Windows ACL Configuration

Best Practice Guide

March 2020

NOTICES

The information contained in this manual has been reviewed for accuracy. But it could include typographical errors or technical inaccuracies. Changes are made to the document periodically. These changes will be incorporated in new editions of the publication. QSAN may make improvements or changes in the products. All features, functionality, and product specifications are subject to change without prior notice or obligation. All statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products.

All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

PREFACE

About This Guide

This best practice guide provides technical guidance for assigning/modifying the permission when using QSAN products which provides CIFS service, and it is intended for use by system administrators, SAN/NAS designers, storage consultants, or anyone who has purchased these products and is familiar with server and computer network, network administration, storage system installation and configuration, network attached storage management, and relevant protocols.

CAUTION:
Do NOT attempt to service, change, disassemble or upgrade the equipment's components by yourself. Doing so may violate your warranty and expose you to electric shock. Refer all servicing to authorized service personnel. Please always follow the instructions in this owner's manual.

Information, Tip and Caution

This manual uses the following symbols to draw attention to important safety and operational information.

INFORMATION:
INFORMATION provides useful knowledge, definition, or terminology for reference.

TIP:
TIP provides helpful suggestions for performing tasks more effectively.

CAUTION:
CAUTION indicates that failure to take a specified action could result in damage to the system.

TABLE OF CONTENT

1 OVERVIEW

1.1 Audience

This document is applicable for those technical members who are familiar with QSAN products, and for those who are good at network trouble shooting, Windows Server and Unix-Like OS operations, and basic hardware installations.

Please read this document carefully before trying to adjust any parameter on server side. Doing an adjustment with wrong understanding may lead you to get a worse performance experience than ever. If you have any questions about the adjustment, please consult QSAN Technical Support for further assistance.

1.2 What is Windows ACL

Windows ACL is using 13 kinds of detailed permissions designed for the NTFS file system from Microsoft. The application object can be a specific user or group. Under this structure, the administrator can make more detailed configuration of folder or file access. In the Windows AD domain architecture that has been widely adopted by many enterprises, ACL permissions can be extended to domain users and groups. Regardless of which computer the user uses to log in, as long as the accounts are the same, the permissions rules will be the same. IT staff does not need to make separate rules for permissions control for each server or workstation PC, which can greatly increase management efficiency.

In order to integrate AD domain with QSAN XCubeNAS, QSAN QSM supports the functionality of combining NAS with AD server, QSAN QSM brings you:

1. The function to enable Windows ACL per any folder and sub-folder
2. Fully supported the 13 advanced permissions
3. The ability to preview the final permission from QSM Shared Folder page
4. Supporting domain group and account
5. ACL permission can be applied to CIFS shared folder, AFP, FTP, WebDAV, and Rsync protocol

1.3 When do I need to use Windows ACL

As mentioned in the above section, Windows ACL provides up to 13 permissions for all users and groups in this local and domain (if the NAS has successfully joined AD). If the configuration and the purpose didn’t be planned properly, it may happen that no one can access certain folders or files. Of course, this error situation can be resolved by the admin account to obtain ownership, but the time and labor between the problem and its resolution is also an intangible cost.

QSAN QSM provides the ability to assign simple permission for local/domain account, like Read Only, Read Write, and Deny, if the environment and the usage of the NAS is simple, e.g., sharing data/file quickly for your friends, accessing the data in the shared folder from network folder provided by QSAN XCubeNAS, you don't really need to use Windows ACL permission. In other word, if you were going to implement the XCubeNAS into an enterprise, where there are lots of employees accessing the same shared folder, and there are also lots of files have to have security or special credential before a user can access/log in, QSAN QSM will definitely meets your requirement to deploy Windows ACL permission.

2 CONFIGURATION

2.1 Network and AD Configuration

Please make sure the followings are configured properly based on the environment, you don't need to set each setting to be exactly the same, please try to adjust and find the best ones:

- IP – configure the IP of the management port of the NAS unit properly, make sure that the IP can ping to the AD server and the DNS
- Account – please check the Administrator account of the AD domain, it is necessary to use the account with Administrator permission while trying to join AD from the XCubeNAS
- AD –
  - DNS – make sure the DNS configured on the XCubeNAS is the same one as the AD server
  - Time – it must to adjust the time to be the same (or close) to the AD server on the XCubeNAS system

2.2 How to Enable Windows ACL and Basic Usage

Please follow this Video for trying to set up Windows ACL permission, you may need to firstly check how to create a Shared Folder on XCubeNAS from Here.

INFORMATION:

- Windows ACL and Advanced ACL won't be able to use if Anonymous Access function is enabled on any Shared Folder on the XCubeNAS unit. Enabling Windows ACL or Advanced ACL will disable Anonymous Access function.
- If there is snapshot taken on the Shared Folder already, and the Windows ACL permission is enabled after that, any users assigned with Read + Write permission to this folder won't be able to grant

permission for the taken snapshot. If you were checking the Previous Version of the shared folder from Windows client, there will be a popped-up window telling that the permission is denied, which is normal to see such result.

TIP:

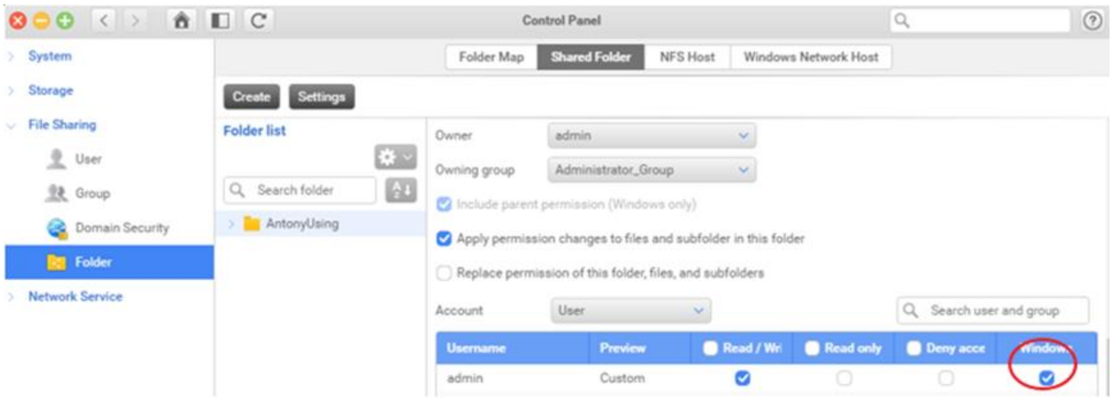
Every sub-folder under the main Shared Folder will be able to assign specific permission with Windows ACL permission after Windows ACL is enabled.

