SGI NAS

CIFS User Guide

Release 3.1.x

007-5949-001

SGI reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use.

Refer to the latest product announcement or contact your local SGI representative for information on feature and product availability.

This document includes the latest information available at the time of publication.

TRADEMARKS AND ATTRIBUTIONS

Document Number: 007-5949-001

Table of Contents

1 Overview

1.1 Purpose

This guide describes how to create the CIFS share on the SGI NAS side, operate shares in workgroup and domain modes, Active directory integration tips, give permissions to specified users, and create identity mappings.

1.2 Audience

The audience for this guide is SGI NAS administrators, system administrators, users or any other involved parties.

1.3 Document conventions

- SGI NAS Management Console (NMC) commands:

```
nmc:/$
```

- UNIX shell commands:

```
#
```

- A note or another piece of important information:

1.4 Introduction

SGI NAS provides one of the best existing kernel and ZFS-integrated CIFS stacks, with native support for Windows Access Control Lists (ACL).
This document explains how to use CIFS capabilities to share SGI NAS folders for:

- Anonymous access
- Authenticated access in:
  - Workgroup mode
  - Domain mode

> CIFS service operational mode is system-wide, and it is either workgroup or domain. To state the same differently, SGI NAS cannot provide some CIFS shares to workgroup users and, simultaneously, other shares to users joined via Active Directory.
>
> By default, NexentaStor operates in workgroup mode. The default pre-configured workgroup name is: **WORKGROUP**.

1.5 What mode to choose?

The system administrator decides which mode can best match the company's network configuration needs.

Basically, workgroups are used in small companies or home networks and can be best understood as group of loosely connected computers. It means that each computer is sustainable on its own. It has its own user list, it’s own access control and its own resources. In order for a user to access resources on another workgroup computer, that exact user must be setup on the other computer. This method is simple to design and implement, but since your network is growing it becomes difficult for management. For example, a user needs an account on all the computers it needs to access and any account changes, (i.e. password changing) are need to be done on all the computers in a workgroup. It's not applicable for a network of 50 computer systems.

Workgroup mode:

- Applies in small networks (less than 10 computers)
- Easy to setup and doesn't require any additional knowledge
- Requires setting up account and password on each and every computer

Domain is a trusted group of computers that share security, access control and have data passed down from a centralized domain controller server or servers. Domain mode requires additional arrangements on Windows side, i.e it requires configured Domain Controller with DNS (Windows Server 2003/2008) which handles all the aspects of granting user permission to login. Domain mode is commonly used in large networks and provide advanced centralized management and security, but more complex in design and implementation at the same time.

Domain mode:

- Single location for all user accounts, groups and computers, passwords are the same for all computers.
- Requires configured Domain Controller (or two: primary and backup) with Active Directory and DNS server.
- More difficult to set up and requires additional knowledge.

Independently of whether you use appliance's CIFS for anonymous access, authenticated (workgroup) or in domain mode, the very first step is to configure CIFS server on SGI NAS. Read more about that in corresponding sections of this document:

1.6 Terminology

Check out the following table to view terms that used in this document:

Term	Description
CIFS[A]	Decipher as 'Common Internet File System' is an application-layer network protocol mainly used to provide shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. Mainly works with computers running Windows OS.
Active Directory	Active Directory is a technology that uses modified versions of existing protocols and services that provides a variety of network services, including: LDAP, Kerberos-based authentication, DNS-based naming, etc.
ID mapping	The possibility to integrate and give an access to Unix shared filesystems to Windows users. Mapping Windows SID to UNIX UID and GID.
Workgroup mode	The way to map CIFS share on SGI NAS to Windows OS without using domain.
Domain mode	The mode in which SGI NAS joins Active Directory.
Member Server	Is a computer that runs an operating system in the Windows 200x Server family, belongs to a domain and is not a domain controller.
Domain Controller	Is a computer that runs an operating system in the Windows 200x Server family and uses Active Directory to store a read-write copy of the domain database, participate in multimaster replication, and authenticate users.
Anonymous access	Access to CIFS share with user 'smb'

[A] Read more on http://en.wikipedia.org/wiki/CIFS

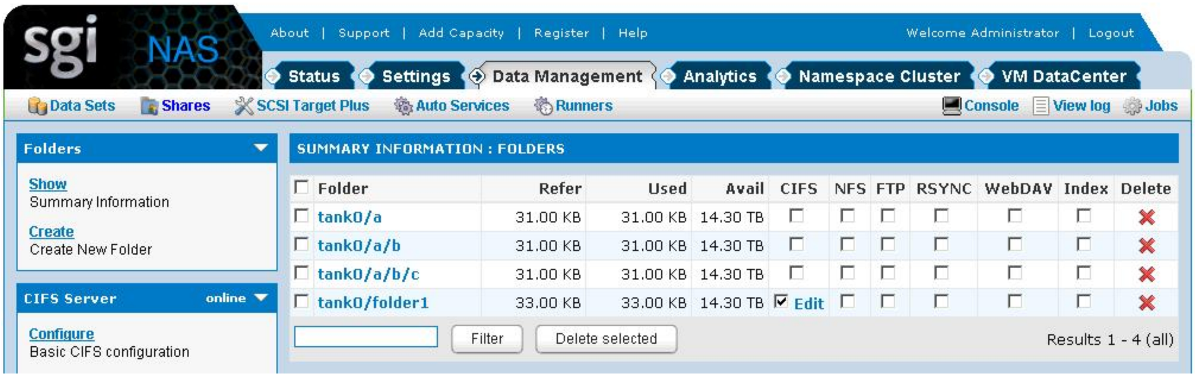
Authorized access	Access to CIFS share in Workgroup or domain mode with any user which have permissions to do it.
ACL	**ACL or Access Control List** is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
ACE	**ACE** or **Access Control Entry**
LDAP	**LDAP, or Lightweight Directory Access Protocol,** is a client-server protocol for accessing directory services. It runs over TCP/IP or other connection oriented transfer services.
SID	**SID, or Security Identifier**, is a unique name (an alphanumeric character string) which is assigned by a Windows Domain controller during the log on process that is used to identify a subject, such as a user or a group of users in a network of NT/2000 systems.
UID/GID	**UID**, **GID** or **User/Group identifier**, is a numeric value with which Unix-like operating systems identify *users* or groups within the kernel.

2 Managing the CIFS shares

2.1 Workgroup mode-Anonymous access

Anonymous access to CIFS allows anonymous users and authenticated users with limited permissions to browse the entire share and perform any actions, i.e. read, execute, write, copy, delete, etc. any files in this share.

SGI NAS provides a unified view of all network shares and simple consistent way to share appliance's folders via NFS, CIFS, FTP, WebDAV and RSYNC. In NMV, go to **Data Management** → **Shares** to view the shared folders:



SUMMARY INFORMATION : FOLDERS

□ Folder	Refer	Used	Avail	CIFS	NFS	FTP	RSYNC	WebDAV	Index	Delete
□ tank0/a	31.00 KB	31.00 KB	14.30 TB	□	□	□	□	□	□	✗
□ tank0/a/b	31.00 KB	31.00 KB	14.30 TB	□	□	□	□	□	□	✗
□ tank0/a/b/c	31.00 KB	31.00 KB	14.30 TB	□	□	□	□	□	□	✗
□ tank0/folder1	33.00 KB	33.00 KB	14.30 TB	☑ Edit	□	□	□	□	□	✗

Results 1 - 4 (all)

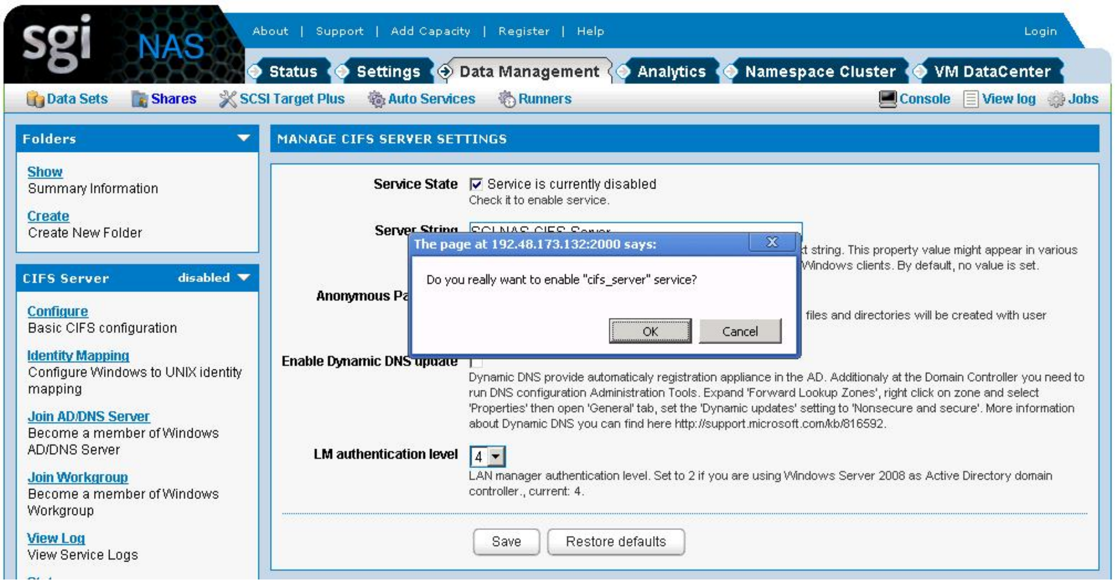
The corresponding NMC commands are '**show share**' and '**show folder**' (or '**df**'), for instance:

```
nmc:/$ show share
FOLDER                       CIFS    NFS    RSYNC  FTP    WEBDAV
myfolder/folder1              Yes     -       -     -       -
```

2.1.1 Configuring CIFS server

By default, SGI NAS is setup for Workgroup mode.

1. Check that CIFS server is properly configured. Check Service State, if it's unckecked to enable cifs service service:



MANAGE CIFS SERVER SETTINGS

Service State ☑ Service is currently disabled
Check it to enable service.

Server String SGI NAS CIFS Server
…t string. This property value might appear in various Windows clients. By default, no value is set.

Anonymous Pa…
files and directories will be created with user

The page at 192.48.173.132:2000 says:

Do you really want to enable "cifs_server" service?

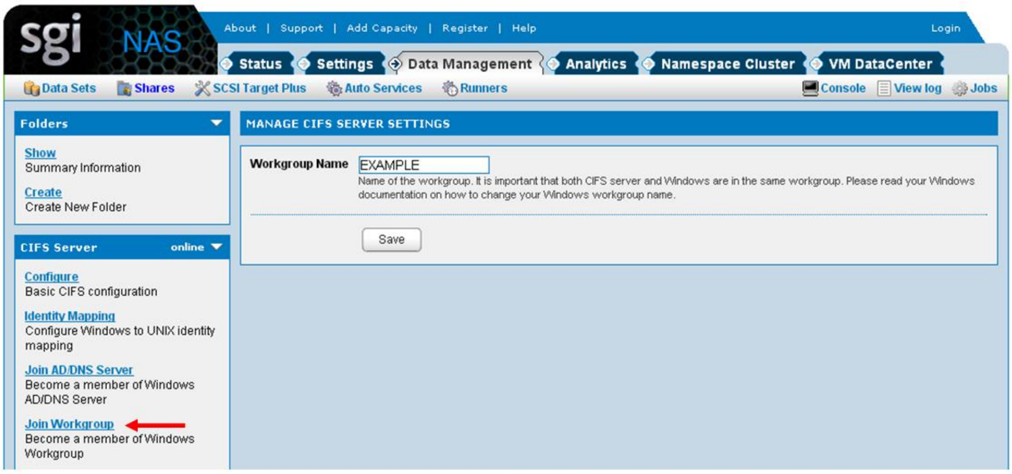
OK Cancel

Enable Dynamic DNS update □
Dynamic DNS provide automaticaly registration appliance in the AD. Additionaly at the Domain Controller you need to run DNS configuration Administration Tools. Expand 'Forward Lookup Zones', right click on zone and select 'Properties' then open 'General' tab, set the 'Dynamic updates' setting to 'Nonsecure and secure'. More information about Dynamic DNS you can find here http://support.microsoft.com/kb/816592.

LM authentication level 4
LAN manager authentication level. Set to 2 if you are using Windows Server 2008 as Active Directory domain controller., current: 4.

2. By default, the pre-configured group of CIFS users is: **WORKGROUP**. If this group name works for you, you do not need to change anything. Otherwise, to change the default:

   In NMV go to **Settings** → **Data Management**→ **Shares** and click on **<u>Join Workgroup</u>** link:



MANAGE CIFS SERVER SETTINGS

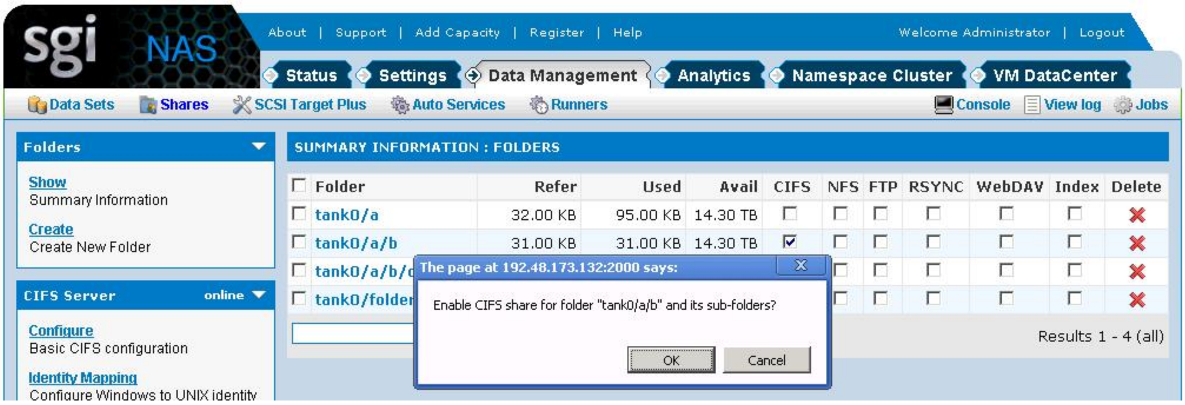
Workgroup Name EXAMPLE
Name of the workgroup. It is important that both CIFS server and Windows are in the same workgroup. Please read your Windows documentation on how to change your Windows workgroup name.

