



NAStorage

Administrator Guide

Security Policy Of NAStorage Under Macintosh Environment

Version 1.00

10/01/2002

Prepared by:

Leon Hsu

TS Engineer

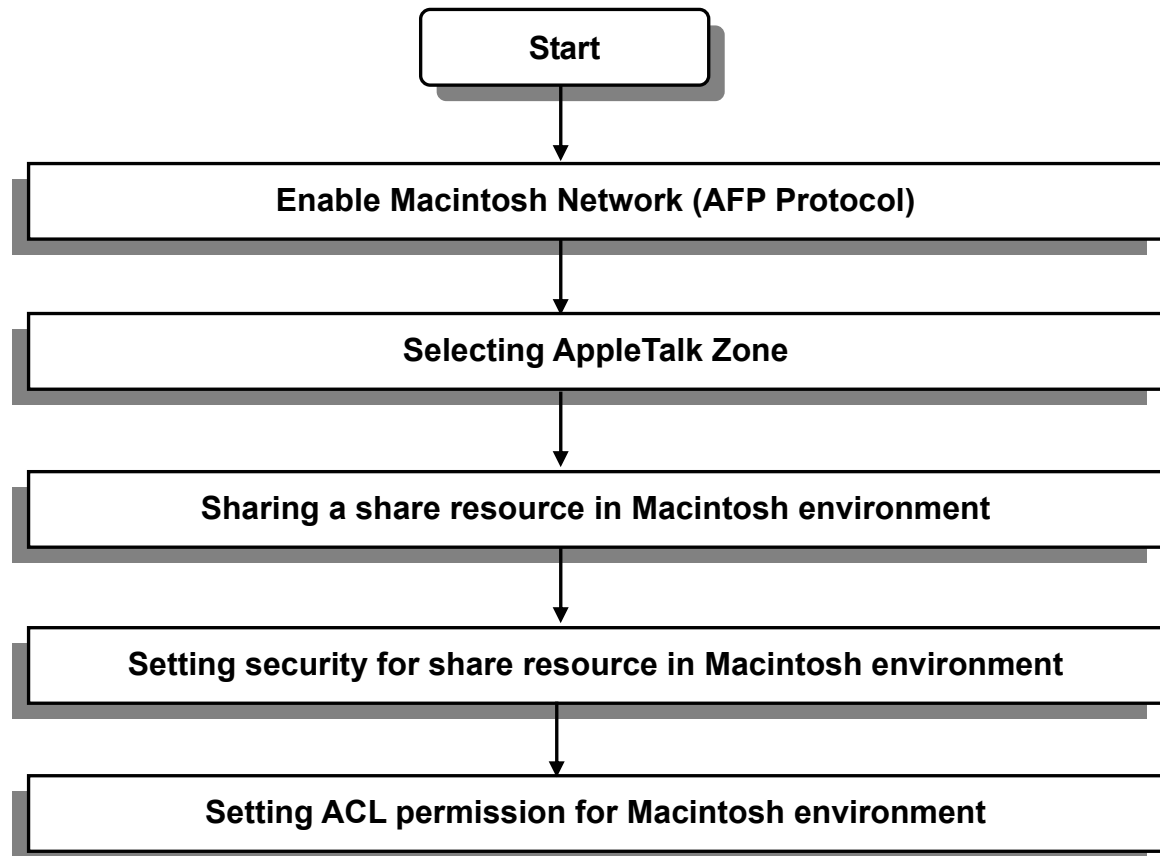
Ingrasys Technology Inc.

E-mail: support@ingrasys.com

NAS Server supports two kinds of protocols used for Mac OS clients - AppleTalk and TCP/IP (Open Transport). Also, NAS Server provides two kind of security policy for Macintosh Network AFP client.

- **Local account authentication** - Authenticate user using NAS Server's local user database.
- **Local and domain authentication** - If 'Microsoft Network' is enabled, you can enable both local or domain authentication for AFP client.
- **Current Zone** - A division between groups of machines when viewed using AppleTalk. AppleTalk Zones can be seen in the Chooser, the AppleTalk Control Panel, and the Network Browser. (there's no Chooser in OS X)
- **Address** - It is a unique number that identify the server on the network. The number on the left of the dot is the network number. The number on the right of the dot is the node number.

Security Policy of NASStorage under Macintosh Environment



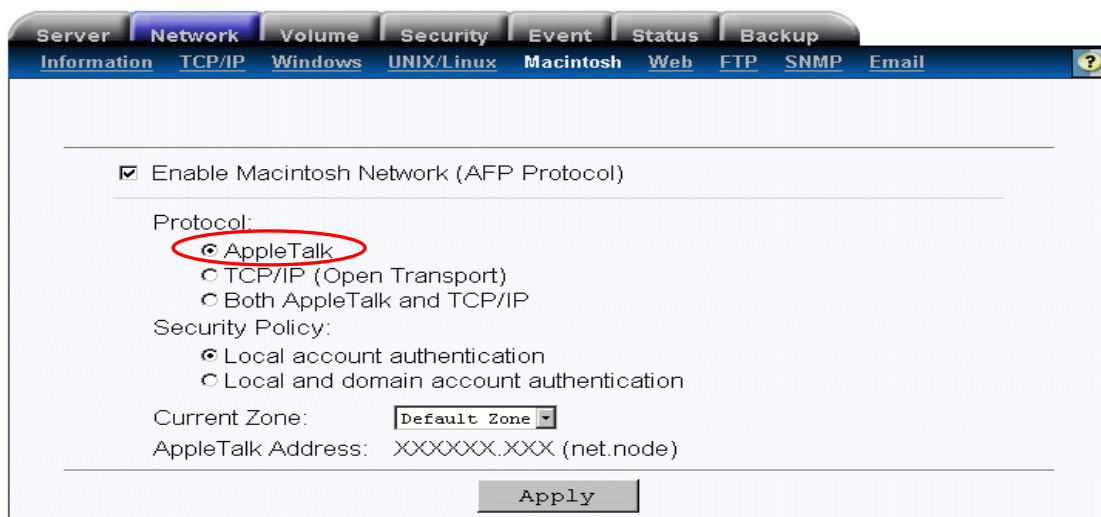
1. Enabled Macintosh Network (AFP Protocol)

For file accessing, users can access NASStorage via Macintosh Network (AFP Protocol). NASStorage Server supports two kinds of protocols used for Mac OS clients - AppleTalk and TCP/IP (Open Transport). You just need enable Macintosh Network (AFP Protocol) for NASStorage.

A. Apple talk

This mode NASStorage server will use “Apple Talk” to communicate, that mean Mac clients also need use “Apple Talk” protocol to find the NASStorage server.

Configuration flow: “**Network–Macintosh**”→ Enable –“**Enable Macintosh Network (AFP Protocols)**” check box →Select “**Apple Talk**” → then “**Apply**”.



