connected data

WHITE PAPER

Understanding Transporter Concepts

Contents

Introduction

Transporter is a private file sync and share appliance that allows businesses to deploy their own cloud service. It eliminates the privacy concerns, lack of control, and recurring costs of public cloud file sharing services like Box and Dropbox. It also gives corporate IT the ability to regain control over how their company's employees share sensitive company files when away from the office.

All Transporter products add value to an existing Network Attached Storage (NAS) environment with simplified file sharing. However, Transporter 75, 150 and 500 products have the additional capability of being able to integrate directly with an existing NAS or Windows-based storage system enabling mobile users to share and sync folders easily and without the need of a VPN. This means there's no need to bypass corporate security polices through unauthorized use of public cloud services like Box, Dropbox and Google Drive. While these capabilities present a huge advantage for both corporate executives and IT professionals, it also introduces several conceptual differences for experienced NAS administrators.

This white paper is intended for IT or storage professionals with experience in deploying and managing traditional file servers and NAS appliances. Readers of this paper will learn the conceptual differences between a traditional NAS file sharing appliance and Transporter. This knowledge is essential to quickly and efficiently configure and deploy a Transporter either as a standalone or integrated product in a traditional NAS environment.

Large organizations will benefit from using the Connected Data Transporter Directory Connector (TDC). TDC provides a NAS administrator the ability to leverage their organization's Active Directory user information to quickly populate Transporter for even faster deployment. For organizations requiring a higher level of Active Directory support, Connected Data has integrated Transporter 75, 150 and 500 with One Login, a leading single sign-on service.

Topics covered in this white paper include:

- Folder hierarchies
- Folder creation
- Assigning folder permissions
- Propagating group policy
- Active Directory integration
- NAS integration
- Sharing folders between NAS and Transporter

Definition of Terms

To ensure readers have the same understanding of common terms, the following definitions are provided and used throughout this document.

Organization

An Organization is a set of Transporter users who have one common administrator, the Organization Administrator. The Organization Administrator also referred to as the Org Admin invites and removes Organization Users. Both the Organization Administrator account and the Organization itself are created during setup of your first Transporter unit. Often, the Organization Administrator, Org Admin, and the Administrator are all the same person.

Administrator

The primary person in a business environment responsible for deploying and managing IT equipment. This person is often called on to resolve hardware and software problems, install updates, and generally help employees with their IT problems.

Organization User

A person invited to join an organization. Once the invitation is accepted, this user creates their own Transporter account and becomes a member of that organization. Accepting the invitation also grants folder sharing privileges within the organization. A user can also receive and accept invitations to other organizations. Once accepted, the user gains folder sharing privilege's for this organization in addition to previously accepted invitations.

Guest User

An individual that resides outside an organization who is invited by an Organization User to have shared access to specific files and folders. A guest user will need to establish an account on Transporter using the desktop application.

Folder Hierarchies

Traditional NAS Server: Administrator-driven Folder Hierarchy

A common practice within IT is to establish a set of guidelines or policies that govern the amount of storage provided to each application, department, and user. Based on these guidelines, IT administrators will then establish a folder framework on a storage system before adding it to an existing network. Once created, the folder structure will provide a persistent file/data storage target when it's made available to applications and users in a live production environment.

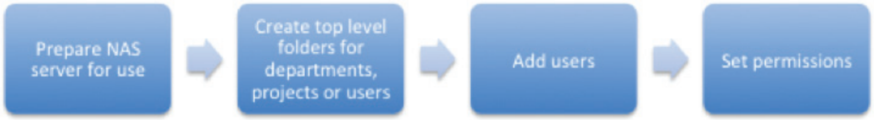
Traditionally, folder organization tends to be arranged in a hierarchy with a set of file sharing permissions. These can also be applied to subfolders before placing this new storage system into a live environment.

The underlying infrastructure that makes this possible is the directory service that's used to:

- Assign and enforce security policies based on a set of file/folder attributes
- Authenticate and authorize files and folders
- Determine whether a person is an administrator or a user with sufficient permissions/privileges to access a file, folder or subfolder
- Set read only or read/write access privileges

When a user requires access to a folder, a request must be made to the IT administrator to change permissions and grant access. Once a request is placed, there's often a lag time before access is granted depending on the administrator's workload, and the need to gain management approval.

Figure 1. Administration steps needed to prepare a NAS server for use.


Prepare NAS server for use
Create top level folders for departments, projects or users
Add users
Set permissions

Transporter: User-Driven Folder Hierarchy

By comparison, there's no top-level folder structure that needs to be created on a Transporter. An administrator simply deploys the Transporter on their network behind the firewall and starts by creating user accounts. Upon account creation, users will receive an invitation email instructing them to install the desktop application, much like they would for a public cloud service like Box or Dropbox.

