NAS 471
Introduction to Windows ACL

Use Windows ACL to manage
your access permissions

ASUSTOR COLLEGE

asustor

COURSE OBJECTIVES

Upon completion of this course you should be able to:

1. Understand the basic principles of using Windows ACL with your ASUSTOR NAS
2. Use Windows ACL to manage data access permissions on your ASUSTOR NAS

PREREQUISITES

Course Prerequisites:
NAS 106: Using NAS with Microsoft Windows

Students are expected to have a working knowledge of:
ASUSTOR NAS installation and initialization
Creating storage volumes and shared folders
Creating local users and groups in ADM

OUTLINE

1. Introduction to Windows ACL

1.1 What is Windows ACL?

Windows ACL is the 13 different types of file permissions designed by Microsoft for NTFS file systems which can be applied to specific users and groups. Within this type of infrastructure, administrators can make more detailed and precise access permission configurations

Furthermore, in the Windows AD domain infrastructure (widely used by businesses), Windows ACL permissions can be applied to all users and groups in the domain. Users can use any computer in the network to log in, and as long as they use the same account name, all permissions will remain the same. IT staff will not need to configure permissions for each individual server and PC workstation, significantly increasing management efficiency.

In order to more closely integrate ASUSTOR NAS with AD domains, simplifying IT management and increasing productivity, ASUSTOR has deeply integrated the Windows ACL permissions system with ADM, providing the following unique features:

1. The ability to enable Windows ACL for individual shared folders
2. Comprehensive support for all 13 types of Windows ACL permissions
3. Ability to view Windows ACL effective permissions in detail from within ADM
4. Support for network users and groups
5. Ability to apply ACL permissions to Samba, File Explorer, AFP, FTP, WebDAV, Rsync file transfer protocols

1.2 Do I need to enable Windows ACL?

As described in the previous section, Windows ACL provides up to 13 different permission settings that can be applied to all users and groups on the NAS and on the domain (if the NAS has been added to a Windows AD domain). In the event of improper planning or configuration of permissions, there is the possibility that all users will not be able to access a certain folder or file. Obviously, this type of error can be resolved by using an administrator account, but the amount of wasted time from when the problem first occurs to when it gets resolved can be seen as a significant intangible cost to businesses.

ASUSTOR NAS was developed based on the Linux operating system, so ADM's native settings utilize the Linux permission management mechanism:

Applicable permissions: RW (Read & Write), RO (Read Only), DA (Deny Access)

Permissions may be applied to: "Owner", the group that the owner is a part of and "Other".

The smaller number of options allows for simpler configuration. However, the flexibility and adjustability of the permissions is very limited. For example, when using the Linux permissions mechanism, it is not possible to give a user the ability to edit a file while not giving them permission to delete the file.

If you are only using your NAS between yourself and a limited number of family and friends, then it is recommended that you use ADM's original permissions management mechanism. However, if your NAS is being used for business data storage, it is suggested you first consult with your IT staff to decide if it is appropriate to enable Windows ACL permissions and then complete a permissions deployment plan should you decide to use it.

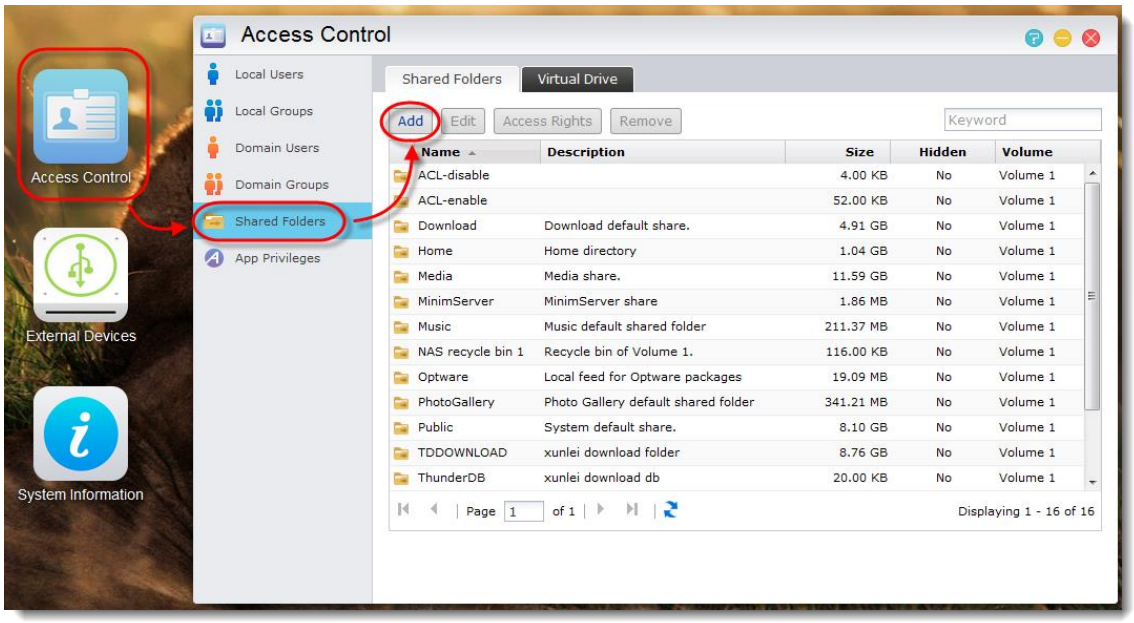
We have provided the flexibility for you to enable or disable Windows ACL for single shared folders, which is very helpful for assessment and planning. You can create a shared folder for testing, enable Windows ACL and then configure permissions settings. Afterwards you can check if the results are what you expected them to be. Once you get the results that you require you can then apply the settings to the shared folder of your choice. This allows you to avoid any mistakes or errors in planning that could deny access to important data, affecting the operation of your business.