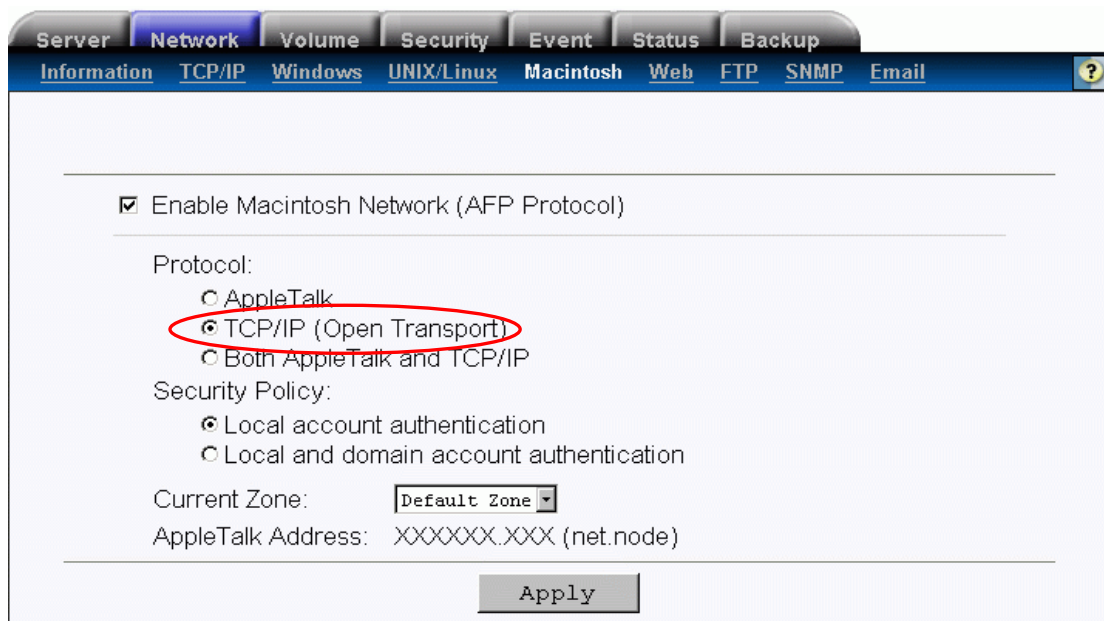
You can find the NASStorage server by “**Connect to server**” function.



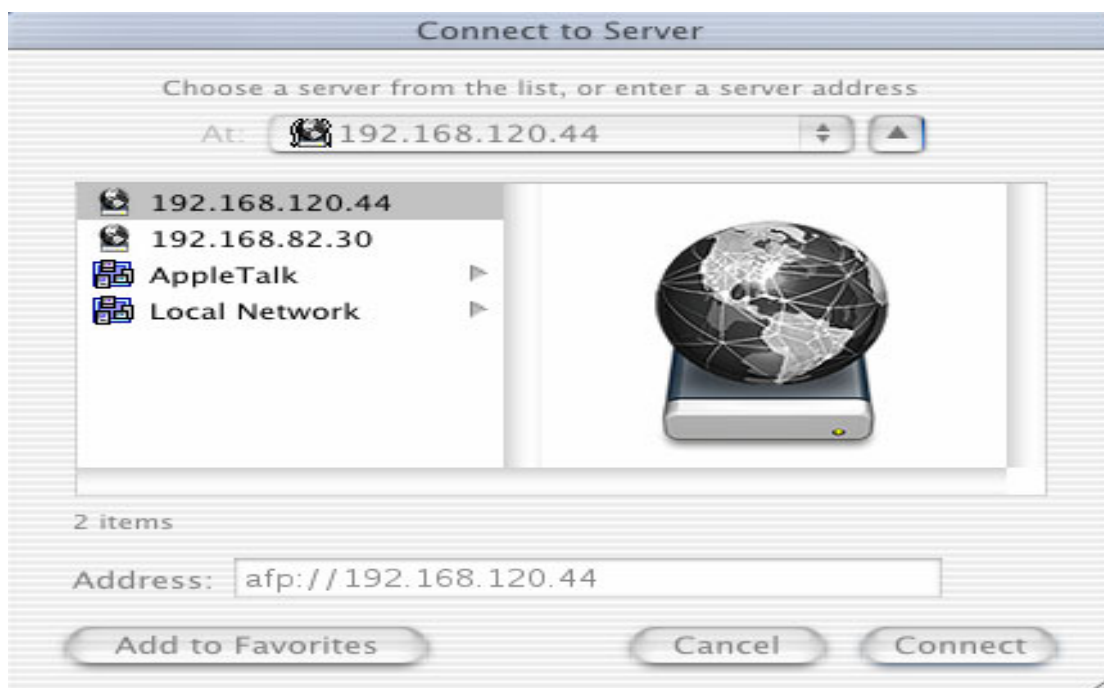
B. TCP/IP (Open Transport)

In this mode, if Mac clients want to find the NASStorage server, it must use IP address to find.

Configuration flow: “**Network–Macintosh**“→ “**Enable**” check box –Enable Unix/Linux Network (NFS Protocols)→Select “**TCP/IP (Open Transport)**” → then “**Apply**”.



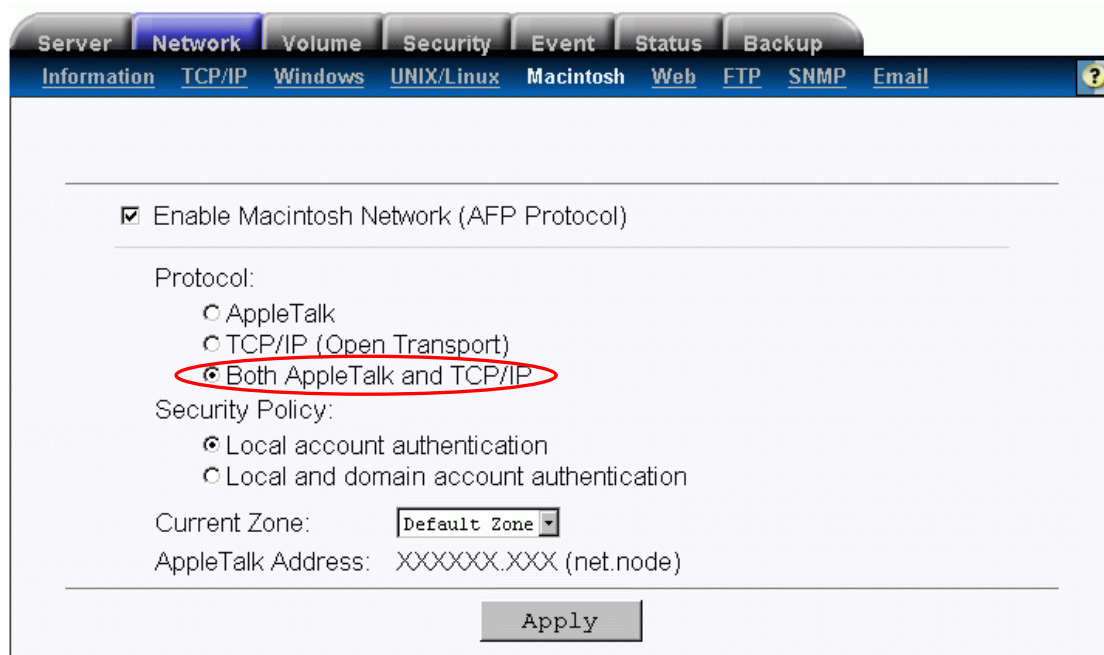
In MAC client, you can enter the NASStorage server IP address to connect NASStorage server