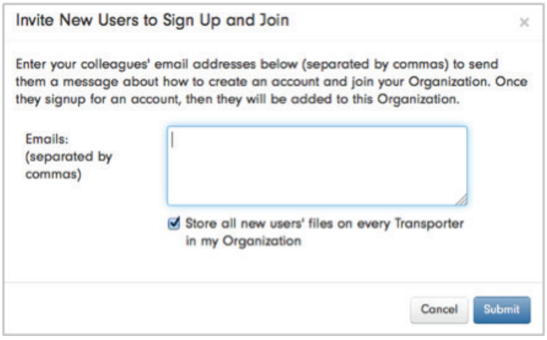
Once the user has installed the desktop application, they will see a newly created Transporter folder that looks just like a normal folder on their computer. Within this folder:

- Users create their own folder hierarchy
- Users then assign either read and write or read-only access privileges to other users

This is based on the level of access each user needs and the type of information stored. Users then invite others to share the folder and its contents once the invitation is accepted and the Transporter software is installed. Invited users will then have assigned privileges to all files and subfolders within the shared folder.

Therefore, responsibility for setting folder security and access privileges is undertaken by the users themselves. For example, a user may be a department manager who only invites their team to share the folder. Accepting this invitation establishes access and sharing privileges for members of their department. However, no one else will have access to the folder or even know that it exists.

Figure 2. This administrator screen invites team members into an organization.



Invite New Users to Sign Up and Join

Enter your colleagues' email addresses below (separated by commas) to send them a message about how to create an account and join your Organization. Once they signup for an account, then they will be added to this Organization.

Emails: (separated by commas)

☑ Store all new users' files on every Transporter in my Organization

This new file sync and share methodology was invented by public cloud file sharing services like Dropbox, but can be applied and deployed on private appliances like Transporter. The philosophies and concepts behind this new type of file sync and share approach have many advantages over a traditional storage system:

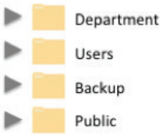
- Administrative effort required to deploy a file sharing solution is dramatically reduced, allowing IT staff to focus on higher value work that is more strategic or initiative based
- Users can now self-organize the folders and subfolders using a method that makes sense to them, reducing time spent searching for files and improving productivity
- Users set and modify access privileges to their shared folders based on individual needs or corporate policies
- Users can access files from anywhere, and on any device without the need for complex and expensive VPNs
- Files are automatically synced between devices to ensure everyone is sharing the most recent versions
- Automated, real-time syncing protects files from common issues such as hard drive failure
- Incremental capacity can be added quickly and efficiently without adding complexity
- Versioning and undelete features common with the new approach add further protection against accidental modification or deletion in collaborative environments

Folder Creation

NAS

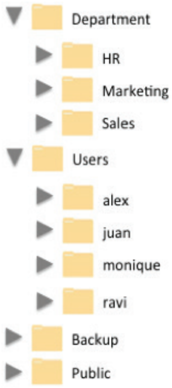
When deploying a new file server or NAS system, most administrators will start with a disk or volume that has no files or data. They will then define the folder structure best suited to their organization. Often these top-level folders are organized by department name, department function, public/shared information, user base, or something specific to the business.

Figure 3. An example of a top-level folder layout a NAS administrator may create.



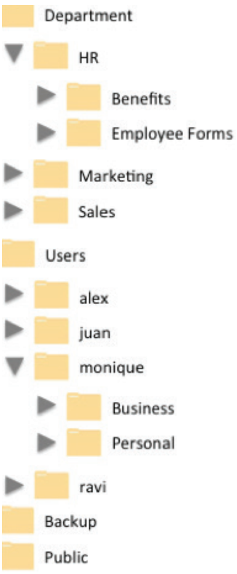
Once the top-level folder structure is created, a NAS administrator will then create subfolders. Often a company's departments will be listed by name and users will be listed by their alias'.

Figure 4. Illustrates how a NAS administrator could create and maintain department and user subfolders.



Once subfolders are created, the NAS administrator will most likely consider this part of the NAS setup to be complete. It's expected that members of each department responsible for a subfolder will then create additional nested folders and populate these using an established set of rules.

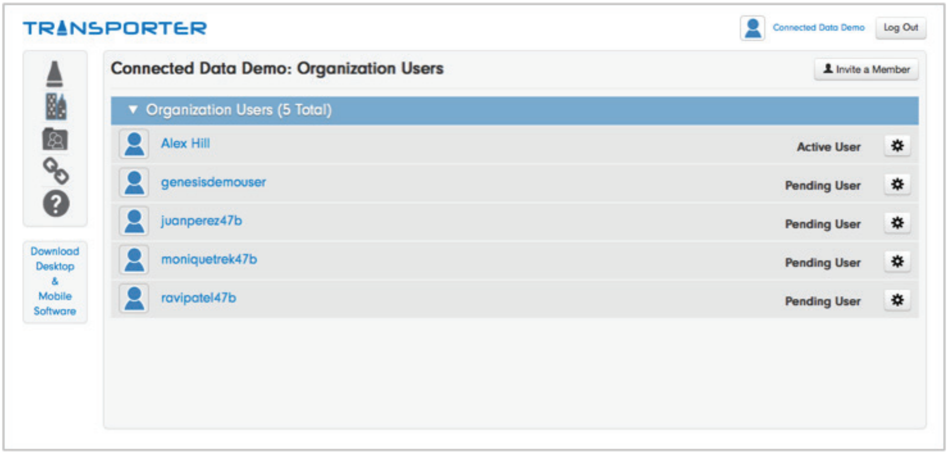
Figure 5. Diagrams how an in-use NAS file system may look.