Corresponding NMC command:

```
nmc:/$ setup network service cifs-server join_workgroup
```

2.1.2 Create a CIFS share

In NMV go to **Data Management** → **Shares**, click on the checkbox under CIFS, opposite the folder you want to share. In the following example, we are sharing folder '**tank0/a/b**':



SUMMARY INFORMATION : FOLDERS

□ Folder	Refer	Used	Avail	CIFS	NFS	FTP	RSYNC	WebDAV	Index	Delete
□ tank0/a	32.00 KB	95.00 KB	14.30 TB	□	□	□	□	□	□	✕
□ tank0/a/b	31.00 KB	31.00 KB	14.30 TB	☑	□	□	□	□	□	✕
□ tank0/a/b/c					□	□	□	□	□	✕
□ tank0/folder					□	□	□	□	□	✕

Results 1 - 4 (all)

The page at 192.48.173.132:2000 says:

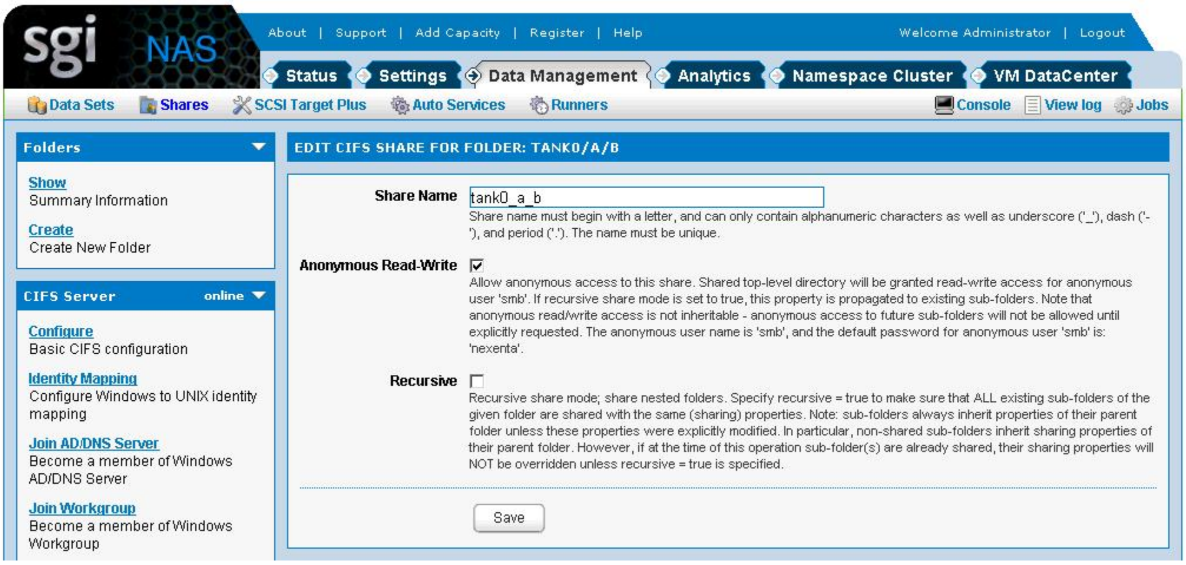
Enable CIFS share for folder "tank0/a/b" and its sub-folders?

Corresponding NMC command:

```
nmc:/$ setup folder tank0/a/b share
```

The operation is recursive – it'll share the folder and its sub-folders. Note, that in the example above **'tank0/a/b/c'** got shared as well. However, '**tank0/a**' doesn't get shared.

Click **Edit** to edit the shared folder's settings.



EDIT CIFS SHARE FOR FOLDER: TANK0/A/B

Share Name: tank0_a_b

Share name must begin with a letter, and can only contain alphanumeric characters as well as underscore ('_'), dash ('-'), and period ('.'). The name must be unique.

Anonymous Read-Write ☑

Allow anonymous access to this share. Shared top-level directory will be granted read-write access for anonymous user 'smb'. If recursive share mode is set to true, this property is propagated to existing sub-folders. Note that anonymous read/write access is not inheritable - anonymous access to future sub-folders will not be allowed until explicitly requested. The anonymous user name is 'smb', and the default password for anonymous user 'smb' is: 'nexenta'.

Recursive □

Recursive share mode; share nested folders. Specify recursive = true to make sure that ALL existing sub-folders of the given folder are shared with the same (sharing) properties. Note: sub-folders always inherit properties of their parent folder unless these properties were explicitly modified. In particular, non-shared sub-folders inherit sharing properties of their parent folder. However, if at the time of this operation sub-folder(s) are already shared, their sharing properties will NOT be overridden unless recursive = true is specified.

The screenshot above contains several important pieces of information:

1) Anonymous username

The built-in anonymous username is: '**smb**'. Unless you are using Active Directory (Section 2.3.2.Joining Active Directory), this is the name you will need to specify to access the share.

Anonymous read/write access is enabled by default.

2) Anonymous password

If you forgot the password, in NMV go to CIFS Server Settings (under **Data Management** → **Shares**), click on **Configure**, and re-enter the password. In NMC, the corresponding command is:

```
nmc:/$ setup network service cifs-server configure
```

3) Share name:

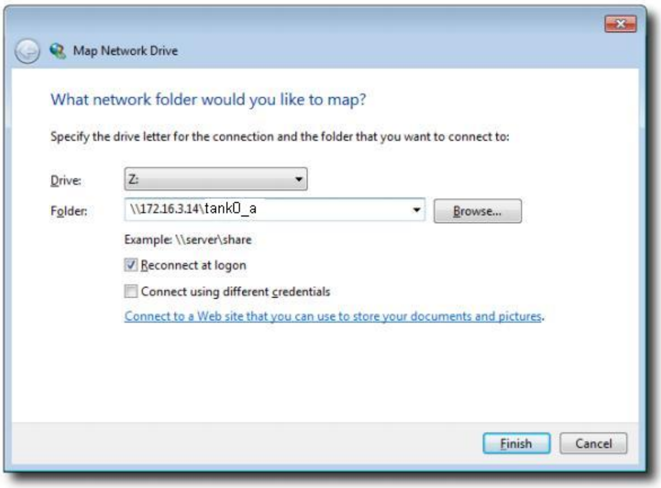
By convention, a folder named '**volume-name/folder-name**' becomes a CIFS share named '**volume-name_folder-name**'.

That fact is reflected on the previous screenshot: '**tank0/a/b**' is visible on CIFS clients under name '**tank0_a_b**' (see above).

You may change the appliance's generated CIFS share name by simply editing the corresponding field.

2.1.3 Map CIFS share on Windows computer

Next, on Windows machine go to **My Computer** → **Tools** → **Map Network drive** and fill the corresponding field with the appliance's hostname or IP address:



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\172.16.3.14\tank0_a

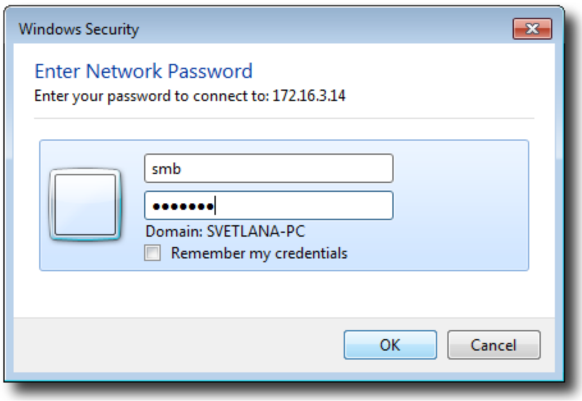
Example: \\server\share

☑ Reconnect at logon

☐ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

The very first time, login and password are required:


Windows Security

Enter Network Password

Enter your password to connect to: 172.16.3.14

smb

•••••••

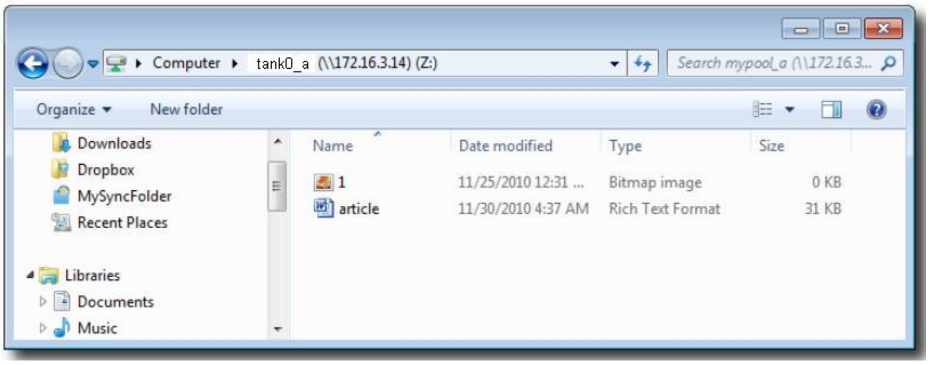
Domain: SVETLANA-PC

□ Remember my credentials

If you forgot the password, please go to CIFS Server Settings (under **Data Management** → **Shares**→ **Configure)** and re-enter the password. In NMC the corresponding command is:

```
nmc:/$ setup network service cifs-server configure
```

After successful authentication the shared folders show up:


Computer ▸ tank0_a (\\172.16.3.14) (Z:)

Search mypool_a (\\172.16.3...

Name	Date modified	Type	Size
1	11/25/2010 12:31 ...	Bitmap image	0 KB
article	11/30/2010 4:37 AM	Rich Text Format	31 KB

Depending on your Windows version, you can modify the ACL of these directories using Windows ACL editor (Right click **Properties** → **Security tab**).

Assuming anonymous access is enabled, we can now start using the SGI NAS folders as Windows directories.

2.2 Workgroup mode-Authenticated access

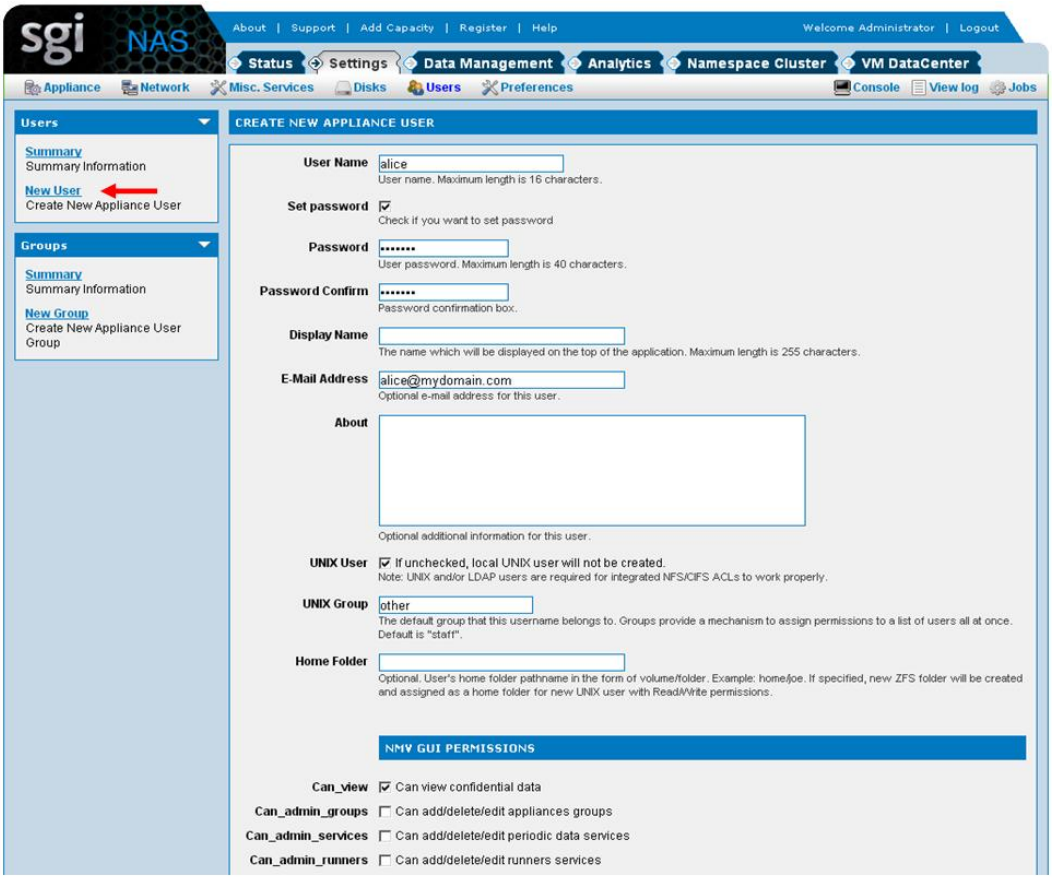
Authenticated method provides access to shares only to users which are authorized to access and allows to perform the actions according to permissions specified by Administrator. When users connect to a shared folder, they can open, save, delete, create, modify files and delete folders, and perform other tasks, depending on the level of granted permissions. Note, that you can't use name-based mapping in workgroup mode. Read more in 2.4.ID mapping and 2.5.ACLs sections.

2.2.1 Configuring CIFS Server

Check the corresponding section above 2.1.2.Configuring CIFS server

2.2.2 Creating a new appliance user

Create new appliance's user named '**alice**'. In NMV go to **Settings** →**Users** and click on **New User** link:



CREATE NEW APPLIANCE USER

User Name: alice
User name. Maximum length is 16 characters.

Set password: ☑
Check if you want to set password

Password: •••••••
User password. Maximum length is 40 characters.

Password Confirm: •••••••
Password confirmation box.

Display Name:
The name which will be displayed on the top of the application. Maximum length is 255 characters.

E-Mail Address: alice@mydomain.com
Optional e-mail address for this user.

About:
Optional additional information for this user.

UNIX User: ☑ If unchecked, local UNIX user will not be created.
Note: UNIX and/or LDAP users are required for integrated NFS/CIFS ACLs to work properly.

UNIX Group: other
The default group that this username belongs to. Groups provide a mechanism to assign permissions to a list of users all at once. Default is "staff".

Home Folder:
Optional. User's home folder pathname in the form of volume/folder. Example: home/joe. If specified, new ZFS folder will be created and assigned as a home folder for new UNIX user with Read/Write permissions.

