Charles Sturt University

Share Administrators User Guide

[Interim replacement for the Share Admin page]

Division of Information Technology

For further information please contact the IT Service Desk

Contents

Overview

The Division of Information Technology (DIT) provides a reliable, centrally managed location for storing, sharing and securing files. The S: Drive is a safe and secure network file storage area with easy access from Windows and Mac computers.

Each of the university's faculties, schools, offices, divisions, institutes and centres has shared folders on the S: Drive which can be accessed through the university network at any time both on and off campus. To access the university network when off campus, use either Virtual Desktop Infrastructure (VDI) or Virtual Private Network (VPN).

The P: Drive is provided on the university network for all users to create, store and manage personal files and folders. Users only have access to their own P: Drive. SAs cannot grant access to staff P: Drives.

This guide

This guide provides instructions on how to manage access permissions for users to folders on the S: Drive (shared drive) using Windows File Explorer.

This is an interim guide replacing the Share Admins Page while DIT progressively migrates S: Drive management to the new Share Group Structure. If you have already been migrated to the new Share Group Structure this guide is not relevant.

Share Administrator role

Staff responsible for the management of the folders in their area are called Share Administrators (SAs). SAs are given full control of their storage area in order to manage the file and folder access requirements.

Once SAs grant the appropriate permissions, staff can easily access their area on the S: Drive to collaborate and share files.

SAs are also responsible for the management of Microsoft (MS) Outlook distribution lists for their area.

Help is available by contacting the IT Service Desk.

Share Administrator responsibilities

Share Administrators must:

- only give access permission to different areas of the S: Drive to the relevant staff to avoid any unauthorised viewing of files and folders
- never use the EVERYONE group or the SEC Staff group to manage or grant permissions to any folders or files
- ensure their SA role and responsibilities are handed over to an appropriate staff member within their area if they leave the section or university.

Share Administrators are responsible for:

- adding and removing staff members as required for the designated file storage area
- setting permissions for access to folders and subfolders
- creating and managing new folders
- encouraging staff to save their work to the S: Drive

Files stored in the common folders are located on central file servers.

Levels of access permission

Staff are automatically assigned access to the S: Drive but need to contact the relevant SA to request access to the folders for their particular area. There are four levels of access which can be granted to users.

Full Access

- SAs and DIT staff only
- Ability to read, write, create and delete any files and folders
- Ability to manage the permissions on the folders and sub folders

If you are granting full access to a staff member provide this training document to them first and ensure they are aware of their responsibilities as a new SA

Access should not be granted until this has been completed. If you require assistance please contact the IT Service Desk.

Modify Access

- The most common access permission granted to users who access the S: Drive
- Ability to read, write, create and delete files and folders
- Cannot manage or grant permissions on the folders

Read Execute Access

- When staff need to be able to access a file but are not required to change the data e.g a policy or a minutes folder where all staff need access but only the administrative staff are responsible for changes
- Ability to read the files in a folder and to run the file if it is executable
- Cannot write, save, create new files/folders or delete any files/folders
- “Read & Execute” access permissions include “List Folder” contents and “Read” permissions.
- This is the default set of access permissions granted when you add a user.

List Access

- When staff need access to higher order folder/s to navigate to a sub-folder where a file is located
- Commonly used when staff need to access a file or folder in another department or business area
- Staff with access can see the name of other files or folders as they navigate to the folder that they have access to - be aware of sensitive files or folder names that might be viewed
- Grant list access to all of the folders above the sub-folder, then grant either modfiy or read access to the sub-folder that contains the files required

Default permissions

Shared drive folders have a number of default group security permissions which should not be removed or changed. The * symbol below signifies more than 1 group of this name.

- SYSTEM: Used by the system storing the files for managing those files
- *-SEC-File-Managers: Division of Information Technology staff responsible for day to day operations of the storage environment
- *-SA: The Security Administrators who manage access to folders and files for the faculty or school

- Domain Admins: Domain Administrators
- Administrators: Local administrators

Managing access permissions

Getting started

Before you can apply access permissions to files and folders in the S: Drive you need to:

- be a share administrator (SA) or have full security permission on the folder you wish to make changes to
- be logged into a computer with your Charles Sturt login
- know the login name, email address or group – you can only give access to Charles Sturt staff accounts
- decide what level of access permissions you are assigning the user or group.