C. Both AppleTalk and TCP/IP

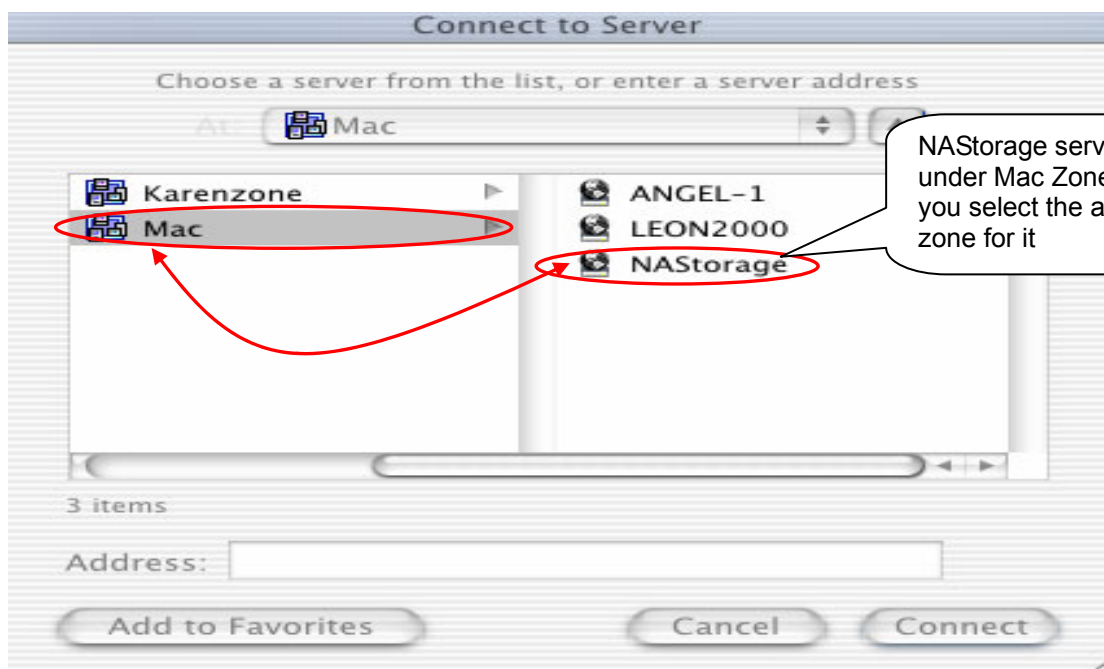
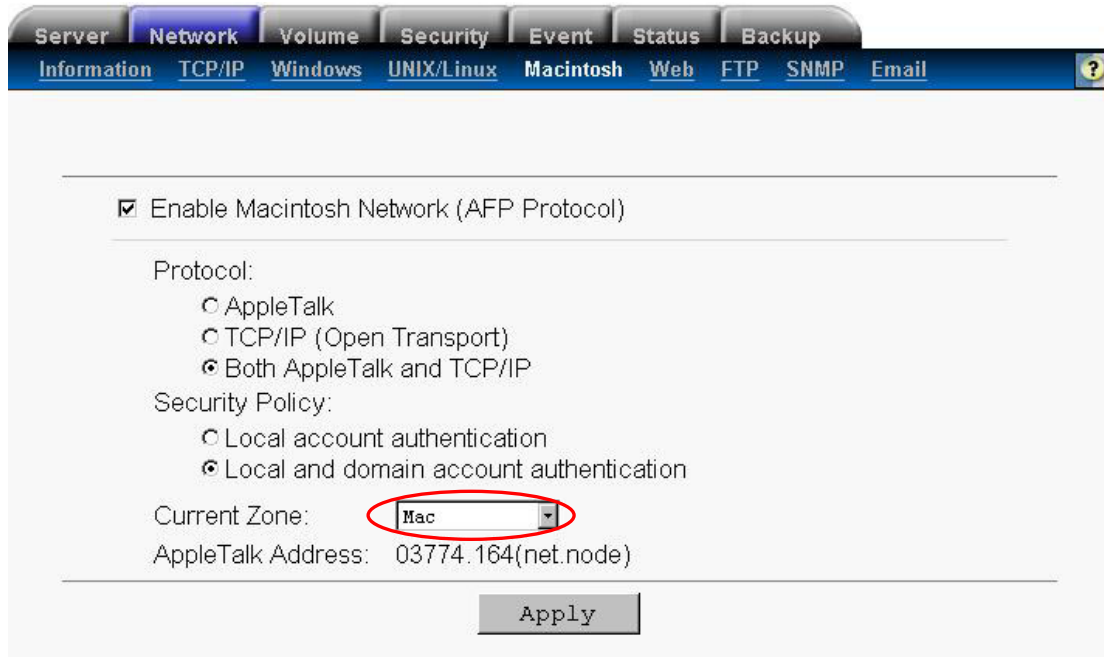
If you select this mode for NASStorage, Mac clients can find this server by Apple Talk or TCP/IP

Configuration flow: **“Network–Macintosh“**→ **“Enable”** check box –Enable Unix/Linux Network (NFS Protocols)→Select **“Both Apple Talk and TCP/IP”** → then **“Apply”**.