2. Configuring Windows ACL

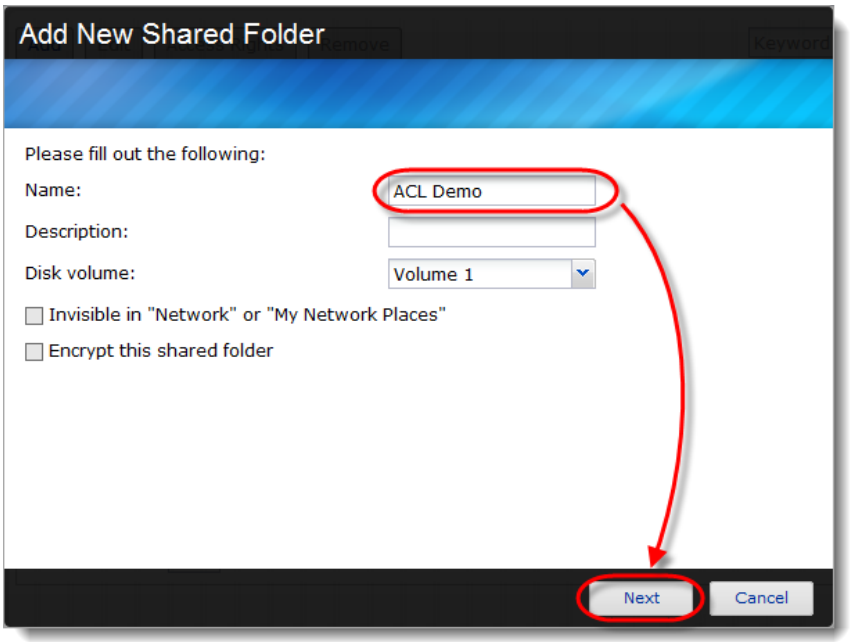
2.1 Enabling Windows ACL

Creating a new shared folder

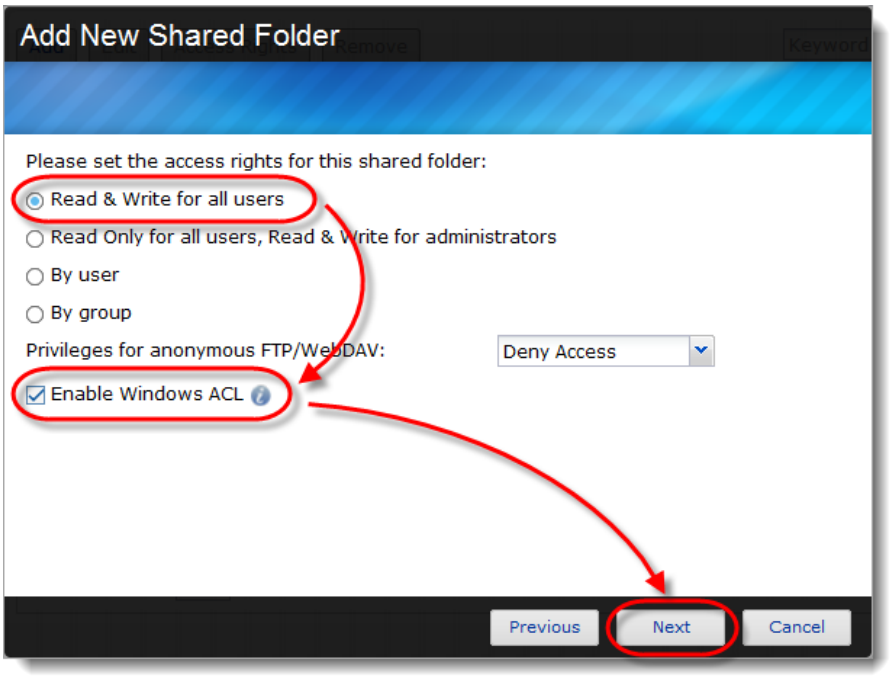
Log into ADM using the “admin” account or a user account belonging the “administrators” group. Select **[Access Control]** → **[Shared Folders]** →**[Add]**.



Enter a name for your new shared folder and then click on **[Next]**.

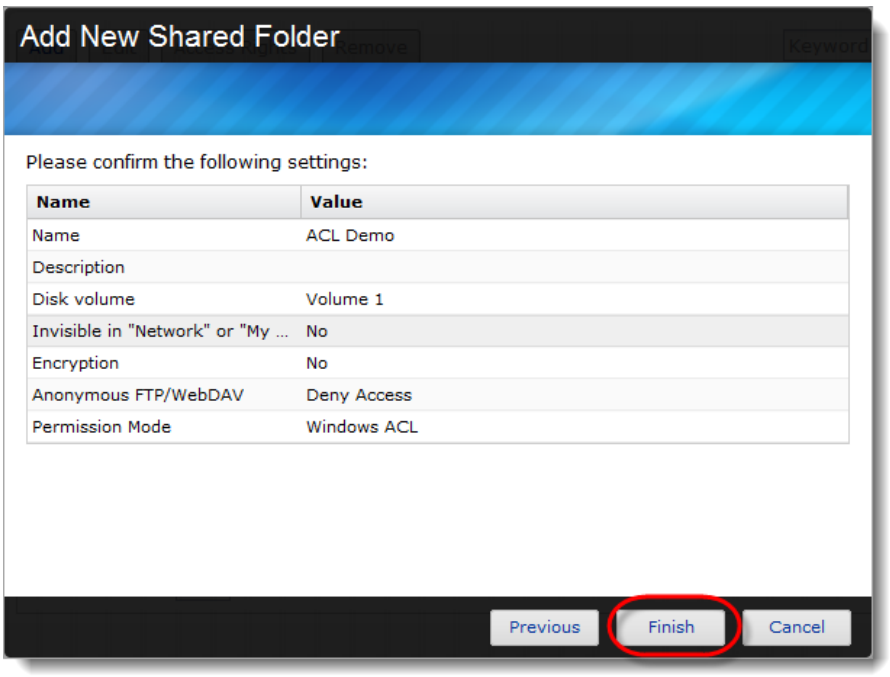


After setting the access rights for the shared folder, select the **[Enable Windows ACL]** checkbox and then click on **[Next]**.