The following Folders do not support Windows ACL: User Home, User Homes, Web, Recycle Bin, Virtual Volume, and USB External Drive.

Windows ACL permission will be able to assign from Windows Client once the Windows ACL function is enabled on the XCubeNAS.

2.3 The 13 Permissions of Windows ACL

QSAN follows the standard definition of Windows ACL policy, to provide the 13 permissions that user may check from below location on the XCubeNAS' web UI:



Owner: admin

Owning group: Administrator_Group

☑ Include parent permission (Windows only)

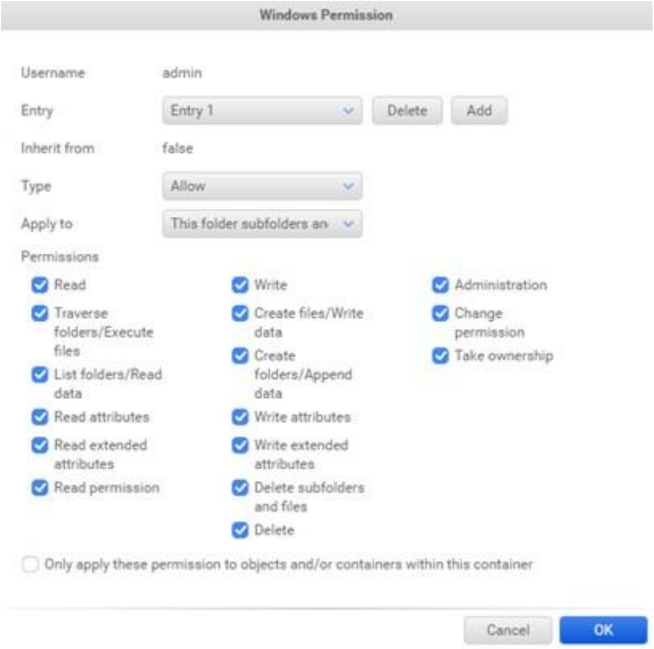
☑ Apply permission changes to files and subfolder in this folder

□ Replace permission of this folder, files, and subfolders

Account: User

Search user and group

Username	Preview	Read / Wri	Read only	Deny acce	Window
admin	Custom	☑	□	□	☑



Windows Permission

Username: admin

Entry: Entry 1 | Delete | Add

Inherit from: false

Type: Allow

Apply to: This folder subfolders an

Permissions

☑ Read	☑ Write	☑ Administration
☑ Traverse folders/Execute files	☑ Create files/Write data	☑ Change permission
☑ List folders/Read data	☑ Create folders/Append data	☑ Take ownership
☑ Read attributes	☑ Write attributes	
☑ Read extended attributes	☑ Write extended attributes	
☑ Read permission	☑ Delete subfolders and files	
	☑ Delete	

□ Only apply these permission to objects and/or containers within this container

- Entry: The maximum Entry is 250, and if the permissions assigned for this Shared Folder are contradictory, the final permission will follow this policy - ***Deny > Read + Write > Read Only > Inherit > None*** - so, if there are multiple entries, or, if there are Group permission plus Account permission, the above priority will be helpful to determine the final result.
- Inherit: If the current folder you are trying to assign the permission is a sub-folder under the main folder (the First-Layer Shared Folder you have created), this value could be true, which means the permission on this sub-folder will be inherited from the main folder if there is no additional explicit permission for this sub-folder.

TIP:

Every sub-folder under the main Shared Folder will be able to assign specific permission with Windows ACL permission after Windows ACL is enabled.

The following Folders do not support Windows ACL: User Home, User Homes, Web, Recycle Bin, Virtual Volume, and USB External Drive.

Windows ACL permission will be able to assign from Windows Client once the Windows ACL function is enabled on the XCubeNAS.

- Apply to: From the drop-down menu, you can select where the permission will be applied. The way in which the permission will be applied will be determined by whether or not you select the “Only apply these permissions to objects and/or containers within this container” checkbox. As there are lots of combination, we will explain the details via the list below.

If **“Only apply these permissions to objects and/or containers within this container”** is unchecked (default):

	TO CURRENT FOLDER	TO SUB-FOLDERS WITHIN THE CURRENT FOLDER	TO FILES WITHIN THE CURRENT FOLDER	TO ALL SUBSEQUENT SUB-FOLDERS	TO FILES WITHIN ALL SUBSEQUENT SUB-FOLDERS
Files only			V		V
Subfolders only		V		V	
Subfolders and files only		V	V	V	V
This folder only	V				
This folder and files	V		V		
This folder and subfolders	V	V		V	
This folder subfolders and files (default)	V	V	V	V	V

If **“Only apply these permissions to objects and/or containers within this container”** is checked:

	TO CURRENT FOLDER	TO SUB-FOLDERS WITHIN THE CURRENT FOLDER	TO FILES WITHIN THE CURRENT FOLDER	TO ALL SUBSEQUENT SUB-FOLDERS	TO FILES WITHIN ALL SUBSEQUENT SUB-FOLDERS
Files only			V		
Subfolders only		V			
Subfolders and files only		V	V		
This folder only	V				
This folder and files	V		V		
This folder and subfolders	V	V			
This folder subfolders and files (default)	V	V	V		

TIP:

The 13 types of Windows ACL permissions are described below:

Traverse folder/execute file: Traverse Folder allows or denies moving through folders to reach other files or folders, even if the user has no permissions for the traversed folders (applies to folders only). Execute File allows or denies running program files (applies to files only).