Transporter

Like NAS, most Transporter administrators will start with a clean disk or volume. However, Transporter doesn't require the top-level folders usually established on a NAS volume. Instead, they start by inviting employees to the Transporter but to expedite the initial setup process, we provide an Active Directory connector. In business, this connector provides Transporter with all the information necessary to identify and prepare the system for its users. Users then create an account on Transporter as part of the onboarding process and then they start creating folders and inviting others to share the contents of these new folders. This approach is called self organization.

Figure 6. Highlights an administrator's screen after invitations were sent to several users. In this example, Alex has accepted the invitation, created his account, and assigned himself the username "Alex Hill". All other users are referenced by their email alias, this will change once the invitation is accepted and an account is created.



Connected Data Demo: Organization Users

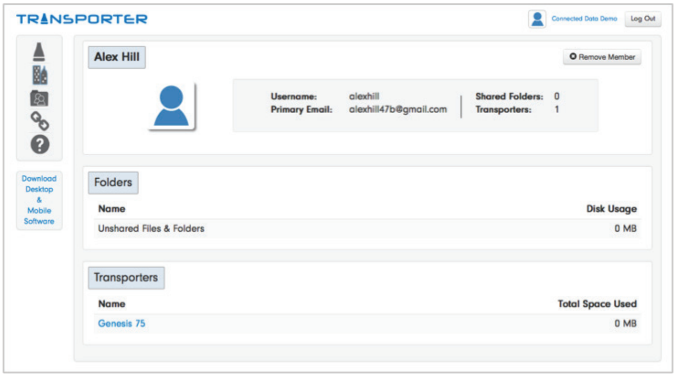
▼ Organization Users (5 Total)

Alex Hill	Active User
genesisdemouser	Pending User
juanperez47b	Pending User
moniquetrek47b	Pending User
ravipatel47b	Pending User

Unlike NAS systems that tend to have very deep hierarchal file systems, Transporter was designed to have a flatter, easier to use folder structure. Instead of going deeper and deeper to find a file or folder, Transporter user's create more high-level folders using a naming convention that's logical for their environment. By issuing member invitations, the contents of these new folders can then be shared (refer below for a more detailed discussion of sharing permissions).

It should be noted that in environments with multiple Transporters, the administrator assigns where a user's data resides. Once a folder is shared, Transporter's default status is that a shared folder can be located on any Transporter within the organization. However, an administrator can increase or decrease capacity based on the business requirements.

Figure 7. This is the administrator's view of Alex's user account and illustrates that Alex has accepted the invitation, he's ready to create, populate, and share folders by inviting other members.



Alex Hill

Username: alexhill
Primary Email: alexhill47b@gmail.com
Shared Folders: 0
Transporters: 1

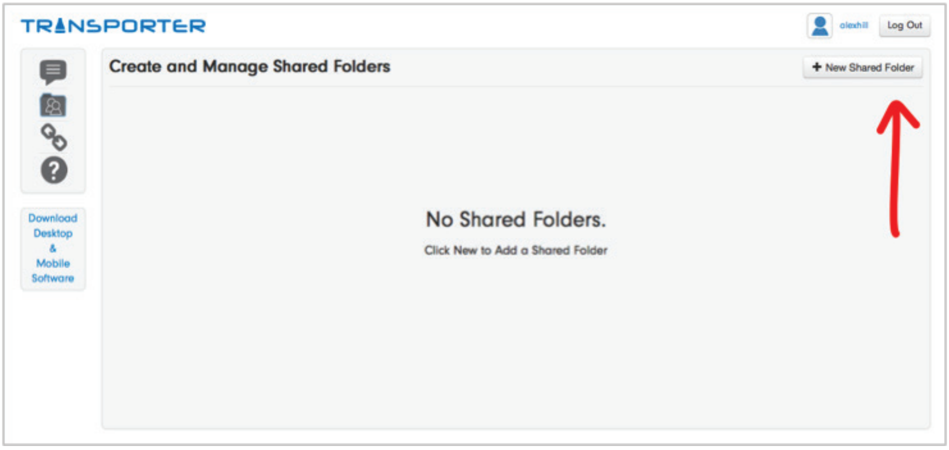
Folders

Name	Disk Usage
Unshared Files & Folders	0 MB

Transporters

Name	Total Space Used
Genesis 75	0 MB

Figure 8. As a user, this is the screen that Alex see's once his user account has been established. He is now ready to create, populate, and share folders by inviting other members.



Create and Manage Shared Folders

No Shared Folders.

Click New to Add a Shared Folder

Figure 9. As a user, this is the screen that Alex see's once his user account has been established. He is now ready to create, populate, and share folders by inviting other members.