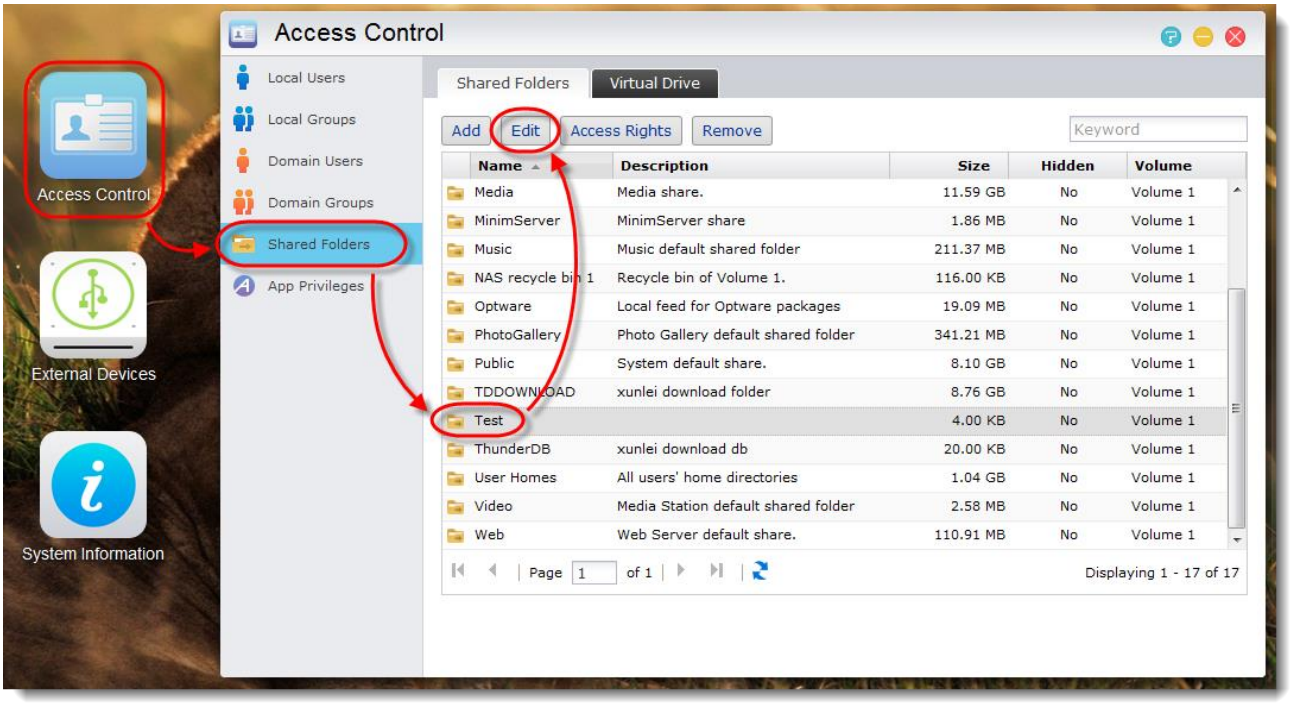
***Note**: Shared folder access rights are the first layer of permissions checking. If a user or group has not been assigned "Read & Write" permissions here, any Windows ACL permissions assigned to them will be blocked. Therefore, it is recommended that you configure more lenient access rights for shared folders that have Windows ACL enabled and then use Windows ACL to further configure more specific permissions later.*

Click on **[Finish]** to complete the creation of the shared folder.

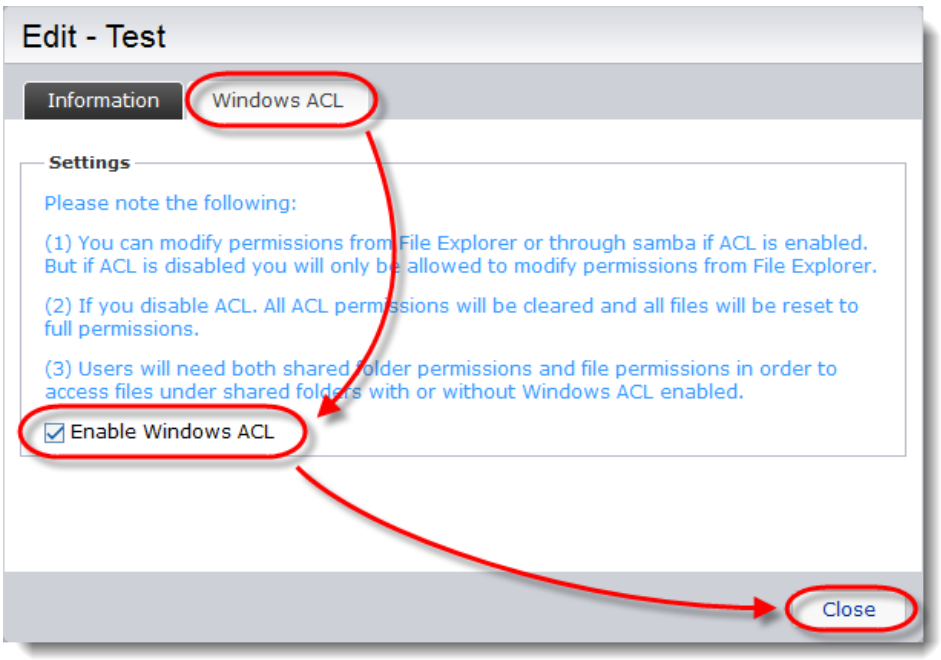


Enabling Windows ACL for already existing shared folders

Log into ADM using the "admin" account or a user account belonging the "administrators" group. Select **[Access Control]** → **[Shared Folders]** → **[*The shared folder that you wish to enable Windows ACL for*]**→**[Edit]**.



Select the **[Windows ACL]** tab, select the **[Enable Windows ACL]** checkbox and then click on **[Close]**.



About Windows ACL

1. After enabling Windows ACL for a shared folder, the shared folder and all subfolders and files contained within it can be assigned user or group permissions.

2. The following shared folders do not support Windows ACL permissions: Home, User Homes, PhotoGallery, Web, Surveillance, MyArchive, Network Recycle Bin, virtual devices, external devices (USB hard drives, optical drives).

