

Factors to Consider when building your folder structure

- [Who will be creating the folders?](#)
- [Who will need access?](#)
- [Personal Folders](#)
- [Advanced Folder Settings](#)
- [Limitations](#)

Who will be creating the structure?

Short:

The ability to create root level folders is dictated by the employee permission 'Create root-level folders.' This permission is not for Admin users only. Employees with this permission will be able to create root level folders. To allocate this permission to an existing employee, navigate to 'People' - > 'Manage Employees' -> Select a user's profile -> Allocate permissions at the bottom of the screen under 'User Access'.

If a user is granted upload rights on a folder, they will have the ability to create subfolders within that folder.

[Employee Permissions](#)

TIP! If you are using the ShareFile User Management Tool to provision users directly from AD, you can allocate the 'Create root-level folders' permission to users at the time of group rule creation.

[ShareFile User Management Tool](#)

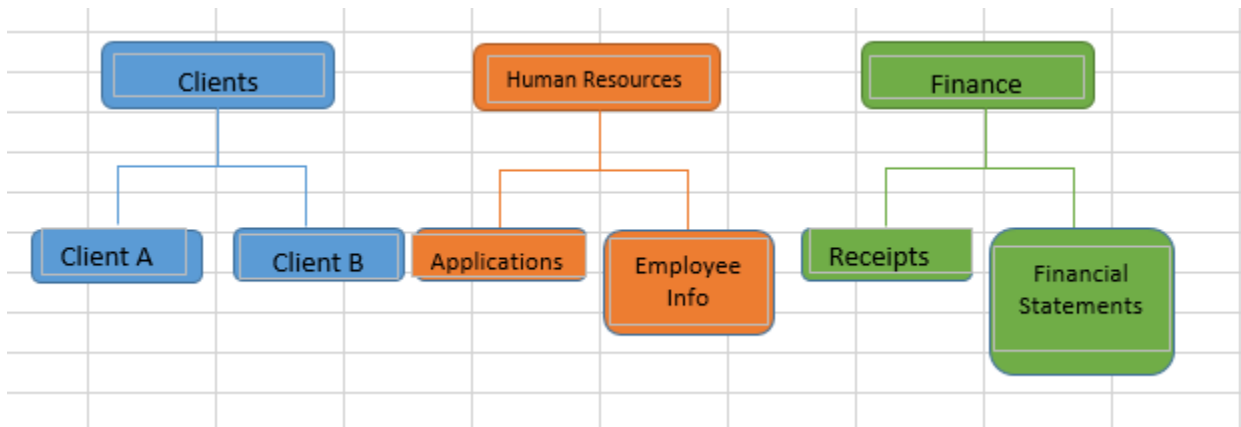
More info:

For planning purposes, it's best to think about your structure from the top down. This is due to ShareFile's enforcement of folder settings, user access, and permissions via a 'trickle down' or 'waterfall' policy. For example, a retention policy at the root-level will be enforced on all subfolders underneath the root. Same goes for folder access and permissions, newly created subfolders will always inherit the permissions of the folder above.

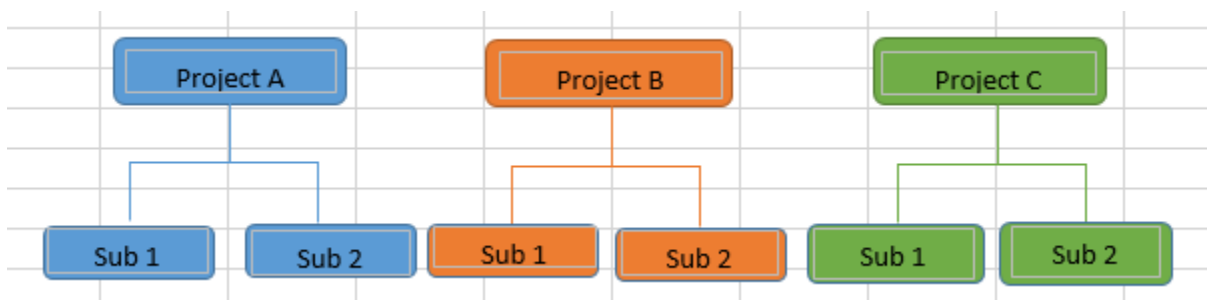
Two options to consider: Do you only allow IT Admins the ability to create a rigid root level folder structure? Or would you prefer giving end users the ability to build the structure organically?