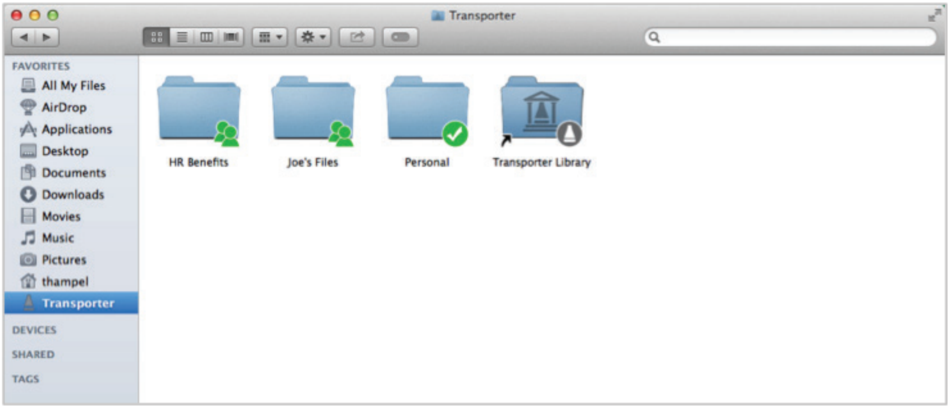
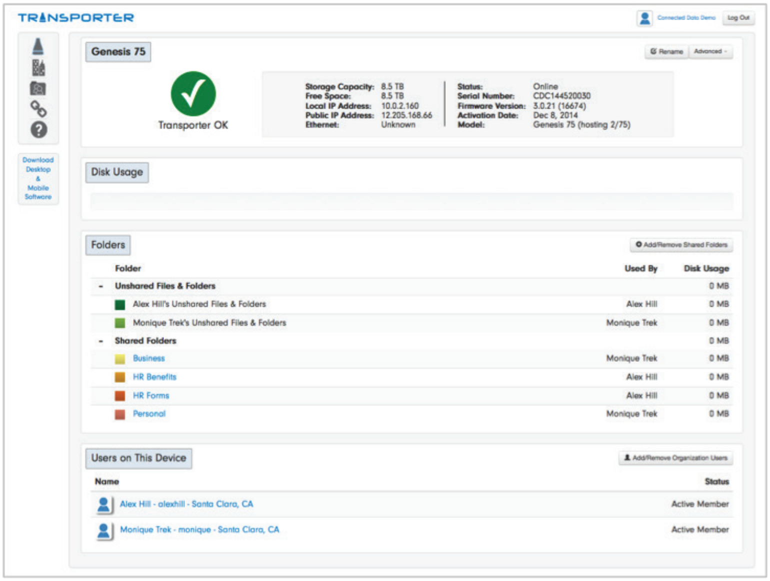


Figure 10. Demonstrates how a Transporter folder structure compares to one created on the NAS system. Note: due to space constraints this example isn't a complete comparison of folders and users.


TRANSPORTER
Connected Data Demo
Log Out
Rename
Advanced
Download Desktop & Mobile Software
Transporter OK
Add/Remove Shared Folders
Add/Remove Organization Users

Genesis 75

Storage Capacity:	8.5 TB	Status:	Online
Free Space:	8.5 TB	Serial Number:	CDC144520030
Local IP Address:	10.0.2.160	Firmware Version:	3.0.21 (16674)
Public IP Address:	12.205.168.66	Activation Date:	Dec 8, 2014
Ethernet:	Unknown	Model:	Genesis 75 (hosting 2/75)

Disk Usage

Folders

Folder	Used By	Disk Usage
- Unshared Files & Folders		0 MB
🟩 Alex Hill's Unshared Files & Folders	Alex Hill	0 MB
🟩 Monique Trek's Unshared Files & Folders	Monique Trek	0 MB
- Shared Folders		0 MB
🟨 Business	Monique Trek	0 MB
🟧 HR Benefits	Alex Hill	0 MB
🟥 HR Forms	Alex Hill	0 MB
🟥 Personal	Monique Trek	0 MB

Users on This Device

Name	Status
Alex Hill - alexhill - Santa Clara, CA	Active Member
Monique Trek - monique - Santa Clara, CA	Active Member

NAS Integration

Till now, this white paper has explained the conceptual differences creating folders on Transporter verses a traditional NAS system. Although Transporter can be deployed as a stand alone private cloud file sharing solution, it can also easily be integrated with an existing on-premise NAS file server. By mapping shares using the Transporter Network Storage Connector feature (standard on all rack mount Transporters), users will have the same level of access and security to designated NAS folders as they would to folders located on a stand-alone Transporter. This enables mobile users to access and sync files from these storage systems via Transporter without the need of a VPN.

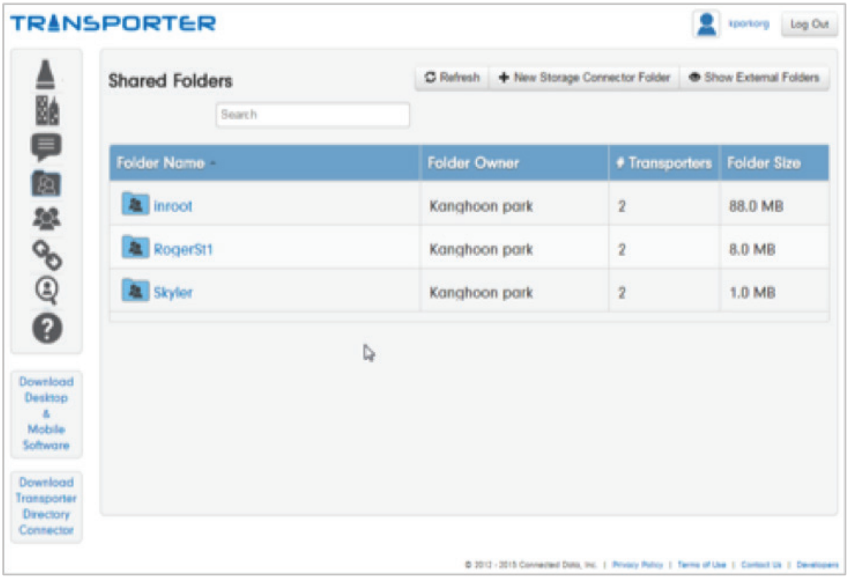
When paired with a NAS system, Transporter will bi-directionally and transparently sync with its paired NAS partner along with other Transporters that are moving data to where it's required. Any number of Transporters can be deployed and connected to as many NAS systems as required.