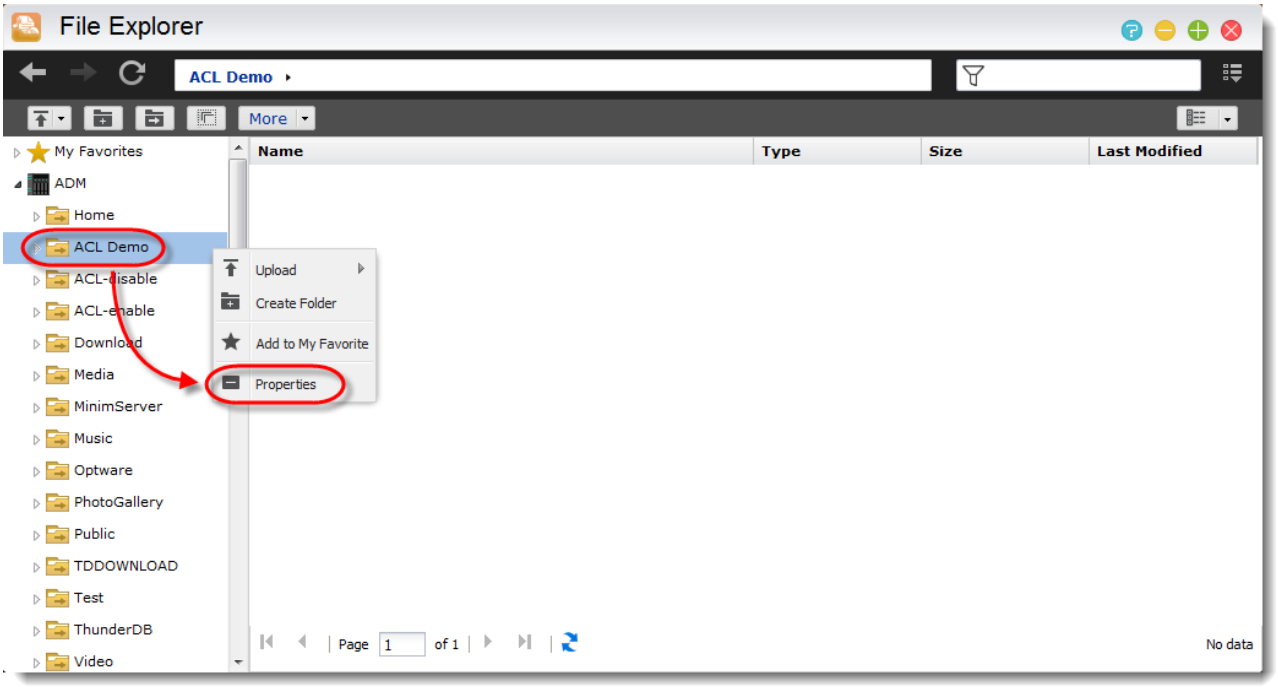
3. After enabling Windows ACL you will be able to use ADM's File Explorer or Microsoft Windows Explorer to configure permissions. After disabling Windows ACL you will only be able to configure permissions from within ADM's File Explorer.

4. If you enable Windows ACL and then later decide to disable it, all file and folders will be re-assigned with Read & Write permissions for all users.

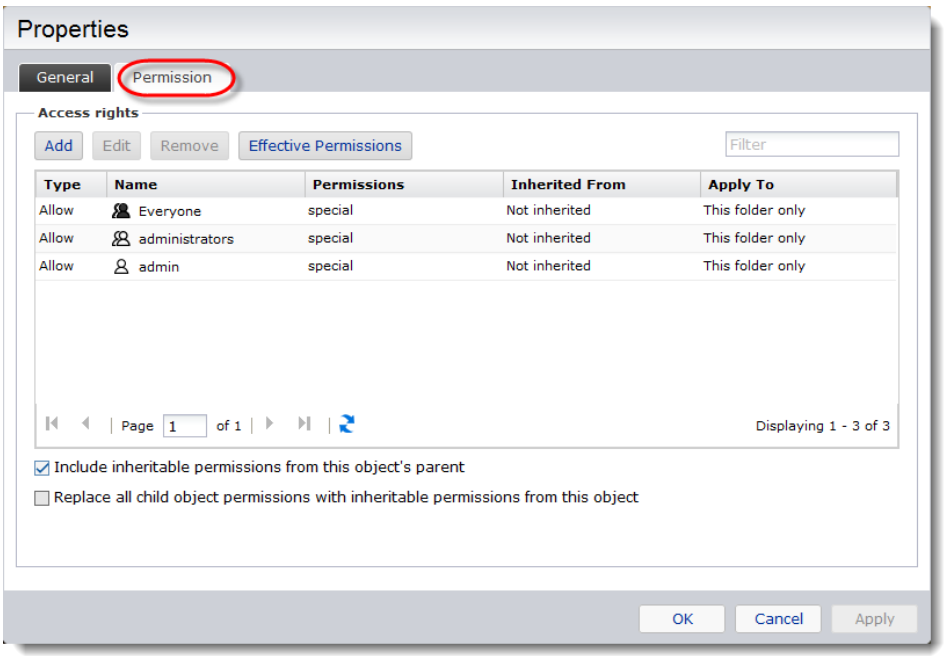
5. No matter if you are using Windows ACL or not, users will still require shared folder and file permissions in order to access files.

2.2 Configuring Windows ACL permissions with ADM File Explorer

From ADM, open File Explorer and then select a shared folder (or subfolder or file) that you have enabled Windows ACL for. Right-click on the shared folder and then select **[Properties]**.



From the properties window, select the **[Permission]** tab. Here you will be able to see the currently configured permissions for the folder. You can also manage permissions for the folder here.



After enabling windows ACL for a shared folder, the system by default will assign “Read & Write, but cannot Delete” permissions to “Everyone”, “administrators” and the “admin” account. These permissions will be applied to the shared folder only and will not be inherited by objects below. These default permissions can be modified by using the [Edit] or [Remove] buttons.

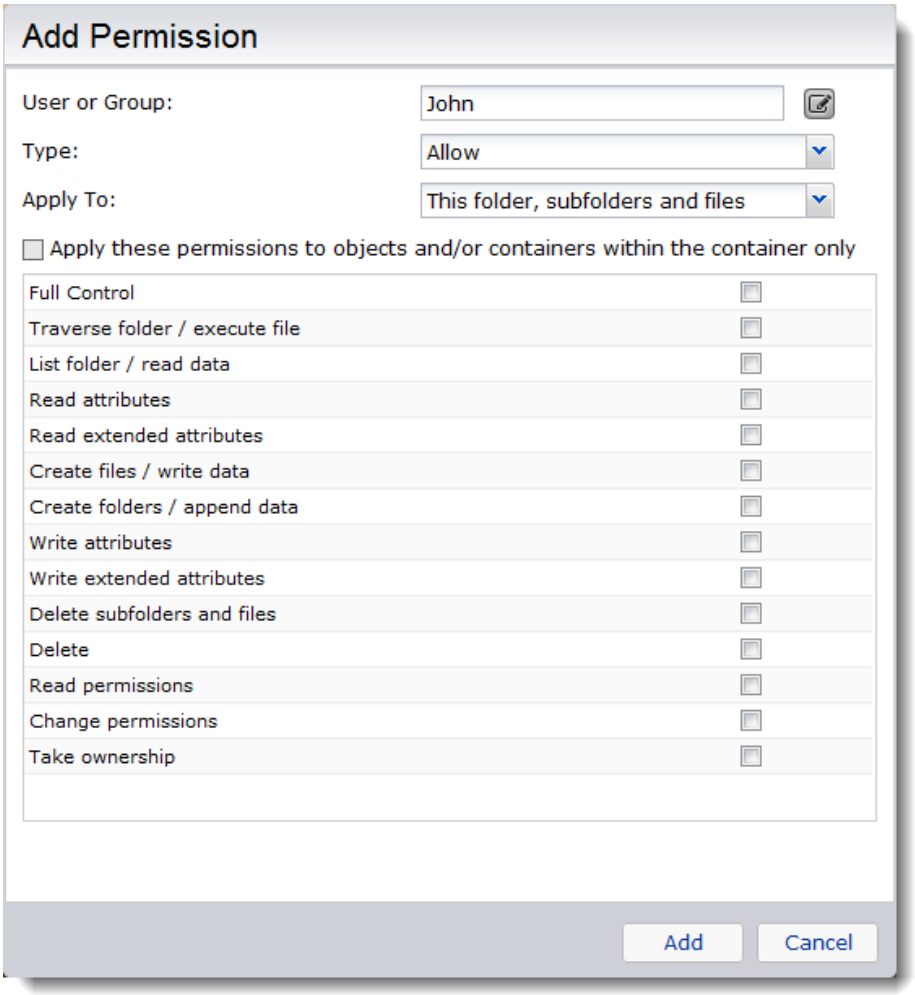
Note: *An individual file or folder can utilize up to a maximum of 250 Windows ACL permissions (including inherited permissions).*