List folder/read data: List Folder allows or denies viewing file names and subfolder names within the folder (applies to folders only). Read Data allows or denies viewing data in files (applies to files only).

Read attributes: Allows or denies viewing the attributes of a file or folder, such as read-only, hidden, compressed and encrypted.

Read extended attributes: Allows or denies viewing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.

Create files/write data: Create Files allows or denies creating files within the folder (applies to folders only). Write Data allows or denies making changes to the file and overwriting existing content (applies to files only).

Create folders/append data: Create Folders allows or denies creating folders within the folder (applies to folders only). Append Data allows or denies making changes to the end of the file but not changing, deleting, or overwriting existing data (applies to files only).

Write attributes: Allows or denies changing the attributes of a file or folder.

Write extended attributes: Allows or denies changing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.

Delete subfolders and files: Allows or denies deleting subfolders and files, even if the Delete permission has not been granted on the subfolder or file (applies to folders).

Delete: Allows or denies deleting the file or folder.

Read permissions: Allows or denies reading permissions of the file or folder.

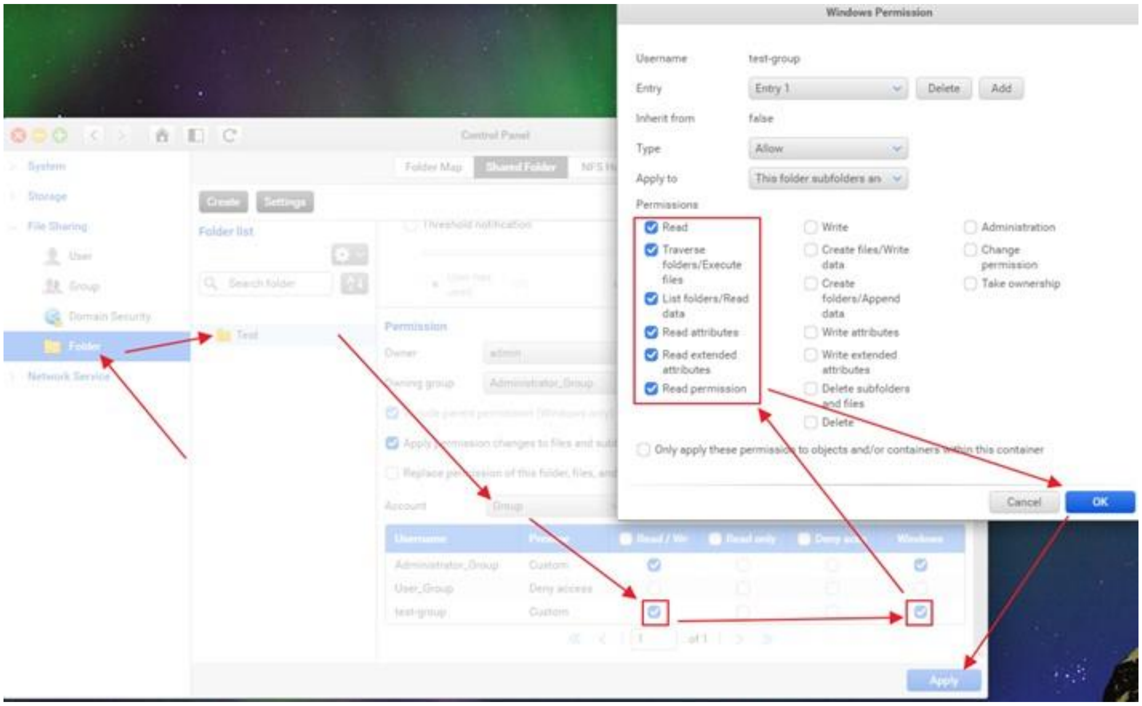
Change permissions: Allows or denies changing permissions of the file or folder.

Take ownership: Allows or denies taking ownership of the file or folder. The owner of a file or folder can always change permissions on it, regardless of any existing permissions that protect the file or folder.

2.4 Suggested Configuration

It is complex to realize the overall spec for the 13 permissions, and most of time there will be only a few permissions/options applied in the production environment. Here comes the recommended configuration for general usage.

1. Create a User Group that includes the User accounts in your XCubeNAS system
2. Visit Shared Folder page, click the folder you would like to assign permission to, change to User Group, make sure the Read + Write permission of the Samba ACL is checked, click the Windows checkbox, make the Permissions to be Read (only), click OK and Apply



Windows Permission

Username test-group
Entry Entry 1 Delete Add
Inherit from false
Type Allow
Apply to This folder subfolders an

Permissions

☑ Read
☑ Traverse folders/Execute files
☑ List folders/Read data
☑ Read attributes
☑ Read extended attributes
☑ Read permission

□ Write
□ Create files/Write data
□ Create folders/Append data
□ Write attributes
□ Write extended attributes
□ Delete subfolders and files
□ Delete

□ Administration
□ Change permission
□ Take ownership

□ Only apply these permission to objects and/or containers within this container

Cancel OK

INFORMATION:

- Windows ACL and Advanced ACL won't be able to use if Anonymous Access function is enabled on any Shared Folder on the XCubeNAS unit. Enabling Windows ACL or Advanced ACL will disable Anonymous Access function.
- If there is snapshot taken on the Shared Folder already, and the Windows ACL permission is enabled after that, any users assigned

with Read + Write permission to this folder won't be able to grant permission for the taken snapshot. If you were checking the Previous Version of the shared folder from Windows client, there will be a popped-up window telling that the permission is denied, which is normal to see such result.