Transporter rack mount models 75, 150, and 500 have all the necessary features needed to integrate with on-premise storage systems located behind an organization's firewall. Integration candidates are storage systems that expose SMB/CIFS and run NetApp ONTAP 7, Microsoft Windows Server 2008 R2, or later. This type of integration provides many new sharing capabilities and is 100% non-disruptive with existing NAS systems and existing applications.

Path Creation

Once a rack mount Transporter has been deployed the NAS Administrator will establish a path between Transporter and the folders located on each NAS system. The folder and its contents will then be replicated on Transporter. As files located on Transporter are modified they will then be synchronized with the same files located on the NAS system and visa versa. In the event there's a conflict, where the same file is updated at exactly the same moment in both locations, priority will be given to the file on the NAS system and the file on Transporter will be saved with a new version number. This method ensures that both sets of edits are saved and available. Thus, edits to both files will be retained without being overwritten and can be accessed using the version number.

Figure 11. To create a path between storage systems the Administrator would select the "New Storage Connector Folder" tab using the administration screen shown below.

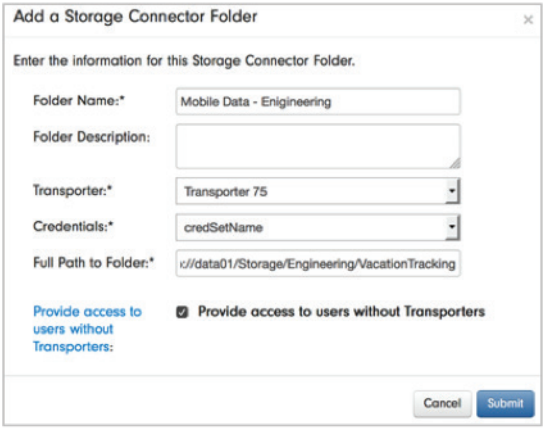

TRANSPORTER
Log Out
Refresh
New Storage Connector Folder
Show External Folders
Search
Download Desktop & Mobile Software
Download Transporter Directory Connector

Shared Folders

Folder Name	Folder Owner	# Transporters	Folder Size
inroot	Kanghoon park	2	88.0 MB
RogerSt1	Kanghoon park	2	8.0 MB
Skyler	Kanghoon park	2	1.0 MB

© 2012 - 2015 Connected Data, Inc. | Privacy Policy | Terms of Use | Contact Us | Developers

Figure 12. Once selected the dialog box below will appear. It enables the Administrator to link a rack mount Transporter with the identified NAS folder creating a path between both systems.



Add a Storage Connector Folder

Enter the information for this Storage Connector Folder.

Folder Name:*	Mobile Data - Enigineering
Folder Description:	
Transporter:*	Transporter 75
Credentials:*	credSetName
Full Path to Folder:*	://data01/Storage/Engineering/VacationTracking
Provide access to users without Transporters:	☑ Provide access to users without Transporters

The Administrator then enters the folder name, selects the Transporter to locate a copy of the folder (including its contents), its credentials, file system path, and clicks the submit button. Once completed, a folder is created on the designated Transporter and a copy of the NAS folder's contents is then added to the folder. Now the folder is ready to be shared with organization and/or guest users via the same email invitation method described above. Now users have the same level of access to files and folders located on their NAS system (VPN access no longer needed) as they would to files and folders only located on Transporter.

Should users need access to folders located on the same or other NAS systems, the Administrator would simply repeat the steps outlined in this section using a different path name. This method quickly enables mobile users to access and modify files located in different folders on different NAS systems. Any edits or updates to these files will be automatically synchronized with the NAS system. In parallel, users can access and modify these same files directly on their NAS system, via the VPN, and their changes are automatically synchronized with Transporter. This type of replication and synchronization provides another level of redundancy should there be an equipment failure.

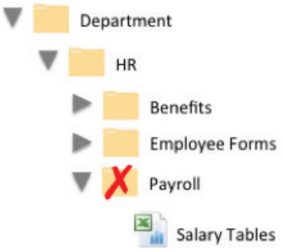
Assigning Folder Permissions

NAS

A common practice for NAS administrators setting up a NAS-based file system (folder structure), is to also set file/folder permissions. Once set, these permissions protect private information from being accessed by non-authorized individuals. Although visible, files and folders cannot be accessed by users that don't have access authority as set by the NAS administrator. NAS administrators often view the process of setting file/folder permissions to be cumbersome and time consuming. They would prefer to use this time on other, higher value tasks.

When using NAS, only the administrator can change the permission settings. Should a user want access to a folder, the user will submit an IT request that often has to be approved by one or more senior level people. Only after receiving these approvals will the administrator modify permissions to enable access. This process often frustrates users because they are facing a deadline and need immediate file/folder access to complete their work.