Using distribution lists to manage permissions (recommended)

DIT recommends using groups, also known as '**Distribution Lists**', as the most efficient way to manage S: Drive permissions.

Adding a distribution list from the MS Outlook Global Address list to your folders gives all members of that distribution list permission to that folder.

This means that when you update the membership of the distribution list you are also automatically updating the permissions for that group on the S: Drive.

- Add new staff members to your distribution lists – this adds them to the S: Drive folders to which that group has access.
- Remove staff from the distribution lists when they leave - this removes their access from all folders that list has access to.

To add users to a distribution list:

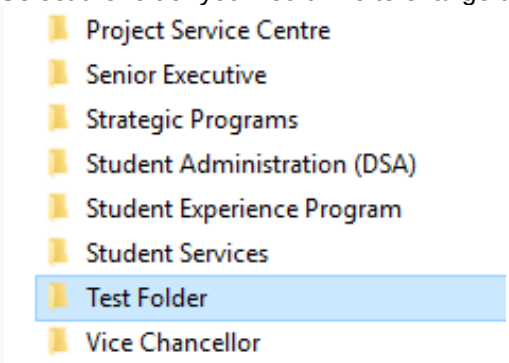
1. Go to https://itservices.csu.edu.au
2. Select Users
3. Select Add Users to AD Group

Note: When you add a distribution list to a folder you are giving all members of the group the same permission level (modify, read-execute, or list access).

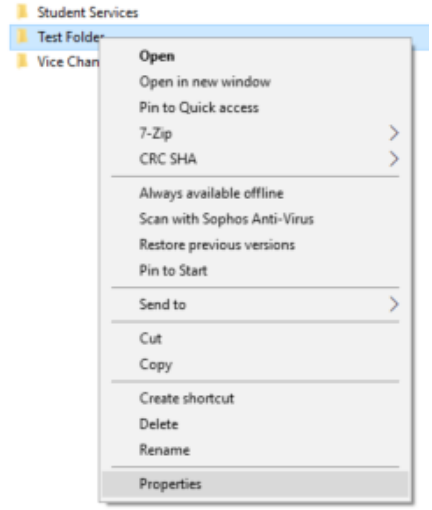
Using Windows File Explorer to apply access permissions

1. Open Windows File Explorer
2. Scroll down and click on the S:Drive (S:)

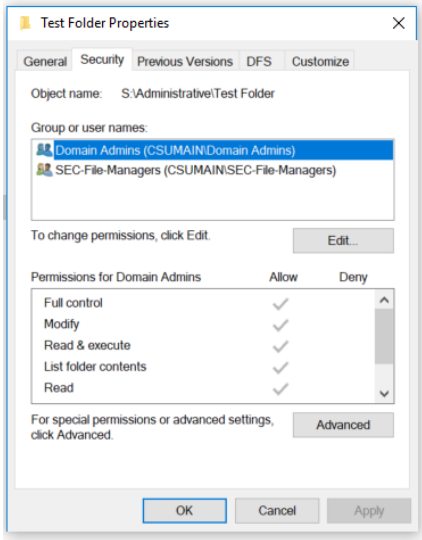
3. Select the folder you would like to change access permission on



