



**GroupDrive**

**GroupDrive Collaboration Server  
Using UNC Paths for Data Storage & Scalability  
Quick Start Guide**

## Notices

Copyright 2010 South River Technologies, Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement, OEM, or reseller agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of South River Technologies, Inc.

South River Technologies<sup>®</sup>, GroupDrive Collaboration Server<sup>®</sup>, Cornerstone MFT<sup>™</sup>, Titan FTP Server<sup>®</sup>, DMZedge Server<sup>™</sup>, and WebDrive<sup>®</sup> are trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP, and Windows Vista are trademarks of Microsoft Corporation, Inc. The names of other actual companies and products mentioned herein may be the trademarks of their respective owners. Any information in this document about compatible products or services should not be construed in any way to suggest SRT endorsement of that product or service.

South River Technologies, Inc.  
2635 Riva Road  
Suite 100  
Annapolis, Maryland 21401  
USA  
Telephone: 410-266-0667  
Fax: 410-266-1191  
[www.southrivertech.com](http://www.southrivertech.com)

**Please Note:** Some screens in this quick start guide contain options that do not pertain to UNC paths. For the purpose of this UNC path quick start guide, we will guide you through these options without configuring additional settings. If you need additional information regarding these steps, please see the [GroupDrive Administrator User's Guide](#). A complete listing of our Quick Start Guides is also available at our [Web site](#) and a listing of Frequently Asked Questions (FAQ) is available at our [Knowledgebase Support Center](#).

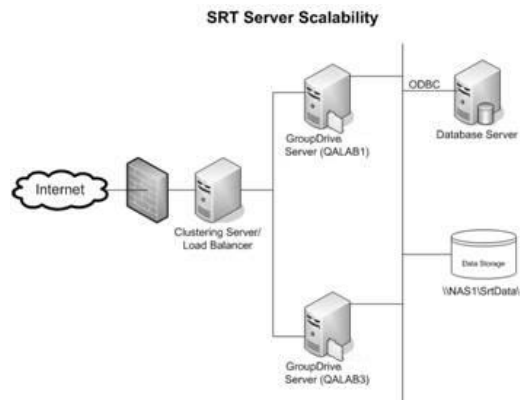
## UNC Paths—Overview

GroupDrive Collaboration Server supports a powerful feature that allows for the storage and access of data that is physically stored on any server in your network. Remote data is accessed by a public UNC (Universal/Uniform Naming Convention) that specifies the computer name, share name, and optional subdirectory where the data is stored. For example: a computer named **QALAB1**, has a shared folder called **SrtData**, and a subdirectory named **Cluster Test**. The UNC that references this location is:

```
\\QALAB1\SrtData\Cluster Test\
```

The main benefit to using UNC's to refer to data storage locations is scalability. GroupDrive Collaboration Server supports the ability to be deployed in a scalable environment, meaning that one or more servers can run in parallel and can access the same back end data storage to service the same front end clients.

If you intend to scale your GroupDrive Collaboration Server to multiple boxes, you need to configure the primary server so that all data files are accessed by UNC share rather than a local drive or a mapped network drive letter.



For illustration purposes, let's assume that you will have multiple GroupDrive Servers in your multi server cluster. QALAB1 is the primary/first Server that will be installed; QALAB3 will be backup server that will be added at a later date. In a multi-server environment, there are two scenarios, but both require the same configuration.

Scenario 1—User data will be stored on a local fixed disk, on the QALAB1 primary server box. Both QALAB1 and QALAB3 Servers will need access to the same data.

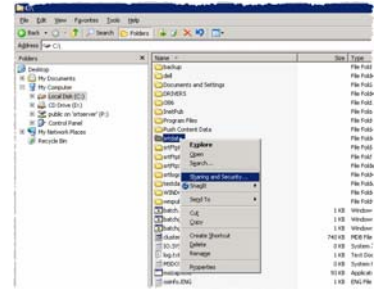
Scenario 2—User data will be stored on a remote/third box on the network, a box that is neither QALAB1 nor QALAB3. For example, Network Attached Storage (NAS1).

For either scenario, the configuration setup is basically the same.

