Groupdrive - Permissions - Permission Management

10.09.2026 05:04:52

FAQ-Artikel-Ausdruck

Kategorie:	Datenspeicher & Datenablage::Gruppenlaufwerk	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	12:04:13 - 28.08.2026

Lösung (öffentlich)

Group Drive - Permissions - Permission Management Permissions on the Group Drive ↔ on the Group

Group Drives use groups to manage access permissions. This results in two independent permission levels: the contacts of the group drive, and the members or managers of the associated group.

At the time the group drive is created, the administrators and deputies listed in the request are set as managers of the associated group.

Contacts of the group drive (managed via [1]group drive management in the SSP):

-

Controls the visibility of the drive in the SSP

-

Controls access to functions within the SSP (e.g., adjusting NFS clients)

-

Controls the contact persons (for information, or in case ZIH needs to get in touch)

Members and managers of the group (managed via [2]group management in the SSP):

-

Members of the group receive access permissions to the group drive

-

Managers of the group can grant access permissions to further users

Please note: Changes to the contacts of a group drive have no effect on the access rights or their management.

If a group drive is to be handed over to someone else, both permission levels must therefore be taken into account. Both the responsibilities for the group drive and the management of the associated group should be handed over accordingly.

UNIX Access Permissions

UNIX permissions are a fundamental access control system for UNIX-like operating systems.

There are three permission subjects: the owner, the group, and all others. Each subject has three possible permissions: read, write, and execute (where “execute” for directories means the ability to enter the folder).

In the context of Group Drives, the group plays a central role in access control, as shared access is primarily organized through it. The owner is typically the user who created the file. Other users do not have access to the Group Drive by default unless explicitly granted.

If the Group Drive is accessed via the NFS protocol, additional specifics apply – see [3]Special permissions for NFS access.

UNIX Default Permissions

Group Drives with UNIX permissions are assigned an administrators group, in which administrators and deputies are members and maintain administrative rights.

-

The administrator of the Group Drive is the UNIX owner of the main directory

-

The administrators group is the UNIX group of the drive

-

The permissions are set to 2770 (setgid - rwx - rwx - ---):

-

setgid: All newly created files and folders within the Group Drive inherit the administrator group

-

rwx: The administrator and the administrators group have full access rights

-

---: All other users have no permissions

-

For new files and folders: The UNIX owner is always the user who created the file. The group is automatically inherited for all new files and folders via setgid

The UNIX permission scheme used for our Group Drives is not intended to be modified by users. The group is the primary permission holder and should generally not be changed.

NTFS Access Permissions

NTFS is the default file system on Windows and provides a detailed permission model for files and folders.

In contrast to classic UNIX permissions, NTFS uses an extended access control model (ACLs – Access Control Lists), where permissions can be defined in a very granular way for individual users and groups.

This allows permissions to be assigned to arbitrary combinations of users and groups. In addition, permissions can be inherited, restricted, or explicitly denied, enabling a very flexible but also more complex administration model.

For Group Drives with NTFS permissions, users receive a predefined ACL structure based on IDM groups. Experienced users can adjust NTFS permissions if needed to flexibly adapt the permission structure.

NTFS Default Permissions

Group Drives with NTFS permissions are assigned an administrators group and optionally a user group.

Domain Administrators (predefined group)

-

These are central system administrators (ZIH admins)

-

They are granted access to provide support and troubleshoot issues

-

This permission can be removed (however, in this case, we may no longer be able to assist with certain problems)

Administrators Group (IDM group)

-

A dedicated administrative group created for each Group Drive

-

Has full access rights (read, write, modify, delete, and permission management)

-

Permissions are inherited by default to newly created files

-

Should never be deleted, as this would make the Group Drive unmanageable

User Group (IDM group)

-

Defined in the application form and optional

-

Exists only for NTFS-based Group Drives

-

Has restricted access rights (read, modify)

-

Permissions are inherited by default to new files

The permission scheme may differ for older drives. The scheme described above applies to newly created Group Drives.

Adjusting the Permission Scheme

Experienced users can also adjust permissions directly on the file system. However, since this can render the group drive unusable, we only recommend it for users who are familiar with the permission systems:

-

[4]Adjusting UNIX permissions

-

[5]Adjusting NTFS permissions

[1] https://selfservice.tu-dresden.de/services/groupdrive/overview/
[2] https://selfservice.tu-dresden.de/services/group-management/groups/
[3] https://faq.tickets.tu-dresden.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=1537;
[4] https://faq.tickets.tu-dresden.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=1535;
[5] https://faq.tickets.tu-dresden.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=1534;