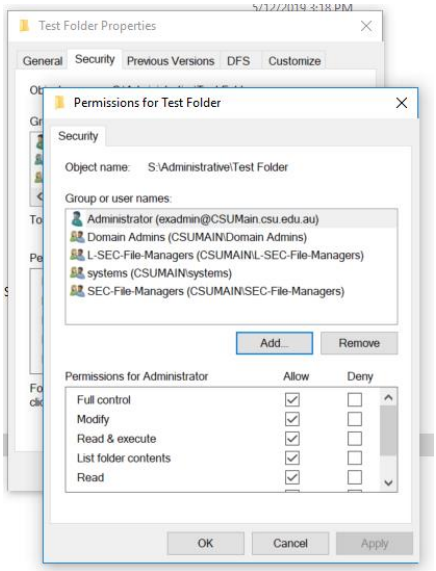
4. Right click and select Properties



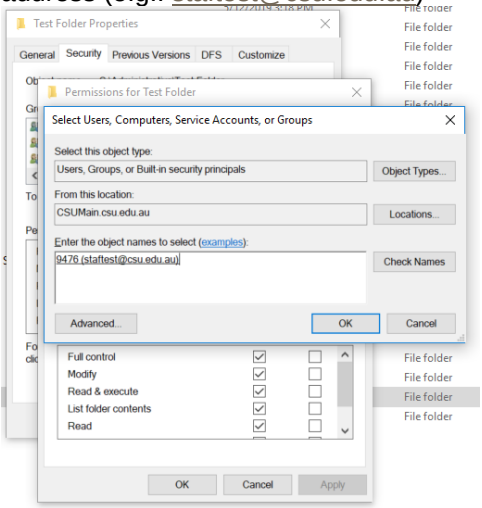
5. Select the Security tab at the top
6. Click the Edit button



7. Click the Add button

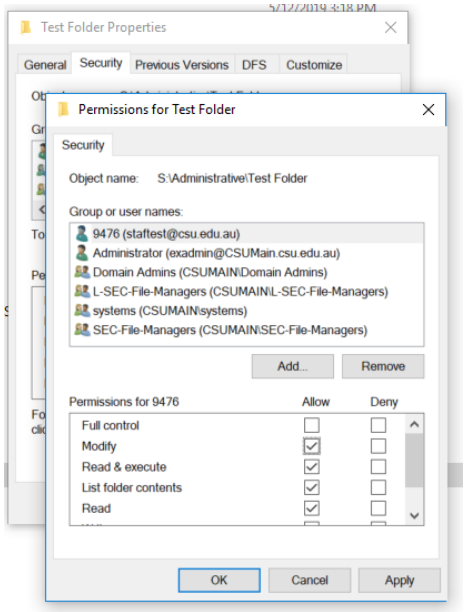


8. In the “Enter the object names to select (examples)” field enter the user’s login (e.g. staftest) or email address (e.g.: staftest@csu.edu.au)



9. Click the Check Names button and ensure it is the right user then click OK
10. Under the “Group or user names” click the user or group to highlight

11. In the “Permissions for” box tick the Allow box next to the level of access permissions that is required or untick the Allow box next to the level of access permissions that is not required.



12. Click OK
13. Click OK to close

Using Windows File Explorer to remove access permissions

1. Open Windows File Explorer
2. Right click on the required folder and select Properties
3. Select the Security tab and click the Edit button
4. In the “Group or user names:” box click the user or group you wish to remove access to.
   Note: Do not remove or change the Sec-File-Managers, System and Domain Admins or Administrator groups from the folder as these are used by the System, DIT support and backup environment.
5. Click on the Remove button and then click OK
6. Click OK to close

Folder management

SAs have the administrative right to be able to create new folders in their business area at their discretion and are responsible for managing all folders and their various levels of access. The more folders created means more management required so consider the need for new folders carefully.

Note: Staff with modify access can also create new folders but cannot give access to other users.

Creating new folders

To create a new folder on the S: Drive using Windows Explorer:

1. Navigate to the location where you would like to create the new folder
2. Right click and select New - Folder
3. Use the Windows File Explorer to administer permission levels to new folders and grant access for other users or groups.