NMV GUI PERMISSIONS

Can_view: ☑ Can view confidential data

Can_admin_groups: □ Can add/delete/edit appliances groups

Can_admin_services: □ Can add/delete/edit periodic data services

Can_admin_runners: □ Can add/delete/edit runners services

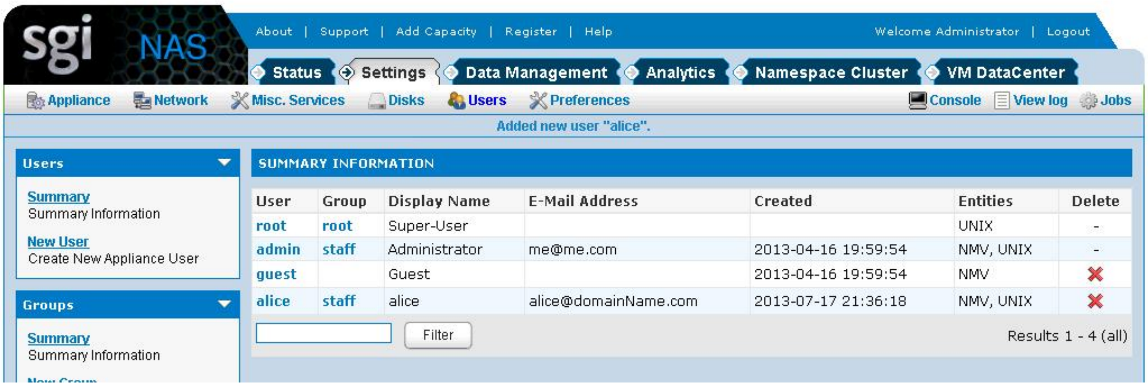
Fill the required fields and click '**Create New UI User**'

Corresponding NMC command:

```
nmc:/$ setup appliance user
Option ?  create
New User               : alice
Home folder            :
Description            :
Default group          : other
Password               : xxxxxx
```

```
Confirm password     : xxxxxx
```

This newly created user shows up in NMV:



Added new user "alice".

Summary
Summary Information

New User
Create New Appliance User

Summary
Summary Information

SUMMARY INFORMATION

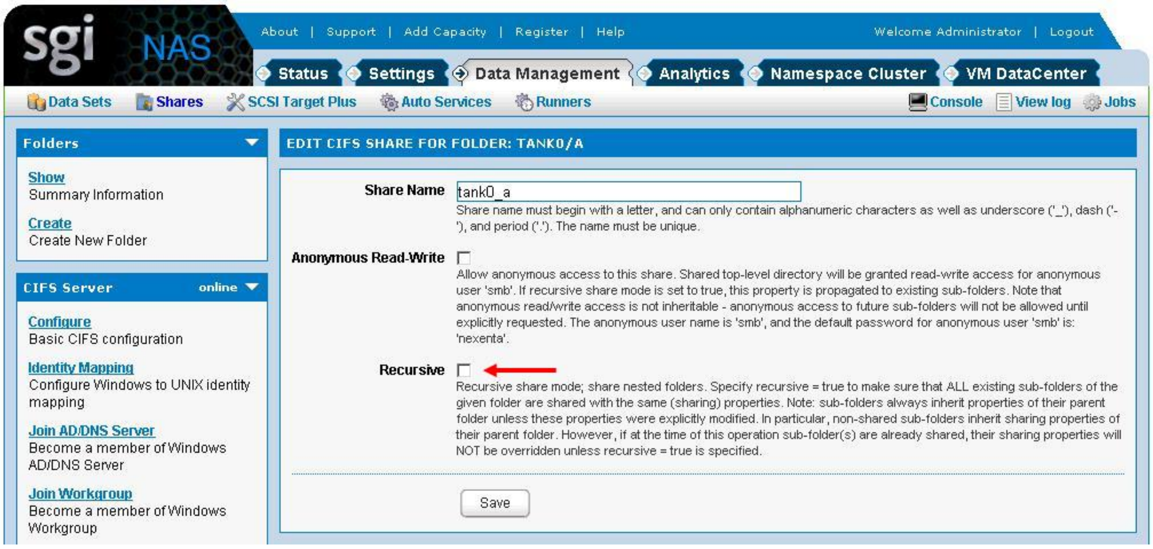
User	Group	Display Name	E-Mail Address	Created	Entities	Delete
root	root	Super-User			UNIX	-
admin	staff	Administrator	me@me.com	2013-04-16 19:59:54	NMV, UNIX	-
guest		Guest		2013-04-16 19:59:54	NMV	✕
alice	staff	alice	alice@domainName.com	2013-07-17 21:36:18	NMV, UNIX	✕

Results 1 - 4 (all)

Read more about creating and managing users and groups in SGI NAS User Guide 3.x Section 17. Managing the users.

2.2.3 Creating a CIFS share with restricted access

Next, share an appliance's folder for access from Windows machines as it described in 2.1.3.Create a CIFS share. The only difference is that anonymous access must be set as **false**. In NMV **Data Management** → **Shares**, press **Edit** near the CIFS share mark and uncheck the '**Anonymous Read-Write**' checkbox:



Show
Summary Information

Create
Create New Folder

Configure
Basic CIFS configuration

Identity Mapping
Configure Windows to UNIX identity mapping

Join AD/DNS Server
Become a member of Windows AD/DNS Server

Join Workgroup
Become a member of Windows Workgroup

EDIT CIFS SHARE FOR FOLDER: TANK0/A

Share Name: tank0_a
Share name must begin with a letter, and can only contain alphanumeric characters as well as underscore ('_'), dash ('-'), and period ('.'). The name must be unique.

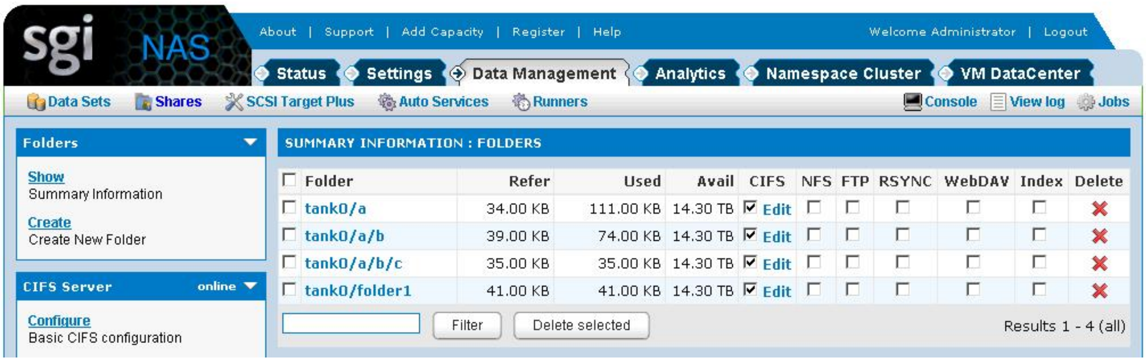
Anonymous Read-Write ☐
Allow anonymous access to this share. Shared top-level directory will be granted read-write access for anonymous user 'smb'. If recursive share mode is set to true, this property is propagated to existing sub-folders. Note that anonymous read/write access is not inheritable - anonymous access to future sub-folders will not be allowed until explicitly requested. The anonymous user name is 'smb', and the default password for anonymous user 'smb' is: 'nexenta'.

Recursive ☐
Recursive share mode; share nested folders. Specify recursive = true to make sure that ALL existing sub-folders of the given folder are shared with the same (sharing) properties. Note: sub-folders always inherit properties of their parent folder unless these properties were explicitly modified. In particular, non-shared sub-folders inherit sharing properties of their parent folder. However, if at the time of this operation sub-folder(s) are already shared, their sharing properties will NOT be overridden unless recursive = true is specified.

In NMC this parameter is specified during the share creation time:

```
nmc:/$ share folder tank0/a
show   cifs   ftp   nfs   rsync  webdav <?>
nmc@zhost:/$ share folder tank0/a cifs
Share Name             : tank0_a
Anonymous Read-Write : false
Recursive              : true
Added CIFS share for folder 'tank0/a'
```

The folder 'tank0/a' is now CIFS-shared, and can be seen as shared in NMC and NMV:



SUMMARY INFORMATION : FOLDERS

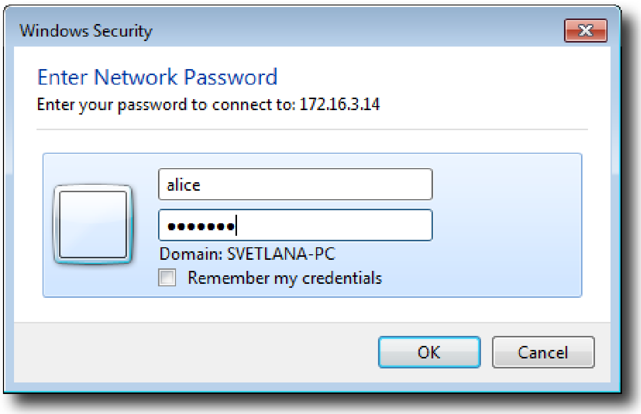
□ Folder	Refer	Used	Avail	CIFS	NFS	FTP	RSYNC	WebDAV	Index	Delete
□ tank0/a	34.00 KB	111.00 KB	14.30 TB	☑ Edit	□	□	□	□	□	✗
□ tank0/a/b	39.00 KB	74.00 KB	14.30 TB	☑ Edit	□	□	□	□	□	✗
□ tank0/a/b/c	35.00 KB	35.00 KB	14.30 TB	☑ Edit	□	□	□	□	□	✗
□ tank0/folder1	41.00 KB	41.00 KB	14.30 TB	☑ Edit	□	□	□	□	□	✗

Results 1 - 4 (all)

2.2.4 Access the share as authenticated user

1. Map network drive as it described in 2.1.4.Map CIFS share on Windows machine

2. Log in from Windows as user 'alice':



Enter Network Password

Enter your password to connect to: 172.16.3.14

alice

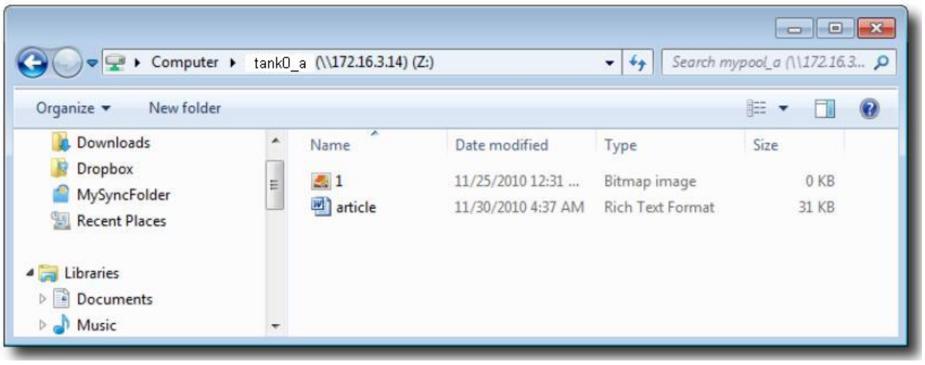
•••••••

Domain: SVETLANA-PC

□ Remember my credentials

Use correct user password to login. In our current example, the password for user '**alice**' was specified at user creation time (see step **1** above).

Once logged in as 'alice', the appliance's folder and its content shows up:

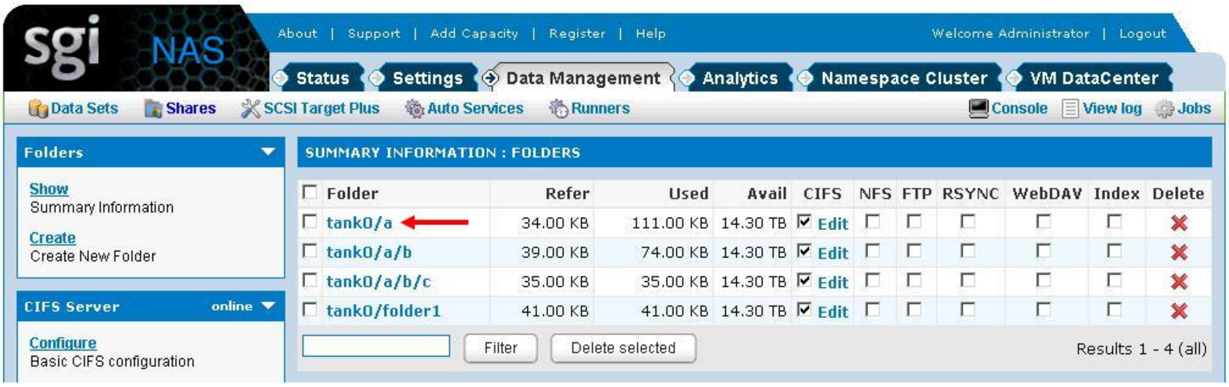


Name	Date modified	Type	Size
1	11/25/2010 12:31 ...	Bitmap image	0 KB
article	11/30/2010 4:37 AM	Rich Text Format	31 KB

Note, that at this point user 'alice' can read files, but not write, delete, etc.

Read access to CIFS-shared folders is granted by default. Write access need to be explicitly granted – via the corresponding operation on the shared folder's **ACL**.

To view current ACL in NMV click on share **tank0/a:**

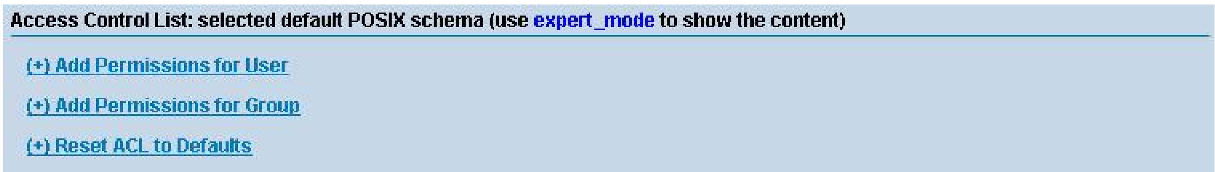


SUMMARY INFORMATION : FOLDERS

☐ Folder	Refer	Used	Avail	CIFS	NFS	FTP	RSYNC	WebDAV	Index	Delete
☐ tank0/a	34.00 KB	111.00 KB	14.30 TB	☑ Edit	☐	☐	☐	☐	☐	✗
☐ tank0/a/b	39.00 KB	74.00 KB	14.30 TB	☑ Edit	☐	☐	☐	☐	☐	✗
☐ tank0/a/b/c	35.00 KB	35.00 KB	14.30 TB	☑ Edit	☐	☐	☐	☐	☐	✗
☐ tank0/folder1	41.00 KB	41.00 KB	14.30 TB	☑ Edit	☐	☐	☐	☐	☐	✗

Results 1 - 4 (all)

On the next screen ACL and other folders properties are located:



Access Control List: selected default POSIX schema (use expert_mode to show the content)

