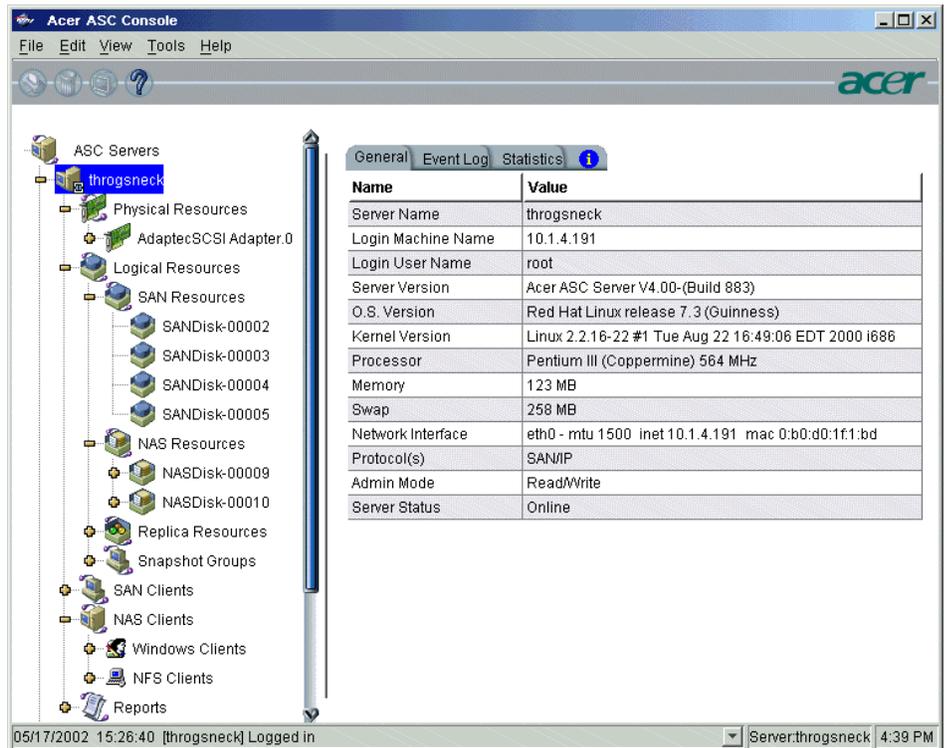
## SCSI device throughput

To check the throughput for a SCSI device:

Right-click on the device (under *Physical Resources*).

Select *Test* from the menu.

The system will test the device and then display the throughput results on the screen.

## Logical Resources



Logical resources are all of the resources defined on the ASC Server, including SAN Resources, NAS Resources, Replica Resources, and Snapshot Groups.

SAN and NAS logical resources consist of sets of storage blocks from one or more physical hard disk drives. This allows the creation of logical resources that contain a portion of a larger physical disk device or an aggregation of multiple physical disk devices.

Clients do not gain access to physical resources; they only have access to logical resources. This means that an administrator must configure each physical resource to one or more logical resources so that they can be assigned to the clients.

When you highlight a SAN or NAS Resource, you will see a small icon next to each device that is being used by the resource.
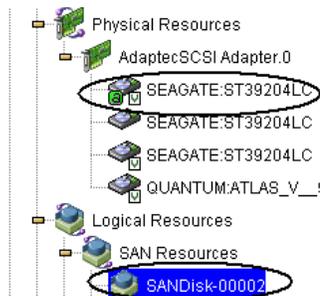
In addition, when you highlight a SAN or NAS Resource, you will see a *GUID* field in the right-hand pane.

| Status | Online |
|---|---|
| Virtual ID | 2 |
| GUID | d5823224-2096-d048-d64f-00ec670eaf9a |
| Write Cache | Disabled |

The GUID (Global Unique Identifier) is the permanent identifier for this virtual device.  The virtual ID, *SANDisk-00002*, is not. You should make note of the GUID, because, in the event of a disaster, this identifier will be important if you need to rebuild your system and import this disk.

Replica Resources are replica disks that are being used by a remote server.

Snapshot groups are groups of drives (virtual drives and service enabled drives) that will be grouped together for snapshot synchronization purposes. When one drive in the group is to be replicated or backed up, the entire group will be snapped together to maintain a consistent image.

## Write caching

You can leverage a third party disk subsystem's built-in caching mechanism to improve I/O performance. Write caching allows the third party disk subsystem to utilize its internal cache to accelerate I/O.

To write cache a resource, right-click on it and select *Write Cache --> Enable*.

## ASC SAN Clients
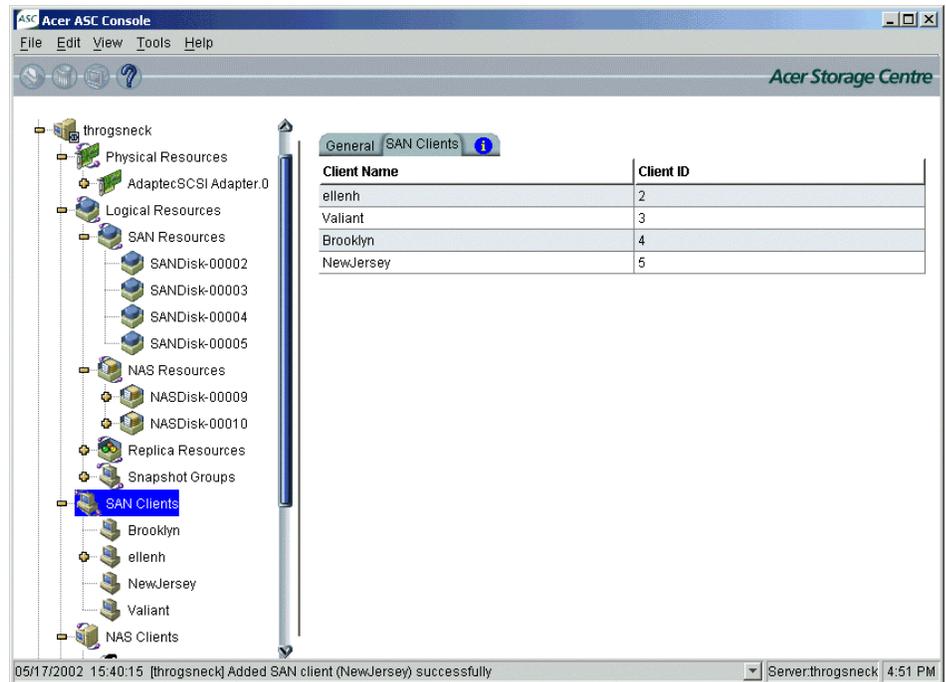


ASC SAN Clients are the actual file and application servers that utilize the storage resources via the ASC Server.

These SAN Clients access their storage resources via software-emulated virtual adapters (for SAN/IP) . The storage resources appear as locally attached devices to the SAN Clients' operating systems (Windows NT, Windows 2000, Linux, Solaris, etc.) even though the SCSI devices are actually located at the ASC Server.

When you highlight a specific SAN client, the right-hand pane displays the Client ID, type, and authentication status, as well as information about the client machine.

Note: From the Console you can add SAN clients so you can start allocating resources to the clients. This is called the authorization process. However, for SAN/IP clients, even when the clients are added, you still need to go to the client host to install the client software and authenticate to the server, using the proper username/password. That establishes the authentication credential for all subsequent operation. Until that is done, the console will show that the client is not authenticated.  To authenticate, you must add the server to the client. For Windows clients, you can use the Add Server option in the SAN Client Monitor. For Linux, Solaris, AIX, and HP-UX clients, you can execute ./sanclient monitor from /usr/local/sanclient/bin.

The *Resources* tab displays a list of SAN Resources that are allocated to this client. The adapter, SCSI ID and LUN are relative to this ASC SAN client only; other clients that may have access to the SAN Resource may have different adapter SCSI ID and LUN information.

### Change the ACSL

You can change the ACSL (adapter, channel, SCSI, LUN) for a SAN Resource assigned to a SAN client if the device is not currently attached to the client. To change, right-click on the SAN Resource under the SAN Client object (you cannot do this from the *SAN Resources* object) and select *Properties*. You can enter a new adapter, SCSI ID, or LUN.

Notes for Windows clients:

One SAN Resource for each Windows SAN client must have a LUN of 0. Otherwise, the operating system will not see the devices assigned to the SAN client.

If you reassign a different device with the same LUN, you must restart the SAN Client Monitor in order to access the newly assigned device.

## ASC NAS Clients
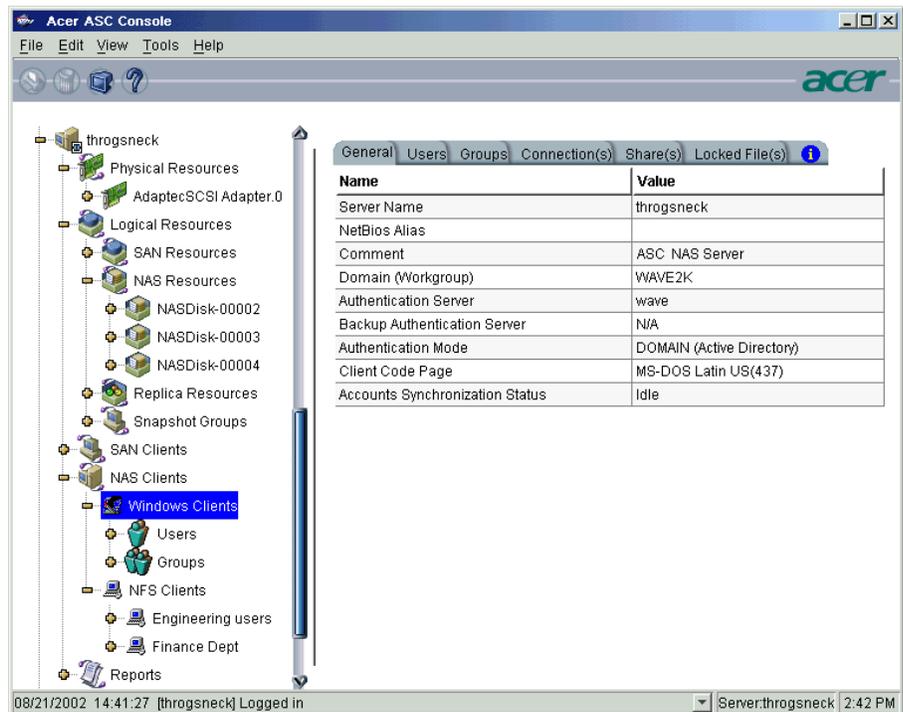


ASC NAS Clients are the users and groups that access NAS resources via the ASC Server. There are two types of NAS clients you will see:

- Windows clients - These clients use the Common Internet File System (CIFS) protocol to work together and share documents. Because many operating systems support CIFS, it is possible to have clients using other operating systems listed as Windows clients.

- NFS clients - These clients are usually Unix clients using the Network File System (NFS) protocol.

You will only see *Users* and *Groups* under *Windows Clients* if the NAS authentication mode is *Server* or *Domain*. If the authentication mode is *Share*, you will not see any users listed because there is no authentication server and any Windows client can access a share (provided he/she knows the password).

If the authentication mode is *Server*, you will only see groups if the authentication server is a Primary Domain Controller (PDC)/Domain Controller.

To update the list of users/groups, right-click on the *Windows Clients* object and select *Refresh Windows Clients*.

Information on the *Connection(s), Share(s),* and *Locked File(s)* tabs is updated every few seconds.  You can set the interval by right-clicking on the *Windows Clients* object and selecting *Start Connection Status Refresh*.

Refer to <u>'NAS Configuration'</u> for more information about NAS and authentication modes for Windows clients.

## Console Options

**To set options for the Console:**

Select *Tools --> Console Options*.
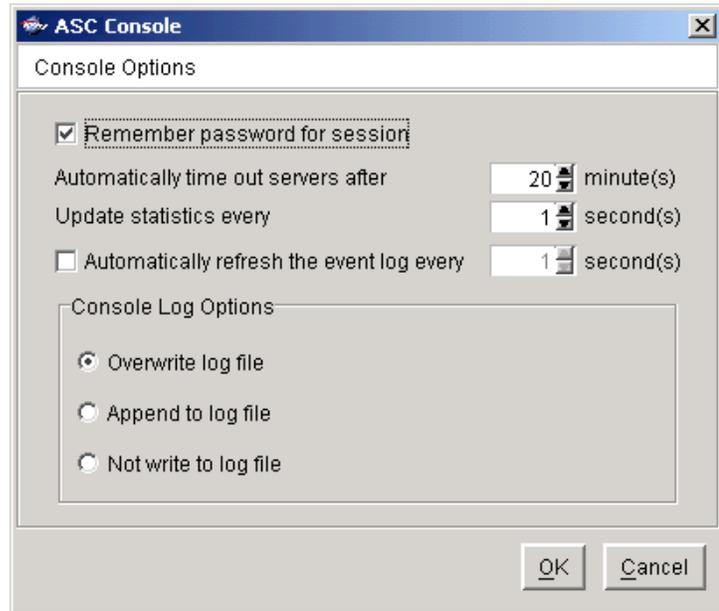


Make any necessary changes.

*Remember password for session* - If the Console is already connected to a server, when you attempt to open a second, third, or subsequent server, the Console will use the credentials that were used for the last successful connection. If this option is unchecked, you will be prompted to enter a password for every server you try to open.

*Automatically time out servers after nn minute(s)* - The Console will collapse a server that has been idle for the number of minutes you specify. If you need to access the server again, you will have to reconnect to it. The default is 10 minutes.

*Update statistics every nn second(s)* - The Console will update statistics by the frequency you specify.

Automatically refresh the event log every nn second(s) - The Console will update the event log by the frequency you specify, only when you are viewing it.

Console Log Options - The Console log (ipstorconsole.log) is kept on the local machine and stores information about the local version of the Console. The Console log is displayed at the very bottom of the Console screen.

| | |
|---|---|
| 05/17/2002 15:40:15 [throgsneck] Added SAN client (NewJersey) successfully | ▼ Server:throgsneck 5:02 PM |
| 05/17/2002 15:40:15 [throgsneck] Added SAN client (NewJersey) successfully | |
| 05/17/2002 15:40:09 [throgsneck] Added SAN client (Brooklyn) successfully | |
| 05/17/2002 15:40:02 [throgsneck] Added SAN client (Valiant) successfully | |
| 05/17/2002 15:26:40 [throgsneck] Logged in | |
| 05/17/2002 15:26:34 [throgsneck] Logged out | ▼ |

The options affect how information for each Console session will be maintained:

Overwrite log file - Overwrite the information from the last Console session when you start a new session.

Append to log file - Keep all session information.

Do not write to log file - Do not maintain a Console log.
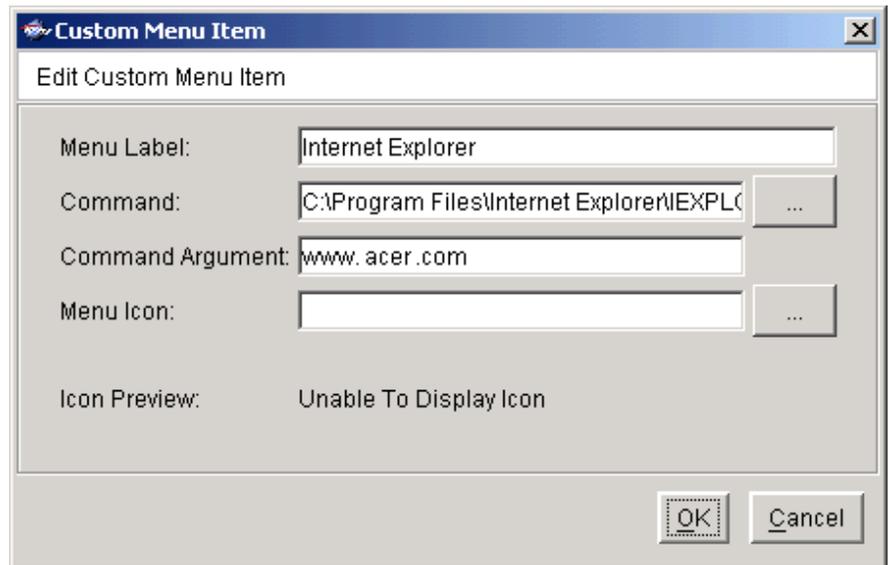
**Create custom menu**

You can create a menu in the ASC Management Console from which you can launch external applications. This can add to the convenience of ASC's centralized management paradigm by allowing your administrators to start all of their applications from a single place. The *Custom* menu will appear in your Console along with the normal menu (between *Tools* and *Help*).

To create a custom menu:
Select *Tools* --> *Set up Custom Menu*.
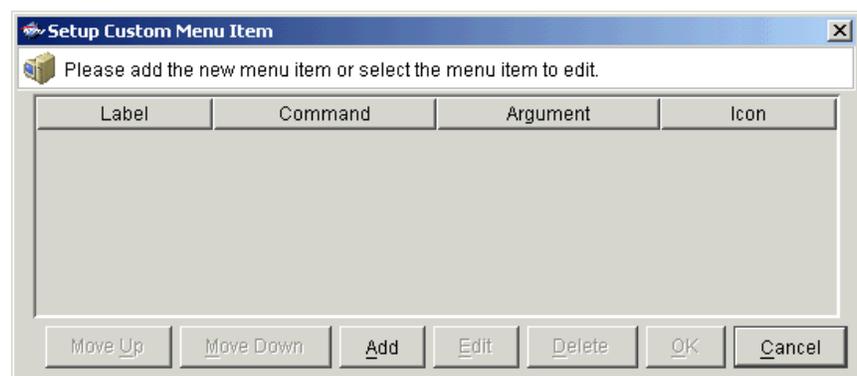


Click *Add* and enter the information needed to launch this application.

*Menu Label* - The application title that will be displayed in the *Custom* menu.

*Command* - The file (usually an.exe) that launches this application.

*Command Argument* - An argument that will be passed to the application. If you are launching an Internet browser, this could be a URL.

*Menu Icon* - The graphics file that contains the icon for this application. This will be displayed in the *Custom* menu.

## CONFIGURE ASC SAN RESOURCES

Once you have physically attached your physical SCSI/Fibre Channel devices to your ASC Server you are ready to create SAN Resources to be used by your ASC SAN Clients. This configuration can be done entirely from the ASC Console.

Understanding how to create and manage SAN Resources is critical to a successful ASC storage network. Please read this section carefully before creating and assigning SAN Resources.

### SAN Resources

SAN Resources are logically mapped devices on the ASC Server. They are comprised of physical storage devices, known as *Physical Resources* in ASC. Physical resources are the actual SCSI and/or Fibre Channel devices attached to the server. These devices can be hard disks, tape drives, device libraries, JBODs and RAID cabinets.

Clients do not have access to physical resources; they have access only to SAN Resources. This means that physical resources must be defined as SAN (or NAS) Resources first, and then assigned to the clients so they can access them

When a SAN Resource is assigned to a client, a virtual adapter is defined for that client. The SAN Resource is assigned a virtual SCSI ID on the virtual adapter. This mimics the configuration of actual SCSI storage devices and adapters, allowing the operating system and applications to treat them like any other SCSI device.

There are three types of SAN Resources: virtual devices, direct devices, and service enabled devices.

### Virtual Devices

ASC has the ability to aggregate multiple physical storage devices (such as JBODs and RAIDs) of various interface protocols (such as SCSI or Fibre Channel) into logical *storage pools*. From these storage pools, virtual devices can be created and provisioned to application servers and end users. This is called *storage virtualization*.

Virtual devices are defined as sets of storage blocks from one or more physical hard disk drives. This allows the creation of virtual devices that can be a portion of a larger physical disk drive, or an aggregation of multiple physical disk drives.

Virtual devices offer the added capability of disk expansion. Additional storage blocks can be appended to the end of existing virtual devices without erasing the data on the disk.

Virtual devices can only be assembled from hard disk storage. It does not work for CD-ROM, tape, libraries, or removable media.

When a virtual device is allocated to an application server, the server thinks that an actual SCSI storage device has been physically plugged into it.

