

How to display the folders that are not accessible by a particular user

1) Search for the particular user and display the user info:

The screenshot shows the Permission Analyzer interface. On the left, the 'Filter on members' pane has a search icon circled in yellow. A modal window titled 'Include or exclude members (users and groups)' is open, with the search term 'jess' entered and circled in yellow. The search results table shows two entries: 'TESTDOMAIN\Jess Young' and 'TESTDOMAIN\Jessie Robertson'. The 'Show member info' button for the second entry is circled in yellow. The background shows a file tree with permissions for paths like '\\dataserver01\projects' and '\\dataserver01\data'. At the bottom, the 'Effective permissions' pane shows a list of members and their permissions.

Path - 61 items found	Permission	Owner	Inherit parent ACL
> \\dataserver01\projects	Full		Yes
> \\dataserver01\data	Full		Yes

Account name	Display name	Domain / computer
TESTDOMAIN\Jess Young	Jess Young	TESTDOMAIN
TESTDOMAIN\Jessie Robertson	Jessie Robertson	TESTDOMAIN

Member	Permission	Inheritance flags	From folder
> WORKSTATION\Administrators [local group]	Full		
> WORKSTATION\SYSTEM [local group]	Full		
> WORKSTATION\Gebruikers [local group]	Read and execute		
> WORKSTATION\Geverifieerde gebruikers [local group]	Modify		

2) Copy all the nested group membership as CSV to the clipboard:

The screenshot displays the Permission Analyzer interface. A 'Member info' dialog box is open, showing details for user 'Jessie Robertson'. The 'Member of' section is expanded, showing a list of groups with their descriptions and inheritance flags. A yellow circle highlights the 'Copy to clipboard' button at the bottom of the dialog.

Member info dialog - Member of section:

Group	Description	Via group
TESTDOMAIN\Database admins	[global group]	Intranet Developers
TESTDOMAIN\Domain Users	All domain users [global group]	
TESTDOMAIN\Intranet Developers	Developers of the Intranet websit...	
TESTDOMAIN\Product designers	[global group]	
TESTDOMAIN\Users	Users are prevented from making...	Domain Users

Main window - Path - 61 items found:

Path	Permission	Owner	Inherit parent ACL
\\dataserver01\projects	Full		Yes
\\dataserver01\data	Full		Yes

Main window - Effective permissions:

Member	Permission	Inheritance flags	From folder
WORKSTATION\Administrators [local group]	Full		
WORKSTATION\SYSTEM [local group]	Full		
WORKSTATION\Gebruikers [local group]	Read and execute		
WORKSTATION\Gevenifieerde gebruikers [local group]	Modify		

3) Add all the groups as Exclude filter

- Paste the CSV files in Excel
- Use the first column (account name) and remove the domain name
- Open the Search Members dialog in Permission Analyzer
- Expand the search box
- Paste all the groups in the search box and add all the groups as Exclude filter:

The screenshot shows the Permission Analyzer interface. On the left, the 'Filter on members' dialog is open, with a search icon circled in yellow. In the center, the 'Include or exclude members (users and groups)' dialog is open, showing a search box with a list of groups. A yellow arrow points to the search box with the text 'Expand the search box'. Another yellow arrow points to the search box with the text 'Paste the groups from the CSV file'. At the bottom of the dialog, the 'Exclude selected members' button is circled in yellow. The background shows a file tree with permissions for '\\dataserver01\projects' and '\\dataserver01\data'. The bottom of the screen shows a table of members and their permissions.

Path - 61 items found	Permission	Owner	Inherit parent ACL
> \\dataserver01\projects	Full		Yes
> \\dataserver01\data	Full		Yes

Account name	Display name	Domain / computer
TESTDOMAIN\Database admins	[global group]	TESTDOMAIN
TESTDOMAIN\Domain Users	All domain users [global group]	TESTDOMAIN
TESTDOMAIN\Intranet Developers	Developers of the intranet website [global group]	TESTDOMAIN
TESTDOMAIN\Intranet Users	Users of the intranet website [global group]	TESTDOMAIN
TESTDOMAIN\Product designers	[global group]	TESTDOMAIN
TESTDOMAIN\Users	Users are prevented from making accidental or intentional system-wide...	TESTDOMAIN

Member	Permission	Inheritance flags	From folder
> WORKSTATION\Administrators [local group]	Full		
> WORKSTATION\SYSTEM [local group]	Full		
> WORKSTATION\Gebruikers [local group]	Read and execute		
> WORKSTATION\Geverifieerde gebruikers [local group]	Modify		

4) All the groups of this particular user are now added as exclude filter. You may want to add the user account to the exclude list as well. Apply the filter in the toolbar to view the results:

The screenshot shows the 'Permission Analyzer' application interface. The 'Filter on members' sidebar is active, showing 'Member filter options' with 'Users', 'Groups', 'Built-in groups', and 'Group memberships' all checked. Under 'Include or exclude users/groups', several groups are listed, including 'TESTDOMAIN\Database admins' and 'TESTDOMAIN\Users'. A yellow text box states: 'All the groups of the user will be excluded from the overview. Apply the filters in the toolbar'. The main pane shows a file tree with two items: '\\dataserver01\projects' and '\\dataserver01\data', both with 'Full' permissions. The bottom pane shows 'Effective permissions' for the selected file, listing members like 'WORKSTATION\Administrators' and 'WORKSTATION\SYSTEM' with their respective permissions.

Member filter options:

- Include:
 - Users
 - Groups
 - Built-in groups
 - Group memberships
- Include or exclude users/groups:
 - TESTDOMAIN\Database admins [global group]
 - TESTDOMAIN\Domain Users [global group]
 - TESTDOMAIN\Intranet Developers [global group]
 - TESTDOMAIN\Intranet Users [global group]
 - TESTDOMAIN\Product designers [global group]
 - TESTDOMAIN\Users [domain built-in group]

File Tree:

Path	Permission	Inherit parent ACL
> \\dataserver01\projects	Full	Yes
> \\dataserver01\data	Full	Yes

Effective permissions:

Member	Permission	Inheritance flags	From folder
> WORKSTATION\Administrators [local group]	Full		
> WORKSTATION\Gebruikers [local group]	Read and execute		
> WORKSTATION\Geverifieerde gebruikers [local group]	Modify		
> WORKSTATION\SYSTEM [local group]	Full		