Managing Data Permissions

Virtual Desktop Service

Toby vanRoojen
December 02, 2020

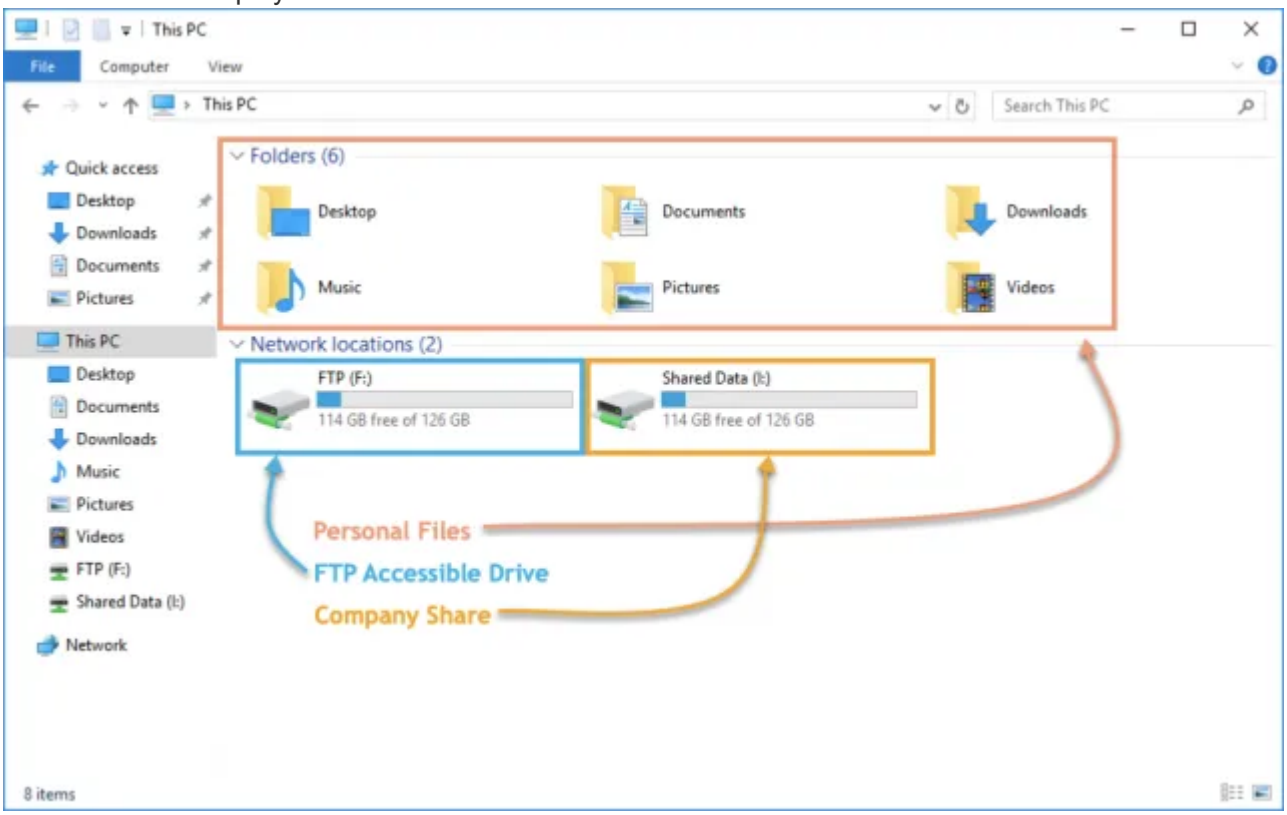
Table of Contents

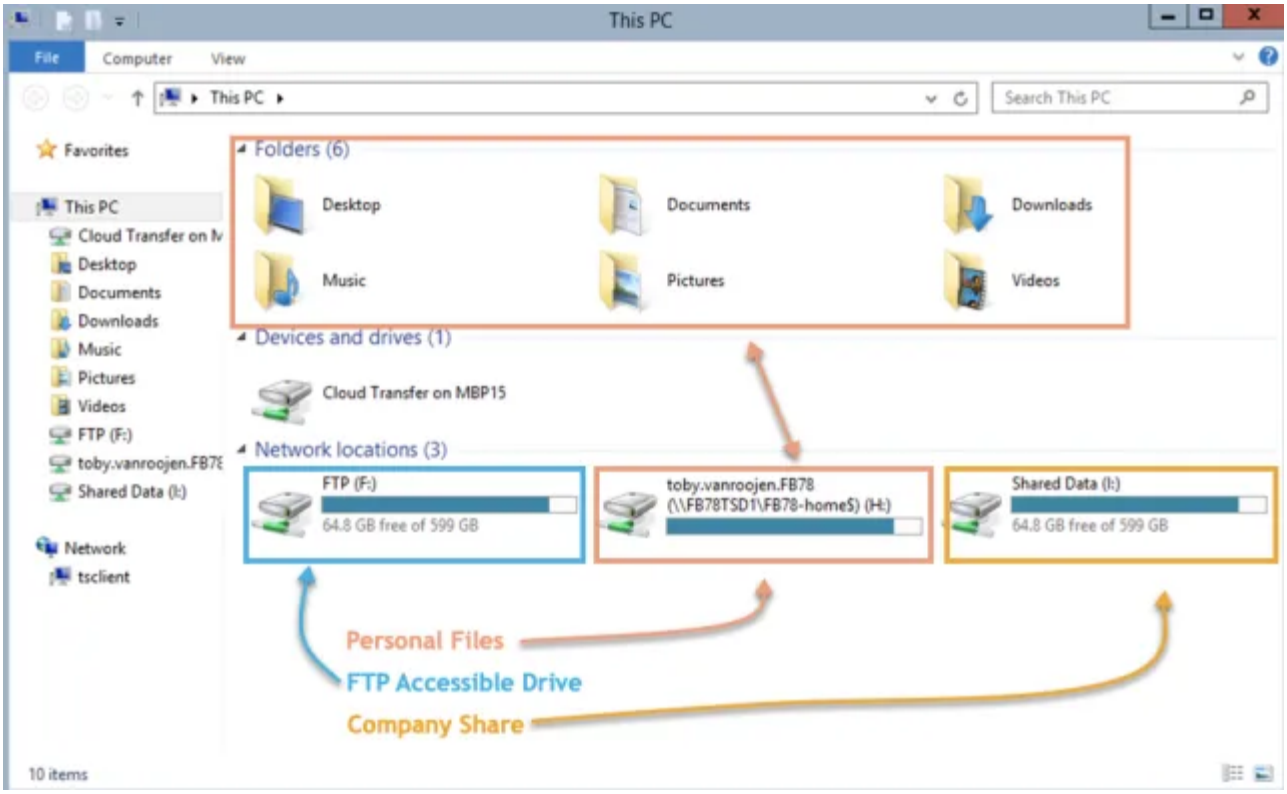
Managing Data Permissions

End user perspective

Virtual Desktop end users can have access to several mapped drives. These drives includes an FTPs accessible team share, a Company File Share and their Home drive (for their documents, desktop, etc…) . All of these mapped drives reference back to a central storage layer on either a storage services (such as Azure NetApp Files) or on a file server VM.

Depending on the configuration the user may of may not have the H: or F: drives exposed, they may only see their Desktop, Documents, etc… folders. Additionally, different Drive letters are occasionally set by the VDS administrator at deployment.





