

How to set up your ReadyNAS for Individual user based control over shares.

I hope this manual helps you out of a spot. I got totally confused with setting up a ReadyNAS for a controlled user/share environment and finally had to resort to forums and personal research to get on top of it. I may be simple but I am not dumb, I work for a global IT support company and found the ReadyNAS set up to be complicated enough to scare users away from a great product.

This manual is written to suit my basic needs and may not be suitable for others, but I do hope it contains some useful pointers, that could get others out of a spot. I write with the assumption that the user has a firm grasp of networking and sharing policy, and that the administrator has already set the ReadyNAS up ready for configuration. It is not a “ReadyNAS set up guide for Dummies” nor is it an exhaustive encyclopedia on ReadyNAS and its integrated technology. It is (I trust) an overview of how to set up a ReadyNAS for use in (what I would have imagined) the most commonly required configuration for small to medium businesses.

Step 1. Prepare the ReadyNAS for configuration by setting the security mode to “User”

*WARNING- If you have already been using the NAS in “Share” mode and have shares set up with data on them, be sure to copy all data off the NAS and delete the shares. (This is not the only way around this but is simplest. If you have too much data or think you are capable of more advanced forms of data relocation see the notes at the end of this manual) The reason for doing this is if you incorrectly set up users it is possible to lock yourself away from your own data.

- a) First log into your NAS box via your web browser. This is done by simply entering the LAN IP address of the device into the address bar followed by “/admin”. So for example the url might read: <http://192.168.1.100/admin> Depending on your browser and settings you may be greeted with a “security certificate error” message.

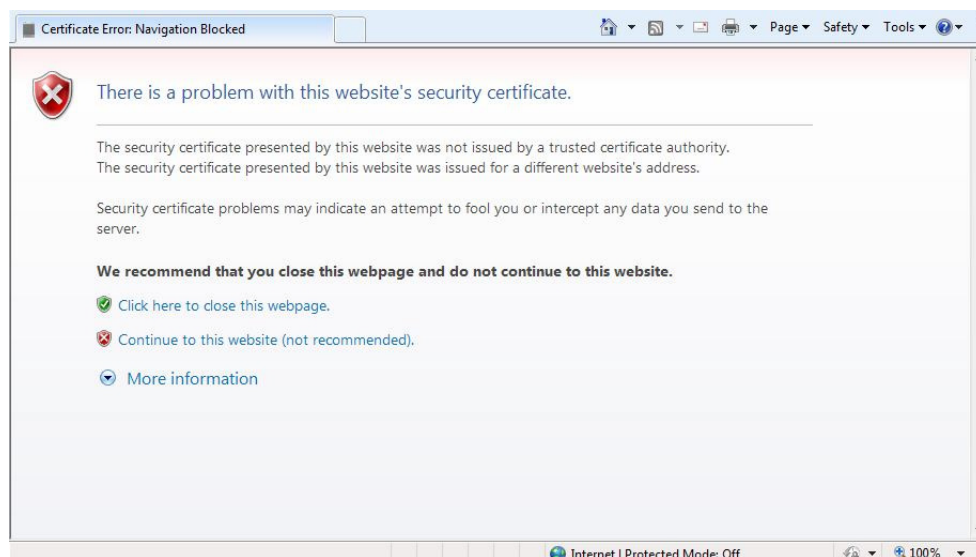


Figure 1. Certificate Error

Note: See <https://readynas.sphardy.com/web/readynas/how-to-migrate-to-user-security-mode> for an alternative way to migrate to user mode without requiring existing shares to be removed and restored

Ignore the error message and do whatever you have to do to continue to the next stage. A login box should then show. Fill out your login credentials and click "OK". The ReadyNAS "Frontview" Homepage should load. On the left hand side find the "Security Mode" link under "Security" and click on that.