Include inheritable permissions from this object’s parent: This option is enabled by default. The system will automatically configure sub folders and files to inherit permissions from the object above it. Disabling this option will reject all inheritable permissions and only keep newly added permissions.

Replace all child object permissions with inheritable permissions from this object: Enabling this option will replace all subfolder and file permissions with ones from the parent object.

The management functions that you will be able to use here are as follows:

Add
Click on the **[Add]** button to create a new permission for the object.



User or group: specify the user or group you want to apply the permission to.

Type: Select [Allow] or [Deny] to grant or deny the permission to the user or group.

Apply To: This option will only appear when adding permissions to a folder. 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 **[Apply these permissions to objects and/or containers within the container only]** checkbox.

When the **[Apply these permissions to objects and/or containers within the container only]** checkbox is unchecked:

Apply To	Apply permission to current folder	Apply permission to subfolders within the current folder	Apply permission to files within the current folder	Apply permission to all subsequent subfolders	Apply permission to files within all subsequent sub folders
This folder only	V				
This folder, subfolders and files	V	V	V	V	V
This folder and subfolders	V	V		V	
This folder and files	V		V		V
Subfolders and files only		V	V	V	V
Subfolders only		V		V	
Files only			V		V

When the **[Apply these permissions to objects and/or containers within the container only]** checkbox is checked:

Apply To	Apply permission to current folder	Apply permission to subfolders within the current folder	Apply permission to files within the current folder	Apply permission to all subsequent subfolders	Apply permission to files within all subsequent sub folders
This folder only	V				
This folder, subfolders and files	V	V	V		
This folder and subfolders	V	V			
This folder and files	V		V		
Subfolders and files only		V	V		
Subfolders only		V			
Files only			V		

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.

Edit
Selecting a permission and then clicking on the [Edit] button will allow you to modify the permission.

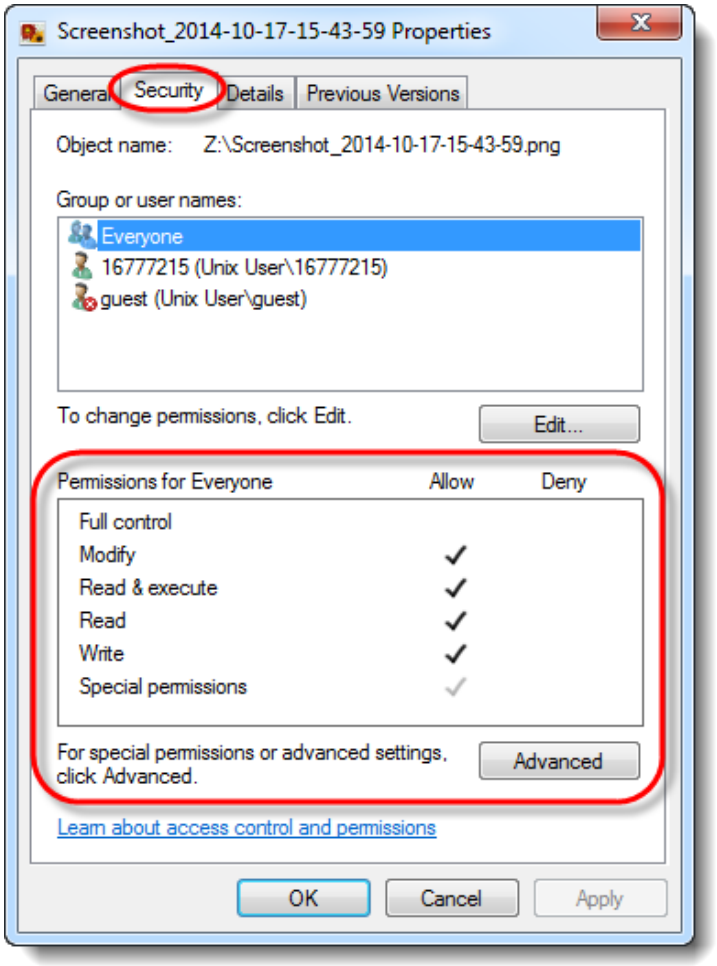
Remove
Selecting a permission and then clicking on [Remove] will remove the permission from the current object.

Effective Permissions
Clicking on the [Effective Permissions] button and then selecting a user from the list will allow you to view the user's effective permissions with regards to the specified folder or file. Effective permissions are determined from the combination of Windows ACL permissions and shared folder access rights.

2.3 Configuring Windows ACL permissions with Windows Explorer

1. First, use a Windows administrator account to map a Windows ACL enabled shared folder as a network drive. For more information, please see NAS 106: Using NAS with Microsoft Windows.

2. Right-click on any file or subfolder within the shared folder and then select **[Properties]**. Next, select the **[Security]** tab. Here, you will be able to see a list of users and groups and their ACL permissions for the file or subfolder.