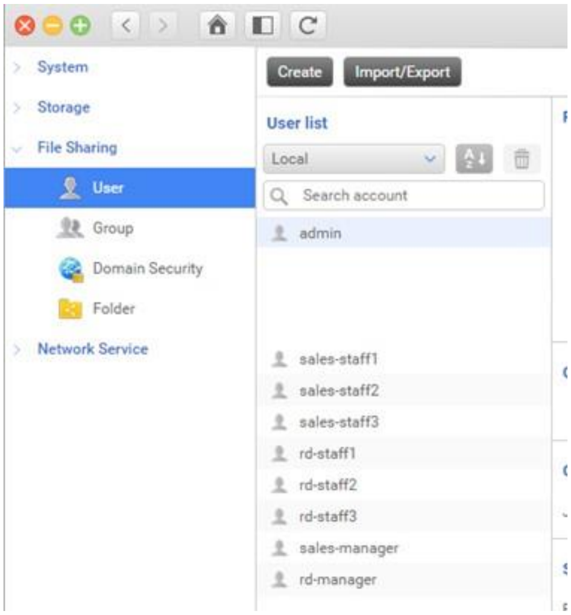
Result: The User accounts that are in this User Group will have Read Only permission for this folder and sub-folders, so everyone can see and read/copy the data in this folder and sub-folders.

3. Remember the Entry Policy mentioned above, Read + Write permission is greater than Read Only, so if you have special User account that requires Read + Write permission (or any higher permission than Read Only), you may change to User account and assign specific User account to have Read + Write permission for this folder (or sub-folder). E.g., the members in the sales Dept. have Read Only + add new file (configured through Windows ACL) permission for the folder-A, but cannot delete or modify the files, and only the supervisor possesses the Read + Write permission for the folder-A to modify or delete the files

3 CASE STUDY

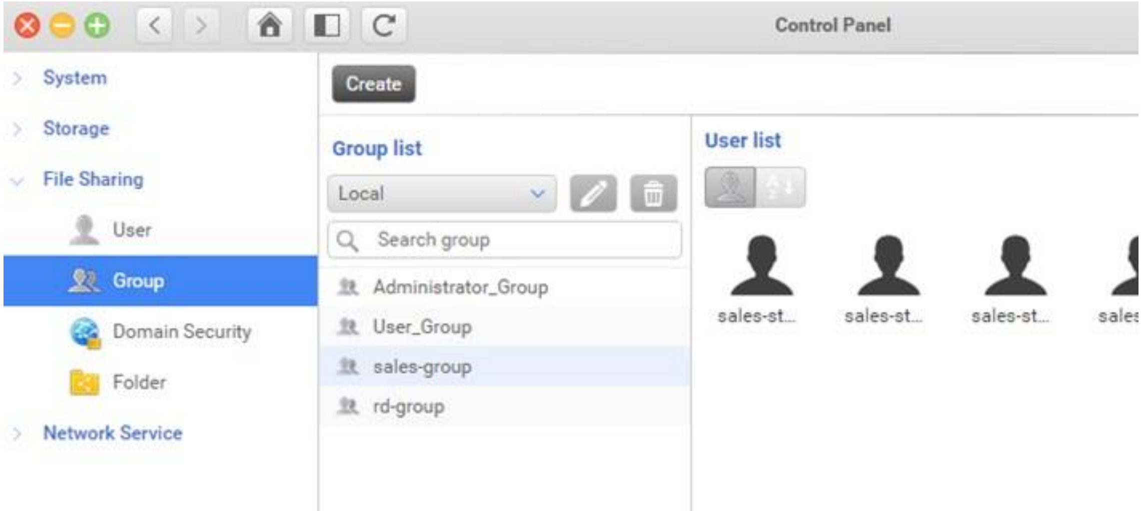
3.1 Case 1 – Allowing Specific User Possessing Read + Write

Presuming that there are two Dept., Sales and RD, and there is one shared folder for each Dept., staffs have permission to add and read the file, but cannot delete or modify, files can only be modified or deleted by the Dept. Manager.



admin
sales-staff1
sales-staff2
sales-staff3
rd-staff1
rd-staff2
rd-staff3
sales-manager
rd-manager

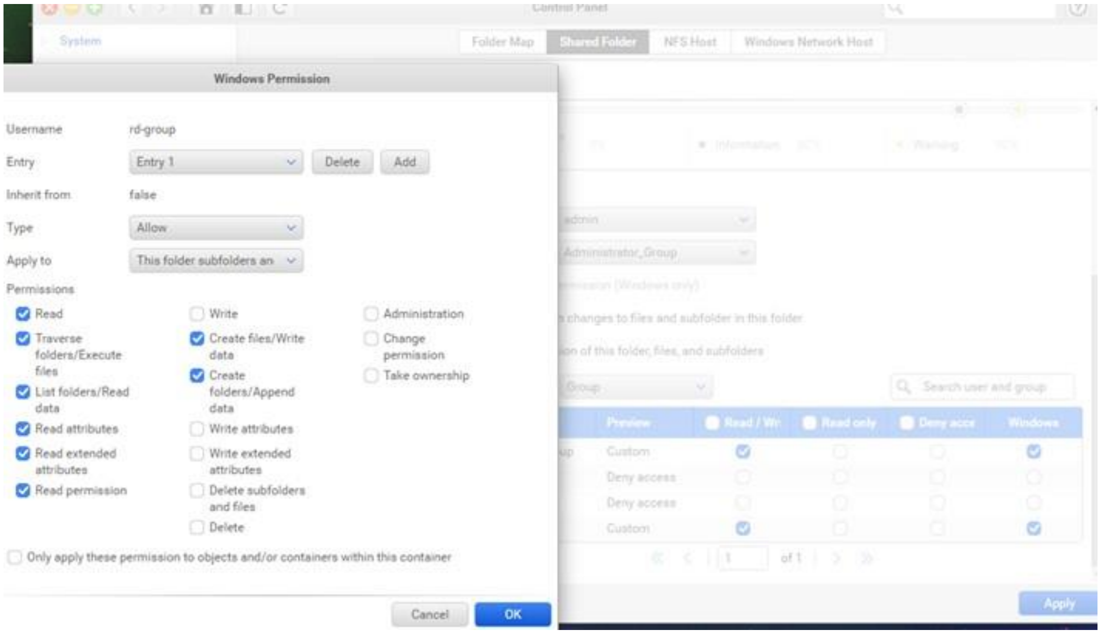
And they are in the corresponding User Group