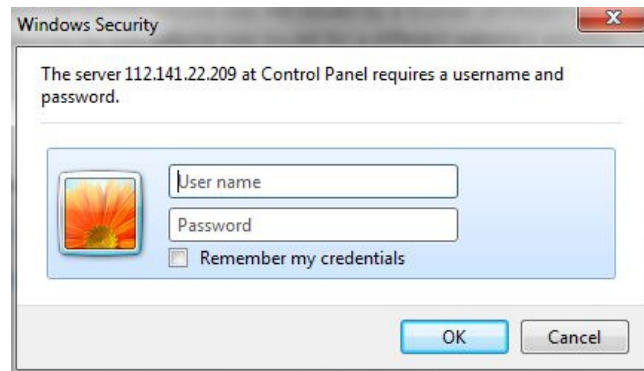


Figure 2. Login Dialogue

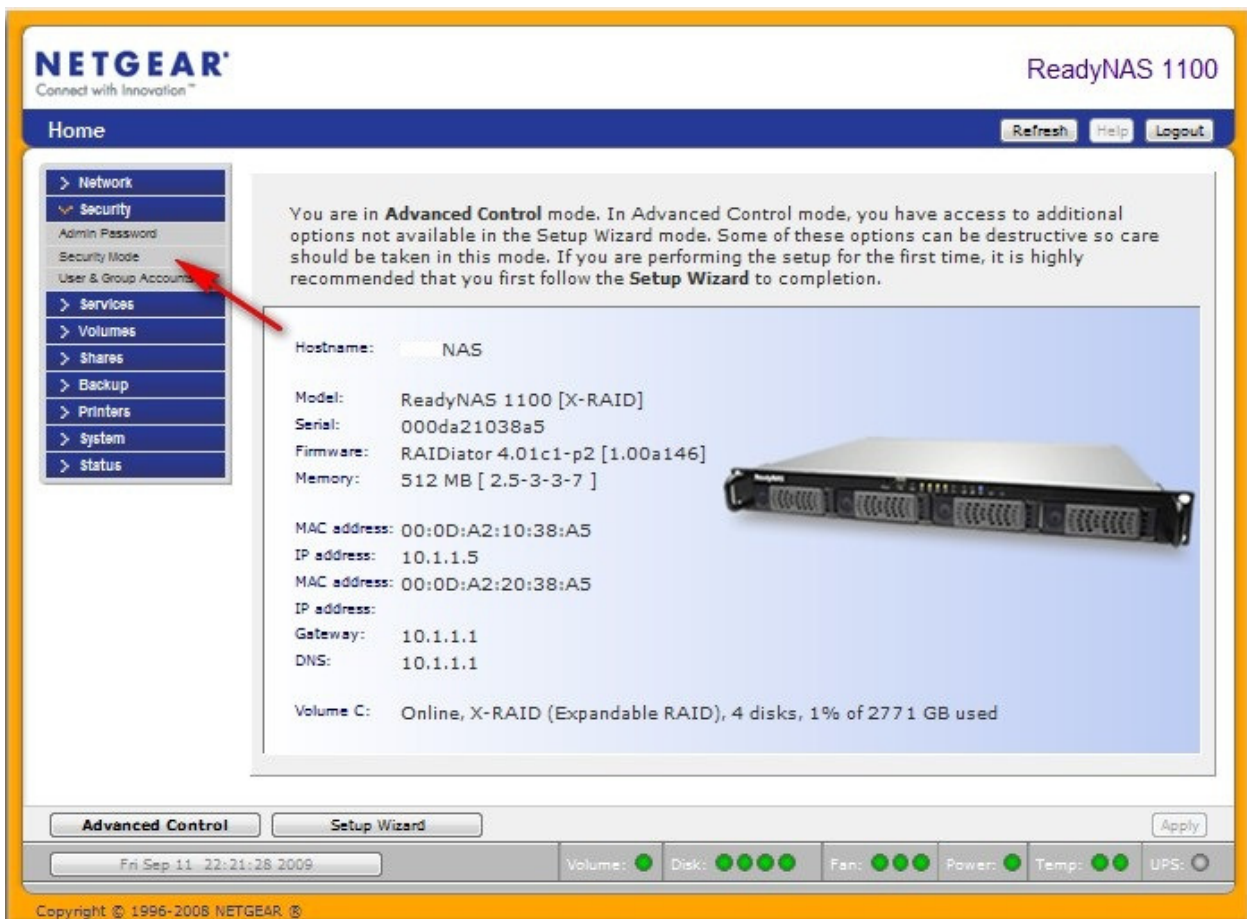


Figure 3. ReadyNAS Frontview Homepage (1100 Model)

- b) Set the Security mode to “User” and enter the correct workgroup name. You may get a pop “Message from Webpage”. Read it carefully and make sure you understand the implications of what you are doing before proceeding. If you have backed up all data and/or are confident about what you are doing. Click “OK” then “Apply” at the bottom of the page.