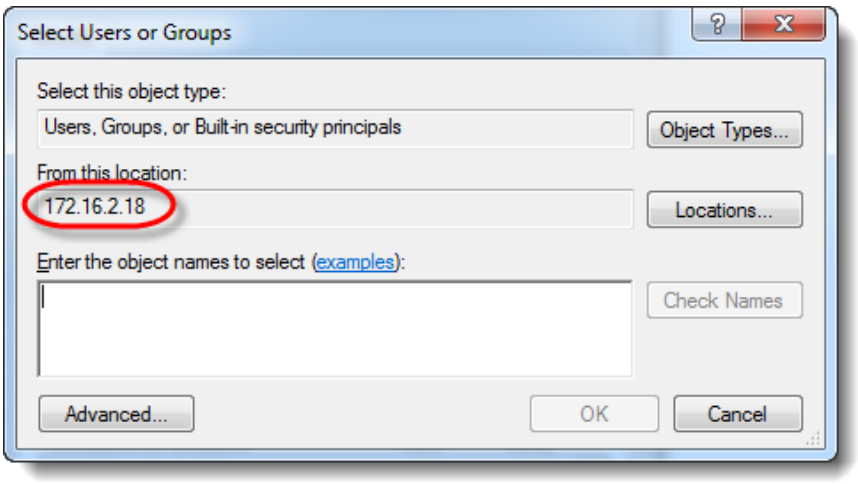


If an object simultaneously has inherited permissions from its parent and also explicit permissions, the inherited permissions will be checked in grey while the explicit permissions will be checked in black.

3. Click on **[Edit]** → **[Add]**. In the [From this location:] field you should see the following information:

   If the NAS has been added to a Windows AD domain you will see the AD domain name.

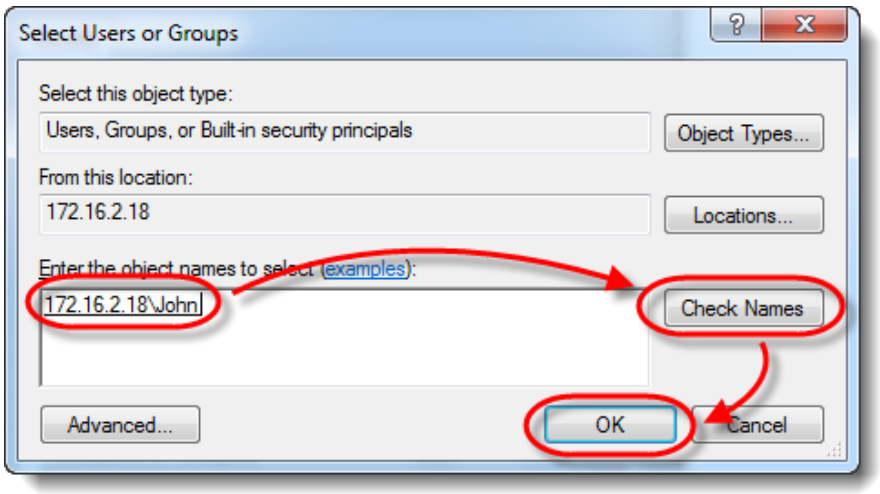
   If the NAS has not been added to a Windows AD domain, you will see the NAS's IP address.



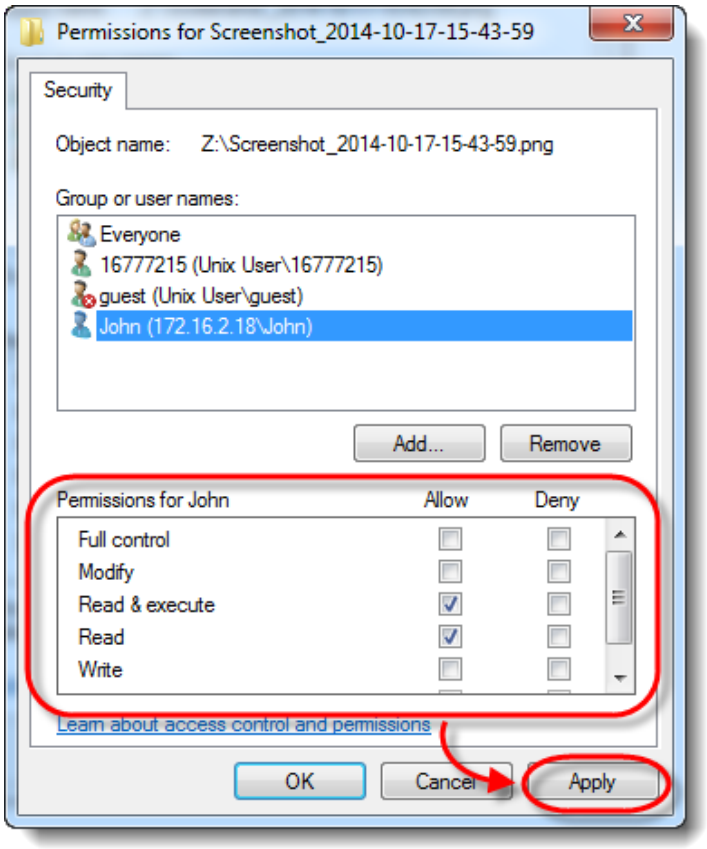
4. In the **[Enter the object names to select]** field, enter the following information:

   If the NAS has been added to a Windows AD domain, enter the domain user or group name and then click on **[Check Names]** in order to verify the user/group name. Then, click on **[OK]**.

   If the NAS has not been added to a Windows AD domain, enter the ADM local user or group name and then click on **[Check Name]** in order to verify the user/group name. Then, click on **[OK]**.



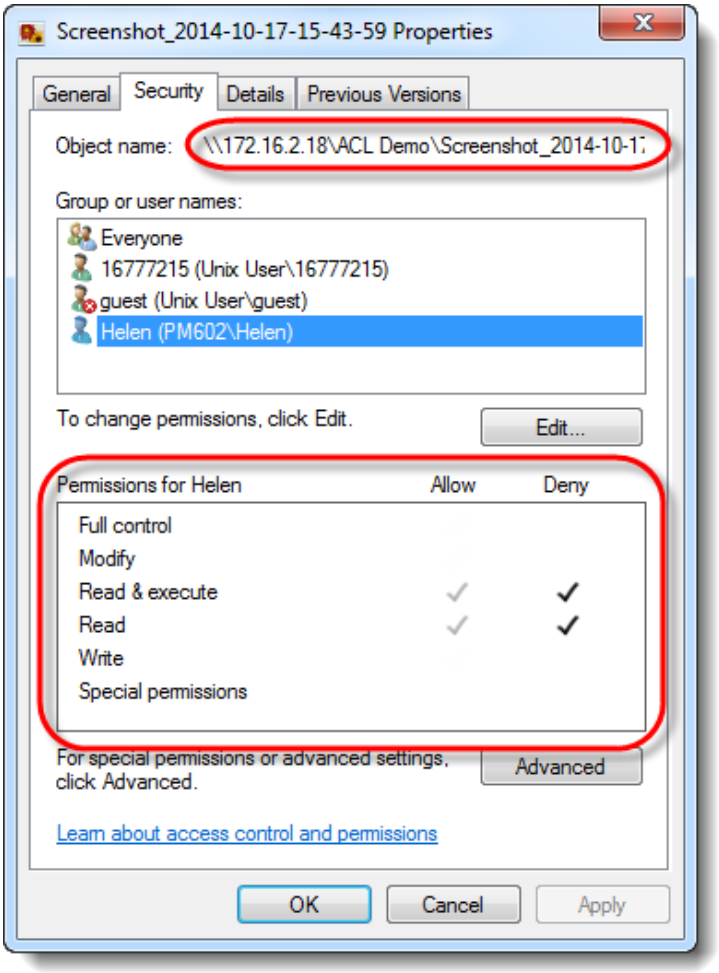
5. Now, you should be able to see the newly added user or group in [Group or user names:] list. Select the user or group and then use the **[Allow]** and **[Deny]** checkboxes to configure their access permissions for the object. Once you are done, click on **[Apply]**.



