Charles Sturt University

Guidelines for Share Administration

Division of Information Technology

Charles Sturt University

March 2015

Charles Sturt University

Contents

Introduction

The Division of Information Technology (DIT) provides a reliable, centrally managed location for storing, sharing and securing files. Known as the **S drive (**or **Shared Drive),** this is a safe and secure network file storage area with easy access from Windows & Macintosh computers.

Each of the University's Faculties, Schools, Offices, Divisions, Institutes and Centres have 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, either Thin Client or Virtual Private Network (VPN) can be used.

Staff responsible for the management of these folders in their area are called **Share Administrator/s** (or **SA/s**).

SAs are given full control of their storage area in order to manage the file and folder access requirements for staff in their area.

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. For more information on distribution lists refer to the *Guidelines for Distribution List administration.pdf* in the Email and Calendar section at the following link.
http://www.csu.edu.au/division/dit/staff/training/self-help/collaboration-and-communications

SA or S drive assistance is available by contacting the DIT Service Desk.

Share Administrator Responsibilities

Share Administrators MUST

- Read and adhere to the guidelines and instructions in this training document in managing permissions
- Be vigilant as to who is given access permission to different areas of the S drive. This will help 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 and
- Ensure the SA role and responsibilities are handed over to an appropriate staff member within their area if the current SA leaves the section or University

Share Administrators will have responsibility for the following in their business area:

- Adding new members of staff to the designated file storage area
- Setting permissions for access to folders
- Setting permissions for access to sub folders
- Creating and managing new folders
- Encouraging staff to save their work to the S drive and

- Removing staff members from folders when they leave or are transferred to other areas of the University

SAs should be aware that files stored in the common folders are located on **central file servers**, which physically reside on either the Wagga or Bathurst campus. The file server used for your department would most likely reside on the campus with the greatest number of personnel.

SAs should encourage staff to save their work to the S and P (Personal) drives. The P drive is provided on the CSU 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.

Share Administrator Management Tool

The Share Admin Management Tool is used by SAs to set staff permission levels to S drive folders. This tool simplifies the process of managing folder permissions on the S drive.

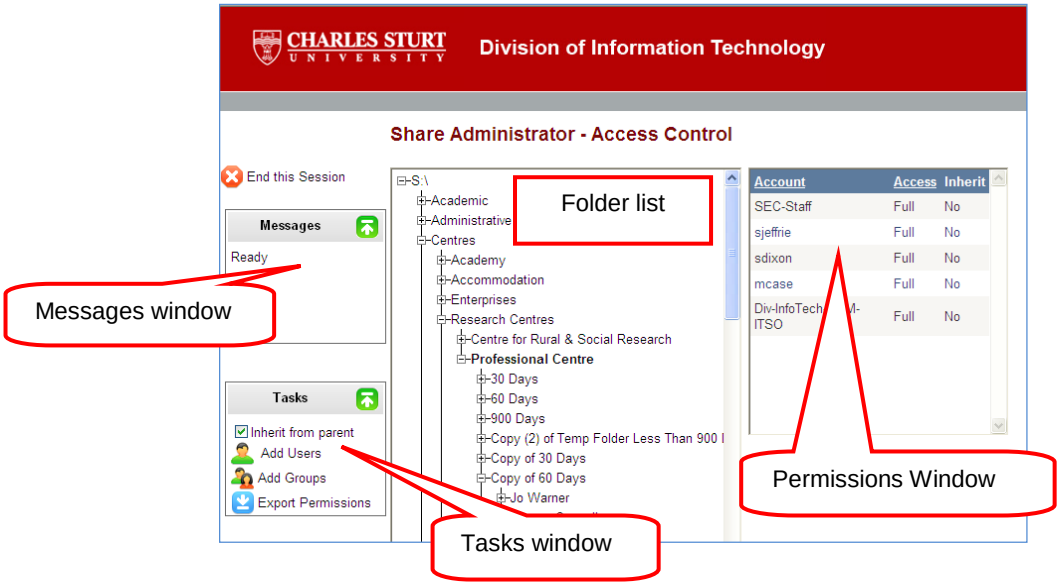
Access

All users have access to the SA Management Tool. SAs are granted access to be able to perform SA duties for their business area by logging a Service Desk request. SAs are required to specify what area on the S drive they will need access to.