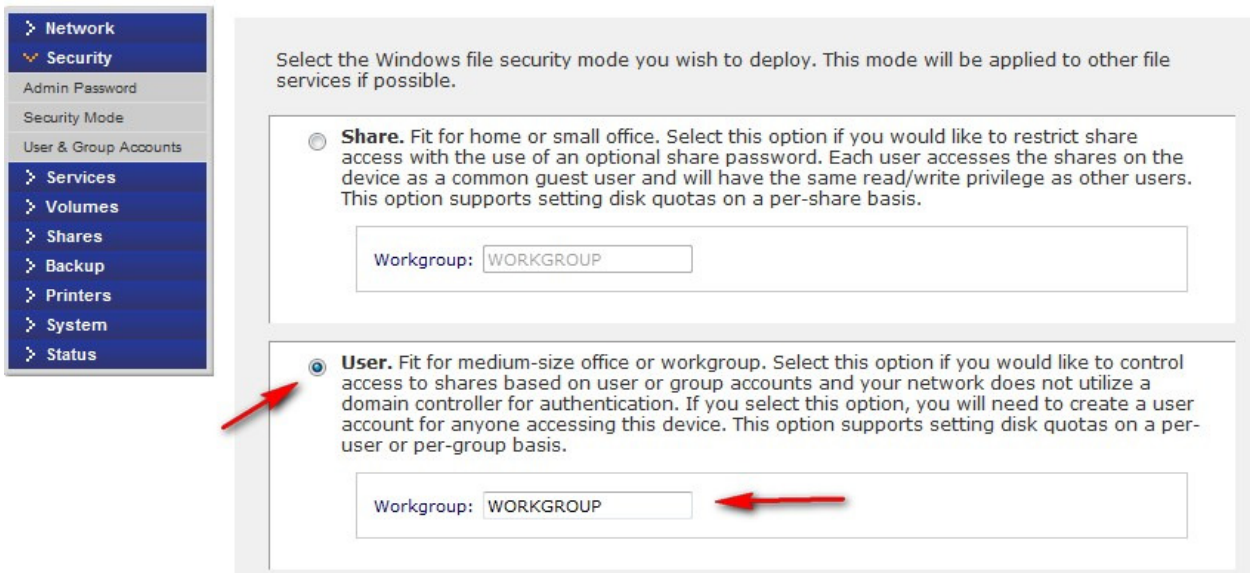


Figure 4. Change Security Mode

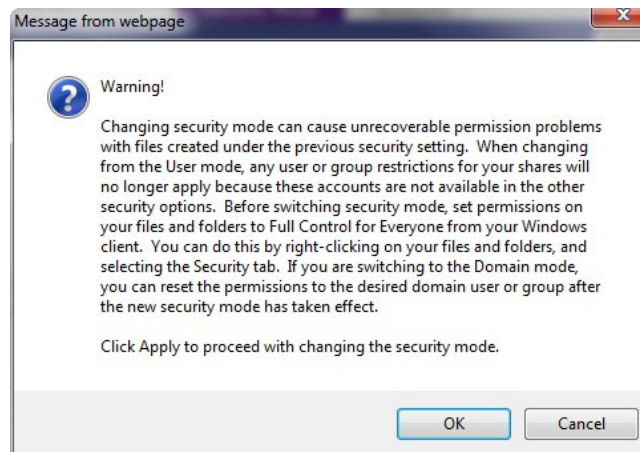


Figure 5. Warning Message

Wait for the changes to take affect before proceeding. You may get a message saying “changes are being performed in the background”. Click OK to this and wait till you are notified of completed changes. You can check in the system logs to make sure this has happened. (Status > Logs)

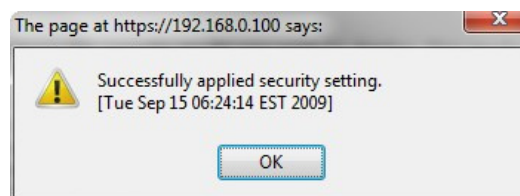


Figure 6. Security Setting Changed

Step 2. Prepare your workspace sharing map.

Preparation. Where EVERYone fails. Yep and you've probably read it in every home brewed guide you bother to download. "Every second of preparation makes everyone's life a lot easierEven yours" Here is where you need to sit down and consider how you want your sharing system to work. Who you want to have access to what. How they access it. When they access it. To save detailing every possible option and configuration, I have come up with a typical scenario that can be easily understood, and simply modified to fit most applications.

Scenario: Company “ABC Trading” has recently upgraded their onsite infrastructure to include a ReadyNAS NV + network attached storage device. They need to use the device as a secure backup location, a temporary directory for file transfers within the organization, and a secure sharing space that will allow limited access to public users visiting the network. They have 5 permanent desktop PCs on the network. Each of which needs a private backup directory on the NAS accessible only by the user of the PC and a File administrator. The company has two main departments (sales/marketing & accounts) that would like to share files but keep access to files relative to each department, restricted to that department only. They need a share for files that need to be shifted around the entire company, but must be kept private from visitors to the network. And finally they need somewhere that any user on the network can store, share, transfer..... files with any other user on the entire network.

Sound interesting.....? It is...!! First let's consider the shares that you will need to create. We need one for every PC permanently attached to the network. So that is 5 straight away. Next we need one for each department. That makes another 2, (we're up to 7), one for the entire company, and one for public access....! So a total of 9 shared directories we need to create. Next the users. I always create two file administrator accounts. Just to be sure. One for each machine, so another five. Total $2 + 5 = 7$. Also we need to create some groups. For now we will just make three. Accounts, Sales & Marketing, and ABC trading.

Soooo....what is all this leading to.....well to make the set up of you NAS a LOT easier, you need to draw up a “permissions map”. Rather than describe how....I’m just going to show you one. ☺

[illegible]

After about 5 minutes of studying that I'm sure even the greenest of Network administrators could understand that diagram. It simply lists Users, Shares, and Groups and the correlation and permissions associated with each. Now that you can see mine, I strongly recommend you go and sketch up one of your own. I promise you it will make setting up your NAS a LOT easier.

Step 3. [Set up your Shares.](#)

Setting up Shares on a ReadyNAS is truly a simple operation. First let's go back to our Permissions Map. How many shares were there..? Nine in total, by the names of the blue boxes. OK so let's add them....! From the home page of Frontview, navigate to the "Add Shares" page.

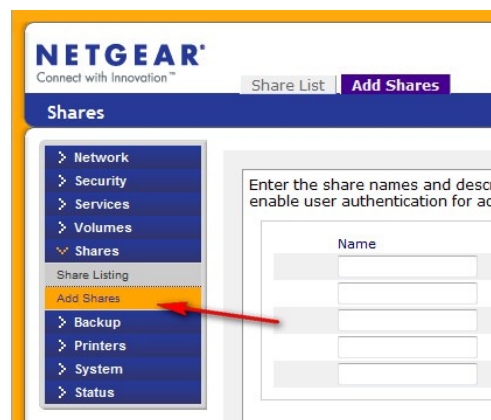


Figure 7. Add Shares

From here, this step is pretty easy. Setting up the shares simply involves entering the name of the share, a description (not needed but there for your convenience), and making sure that the "public" box is un ticked for shares that you don't want public. Once you have entered data in all the neccasserry fields click "Apply" at the bottom of the page.

Enter the share names and descriptions you wish to add. Deselect the Public Access checkbox if you wish to enable user authentication for access to this share via CIFS and AFP protocols.

Name	Description	Public Access
machine1	private directory for Machine 1	<input type="checkbox"/>
machine2	private directory for Machine 2	<input type="checkbox"/>
machine3	private directory for Machine 3	<input type="checkbox"/>
machine4	private directory for Machine 4	<input type="checkbox"/>
machine5	private directory for Machine 5	<input type="checkbox"/>

Figure 8. Adding Share, Three steps

When you click on “Apply” you should be greeted with an alert similar to below:

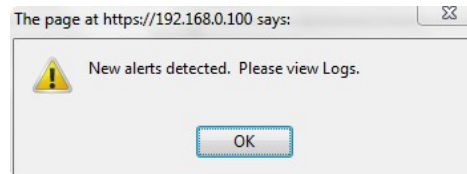


Figure 9. Alert Box

And the second lot.....note how I left the “public” box ticked for the Public share.