2. Selecting AppleTalk Zone

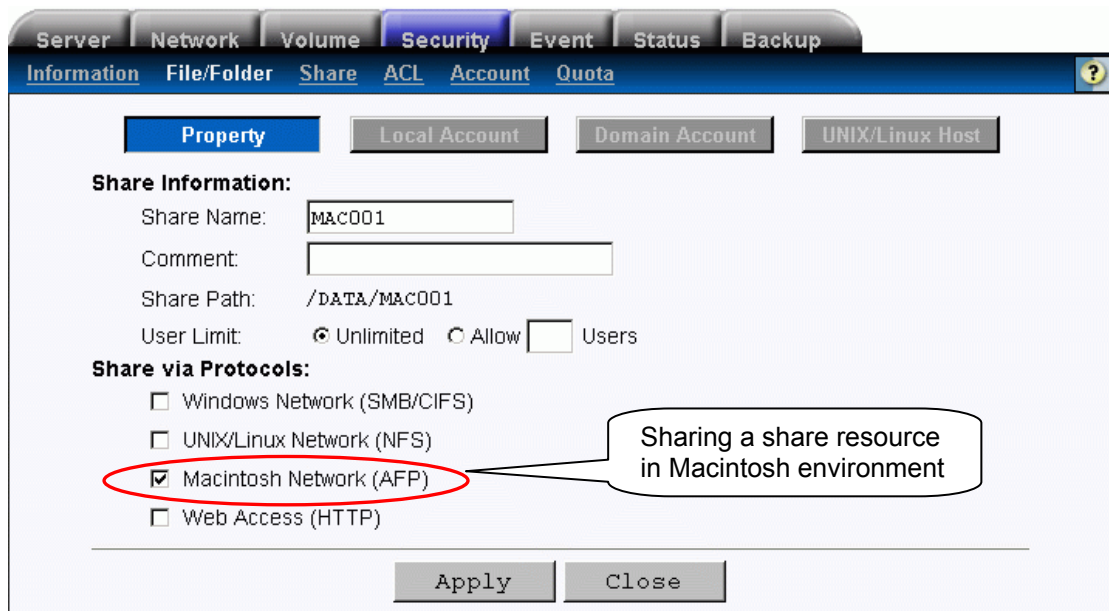
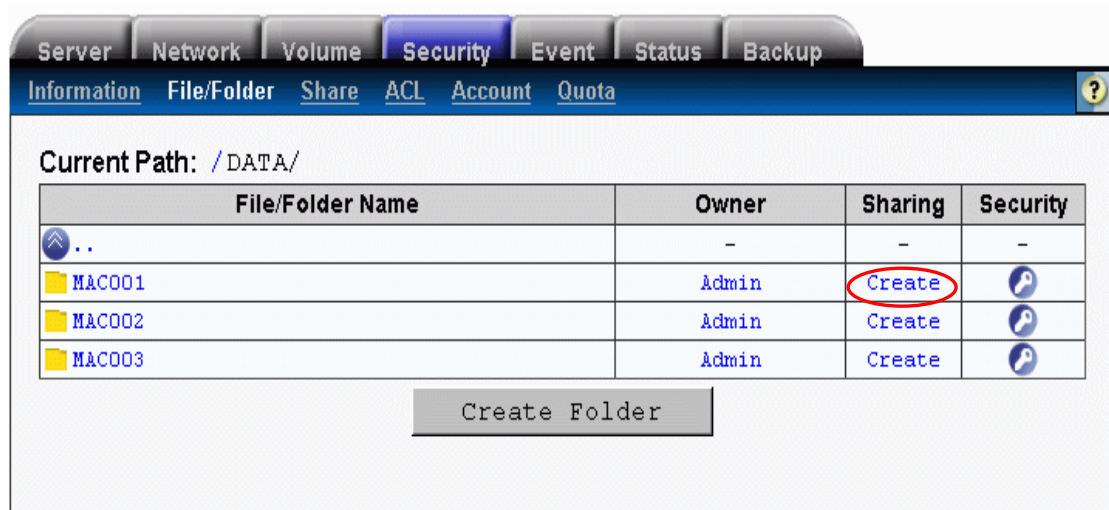
NAStorage server support “Apple Talk Zone” mode, you can select a zone which you want NAStorage server joins. An AppleTalk zone is a logical group of nodes or networks that is defined when the network administrator configures the network. The nodes or networks need not be physically contiguous to belong to the same AppleTalk zone.



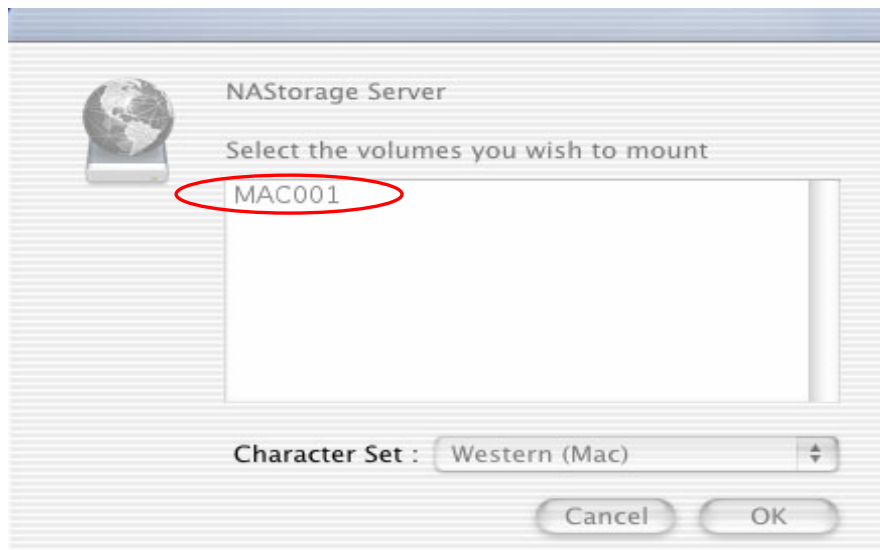
3. Share a share resource in Macintosh environment

If someone want to share a share resource from NASTorage in Macintosh environment, just need enable “Macintosh Network (AFP)” for share resource.

Configuration flow: “**Security Manager–File/Folder** “→click “**create**” → enable “**Macintosh Network (AFP)**” →then **Apply**.



You can connect the NASTorage server by "Apple Talk" or "TCP/IP" protocol and you will find this share already shared under this server volume list.



There's one thing need concern, when you connect to the NASTorage server by MAC client, you just can see the volumes which you have permission under Macintosh environment.

4. Setting security for share resource in Macintosh environment

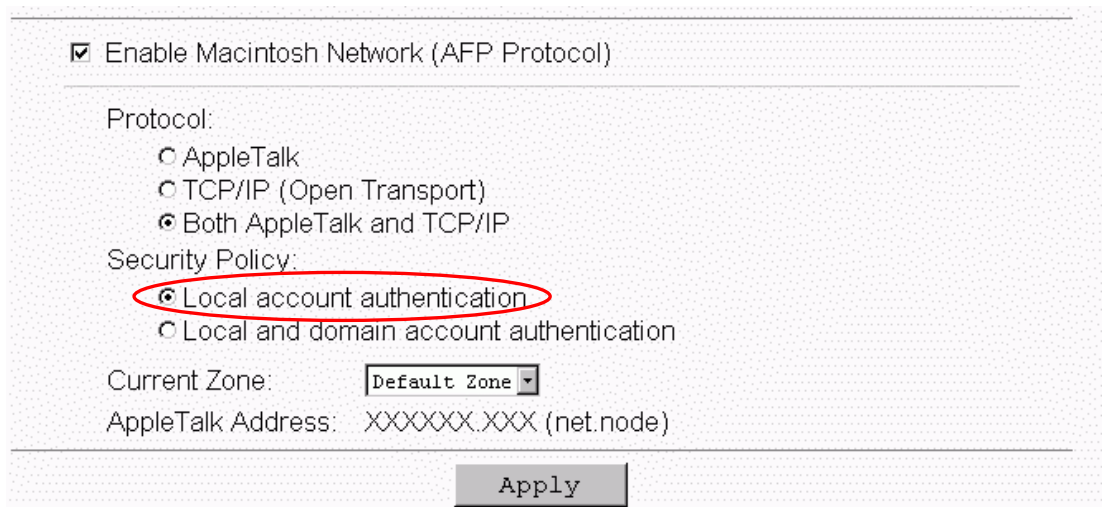
NAS Server provides two kind of security policy for Macintosh Network AFP client.