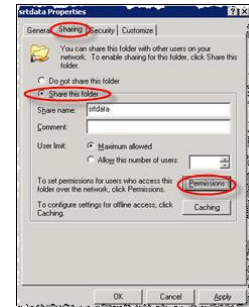
## Configuring the UNC

The UNC must be configured so that it can be accessed by the GroupDrive Server. This requires a UNC *share* and NTFS (NT File System) permissions adjustments to the folder where the data is stored.

1. Run **Windows Explorer** and locate the directory where data will be stored. For our example, all data is stored under **C:\SRTDATA\**. Right-click on the folder and select **Sharing and Security** from the pop-up menu. This will display the *UNC Sharing dialog* for the selected folder.

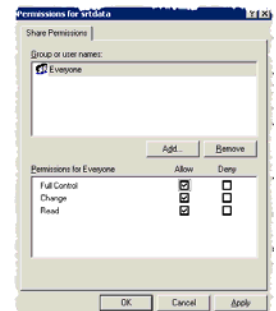


2. Select the **Sharing** tab and then select the **Share This Folder** radio button. When you are finished, click **Permissions**.



3. Update the **Permissions** on the share so that the GroupDrive servers will be able to access data on the share.\* Once you have properly set the permissions for the NTFS folder and share, click **OK**.

\*Incorrect permissions will prevent GroupDrive Server from being able to access the data. Typically the GroupDrive Service runs under the context of a special built-in Windows system account, such as *Local System* or *Local Service*. These built-in accounts do not have proper NTFS rights to access files stored on remote UNC's. There are two options: you can either grant full NTFS rights to all users that will allow GroupDrive Collaboration Server to gain access to the UNC, or you can create a special NT user account for the GroupDrive Server Service, and then add that special NT user account to the ACL (Access Control List) list for both the share and the underlying NTFS file system. (NOTE: the ACL for the *Share* is different than the ACL for the underlying folder on the NTFS drive.) After you create a special NT user account for the GroupDrive Collaboration Server, you must give that NT user account an *Access Control Entry (ACE)* for the underlying folder **and** an *ACE in the Access Control List (ACL)* for the Share so that the special NT user account can access the data on the UNC share.



See the [Appendix](#) for more information about creating a special NT User Account.

## Updating the User Data Directory

Once you have configured the UNC for access by the GroupDrive Collaboration Server, you can run the GroupDrive Collaboration Server *Administrator* and launch the **New Server Wizard** to [configure your server](#) or you can [reconfigure an existing server](#) to use the UNC instead of the local drive.

### Configure your GroupDrive Collaboration Server using the New Server Wizard

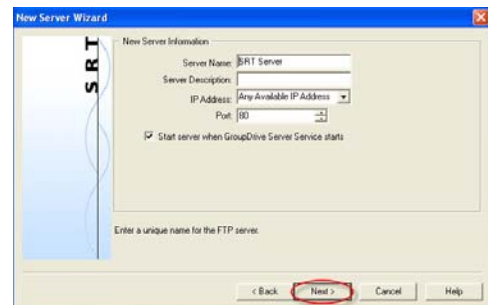
1. Run the GroupDrive *Administration Utility* and select **New Server Wizard**. The *New Server Wizard* will launch.



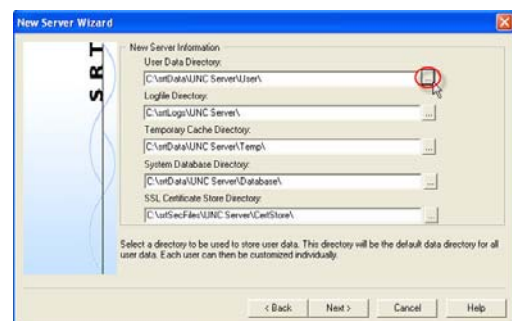
2. Select the **Server Type** (clustered or non-clustered).



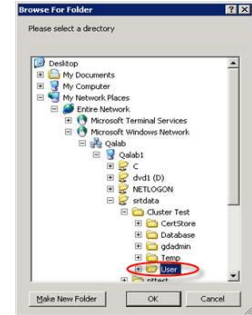
3. Type a unique **Server Name**. Type a **Server Description** (optional). Click the drop-down arrow to select your **IP Address**. (*Any available IP address* indicates that the server will listen on all IP addresses that are configured on the PC, along with the local IP address of 127.0.0.0, also known as *localhost*.) Select the **Port number** by using the up/down arrows. Click **Next**.