Name	Description	Public Access
salesmarketing	Sales and Marketing Share	<input type="checkbox"/>
accounts	Accounts Share	<input type="checkbox"/>
abctrading	Company Share	<input type="checkbox"/>
public	Public share	<input checked="" type="checkbox"/>

Figure 10. Public share

Double check all your shares are in place by visiting the “shares listing” page. I should look something like this:

- > Network
- > Security
- > Services
- > Volumes
- > **Shares**
 - Share Listing
 - Add Shares
- > Backup
- > Printers
- > System
- > Status

Shares on RAID Volumes

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. For instruction on how to access the shares,

Share Name	Description	CIFS	HTTP/S	Delete
abctrading	Company Share			<input type="checkbox"/>
accounts	Accounts Share			<input type="checkbox"/>
backup	Backup Share			<input type="checkbox"/>
machine1	private directory for Ma			<input type="checkbox"/>
machine2	private directory for Ma			<input type="checkbox"/>
machine3	private directory for Ma			<input type="checkbox"/>
machine4	private directory for Ma			<input type="checkbox"/>
machine5	private directory for Ma			<input type="checkbox"/>
media	Media Server Share			<input type="checkbox"/>
public	Public share			<input type="checkbox"/>
salesmarketir	Sales and Marketing Shi			<input type="checkbox"/>

Figure 11. Share listing

Step 4. [Set up Users and Groups.](#)

OK....Now you have your shares set up we should set up the Users and Groups that will be accessing the shares and what permissions they will have when they get there. Personally I find it easier to set up the groups first then the users. So from our chart above we only have two groups: "Accounts" and "Sales & Marketing" Let's set them up now.

From the Menu on the left select "Security > User & Group Accounts"

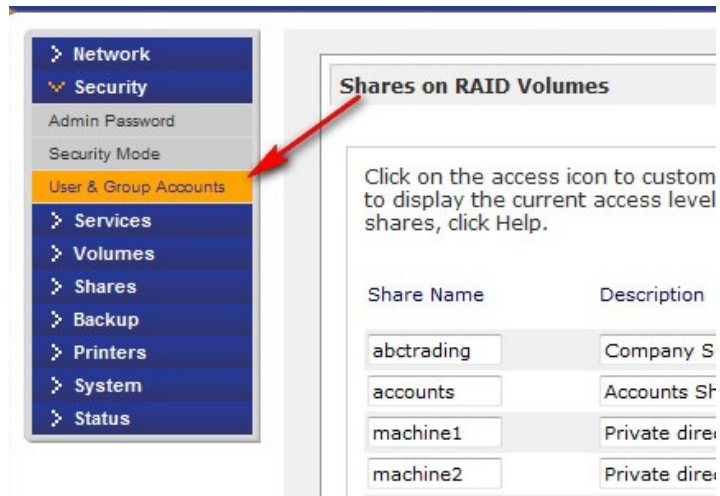


Figure 12. User & Group Accounts

You should see a page like this:

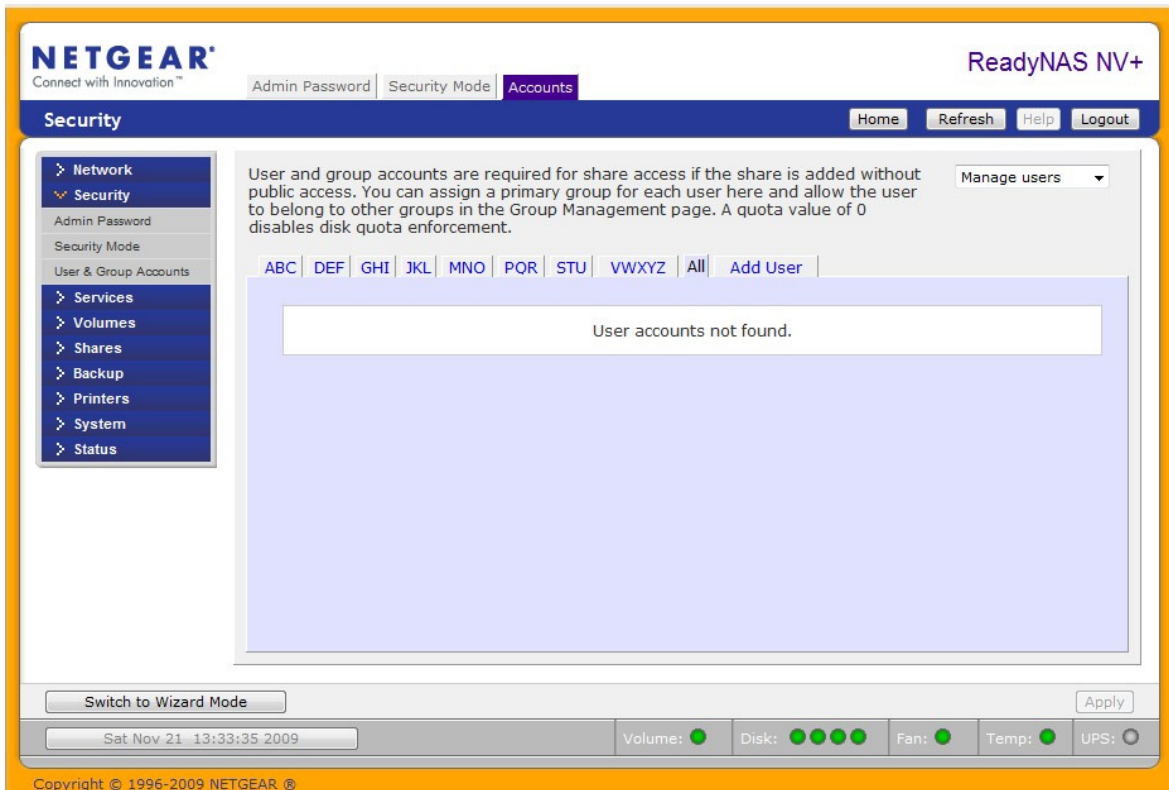


Figure 13. User & Group Page

At the top right of this page select “Manage Groups” from the dropdown menu. Then select the “Add Group” tab from the tabs along the top of the add groups window.