Virtual devices are assigned to virtual adapter 0 (zero) when mapped to a client. If there are more than 15 virtual devices, a new adapter will be defined.
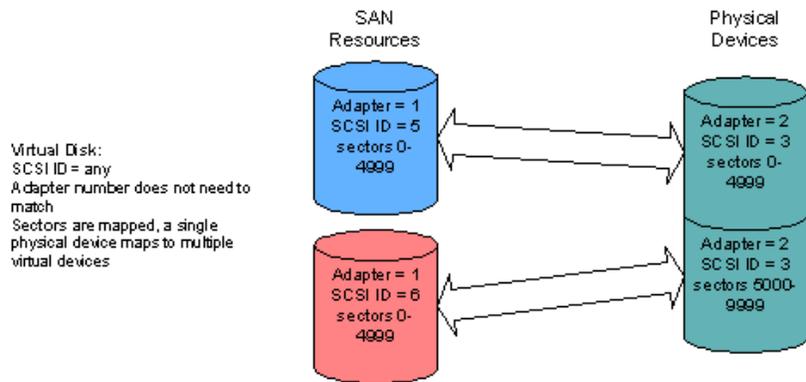
Note: We do not recommend storing system files, page files, swap files, etc. on ASC virtual devices.

**SAN Resources virtualization examples**

The following diagrams show how physical disks can be mapped into virtual devices.
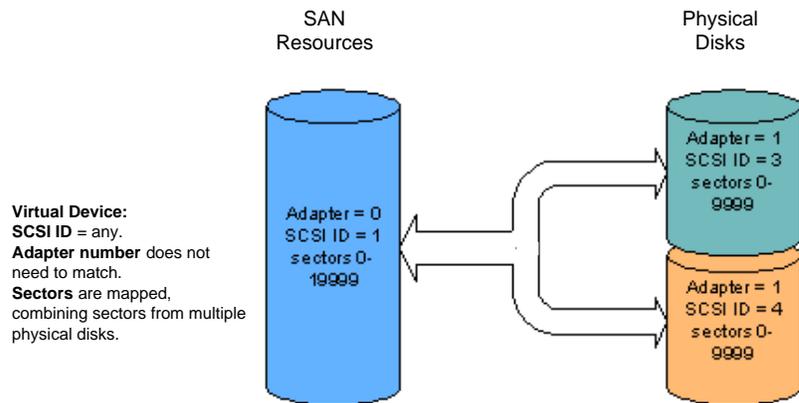


This diagram shows a virtual device being created out of two physical disks. This allows you to create very large virtual devices for application servers with large storage requirements. Also, if the storage device needs to grow, additional physical disks may be added to increase the size of a virtual device. Note that this will require that the client application server resize the partition and file system on the virtual device.

SAN Resources — Physical Devices

Virtual Disk:
SCSI ID = any
Adapter number does not need to match
Sectors are mapped, a single physical device maps to multiple virtual devices

Adapter = 1 SCSI ID = 5 sectors 0-4999

Adapter = 1 SCSI ID = 6 sectors 0-4999

Adapter = 2 SCSI ID = 3 sectors 0-4999

Adapter = 2 SCSI ID = 3 sectors 5000-9999

This example shows a single physical disk split into two virtual devices. This is useful when a single large device exists, such as a RAID, which could be shared among multiple client application servers.

Virtual devices can be created using various combining and splitting methods, although you will probably not create them in this manner in the beginning. You may end up with devices like this after growing virtual devices over time.

**Direct devices**

Direct devices are directly mapped SCSI devices. Direct devices can be created from hard disks, tape drives, device libraries, JBODs, and RAID cabinets.

Because they are not virtualized, direct devices cannot take advantage of ASC's advanced storage management options, such as mirroring or snapshot copy.

Direct devices, such as tape drives, device libraries, JBODs, and RAID cabinets, can be used to back up data on your storage network.

A characteristic of some application software, such as backup tools and devices, require that they address the SCSI ID directly. This is true for library devices and the drives within the library; the software uses the SCSI IDs to address the library and drives. For this reason, direct devices use fixed SCSI IDs that cannot be changed.

Designating a hard drive as a direct device can be useful for data migration into ASC.  Data on an existing disk can be brought into ASC as a direct device. The data can then be copied using Linux's dd command to a virtualized disk that does not contain any data or have any clients attached so that it can take advantage of ASC's virtualization and advanced storage management options.

**Service enabled devices**

Service enabled devices are hard drives with existing data that can be accessed by ASC to make use of all key ASC storage services (mirroring, snapshot, etc.), without any migration/copying, without any modification of data, and with minimal downtime. Service enabled devices are used to migrate existing drives into the SAN.

Because service enabled devices are preserved intact, and existing data is not moved, the devices are not virtualized and cannot be expanded. Service enabled devices are all maintained in a one-to-one mapping relationship (one physical disk equals one logical device). Unlike virtual devices, they cannot be combined or split into multiple logical devices.

## Procedure to create SAN resources

SAN Resources are created in the ASC Console.

Note: After you make any configuration changes, you must restart the client in order for the changes to take effect.  For Windows clients, if you add or delete SAN Resources you can use the Rescan option in the SAN Client Monitor instead.  For other changes, you will still need to restart the client. After you create a new virtual device, assign it to a client, and restart the client (or rescan), you will need to write a signature, create a partition, and format the drive so that the client can use it.

### Prepare devices to become SAN Resources

The ASC Server detects new devices when you connect to it. (You can also detect new devices by executing the *Rescan* command.)

You can use one of ASC's disk preparation options to change the category of a device.  This is important to do if you want to create a logical resource using a device that is currently *unassigned*.

- The ASC Server detects new devices when you connect to it (or when you execute the *Rescan* command). When they are detected you will see a dialog box notifying you of the new devices.  At this point you can highlight a device and press the *Prepare Disk* button to prepare it.

- At any time, you can prepare a single unassigned device by doing the following: Highlight the device, right-click, select *Properties* and select the device category. (You can find all unassigned devices under the *Physical Resources/Adapters* node of the tree view.)

- For multiple unassigned devices, highlight *Physical Resources*, right-click and select *Prepare Disks*. This launches a wizard that allows you to virtualize, unassign, or import multiple devices at the same time.
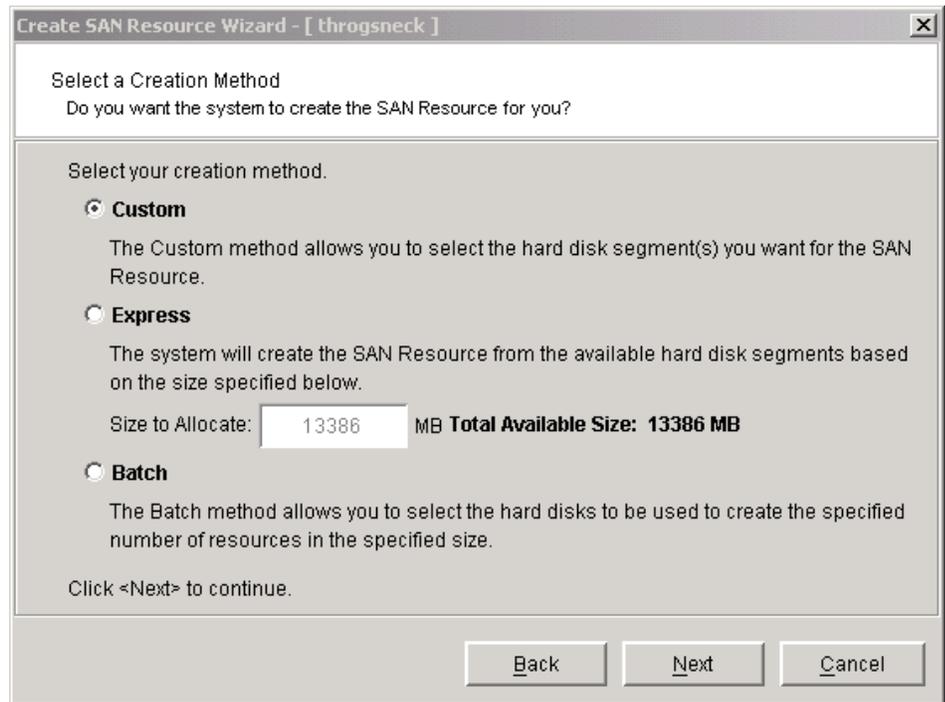
**Create a virtual device SAN Resources**

Note: Each ASC Server supports a <u>maximum of 1024 SAN Resources</u>.

Right-click on *SAN Resources* and select *New*.

Select *Virtual Device*.
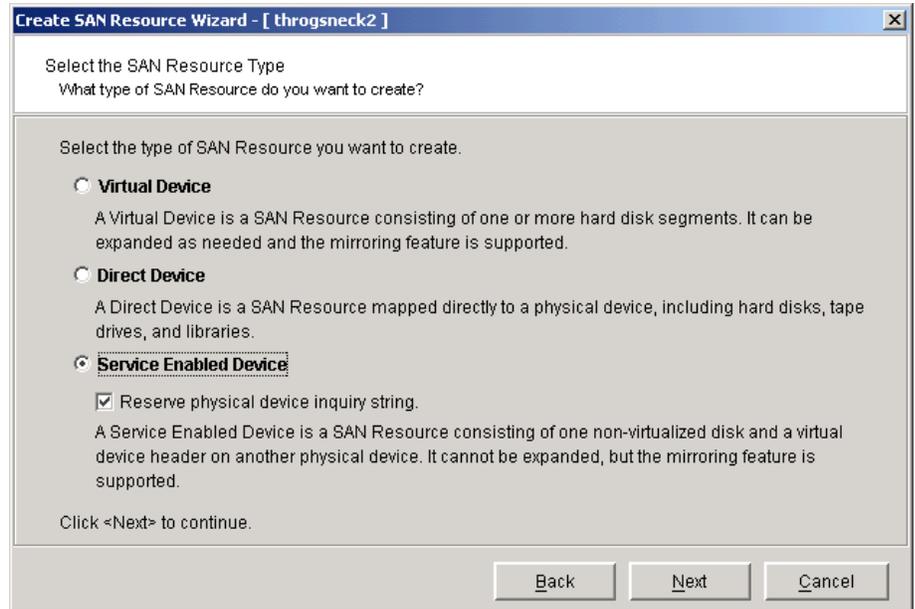
Select how you want to create this virtual device.



*Custom* lets you select which physical device(s) to use and lets you designate how much space to allocate from each.

*Express* lets you designate how much space to allocate and then automatically creates a virtual device using all available devices.

*Batch* lets you create multiple SAN Resources at one time. These SAN Resources will all be the same size.

If you select *Custom*, you will see the following windows:
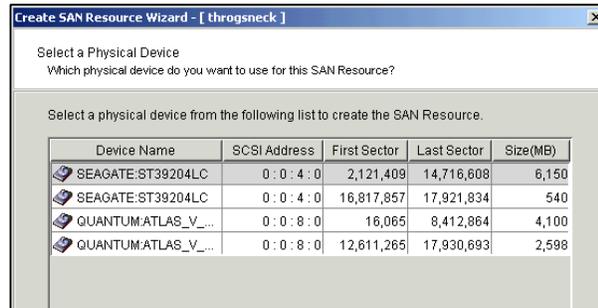


Select either an entirely unallocated or partially unallocated device.

Only one device can be selected at a time from this dialog. To create a virtual device SAN Resource from multiple physical devices, you will need to add the devices one at a time. After selecting the parameters for the first device, you will have the option to add more devices.
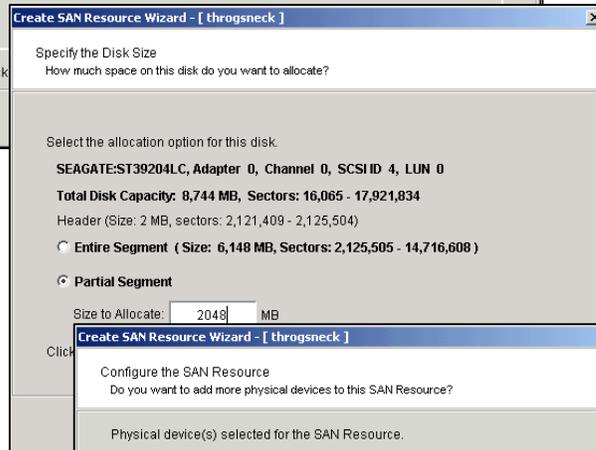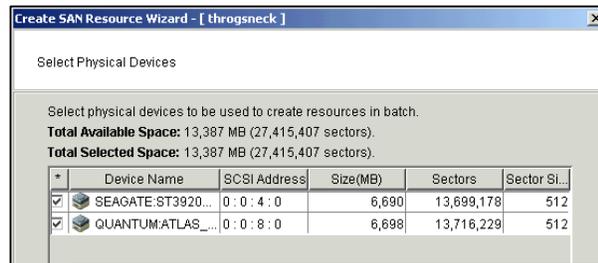
Indicate how much space to allocate from this device.

Click *Add More* if you want to add another physical device to this SAN Resource.
If you select to add more devices, you will go back to the physical device selection screen where you can select another device.

If you select *Batch*, you will see the following window:



Select either an entirely unallocated or partially unallocated device.
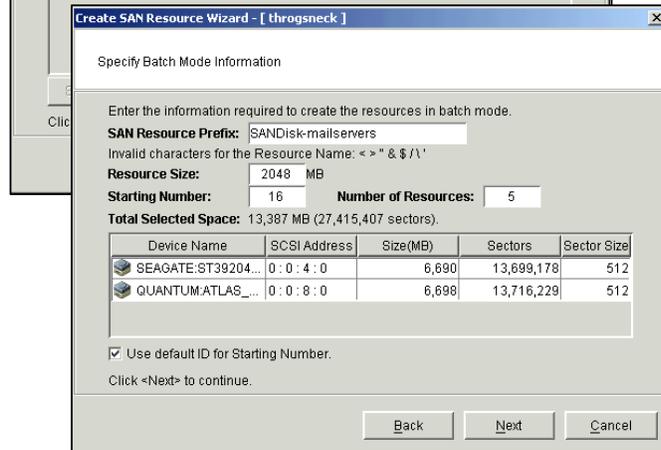
Indicate how to name each resource. The *SAN Resource Prefix* is combined with the *starting number* to form the name of each SAN Resource. You can uncheck the *Use default ID for Starting Number* option to restart numbering from one.

In the *Resource Size* field, indicate how much space to allocate for each resource.

Indicate how many SAN Resources to create in the *Number of Resources* field.
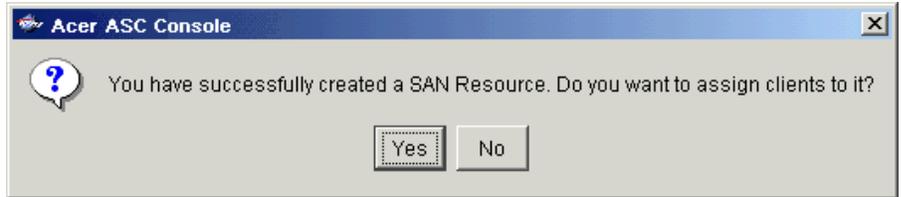
(*Express* and *Custom* only) Enter a name for the new SAN Resource.
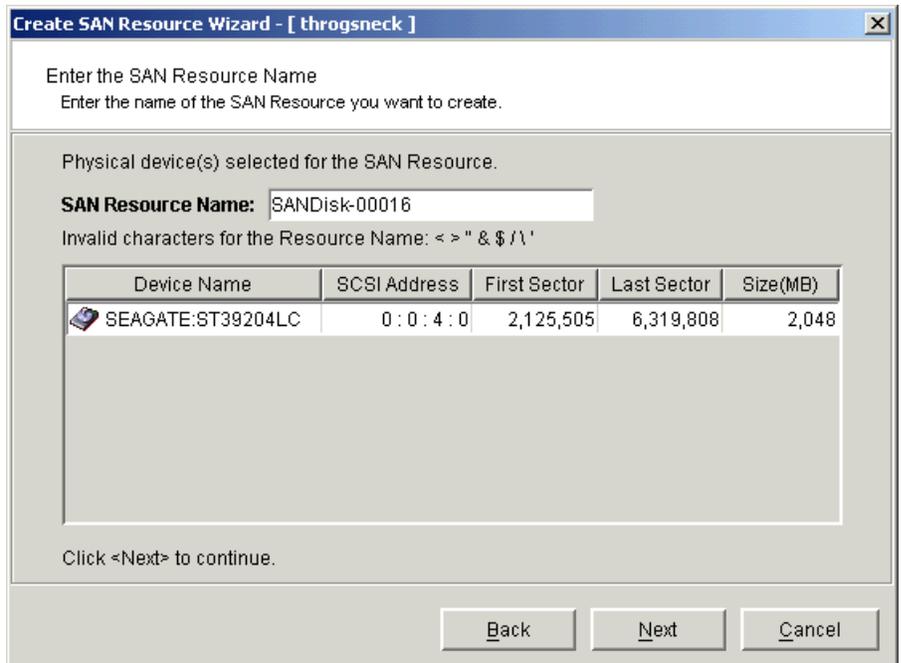


The name is not case sensitive.

Confirm that all information is correct and then click *Finish* to create the virtual device SAN Resource.

(*Express* and *Custom* only) Indicate if you would like to assign the new SAN Resource to a client.



If you select Yes, the Assign a SAN Resource Wizard will be launched.

Note: After you assign the SAN Resource to a client, you will need to restart the client (for Windows clients, you can rescan devices from the SAN Client Monitor instead). You will also need to write a signature, create a partition, and format the drive so that the client can use it.

**Create a direct device or service enabled device SAN Resources**

Simply follow the instructions on the screen and the second Node should join the Cluster without any further difficulties.

Right-click on *SAN Resources* and select *New*.

Select *Direct Device* or *Service Enabled Device*.



If you are creating a *Service Enabled Device*, determine if you want to preserve the physical device's inquiry string. Preserving it treats the physical device as

the original physical disk instead of treating it as a Acer device. This can be useful for vendors who only recognize their own storage devices.

Select how you want to create this device.

*Custom* lets you select one physical device(s) to use.

*Batch* lets you create multiple SAN Resources at one time.

Select the device that you want to make into a direct/service enabled device.