Administrator_Group
User_Group
sales-group
rd-group

sales-st...
sales-st...
sales-st...
sales

According to the scenario, the User Group permission should be defined like this



Windows Permission

Username: rd-group

Entry: Entry 1 (Delete, Add)

Inherit from: false

Type: Allow

Apply to: This folder subfolders an

Permissions

☑ Read
☑ Traverse folders/Execute files
☑ List folders/Read data
☑ Read attributes
☑ Read extended attributes
☑ Read permission

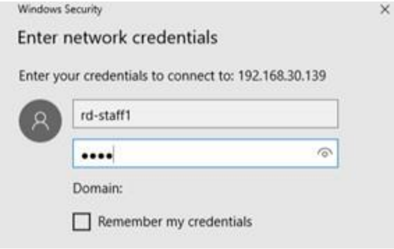
□ Write
☑ Create files/Write data
☑ Create folders/Append data
□ Write attributes
□ Write extended attributes
□ Delete subfolders and files
□ Delete

□ Administration
□ Change permission
□ Take ownership

□ Only apply these permission to objects and/or containers within this container

So that staffs will grant the mentioned permissions, but cannot delete or modify files.

Let’s log in via the created User account



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.30.139

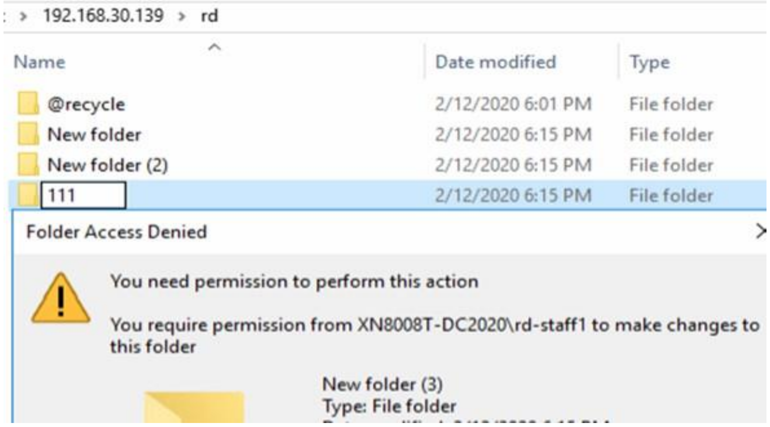
rd-staff1

••••

Domain:

□ Remember my credentials

And verify the permission



> 192.168.30.139 > rd

Name	Date modified	Type
@recycle	2/12/2020 6:01 PM	File folder
New folder	2/12/2020 6:15 PM	File folder
New folder (2)	2/12/2020 6:15 PM	File folder
111	2/12/2020 6:15 PM	File folder

Folder Access Denied

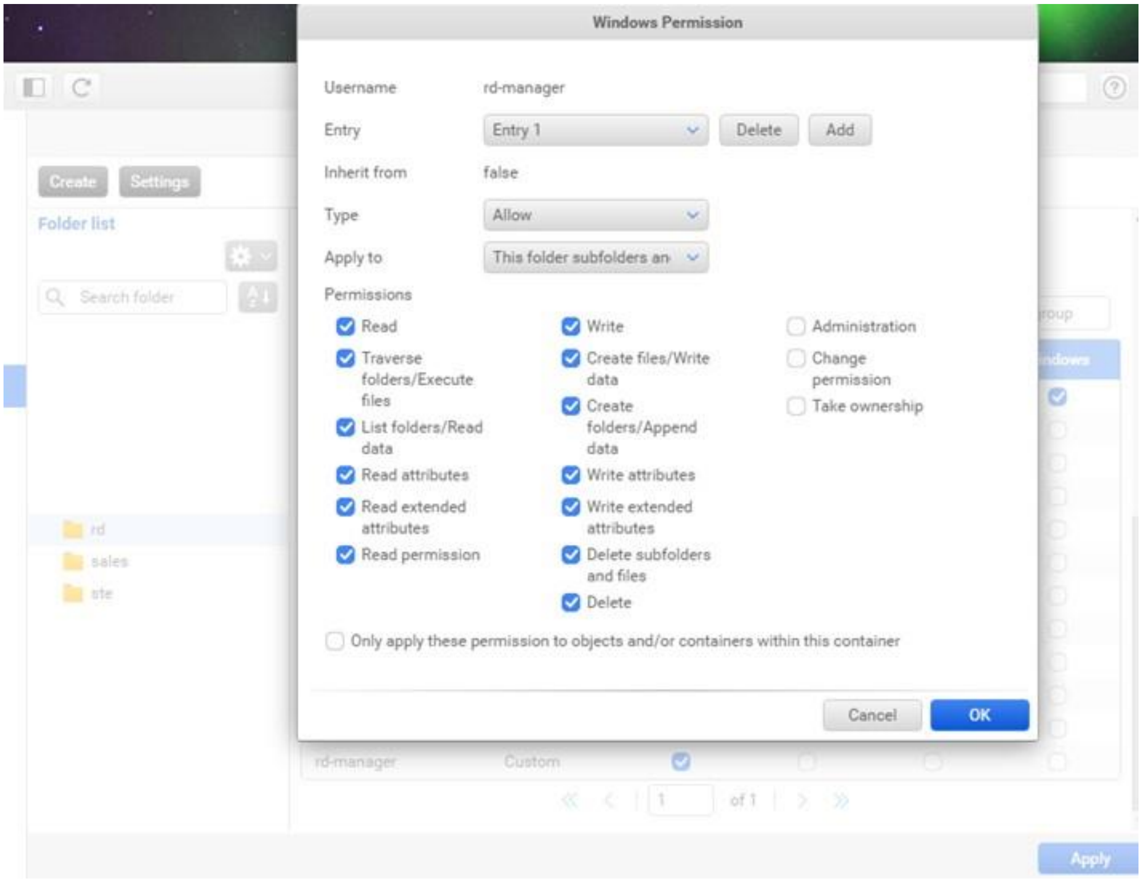
You need permission to perform this action

You require permission from XN8008T-DC2020\rd-staff1 to make changes to this folder

New folder (3)
Type: File folder

Success! This User account can only create and read the file, but cannot delete or modify.