(+) Add Permissions for User

(+) Add Permissions for Group

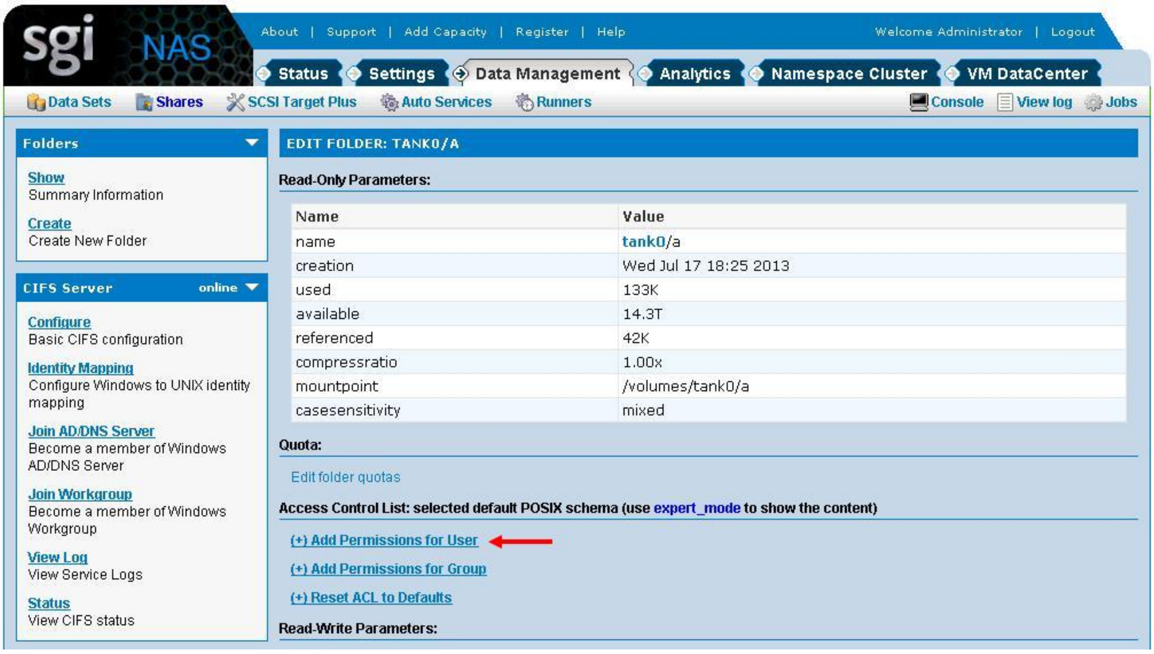
(+) Reset ACL to Defaults

Note, that on the screen above ACL list is empty. It means that ACL for this folder is configured by default. You can view expanded output in NMC:

```
nmc:/$ show folder tank0/a acl
=============== tank0/a  (user owner: root, group owner: root)
===============
ENTITY              ALLOW                                  DENY
owner@       add_file, add_subdirectory,

        append_data, execute,
             list_directory, read_data,
             write_acl, write_attributes,
             write_data, write_owner,
             write_xattr

group@       execute, list_directory,            add_file, add_subdirectory,
             read_data                           append_data, write_data

everyone@    execute, list_directory,            add_file, add_subdirectory,
             read_acl, read_attributes,          append_data, write_acl,
             read_data, read_xattr,              write_attributes,
write_data,
             synchronize                         write_owner, write_xattr
```

2.2.5 Granting permissions to user

Next, we grant write access to user 'alice' from NMV by clicking on share **tank0/a** link and choosing **(+) Add Permissions for User**:



EDIT FOLDER: TANK0/A

Read-Only Parameters:

Name	Value
name	tank0/a
creation	Wed Jul 17 18:25 2013
used	133K
available	14.3T
referenced	42K
compressratio	1.00x
mountpoint	/volumes/tank0/a
casesensitivity	mixed

Quota:

Edit folder quotas

Access Control List: selected default POSIX schema (use expert_mode to show the content)

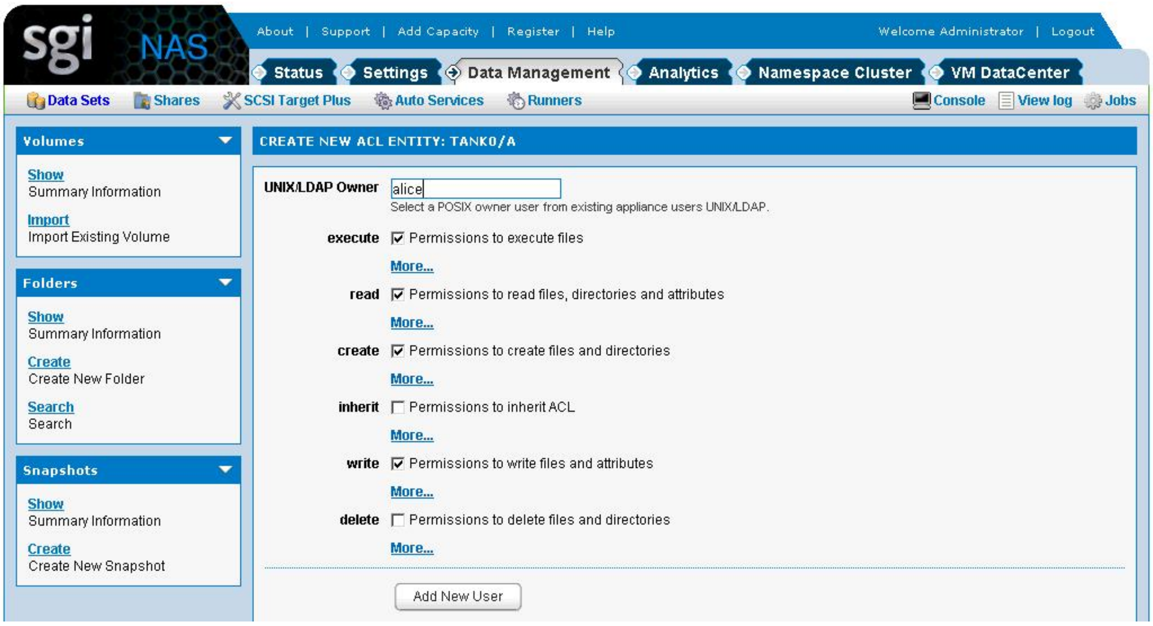
(+) Add Permissions for User

(+) Add Permissions for Group

(+) Reset ACL to Defaults

Read-Write Parameters:

Specify the user's name and access rights on the next screen:



CREATE NEW ACL ENTITY: TANK0/A

UNIX/LDAP Owner: alice

Select a POSIX owner user from existing appliance users UNIX/LDAP.

execute ☑ Permissions to execute files
More...

read ☑ Permissions to read files, directories and attributes
More...

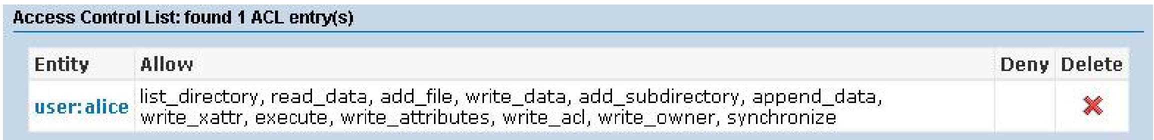
create ☑ Permissions to create files and directories
More...

inherit □ Permissions to inherit ACL
More...

write ☑ Permissions to write files and attributes
More...

delete □ Permissions to delete files and directories
More...

The newly created entity appears in share's properties:



Access Control List: found 1 ACL entry(s)

Entity	Allow	Deny	Delete
user:alice	list_directory, read_data, add_file, write_data, add_subdirectory, append_data, write_xattr, execute, write_attributes, write_acl, write_owner, synchronize		✗

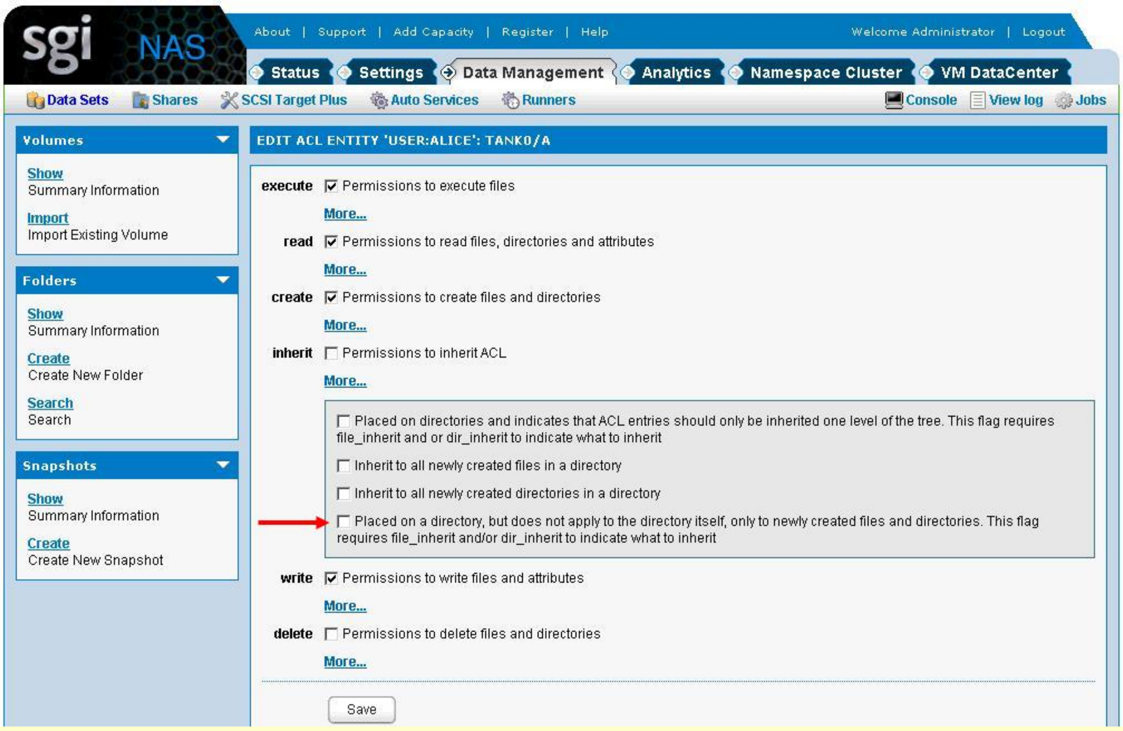
Corresponding NMC command:

```
nmc:/$ setup folder tank0/a acl
Entity type                         : user
User                                : alice
Permissions                         :  (Use SPACEBAR for multiple selection)
 DELETE *add_subdirectory *add_file *execute *read_xattr *read_attributes
*list_directory *read_data *read_acl *delete  delete_child  inherit_only
 no_propagate  file_inherit  dir_inherit *write_data *write_xattr
 write_owner  write_attributes  write_acl
  ------------------------------------------------------------------------
-----
  Select one or multiple permissions for 'user:alice' to access 'vol1/a'.
Hit
  DELETE to delete all permissions granted to 'user:alice'. Navigate with
arrow
  keys (or hjkl), or Ctrl-C to exit.
```

In the example above **'*'** marks extended attributes indicate permissions that were selected to be grante to 'alice'. In this particular example we are granting 'alice' almost all permissions...

Note the '**inherit_only**' flag. It is placed on a directory, but applicable to newly created files and sub-directories. It means that it is not applied to the directory itself. This flag requires file_inherit and/or dir_inherit to indicate what to inherit.

This may become a source of confusion for SGI NAS users. For new UNIX users it is recommended to make sure that '**inherit only**' is unchecked. In NMV, go to **Data Management** → **Shares** click on the corresponding folder and choose either **(+) Add Permissions for User/Group** or click on the existing ACE to make changes:



EDIT ACL ENTITY 'USER:ALICE': TANK0/A

execute ☑ Permissions to execute files

read ☑ Permissions to read files, directories and attributes

create ☑ Permissions to create files and directories

inherit □ Permissions to inherit ACL

□ Placed on directories and indicates that ACL entries should only be inherited one level of the tree. This flag requires file_inherit and or dir_inherit to indicate what to inherit

□ Inherit to all newly created files in a directory

□ Inherit to all newly created directories in a directory

□ Placed on a directory, but does not apply to the directory itself, only to newly created files and directories. This flag requires file_inherit and/or dir_inherit to indicate what to inherit

write ☑ Permissions to write files and attributes

delete □ Permissions to delete files and directories

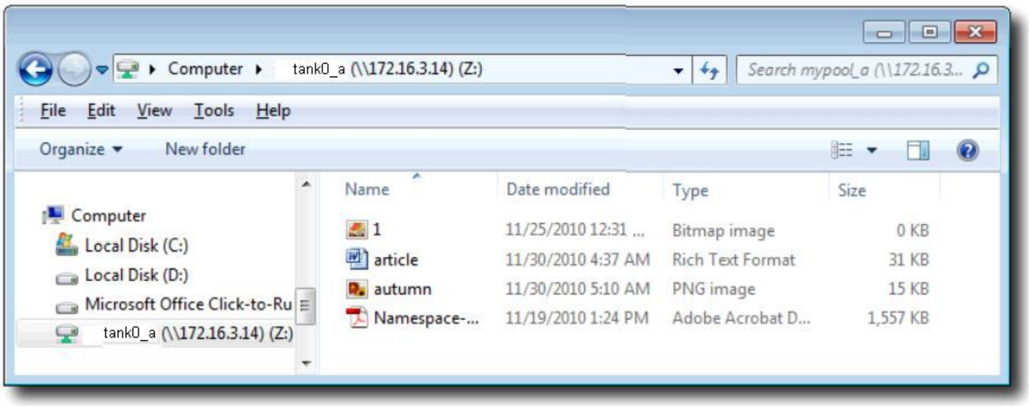
To see the folder's ACL in NMC, run:

```
nmc:/$ show folder <foldername> acl
```

To manage folder ACL, run

```
nmc:/$ setup folder <foldername>acl
```

At this point user alice can write. For instance, drag and drop a *.png or *.pdf into the shared folder:


Computer ▸ tank0_a (\\172.16.3.14) (Z:)
Search mypool_a (\\172.16.3...
File
Edit
View
Tools
Help
Organize ▾
New folder
Computer
Local Disk (C:)
Local Disk (D:)
Microsoft Office Click-to-Ru
tank0_a (\\172.16.3.14) (Z:)

Name	Date modified	Type	Size
1	11/25/2010 12:31 ...	Bitmap image	0 KB
article	11/30/2010 4:37 AM	Rich Text Format	31 KB
autumn	11/30/2010 5:10 AM	PNG image	15 KB
Namespace-...	11/19/2010 1:24 PM	Adobe Acrobat D...	1,557 KB

Do **not** use name based mapping in workgroup mode. If you do, the mapping daemon (called **idmap**) will try to search Active Directory (next Section) to resolve the names, and will most probably fail. See “Using Active Directory” for details.

The next section details SGI NAS usage in domain mode, via Active Directory.

2.3 Domain mode

Domain mode is associated with integrating SGI NAS to Active Directory or joining AD.