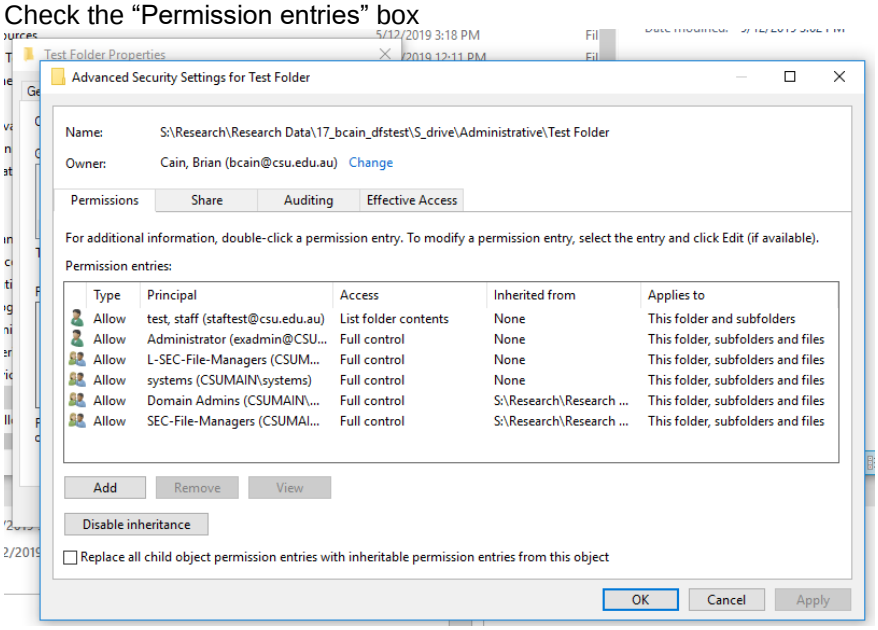
Parent and child folders

- Folders above your created folder are known as parent folders.
- Subfolders within your created folder are known as child folders.

Folder permissions are inherited by all subfolders and files created below the parent folder unless inheritance is turned off.

Check folder access permissions

1. Right click on the folder and select Properties
2. Select the Security tab and click the Advanced button
3. Check the “Permission entries” box



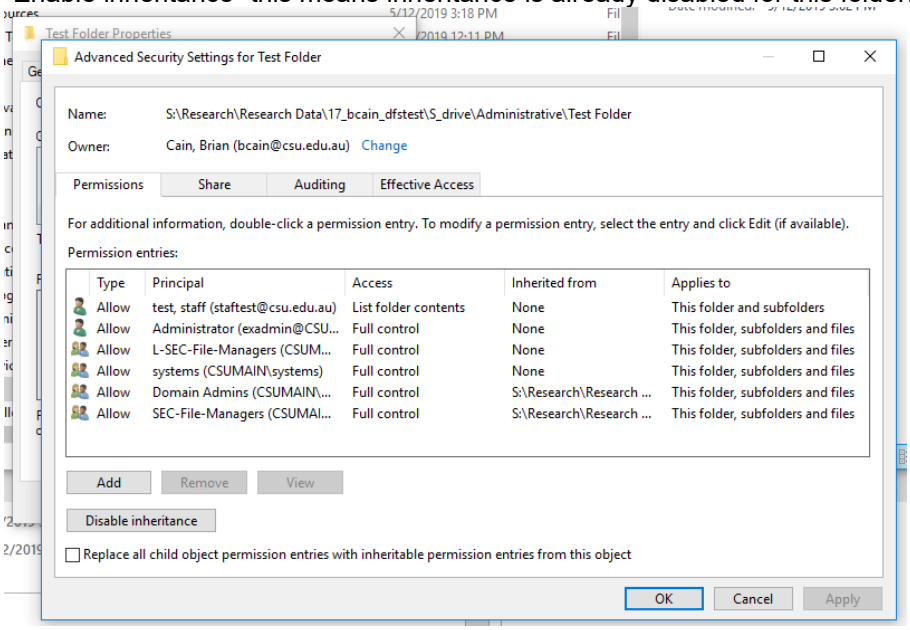
4. Check under the “inherited from” column to see where this permission has been inherited from – if you see “None” this means that this permission has been set directly on this folder