A list of the physical resources that have been reserved for this purpose are displayed. For direct devices, both hard disk and non-hard disk devices are shown.
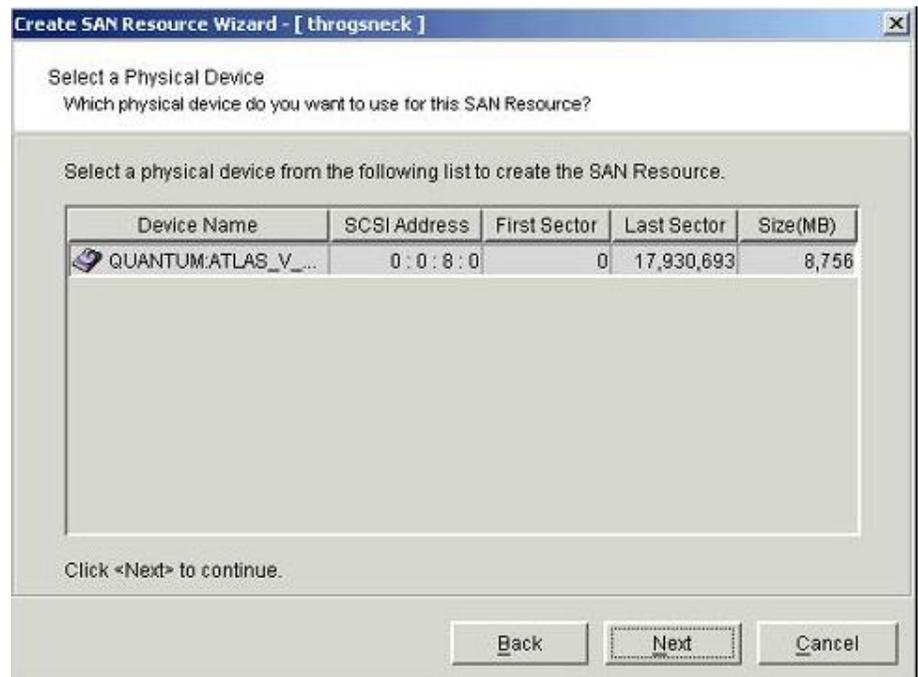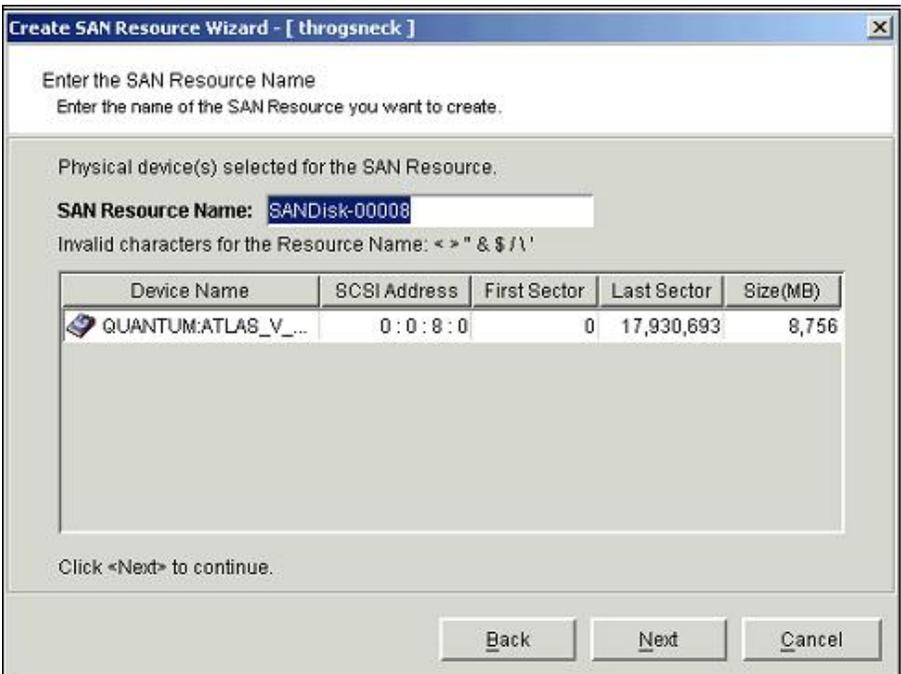


(Service enabled devices only) Select the physical device for the service enabled device's virtual header.
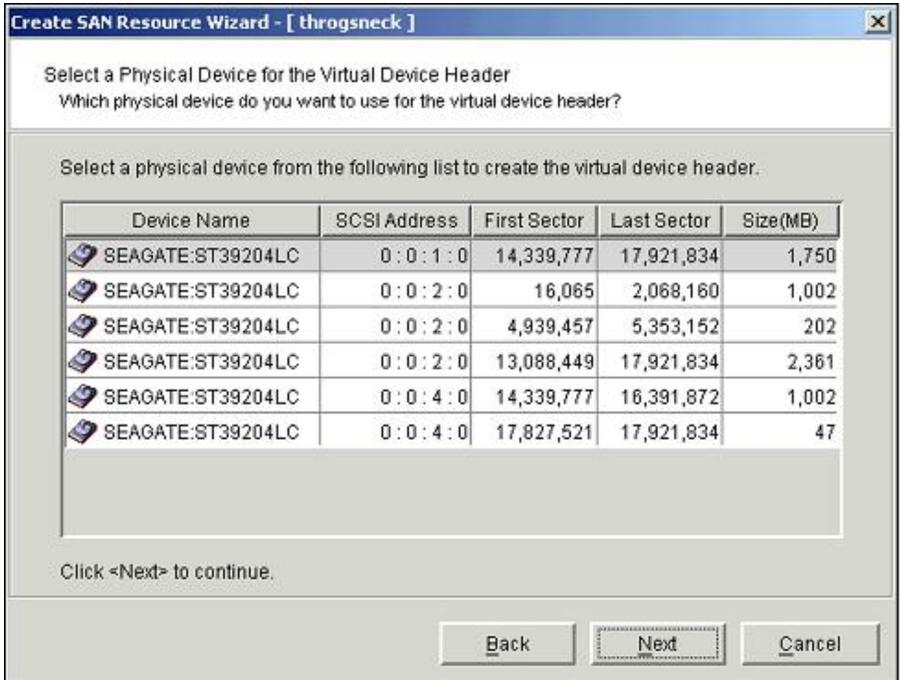
Even though service enabled devices are used as is, a virtual header is created on another physical device to allow ASC's storage services to be supported.
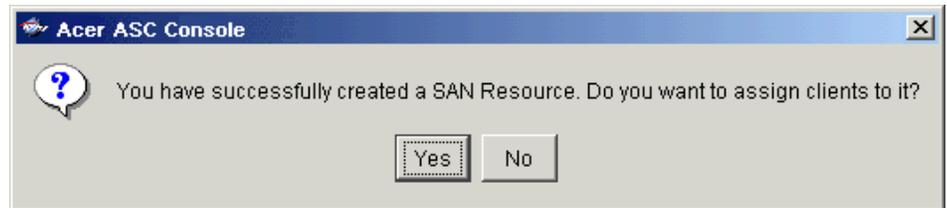
Enter a name for the new SAN Resource.



*Note: The name is not case sensitive.*

Confirm that all of the information is correct and then click *Finish* to create the SAN Resource.

Indicate if you would like to assign the new SAN Resource to a client.



If you select *Yes*, the *Assign a SAN Resource Wizard* will be launched.

## Assign resources to one or more clients

Notes:

The wizard can also be launched from the Create SAN Resource wizard.

If this server has multiple protocols enabled, select the type of client to which you will be assigning this SAN Resource.

Select the SAN Resource to be assigned.

*Read/Write* - Only one client can access this SAN Resource at a time.  All others (including *Read Only*) will be denied access. This is the default.

*Read/Write Non-Exclusive* - Two clients can connect at the same time with both read and write access.  You should be careful with this option because if you have multiple clients writing to a device at the same time, you have the potential to corrupt data.  This option should only be used by clustered servers, because the cluster itself prevents multiple clients from writing at the same time.

*Read Only* - This client will have read only access to the SAN Resource.  This option is useful for a read-only disk.

*Note: Fibre Channel SAN client is not supported under ASC 4.0 Express.*

For SAN/IP clients, you will see the following screen:
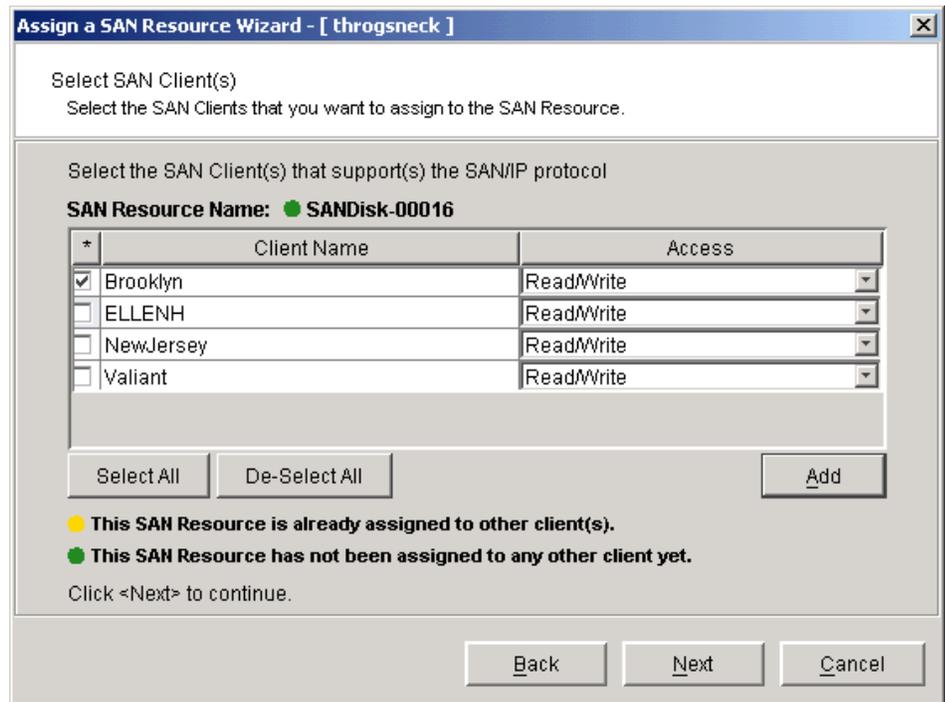


If the SAN/IP client that you want to assign to the SAN Resource does not appear on the list, click the *Add* button.

You can add any application server, even if it is currently offline or has not yet had ASC Client software installed. However, in order for the server to use the ASC storage resources, you must install the ASC SAN Client software on the server and "authorize" the client's access to the ASC SAN resources.

Note: You must enter the client's name, not an IP address.

For iSCSI clients, you will see the following screen:
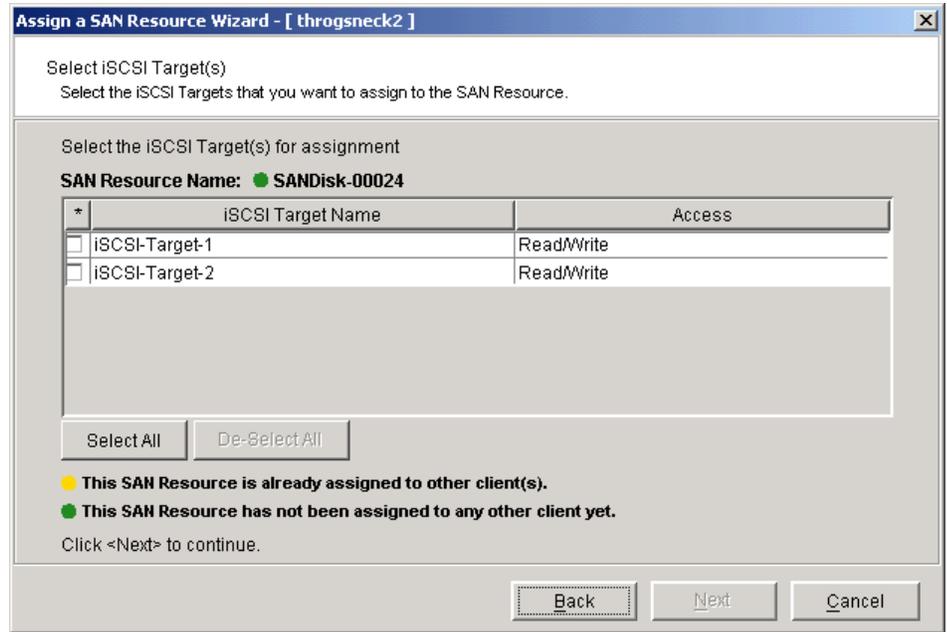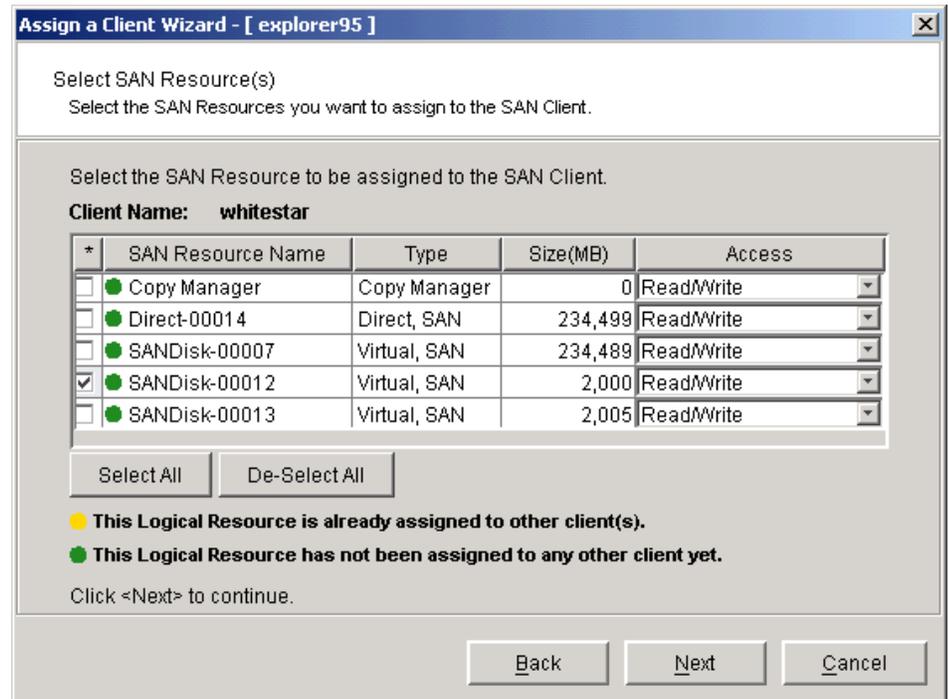
## Assign a client to one or more SAN Resources

Notes:

Right-click on a SAN Client and select *Assign*.

Select the SAN Resource to be assigned.



*Read/Write* - Only one client can access this SAN Resource at a time.  All others (including *Read Only*) will be denied access by default.

*Read/Write Non-Exclusive* - Two clients can connect at the same time with both read and write access.  You should be careful with this option because if you have multiple clients writing to a device at the same time, you have the potential to corrupt data.  This option should only be used by clustered servers, because the cluster itself prevents multiple clients from writing at the same time.

*Read Only* - This client will have read only access to the SAN Resource.  This option is useful for a read-only disk.

## Expand a virtual device

Once owner and fail back timing.

Since virtual devices do not represent actual physical resources, they can be expanded as more storage is needed. The virtual device can be increased in size by adding more blocks of storage from any unallocated space from the same server.

Note that you will still need to repartition the virtual devices and adjust/create/resize any file-systems on the partition after the virtual device is expanded. Since partition and file-system formats are specific to the operating system that the client is running, the administrator must perform these tasks directly from the client. You can use tools like:

- *Partition Magic*,

- *Windows 2000 Dynamic Disk*,

- or *Veritas Volume Manager*

to add more drives to expand existing volume on-the-fly in real time (without application down time).

Notes:
We do not recommend expanding a virtual device (SAN or NAS) while clients are accessing the drives. However, when expanding an XFS resource, NAS clients can remain connected.

Right-click on a virtual device (SAN or NAS) and select *Expand*.

Select how you want to expand the virtual device.
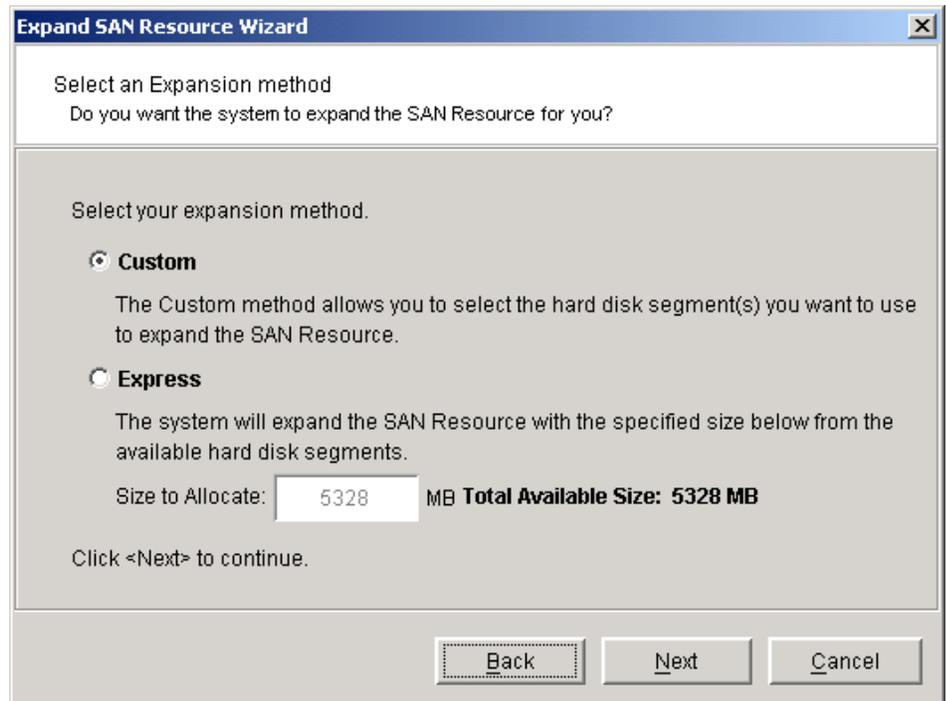


*Custom* lets you select which physical device(s) to use and lets you designate how much space to allocate from each.

*Express* lets you designate how much space to allocate and then automatically creates a virtual device using all available devices.

The *Size to Allocate* is the maximum space available on all available devices. If this drive is mirrored, this number will be half the full amount because the mirrored drive will need an equal amount of space.

If you select *Custom*, you will see the following windows:



Confirm that all information is correct and then click *Finish* to expand the virtual device.

Windows 2000 Dynamic disks

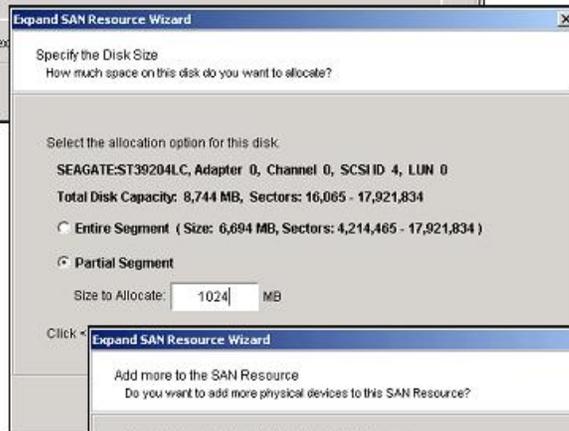Expansion of dynamic disks using the Expand SAN Resource Wizard is not supported for clients using either SAN/IP.  Due to the nature of dynamic disks, it is not safe to alter the size of the virtual device.  However, dynamic disks do provide an alternative method to extend the dynamic volume.

To extend a dynamic volume using SAN Resources, use the following steps:

- Create a new SAN Resource and assign it to the ASC Client.  This will become an additional disk which will be used to extend the dynamic volume.

- Use Disk Manager to write the disk signature and upgrade the disk to "Dynamic".

- Use Disk Manager to extend the dynamic volume.

- The new SAN Resource should be available in the list box of the Dynamic Disk expansion dialog.

AIX clients

Expanding an ASC virtual disk will not change the size of the existing AIX volume group. To expand the volume group, a new disk has to be assigned and the *extendvg* command should be used to enlarge the size of the volume group.

## Delete a SAN Resource

If the ASC device is removed while logical volumes exist, you will not be able to remove the logical volumes and the system will display error messages.

- Detach the SAN Resource from any client that is using it.

- For Windows clients, launch the ASC SAN Client Monitor and click the *Stop Client* button.

- For other clients, type ./sanclient stop from /usr/local/sanclient/bin.

- In the Console, highlight the SAN Resource, right-click and select *Delete*.

## MANAGE ASC SAN CLIENTS

ASC SAN Clients are the file and application servers that access ASC SAN Resources. Since SAN Resources appear as locally attached SCSI devices, the applications, such as file services, databases, web and email servers, do not need to be modified to utilize the storage.

On the other hand, since the storage is not locally attached, there is some configuration needed to locate and mount the required storage.

### Add & configure an ASC client

The ASC Server grants storage access to the Client. But, in order for a Client to be able to access storage, you must establish a trusted relationship between the Client and Server. This prevents other computers from masquerading as the Client and accessing storage that it does not have rights to. In order to establish a trusted relationship, you must:

Add the Client in the Console and assign storage resources to the Client.

Refer to the section 'Assign a SAN Resource to one or more clients' for more information.

Add the Server to the Client.

For Windows Clients, you can use the *Add Server* option in the SAN Client Monitor program. For Linux or Solaris Clients, you can execute *./sanclient monitor* from /usr/local/sanclient/bin to connect and authenticate the Client to a Server. You must enter the Client's hostname or root user name and password.

This process authorizes the access to the Server and needs to be done only once per client-to-server relationship. Subsequent access to a Server from a Client retains the authorization. Credentials do not need to be re-entered unless the software is re-installed.

When a SAN Resource is assigned to a Client, the Client does not need to obtain additional authorization to access the new resource. There is only a single, persistent authorization maintained between the Client and Server.

Note: Each SAN Client needs a unique name.  You should not duplicate the name of an ASC Server.

Multiple Servers

The Client must obtain authorization from each and every Server that it attaches to for SAN Resources. Every time the Client attaches to a new Server, the first connection needs to be authorized, as described above. The Client software will retain authorized connections to any number of ASC Servers.

## ASC SAN Client on Linux

All configuration of the Client is done through the ASC Console. Once configured, the ASC SAN Client software connects to the appropriate ASC Servers and gets its assigned resources.

Note: If you assign additional resources to the Client from a new Server after you have installed the Client, you will need to add that Server to the Client. You will also need to restart the Client in order for the changes to take effect.