2.3.1 Pre-requisites

The list of items needed for the installation is:

- Either Windows 2003 Server with Active Directory configured or Windows 2008 Server SP2 or higher version with Active Directory configured.
- DNS Server installed and working as part of the Active Directory Environment

The main thing that is required to start to work in the domain mode is configured domain controller and DNS server. There are many instructions and guides in the Internet on how to perform the setup, for instance you may use these links:

Step-by-step guide for Windows Server 2008 Domain Controller and DNS server setup

Step-by-step guide for Windows Server 2003 Domain Controller and DNS server setup

Please note this occasional mistake: for the join to succeed, the appliance must be setup so that the Active Directory Domain is the same as the DNS Domain of the appliance.

In general, Active Directory functionality depends on the **proper configuration of the DNS infrastructure**. Microsoft Knowledge Base article "Troubleshooting Active Directory—Related DNS Problems" describes the corresponding requirements. Those include DNS server and zone configuration and proper delegations in parent DNS zones, and presence of DNS domain controller locator records (SRV records). These and other guidelines are further described in the User Guide.

When Domain Controller is properly set up, joining SGI NAS to Active Directory can be started.

2.3.2 Joining Active Directory

2.3.2.1 Configuring Windows

There are two different scenarios of adding SGI NAS appliance to Windows Active Directory (or, joining Active Directory):

1. SGI NAS computer object is already registered with the Active Directory

2. SGI NAS computer object is not present in the Active Directory

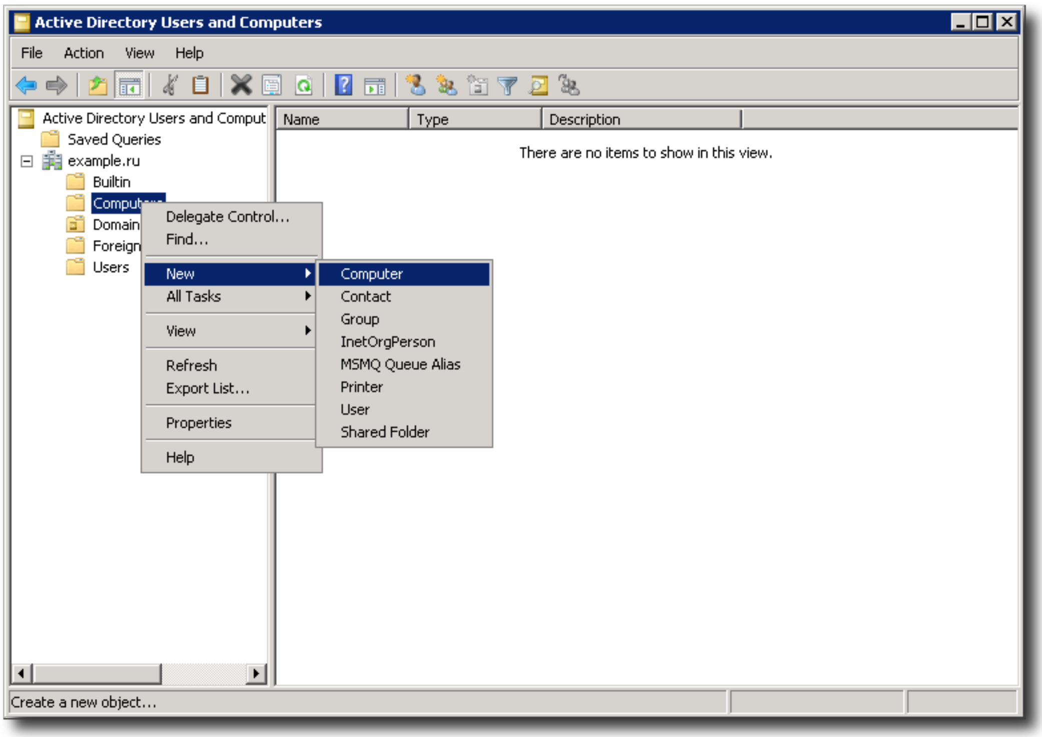
It is important to distinguish between these two cases. In general, creation of the **new** record in the Active Directory database requires **administrative** privileges.

If the computer object that represents SGI NAS appliance is already present in the Active Directory, you can use any valid user account to join the appliance to Active Directory – assuming this particular account has **Full Control** over this particular computer (appliance).

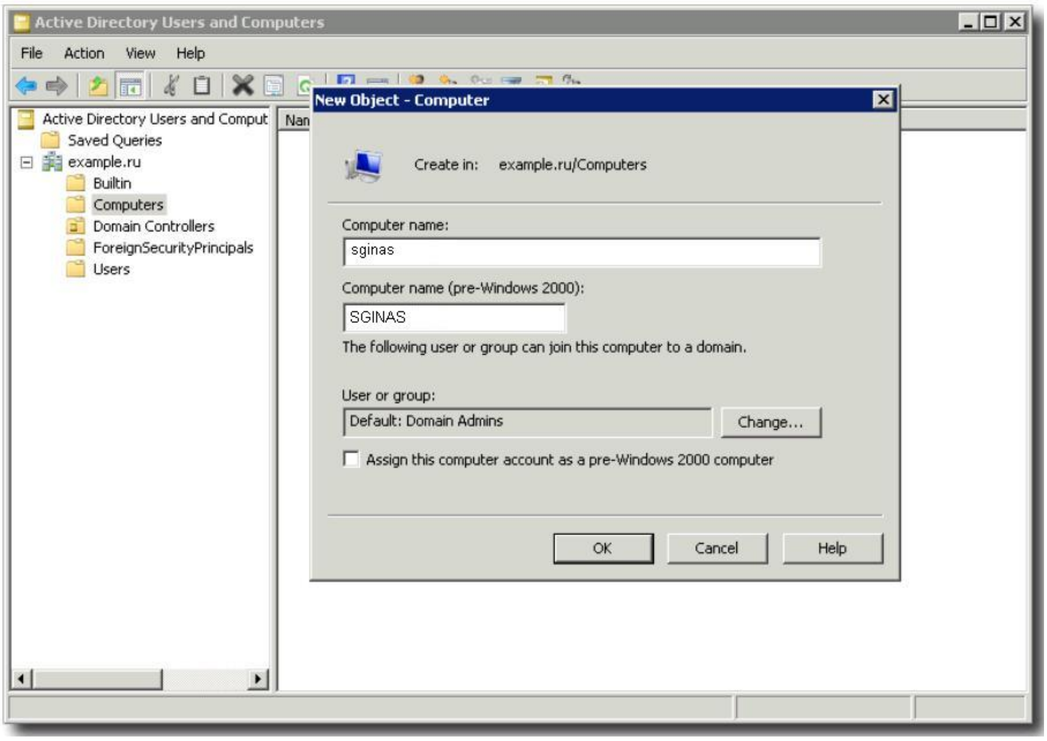
Importantly – in the case of the pre-existing computer object in the AD, account used to join the appliance to the Active Directory does not necessarily need to have administrative privileges.

The following assumes that the SGI NAS appliance is **not** present yet in the Active Directory database. The very first step in this case is for the **Windows Administrator** to create a corresponding computer object. In more detail:

Step 1. Start Microsoft Management Console, right click on Computers, and select New:



Step 2. Specify SGI NAS appliance – by hostname:



Active Directory Users and Computers
File Action View Help
Active Directory Users and Comput
Saved Queries
example.ru
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Nan

New Object - Computer

Create in: example.ru/Computers

Computer name:
sginas

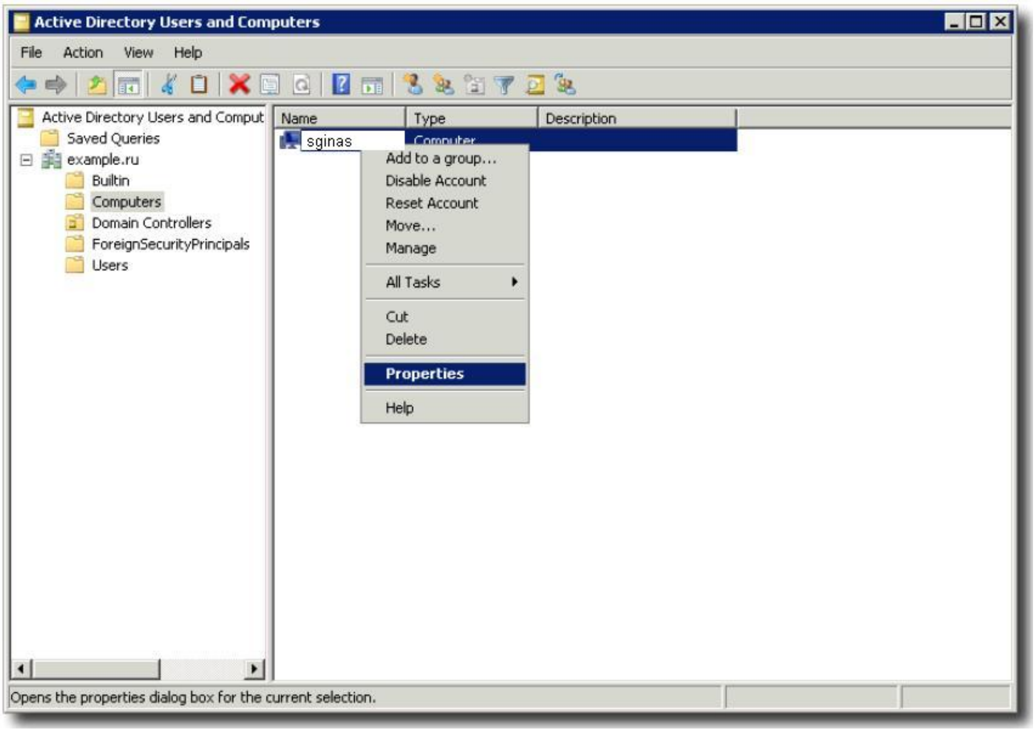
Computer name (pre-Windows 2000):
SGINAS

The following user or group can join this computer to a domain.

User or group:
Default: Domain Admins

□ Assign this computer account as a pre-Windows 2000 computer

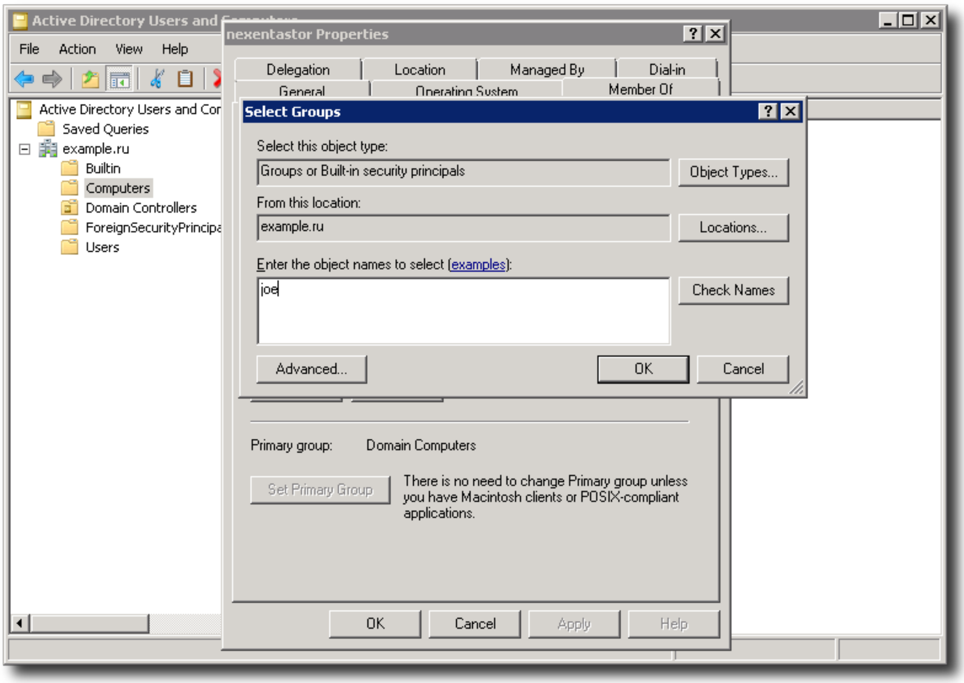
Step 3. Once the computer is added, right click on it and select **Properties**:



Name	Type	Description
sginas	Computer	

Opens the properties dialog box for the current selection.

Step 4. Optionally, add users/groups that will use this computer and will perform join operation. Click on **Security tab**, type in user (or group) name, and click on **Check Names** button.



Select Groups

Select this object type:
Groups or Built-in security principals

From this location:
example.ru

Enter the object names to select (examples):
joe

Primary group: Domain Computers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

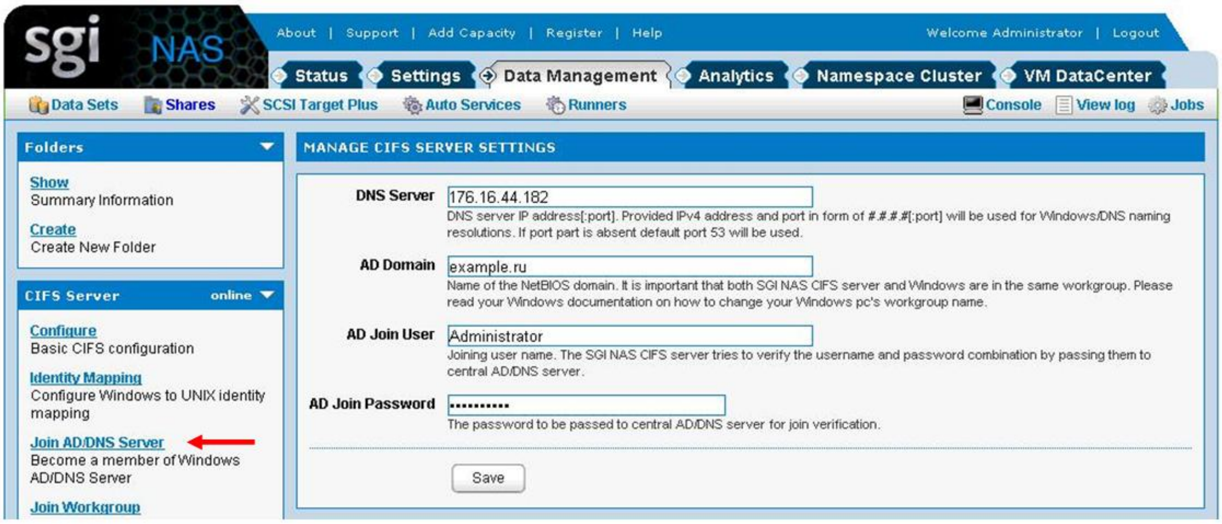
Make sure to provide the newly added computer users with **Full Control** over this computer.