Share Administrator Access Control Page

The Access Control page is the command centre of the SA Management Tool. The page is described in more detail below:

- **Messages Window** – this window will display the status of an operation you have requested. The window can be expanded or contracted using the arrow button to the right of the '**Messages**' heading
- **Tasks Window** – add users or groups to a folder using the buttons in this window
- **Folder list** – displays the folder structure you have access to, including folders and sub-folders
- **Permissions Window** – displays a list of users/group and the permissions applied to each



Share Administrators List

SAs can use the SA Management Tool to find out who all the current SAs are for various areas of the S drive.

Click on '**List of Share Administrators**' at the top of the Share Administrator – Access Control window to access the list..

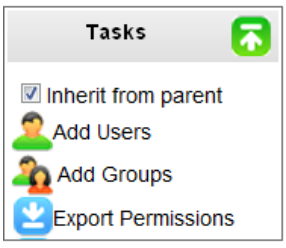
Backing up your Permissions

It is important for SAs to keep detailed copies of the permissions set for each folder so that, in the case of a major problem occurring, you are able to re-enter the correct permissions.

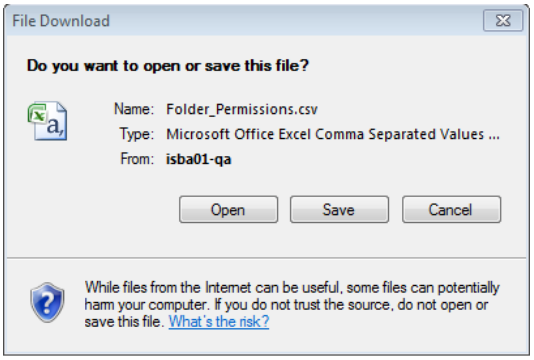
Note - DIT is able to restore the folder structure but not the permissions for files or folders that have been set.

To export a list of the permissions you have set and save for ease of SA management:

1. Choose **Export Permissions** from the **Tasks** window

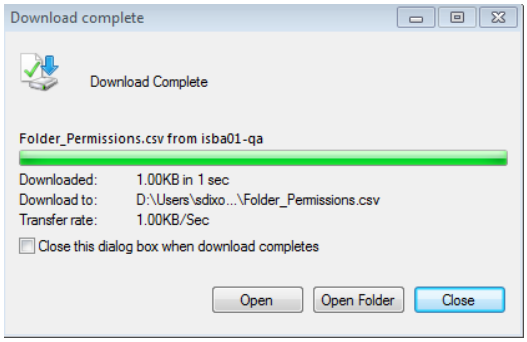


2. A File Download window will appear '***Do you want to open or save this file?'***
   Select '**Save**'



3. You will be prompted for a location to save the file. Choose a secure location such as your **P drive**. Make sure you take note of where you have saved the file for future reference. It is important to update this back up of your set permissions regularly to ensure you can reapply current permissions, if required

4. You will receive a message that your download is complete



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. More folders created means more management required so SAs should 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. Create the folder and give it a meaningful name

Parent and Child Folders

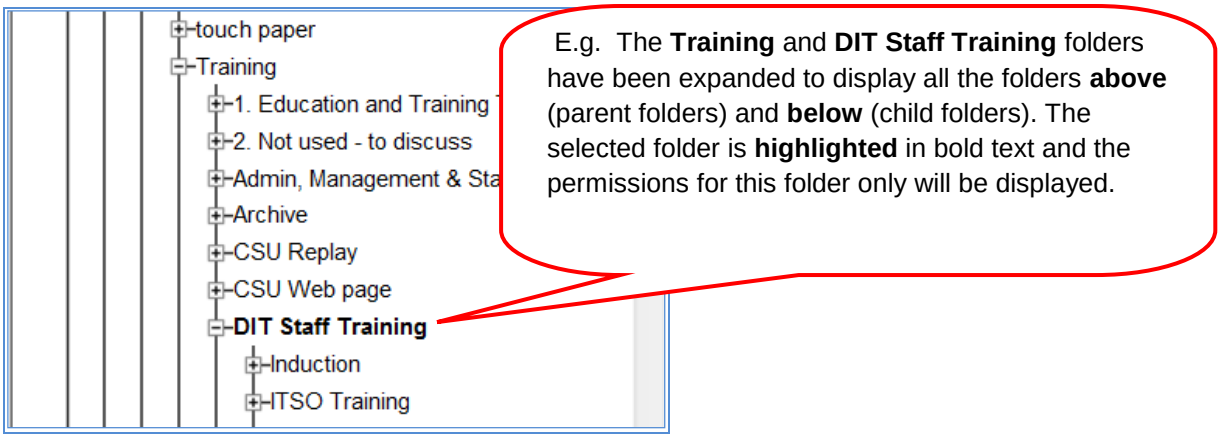
Folders above your created folder are known as **parent folders**. Sub-folders within your created folder are known as **child folders**.