### Start/stop the ASC SAN Client processes

In order for the Client to be able to access SAN resources, the Client software must be started. You can type the following commands from /usr/local/sanclient/bin:

| | |
|---|---|
| ./sanclient start | starts the Client. |
| ./sanclient stop | stops the Client, detaching all devices in use by the Client. |
| ./sanclient restart | restarts (stops and then starts) the Client. |
| ./sanclient status | displays the current status of the Client. |
| ./sanclient devices | (Solaris, HP-UX, and AIX only) displays a list of ASC devices that are available for use. |

Note:
Before stopping the Client, make sure all read/write operations are complete and make sure all of the ASC devices are not being used and are not mounted.

### Add/delete/display/rescan ASC Servers

The Client has a program that allows you to:

- Add and delete ASC Servers.

- Display the Client's current configuration.

- Display a list of ASC devices - for SAN/IP Clients only.

- Rescan ASC devices - eliminates the need to restart the Client after adding a virtual device to an existing adapter, deleting a virtual device, or expanding a virtual devices for Linux and Solaris 8 Clients.

- Attach/detach SAN devices.

- Execute the following from /usr/local/sanclient/bin:

  - ./sanclient monitor

- Select which action you would like to take.

- If you are adding a Server, enter the ASC Server name, login name (hostname or root user name), and password.

- If you are deleting a Server, you should back up /usr/local/sanclient/etc/ipstorclntd.conf before proceeding.  After you have done that, enter the Server name that you want to delete.

- If you want to view the Client's configuration, enter the login ID and password for the Client.
The Client must be started to view the configuration.
You will see information similar to the following for each Server that the Client accesses:

Configured ASC Server(s) on client localhost:

        1) washington


        Server washington :
        Adapter (0) SCSI ID 7.
        Device Name: DIRECT-2
        Attach Mode: Exclusive Read Write
        SCSI ID: 4
        Device ID: 2
        # Read Commands:              0
        # Write Commands:             0
        # Misc. Commands:             3
        Total Bytes Read:             0
        Total Bytes Written:          0

**Add/delete/expand a virtual drive**

You can add a virtual device to an existing adapter, delete a virtual device, or expand a virtual device without having to restart your Linux or Solaris 8 Client. You can also expand a virtual device without having to restart your Solaris 6 or 7 Client (add or delete requires a restart).

- With the Client running, make sure that the virtual device to be expanded or deleted is NOT in use.

- The disk cannot be mounted or have any files open. You also cannot be using fdisk, mkfs, fsck, etc.

- In the Console, add, delete, or expand the virtual device.

- Execute the following from /usr/local/sanclient/bin:

  - ./sanclient monitor

- Select *Rescan ASC SAN Devices*.

- As appropriate, follow your operating system's instructions for creating a new partition, extending an existing partition, or, if desired, mounting the new disk/partitions.

## ASC SAN Client on Windows NT/2000/2003

Once installed, the ASC SAN Client software runs as a Windows NT/2000 service. The service is configured to start automatically when Windows starts. The configuration of the storage resources used by the Client is done through the ASC Console.

Once configured, the ASC SAN Client software connects to the appropriate ASC Servers and gets the assigned resources.

*Note*: *If you assign additional resources to the Client from a new Server after you have installed the Client, you will need to add that Server from the Client Monitor.*

### ASC SAN Client Monitor

The ASC SAN Client Monitor runs on the Client computer. It allows you to stop/start the Client, connect/disconnect a Server, attach/detach devices, add/delete/organize Servers, set debug options, filter the Event Viewer information, and monitor the status of the Client's connections to its SAN Resources and Servers.

To launch the ASC SAN Client Monitor:
(*Start --> Programs --> Acer ASC --> SAN Client Monitor*)
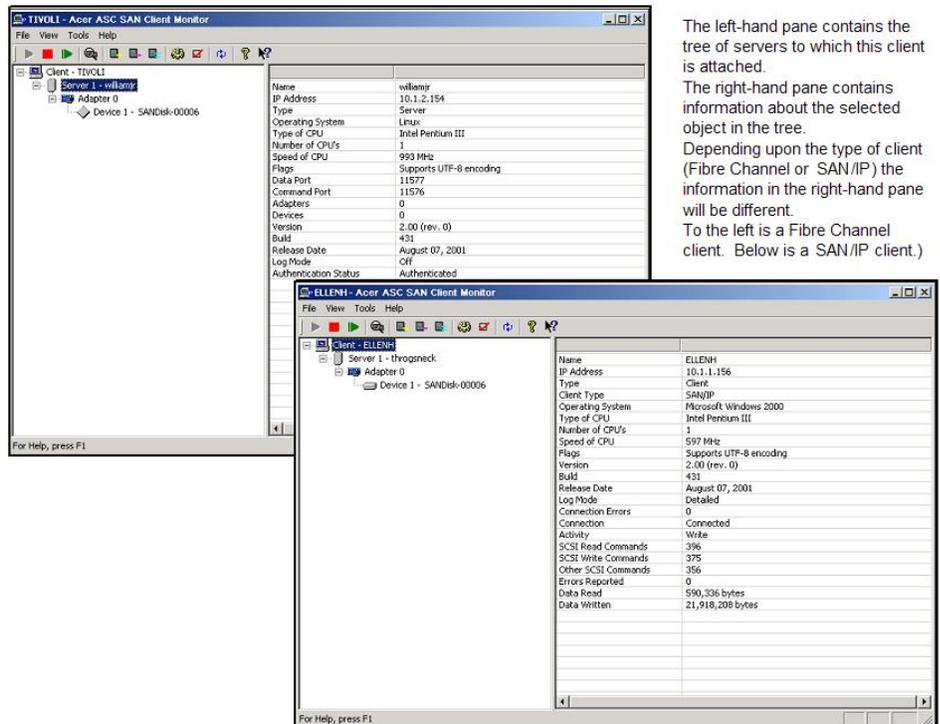
The left-hand pane contains the tree of servers to which this client is attached.

The right-hand pane contains information about the selected object in the tree.

Depending upon the type of client (Fibre Channel or SAN/IP) the information in the right-hand pane will be different.

To the left is a Fibre Channel client. Below is a SAN/IP client.)

In order to see information about a Server and its devices, you must be connected to the Server. When you start the Monitor, it attempts to connect to each Server. If it cannot connect to a Server, you will see a red X on the Server.

**Refresh the Monitor display**

The statistics in the right-hand pane are refreshed automatically, based on the time interval you set under *Options*  .

If you have formatted any devices, click the *Refresh* button  to update partition, file system, and size information.

If you have added/deleted/changed any devices or SAN Resources assigned to this Client, click the *Rescan Devices* button  . This re-scans the Client's local devices to see any configuration changes and rescans all Servers looking for new/deleted/changed SAN Resources. If you are on a Server object and you right-click and select *Rescan*, it will rescan only that Server.

**Stop and start the client**

Stop the Client

Stopping the Client services will detach the virtual devices and direct devices in use by the Client, allowing the ASC administrator to manage or modify the SAN Resources safely.

Note: Before stopping the Client, make sure all read/write operations are complete.

Start the Client

Starting the Client services re-establishes the connection to all of the ASC Servers and attaches to the SAN Resources assigned to this Client.

Note: If you added or deleted SAN Resources for this Client in the Console, use the *Rescan Devices* button to have the changes take effect.  For other configuration changes, you will need to restart the Client.

Restart the Client

To stop/start the Client, click the Restart Client button  .  This stops the Client and then restarts it for you.

Note: If the Windows NT/2000 Client loses its connection to the ASC Server due to a network issue, or the ASC Server is shut down and you click the Stop Client or Restart Client buttons, the Windows NT/2000 Client will retry its connection to the ASC Server for five minutes before timing out. During this time the Client Monitor will be inaccessible.

**Connect/Disconnect a server**

When you disconnect a Server, it will still appear in the tree but it will not be monitored and you will not see statistics for it.

Conversely, when you connect to a Server, it will be monitored and you will see statistics for it.

To connect/disconnect, right-click on the Server and select the appropriate option.

**Add an ASC Server**

Click the *Add Server* button.

This starts a wizard that will guide you through the process.
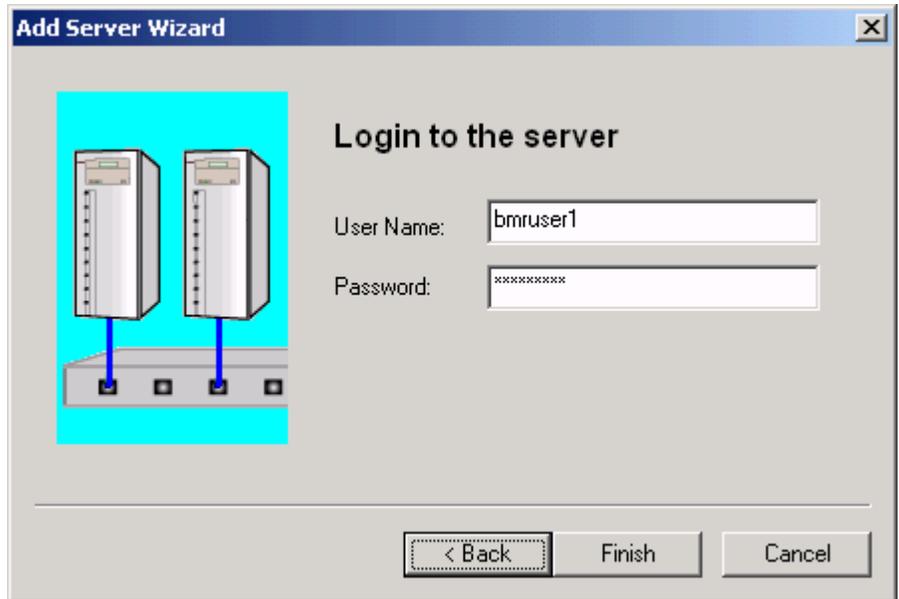
Enter the name of the ASC Server.



Enter the IP address.

The *IP address* and port are used for configuration and system maintenance commands. The communication takes place over TCP and is used to connect to the Server.

Enter the Client's hostname or root user name and password.



When you click *Finish*, the Client connects to the Server, verifies the user name and password, and authorizes the Client to use Resources from that Server.

If you have found the machine, but it is not an ASC Server, or the Server software has not been started, you will see a message like this:

Cannot add this client (clientname) to the ASC Server "myserver".
Server is not running ASC.

If the computer is not found, you will see a message like this:

Cannot add this client (clientname) to the ASC Server "myserver".
Server not found.

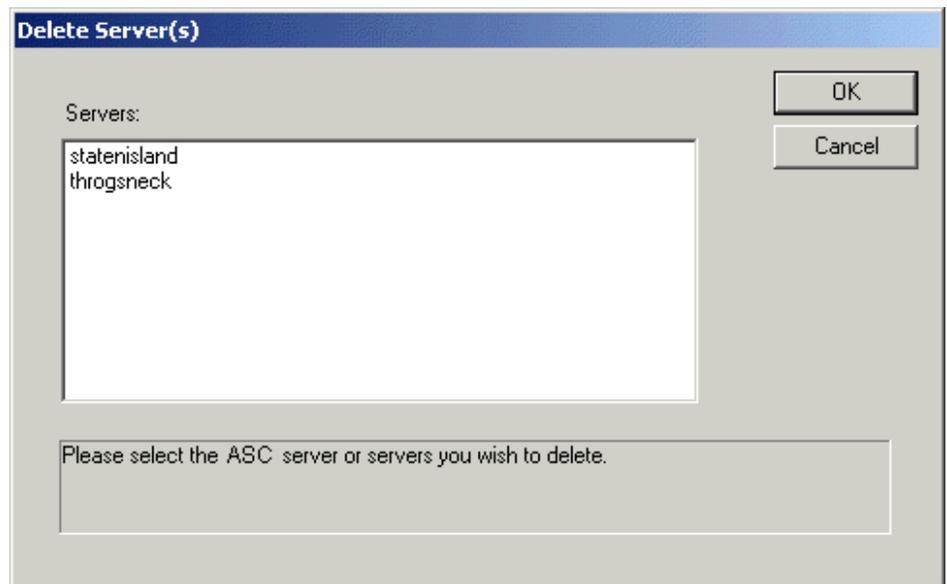If you entered an invalid user name and/or password, you will see a message like this:

Cannot add this client (clientname) to the ASC Server "myserver".
RPC authentication error.

### Delete a Server

You can delete one or more Servers.  If you delete a Server, the Client will no longer be able to access storage through that Server.

Click the *Delete Server* button  .



Select one or more ASC Servers and click *OK*.

**Organize Servers**

This option lets you add and delete Servers as well as edit the address and login information for each Server. You can also rearrange the order of Servers listed in the Monitor.

You may also want to use this option if the Client is not currently connected but you want to see the list of Servers to which it normally connects.

Click the *Organize Servers* button          .
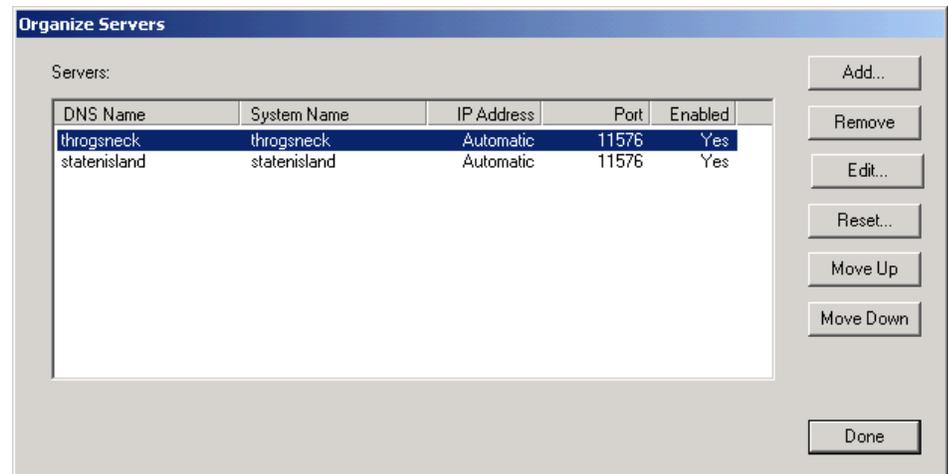


Select the function you would like to perform.

*Add* - Add a new ASC Server.

*Remove* - Remove an ASC Server from the Client.

*Edit* - Change the Server that you are connecting to (if the Server's name has changed), set/change the way the server is located.

*Reset* - Change the user name and password used for authentication between the Client and Server.

*Move Up/Move Down* - Re-order the Servers in the list.

**Set dependent services to start after ASC services**

If you have applications running on your Client Machine (such as Microsoft IIS, Exchange, or SQL Server) that access your SAN storage resources, you must make sure that the ASC services are started before these application's services start.  To do this:



Click the *Dependent Services* button        .
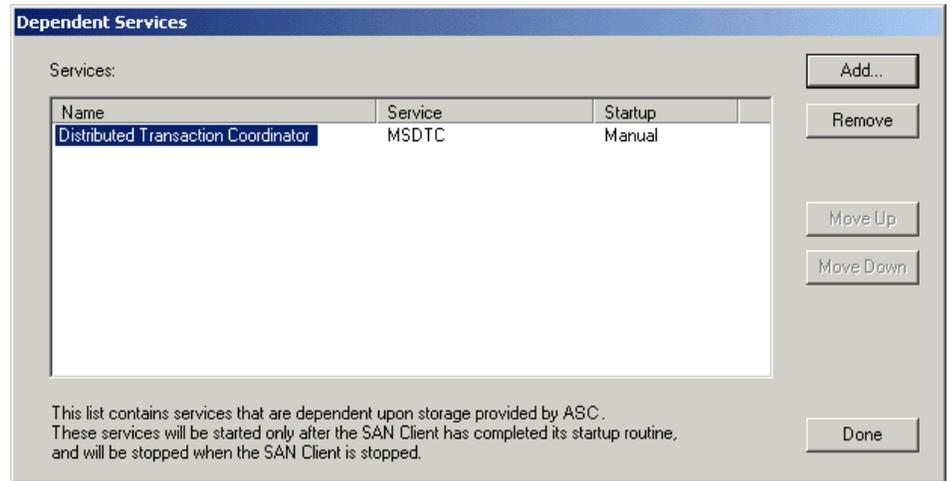


Add the services that should only start after ASC starts.

ASC will set each service's *Startup Type* to *Manual* and will become responsible for starting the services, in the listed order, after ASC has started.  Therefore, it is important to list your services in the correct order.  This is especially true if an application has multiple services, but these services do not automatically start each other.

Note: It is very important that you only select services that are dependent on ASC.  You do not want to add critical services (such as DNS Client, Event Log, Logical Disk Manager, or SNMP) that must start before ASC.

**Register tape devices for use with backup software**

You must register your tape drives and libraries if your backup software requires the drivers for these devices be loaded prior to loading the backup software.

Once you register a device and reboot, ASC loads the device drivers when ASC starts.

To register a device:

- Right-click on the tape drive or library and select *Register*.

- Reboot your computer.

**Register disks for drive priority**

You can register a virtual device so that it will have the priority to get the first available drive letter during a reboot. To register a disk:

Right-click on the disk and select *Register*.

**Filter Event Viewer information and set client options**

You can configure the amount of detail about the ASC Client's activity and performance that will be written to the Windows Event Viewer. You can also enter domain information and enable a system tracer.

You can also determine if you want the Client to automatically start when this computer starts and how often to refresh information in the Monitor.

Click the *Options* button
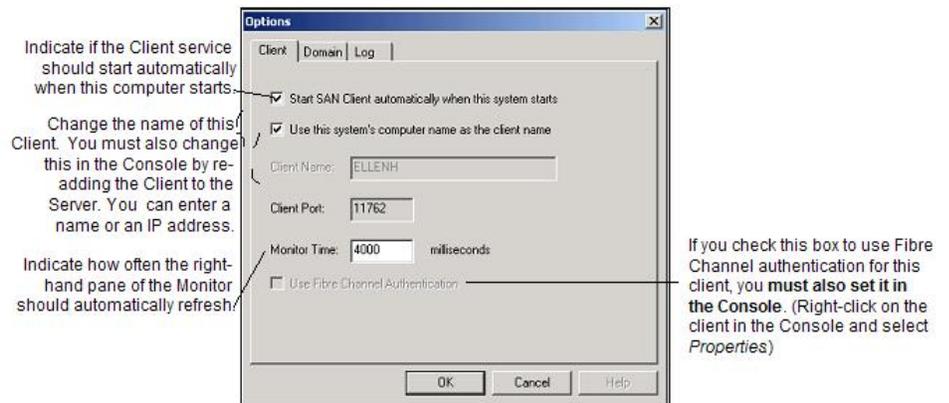


Select the *Domain* tab, and if applicable, enter information about your domain.
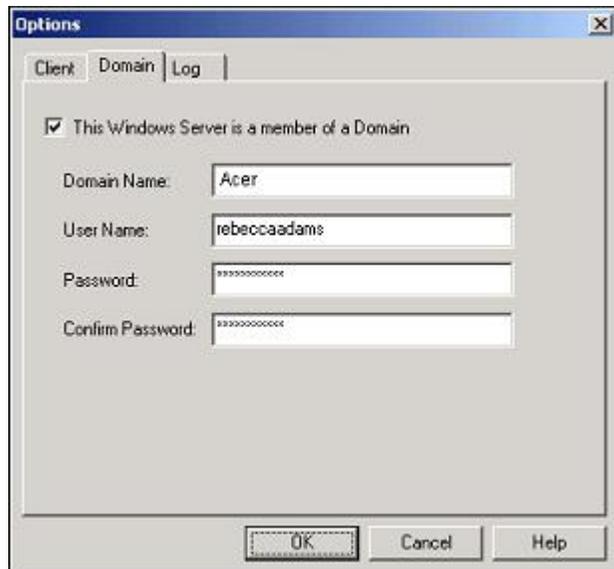
Select the *Log* tab.
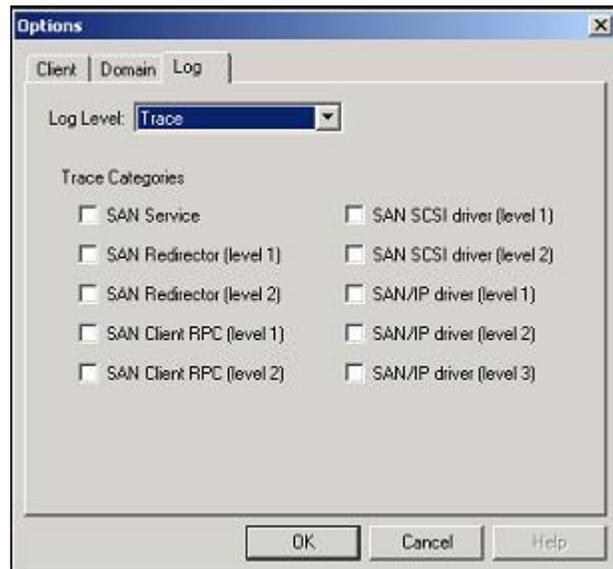


To filter the events being written to the Event Viewer, select one of the levels in the *Log Level* field.