> Using Microsoft Management Console and performing Steps 1 through 4 (above) can be skipped in either one of the following two cases:
>
> (1) Account with administrative privileges is used to perform join operation.
>
> (2) A record of computer object representing appliance already exists.

The rest of this section assumes that either (1) or (2) above (or both the (1) and the (2)) are true.

2.3.2.2 Configuring SGI NAS

To join Active Directory, and subsequently get access to the centralized authentication and authorization information, in NMV go to **Data Management** → **Shares** and click on **Join AD/DNS Server** link:



Summary Information

Create New Folder

Basic CIFS configuration

Configure Windows to UNIX identity mapping

Become a member of Windows AD/DNS Server

MANAGE CIFS SERVER SETTINGS

DNS Server: 176.16.44.182

DNS server IP address[:port]. Provided IPv4 address and port in form of #.#.#.#[:port] will be used for Windows/DNS naming resolutions. If port part is absent default port 53 will be used.

AD Domain: example.ru

Name of the NetBIOS domain. It is important that both SGI NAS CIFS server and Windows are in the same workgroup. Please read your Windows documentation on how to change your Windows pc's workgroup name.

AD Join User: Administrator

Joining user name. The SGI NAS CIFS server tries to verify the username and password combination by passing them to central AD/DNS server.

AD Join Password: ••••••••••

The password to be passed to central AD/DNS server for join verification.

NMC provides the similar functionality, via 'setup network service cifs-server join-ads':

```
nmc:/$ setup network service cifs-server join_ads
DNS Server IP address, port : 172.16.44.182
AD Server IP address, port  : 172.16.44.182
AD Domain Name              : example.ru
AD Join User                : Administrator
AD Join Password            : xxxxxxxxx
```

Successful join is persistent across reboots.
If you encounter any trouble with joining SGI NAS to Active Directory see 3.Troubleshooting section.

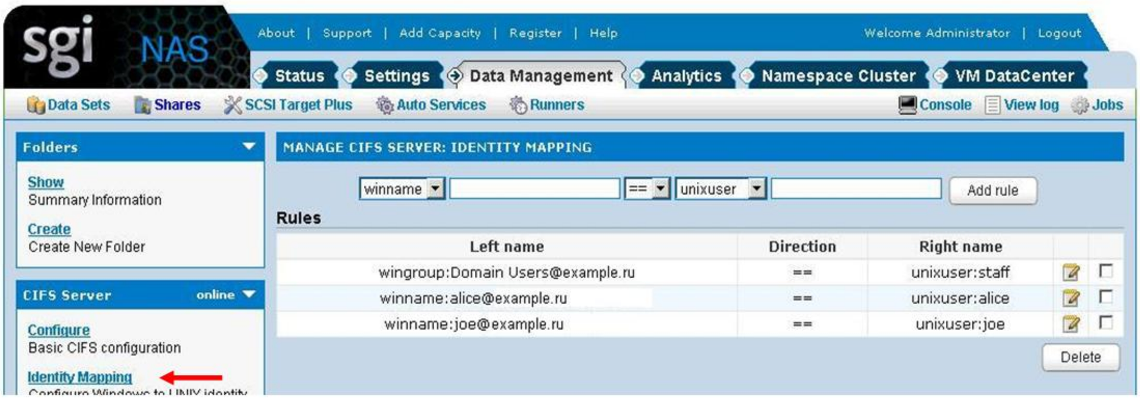
2.3.2.3 Creating CIFS share

Follow the instructions in section 2.1.2.Create a CIFS share

2.4 ID mapping

User name equivalence between Windows users and groups and their counterparts in UNIX is established via appliance's '**idmap**' facility. It is need to establish the connection between Windows and SGI NAS Users and give the the permission to system administrators to distinguish the access to the SGI NAS shares. The '**idmap**' mappings persist across reboots. To use CIFS shares for authenticated access, please make sure to establish the mapping.

To map Windows users/groups onto UNIX users/groups, in NMV go to **Data Management** → **Shares** and click on the **Identity Mapping** link:



MANAGE CIFS SERVER: IDENTITY MAPPING

winname ▾ [ ] == ▾ unixuser ▾ [ ] Add rule

Rules

Left name	Direction	Right name		
wingroup:Domain Users@example.ru	==	unixuser:staff		□
winname:alice@example.ru	==	unixuser:alice		□
winname:joe@example.ru	==	unixuser:joe		□

Delete

The example above shows several identity mappings. Group of Windows users called “Domain Users” is mapped onto Unix group 'staff'. Windows user 'joe' is mapped onto Unix user 'joe', and Windows user 'Alice' – onto user 'alice'. All mappings are bi-directional in this case – notice the '==' sign in the table above.

NMC provides the similar functionality with the following command:

```
nmc:/$ setup network service cifs-server idmap
```

Windows user name must be specified by using one of the following formats:

1) **winuser:username@domain-name**
2) **winuser:'domain-name\username'**

Unix user name must be specified in the following format:

unixuser:username

Note, that Windows user names are case **insensitive**, while Solaris user names are case **sensitive**.

Examples:

a) map all users in the domain mydomain.com:

winuser:'*@mydomain.com'==unixuser:'*'

b) map Unix user 'joe' to Windows user Joe in the domain mydomain.com:

winuser:'Joe@mydomain.com'==unixuser:joe

2. There are so called 'well-known' Windows user and group names, that are supported by 'idmap':

- **Administrator**
- **Guest**
- **KRBTGT**
- **Domain Admins**
- **Domain Users**
- **Domain Guest**
- **Domain Computers**
- **Domain Controllers**

When idmap rules are added, these well-known names will be expanded to canonical form. That is, either the default domain name will be added (for names that are not well-known) or an appropriate built-in domain name will be added. Depending on the particular well-known name, this domain name might be null, BUILTIN, or the local host name.

For example:

If you map wingroup 'Administrators' to unixgroup 'sysadmin':

```
nmc:/$ setup network service cifs-server idmap
Mappings Rules : wingroup:Administrators==unixgroup:sysadmin
```

it will be automatically mapped with @BUILTIN virtual domain:

```
nmc:/$ show network service cifs-server idmap
add     wingroup:Administrators@BUILTIN unixgroup:sysadmin
```

it will be automatically mapped with @BUILTIN virtual domain:

```
nmc:/$ show network service cifs-server idmap
add     wingroup:Administrators@BUILTIN unixgroup:sysadmin
```

2.5 ACLs

SGI NAS provides native extended Access Control Lists (ACLs), capable of handling CIFS ACLs, as well as NFSv4 ACLs, as well as POSIX permissions natively in the same filesystem.

The appliance supports full management of per-user, per-group, per-folder ACLs in its user interface, while also populating the system with accounts and groups that you may have already defined in LDAP-based directory service. There is no support for Active Directory yet. For Active Directory use ID mapping.
SGI NAS User and Access Control management has the following characteristics:

- Support both local and LDAP managed users and groups. In LDAP configurations, the local users and groups can be used to override centralized settings. After configuring LDAP client LDAP users are automatically discovered and added by the appliance.
- Native extended Access Control Lists (ACLs), that are both CIFS and NFSv4 compliant.

The users and groups can be retrieved, created and deleted, extended permissions can be modified, and all the rest related management operations can be executed using either NMV or/and NMC.

Note, that using the group ACLs is much more efficient than using per-user ACLs. For example, if a new user is added to Administrators group he is automatically granted with all the group permissions.

SGI NAS ACLs are native across ZFS, CIFS, and NFSv4, and as such have no conflict in how they are operated on. Generally, one accomplishes ACL management via the following tasks:

- local user or LDAP configuration
- definition of per-user or per-group capabilities per volume or folder
- overall management of ACLs and ACEs system wide, allowing overriding of end user activity via CIFS/NFS

> A note on NFSv3 vs. ACL
>
> NFSv3 relies on POSIX permissions, which are a subset of ZFS extended ACLs. Thus, NFSv3 clients will only check with the POSIX level permissions.
>
> However, even though POSIX permissions may otherwise grant a permission to a user, that will be nullified if the extended ACL on the server is defined and otherwise denies that access.

2.6 Known limitations:

Currently, CIFS service has the following limitations:

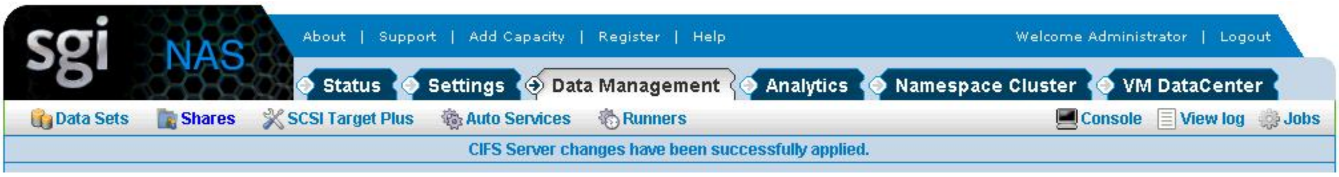
- Doesn't support sharing of 'child' ZFS filesystems

- Doesn't support OpenSolaris 'Zones'

3 Troubleshooting

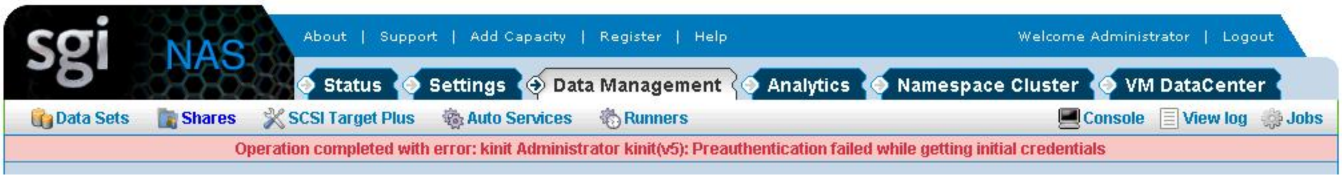
3.1 Initial troubleshooting steps

Successful join, or a failure to join Active Directory – both manifest themselves with the corresponding NMC or NMV printed messages. View the GUI examples:
The join is successful:



CIFS Server changes have been successfully applied.

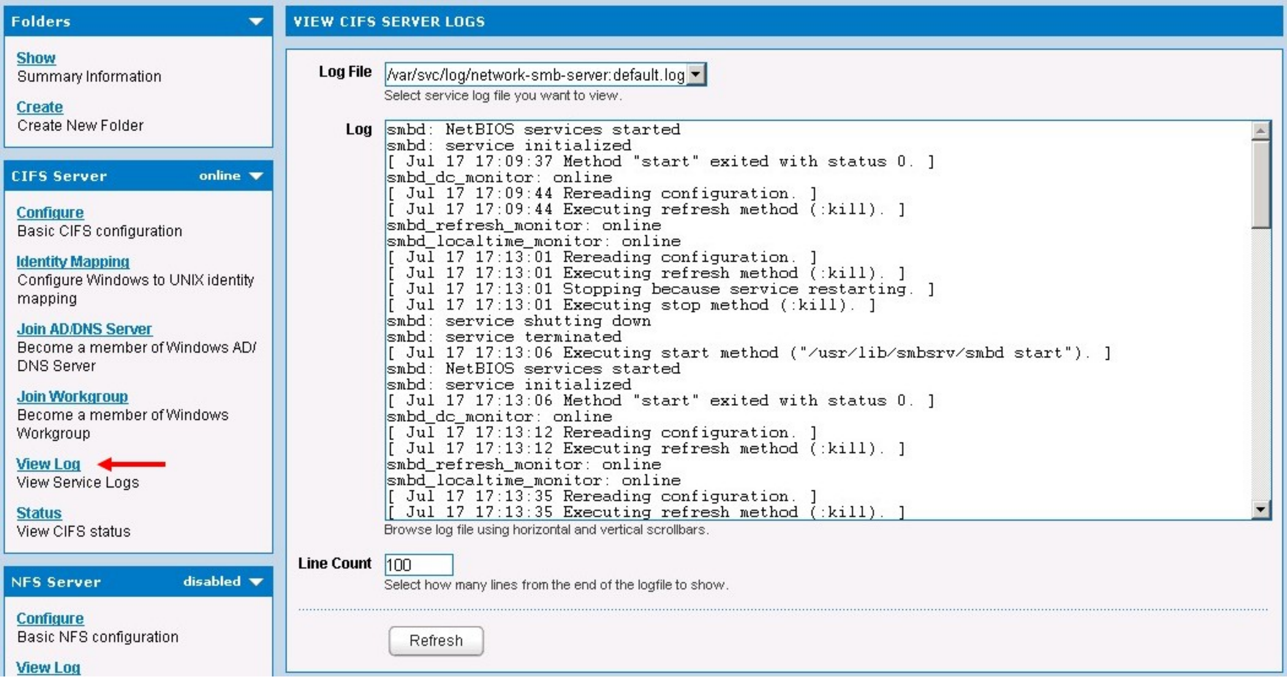
The join is unsuccessful:



Operation completed with error: kinit Administrator kinit(v5): Preauthentication failed while getting initial credentials

According to the error message, you can start troubleshooting the problem.

For troubleshooting, the first place to look would be the log files. In the NMV go to **Data Management** → **Shares** and click on **View Log** link:



Log File /var/svc/log/network-smb-server:default.log
Select service log file you want to view.

Log

```
smbd: NetBIOS services started
smbd: service initialized
[ Jul 17 17:09:37 Method "start" exited with status 0. ]
smbd_dc_monitor: online
[ Jul 17 17:09:44 Rereading configuration. ]
[ Jul 17 17:09:44 Executing refresh method (:kill). ]
smbd_refresh_monitor: online
smbd_localtime_monitor: online
[ Jul 17 17:13:01 Rereading configuration. ]
[ Jul 17 17:13:01 Executing refresh method (:kill). ]
[ Jul 17 17:13:01 Stopping because service restarting. ]
[ Jul 17 17:13:01 Executing stop method (:kill). ]
smbd: service shutting down
smbd: service terminated
[ Jul 17 17:13:06 Executing start method ("/usr/lib/smbsrv/smbd start"). ]
smbd: NetBIOS services started
smbd: service initialized
[ Jul 17 17:13:06 Method "start" exited with status 0. ]
smbd_dc_monitor: online
[ Jul 17 17:13:12 Rereading configuration. ]
[ Jul 17 17:13:12 Executing refresh method (:kill). ]
smbd_refresh_monitor: online
smbd_localtime_monitor: online
[ Jul 17 17:13:35 Rereading configuration. ]
[ Jul 17 17:13:35 Executing refresh method (:kill). ]
```

Browse log file using horizontal and vertical scrollbars.

Line Count 100
Select how many lines from the end of the logfile to show.