New folders created will automatically inherit permissions from the parent folder unless specifically overridden by the SA. You must use the SA Management Tool to administer permission levels to new folders and grant access for other users or groups.

Using the Folder List to Manage Folders

SAs can view all folders and sub folders within their areas S drive in the SA Management Tool. To expand and view your folders:

1. Go to the Folder List
2. Expand the folders by clicking on the plus sign ⊞ next to your area's folder
3. Keep expanding (using the plus sign) until you get to the folder you are looking for
4. Click on the folder to select it
5. When the folder is selected, you can:
   - view the current permissions for that folder
   - add or remove users
   - change users and groups access level from the permissions window



Undo Changes

If you have made some changes and have not saved, you can use '**Undo Changes**' in the Tasks Window to undo changes you have made. If you have already saved, you **cannot** undo changes and you will need to undo or reapply what you have changed manually.

Understanding Permissions

Staff are automatically assigned access to the S drive but will need to contact the relevant SA to request access to the folders for their particular Faculty/School/Offices/Division/Institute/Centre. SAs are responsible for ensuring validity of access, adding and removing staff as required and monitoring correct user/group permissions.
There are four levels of access which can be granted to users:

- **Full Access** - *SAs and DIT staff only*

- **Modify Access** – *read, write, create and delete*
- **Read Access** – *read only*
- **List Access** – *list only*

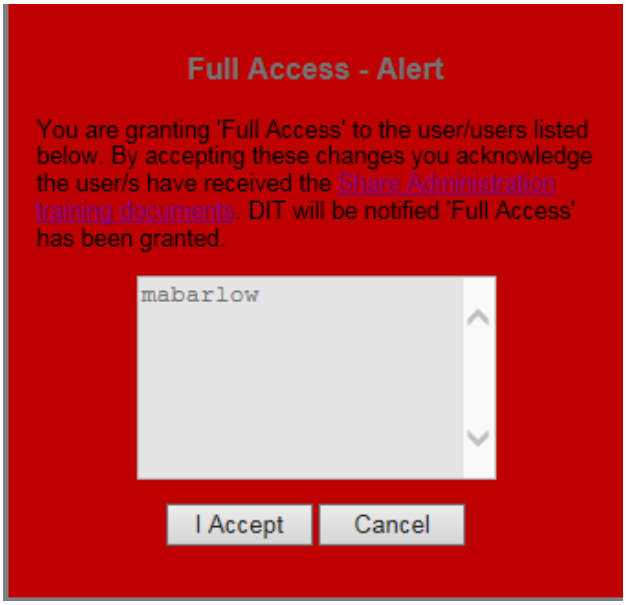
Full Access

Staff with full access to a folder have the ability to **read, write, create and delete any files and folders** in that folder as well as all sub-folders (sub-folder permissions are usually inherited from their parent folder - see **inheritance** for more information).

Full access also grants staff the ability to **manage the permissions** on the folders and sub folders. Full access permission should only be granted to DIT staff and SAs.
When a staff member is granted full access they effectively become an SA, which means they can be held responsible for any breaches of confidentiality or unauthorised viewing of files and folders resulting from the allocation of these privileges. SAs who grant full access to staff can also be held responsible.

Before granting full access to a staff member, SAs are required to provide this training document to the staff member being granted full access. You should also 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 DIT Service Desk.

Note - for security purposes DIT are notified by email when any staff member is granted full access. The following warning screen is displayed when a SA grants full access to a user.



Full Access - ALERT

Warning:
Be particularly careful when granting a staff member full access! Understanding SA responsibilities is essential. You are accountable for the staff members actions until they have received the SA responsibilities document.

Modify Access

Users with modify access can **read, write, create and delete files and folders**.
This is the permission that should be given to most members of staff who access your area of the S drive.
Modify access is almost the same as full access, however with modify access staff cannot manage or grant permissions on the folders and are not SAs.

Read Access

Staff with read access can **read the files** in a folder but cannot write, save, create new files/folders or delete any files/folders.
This access would be given to staff when they need to be able to access the data (i.e. read a document) but are not required to change the data. An example of this may be a policy or a minutes folder where all staff need access but which the administrative staff are responsible for changes.