Turn off folder inheritance

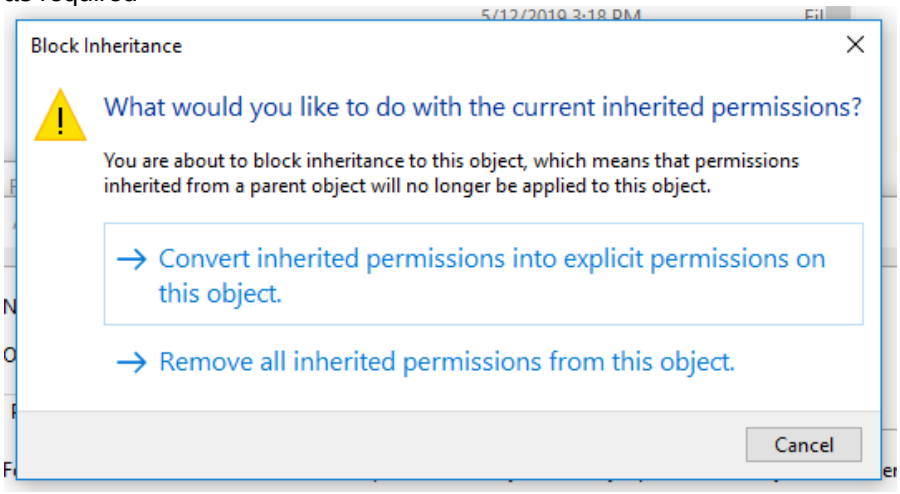
Turning off or breaking inheritance means the permissions from the parent folder are copied to the child folder, but any further changes you make to access permissions are independent to the parent folder and are only applied to the child folder and any of its subfolders.

1. Right click on the required folder and select Properties
2. Select the Security tab and click the Advanced button

3. Select the Permission tab and click “Disable inheritance” button. Note: If the only button you see is “Enable inheritance” this means inheritance is already disabled for this folder.



4. Select the option to “Convert inherited permissions into explicit permissions on this object" - this keeps the previously inherited permissions but we can now manually add or remove these access permissions as required



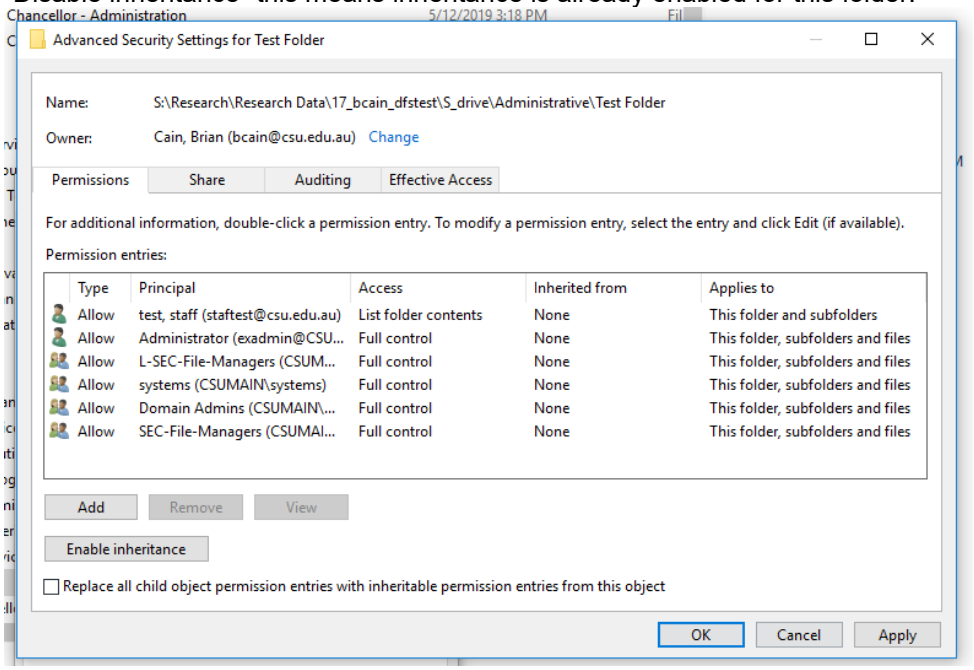
Note: Do not select "Remove all inherited permissions from this object" as all access permissions will be removed including your own. The domain admins, SA, sec-file-manager groups should not be removed. By disabling inheritance any access permissions changes made on the parent folder do not propagate to this folder.