In NMC, the corresponding command is:

```
nmc:/$ show network service cifs-server log
```

This command has two 'completions': '**network-smb-server:default.log**' and '**messages**'. Select 'messages'; the following shows an example of 'messages' log:

```
Dec  3 03:11:34 sginas idmap[355]: [ID 523480
daemon.notice] AD lookup of w     inname
Administrator@Svetlana-PC failed, error code -9961

Dec  3 03:12:29 sginas last message repeated 7 times

Dec  3 03:12:54 sginas smbd[374]: [ID 812811
daemon.notice] logon[SVETLANA-     PC\alice]: WRONG_PASSWORD

Dec  3 03:13:01 sginas last message repeated 10 times

Dec  3 03:13:15 sginas idmap[355]: [ID 523480
daemon.notice] AD lookup of w     inname
Administrator@Svetlana-PC failed, error code -9961

Dec  3 03:13:28 sginas last message repeated 14 times

Dec  3 03:13:58 sginas smbsrv: [ID 138215 kern.notice]
NOTICE: smbd[SGI         STOR\guest]: vol1_folder1 share not
found

Dec  3 03:13:58 sginas last message repeated 3 times
```

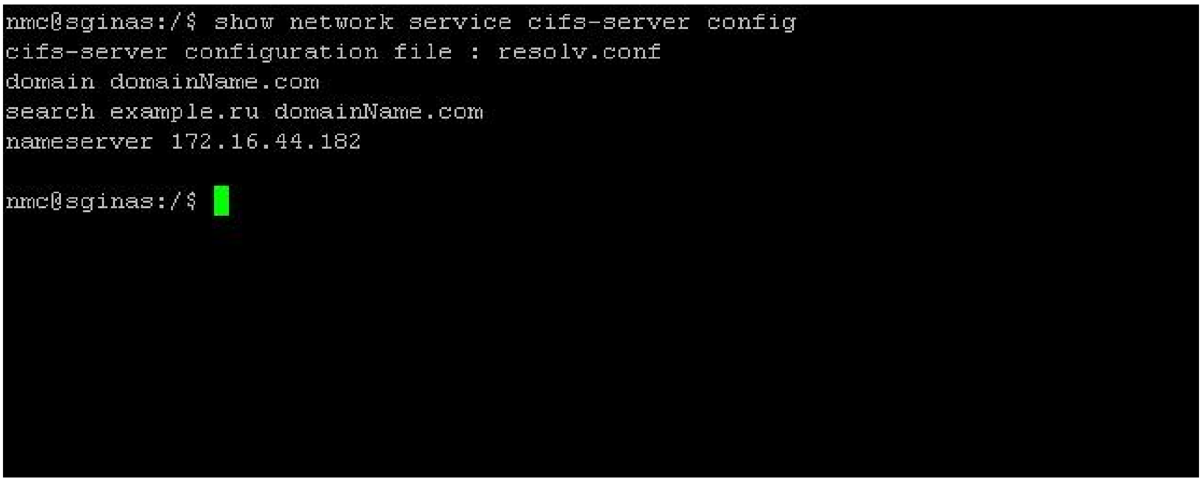
3.2 General troubleshooting

The following troubleshooting tips are common for all versions of Windows Servers:

1. Make sure time is in sync using same NTP Server for both Domain Controller and SGI NAS.
2. Verify DNS is properly configured.

Verify DNS is configured properly making sure both 'domain' and 'search' parameters are pointed to the Active Directory domain name. Parameter for 'nameserver' should have the IP address of a DNS server within the Active Directory environment. To check the configuration, run the following NMC command:

```
    nmc:/$ show network service cifs-server config
```



```
nmc@sginas:/$ show network service cifs-server config
cifs-server configuration file : resolv.conf
domain domainName.com
search example.ru domainName.com
nameserver 172.16.44.182

nmc@sginas:/$
```

Note, that in the example above 'domainName.com' – is the domain name of the appliance, 'example.ru' is the AD Domain, '172.16.44.182' is the IP address of the AD Domain.

If any corrections need to be applied, run the following nmc-command to edit the file in vim editor:

```
nmc:/$ setup network service cifs-server edit-settings
resolv.conf
```

Note:

If network interface is configured as DHCP, DHCP server's '**name-servers list**' should contain DNS server which is used for domain. Otherwise, the list will be updated after reboot and AD connection will be lost.

3. Validate Kerberos configuration:

```
# kinit <name of AD user>
```

A successful Kerberos test will not return any feedback, and the 'klist' command will show a ticket granting ticket (TGT) from the Active Directory DC/KDC.

Similar to 'nslookup' or 'dig', this command needs to be executed using the modified (but not committed) Kerberos configuration. Here, again - first, try to join AD. If (and only if) the join is unsuccessful, use /tmp/.nms-krb5.conf.saved instead of /etc/krb5/krb5.conf.[1] And then, try the 'kinit' and/or 'klist' command.

4. Verify SRV Record.

Use '**dig**' command to verify SRV Record.

[1] As of SGI NAS 3.1.4.1 (and later), the Kerberos configuration file krb5.conf is no longer used (applicable).

To enter bash shell, run:

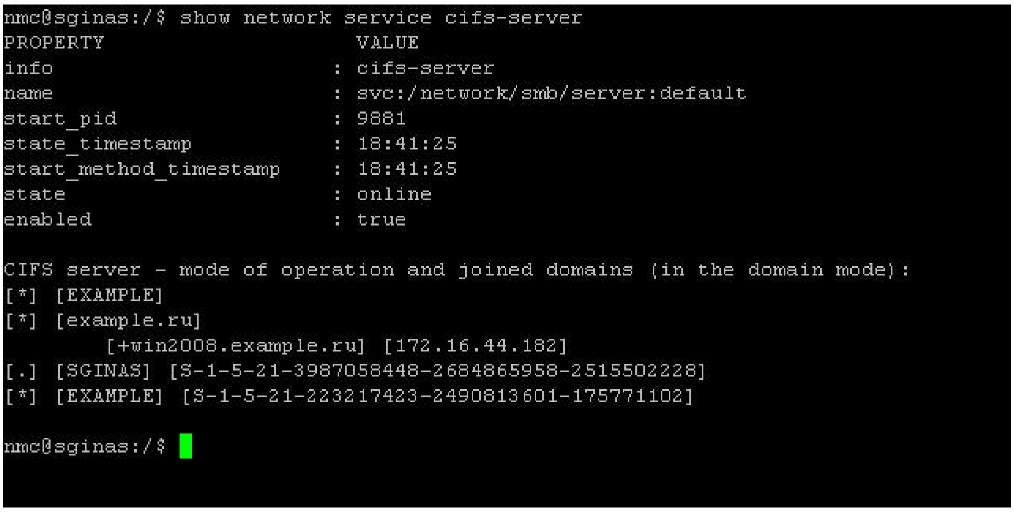
```
nmc:/$ dig '@172.16.44.182'_ldap._tcp.dc_msdcs.example.ru SRV
+short
```

Right configuration should return no answer.

5. Verify SGI NAS has joined the domain

Going back to the SSH session, run the following command to see smbadm list and verify that the SGI NAS has joined the domain with the command:

```
nmc:/$ show network service cifs-server
```



```
nmc@sginas:/$ show network service cifs-server
PROPERTY                     VALUE
info                       : cifs-server
name                       : svc:/network/smb/server:default
start_pid                  : 9881
state_timestamp            : 18:41:25
start_method_timestamp     : 18:41:25
state                      : online
enabled                    : true

CIFS server - mode of operation and joined domains (in the domain mode):
[*] [EXAMPLE]
[*] [example.ru]
        [+win2008.example.ru] [172.16.44.182]
[.] [SGINAS] [S-1-5-21-3987058448-2684865958-2515502228]
[*] [EXAMPLE] [S-1-5-21-223217423-2490813601-175771102]

nmc@sginas:/$
```

3.3 Windows Server 2008 troubleshooting tips

- Known Kerberos bug in Windows 2008 Server SP1 - please upgrade to SP2.
- For SGI NAS 3.1.x and later, the default 'lmauth_level' is '4'. This causes SGI NAS to send an NTLMv2 hash. For SGI NAS 3.0.x and earlier, the default 'lmauth_level' is '2'. This causes SGI NAS to send an NTML hash instead of an NTLMv2 hash. Newer versions of Windows are typically configured to refuse authentication that uses NTML hash. If you are having trouble authenticating, make sure the 'lmauth_level' is set to '4' using the command:

```
# sharectl set -p lmauth_level=4 smb
```

- Verify that 'lmauth_level=4' is set using the command:

```
# sharectl get smb
```

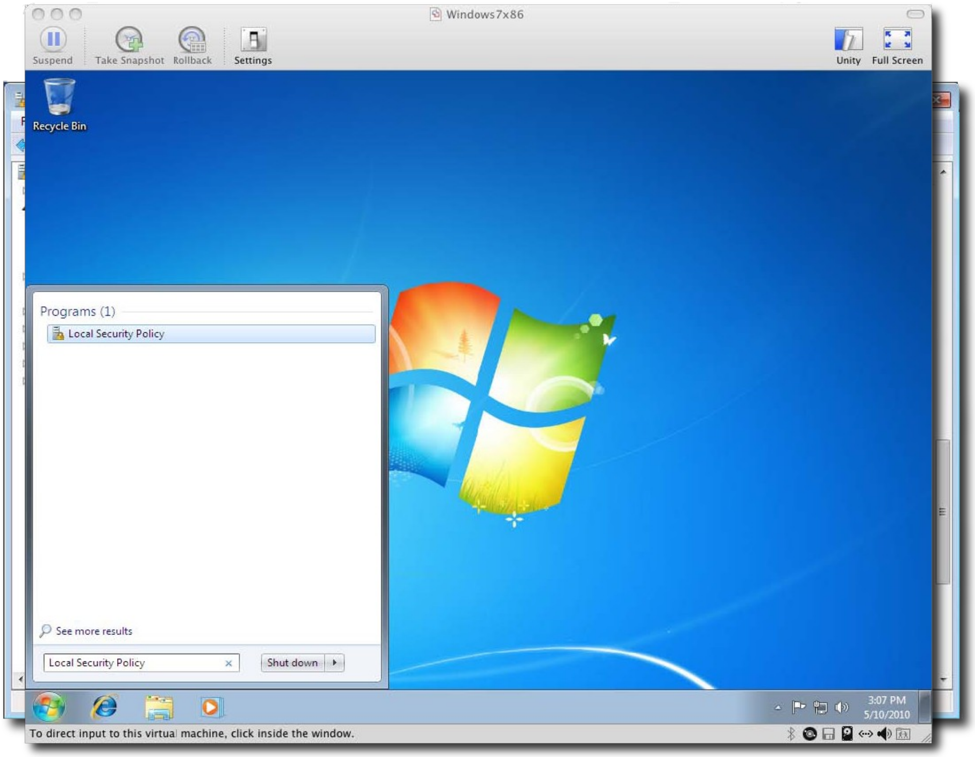
Note:

NTLMv2 authentication is mandatory only when LMCompatibilityLevel is set to 5 on your Windows 2008 domain controller. A value of 0-4 for LMCompatibilityLevel means that NTLMv2 authentication is not mandatory. By default, LMCompatibilityLevel is set to 3.

3.4 Windows 7 troubleshooting tips

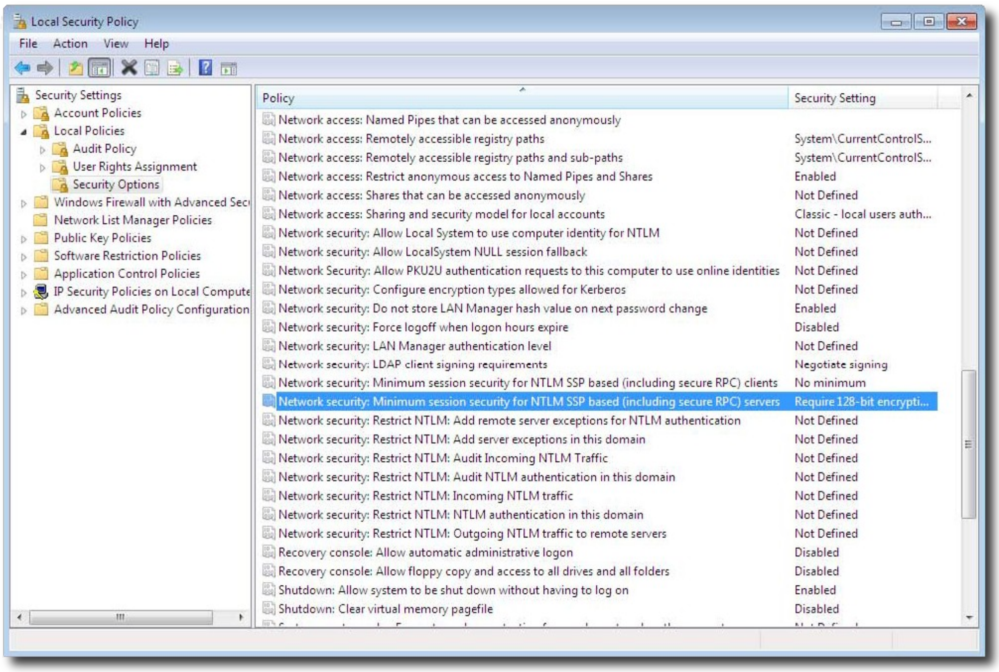
Authorized access to SGI NAS shares from Windows 7 in Workgroup mode should work automatically with default Windows settings. If you have problems with access, use the following recommendations before mounting CIFS share.

Step 1: Search for '**Local Security Policy**' and open.