Figure 13. Here, an administrator has set Payroll folder permissions to prevent access and sharing with other users. A document such as a salary spreadsheet cannot be accessed, copied, or moved between unauthorized users. Authorized users can access this and other HR files and subfolders.



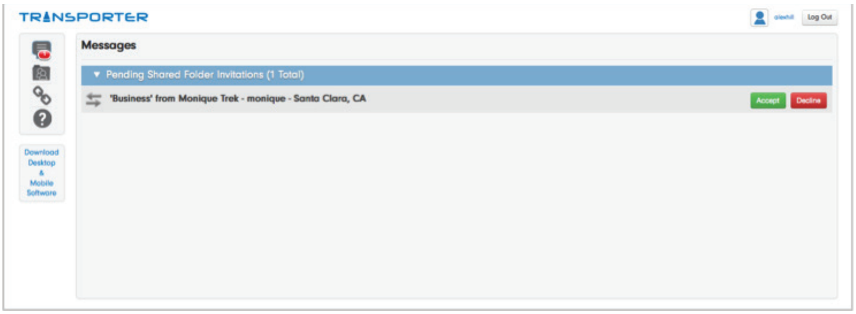
Department
HR
Benefits
Employee Forms
Payroll
Salary Tables

Transporter

By contrast to the NAS storage solution, the administrator is no longer responsible for establishing and managing folder permissions. Instead the administrator simply invites users or department managers to create accounts on Transporter. It then becomes the responsibility of these department managers to create their departments' folders.

Once created, the department manager would set permissions for each folder based on the function of their team and/or user by issuing invitations to share folders. It's no longer the responsibility of the NAS administrator to change file system permissions. In fact, the administrator is now free to perform other, higher value tasks.

Figure 14. Monique wants to share her "Business" folder with Alex, her invitation is now waiting to be accepted or declined in his messages icon. Once accepted, he will have access to her "Business" folder.



TRANSPORTER
alexhill Log Out
Download Desktop & Mobile Software

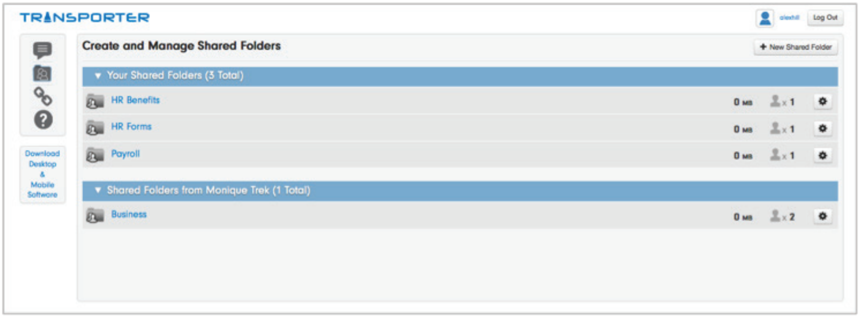
Messages

▼ Pending Shared Folder Invitations (1 Total)

'Business' from Monique Trek - monique - Santa Clara, CA Accept Decline

As Alex sets up and populates his folders, he's also thinking about which folders he needs to share. As the HR manager he understands that he needs to share the "Benefits" and "Forms" folders, and that he needs to keep employee compensation private. He creates a "Payroll" folder but doesn't invite anyone to share its contents which makes it a private folder.

Figure 15. Illustrates Alex's folders after accepting Monique's invitation. Although the "Payroll" folder is displayed as a shared folder, it's actually not visible to anyone else because he didn't send invitations (refer to the next figure).



TRANSPORTER
alexhill Log Out
Download Desktop & Mobile Software

Create and Manage Shared Folders + New Shared Folder

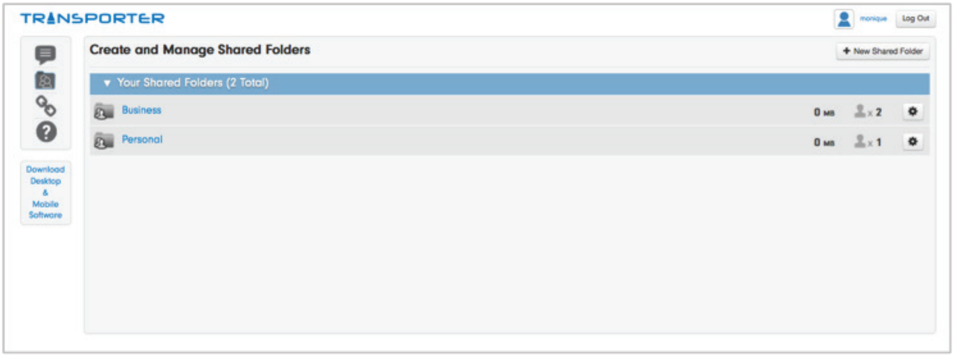
▼ Your Shared Folders (3 Total)

HR Benefits 0 MB x 1
HR Forms 0 MB x 1
Payroll 0 MB x 1

▼ Shared Folders from Monique Trek (1 Total)

Business 0 MB x 2

Figure 16. Because Alex didn't send an invitation to share, Monique doesn't see Alex's "Payroll" folder.