Note that regardless of which level you choose, there are several events that will always be written to the Event Viewer (driver not loaded, service failed to start, service started, service stopped).

Five levels are available for use:

Off – No activity will be recorded.

Errors only – Only errors will be recorded.

Brief – Errors and warnings will be recorded.

Detailed – (Default) Errors, warnings and informational messages will be recorded.

Trace – This is the highest level of activity tracing. Debugging messages will be written to the trace log. In addition, all errors, warnings and informational messages will be recorded in the Event Viewer.

If you select the *Trace* level, specify which portions of the ASC Client will be traced.

When enabled, the trace information will be logged to a file called FSNTrace.log located in the \Acer\ASC\Logs directory.

*Warning*: *The debug parameters should not be adjusted unless directed to do so by Acer technical support. Adjusting these parameters can impact system performance.*

## ASC SAN Client on NetWare

### Start the client

You can start the client by typing the following command from the NetWare console screen to start the client:

> Sanon
>
> ISCMD Start Server=*serverIPAddress*

When prompted, enter your username and password.

Type the following to mount your volumes:

> Mount all

If you change a LUN or add a device, you will need to restart the Client in order for the changes to take effect.

### Set the client to automatically start after server reboot

To start the SAN Client automatically upon boot up, add the following to the end of the Autoexec.ncf file.

> Sanon
>
> Iscmd start server= x x x x noscreen=1

### Stopping and removing the client

Unmap the share on the Windows side.

Dismount the ASC SAN/IP device from the Novell server.

Go to the Novell server and type the following:

> ISCMD Stop server=*serverIPAddress*

Type the following:

> ISCMD Remove server=*serverIPAddress*

In the ASC Console, right-click on the SAN/IP client, unassign the device, and then delete the client.

To uninstall the client, refer to the sanon.ncf file in the sys:\system directory to find the files that need to be removed.

**Disk copies**

If you mirror, copy, or replicate a virtual device you cannot assign the copy to the same client to which the primary is assigned unless you first rename the Novell volume to a different name. The operating system does not handle the device the same way as other operating systems do.
For example, with Windows 2000, if the replica is assigned to the same server as the primary, a different drive letter is assigned by the operating system.

**Troubleshooting**

**ISCMD command log**: Run the ISCMD command with option DEBUG=2. The debugging message will be written to the log file ISCMD.LOG located in the directory SYS:\SYSTEM.

For example: *ICCMD Start Server=serverIPAddress Debug=2*

**ASC SAN client trace log:**  Run the command SANDRV +debug +ip3 on the NetWare System Console. The trace log will be written to the log file TRACELOG.XML located in the directory SYS:\SYSTEM.

**Uninstall a SAN client**

**Do the following to uninstall SAN Client software:**

| Operating System | Command/Instructions |
|---|---|
| Windows NT / Windows 2000 | You can use *Add/Remove Programs* from the Control Panel or:<br><br>1. Insert the ASC installation CD in to your CD-ROM drive.<br><br>2. Select *Install Products --> Install ASC SAN Client* and follow the on-screen instructions to uninstall the Client.  If you will be installing a newer version of the Client software, you will have to reboot the machine during the un-install process. Afterwards, you will have to run the SAN Client installation again to install the new software. |
| Linux | Log on to the system as root and remove the client software by executing the following command:<br><br>rpm -e sanclient |
| NetWare | Refer to the sanon.ncf file in the sys:\system directory to find the files that need to be removed. |

# MANAGE THE ASC SERVER

The ASC Server is a storage server designed to require little or no maintenance.

All day-to-day ASC administrative functions can be performed through the ASC Console. However, there may be situations when direct access to the Server is required, particularly during initial setup and configuring of physical storage devices attached to the Server or for troubleshooting purposes.

If access to the Server's operating system is required, it can be done either directly or remotely from computers on the SAN.

## Start the ASC Server

Execute the following commands to start the ASC Server processes:

```
cd /usr/local/asc/bin

./asc start
```

You should see the processes start.

If the server is already started, you can use *./asc restart* to stop and then start the processes

## Set ASC to start automatically upon bootup

Execute the following commands:

From the directory /etc/rc.d/rc3.d on the Server, enter the following command:

```
ln -s /usr/local/asc/bin/asc S99asc
```

This command is case sensitive. The file *S99asc* will be created.  You can verify using the command:  ls -l  S99asc

Reboot the server to verify ASC starts.

To stop ASC from starting on bootup, delete the file /etc/rc.d/rc3.d/S99asc.

## Stop the ASC Server

Warning: Stopping the ASC Server processes will shut down all access to the storage resources managed by the Server. This can halt processing on your application servers, or even cause them to crash, depending upon how they behave if a disk is unexpectedly shut off or removed. It is recommended that you make sure your application servers are not accessing the storage resources when you stop the ASC Server processes.

To shut down the ASC Server processes, execute the following commands:

```
cd /usr/local/asc/bin

./asc stop
```

You should see the processes stopped

## Linux ASC servers enabled with NAS

To allow the ASC server to shut down smoothly when using "reboot", "shutdown", or "halt" commands, add the following symbolic links in the /etc/rc.d/rc0.d and /etc/rc.d/rc6.d directories:

ln -s /usr/local/asc/bin/asc K00asc

This will force Linux to stop ASC before stopping NFS and networking services.

## Log into the ASC Server

You can log in directly from a keyboard/display connected directly to the Server. There is no graphical user interface (GUI) shell required.

By default, the root user is the only user that has login privileges to the operating system. Other ASC administrators do *not*.

To log in, enter the username and the password for the root user.

*Warning: You should not allow login access to your ASC Server to anyone except your most trusted system or storage administrators. Administrators with login access to the Server have the ability to modify, damage or destroy data managed by the Server.*

### Telnet access

By default, ASC administrators do not have telnet access to the Server. The Server is configured to deny all TCP/IP access, including telnet.

(Linux Server only) To grant telnet access to another computer on the network:

Log into the Server directly (on the local console keyboard and display).

Change the etc/passwd file.

For the appropriate administrator, change the line that looks like:

Username:/dev/nul:/dev/null

To:

Username:/homedirectory:/bin/bash

Where Username is an actual administrator name and homedirectory is the actual home directory.

*Note: For a more secure session, you may want to use the program ssh, which is supplied by some versions of the Linux operating system. Please refer to the Linux manual that came with your operating system for more details about configuration.*

## Check the ASC Server processes

You can type the following command from the shell prompt to check the ASC Server processes:

cd /usr/local/asc/bin

./asc status

On Linux, you should see the following:

| | |
|---|---|
| Status of ASC SNMPD Module | [Running] |
| Status of ASC Authentication Module | [Running] |
| Status of ASC Server (FSNBase) Module | [Running] |
| Status of ASC Server (Upcall) Module | [Running] |
| Status of ASC Server (Transport) | [Running] |
| Status of ASC Server (Application) | [Running] |
| Status of ASC Advanced Backup Module | [Running] |
| Status of ASC Communication Module | [Running] |
| Status of ASC FC Target Module | [Running] |
| Status of ASC Logger Module | [Running] |
| Status of ASC Local Client (Daemon) | [Running] |
| Status of ASC Local Client (Redirector) | [Running] |
| Status of ASC NAS MGTD Module | [Running] |
| Status of ASC NAS NMBD Module | [Running] |
| Status of ASC NAS SMBD Module | [Running] |
| Status of ASC NAS MOUNTD Module | [Running] |
| Status of ASC NAS NFSD Module | [Running] |
| Status of ASC Self Monitor Module | [Running] |
| Status of ASC Failover Module | [Running] |

You will only see this process if Fibre Channel Target Mode is enabled. → Status of ASC FC Target Module

You will only see these processes if NAS is enabled.

You will only see this process if Failover is enabled. → Status of ASC Failover Module

## Check physical resources

When adding physical resources or testing to see if the physical resources are present, the cat /proc/scsi/scsi command can be executed from the shell prompt in Linux:

These commands display the SCSI devices attached to the ASC Server. For example, in Linux you will see something similar to the following:

```
[root@NAS700 root]# cat /proc/scsi/scsi
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: MegaRAID Model: LD0 RAID1 35002R Rev: 1L15
  Type:   Direct-Access                    ANSI SCSI revision: 02
Host: scsi2 Channel: 04 Id: 06 Lun: 00
  Vendor: ESG-SHV  Model: SCA HSBP M22      Rev: 0.06
  Type:   Processor                        ANSI SCSI revision: 02
Host: scsi3 Channel: 00 Id: 00 Lun: 00
  Vendor: Acer      Model: Altos S205F      Rev: 3310
  Type:   Direct-Access                    ANSI SCSI revision: 03
Host: scsi3 Channel: 00 Id: 00 Lun: 01
  Vendor: Acer      Model: Altos S205F      Rev: 3310
  Type:   Direct-Access                    ANSI SCSI revision: 03
Host: scsi3 Channel: 00 Id: 01 Lun: 00
  Vendor: Acer      Model: Altos S205F      Rev: 3310
  Type:   Processor                        ANSI SCSI revision: 03
Host: scsi5 Channel: 00 Id: 00 Lun: 00
  Vendor: USB       Model: Flash Drive      Rev: 1.12
  Type:   Direct-Access                    ANSI SCSI revision: 02
[root@NAS700 root]# █
```

## NAS CONFIGURATION

Network Attached Storage, or NAS, is another piece of the storage management picture.

NAS refers to storage and data that can be accessed directly from the storage network and represents a quick and easy way to add general purpose, shareable, storage space for users and groups.  With NAS, users can access data and storage via a network interface using protocols including NFS (Network File System) and CIFS (Common Internet File System).

NAS contrasts with SAN in several key ways:

- NAS offers shared files/folders instead of devices (SAN).

- SAN storage provides block level data storage and is ideal for high performance, low latency applications, such as databases.

- NAS uses file-based access and is ideal for providing data and file sharing for users and groups.

Implemented together, SAN and NAS help to reduce costs and simplify storage and data management.

Before ASC, a NAS box was a separate storage device with a built-in network interface, network operating system, and storage allocation software (basically a simplified, dedicated file server). The NAS box was plugged directly onto the corporate LAN, making itself accessible with one or multiple "file shares". Users and groups were assigned read/write privileges and a space quota. As the number of users grew, and as free space became low, additional NAS boxes could be plugged in.

This architecture has become more of a problem than a long-term solution. Traditional NAS boxes become yet another piece of hardware requiring their own backup, space allocation, and management GUI.

In ASC, NAS is simply another network storage service on your storage network. NAS uses the same storage devices that SAN uses, eliminating the need for separate devices.  Another advantage of providing NAS within ASC is that the advanced storage options such as snapshot and mirroring are uniformly applied to both SAN and NAS resources under a single set of storage management policy.

The NAS clients can be located anywhere on the network, as long as they have access to the ASC Server.

All NAS configuration is done through the ASC Console and can be found under the *NAS Resources* and *NAS Clients* objects in the tree.
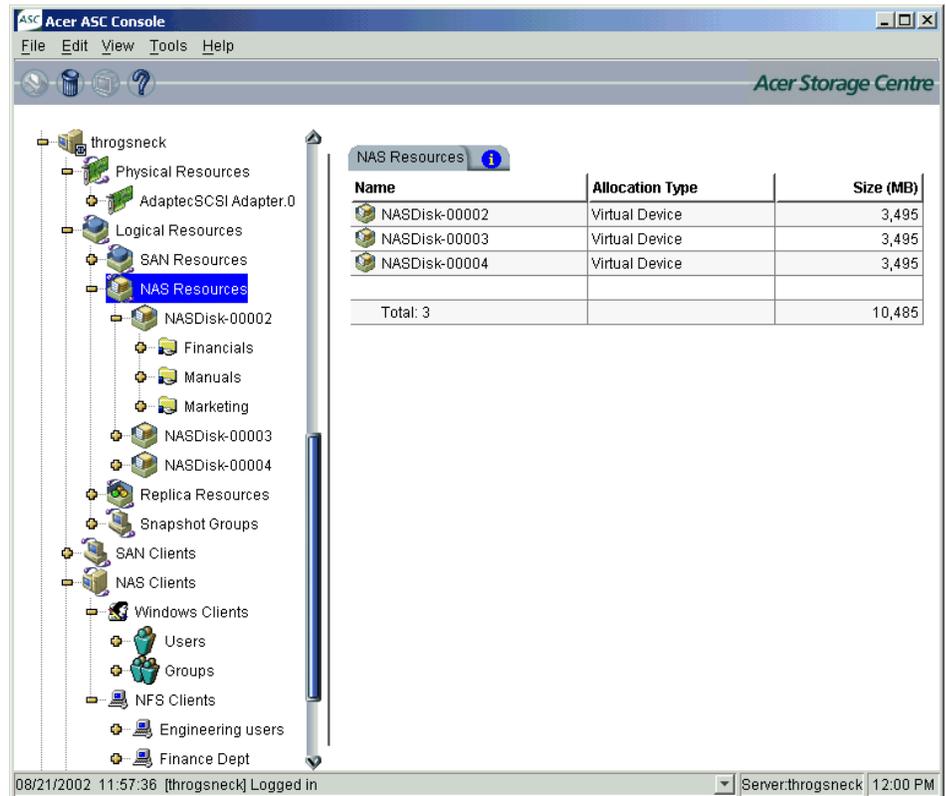


Note: If you do not see the NAS objects, the NAS option is not loaded on your ASC Server.  To enable it, you will need to start the Console, connect to this server, right-click on the server and select *Options --> Enable NAS*.

When you highlight the *NAS Resources* object, a list of current NAS Resources is displayed in the right pane.  Under each NAS Resource, you will see a list of folders and shares.  If the folder has a hand holding it, it has been assigned as a share.

There are two types of NAS clients you will see:

- Windows clients - These clients use the Common Internet File System (CIFS) protocol to work together and share documents. Because many operating systems support CIFS, it is possible to have clients using other operating systems listed as Windows clients.

- NFS clients - These clients are usually Unix clients using the Network File System (NFS) protocol.

To update the list of users/groups, right-click on the *Windows Clients* object and select *Refresh Windows Clients*.

Information on the *Connection(s), Share(s),* and *Locked File(s)* tabs is updated every few seconds.  You can set the interval by right-clicking on the *Windows Clients* object and selecting *Start Connection Status Refresh*.

## General NAS configuration sequence

The configuration of NAS requires several steps that are outlined below:

1.  Prepare for authentication.
    If you are using Active Directory, Access Control Lists (ACLs), or Network Information Service (NIS), verify that the appropriate packages are installed before enabling NAS and make any appropriate configuration changes.
    Refer to the Active Directory, Access Control Lists (ACLs), or Network Information Service (NIS) sections for more details.

2.  Enable NAS.
    (NFS protocol only) Add N.
    You do not need to add Windows clients.  If you are using the Share authentication mode, any Windows client can access a share (provided he/she knows the password).  In Server or Domain authentication mode, the list of users comes from the authentication server.

3.  Create a NAS resource.
    (Optionally) Limit the amount of storage each Windows user can have.

4.  Add/share folders and assign clients.
    You do not need to create each user's home directory if [homes] is enabled on your ASC server running in server or domain mode. Refer to Homes for more information.

5.  Map/mount the share.

## Prepare for authentication

There are three security modes that you can use to authenticate users/groups trying to access NAS shares.

**Share mode** - Authentication is done by a set of passwords (one *full access* password and one *read only* password) that are set from the Console. This mode does not use an authentication server.

**Domain mode** - The authentication server must be a Primary Domain Controller (PDC) for pure Windows NT or mixed Windows NT/2000 domains, or a Domain Controller for native Windows 2000 domains. The ASC Server and all NAS clients must belong to the domain controlled by this PDC/Domain Controller.

Before you activate *Domain* mode, you will need to create a computer account for the ASC Server in the domain.

- For a Windows 2000 domain, create the account for the ASC Server from *Administrative Tools* --> *Active Directory Users and Computers* --> *Computers.* After creating the account, right-click on the created account and select *Reset Account.* If the computer account for the ASC Server has already been created in the domain, right-click the account and select *Reset Account*, to join the domain again.

- For a Windows NT 4.0 domain, create the account for the ASC Server from *Administrative Tools* --> *Server Manager for Domains.* If the computer account for the ASC Server already exists in the domain, you have to delete the ASC Server account and then add the server again.

**NOTE**: If you ever need to replace your ASC Server (i.e. you replace the server's hard disk), you will need to reset/re-create the computer account for the ASC Server so that it can authenticate itself in the domain.

**Server mode** - Any Windows NT (Server or Workstation), or Windows 2000 (Server or Professional) computer (including a PDC/Domain Controller) can be used to authenticate users.

If you are not using a PDC/Domain Controller for authentication, group information stored on the PDC/Domain Controller cannot be accessed.  Only the users in this server (not including local users) are valid users.

If you use a PDC/Domain Controller for authentication, the ASC Server does not need to log into the NT domain controlled by the PDC/Domain Controller.

**NOTE:** It is important that you do not change your authentication mode once you begin using your NAS system.  If you do change it, you will lose all of your Windows client assignments and/or passwords.

The authentication modes are summarized in the following table:

| | Domain Mode | Server Mode | Share Mode |
|---|---|---|---|
| Requires an authentication server. | Yes. Authentication server must be a PDC/Domain Controller. | Yes. Any server, including a Domain Controller. | No |
| Requires ASC Server & NAS clients to belong to the domain. | Yes | No | No |
| ASC Server retrieves user and group accounts from authentication server. | Yes | Retrieves user information. Will retrieve group information if authentication server is a PDC/Domain Controller. | No |
| Uses only passwords for authentication. | No | No | Yes |

## Active Directory

If your Domain controller is running Windows 2000 Server, the ASC Server can be configured to utilize Microsoft's Active Directory to obtain users and groups. Both Domain and Server security modes can make use of Active Directory.

If you will be using Active Directory, you will need the following:

- Account for ASC - This account should have minimal security, similar to that of the *guest* account (do not use an *Administrator account* or *User with administrator rights*). The account will be used by ASC to access the active directory that ASC will browse to identify the users/groups that will have access to NAS shares. For a more secure account, you can limit this account to have *read access* only to the Organizational Units (OUs) that will be browsed by ASC.

- Your ASC Server and your Active Directory Server must have their clocks synchronized to within five minutes of each other. If they are not synchronized, you can use the *date* command on your ASC Server (Linux or Solaris) to adjust the date and time. However, the system clock on a PC can "drift" over time. Therefore we recommend that you use an automated synchronization service to adjust the system's clock. Refer to the *nptd* service on Linux, or *xntpd* on Solaris, and the *Windows Time* service on Windows for more information.

- The following packages must be installed on a Linux ASC Server *before* enabling NAS:

> cyrus-sasl-1.5.*x*.rpm
> cyrus-sasl-gssapi-1.5.*x*.rpm
> cyrus-sasl-md5-1.5.*x*.rpm
> cyrus-sasl-plain-1.5.*x*.rpm
> krb5-libs-1.2.*x*.rpm
> openldap-2.0.*x*.rpm

You can get these packages from the appropriate directory on the ASC CD:

Utilities/kernel-2.4.21-ipstor/ActiveDirectory

*Note: ASC does not support Active Directory's Nested Groups.*

## Network Information Service (NIS)

The ASC Server can be configured to utilize the Network Information Service (NIS) to obtain a list of users and groups.

If you will be using NIS, you will need to install and configure the NIS client on the ASC Server. On Linux Red Hat v7.3

1. From the ASC Server, type:
   domainname X
   where *X* is the domain name (Example: acer.com)

2. Edit the */etc/hosts* file and add the following information:
   NIS_server_IP
   NIS_server_name
   For example:

   | | |
   |---|---|
   | NIS_server_IP | 10.1.1.4 |
   | NIS_server_name | server1 |

3. Edit /etc/yp.conf and add the following information:
   domain X server NIS_server_name
   ypserver NIS_server_name

For example:

   | |
   |---|
   | domain acerstor.com server server1 |
   | ypserver server1 |

4. Edit /etc/nsswitch.conf and edit the following lines:
   passwd:    files nisplus
   group:     files nisplus

   Change these two lines to:
   passwd:    files nis
   group:     files nis

5. Execute the following command:
   ypbind
   The NIS client should now be running.

6. To confirm that everything is running properly, execute the following

command:
getent passwd

This command should return a user list from the ASC Server and the NIS server.