2.4 Windows ACL permission rules and precautions

2.4.1 ACL Conflicting ACL permissions

If you encounter conflicting Windows ACL permissions, the object's explicit permissions will be given priority. For example, if the user Helen inherits "Allow Read & Execute" permissions for a file but the given explicit permissions for the file are "Deny Read & Execute", then Helen will not be able to access the file.



Conversely, if Helen inherits "Deny Read" permissions but the explicit permission given to the file are "Allow Read", then Helen will be able to access the file.

2.4.2 Rules for moving files and folders

		Copy	Move
Moving within the same shared folder	A1. ACL Disabled	Retain existing permissions	Retain existing permissions
	A2. ACL Enabled	Remove ACL permissions inherited from source folder Remove explicit ACL permissions Apply ACL permissions inherited from destination folder	Remove explicit ACL permissions Retain explicit ACL permissions Apply ACL permissions inherited from destination folder
Moving between different shared folders	B1. ACL Disabled ACL Enabled	Retain existing permissions	Retain existing permissions
	B2. ACL Disabled ACL Enabled	Apply ACL permissions inherited from destination folder	Apply ACL permissions inherited from destination folder
	B3. ACL Enabled ACL Disabled	Remove all ACL permissions Permissions will be reset as “Full access for all users”	Remove all ACL permissions Permissions will be reset as “Full access for all users”
	B4. ACL Enabled ACL Enabled	Remove ACL permissions inherited from source folder Remove explicit ACL permissions Apply ACL permissions inherited from destination folder	Remove ACL permissions inherited from source folder Remove explicit ACL permissions Apply ACL permissions inherited from destination folder

Exceptions: When data is deleted from an ACL enabled shared folder and moved to the Network Recycle Bin the rules from “B3” in the chart above will not apply. This is to prevent the situation where files with “Deny Access” permissions are deleted and moved to the Network Recycle Bin and then become fully accessible to all users. Taking privacy and security into consideration, files from ACL enabled folders that are moved to the Network Recycle Bin will be assigned the permission “Read & Write for Owners, Deny Access for all Other Users”.

2.4.3 File deletion permissions

There are 2 permissions associated with deleting files:

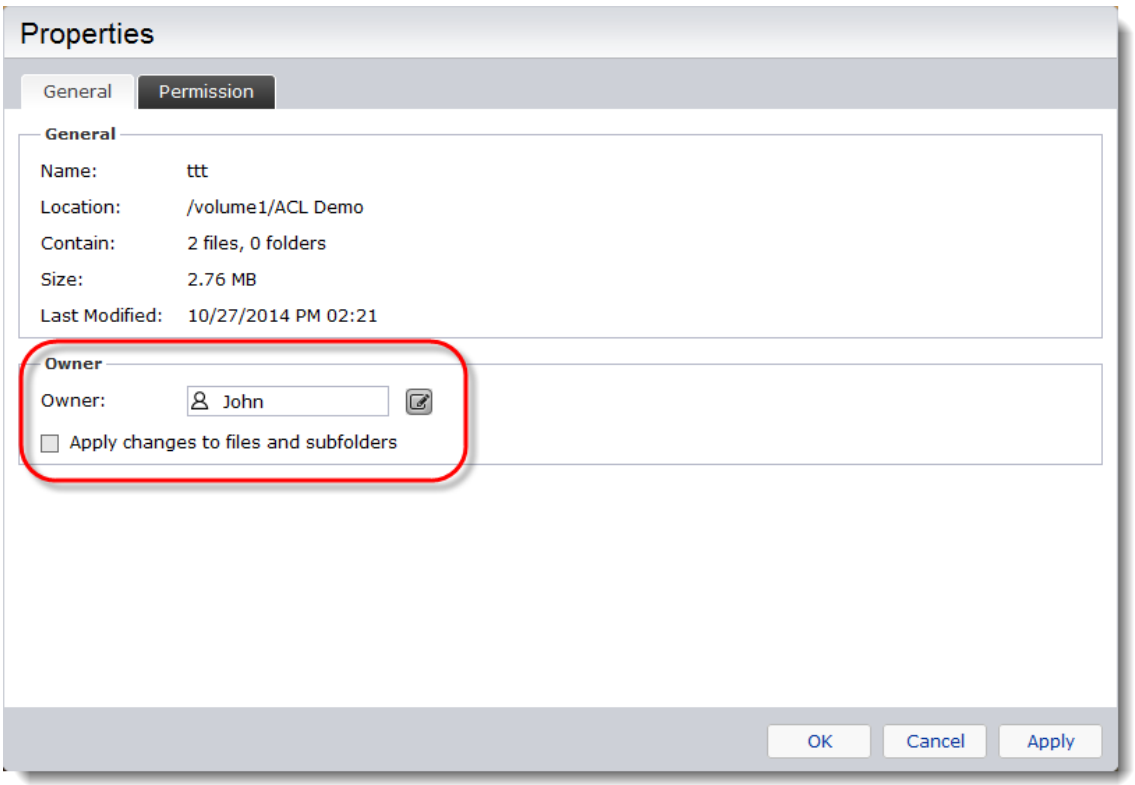
1. User has explicit “Delete” permission for the file
2. User has “Delete subfolders and files” permission for the file’s parent folder.

If any of the above permissions are configured as “Deny”, then the user will not be able to delete the file.

Only if neither of the above permissions has been configured as “Deny” and at least one of them has been configured as “Allow”, will the user be able to delete the file.