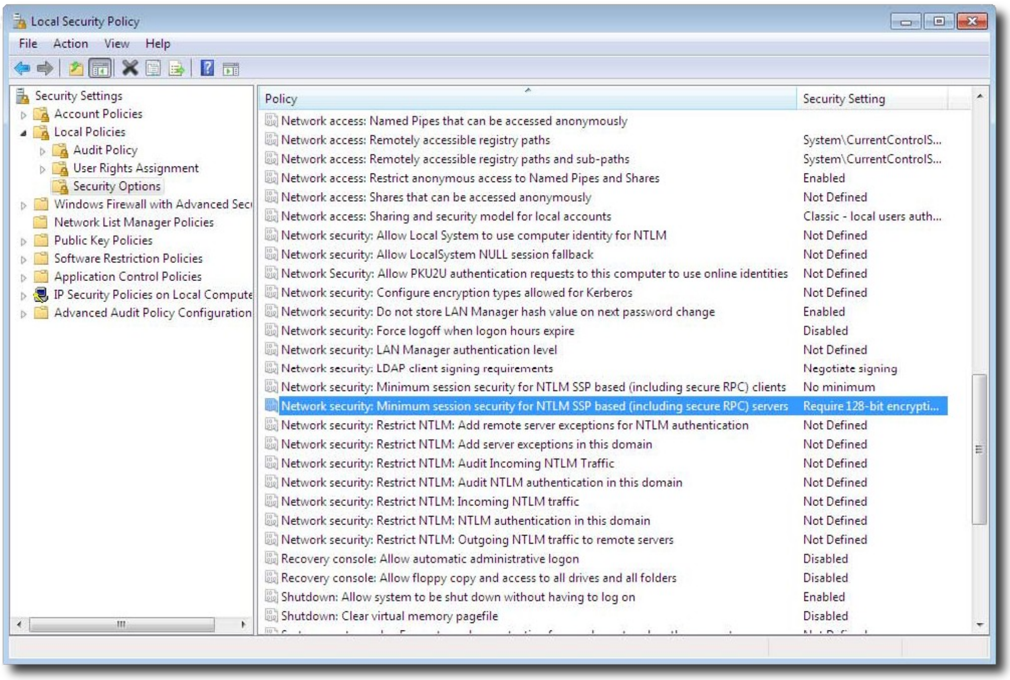
Step 2: Navigate down to **Security Settings** → **Local Policies** → **Security Options** → **Network security**: **Minimum session security for NTLM SSP based (including secure RPC) Clients.**

Step 3: Make sure **'Require NTLMv2 session security'** and **'Require 128-bit encryption'** are unchecked.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users auth...
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled

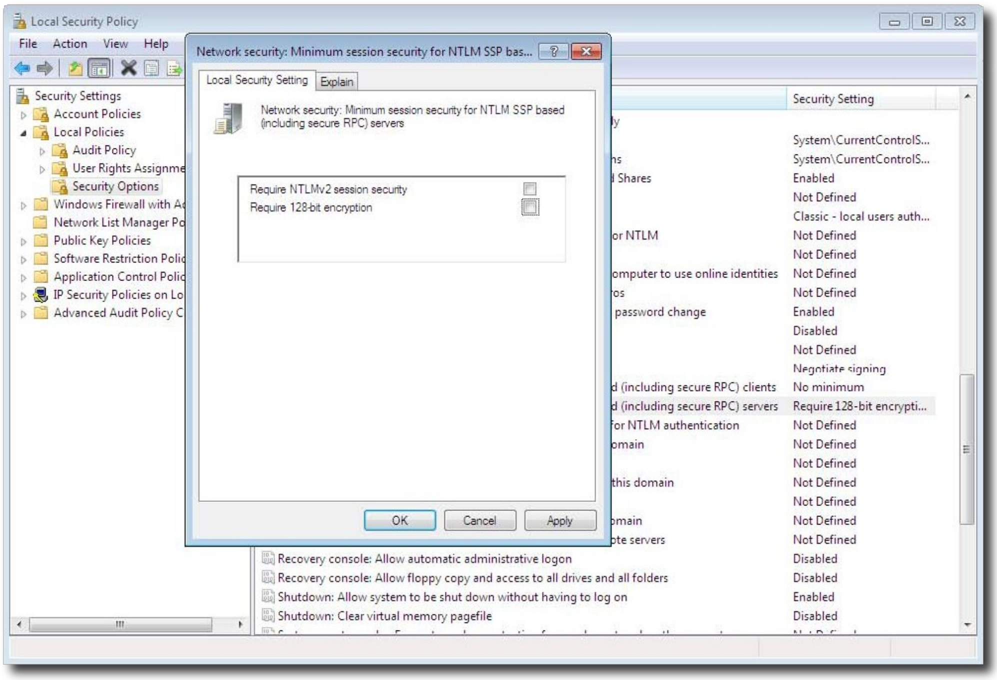
Step 4: Go back and select **Network security**: **Minimum session security for NTLM SSP based (including secure RPC) servers.**



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users auth...
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled

Step 5: Make sure **'Require NTLMv2 session security'** and **'Require 128---bit encryption'** are both unchecked.

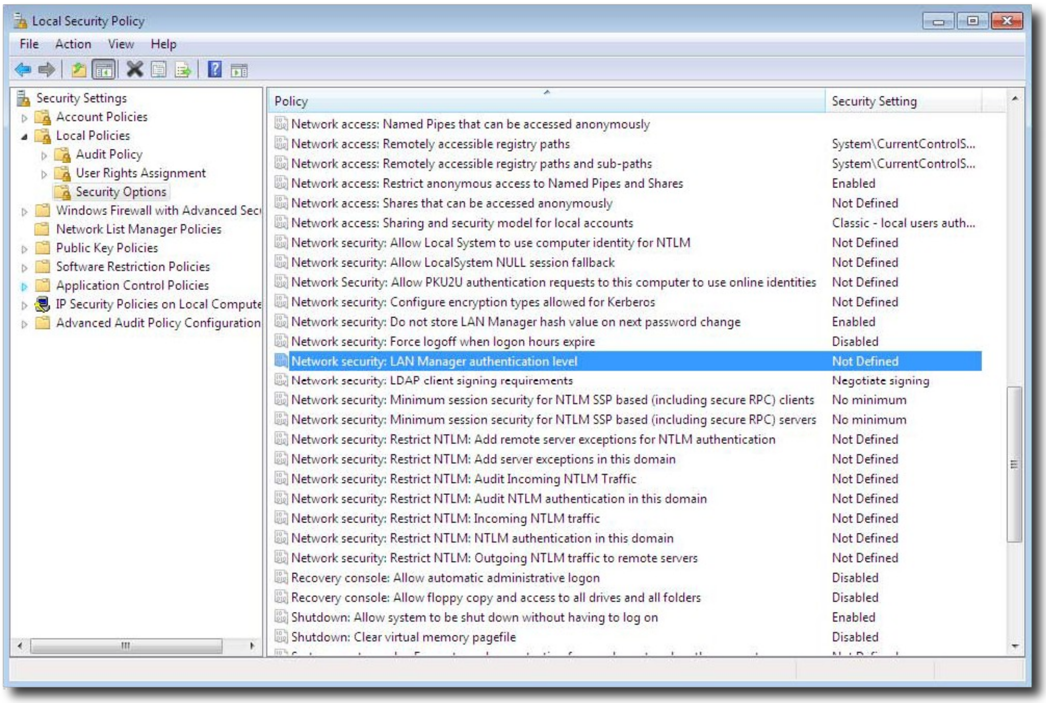


Network security: Minimum session security for NTLM SSP bas...

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

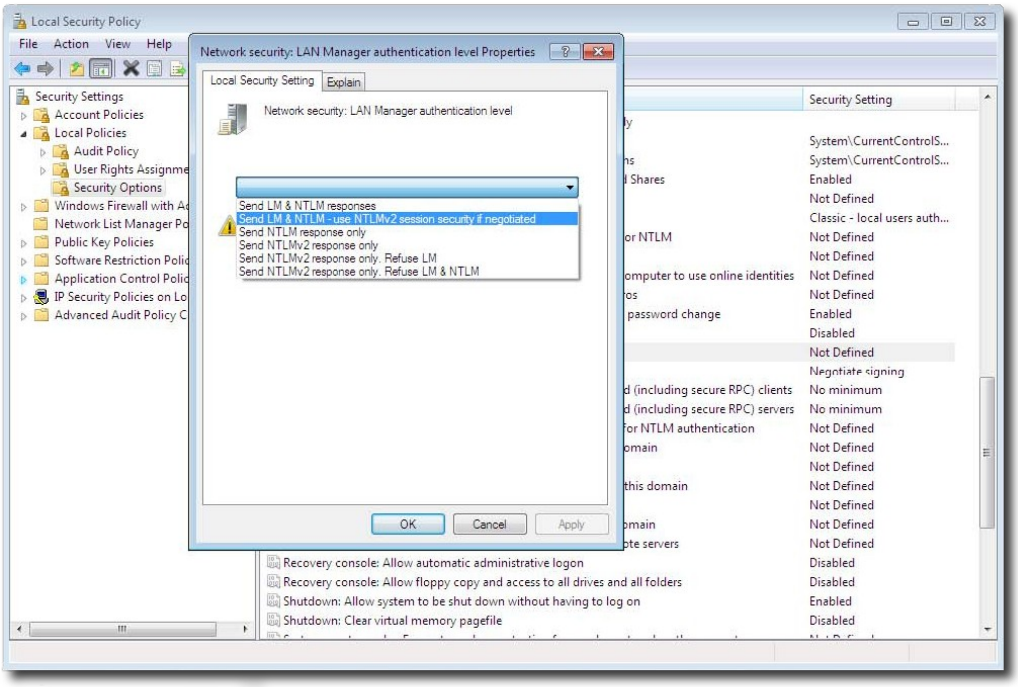
Require NTLMv2 session security □
Require 128-bit encryption ☐

Step 6: Go back and select '**Network security: LAN Manager authentication level**'


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users auth...
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled

Step 7: Select from the pull down menu: **'Send LM & NTLM – use NTLMv2 session security if negotiated'**.

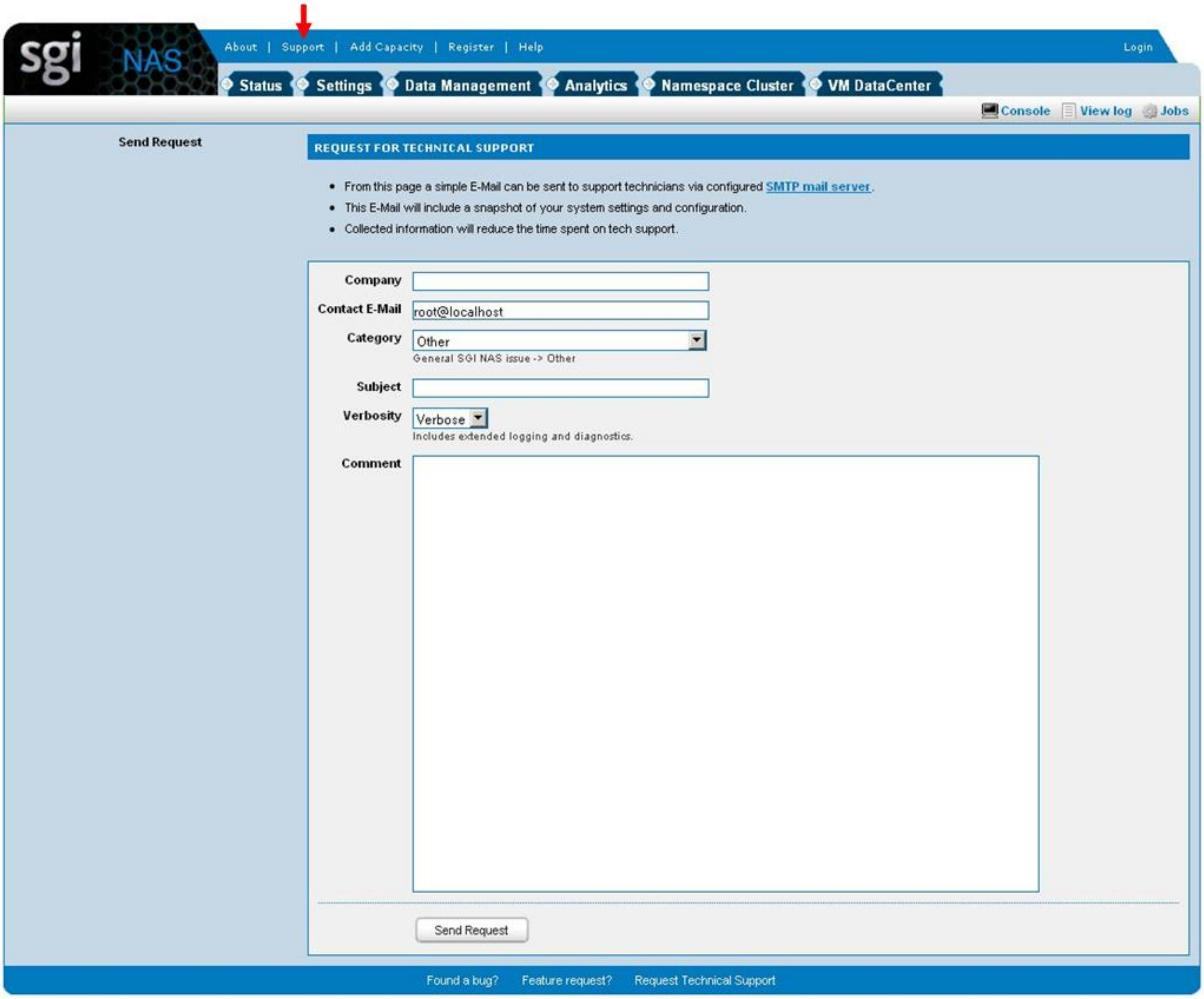

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignme
Security Options
Windows Firewall with A
Network List Manager Po
Public Key Policies
Software Restriction Polic
Application Control Polic
IP Security Policies on Lo
Advanced Audit Policy C
Network security: LAN Manager authentication level Properties
Local Security Setting
Explain
Network security: LAN Manager authentication level
Send LM & NTLM responses
Send LM & NTLM - use NTLMv2 session security if negotiated
Send NTLM response only
Send NTLMv2 response only
Send NTLMv2 response only. Refuse LM
Send NTLMv2 response only. Refuse LM & NTLM
OK
Cancel
Apply
Security Setting
Recovery console: Allow automatic administrative logon
Recovery console: Allow floppy copy and access to all drives and all folders
Shutdown: Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile

Click **Apply**. You are ready to mount the SGI NAS CIFS share.

4 Contact information

4.1 Support request

To contact support at SGI, click the Support link in NMV as marked with a red arrow on the screen below:



REQUEST FOR TECHNICAL SUPPORT

- From this page a simple E-Mail can be sent to support technicians via configured SMTP mail server.
- This E-Mail will include a snapshot of your system settings and configuration.
- Collected information will reduce the time spent on tech support.

Company

Contact E-Mail: root@localhost

Category: Other
General SGI NAS issue -> Other

Subject

Verbosity: Verbose
Includes extended logging and diagnostics.

Comment

or type the following NMC command:

```
nmc:/$ support
```

which will then prompt for a subject and message.

4.2 Other resources

For licensing questions, please contact your SGI sales or support representative.

Product Support

SGI provides a comprehensive product support and maintenance program for its products. For a full description of this program, do one of the following:

- See http://www.sgi.com/support/.

- If you are in North America, contact the Technical Assistance Center at 1 (800) 800 4SGI or contact your authorized service provider.

- If you are outside North America, see the following website for the appropriate Customer Service phone number: http://www.sgi.com/support/supportcenters.html.