The easiest way to answer this question is by understanding your use-case and how the highest level of the folder tree will be organized. Some of the common ShareFile root level folder structures include departmental folders and project folders- utilizing potentially different retention policies. Examples of each can be found below:

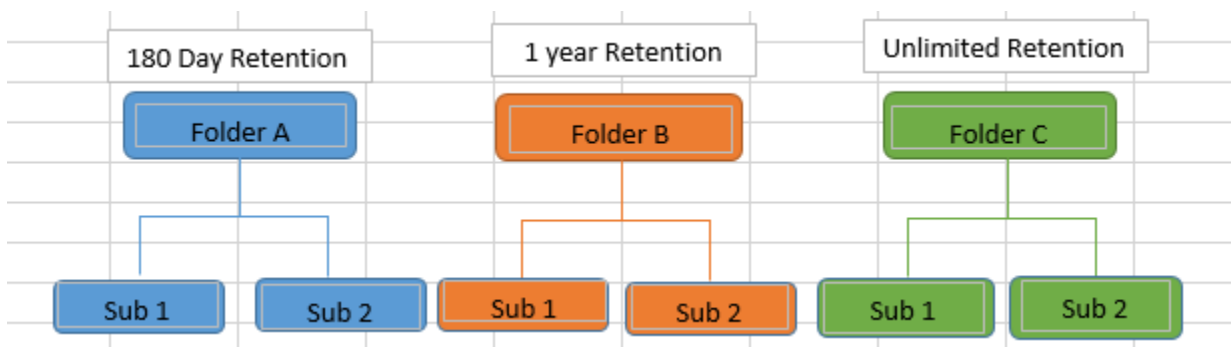
Graph – Departmental folders



Graph – Project folders



Graph – Retention Policy folders



*Before planning your folder structure, it is important to understand the role each ShareFile user will play in building out the tree. For retention policy, it is important to note that the root level retention policy will be enforced throughout all subfolders within that directory.

TIP! Dynamic Folder Templates are an easy way to ensure an organized, consistent folder structure across your ShareFile account. See the article below for more information:

[ShareFile Dynamic Folder Templates](#)

Who will need access?

Short:

Understanding who will be accessing the data in a folder structure is extremely important to the planning process. ShareFile allows for sharing folder access with both internal (employees) and external (clients) users. To share a folder with a user, you will need to be an admin user on the folder, or the creator. Simply navigate to that folder location -> Select the 'People on this Folder' tab -> 'Add People to Folder' -> Select the user and assign permissions -> 'Add'

[Add People to a Folder](#)

TIP! You can add users to a folder in bulk by utilizing distribution groups.

[ShareFile Distribution Groups](#)

More info:

The first step to evaluating folder access should be deciding if the folder tree will be client facing or internal only. We will look at each of these use-cases in more depth below:

Client Facing Structure

This structure assumes that clients will be given access to various folders throughout the tree. This is extremely common with ShareFile as it provides a secure, user-friendly environment for collaborating with various contacts on documents. One important setting that should be considered when building a client facing structure is the inherited folder permissions. As mentioned earlier, ShareFile will automatically apply permissions from the top level folder to new subfolders. This is important to communicate to users working in a client facing structure for the following reason:

Example: If you give a client access to their client folder in ShareFile, and one of your employees creates a new *Internal Only* folder within that structure, the client will need to be manually removed from the new *Internal Only* folder. Remember permissions trickle down from the top level folder, making sub-folders visible to everyone added at the level above.

Folder permissions also need consideration for external user access. ShareFile offers five primary folder options for Enterprise customers: View, Download, Upload, Delete, and Admin. More information on each option can be found in the link below:

[ShareFile Folder Permissions](#)

TIP! Be cautious when applying the 'Admin' permission to client users. This permission will allow the client to add various users to the folder location, delete files, change folder settings such as the 'Expiration Date', as well as remove various users from the folder location (except folder owner).

Worried about your employees granting clients the Admin permission? Take a look at our Access Report to review folder rights: [ShareFile Reporting](#)

Internal Only Structure

This structure assumes that only employees will have access to the Shared Folders stored inside of ShareFile. This use-case offers enhanced access to files on network drives/shares, easy collaboration on documents (workflow/co-editing), and greater tracking of edits, deletions, and sharing of files.

Access to various folders is often assigned by department, active projects, clients, or teams. As discussed earlier, the best way to manage employee permissions to folders is through distribution groups. With the help of our User Management tool, you're able to create distribution groups based on AD security groups, and apply these groups to various folder levels. Please reference the User Management Tool user guide below to learn more about this process:

[ShareFile User Management Tool Setup Guide](#)

Also consider permission sets throughout the various levels. Common deployments will allow Executives, IT Admins, and Managers 'Admin' access at the higher levels of the structure, while general end users will only have upload/download. As you move down the structure into more granular folders, these restrictions are generally relaxed to allow end users the ability to delete items or modify settings on folders that directly relate to their work. Also, for users that edit documents or move them through the folder directory, ShareFile offers tools to greatly enhance efficiency and end user experience. More information on efficiency tools:

[ShareFile Apps & Features](#)

Personal Folders

Short:

Personal Folders are automatically created for each Employee User at the time of provisioning. The user should reserve this location for private use and any folders in this location should not be shared with other users. Any folders that are going to be shared should be created or moved to the 'Shared Folders' area. By default, employees have the ability to upload and download files from this folder. They also will be able to create subfolders and add other users to those subfolders with desired permissions.