2.4.4 Ownership of objects

After Windows ACL has been enabled for a shared folder, each object (subfolders and files) contained within the folder will have an owner. You can view ownership information for an object by selecting it from ADM File Explorer, right-clicking on it and then selecting **[Properties]**. The ownership information will be viewable in the **[Owner]** section of the **[General]** tab.



Owners of an object will be able to configure ACL permissions for it. For example, the user John in the graphic above, is the owner of the ttt folder. Therefore, John will be able to configure ACL permissions for the folder and the subfolder and files contained within it.

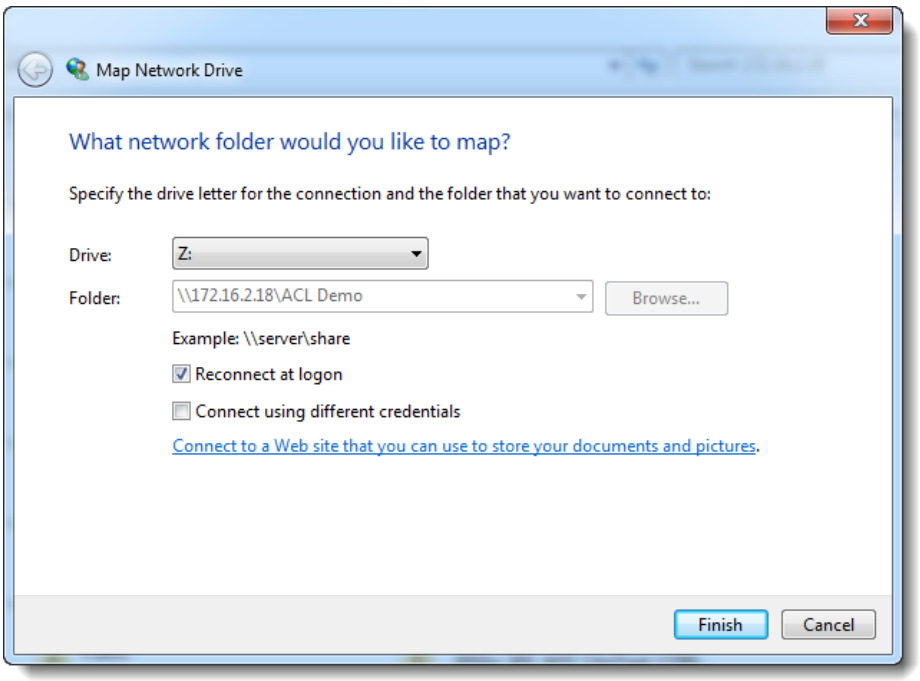
For every newly added object, the creator of the object will be set as the owner by default. Additionally, users in the administrator group will have the ability to modify the ownership of objects. For example, if we wanted to transfer ownership of the ttt folder in the graphic above to other users (i.e., Helen), John and all users in the administrator group would have the ability to transfer ownership. Once Helen becomes an owner of the ttt folder, she will be able to reconfigure permissions for its subfolders and files even if she did not originally have access permissions for them.

2.5 Moving objects to your NAS while maintaining ACL permissions

When all Windows PCs and NAS devices in a network environment have been added to the same Windows AD domain, all user accounts and permissions on the domain can be combined together. However, when moving files or folders from a PC server to a NAS, existing ACL permissions will not be retained (using the rules in section 2.4.2). This causes IT staff to have to reconfigure permissions.

If you wish to maintain existing ACL permissions when moving files or folders to your NAS, you can utilize Fastcopy, a 3rd party software (http://ipmsg.org/tools/fastcopy.html.en). In the example below, we will demonstrate how to use this Fastcopy.

1. First, use a Windows administrator account to map a Windows ACL enabled shared folder as a network drive. For more information, please see NAS 106: Using NAS with Microsoft Windows. In our example we have mapped a shared folder as the network drive "Z:".

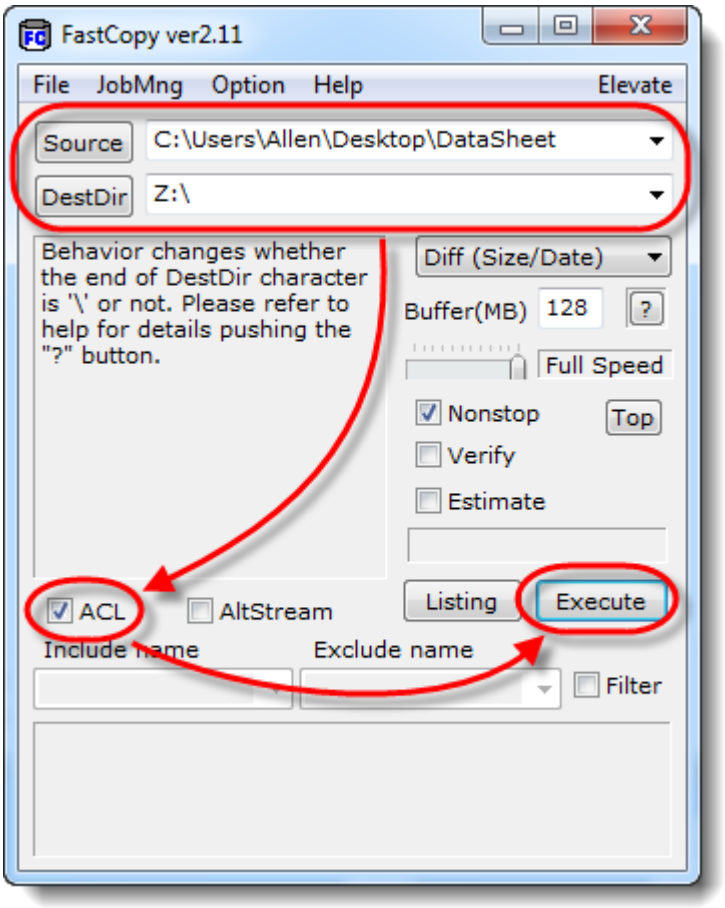


2. Open Fastcopy.

3. **[Source]**: Specify the source folder here.
   [DestDir]: Specify the destination folder here (the "Z:" network drive mapped in step 1)

   Select the **[ACL]** checkbox to ensure that Fastcopy will retain the original ACL permissions of your files when moving them.

   Click on **[Execute]** to begin moving the folder.



4. After the folder has been moved successfully, all data moved to the destination will have retained their ACL permissions from the source (including all explicit and inherited permissions). This data will not inherit any permissions from the parent object at the source.