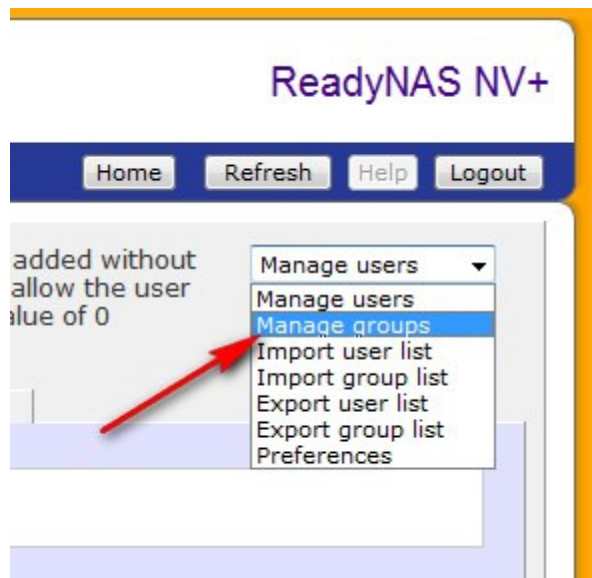


Figure 14. Manage Groups



Figure 15. Add Group

Fill out the names of the groups, then click apply. (I used “sandm” for “sales and marketing”) Don’t worry about the GID or quota boxes at this point in time.



Figure 14. Fill out Group details

Now for the users. Navigate to the users page by selecting “Manage Users” from the dropdown box in the top left of the “user & Group Accounts page (Similar to fig 14). Then select the “add user” Tab (similar to fig 15). Following your chart from earlier and the users in sets of five fill out the details as you go. I find it easier to keep all naming etc in lowercase letters. So details needed from left to right are: username, email address, UID, primary group, password, and quota. The UID and quota you can ignore for now. The email address you can leave out if you want. The username is pretty simple; just replicate the usernames straight off the chart. The primary group you can select from the drop down menu. The details for which group to select can also be found on your chart. If the user belongs to no group just leave it as the default “users”. You have to set up a password for each user when adding them. These passwords can be changed later. **Click Apply**. NOTE: You do not need to add a guest account. It is enabled on all ReadyNAS devices by default.

NETGEAR Connect with Innovation™ ReadyNAS NV+

Admin Password Security Mode Accounts

Security Home Refresh Help Logout

Manage users

User and group accounts are required for share access if the share is added without public access. You can assign a primary group for each user here and allow the user to belong to other groups in the Group Management page. A quota value of 0 disables disk quota enforcement.

ABC DEF GHI JKL MNO POR STU VWXYZ All Add User

Enter user accounts you wish to add. Specify email address if you wish to inform users of their newly activated account, quota warnings and quota violations (A quota value of 0 disables disk quota enforcement). You can leave the UID field blank unless the user intends to access this device via NFS. NFS users typically will want UIDs matching their accounts on other servers.

User	Email	UID	Primary Group	Password	Quota (MB)
fileadmin			users	*****	
manage			users	*****	
mach1			accounts	*****	
mach2			accounts	*****	
mach3			sandm	*****	

Switch to Wizard Mode Apply

Sat Nov 21 14:21:36 2009 Volume: Disk: Fan: Temp: UPS:

Copyright © 1996-2009 NETGEAR ®

Figure 17. Add users

Keep adding users in sets of five until you are done. Be sure to click apply after adding each set. If at any time you need to review all the users you have already click on the “all” tab just next to the “add user” tab. Your final set of users should look something like the screenshot below.