More Info:

Personal Folders are enabled by default on all accounts, but can be disabled to meet a specific use-case or rigid deployment of the ShareFile solution. However, it is best practice to keep these

folders enabled as it allows employees the ability to edit and save documents in a personal location without the need to share files until they're ready.

Furthermore, understanding the presence of each employee's Personal Folders, as well as their ability to be shared out (as mentioned above, this is not recommended, but possible), can alter the way that you view the Shared Folders structure. For example, some use-cases require employees to have full autonomy over their folders. This not only reduces the workload on IT to prepare a defined structure, it also allows the employee to assume full responsibility over how folders/files are shared. In this scenario, employee users work solely out of their Personal Folders where they can create a personalized folder tree with varied access and permission sets based on need.

Conversely, other use cases might require full IT control over folder creation, folder access, and permissions. This deployment would require disabling Personal Folders entirely and forcing employees to work within the defined folder structure as set by IT.

***Please note that disabling Personal Folders should be decided prior to provisioning employee users.**

[ShareFile Personal Folders](#)

TIP! As an Admin, you can always view an employee's Personal Folder to ensure they are adhering to best practices and internal standards. This can be done navigating to:

'People' -> Manage Employees -> Select Profile -> 'View folders and activity logs' -> 'Access Personal Folder'

Advanced Folder Settings

Short:

As a ShareFile Admin, you have the ability to set account-wide folder defaults within the Admin Settings console. These settings will be applied to any net new root-level folders that are created within your account. However, Advanced Folder Settings allows folder Admins to override these defaults to apply custom policies on a per root-level folder basis. More information can be found in the following article:

[Create Folder & Advanced Folder Options](#)

More Info:

To access the Advanced Folder Settings, navigate to the desired folder and hover over 'More Options' next to the folder name. Once the drop-down menu appears, select 'Edit Advanced Folder Settings'. Below is an overview of the options that are available and best practices for using each:

Folder Expiration Date:


This option allows an Admin to create a 'self-destruct' date for the folder and all of the contents within. **It is important to note that all files and folders deleted per a Folder Expiration Date are completely purged from ShareFile and cannot be recovered.**

File Retention Policy:

The File Retention Policy determines how long files are retained within that folder. This applies to all files in the root level, as well as within the subfolders. Adjusting the retention policy to a shorter period of time will take immediate effect. However, if the new policy is shorter than an existing file's upload date, the file will inherit a 7 day warning.

As with the Folder Expiration Date, all files purged per a retention policy cannot be retrieved.

File Versioning:

File versioning allows you to hold previous revisions of a file after the file has been changed or updated. When a new copy of a file is uploaded, the older version will be kept available for download. A blue paper icon  will appear on the same line as the file name to access any previous versions.

Unlike the Expiration and Retention policies, File Versioning can be configured with different policies at the root-level vs. individual subfolder levels.

Sort Order:

Files can be sorted by clicking on any header within the folder. The options are by Title, Mb, Uploaded date, or Creator. The options in Advanced Folder Settings allows you to mandate a default sort order for that particular folder.

StorageZone:

This drop-down menu determines where the data is hosted for Enterprise customers. If an on-premise StorageZone has been configured, it will appear when the folder creator or Admin selects the down arrow. **Please note that updating this field will cause all files to be transferred from the current Zone to the new Target.**

TIP! By default, a user given Admin rights at the root-folder level has the ability to adjust the retention policy on that folder (and therefore all subfolders beneath). However, ShareFile offers a setting that can be enabled by ShareFile Support that only allows employee users with 'Modify account-wide settings' to adjust folder retention policies via Advanced Folder Settings.

Limitations

Although ShareFile does not provide defined parameters regarding folder size, depth, or number of items allowed, the following best practices will ensure optimal performance.

File Path Limit

ShareFile recommends adhering to Microsoft File Path limitations by avoiding path names that exceed 250 characters. Shorten paths by renaming folders and files or moving deep lying folders higher up the tree. This is extremely pertinent if you are planning on deploying the ShareFile Sync for Windows application.

Horizontal not Vertical

As mentioned earlier, it is best practice to keep your folder structure spread wide at either the root level or the second level down. This will prevent a narrow, deep structure from evolving that can cause a poor user experience and strain the ShareFile system. This is linked to the number of calls required when adjusting folder settings, user access, and account wide policies. Furthermore, users will lose productivity if they're required to click through a deep folder tree to access documents.

Limit items in each folder

ShareFile folders should not contain more than 5,000 items within an individual folder. Exceeding this limit will result in slow folder load times and possible time-outs with the Web Application. It is important to note that ShareFile will utilize 'pagination' when the number of items within a folder exceeds 250. This means that users will need to select 'Show more' when attempting to view items 251-500 within a given folder, and again to view 501-750, etc...