- **Local account authentication** - Authenticate user using NAS Server's local user database.
- **Local and domain authentication** - If 'Microsoft Network' is enabled, you can enable both local or domain authentication for AFP client.

A. Local account authentication:

Authenticate user will use NAS Server's local user database. You need change the security policy to “Local account authentication” mode.

Configuration flow: “**Network–Macintosh**” → Select “**Local account authentication**” → then **Apply**.



The screenshot shows the 'Network–Macintosh' configuration window. At the top, the checkbox 'Enable Macintosh Network (AFP Protocol)' is checked. Below this, the 'Protocol:' section has three radio button options: 'AppleTalk', 'TCP/IP (Open Transport)', and 'Both AppleTalk and TCP/IP'. The 'Security Policy:' section has two radio button options: 'Local account authentication' (which is selected and circled in red) and 'Local and domain account authentication'. Below the security policy, there is a 'Current Zone:' dropdown menu set to 'Default Zone' and an 'AppleTalk Address:' field with the placeholder 'XXXXXX.XXX (net.node)'. At the bottom center, there is an 'Apply' button.




After you select this mode, you can assign the permission to local user under Macintosh environment.

Configuration flow: “**Security Manager–Share** “ → click “**Permission**” → “**Local account**” → “**Add**” user from left to right window and select the permission → then **Apply**

Server Network Volume **Security** Event Status Backup

Information File/Folder Share **ACL** Account Quota

List of Shares:

Share Name	Share Path	Permission	
MAC001	/DATA/MAC001		<input type="checkbox"/>
MAC002	/DATA/MAC002		<input type="checkbox"/>
MAC003	/DATA/MAC003		<input type="checkbox"/>

Server Network Volume **Security** Event Status Backup

Information File/Folder Share **ACL** Account Quota



Property **Local Account** Domain Account

Share Information:
Share Name: MAC001
Share Path: /DATA/MAC001

Share Permission:

Specify Privileged Local Account

<p>----- Unselected -----</p> <p>Afpuser02 Afpuser03 Guest Admin Everyone* Admins*</p>	<p>>></p> <p><<</p>	<p>----- Privileged -----</p> <p>RW - Afpuser01</p>
--	---------------------------------	--

 Read/Write (RW)
 Read/Write (RW)

Apply Close

NASStorage will count on the settings here to determine which user can access data from NASStorage with certain read/write permission.

For example (User account **Afpuser01**), you assign Read/Write permission for this user in NASStorage server. Therefore this user can mount the share resource from NASStorage and also can create file/folder in the mount point.

0004

 Connect to the file server "NASStorage Server" as:

Guest

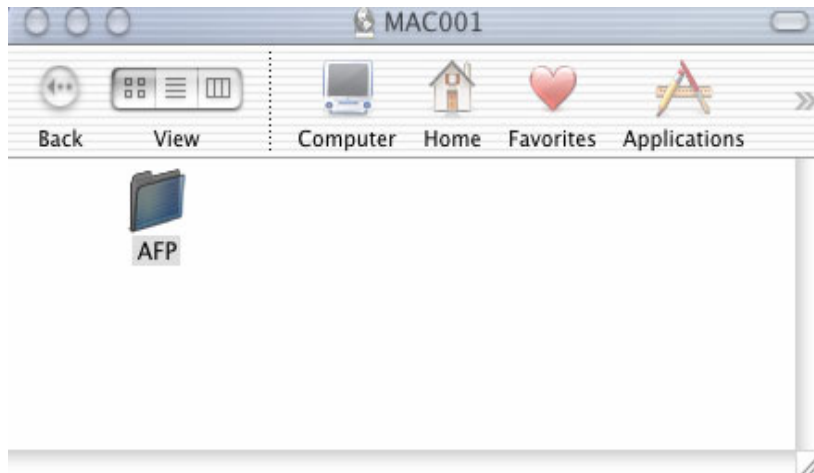
Registered User

Name:

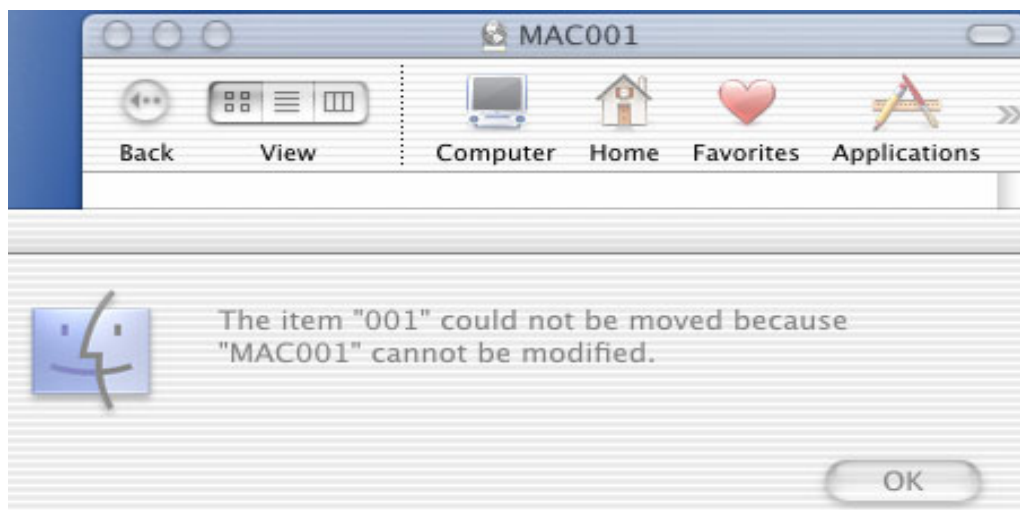
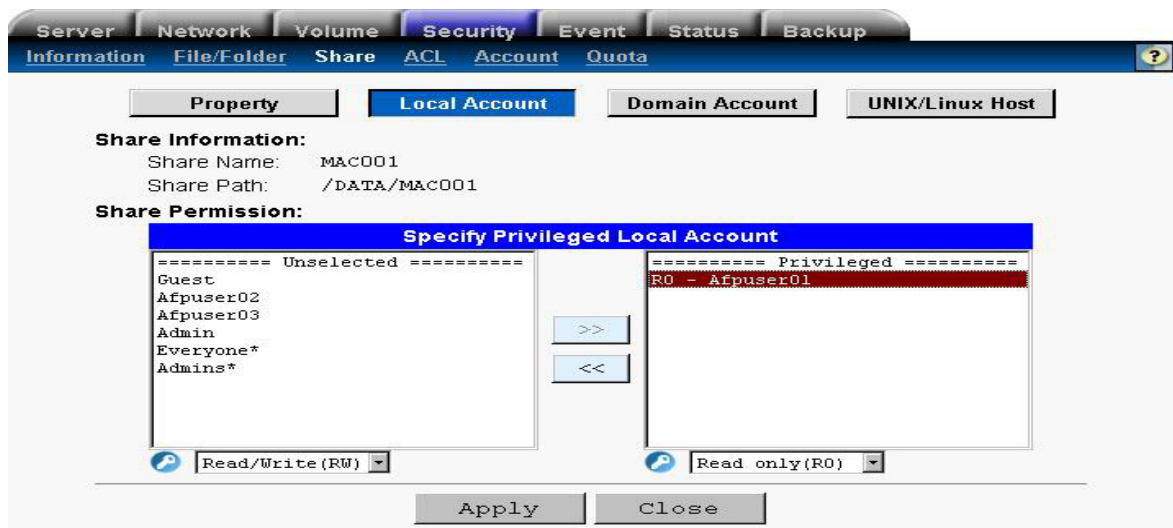
Password:

[Clear Text Password](#)

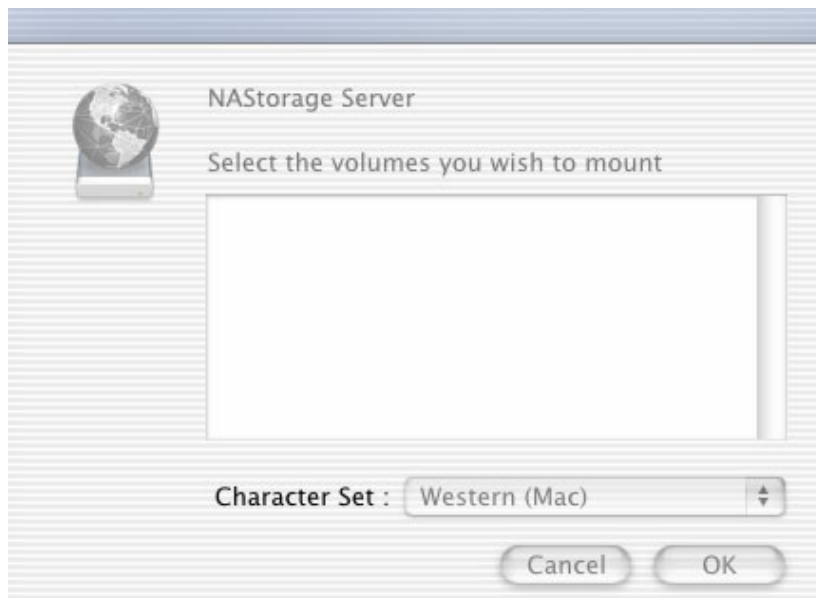
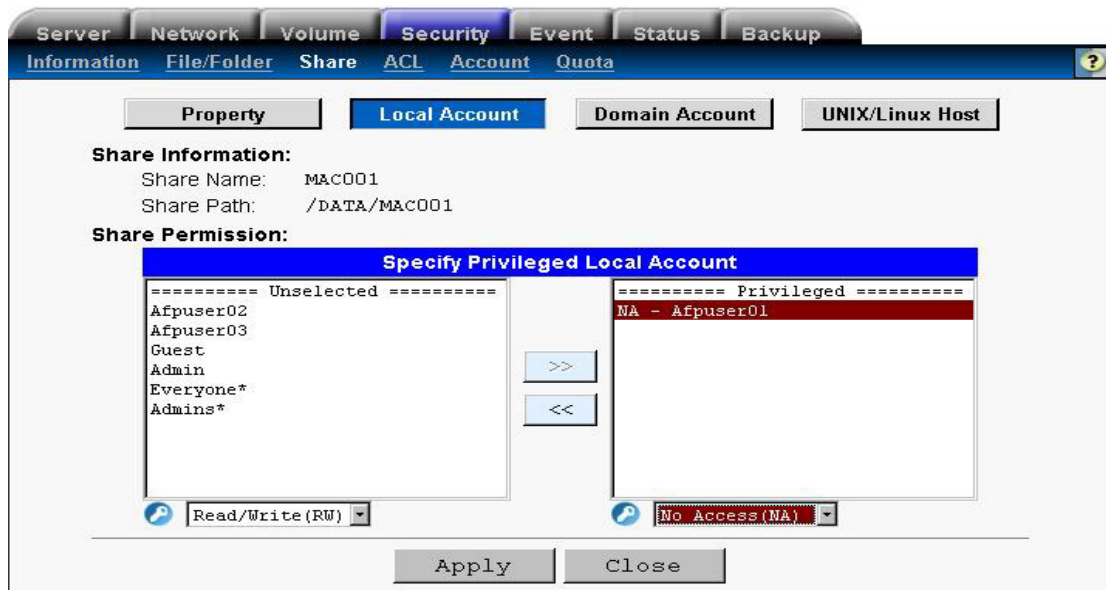
Options... Cancel Connect



If you change the permission Read/Write to Read-Only for “Aftpuser01” user, you can mount this share resource but you don’t have write permission in the mount point.



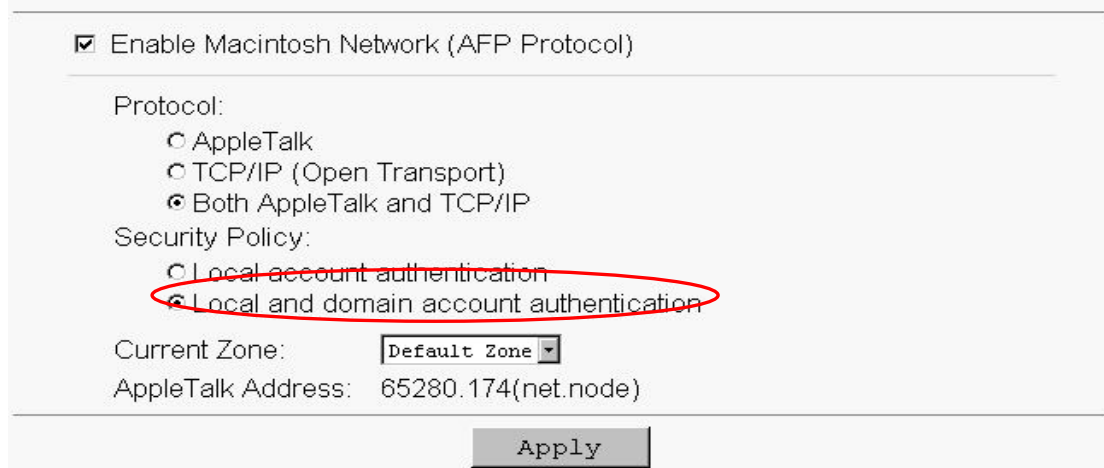
If you assign this user permission to No Access (NA), this user won't see this share under volumes list.