List Access

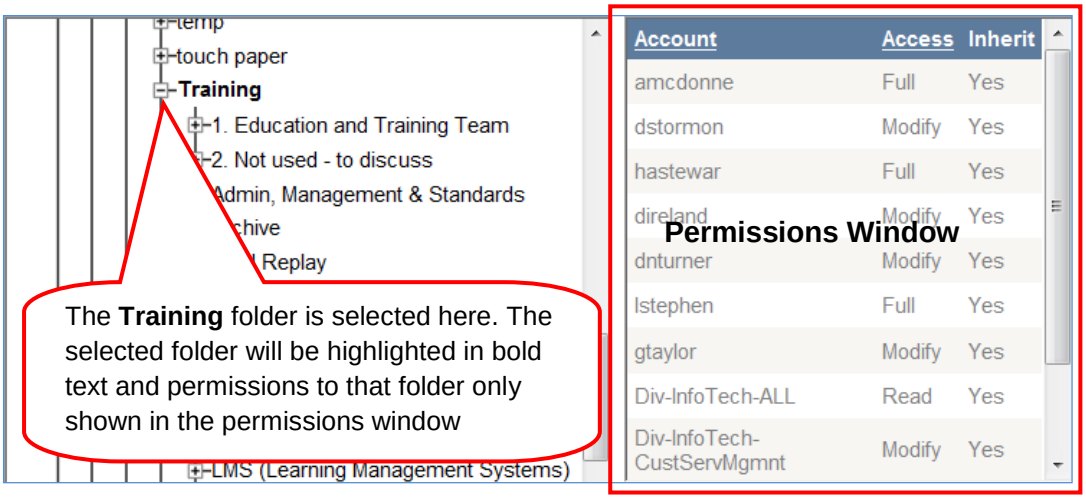
List access is granted to a user when they need access to higher order folder/s to navigate to a sub-folder where a file is located which they need to work with. This is common where staff need to access a file or folder in another department or business area.

Note – If you give a user list access, be aware that users can see the name of other files or folders as they navigate to the folder that they have access to. You should be careful of sensitive files or folder names that might be viewed.

You need to grant list access to all of the folders above the sub-folder for the staff member to gain access. You can then grant either modfiy or read access to the sub-folder that contains the files required.

Permissions Window

The **Permissions Window** is shown to the right of the Folder List on the SA Management Tool.



The Permissions Window displays a complete list of permissions applied to the folder you have selected in the folder list.

The access permission level granted to each of these users and groups is clearly displayed as well as any **inherited** permissions.

Once you have granted permissions you will need to click on **SAVE** in the Tasks window.

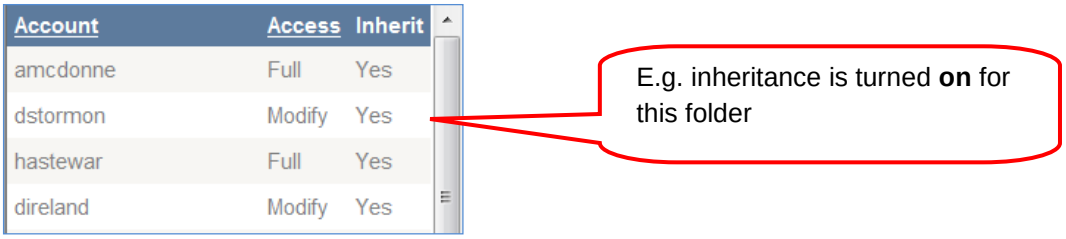
Inheritance

New folders have inheritance turned on by default. As the name implies, any child folders created under a parent folder will automatically inherit the permissions of their parent folder.

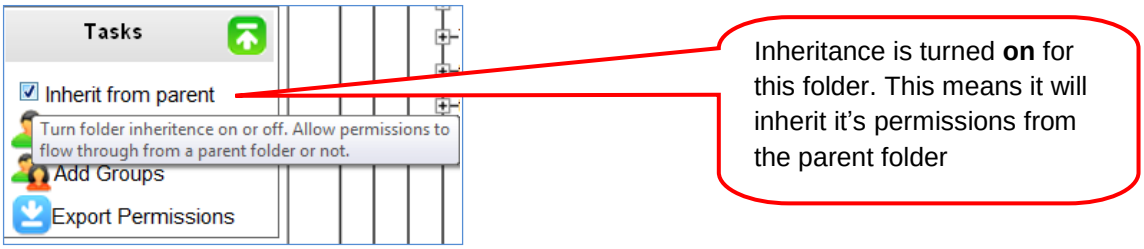
What does 'inherit' mean?