And here we assigned Read + Write permission for Manager account



Windows Permission

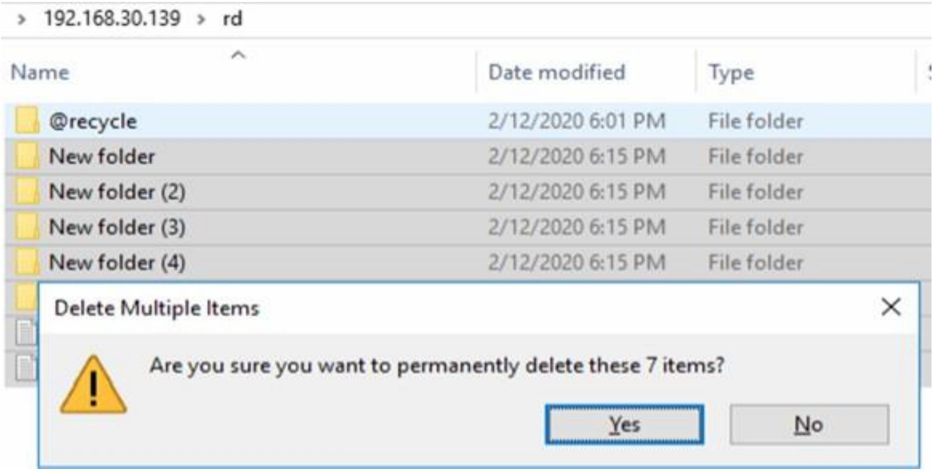
Username	rd-manager
Entry	Entry 1
Inherit from	false
Type	Allow
Apply to	This folder subfolders an

Permissions

- ☑ Read
- ☑ Traverse folders/Execute files
- ☑ List folders/Read data
- ☑ Read attributes
- ☑ Read extended attributes
- ☑ Read permission
- ☑ Write
- ☑ Create files/Write data
- ☑ Create folders/Append data
- ☑ Write attributes
- ☑ Write extended attributes
- ☑ Delete subfolders and files
- ☑ Delete
- □ Administration
- □ Change permission
- □ Take ownership

□ Only apply these permission to objects and/or containers within this container

Trying to delete the created files and folders



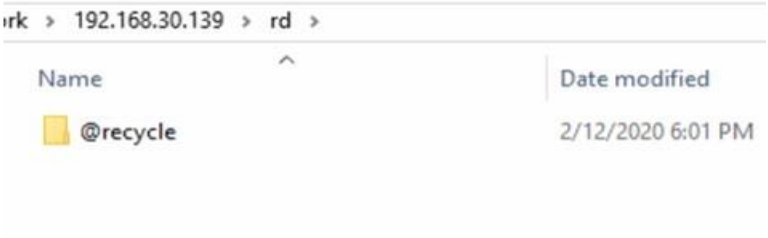
› 192.168.30.139 › rd

Name	Date modified	Type
@recycle	2/12/2020 6:01 PM	File folder
New folder	2/12/2020 6:15 PM	File folder
New folder (2)	2/12/2020 6:15 PM	File folder
New folder (3)	2/12/2020 6:15 PM	File folder
New folder (4)	2/12/2020 6:15 PM	File folder

Delete Multiple Items

Are you sure you want to permanently delete these 7 items?

Success!


ırk > 192.168.30.139 > rd >

Name	Date modified
@recycle	2/12/2020 6:01 PM

3.2 Case 2 – FastCopy to replicate data from Windows to NAS

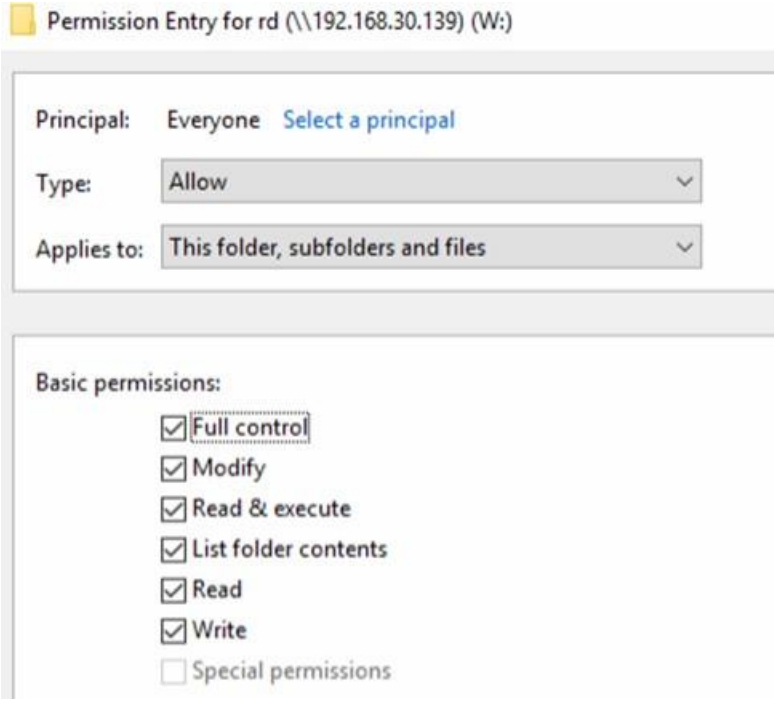
If you are still using Windows with CIFS file sharing in your IT environment, and would like to transform to the architecture of NAS + CIFS, the most important thing is the file transferring with Windows ACL permission attached, here is the easiest way to transfer the files while the environment has AD domain joined.

1. Please make sure that your XCubeNAS is in the same AD domain as your Windows server
2. Please log in QSM of your XCubeNAS, create a Shared Folder that you would like to make as the destination of the backup from Windows Server, remember to assign the correct permission to this Shared Folder, the Read + Write permission must be given
3. Please map the Shared Folder as a Network Drive from your Windows Server, please refer to This video for the detailed operation

INFORMATION:

It is necessary to use the Admin account of QSM to log in the CIFS Shared Folder on the Windows Server.