Create and Manage Shared Folders

▼ Your Shared Folders (2 Total)

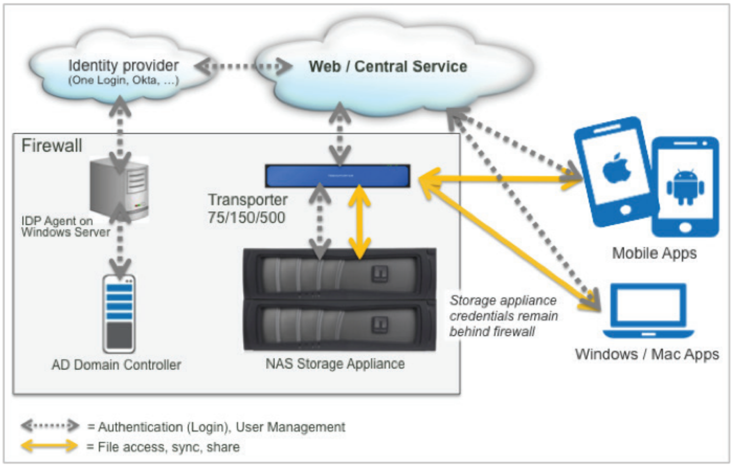
Business	0 MB	x 2	⚙
Personal	0 MB	x 1	⚙

Active Directory Integration

Earlier, we discussed the initial setup process could be expedited using Transporter's Active Directory (AD) connector because it provides Transporter with all the information necessary to identify and prepare the system for its users. Once an Administrator has performed the initial Transporter setup, users then create an account on Transporter as part of the onboarding process. On completion, they create folders and invite others to share the contents of these new folders.

However, Administrators in larger organizations may desire a higher level of integration between AD and Transporter to use already established AD settings to provision and de-provision user accounts on their deployed Transporter. These capabilities can only be implemented on a clean Transporter that has no files or assigned users.

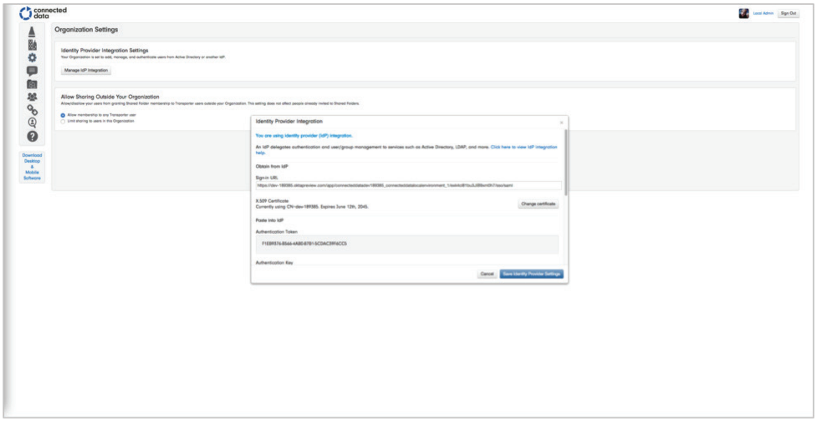
Figure 17. Illustrates the AD integration topology behind an organization's firewall.



To integrate AD with Transporter, the organization will already have deployed an AD Domain Controller that's usually located on a data center server. An Identity Provider Agent is also deployed on the same Windows server as AD. The identity provider enables single sign-on and one of the best known identity providers is One Login which is also used by Transporter. Once deployed in the cloud, the identity provider integrates with Transporter's Central Service to enable Transporter to track any changes to AD user login information.

Once established, this type of provisioning will automatically create a Transporter account for every AD listed user. This capability removes the need for users to create their own accounts when they accept the first invitation to share a folder and its contents. When an AD listed user is removed or their sharing status revised, Transporter will make the same adjustments. This form of de-provisioning will cause all downloaded files and folders to be remote wiped from a user's device without removing other personal data.

Figure 18. Shows an administrator screen performing the initial identity provider integration setup. This implementation enables all AD users to have membership with all Transporters located in this organization. However, it is also possible to limit membership to only designated Transporters. The overlay dialog box is used to enter the path to the AD server with the Identity Provider Agent. This screen is also used by the administrator to provide the authentication token.



Organization Settings

Identity Provider Integration Settings

Your Organization is set to add, manage, and authenticate users from Active Directory or another IdP.

Allow Sharing Outside Your Organization

Allow/disallow your users from granting Shared Folder membership to Transporter users outside your Organization. This setting does not affect people already invited to Shared Folders.

● Allow membership to any Transporter user
○ Limit sharing to users in this Organization

Identity Provider Integration

You are using identity provider (IdP) integration.

An IdP delegates authentication and user/group management to services such as Active Directory, LDAP, and more. Click here to view IdP integration help.

Obtain from IdP

Sign-in URL
https://dev-189385.oktapreview.com/app/connecteddatadev189385_connecteddatalocalenvironment_1/[illegible]/sso/saml

X.509 Certificate
Currently using CN=dev-189385. Expires June 12th, 2045.

Paste into IdP

Authentication Token
F1E89376-B566-4AB0-87B1-5CDAC39F6CC5

Authentication Key

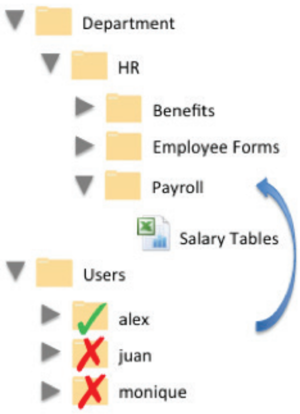
Propagating Group Policy

NAS

NAS administrators often establish hierarchical group policies. These enable a network administrator in charge of the directory services to implement specific configurations for users and computers. Group policies can also be used to define user, security, and networking policies at the machine level.