Notes:

- If the NIS client is rebooted, you need to repeat steps 1 and 5 to start the NIS client.

- To stop using the NIS client type:
  killall ypbind.

**Enable NAS**

1. In the Console, right-click on the server and select *Options --> Enable NAS.*

2. Select which security mode you will use to authenticate users/groups.
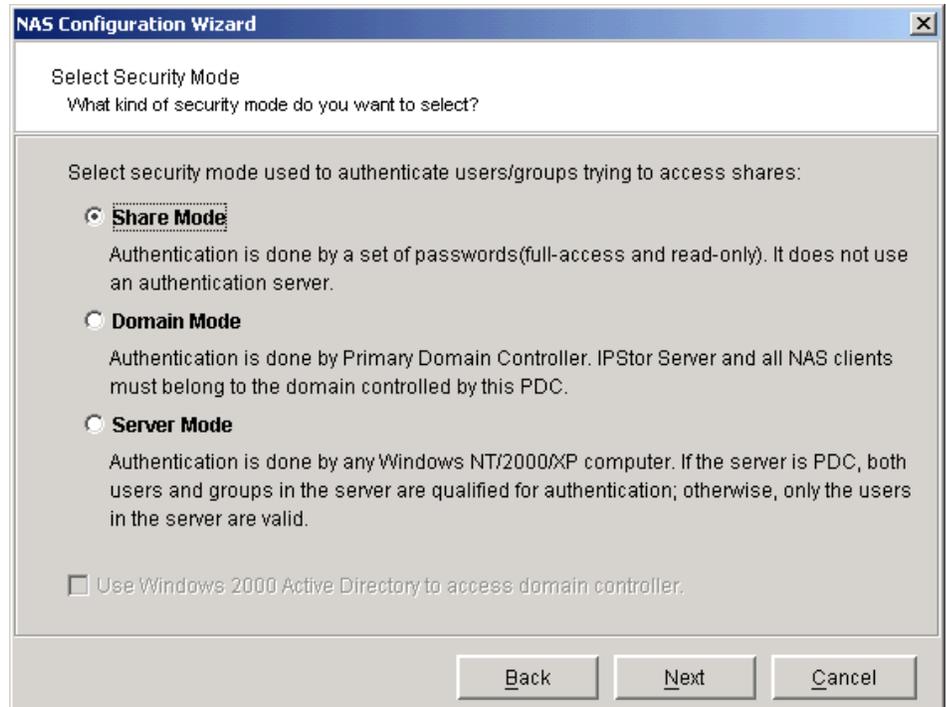


There are three security modes that you can use to authenticate users/groups trying to access NAS shares.

**Share mode** - (Default) Authentication is done by a set of passwords (one *full access* password and one *read only* password) that are set from the Console. This mode does not use an authentication server.

**Domain mode** - The authentication server must be a Primary Domain Controller (PDC) for pure Windows NT or mixed Windows NT/2000 domains, or a Domain Controller for native Windows 2000 domains. The ASC Server and all NAS clients must belong to the domain controlled by this PDC/Domain Controller.

**Server mode** - Any Windows NT (Server or Workstation), or Windows 2000 (Server or Professional) computer (including a PDC/Domain Controller) can be used to authenticate users.

**NOTE:** *It is important that you do not change your authentication mode once you begin using your NAS system.  If you do change it, you will lose all of your*

*share assignments.*

*For more information about authentication modes, refer to Prepare for authentication.*

3. (Domain and Server modes) Enter your authentication servers and domain information.



*Primary Authentication Server* - Enter the name of the server (not an IP address) from which the ASC Server will get the user account information. The ASC Server will use this server to authenticate users when they try to share a NAS resource. The server's name must be resolvable.

*Backup Authentication Server* - You can optionally enter a server name (not an IP address) to use for authentication if the primary authentication server is a PDC and is not available. If your primary authentication server is a PDC, the backup authentication server has to be your BDC. The server's name must be resolvable.

*Domain/Workgroup* - For *Domain mode*, enter the NT domain that the ASC Server must join. For *Server mode*, enter the workgroup that the ASC Server must join.  If you are using Active Directory you will not see this field.

4.  (Domain and Server modes with Active Directory)
    Enter information about the account ASC will use to log into Active
    Directory.



*User* - Enter the account ASC will use to log into Active Directory.

*Password* - Enter a valid password for this account.

*Confirm Password* - Re-enter the password for this account.

*Bind Point* - You can use the *Bind Point* to mark where in the OU tree ASC will
start browsing from. This is useful if ASC's user account does not have root
access to the entire OU tree. Without this access, ASC cannot see anything in
the tree.  In this case, enter a *Bind Point* to direct ASC to a starting point or a
single tree such as the /Engineering or /Accounting tree. If you leave this field
blank or enter "/", ASC will start at the root of this OU.

(Domain and Server modes with Active Directory) Select the organizational
units to which you will offer NAS shares.

5.  Click in the checkbox next to the OUs to which you want to offer NAS shares.

If you select the checkbox next to the root (/), it will select all OUs.
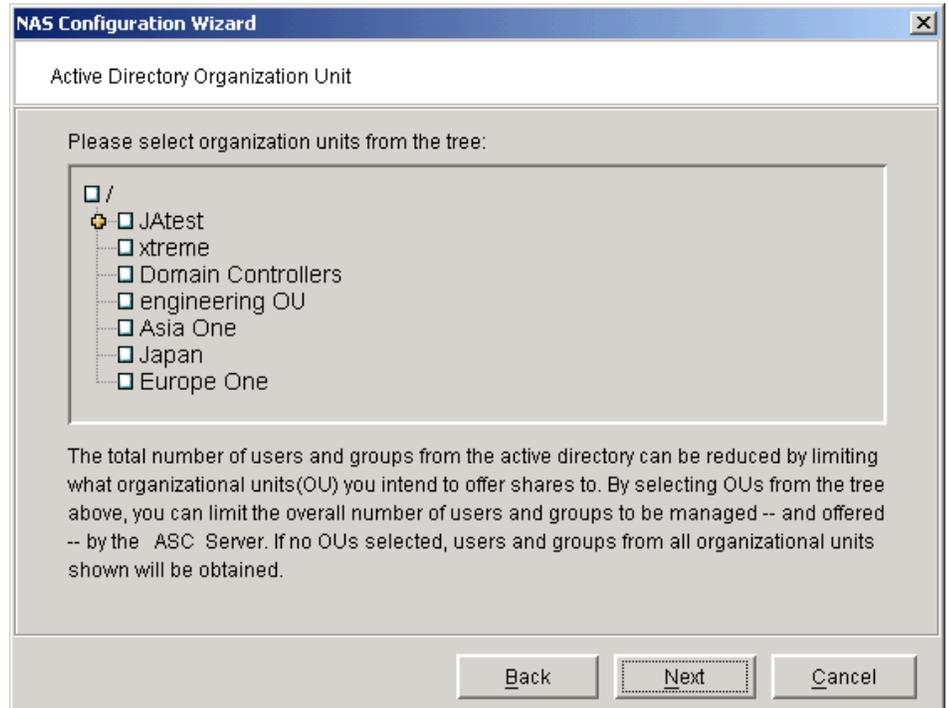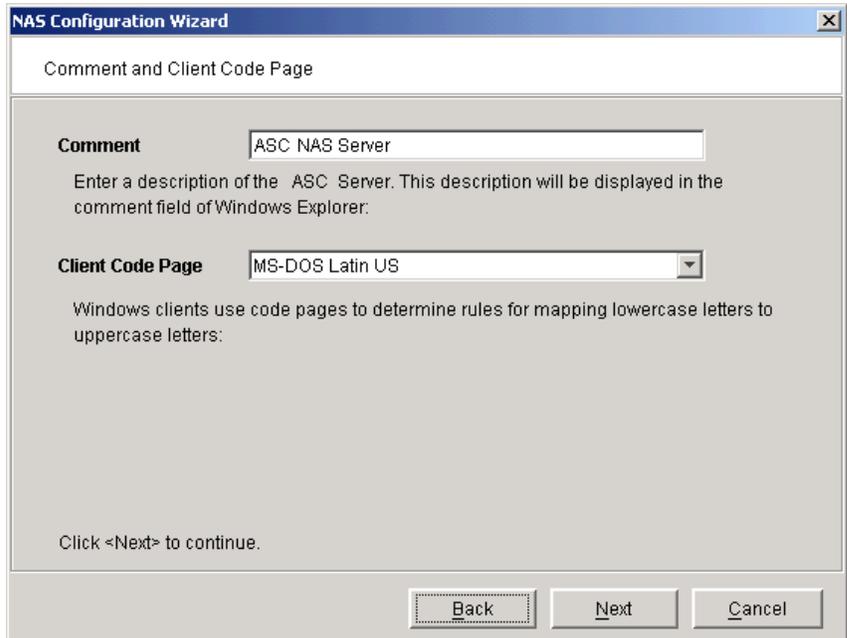
6. (Share mode) Enter the workgroup that the ASC Server must join.
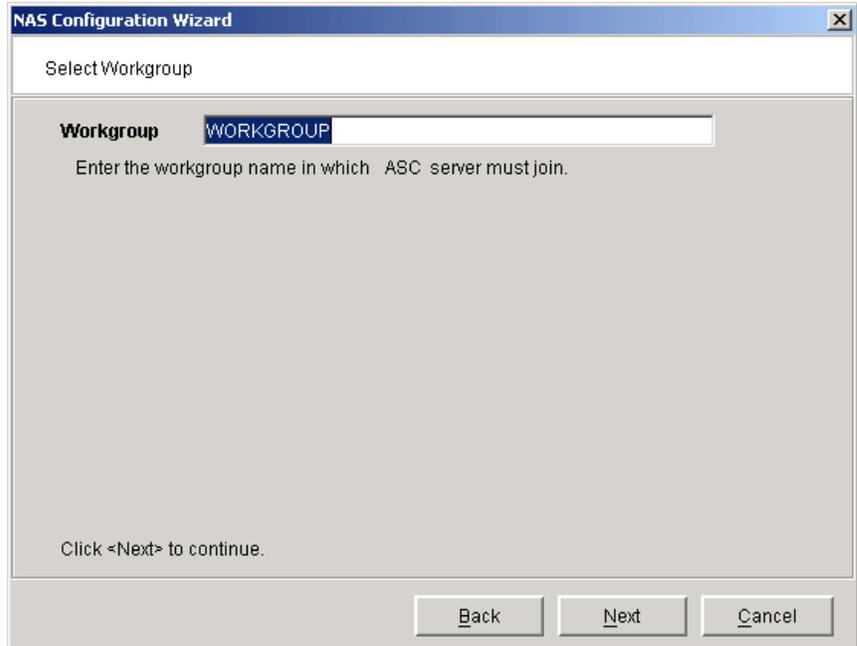


Enter the existing workgroup of your ASC Server or you can group all of your ASC Servers in a new workgroup. This can be useful for locating your ASC Servers in your Windows Explorer.
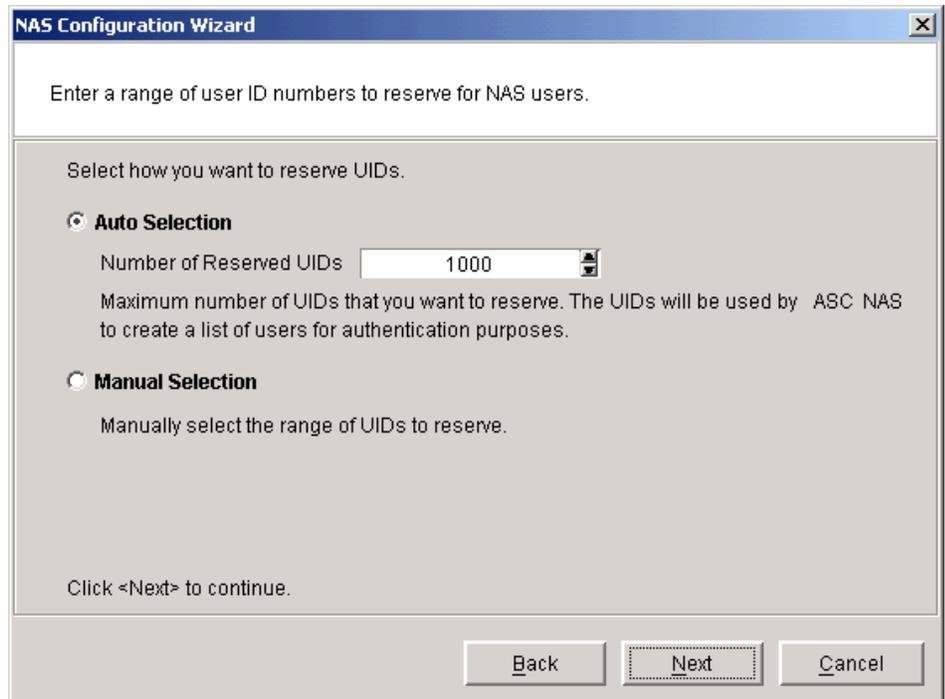
7. (All authentication modes) Enter a comment and the applicable client code page.

*Comment* - Enter a description of the ASC Server. This description will be displayed in the *Comment* field of Windows Explorer, such as when you see a list of computers under *My Network Places*.

*Client Code Page* - Specify the DOS code page that clients accessing Samba are using. To determine what code page a Windows client is using, open a DOS command prompt and type the command chcp. This will output the code page.

(All authentication modes) Select how you want to reserve User IDs.

**NAS Configuration Wizard**

Enter a range of user ID numbers to reserve for NAS users.

Select how you want to reserve UIDs.

◉ **Auto Selection**

    Number of Reserved UIDs     1000

    Maximum number of UIDs that you want to reserve. The UIDs will be used by ASC NAS to create a list of users for authentication purposes.

○ **Manual Selection**

    Manually select the range of UIDs to reserve.

Click <Next> to continue.

[ Back ] [ Next ] [ Cancel ]

UIDs are associated with users on your system (such as administrators).

Auto Selection lets you set the maximum number of UIDs that ASC should use for authentication of your NAS users and then automatically reserves an unused range.

Manual Selection lets you select exactly which range(s) to use. If you select this, you will need to select an available UID range and designate a starting and ending UID.

8. (Server or Domain Mode only) Select how you want to reserve Group IDs (GIDs). GIDs are associated with groups on your system.

*Auto Selection* lets you set the maximum number of GIDs that ASC should use for authentication of your NAS groups and then automatically reserves an unused range.

*Manual Selection* lets you select exactly which range(s) to use. If you select this, you will need to select an available GID range and designate a starting and ending GID.

9. (All authentication modes) Confirm all information and click *Finish* to start the NAS daemons.

If you want to update these settings later, right-click on the *Windows Clients* object (under *NAS Clients*) and select *Properties* or *Set Security Mode*.

## Add NFS clients

1.  Right-click on the *NFS Clients* object and select *Add*.
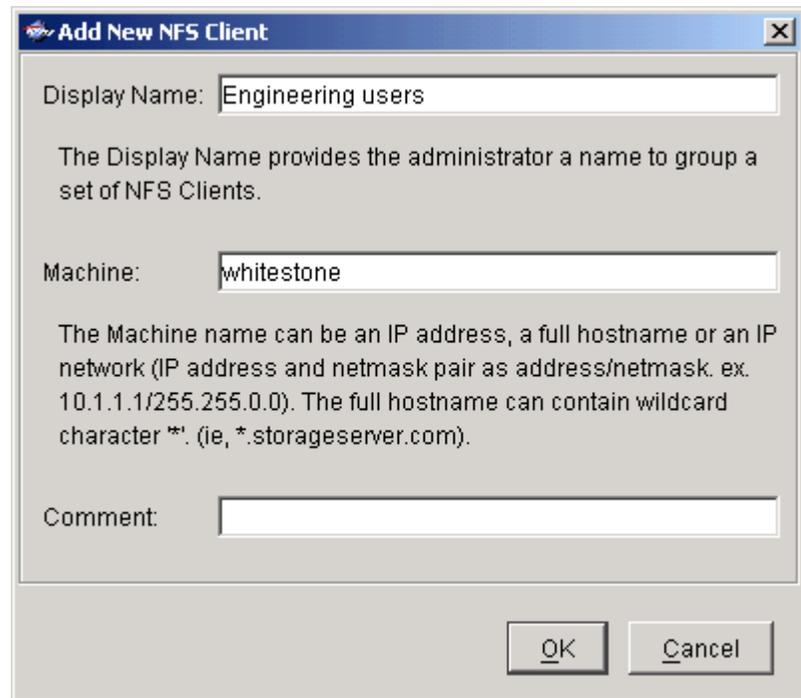


2.  Enter information as applicable.

*Display Name* - This is the name displayed in the Console for this group of one or more NFS clients.  For example, you may want to enter *Finance Department* to indicate where these clients are located.

*Machine(s) - Linux*:These are the machines that will become NFS clients. You can enter an abbreviated name that can be resolved, a fully qualified domain name, or an IP address for a machine. You can also include all machines on an IP sub-network by specifying an IP address and netmask pair as address/netmask.

Machine names can use the wildcard characters * and ?.  For example, *unixbox\** or *unixbox?* includes all clients in that subnet and *\*.acer.com* matches all clients in the domain *acer.com*. But *10.1.1.\** or *10.1.1.?* are not acceptable.

*Solaris*: You can use a DNS domain name in the access by preceding the actual domain name with a dot, such as:
(server1.storageserver.com .storageserver.com)
or an IP network:
(single host: "@192.168.10.2/32", subnet: "@192.168" or "@192.168.0.0" or "@192.168.132/16).

In above example, the "/16" indicates that the first 16 bits in the address are to be used as the mask. For more information, refer to the Solaris share_nfs(1M) man page.

*Comment* - You can optionally enter a description or explanation in this field. This information will be displayed in the right pane of the Console for this client.

## Create a NAS Resource

The maximum number of NAS Resources that can be created is 64. If configured as part of a failover set, the combined number of NAS Resources on each ASC Server must be less than or equal to 64.

1. Right-click on the *NAS Resources* object and select *Create NAS Resource Wizard*.

2. Select how you want to create this NAS Resource.
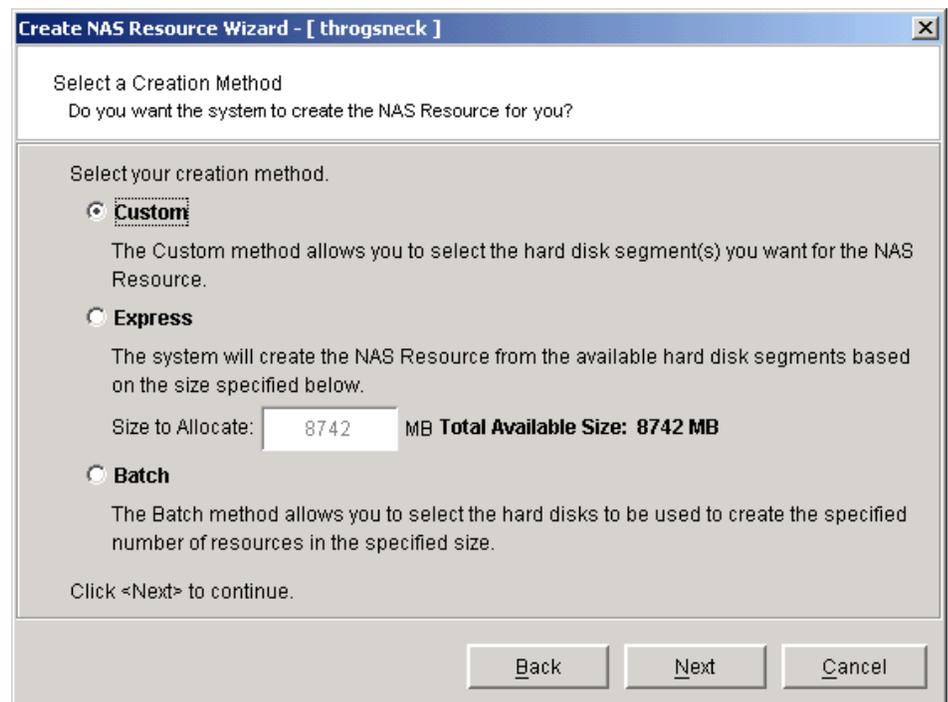


*Custom* lets you select which physical device(s) to use and lets you designate how much space to allocate from each.