5. Click OK
6. Click OK to close

Turn on folder inheritance

1. Right click on the required folder and select Properties
2. Select the Security tab and click the Advanced button

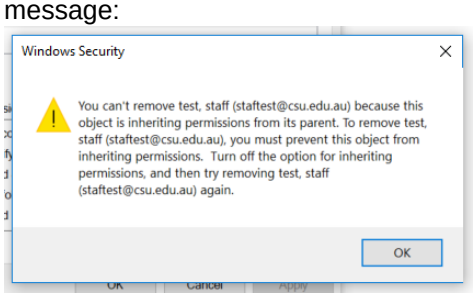
3. Select the Permission tab and click “Enable inheritance” button. Note: If the only button you see is “Disable inheritance” this means inheritance is already enabled for this folder.



4. Click OK
5. Click OK to close

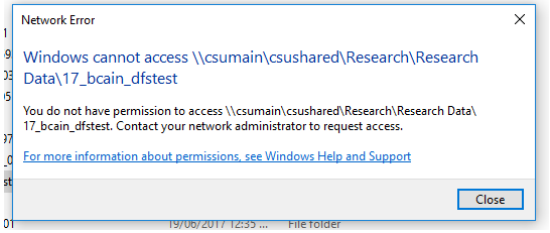
Troubleshooting

1. You are trying to remove a user or group’s access permissions and get the following “Windows Security” message:



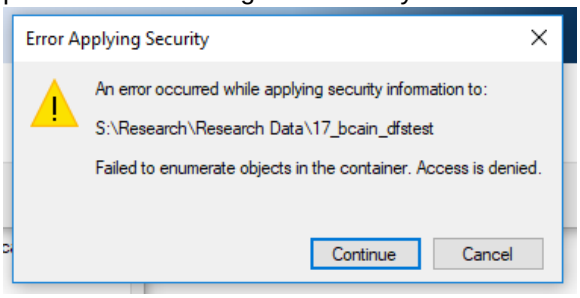
This message is informing you that the folder is currently inheriting its access permissions from a parent folder. Click OK and follow the steps to turn off folder inheritance.

2. The following “Network Error” box tells you that you don’t have access permissions to this folder.

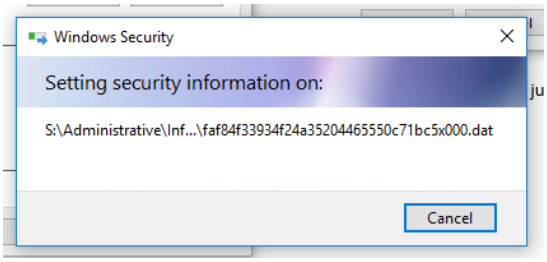


You will need to speak to somebody that has access permissions and ask them to give you permissions. You need at least READ access permissions to open or view access permissions to this folder.

3. The following “Error Applying Security” box tells you that “Access is denied” and that you don’t have permissions to change the security on this folder.



Click the “**Continue**” button to allow access permission to propagate to all subfolders and files. You may have to click “Continue” button a few times so that permissions are propagated down the file structure. Do not click the “Cancel” button as this leads to an inconsistent state where some folders and files have permissions applied and some don’t. You may like to write down the name of the folder or file and search for it later after applying permissions has finished and check its security.



Note: It can take a while for access permissions to be applied as the file structure you are trying to modify access permissions on could have thousands of folders and files.

4. To check if a user is in a group:
   - Go to https://itservices.csu.edu.au
   - Select “Users” from the menu
   - Click “Find Users in AD group”
     - If the group you are looking for does appear under “Select a group below to list all users in them”, click once on the group to highlight then click the “Search” button at the bottom.
     - If the group you are looking for does not appear under “Select a group below to list all users in them” you do not have permissions to view this group. You will need to speak to another SA that may have permissions or contact DIT service desk.

.