Managing permissions

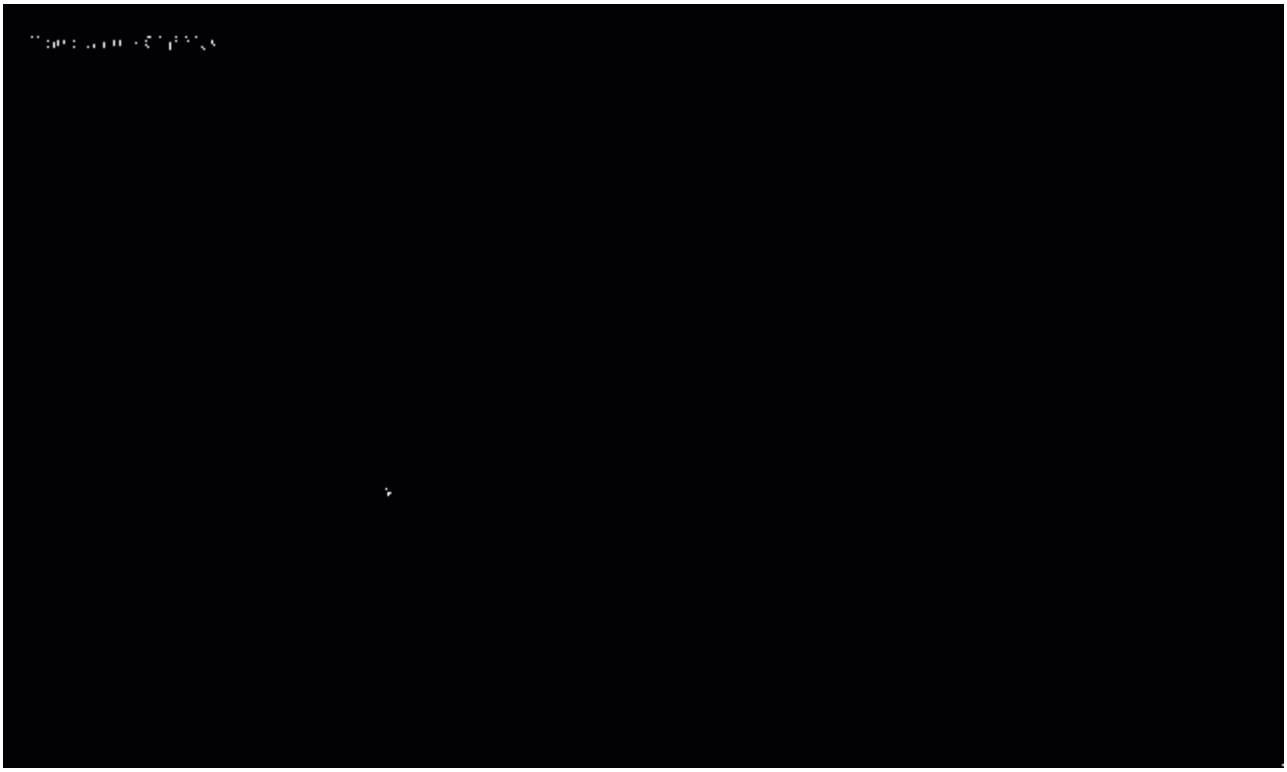
VDS allows admins to edit security groups and folder permissions, all from within the VDS portal.

Security groups

Security groups are managed by clicking: Workspaces > Tenant Name > Users & Groups > under the Groups Section

In this section you can:

1. Create new security groups
2. Add/Remove users to the groups
3. Assign applications to groups
4. Enable/Disable Local Drive access to groups



Folder permissions

Folder Permissions are managed by clicking: Workspaces > Tenant Name > Manage (in the Folders section).

In this section you can:

1. Add/Delete Folders
2. Assign permissions to user or groups
3. Customize permissions to Read Only, Full Control & None