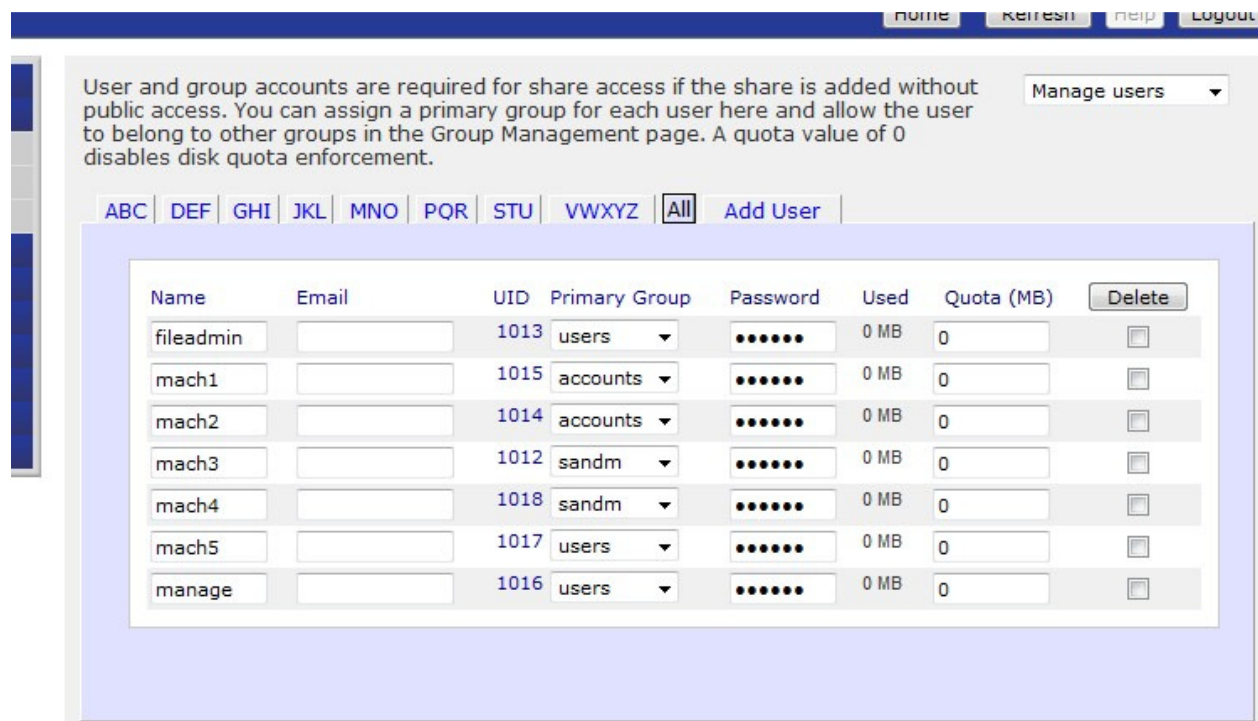


Figure 1815. All Users

So , that hasn't been too hard so far has it...? We have set up the Shares, the Groups, and the Users. And of course all that would have been pretty useless if there wasn't some sort of relationship between them. And that's what we are going to set up now. This relationship is called "permissions". My own definition of permissions is a simple one: "Parameters set to control the ability of users to change files".

If you're wondering why I'm taking so much time to explain all this, it's simply because if you don't understand (even a little bit) and follow closely the next part of the instructions there is a high chance you can create and unmitigated mess of un accessible shares and files. Which I'm sure is not going to do much to benefit your frustration levels. If you can keep in mind that the next step is all about controlling "who can access what" then you should be OK. However you need to remember that you're also controlling who CAN'T access what.

If you have got this far by the skin of your teeth and are totally confused by what you have just read.....the kindest thing I can suggest is for you to blame me for writing a crap manual, stop working on your NAS, and hand the job over to a professional. If you're leaving this manual now.....well "thanks for coming" and I hope you'll have a coffee with me one day, if you're going to stick it out and stay with me.... Then "thanks for coming" and you OWE me a coffee. ☺

Step 4. [Set up Share Permissions.](#)

To begin setting file permissions navigate to the “Share listing” page.(Shares > Share Listing). Then click on the CIFS link next to the share that you need to edit.

NETGEAR Connect with Innovation™ **ReadyNAS NV+**




























Share List Add Shares

Shares Home Refresh Help Logout








Network
Security
Services
Volumes
Shares
Share Listing
Add Shares
Backup
Printers
System
Status

Shares on RAID Volumes

Click on the access icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. For instruction on how to access the shares, click Help.

Share Name	Description	CIFS	HTTP/S	Delete
abctrading	Company Share			
accounts	Accounts Share			
machine1	Private directory for ma			
machine2	Private directory for ma			
machine3	Private directory for ma			
machine4	Private directory for ma			
machine5	Private directory for ma			
public	Public Share			
salesmarketir	Sales and Marketing Shi			

Switch to Wizard Mode Apply

Sat Nov 21 13:19:34 2009 Volume:  Disk:    Fan:  Temp:  UPS: 

Copyright © 1996-2009 NETGEAR ®

You should see a page similar to below.

Display Share List

CIFS HTTP/S Advanced Options

Share Name: abctrading Default Access: Read/write

Share Access Restrictions

Share access for the file protocol can be restricted using the access list(s) below.

Separate entries with comma








☐ Hosts allowed access:

☐ Read-only users:

Read-only groups:

☐ Write-enabled users:

de Apply

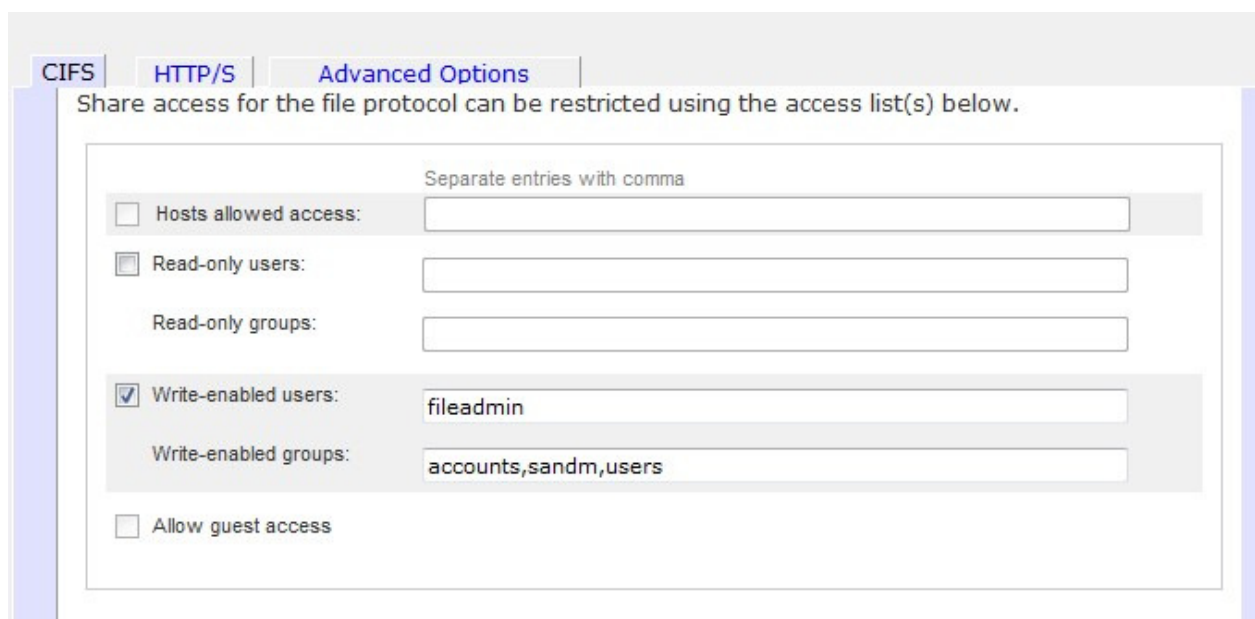
11:37 2009 Volume:  Disk:    Fan:  Temp:  UPS: 