4. Right-Click on the mapped Shared Folder, and choose Properties -> Security -> Advanced, click “Add” button in the popped-up window, and give Everyone the Full control



Permission Entry for rd (\\192.168.30.139) (W:)

Principal: Everyone Select a principal

Type: Allow

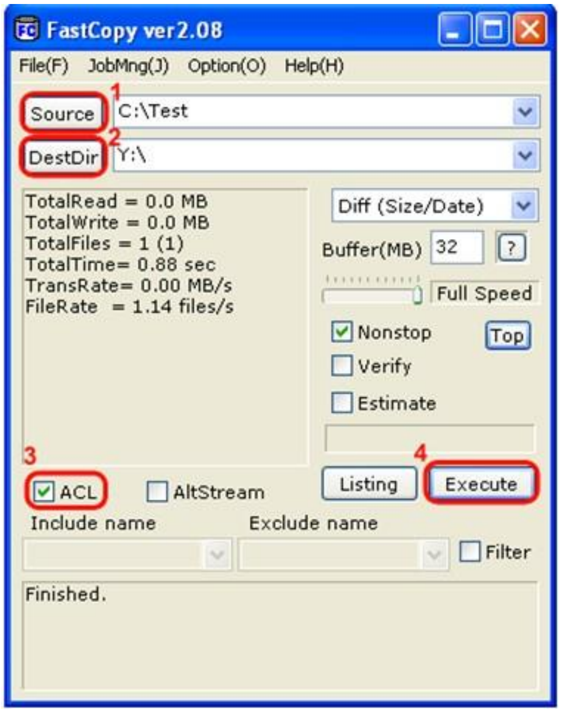
Applies to: This folder, subfolders and files

Basic permissions:

☑ Full control
☑ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☑ Write
□ Special permissions

TIP:
The Everyone permission may need to remove after the files copy is finished, depending on the real usage from customer's environment.

5. Please Download FastCopy from your Windows server, and install it onto the server
6. Execute FastCopy, and follow the steps below to create the copy task



Source C:\Test

DestDir Y:\

```
TotalRead = 0.0 MB
TotalWrite = 0.0 MB
TotalFiles = 1 (1)
TotalTime= 0.88 sec
TransRate= 0.00 MB/s
FileRate  = 1.14 files/s
```

Diff (Size/Date)

Buffer(MB) 32

Full Speed

☑ Nonstop

□ Verify

□ Estimate

☑ ACL

□ AltStream

□ Filter

```
Finished.
```

7. The files will be copied to the destination (the mapped Shared Folder) with the ACL permission attached

INFORMATION:

INFORMATION provides useful knowledge, definition, or terminology for reference.

4 SUPPORT AND OTHER RESOURCES

4.1 Getting Technical Support

After installing your device, locate the serial number on the sticker located on the side of the chassis or register your product at https://qsan.com/en. We recommend registering your product in QSAN website for firmware updates, document download, and latest news in e-blast. To contact QSAN Support, please use the following information.

- Via the Web: https://www.qsan.com/en/contact_support.php
- Via Telephone: +886-2-7720-6355 (Service hours: 09:30 - 18:00, Monday - Friday, UTC+8)
- Via Skype Chat, Skype ID: qsan.support (Service hours: 09:30 - 02:00, Monday - Friday, UTC+8, Summertime: 09:30 - 01:00)
- Via Email: support@qsan.com

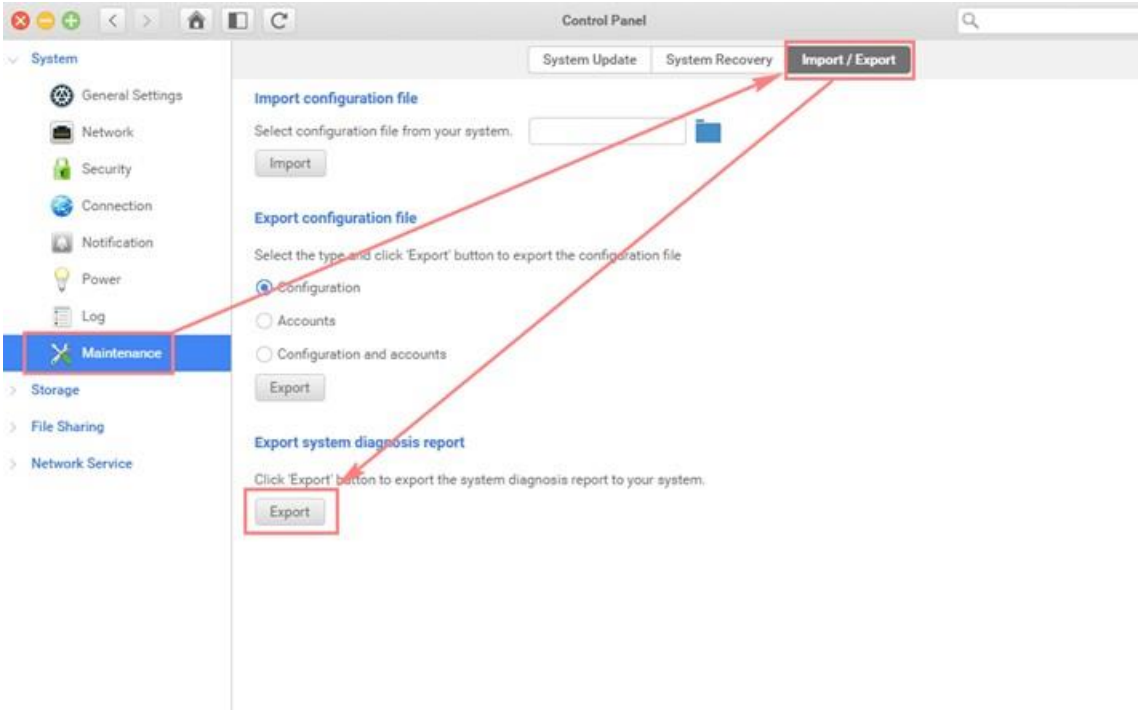
4.1.1 Information to collect

- Product name, model or version, and serial number
- Firmware version
- Error messages or screenshot images
- Product-specific reports and logs
- Add-on products or components installed
- Third-party products or components installed

4.1.2 Information for Technical Support

The following system information is necessary for technical support; please refer to following for what and where to get the information of your XCubeNAS model.