Under the '**Inherit**' list:

- If 'Yes' is displayed - permissions have been copied from the parent folder, and the user or group will have the same level permission as the parent folder
- If 'No' is displayed – the permissions for the parent folder will be different to the permissions shown for this folder for this user or group.



Inherit permissions can be turned **on** or **off** from the Tasks Window. This is done by selecting a folder in the Folder List and a user or group in the Permissions Window.



Breaking inheritance

Essentially, **breaking inheritance** means that you have un-ticked the '**Inherit from parent'** box. The permissions from the parent folder are copied to this folder but any changes you now make are independent to the parent folder and are only applied to the folder and its sub-folders. Examples of inherit permissions can include:

Example 1

Your business area has a main project folder that contains four sub folders for specific projects. Modify permission has been granted to the main project folder to 20 staff in your area. When each of the subfolders is created, all 20 staff by default will inherit the same access to all sub-folders.

If you have five specific team members working on each of the 4 projects and only want them to be able to access the folder they are involved with, you need to:

1. Navigate to one of the sub-folders under the main project folder in the Folder List and select the folder to display the Permissions Window for that folder
2. Un-tick '**Inherit from parent**' in the tasks window
3. Remove the 15 users who do not require access to this folder
   (**Note -** If the users with inherited permission to this folder are part of a group, you will need to remove the group and then add the five users that require access individually.)
4. Save your changes
5. Repeat for each sub-folder and ensure that only the five staff working on the project have modify access

Example 2

Your department has a current project which involves a number of staff members from other departments within the University. You have a folder within your S drive structure which contains all documentation relating to the project. There are four staff from your department, four from Human Resources (HR) and two from Division of Facilities Management (DFM) who require access to the project folder.

To give the users access:

1. Navigate to the project folder in the Folder List and select the folder to display in the Permissions Window for the project folder
2. Un-tick '**Inherit from parent**' in the Tasks Window
3. Remove all the users and groups from your area who do not require access to the folder
4. Add the users from HR and DFM and grant all users in that folder either **read** or **modify** access as required
5. Select each of the parent folders above the folder and grant the users from HR and DFM list access to ensure they can navigate to the project folder
6. Save your changes

Managing Access Permissions for Users and Groups

A feature of the SA Management Tool is the ability to add user groups to folders. This can save time and provide easier management when you are working on updating the permissions of folders for multiple users. **DIT recommends groups as the most efficient way for you to manage S drive permissions**.

Groups are also known as '**Distribution Lists**'. You can add a distribution list from the MS Outlook Global Address list to your folders, thereby giving all members of that distribution list permission to that folder.

This means that by updating the membership of the distribution list you are also automatically updating the permissions for that group on the S drive.

If you have a new staff member starting work in your area and need to give them permissions on the S drive, add the new staff member to your department's distribution lists. This will also add them to the S drive folders to which that group has access. This is also useful when a staff member leaves - you can simply remove the user from the distribution lists, and thereby remove their access from all folders that list has access to.

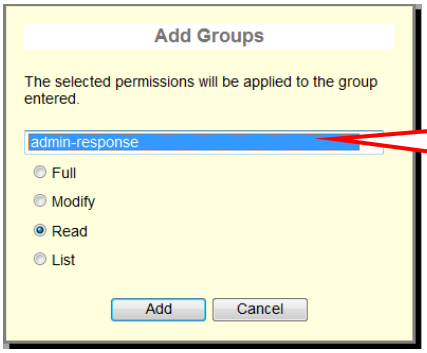
Note - when you add a distribution list to a folder in this manner, you are giving all members of the group the **same** permission level (e.g. modify, read, or list access)

Detailed information on distribution list administration is provided in the *Guidelines for Distribution List administration.pdf* in the Email and Calendar section at the following link. http://www.csu.edu.au/division/dit/staff/training/self-help/collaboration-and-communications

Granting Group Access

To grant permission for a group to access a folder:

1. Navigate to the folder in the Folder List where you wish to add the group
2. Select the folder to display the permissions window for the folder
3. In the Tasks Window select '**Add Groups**'
4. Select your group from the drop down list in the Add Group window. (The groups in the drop down list will mirror the distribution lists in the MS Outlook Global Address List).
5. Select the permission type you require from the options available
6. Click '**Add**'
7. Click **SAVE** in the Tasks window