On the right you will see a scroll bar. Before we do any editing ill run through what I know about each feature.

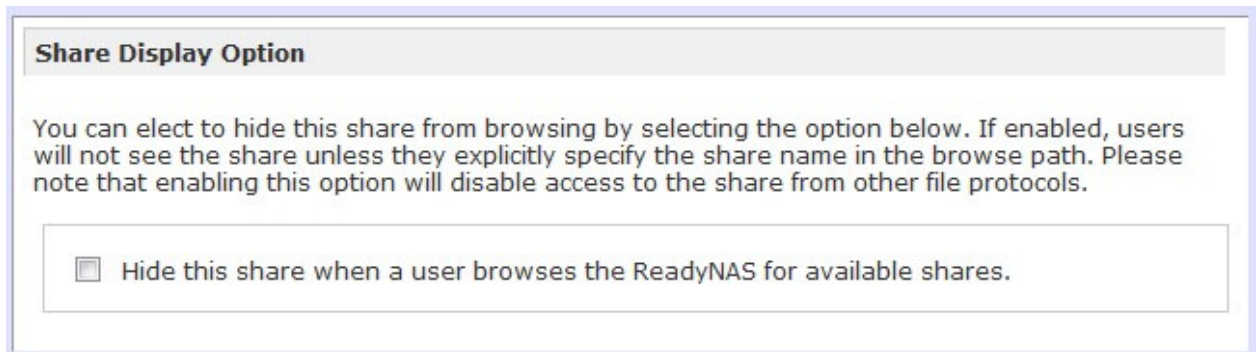
At the top you can see the name of the share you are editing. Beside that is the default access. From factory this is set to “read/write”. This means that any users that are listed to have access to this share can edit save cut and paste, basically full access to all the files on the share. To successfully control users we will set this to “disabled”. (see below)



Next is the “**Share Access Restrictions**” panel. It is here that you can list the users and/or groups that can access this share. The first method of allowing access is by “hostname” (actually IP addresses work here as well). Here you can list the machine names that will be granted access to this share. I’m not going to describe how to use this part here. The next line is labeled “Read-Only Users/groups”. Pretty self explanatory, any users that you want to have “read only” access to the share you can list in here. I don’t use this option to often. The last lines; “Write enabled users/groups” is where you will be doing most of your editing. Here is where you list the users/group that are to have full access to that particular share. In the shot below you can see that rather than adding each user individually (this share is one that we want all but visitors or “guests” to access) I have added the three groups which encompasses all the users. I have also added “fileadmin” in the users list. This is only for peace of mind, in case something happens to the group listings..... (I don’t know enough about the guts of these things to say if it actually helps but it makes me feel better... ☺) The last box, “Allow Guest Access” is a fairly critical one.....unless you want these files available to all and sundry make sure this box is UNTICKED.....!



Scrolling down you will see the **“Share Display Option”** panel. This allows you to hide the share from users when they are browsing the network. Unless you have reason to hide the share (and I mean good reason) leave this one **UNTICKED**.

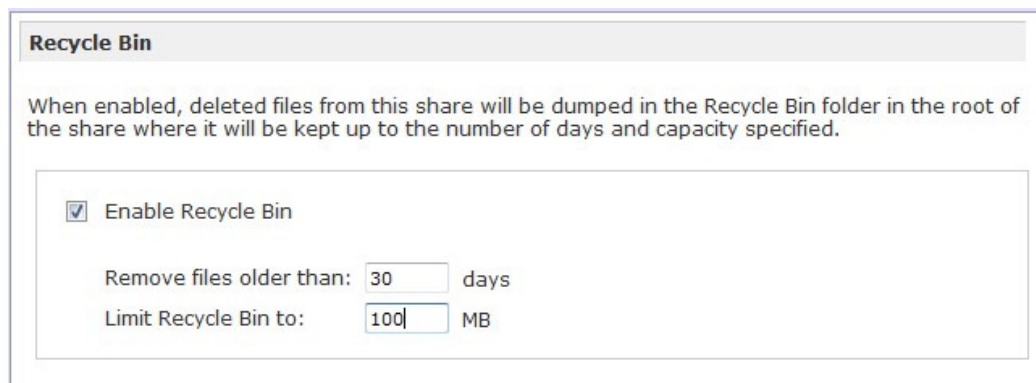


Share Display Option

You can elect to hide this share from browsing by selecting the option below. If enabled, users will not see the share unless they explicitly specify the share name in the browse path. Please note that enabling this option will disable access to the share from other file protocols.