*Express* lets you designate how much space to allocate and then automatically creates a NAS Resource using all available devices.

*Batch* lets you create multiple NAS Resources at one time. These NAS Resources will all be the same size.

If you select *Custom*, you will see the following windows:

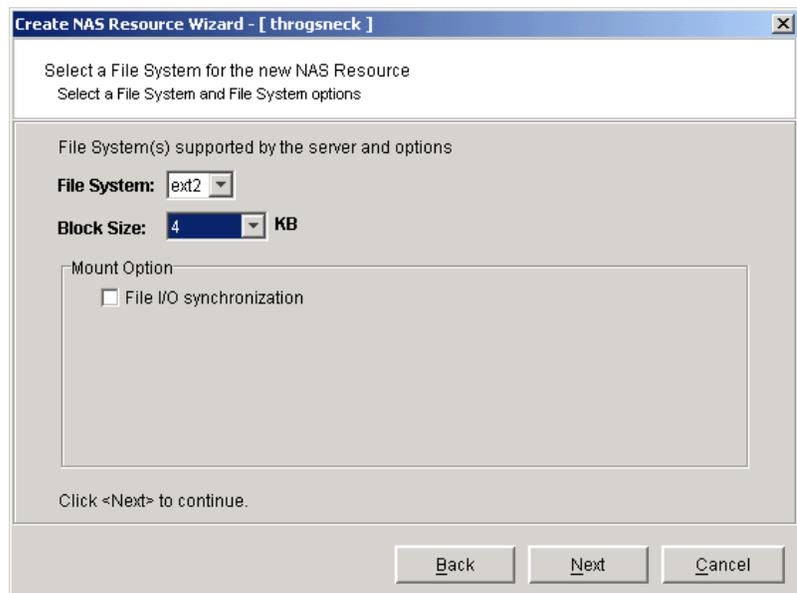If you select *Batch*, you will see the following windows:
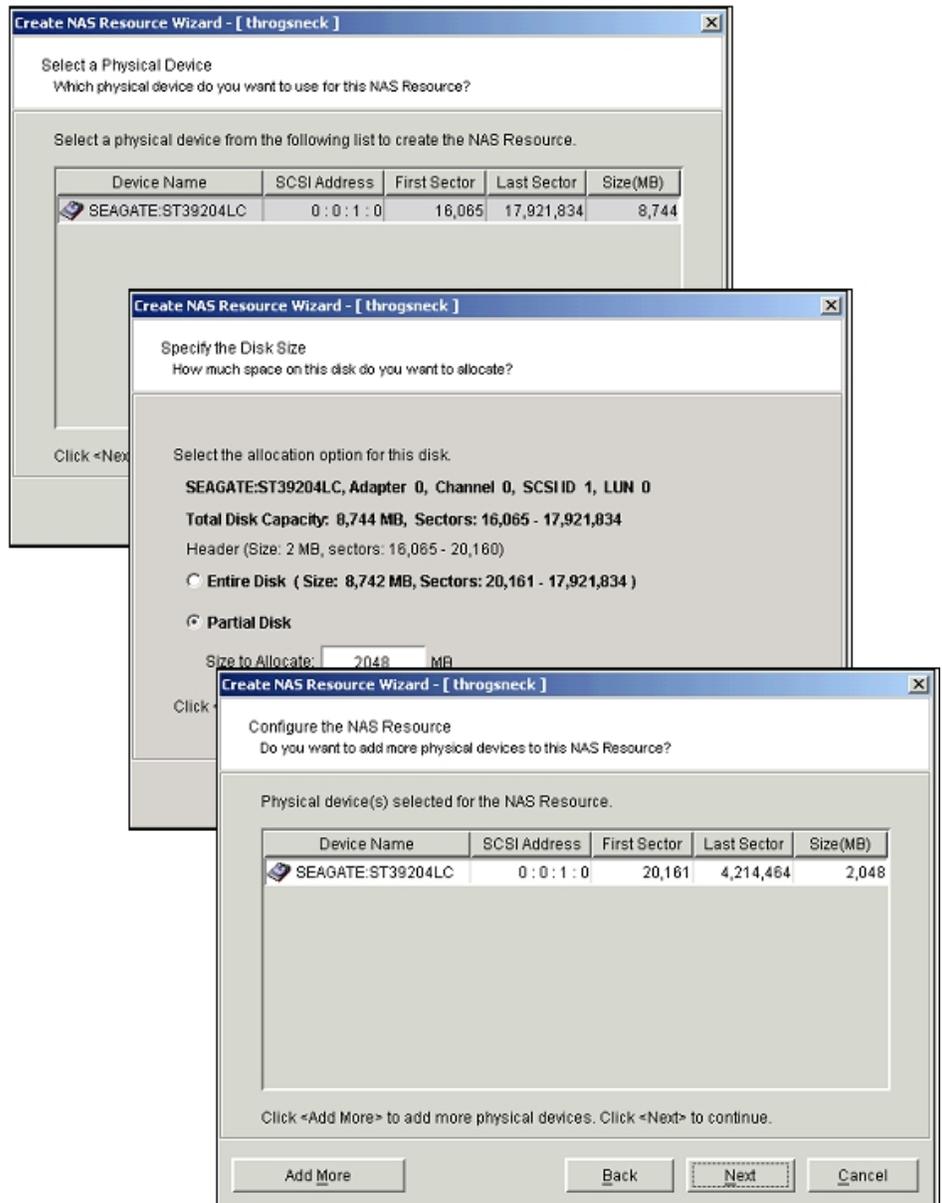
3. (*Express* and *Custom* only) Enter a name for the new NAS Resource.
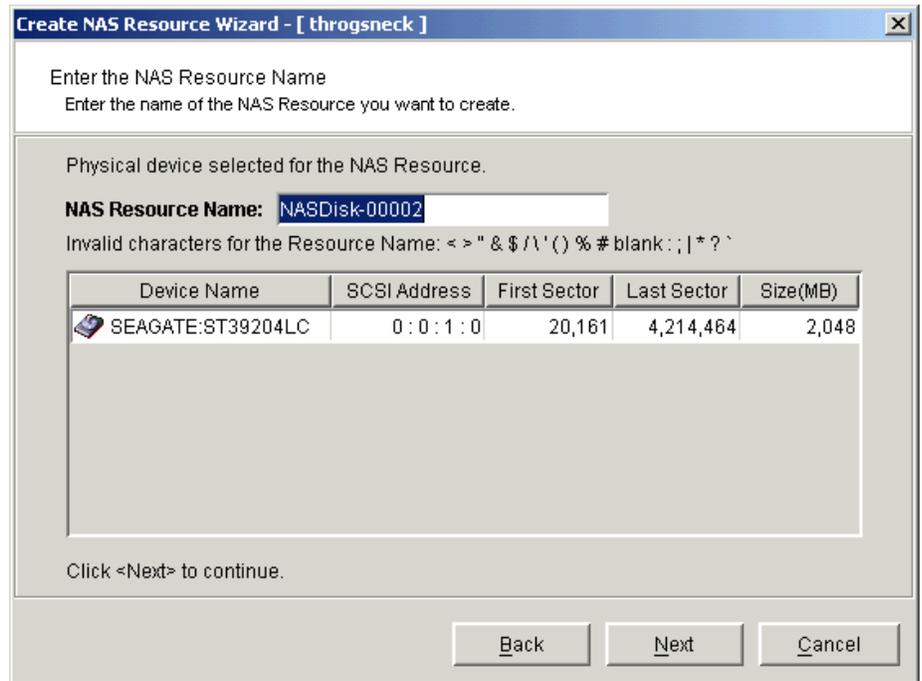


You cannot use blanks or the following characters in the resource name such as
< > " & $ / \ ' ( ) % # : ; | * ` ?

4. Enter information about your file system.

*File System* - ASC automatically detects the file systems supported by the system. If the server has the required ACL rpms installed, *XFS* will appear in the list; otherwise only *EXT3* and *EXT2* will appear.

*Block Size* - The minimum amount of space to use for each file.  For example, if you keep the default of 4, each file will minimally be 4k in size.

*Synchronous File I/O* -  Provides file system caching.  If selected, there will be no file system caching.  This offers greater data integrity but impacts performance.

*Journaling Mode* - (Linux EXT3 only) Specifies the journaling mode for file data. Metadata is always journaled.

- *Journal:* All data is committed into the journal prior to being written into the main file system.

- *Ordered:* This is the default mode.  All data is forced directly out to the main file system prior to its metadata being committed to the journal.

- *Writeback:* Data ordering is not preserved. Data may be written into the main file system after its metadata has been committed to the journal. This is said to be the highest-throughput option.  It guarantees internal file system integrity, but it can allow old data to appear in files after a crash and journal recovery.

Confirm that all information is correct and then click *Finish* to create the NAS Resource. You should wait until the NAS Resource is attached and mounted before continuing with folder assignments.



NOTE: After creating your ASC NAS resources, check the ASC Server for the following file: /etc/group

cat the /etc/group file and note the number for the *nasgrp*.

When using NFS-mounted ASC NAS Resources, log in with a user account that is a member of the group number for *nasgrp*.

## Limit the amount of storage each Windows user can have.

1. Right-click on the NAS Resource and select *Quota Manager*.

You can also right-click on the *Users* object (under *Windows Clients*) or on a specific Windows Client and select *Set Quota*.
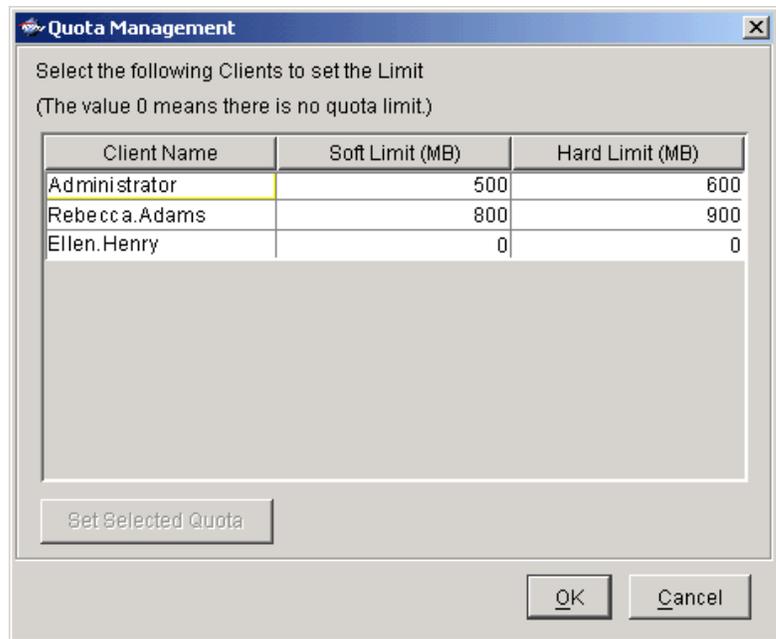


The default is zero, which means there is no limit.

2. Select one or more clients and click the *Set Selected Quota* button.
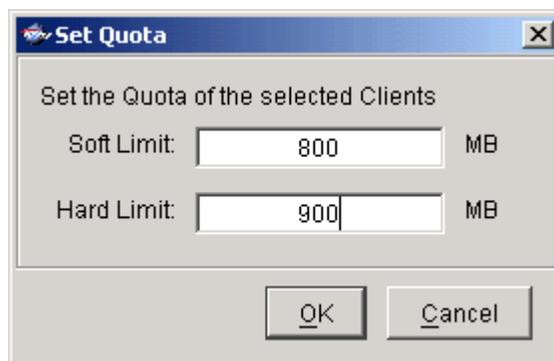


When a Windows Client's usage hits the *Soft Limit*, they will be warned.

When the Client's usage hits the *Hard Limit*, they will be prevented from using additional storage.

## Restore quota data

If you lose the quota information due to filesystem corruption or user error, you can re-apply the quota settings by right-clicking on the NAS Resource and selecting *Resync Quota*.

## Add/share a folder and assign clients

You do not need to create each user's home directory if [homes] is enabled on your ASC server. Refer to Homes for more information.

1. Right-click on a NAS Resource or a folder and select *New Share.*

You can also select *New Folder*. Any time after creating the folder, you can assign clients to it by right-clicking and selecting *Sharing*.

2. Enter a folder name.



The folder name cannot exceed 238 characters.

3. Enter a share name and indicate if you want Windows clients to have access to this share.

```
Create Share Wizard                                              [X]
Configure the Windows Share Setting
  Set the properties of the new Share

     ☑ Enable Windows Sharing

     Share Name: [Manuals                           ]

     Comment:    [For User Guide                     ]

     User limit:    ⦿ Maximum allowed
                    ○ Allow  [ 1 ]⬍ Users




     Click <Next> to continue.

                              [  Back  ]  [  Next  ]  [ Cancel ]
```
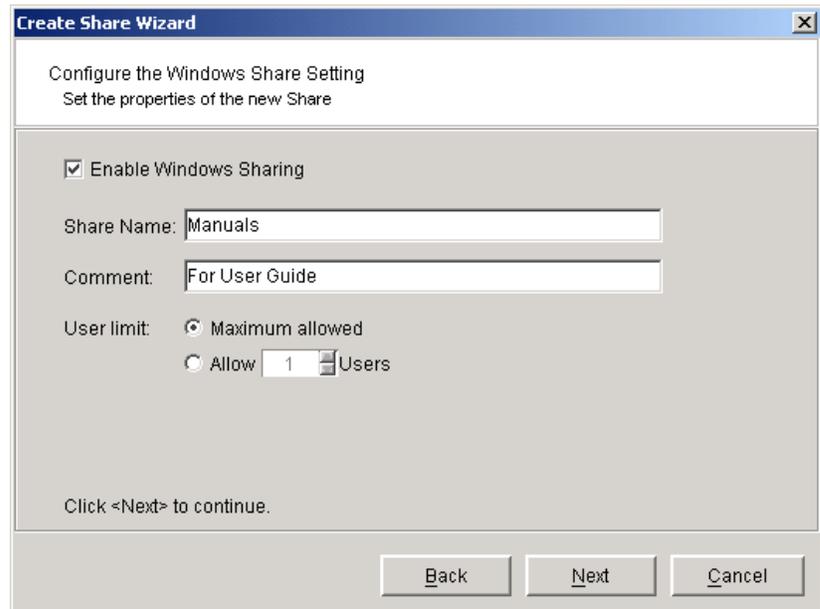
Share names cannot start with a dot or contain the following characters \ / : * ? " < > | # % [ ] = + ; ,

4. (Windows clients) Enter permissions for the Windows clients who will access the share.

If you add new Windows users/groups to your server at a later time, you can assign shared folders to them in two ways:

- You can right-click on the new user in the tree and select *Assign Share*.

- You can right-click on the shared folder, select *Sharing*, click on the *Permission* button, and click on the *Assign Windows Clients* button.

5. (NFS clients) Enter permissions for the NFS clients who will access the share.
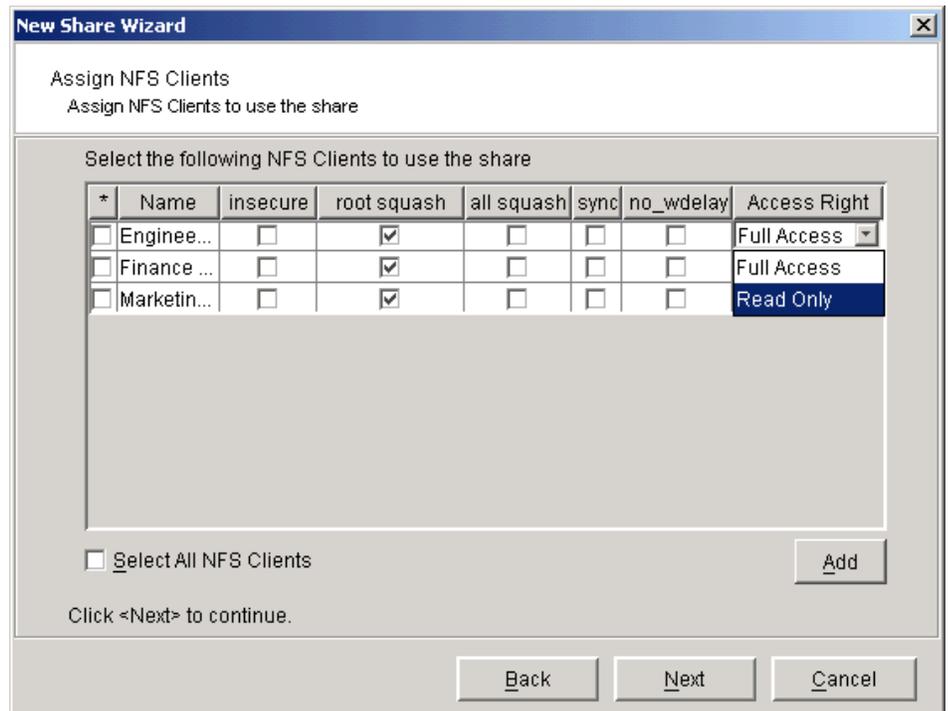


| root_squash | all_squash | Action |
|---|---|---|
| - | - | No UIDs are mapped |
| X | - | UID=0 (root user) is remapped to nfsnobod:nasgrp (default) |
| X | X | All UIDs are mapped to nfsnobod:nasgrp |

If you use ASC's Failover option, we recommend you use the *Sync* and *No_wdelay* options.

If you add new NFS clients at a later time, you can assign shared folders to them in two ways:

- You can right-click on the new client in the tree and select *Assign Share*.

- You can right-click on the shared folder, select *Sharing*, select the *NFS* tab, and click the *Assign NFS Client* button.

## Map/mount the share

### Windows clients

You should map a share for each Windows client so that they have access to the share.  Do the following on each Windows client's computer:

1.  Open *Windows Explorer* (or *My Computer*).

2.  Select *Tools --> Map Network Drive*.

3.  Set the path to the shared folder.

The path is:  \\*hostname*\*sharename*

Note that if [homes] is enabled on your ASC server running in server or domain mode, users can map to \\*hostname*\homes or \\*hostname*\*username*. Refer to Homes for more information.

4.  Enter login information.

For *Share* mode, enter the password you set when you created the share. You can leave the *Connect As* field blank.

For *Server* and *Domain* modes, enter the user's account name in the *Connect As* field and the user's password.  For *Domain* mode, be sure to enter the user's full account name (including domain name).

If your Windows NT/2000 client is authenticated into one domain while your ASC Server is part of another domain, you must enter the following into the *Connect As* or *Username* field:

where *DomainX* is the name of the domain with the drive you wish to map and *UserY* is the username allowed on that Windows machine.  Enter the correct password for *UserY*.

**NFS clients**

You must mount a share for each NFS client so that they have access to the share.  Do the following on each NFS client's computer:

1. Create a directory. (For example:  /mnt/share)

2. Locally, mount the share.

mount *hostname*:/nas/*nasresourcename*/*foldername*  /mnt/share

Note: In the path above, /nas/ is not a variable and must be included in the path.

You can use the following Unix utility to list all of the shares:

```
showmount -e <ASCServerName>
```

3. (AIX clients only) The AIX client uses a high port (above 1024) for NFS. In order for NAS to work correctly, the following line needs to be added to the /etc/rc file:

## Audit NAS shares

You can set ASC to audit the activity in Windows NAS shares. This feature tracks when users do any of the following:

- Connect/disconnect to/from a share
- Create and delete directories
- Open a file
- Rename a file
- Delete a file
- Change permissions

**To use the auditing feature:**

1. Create a NAS Resource.

The audit log is a text file that contains the NAS activity. If you will be auditing multiple shares, you need to make this NAS Resource large enough to hold all of your audit logs.

Note:  We recommend creating the NAS Resource/share on a different physical device than the NAS Resources you will be auditing so that the performance of those NAS Resources is not impacted.

2. Create a share on the newly created NAS Resource that will be used to store the audit log.

Right-click on the new NAS Resource and select *New Share*. Use the wizard to create a share and give it a name such as "auditshare".

3. Right-click on any existing share and select *Sharing* --> *Advanced* button.

If [homes] is enabled on your ASC server running in server or domain mode, you can easily audit all NAS shares beneath the [homes] share by selecting *Windows Clients* --> *Properties* --> *Homes* tab. Refer to Homes for more information.