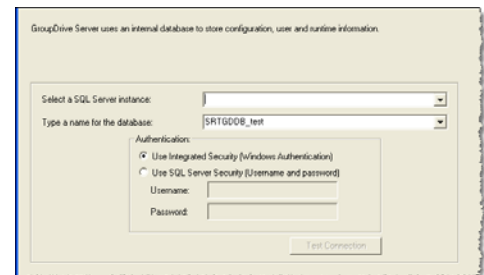
4. Click the **User Data Directory** browse "..." button to browse to the UNC.



- The *Browse for Folder* dialog box will appear. **Browse the Network Places** and find the computer name, share name, and folder where the GroupDrive Collaboration Server *User Data* will be stored. Click **OK**. You will be returned to the GroupDrive *New Server Wizard* to continue configuring your server.

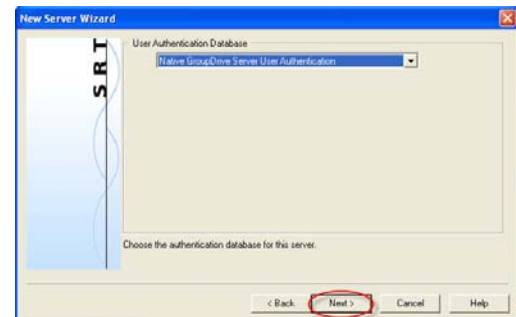


- GroupDrive uses an internal database to store configuration, user and runtime information. Use the drop-down arrow to select the **SQL Server instance**. Type the name of the **SQL database**. Select your **authentication method**. Click **Test Connection** to test the database connection to the GroupDrive server.



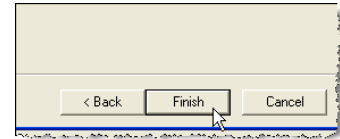
**NOTE:** SRT supports GroupDrive configurations using SQL Server 2005 or later or SQL Server 2005 Express or later, test or production environment. No other databases are supported.

- Select your **User Authentication Database** using the drop-down arrow. For our example we will use **Native GroupDrive Server User Authentication**. \* Click **Next**.

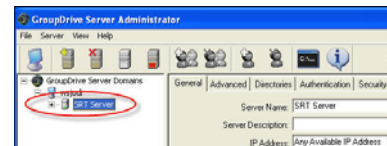


\*Once you select a User Authentication Database option in GroupDrive, you cannot change to a different method after the server wizard has completed. Use the drop-down arrow to select a different type of User Authentication. If you need more information about configuring user authentication, please see the [GroupDrive Administrator User's Guide](#) or the [SRT User Authentication Quick Start Guide](#) for your specific user authentication database.

8. The wizard will walk you through the steps for configuring your **SMTP Mail Server**. Click **Finish** to create the server.

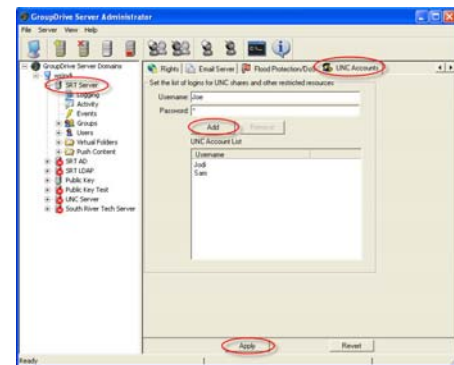


9. Once the server is created, the server starts and appears in the main GroupDrive *Administrator* window. A green icon appears to indicate that the server is running. You may now add users to the system.\*



\*For detailed information pertaining to these configuration options, see the [GroupDrive Collaboration Server Administrator User's Guide](#).

10. Select the **UNC Accounts** tab using the right/left arrows. The *UNC Accounts* tab is used to define a list of domain usernames and passwords that will be used for authentication when GroupDrive Server needs to access a remote *UNC share*.\* Type a **Username**. The Username can be simply a user name or **<username@domain>** or **<domain/username>**. Type a **Password**. The password will be used for authentication against the remote UNC share. Click **Add** to add the new Username/Password to the UNC Account List. Click **Apply**.