☐ Hide this share when a user browses the ReadyNAS for available shares.

Next is the **“Recycle Bin”**. Personally I like this idea, mainly because if you delete something from a network location, that’s it..., you’ll never see it again. So enabling the recycle bin on some or all shares is not such a bad idea. How much space you give it and when it clears out old files depends on a combination of the size of the NAS and personal preference.



Recycle Bin

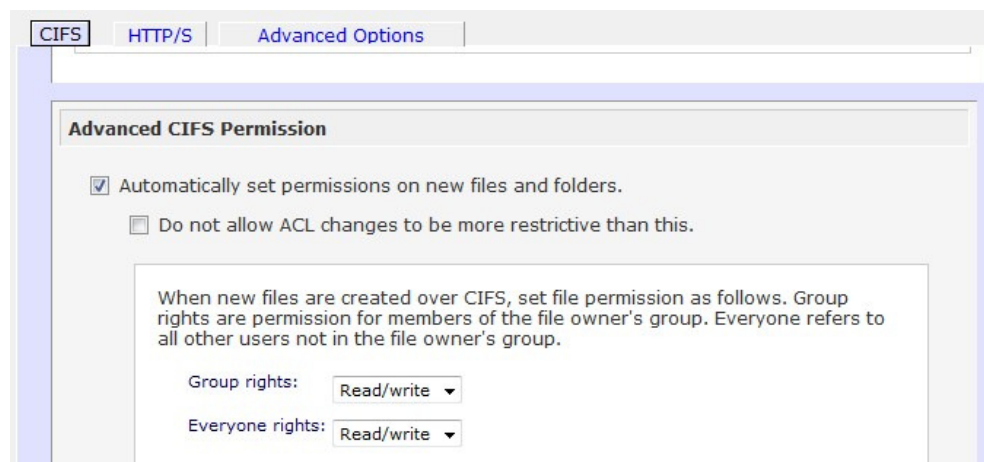
When enabled, deleted files from this share will be dumped in the Recycle Bin folder in the root of the share where it will be kept up to the number of days and capacity specified.

☒ Enable Recycle Bin

Remove files older than: days

Limit Recycle Bin to: MB

“Advanced CFIS Permissions” automatically sets permissions on new files and folders. It is critical you tick this option as pictured below, and ensure that both Group and Everyone permissions are set to **“read/write”** for new file AND folders.



CIFS | HTTP/S | Advanced Options

Advanced CIFS Permission

☒ Automatically set permissions on new files and folders.

☐ Do not allow ACL changes to be more restrictive than this.

When new files are created over CIFS, set file permission as follows. Group rights are permission for members of the file owner's group. Everyone refers to all other users not in the file owner's group.

Group rights:

Everyone rights:

“Opportunistic Locking”I personally am not a fan but it’s your choice. I guess I’d be going against the grain if I was to encourage turning off something that is supposed to enhance performance so here it is left on ☺.

Opportunistic Locking

Opportunistic locking (oplocks) can enhance CIFS performance by allowing files residing on this ReadyNAS to be cached locally on the Windows client, eliminating network latency when files are repeatedly accessed.

☒ Enable oplocks for this share.

And now.....after double checking your settings.....click apply, click apply, click apply.....
“APPLY”get the message...? You should get a number of pop up messages telling you all is ok.....or NOT. If you get any errors double check the spelling of your user names and groups as that is the most frequent cause of problems.

Once you have done one share.....they are all the same. The only thing that varies is the “Share Access Restrictions” panel. And what to add in there can be pretty easily determined from your chart that you drew up earlier. Just to help clarify, below is a chart of the settings that you would user for each share in our example of ABC Company.

Share Name	ABC Company Share Resrictions	
	Write Enabled Groups	Write Enabled Users
abctrading	accounts,sandm	fileadmin
accounts	accounts	fileadmin
machine1	n/a	mach1,fileadmin,manage
machine2	n/a	mach2,fileadmin,manage
machine3	n/a	mach3,fileadmin,manage
machine4	n/a	mach4,fileadmin,manage
machine5	n/a	mach5,fileadmin,manage
public	n/a make sure guest access is allowed	n/a make sure guest access is allowed
salesandma	sandm	fileadmin

Now all that remains is for you to test the shares and their security and then the ReadyNAS is ready for use.....!!!

Notes

The show isn't over till the fat lady sings.....and I guess that applies to home baked IT manuals as well..... ☺

At the start of this document I mentioned a way of avoiding copying all your data if you are modifying the set up of an existing NAS. And I'll try to explain it as best I can. In a scenario where you are setting up new shares with new permissions and want to copy the data from an entire share with one set of permissions to another share with another set, you can use the backup facility built into the NAS. I'm not going to describe that in great length here but with a bit of time and not too much effort it can be done.

The other scenario where you just want to change the permissions of the contents of an existing share after changing the security mode of the NAS from "share" to "user" you can use this little trick. On the "advanced options" tab of the CFIS control on a share you will see an "advanced share permissions" heading. Scroll down a little way and tick the box that says "Set ownership and permission for existing files and folders in this share to the above settings. This option is useful in cases where you are changing security levels and need to workaround file access problems." Then click APPLY. This should make life easier for you.

The pictures and instructions were written based on a number of different Models of ReadyNAS but you should find that largely the instructions are the same.

I guess all there is left to say is if this manual wasn't helpful then I'm sorry.... ☹. However I'm open to suggestions on how to improve and you can email me on windowsseven@lavabit.com with any suggestions and questions you may think I can answer....(as they always say I'm most likely not going to reply..... But that's life...☺)

Thanks for coming.....

Bert