B. Domain account authentication

Authenticate user will use NAS Server's local user database and Windows PDC's user database. You need change the security policy to "Local and domain account authentication" mode.

Configuration flow: "Network-Macintosh" → Select "Local account authentication" → then **Apply**.



Enable Macintosh Network (AFP Protocol)

Protocol:

- AppleTalk
- TCP/IP (Open Transport)
- Both AppleTalk and TCP/IP

Security Policy:

- Local account authentication
- Local and domain account authentication

Current Zone:

AppleTalk Address: 65280.174(net.node)

Configuration flow: "Security Manager-Share" → click "Permission" → "Domain account" → "Add" user from left to right window and select the permission → then **Apply**



Server Network Volume **Security** Event Status Backup

Information File/Folder Share ACL Account Quota

Share Information:
Share Name: MAC001
Share Path: /DATA/MAC001

Share Permission:

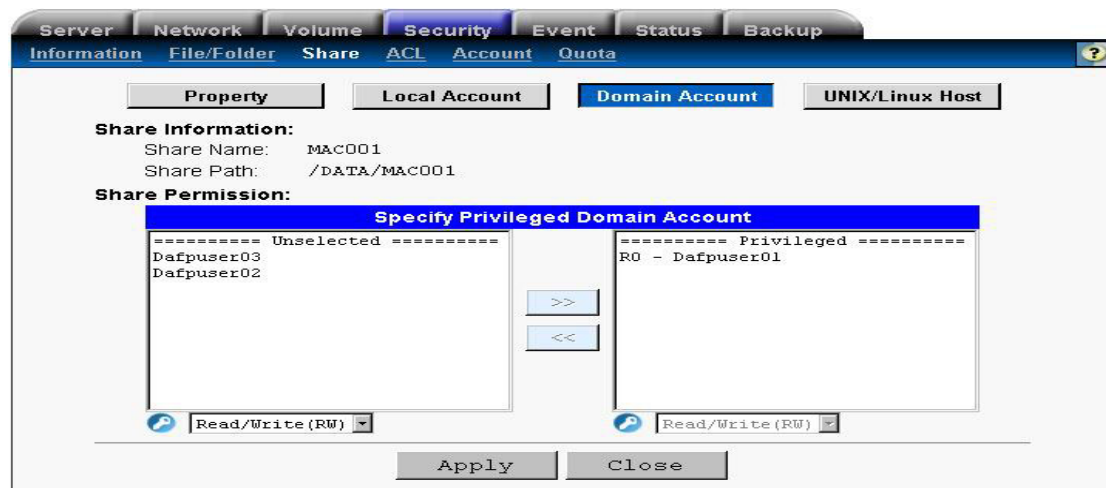
Specify Privileged Domain Account

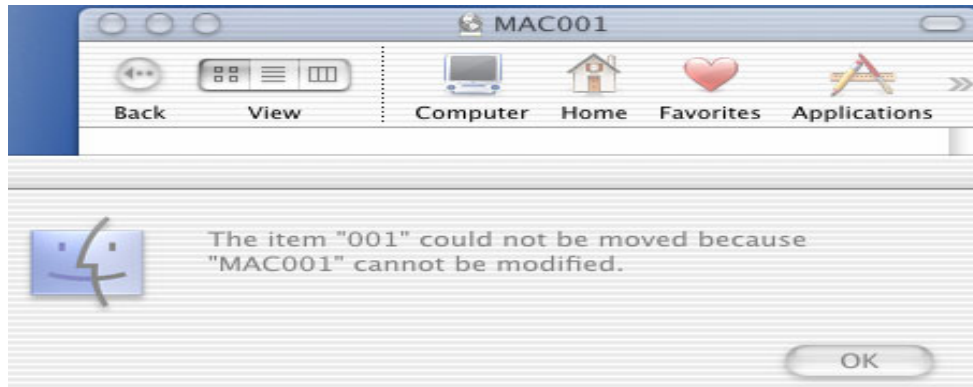
Unselected	Privileged
Dafpuser03	RW - Dafpuser01
Dafpuser02	

For example (Domain user account **Dafpuser01**) you assign Read/Write permission for this user in NASTorage server. Therefore this user can mount the share resource from NASTorage and also can create file/folder in the mount point.