If the technical support requests you to download the service log/debug info, please navigate on the **QSM UI → System → Maintenance → Import/Export**, then click on the "**Export**" button under the Export system diagnosis report for download.



Import configuration file

Select configuration file from your system.

Export configuration file

Select the type and click 'Export' button to export the configuration file

● Configuration

○ Accounts

○ Configuration and accounts

Export system diagnosis report

Click 'Export' button to export the system diagnosis report to your system.

4.2 Documentation Feedback

QSAN is committed to providing documentation that meets and exceeds your expectations. To help us improve the documentation, email any errors, suggestions, or comments to mailto:docsfeedback@qsan.com.

When submitting your feedback, include the document title, part number, revision, and publication date located on the front cover of the document.

ANNOUNCEMENT

Copyright

March 2020

QSAN believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Trademarks

- QSAN, the QSAN logo, XCubeSAN, and QSAN.com are trademarks or registered trademarks of QSAN Technology, Inc.
- Microsoft, Windows, Windows Server, and Hyper-V are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux is a trademark of Linus Torvalds in the United States and/or other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Mac and OS X are trademarks of Apple Inc., registered in the U.S. and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
- VMware, ESXi, and vSphere are registered trademarks or trademarks of VMware, Inc. in the United States and/or other countries.
- Citrix and Xen are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries.
- Other trademarks and trade names used in this document to refer to either the entities claiming the marks and name or their products are the property of their respective owners.

APPENDIX

End-User License Agreement (EULA)

Please read this document carefully before you use our product or open the package containing our product.

YOU AGREE TO ACCEPT TERMS OF THIS EULA BY USING OUR PRODUCT, OPENING THE PACKAGE CONTAINING OUR PRODUCT OR INSTALLING THE SOFTWARE INTO OUR PRODUCT. IF YOU DO NOT AGREE TO TERMS OF THIS EULA, YOU MAY RETURN THE PRODUCT TO THE RESELLER WHERE YOU PURCHASED IT FOR A REFUND IN ACCORDANCE WITH THE RESELLER'S APPLICABLE RETURN POLICY.

General

QSAN Technology, Inc. ("QSAN") is willing to grant you ("User") a license of software, firmware and/or other product sold, manufactured or offered by QSAN ("the Product") pursuant to this EULA.

License Grant

QSAN grants to User a personal, non-exclusive, non-transferable, non-distributable, non- assignable, non-sub-licensable license to install and use the Product pursuant to the terms of this EULA. Any right beyond this EULA will not be granted.

Intellectual Property Right

Intellectual property rights relative to the Product are the property of QSAN or its licensor(s). User will not acquire any intellectual property by this EULA.

License Limitations

User may not, and may not authorize or permit any third party to: (a) use the Product for any purpose other than in connection with the Product or in a manner inconsistent with the design or documentations of the Product; (b) license, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Product or use the Product in any commercial hosted or service bureau environment; (c) reverse engineer, decompile, disassemble or attempt to discover the source code for or any trade secrets related to the Product, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation; (d) adapt, modify, alter, translate or create any derivative works of the Licensed Software; (e) remove, alter or obscure any copyright notice or other proprietary rights notice on the Product; or (f) circumvent or attempt to circumvent any methods employed by QSAN to control access to the components, features or functions of the Product.

Disclaimer

QSAN DISCLAIMS ALL WARRANTIES OF PRODUCT, INCLUDING BUT NOT LIMITED TO ANY MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, TITLE, AND NON-INFRINGEMENT. ALL PRODUCTS ARE PROVIDE "AS IS" WITHOUT WARRANTY OF ANY KIND. QSAN MAKES NO WARRANTY THAT THE PRODUCT WILL BE FREE OF BUGS, ERRORS, VIRUSES OR OTHER DEFECTS.

IN NO EVENT WILL QSAN BE LIABLE FOR THE COST OF COVER OR FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR SIMILAR DAMAGES OR LIABILITIES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO LOSS OF DATA, INFORMATION, REVENUE, PROFIT OR BUSINESS) ARISING OUT OF OR RELATING TO THE USE OR INABILITY TO USE THE PRODUCT OR OTHERWISE UNDER OR IN CONNECTION WITH THIS EULA OR THE PRODUCT, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHER THEORY EVEN IF QSAN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Limitation of Liability

IN ANY CASE, QSAN'S LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS EULA OR THE PRODUCT WILL BE LIMITED TO THE TOTAL AMOUNT ACTUALLY AND ORIGINALLY PAID BY CUSTOMER FOR THE PRODUCT. The foregoing Disclaimer and Limitation of Liability will apply to the maximum extent permitted by applicable law. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the exclusions and limitations set forth above may not apply.

Termination

If User breaches any of its obligations under this EULA, QSAN may terminate this EULA and take remedies available to QSAN immediately.

Miscellaneous

- QSAN reserves the right to modify this EULA.
- QSAN reserves the right to renew the software or firmware anytime.

- QSAN may assign its rights and obligations under this EULA to any third party without condition.
- This EULA will be binding upon and will inure to User's successors and permitted assigns.
- This EULA shall be governed by and constructed according to the laws of R.O.C. Any disputes arising from or in connection with this EULA, User agree to submit to the jurisdiction of Taiwan Shilin district court as first instance trial.

Technical Support

- Do you have any questions or need help troubleshooting a problem? Please contact QSAN Support, we will reply to you as soon as possible.
- Via the Web: https://www.qsan.com/en/contact_support.php
- Via Telephone: +886-2-7720-6355 (Service hours: 09:30 - 18:00, Monday - Friday, UTC+8)
- Via Skype Chat, Skype ID: qsan.support (Service hours: 09:30 - 02:00, Monday - Friday, UTC+8, Summertime: 09:30 - 01:00)
- Via Email: support@qsan.com