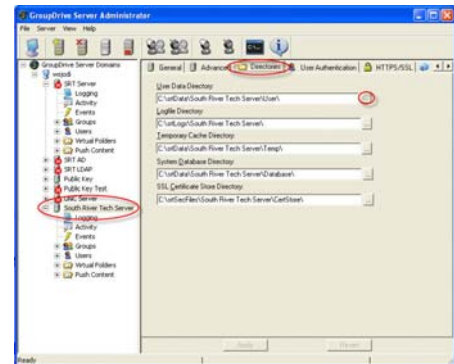


\*GroupDrive Service usually runs under the context of a *Local System NT Account* that is defined for the local PC; therefore, it does not normally have rights to access a UNC resource that is located on a remote server. When GroupDrive attempts to access a file/folder stored on a UNC share, it will attempt to connect/authenticate itself against the remote UNC by sending over a UNC user name and password along with the UNC. See the [Appendix](#) for information about creating a special NT account for GroupDrive Collaboration server.

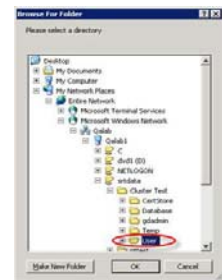
Your GroupDrive server is now configured using UNC paths for Data Storage and Scalability. Once the primary GroupDrive server has been configured to use UNC based data directories, you can install the GroupDrive server on additional nodes.

## Reconfiguring an Existing Server

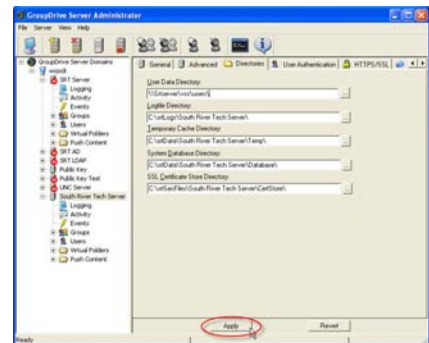
1. To reconfigure an existing server, select the **server** from the *GroupDrive Server Domains* menu tree. Use the left/right arrows to view the *Directories* tab. Click the “...” browse button to browse the **Network** places.



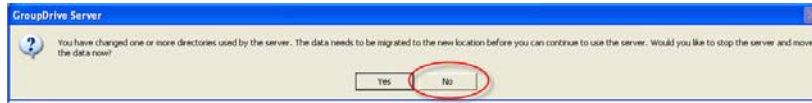
2. In the *Browse for Folder* window, browse the **Network** places to find the *computer name*, *share name*, and the *folder* where the GroupDrive *User Data* will be stored and then Click **OK**.



3. Click **Apply**.

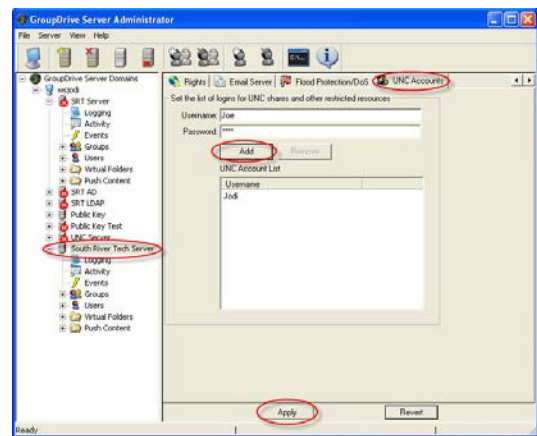


- GroupDrive will ask you if you would like to migrate the data. Click **NO**. If you did not change the *physical location* of the user data, **DO NOT** migrate the data.



\*If you change the *User Data Directory*, GroupDrive will internally update all Shares, Links, and ACLs that referenced that old location to reference the new location. It will also ask you if you would like to migrate all of your user data from the old location to the new location. If you did not change the physical location of the user data, **DO NOT** migrate the data. The reason you do not want to move the data is because the source and the destination are the *same physical location*. But if you tell GroupDrive to move the data, the data will be *moved* and not *copied* so the source data may be deleted.

- Select the **UNC Accounts tab** using the right/left arrows. The UNC Accounts tab is used to define a list of domain usernames and passwords that will be used for authentication when GroupDrive Server needs to access a remote UNC share.\* Type a **Username**. The Username can be simply a user name or `<username@domain>` or `<domain/username>`. Type a **Password**. The password will be used for authentication against the remote UNC share. Click **Add** to add the new Username/Password to the UNC Account List. Click **Apply**.