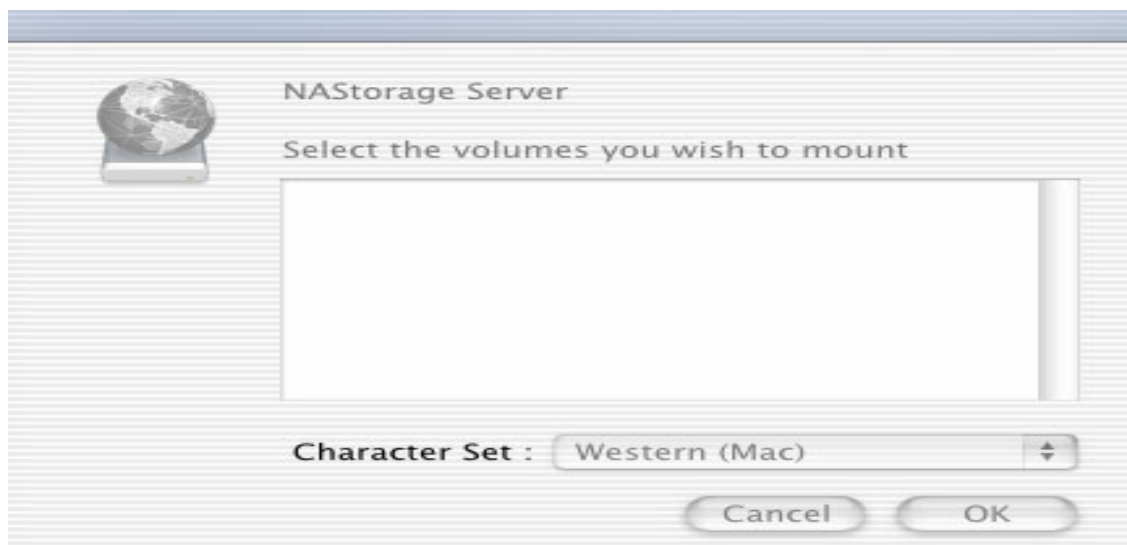
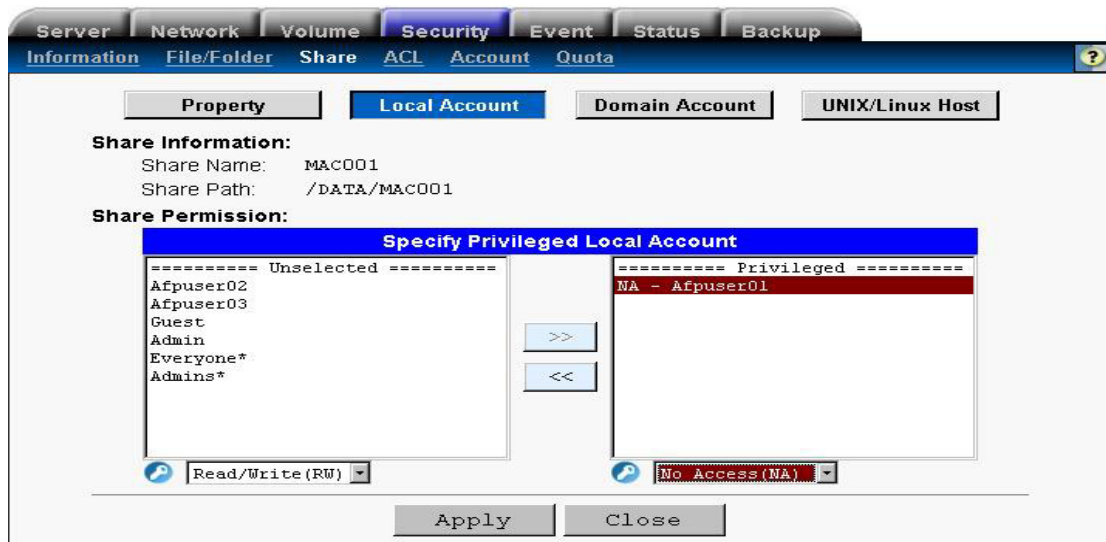


If you change the permission Read/Write to Read-Only for "Dafpuser01" user, you can mount this share resource but you don't have write permission in the mount point.





If you assign this user permission to No Access (NA), this user won't see this share under volumes list.



5. Setting ACL permission for Macintosh environment

In Macintosh environment, NASStorage also support ACL. Access Control Lists (ACL) are associated with each file and folder, as well as the list of users and groups permitted to use that file or folder. When a user is granted access to the file or folder, an ACL node is created and added to the ACL for the file or folder.

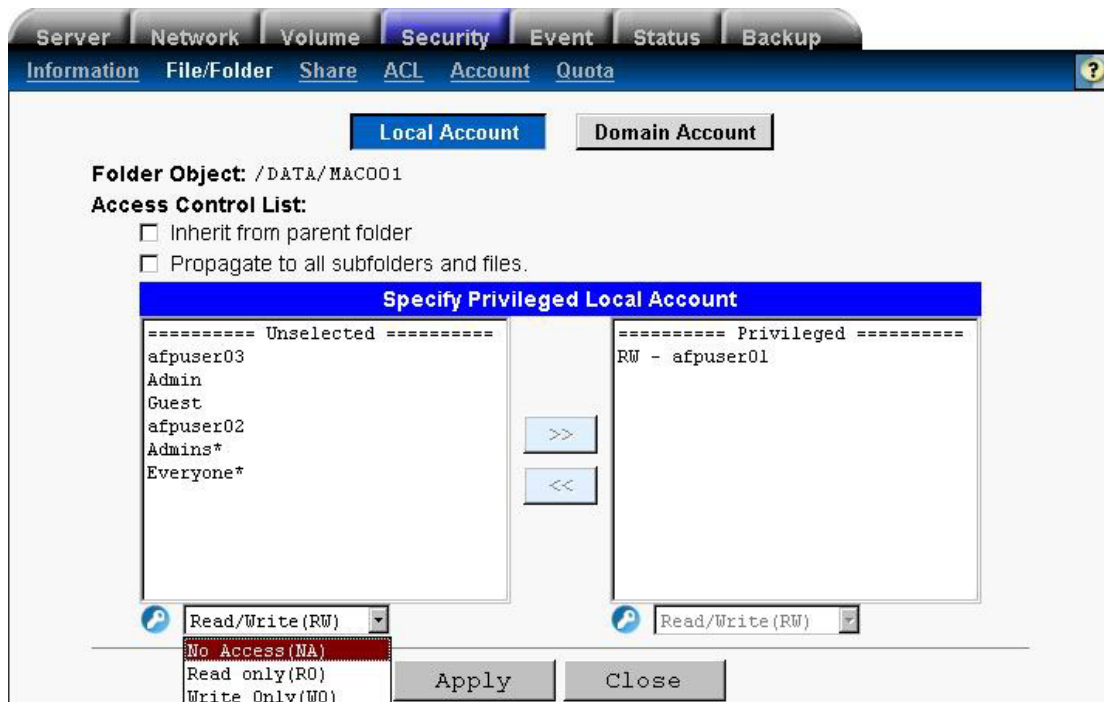
If you assign permissions to a specific user, the UID of that user is allocated to the ACL for the file or folder. If the user is then deleted, and the same name is created as the previous one, the new user does not have permissions to the file or folder, because the UID will not be the same. The administrator will have to reconfigure all the group memberships and access rights to the file and folder.

Note: If the administrator changes the permission on a file or folder that a user is currently accessing, the permission setting do not take immediate effect because of the local handle being used by the user. The new rights will only take effect when the user reconnects to the file or folder.

Configuration flow: **“Security Manager–File/Folder “**→ click **“Security ”** → **“Local account/Domain account ”** → Disable the **“Inherit from parent folder“** check box→Add user from left to right window and select the permission→ then **Apply**



File/Folder Name	Owner	Sharing	Security
..	-	-	-
MAC001	Admin	Modify	
MAC002	Admin	Modify	
MAC003	Admin	Modify	



You can assign the following File/Folder permission to a user in NASTorage server.

No Access (NA): Account has been denied access to the file or folder.

Read Only (RO): Account is allowed to read the file or folder.

Read/Write (RW): Account is allowed to write and read the file or folder.

Write Only (WO): Account is allowed to write the file or folder

Full Control (FC): Account is allowed to read/write and change permission to the file or folder.

You will find the path of ACL node under ACL list page and you can also change the permission for this node.

Configuration flow: **“Security Manager–ACL“** → click **“Permission”** → **“Local account/Domain account”** → Add user from left to right window and select the permission → then **Apply**