4. Select *Audit* and select the share (i.e. "auditshare") that should hold your audit data for this share.

Note that you cannot select *Auditing* and *Anti-Virus* for the same share.

*Note: The "auditshare" should be assigned to a designated system auditor for viewing of the audit data. To prevent compromising the audit, only the designated auditor should have read/write access to it. It is possible to create multiple audit shares and associate your data shares to them. This allows you to designate different auditors and audit-shares for your collection of data shares.*

## NAS properties

You can set NAS properties or update your NAS configuration settings by right-clicking on Windows Clients and selecting Properties.
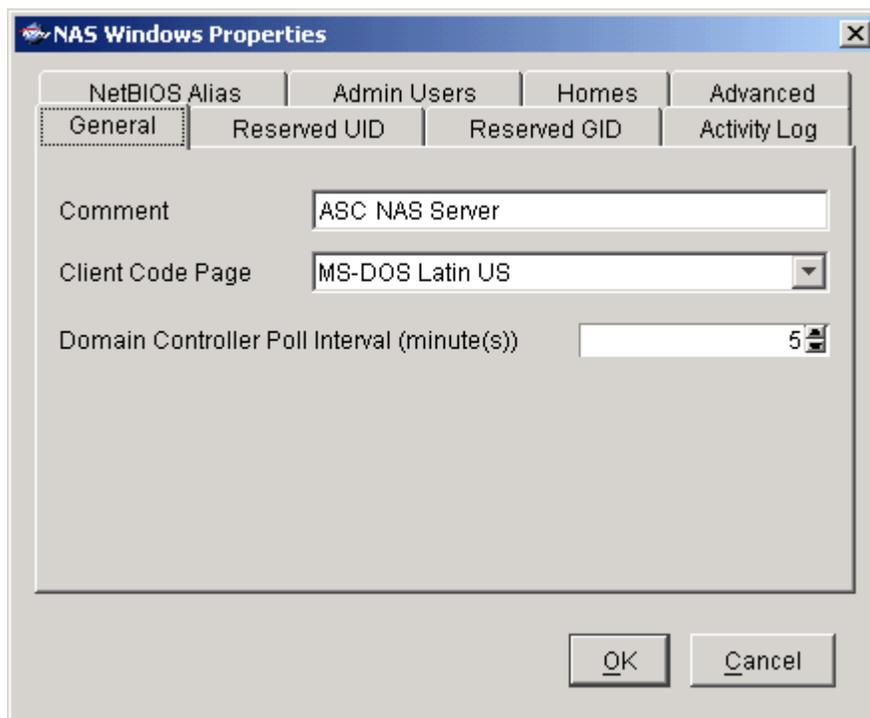


The tabs you will see depend upon your authentication mode.

General

On the *General* tab, you can change your comment and/or client code page and set the interval that determines how often ASC should poll the domain controller for the latest users/groups.

Reserved UID/GID

On the *Reserved UID/GID* tabs, you can select available UID/GID range(s). GID range is for Server and Domain modes only.

Activity Log

On the *Activity Log* tab, determine how long NAS information should be kept for ASC reports.

NetBIOS Alias

On the *NetBIOS Alias* tab, you can set a NetBIOS alias for a Samba server, giving the server more than one NetBIOS name.

Admin Users

(Server and Domain modes only) On the *Admin Users* tab, you can give a user administrative rights by making the user *root* equivalent on the ASC Server.

Homes

(Server and Domain modes only) On the *Homes* tab, you can set [homes] properties and select to audit all NAS shares.

[homes] is a Samba feature that permits users to map to a NAS share based on their username. When you enable [homes], you do not need to create shares for each user. Instead, when the user maps to [homes] on the ASC server, a directory will be created for them based on their username.
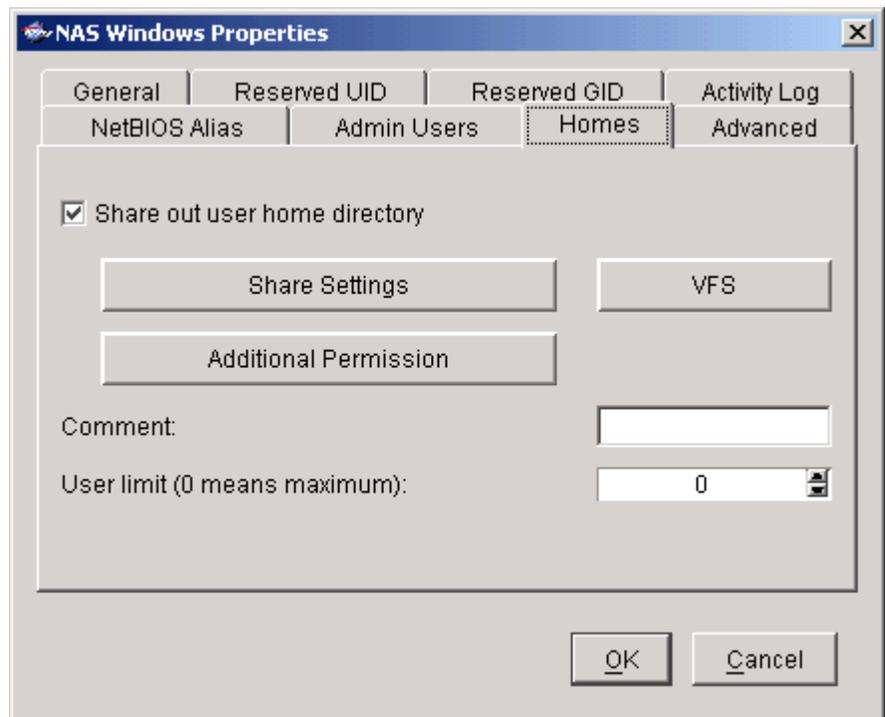


When you check the *Share out use home directory* option, you will see the following:
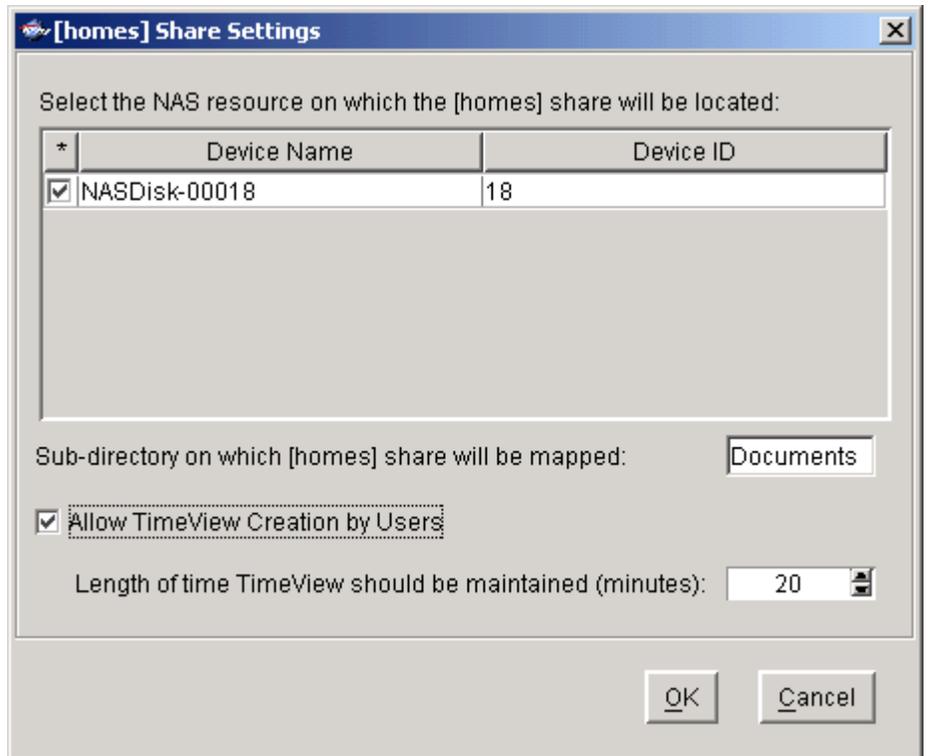
Select the NAS resource on which the [homes] share will be located - Users will map a share on this NAS resource in one of the following ways:

\\servername\homes   (the system uses the username from their current login)
or
\\servername\username

Sub-directory on which [homes] share will be mapped - This sub-directory is a folder that must already exist on a NAS resource. It becomes the root folder for the [homes] share. Shares for users are created beneath, and relative to, this folder. You may want to make this sub-directory a separate share that is assigned to the system administrator only. This way the system administrator can set ACLS, permissions, etc., and have the settings apply to all users.

Allow TimeView Creation by Users - Allows users to auto-mount a read-only version of the latest TimeMark in order to recover data. TimeMark must be enabled for the [homes] share. A TimeView will be automatically created when the user maps to their share with a tilda:

\\servername\~homes (uses the username from their current login)
or
\\servername\~username

Length of time TimeView should be maintained (minutes) - How long the

TimeView should remain mounted. The TimeView will be deleted when this length of time is reached.

Note: If the user is mapped to the TimeView when the length of time expires, the TimeView will be deleted and recreated. This will cause the client to lose its connection and the client will have to remap to the new TimeView.

Advanced

On the Advanced tab, you can change ASC's default global Samba options.

For example, if you have an existing group that you are using, you can change force group from the default nasgrp to your group, such as:

force group = engineering

You can alse set wins server and name resolve order if you do not have any DNS set up and the server is on a different subnet than the CIFS clients. For example:

wins server = 192.168.0.1

name resolve order = wins bcast host lmhosts

If you have Windows users that belong to more than 32 groups, you can set cache supp groups to dynamically load the relevent groups that the user belongs to based on the access required.

NAS directory permissions

You can set basic Unix permissions for NAS directories by right-clicking on a NAS folder and selecting Directory Properties.

**Directory Property** ☒

The permissions on the selected directory are:

Share Security:     NFS

Directory Name:     /nas/data/Pensacola

Owner               root

Group               root

Mode Bits

| | | | |
|---|---|---|---|
| Owner | ☑ Read | ☑ Write | ☑ Execute |
| Group | ☑ Read | ☐ Write | ☑ Execute |
| Other | ☑ Read | ☐ Write | ☑ Execute |

☐ Sticky bit

☐ Include subdirectories

OK     Cancel
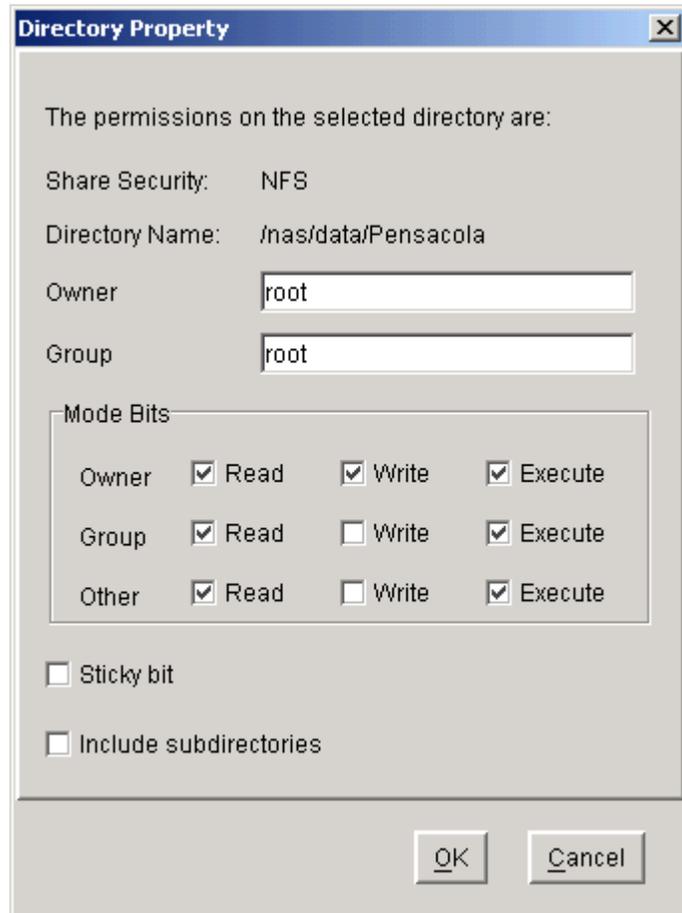
## NAS file information

NAS clients use the shares assigned to them and, depending upon their access rights, can create, share, read, and write files/folders as necessary, keeping the following limitations/suggestions in mind:

- The maximum size of each NAS Resource is dependent upon the operating system of the ASC Server. For RedHat v7.3, each NAS Resource can be up to 2 TB in size. For RedHat v7.2, each NAS Resource can be up to 1 TB in size. For Solaris UFS, each NAS Resource can be up to 1 TB in size.

- The maximum file size is dependent upon the operating system of the ASC Server. Solaris UFS has a 1 TB file size limit. RedHat v7.3 has a 2 TB file size limit. RedHat v7.2 has a 1 TB file size limit. The client software being used by the NAS user may limit this further. For example, NFS v2 has a <2 GB file size limit and CIFS has a 1 TB file size limit.

- You can have a maximum of 100 Windows users/groups per NAS share.

- Do not create files or directories on NFS mounted resources that would be invalid when shared with Windows clients and vice versa. For example, an NFS file or directory with the name * would be invalid for Windows.

- The following names are reserved by Windows: *com1-com9*, *lpt1-lpt9*, *con*, *nul*, *prn*, or *aux*. Even though NFS/Unix clients can use them, Windows clients cannot. Therefore, these names cannot be entered in the Console.

- Folder names cannot start with a dot, contain a blank or contain the following characters \ / : * ? " < > | # %

- Share names cannot start with a dot or contain the following characters \ / : * ? " < > | # % [ ] = + ; ,

- NAS supports the Windows *read* and *write* files attributes.

- Folder attributes on NAS resources are not supported.

- If a Unix user creates NFS files that he/she want to share them with CIFS (Windows) ASC clients, the Unix user needs to set his/her umask to 002 so that all NAS group members can have read/write access to the files.

- While ASC supports file locking for Windows files, there is no file locking between Unix and Windows. This means that a Unix user could open and write to a file that is open (locked) by a Windows user. This is an inherent difference between Unix and Windows.

## NAS utilities

ASC provides several utilities you can use to manage your NAS Resources. They are accessible by right-clicking on a NAS Resource and selecting the appropriate option:

- *Remove/Add Journal* - (Linux only) For backwards compatibility purposes, *Remove Journal* turns an EXT3 filesystem into an EXT2 filesystem.

- *Format* - Formats the NAS Resource and deleting all information on it.

- *Mount/Unmount* - (Depending upon mount status) Allows you to manually mount or unmount a NAS Resource on/from the ASC server. Clients should be disconnected before unmounting.

*File System Checking* - Performs a file check on a NAS resource and fixes any file system errors. This option disconnects all clients before executing file system check.

## Expand a NAS Resource

Since NAS Resources do not represent actual physical resources, they can be expanded as more storage is needed. The resource can be increased in size by adding more blocks of storage from any unallocated space from the same server.

We do not recommend expanding an EXT2 or EXT3 resource while clients are accessing the drives. However, when expanding an XFS resource, NAS clients can remain connected.

## Access Control Lists (ACLs)

ACLs allow administrators to define more fine-grained access to files and directories. Instead of assigning Windows clients permissions at the share level, ACLs allow the permissions to be applied to the files and directories beneath the share. ASC currently supports POSIX ACL.

If you are running ASC NAS in Server/Domain mode, you can assign a share to several users. By default, all assigned users will have full or read-only access to the entire share. Without ACL support, if you want one user to be able to read and write to his/her files but not another's files, you would have to create separate shares. With ACLs, this can be done from the Windows Explorer's security tab without creating additional shares.

### Using ACL attributes

For example, you have one share named "Data" and two users, UserA and UserB.  You want both users to have full access to a common sub-directory called "Everybody" and you want each user to have full access to his/her own directory. These are the steps you would take to accomplish this:

1.  Create a share named "Data" and assign the admin user, UserA, and UserB to the share.

2.  As the admin user, go to your Windows Explorer and map the share. For more information about mapping a share, refer to Map/mount the share.

3.  Modify the security of the base share by selecting *Properties* from Explorer and removing the "write" privilege from 'nasgroup'.

4.  Create three directories at the root of "Data": "UserADirectory", "UserBDirectory", "Everybody".

5.  Right-click on the "UserADirectory" directory and select *Properties –> Security*.

6.  Add users UserA and UserB.

    By default, the newly added users will only have read access.

7.  To give write access, select UserA and check *Allow* for the *Full Control* box.

8.  Apply these same steps for the "UserBDirectory" and "Everybody" directories.

For the "UserBDirectory" directory, give UserB *Full Control*.

For the "Everybody" directory, give both UserA and UserB *Full Control*.

As a result, when UserA or UserB maps to the "Data" share, each user will have both read and write access to his/her own directory and the "Everybody" directory, but only read access to each other's directory.

**Requirements**

In order to use ACLs with NAS:

- The ASC Server must be running Red Hat 7.3 with 2.4.21-ipstor kernel (XFS filesystem).

- The following RPMS must have been installed during the intial installation:

    libacl-2.0.9-0.i386.rpm

    libattr-2.0.7-0.i386.rpm

    dmapi-2.0.2-0.i386.rpm

    acl-2.0.9-0.i386.rpm

    attr-2.0.7-0.i386.rpm

    xfsprogs-2.0.3-0.i386.rpm

    xfsdump-2.0.1-0.i386.rpm

- You must be using Server or Domain mode for authentication.

- Your NAS Resource must be formatted as XFS. It cannot be an EXT3 resource.

Windows users belonging to more than 32 groups

If you have Windows users that belong to more than 32 groups, you can set a Samba option to dynamically load the relevant groups that the user belongs to based on the access required.

Right-click on *Windows Clients* --> *Properties* --> *Advanced* tab --> *Add*.

Name: cache supp groups

Value: yes

Note that if the files and/or directories under the shares have very complicated access control, this can have some performance impact.

**Back up/restore extended attributes on Linux**

When you perform a file-by-file backup or restore of your NAS shares you will also want to back up/restore the extended attributes (ACL attributes and quota information). There are no special steps needed for a raw device (image/block level) backup/restore.

1. For backup:
   Use **"getfacl -R"** and **"getfattr -R-d"** to back up the ACLs/attributes.

These commands can be used to back up/export extended attributes of filesystem objects and should be run in a simple batch file or by using the pre-process command, if your backup application supports this. The files generated by these commands should be backed up by your backup software because they will be used during the restore process to restore ACLs and attributes.

The usage is as follows:
getfacl -R *source* > *file1*
getfattr -R-d *source* > *file2*

Where *source* is the name of the file or directory that will be backed up.
*file1* is the name of the output file that will be used for restoring the ACLs and
*file2* is the name of the output file that will be used for restoring the extended attributes.
The "-R" option is used to list the extended attributes of all files and folders recursively.

Use your backup software to make a backup of your XFS filesystem including *file1* and *file2*.

For restore:

2. Use your restore software to restore your filesystem, directory, or file(s).
   Be sure to restore the files created using the *getfacl* and *getfattr* commands (*file1* and *file2* in our example). These files will be used to apply the ACLs and attributes of the filesystem, directory, or file being restored.

3. Use **"setfacl --restore"** or **"setfattr --restore"** to apply the restored attributes.
   setfacl --restore=*file1*
   setfattr --restore=*file2*

where *file1/file2* are the names of the output files created when using the *getfacl* or *getfattr* command.

For further information on the usage of these utilities, refer to the man pages.

**Acer Altos® NAS 700 Solution Guide**

Free Manuals Download Website

[http://myh66.com](http://myh66.com)

[http://usermanuals.us](http://usermanuals.us)

[http://www.somanuals.com](http://www.somanuals.com)

[http://www.4manuals.cc](http://www.4manuals.cc)

[http://www.manual-lib.com](http://www.manual-lib.com)

[http://www.404manual.com](http://www.404manual.com)

[http://www.luxmanual.com](http://www.luxmanual.com)

[http://aubethermostatmanual.com](http://aubethermostatmanual.com)

Golf course search by state

[http://golfingnear.com](http://golfingnear.com)

Email search by domain

[http://emailbydomain.com](http://emailbydomain.com)

Auto manuals search

[http://auto.somanuals.com](http://auto.somanuals.com)

TV manuals search

[http://tv.somanuals.com](http://tv.somanuals.com)