\*Since GroupDrive Service usually runs under the context of a *Local System NT Account* which is defined for the local PC, it does not normally have rights to access a UNC resource that is located on a remote server. When GroupDrive attempts to access a file/folder stored on a UNC share, it will attempt to connect/authenticate itself against the remote UNC by sending over a UNC user name and password along with the UNC. See the [Appendix](#) for information about creating a special NT account for GroupDrive Collaboration server.

Your GroupDrive server is now reconfigured using UNC paths for Data Storage and Scalability.

## Appendix—Create a Special NT Account

**File access rights** are required by the GroupDrive Server to access data. The GroupDrive Server Service typically runs under the context of the LocalSystem or LocalService account. In earlier versions of Windows, the LocalSystem and LocalService account had read/write permissions to the local file system. In later versions of Windows this is not always true. As the GroupDrive Administrator, you must ensure that the NT User Account being used by the GroupDrive Service has full read and write permission to all data directories used by the Server.

The key issue arises when the GroupDrive server is physically located on a separate box from the data that it will be accessing. Since the *LocalSystem* and *LocalService* accounts are local accounts, these accounts do not typically have adequate access to the UNC share containing the data. In this situation, the GroupDrive Administrator must create a special NT User account on the File Server that has read-write permissions to that data, and then configure the GroupDrive Service to use this domain account. This will ensure that the GroupDrive Service is running under the context of an account that has adequate rights to access the UNC namespace.

### Creating a special NT Account: \*

1. On the PDC, create a new domain user account and make note of the username and password. For our example, we will use *gdcsuser* as the username and *gdcpass* as the password. **NOTE: DO NOT USE THESE NAMES IN YOUR CONFIGURATION; USE SOMETHING VERY DIFFERENT TO PREVENT SOMEONE FROM POSSIBLY HACKING IN TO YOUR SYSTEM!**
2. Make *gdcsuser* a member of the *Domain Admins* and *Domain Users* groups.
3. Open the **Local Security Policy** applet on the **PDC** and under **Security Settings - > Local Policies -> User Rights Assignments** make sure that *gdcsuser* is granted the right to **Access Computer From The Network** and **Act As Part Of Operating System**.
4. Install GroupDrive Server on the PDC and restart the PDC. Open the GroupDrive *Service Manager* applet. The GroupDrive *Service Manager* applet is located in the Windows Control Panel, accessible from the Windows Start Menu under Settings -> Control Panel. Double-click on the *GroupDrive Service Manager* icon in the Windows Control Panel to launch the application. Scroll down to the **GroupDrive Server** service. Right-click on the **GroupDrive Server** service and select **Properties**.
5. Modify the **Log on As:** section so that the GroupDrive Server Service will logon using the *gdcsuser/gdcpass* account that was created.
6. **Stop** then **Restart** the GroupDrive Server Service. -Continued on next page.-

\*If you are going to use the GroupDrive *UNC Accounts* tab to specify a specific user name and password that will be used by GroupDrive to authenticate against the remote UNC, then you do not need to set the GroupDrive Service to run under the context of a special NT User Account. The *UNC Accounts* tab and the *Special NT User Account* are mutually exclusive.

Also, if you are using Windows NT/SAM Authentication or Windows Active Directory Authentication in GroupDrive and you select the *Impersonation* feature, you do not usually need to create a special NT User Account for the GroupDrive Service; nor will you usually need to use the UNC Accounts tab to specify additional user names and passwords for authentication.

The UNC Accounts feature gives the GroupDrive Service the ability to access UNC shares when standard GroupDrive Authentication, or some other non-NT (for example, Active Directory authentication) is used and the GroupDrive Service is running under the context of the standard LocalSystem account.

## **About South River Technologies**

South River Technologies (SRT) is an innovator in managed file transfer and document collaboration software. SRT's software seamlessly integrates access to remote files into the desktop applications that users rely on, creating an instantly familiar interface for collaborating, sharing, and accessing files. SRT's enterprise class server products are built using industry standard encryption, highly granular security configuration controls, and technologies to reduce the risk of network intrusions. Over 60,000 customers, including more than 70 colleges and universities, government agencies such as NASA and FAA and other blue chip companies in more than 110 countries rely on SRT's software to make remote file access and collaboration more efficient for their customers, partners, and distributed workforce. For more information, please visit [www.southrivertech.com](http://www.southrivertech.com).