These policies help administrators define the networking options available to users – including the shared files, folders, and applications they can access. NAS administrators are familiar with these collections of user and computer settings, and often refer to them as Group Policy Objects (GPOs). Typically they are administered from a central interface called the Group Policy Management Console.

Figure 19. In this example, the NAS administrator has granted Alex, a member of the HR department, access to the payroll subfolder. To accomplish this level of cross department file sharing, Alex was made a member of this group policy. This gave him the necessary file sharing and access permissions. Alex could now make a copy of the Salary Tables spreadsheet, if allowed by the assigned group policies.



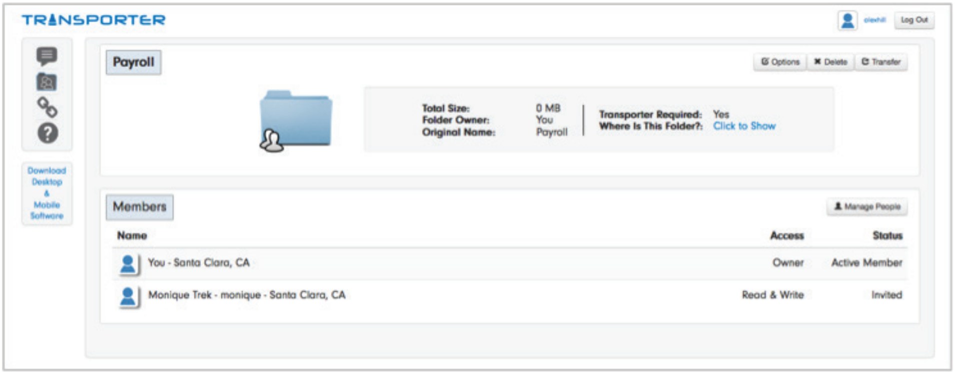
Transporter

In contrast to NAS, each folder on Transporter is created and owned by one user who sends invitations to other users. Acceptance of these invitations effectively creates a dedicated shared folder. Shared folders are independent of the administrator and can be reassigned and reused to save time and effort.

Every time an invitation is accepted, Transporter selects the device(s) on which to store a copy of the shared item. This occurs without any user input and is completely transparent.

Transporter delivers many benefits to an organization because the devices are independent of each other. For example, an administrator can remove a file or folder from a Transporter, or transfer shared folder ownership to another user. In other words, a shared file or folder can remain active even after its creator and original Transporter have both left the organization.

Figure 20. In this example, the NAS administrator has no involvement in setting group sharing permissions for the Payroll folder or any of its contents. In order to give Monique shared access to the Payroll folder and its contents, Alex, as the HR department manager sends an invitation to Monique. By accepting the invitation, Monique gained group access permissions for the shared Salary Tables spreadsheet located in the Payroll folder.



Payroll

Total Size: 0 MB
Folder Owner: You
Original Name: Payroll

Transporter Required: Yes
Where Is This Folder?: Click to Show

Members

Name	Access	Status
You - Santa Clara, CA	Owner	Active Member
Monique Trek - monique - Santa Clara, CA	Read & Write	Invited

Now, both Alex and Monique have access to the Salary Tables spreadsheet displayed in each of their respective folders. However, single instance storage features in Transporter will ensure there is only one copy of this file on each appliance, no matter how many member users share the file. This eliminates users making multiple copies of the same file, and avoids wasting valuable disk space.

In addition, member users can easily collaborate on projects by accessing the same files at the same time. Any edits made by one user would automatically be visible to other users in real time. File synchronization between collaborating users is just one of the many benefits of this architecture. However, some users may want to back track to an earlier version of a file. And, with Transporter that's not a problem because it maintains version control. Any authorized user can access an earlier version of a shared file.

Conclusion

With Transporter, IT has several new file sync and share deployment options because Transporter can:

- Coexist alongside a traditional NAS environment
- Integrate with traditional NAS systems and filers
- Replace traditional NAS systems
- Be deployed as an organization's primary storage

Transporter gives IT Administrators the type of integrated solution and deployment control they want. Its on-premise deployment model along with its peer-to-peer network, security tokens, syncing controls, and remote wipe capabilities make this one of the most secure file sync and share solutions on the market today.

In addition, Transporter's simplified file sharing and NAS integration capabilities eliminate the need for user's to break corporate IT policies by moving private files/folders to the public cloud. This higher level of data security helps safeguard a company's sensitive information from being unintentionally exposed. It also protects against legal exposure by helping organizations conform to corporate governance and government mandated industry regulations such as HIPAA.

You might think that all this privacy and security would make Transporter hard to use but that isn't the case, department managers and individual users have the necessary control and flexibility to establish a folder hierarchy that best suits their needs. These self management capabilities mean that Administration overhead is dramatically reduced to first time deployment, NAS integration, and data backup.

To recap, by offering the same file sync and share convenience of popular cloud services, Transporter solves the IT dilemma by delivering the cloud experience that employees want using private hardware appliances that companies own and control.