Viewing Permissions

Permissions on a NAS share reflect what the NAS server allows for your connected user account. They follow POSIX-style (user/group/other) or ACL (Access Control Lists) models, but visibility depends on the protocol.

Using Finder (Graphical Interface)

1. **Navigate to the Mounted Share**: In Finder, go to the mounted NAS volume (e.g., under /Volumes/ShareName).
2. **Select the File or Folder**: Click on the item you want to inspect.
3. **Get Info**:
    - Right-click (or Control-click) the item and select Get Info (or press Command + I).
    - In the Info window, scroll to the Sharing & Permissions section at the bottom.
4. **Interpret Permissions**:
    - You'll see a list of users/groups with privileges: Read & Write, Read Only, or No Access.
    - The lock icon indicates if changes are possible (locked means read-only from the Mac's perspective).
    - Owner and Group are shown, but these are set on the NAS side.
    - If ACLs are in use (common on SMB shares), you'll see additional entries with more granular controls (e.g., inheritance flags).

This method is user-friendly but may not show all details if the share uses advanced NAS features like snapshots or quotas.

Using Terminal (Command Line)

For more detailed or scripted viewing:

Connecting to the NAS on Your Mac Studio

Before viewing or changing permissions, ensure the NAS is properly connected and mounted on your Mac Studio (running macOS). Since it's on a local LAN, the connection typically uses protocols like SMB (most common for modern NAS devices), AFP (older Apple protocol), or NFS.

1. **Open Finder**: Launch Finder from the Dock or Spotlight (Command + Space, then type "Finder").
2. **Connect to Server**:
   - Go to the menu bar: Finder > Go > Connect to Server (or press Command + K).
   - Enter the NAS address in the format: `smb://NAS-IP-Address/ShareName` (replace `NAS-IP-Address` with the actual IP, e.g., `192.168.1.100`, and `ShareName` with the shared folder name). For AFP, use `afp://`; for NFS, use `nfs://`.
   - If prompted, enter your NAS username and password. You can save these in Keychain Access for automatic future connections.
3. **Mount the Volume**: Click Connect. The NAS share should appear in the Finder sidebar under Locations (or as a mounted volume on the Desktop if enabled in Finder Preferences > General > Show these items on the desktop > Connected servers).
4. **Verify Connection**: If it doesn't mount, check your network (ensure the Mac Studio and NAS are on the same LAN subnet), firewall settings on the NAS, or NAS sharing configurations. Common issues include incorrect credentials or protocol mismatches—most NAS devices (e.g., Synology, QNAP, Western Digital) default to SMB for macOS compatibility.

If the NAS auto-mounts (e.g., via Bonjour/mDNS discovery), it might appear automatically in the Finder sidebar.

1. **Open Terminal**: Search for it in Spotlight (Command + Space).
2. **Navigate to the Share**: Use `cd /Volumes/ShareName` (replace ShareName accordingly).
3. **View Permissions**:
    - Run `ls -l` to list files/folders with permissions. Output looks like:

      `-rw-r--r-- 1 username groupname size date filename`
    - First column: Permissions (e.g., `drwxr-xr-x` for directories; `d` = directory, `r` = read, `w` = write, `x` = execute/search).
    - Next: Owner and group.
    - For ACLs, use `ls -le` to show extended attributes.
    - To view a specific item: `ls -l /path/to/file_or_folder`.
4. **Check Mount Options**: Run `mount | grep /Volumes/ShareName` to see how the share is mounted (e.g., read-write or read-only).

Terminal provides raw, scriptable output—useful for automation or troubleshooting.

Changing Permissions

Changing permissions from the Mac affects the NAS only if the share is mounted with write access and your user has sufficient privileges on the NAS. Otherwise, changes may fail or be temporary. For persistent changes, manage them directly on the NAS (see below).

Using Finder

1. **Open Get Info**: As above, right-click the file/folder > Get Info > Sharing & Permissions.
2. **Unlock if Needed**: Click the lock icon in the bottom-right and enter your Mac admin password (not NAS credentials—this unlocks the interface).

3. **Modify Permissions**:
    - Click the privilege dropdown next to a user/group and select Read & Write, Read Only, etc.
    - To add a user/group: Click the + button, select from the list (local Mac users or NAS-mapped ones).
    - Apply to enclosed items: Check the gear icon > Apply to enclosed items for recursive changes.
4. **Save Changes**: Close the window; changes apply immediately if allowed by the NAS.
5. **Limitations**: If the NAS enforces stricter rules (e.g., via its own ACLs or user quotas), changes may revert or fail with an error like "Operation not permitted."

Using Terminal

1. **Navigate**: `cd /Volumes/ShareName`.
2. **Change Permissions**:
    - Use `chmod` for basic POSIX: e.g., `chmod 755 filename` (sets owner rwx, group/other rx).
        - Numeric mode: 7 = rwx, 6 = rw-, 5 = r-x, etc.
        - Symbolic: `chmod u+w filename` (adds write for user).
    - Recursive: `chmod -R 755 folder/` (applies to all contents).
    - For ownership: `chown username:groupname filename` (requires sudo if not owner; `sudo chown ...`).
3. **Handle ACLs**: Use `chmod +a "user:username allow read,write" filename` to add ACL entries.
4. **Errors**: If you get "Permission denied," check your NAS user privileges or remount with `mount -o rw`.

Be cautious with recursive changes (`-R`) to avoid locking yourself out.

Important Notes on Server-Side Control

- **NAS Controls the Rules**: Permissions viewed/changed on the Mac are proxies for the NAS's settings. For full control:
    - Access the NAS web admin interface: Open a browser on your Mac Studio, enter the NAS IP (e.g., http://192.168.1.100), log in with admin credentials.
    - In the NAS dashboard (e.g., Synology DSM, QNAP QTS):
        - Go to Control Panel > Shared Folders > Edit permissions for the share.
        - Manage users/groups: Add Mac users, set read/write/deny, enable ACLs.
        - Apply advanced features like inheritance or auditing.
    - After changes, remount the share on the Mac to refresh.
- **Security Considerations**:
    - Use strong NAS passwords and enable HTTPS for the admin interface.
    - If using SMB, ensure SMB3 encryption is enabled on the NAS for LAN security.
    - Back up data before bulk permission changes.
    - If the NAS is exposed beyond LAN (e.g., via port forwarding), use VPN for remote access to avoid risks.
- **Troubleshooting**:
    - If permissions don't stick: Check NAS logs via its web interface.
    - Protocol Issues: SMB is recommended for macOS Ventura/Sonoma+; test with `smbutil status NAS-IP` in Terminal.