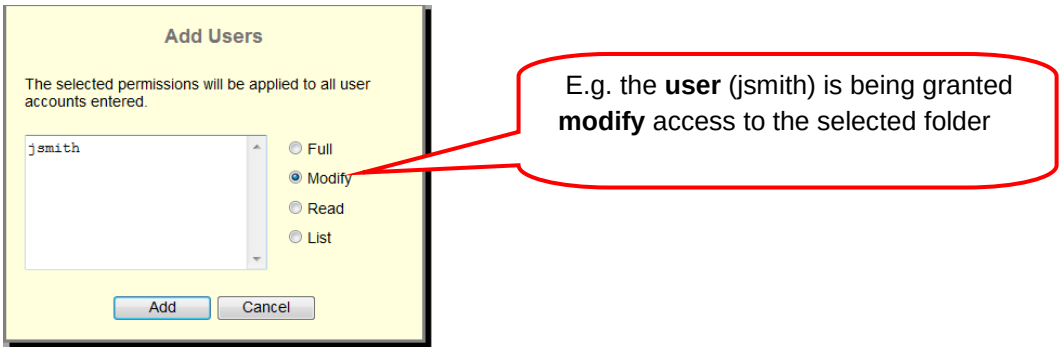
E.g. The admin-response distribution list is being granted r**ead** access to the selected folder

Granting User Access

To grant permission for a user to access a folder:

1. Navigate to the folder in the Folder List where you wish to add the user
2. Select the folder to display the permissions window for the folder
3. In the Tasks Window select '**Add User**'
4. Type the username in the Add Users text box

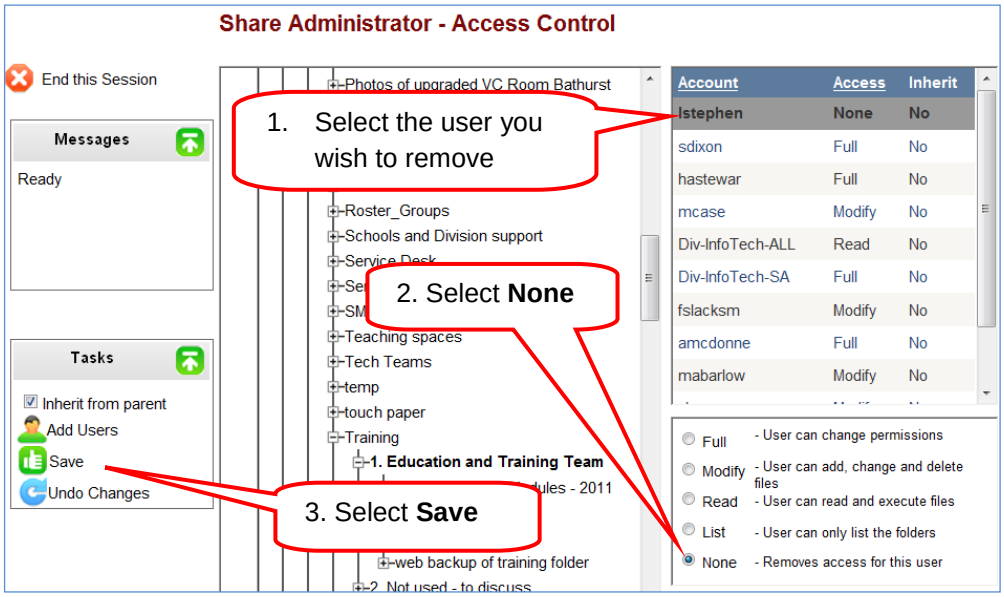
5. Select the permission type you require from the options available
6. Click '**Add**'
7. Click **SAVE** in the Tasks window



Remove User or Group Access

To remove permissions for a user or group to access a folder:

1. Navigate to the folder in the Folder List where you wish to remove the user
2. Select the folder to display the Permissions Window for the folder
3. In the Permissions Window, select the user or group you wish to remove
4. From the resulting options at the bottom of the Permissions Window, select '**None**'
5. Repeat the steps 2 and 3 if you wish to remove multiple users or groups
6. Select '**Save**' from the Tasks Window



Share Administrator Assistance

If you require assistance contact the DIT Service Desk.

http://www.csu.edu.au/division/dit/services/