



GroupDrive

**GroupDrive Collaboration Server
Windows NT Security Accounts Manager (SAM)
User Authentication Quick Start Guide**

February 2010

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[®], GroupDrive Collaboration Server[®], Cornerstone MFT[™], Titan FTP Server[®], DMZedge Server[™], and WebDrive[®], are trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP, and Windows Vista are registered 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

Please Note: Some screens in this instruction contain options that do not pertain to Windows NT SAM Authentication. If you need additional information regarding these steps, please see the [GroupDrive Administrator User's Guide](#). For the purpose of this Windows NT SAM User Authentication quick start guide we will guide you through these options without configuring additional settings.

GroupDrive NT SAM User Authentication—Overview

The following instructions will help you to set up GroupDrive Collaboration Server for user authentication with Microsoft Windows NT Security Accounts Manager (SAM). If you need additional assistance the [GroupDrive User's Guide](#) is available on line. Also, a listing of Frequently Asked Questions (FAQ) is available at our [Knowledgebase Support Center](#).

Group Drive Windows NT SAM (Security Accounts Manager) Authentication

When using Windows NT Authentication, the server administrator will create and delete user accounts using the Windows NT User Manager. The GroupDrive Administrator program can then be used to establish rights and permissions on the server. This has the benefit of providing your NT domain users with a single username/password that they can use to access both the NT domain and the GroupDrive Server. When using Windows NT Authentication some user settings can be overridden in the Administration program; however, no information will ever be written back to the Domain controller. Using Windows NT Authentication is strictly a read-only process.

Create a special NT User Account for use with GroupDrive Collaboration Server

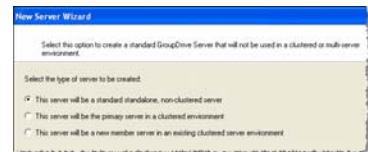
If you would like to use Windows NT SAM (Security Accounts Manager) for user authentication with GroupDrive Collaboration Server, a special NT User Account must be created. The special NT User Account will be used by the GroupDrive Server service when it needs to authenticate GroupDrive clients when they connect to the system (it will **not** be used by the GroupDrive clients to connect to the server). This special NT User Account will be given certain rights not usually available to other NT User accounts. The GroupDrive Server service will also need to be modified to use this new NT User account that will be created. Please see [Appendix A](#) for instructions on how to create a special NT User Account for use with GroupDrive Collaboration Server.

Configure NT SAM User Authentication

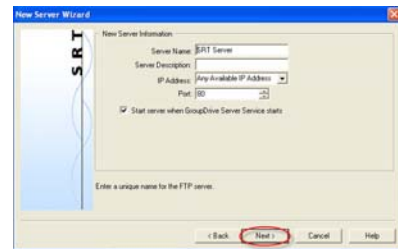
1. Run the GroupDrive Administration Utility and select **New Server Wizard**.



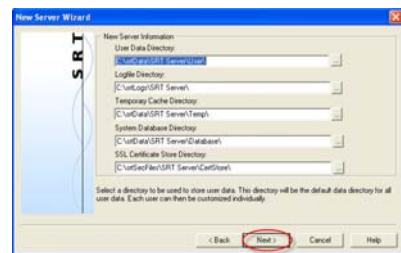
2. Select the **Server Type** (clustered or non-clustered).



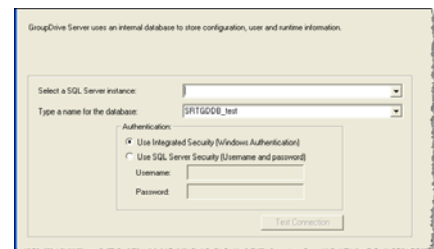
3. Type a unique **Server Name**. Click the drop-down arrow to choose your IP Address. (Any available IP address indicates that 127.0.0.1 is localhost.) Select the Port number by using the up/down arrows. Click **Next**.



4. Use the browse "..." buttons to browse to your User Data Directory, Logfile Directory, Temporary Cache Directory, System Database Directory, and SSL Certificate Store Directory. Click **Next**.



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



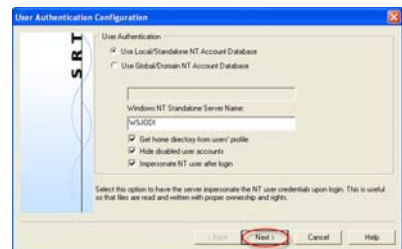
NOTE: SRT supports GroupDrive configurations using SQL Server 2005 or later or SQL Server 2005 Express or later, test or production environment. No other databases are supported.

6. Select **Windows NT/SAM User Authentication** and then click the **Authentication Server Setup** button. This will launch the *Windows NT/SAM User Authentication sub-wizard*.

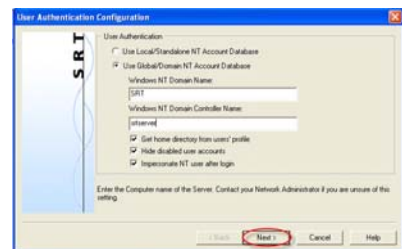


7. Select either **Use Local/Standalone NT account Database** or **Use Global/Domain NT Account Database**. Configuration options will vary depending on which option you choose.

If you select **Use Local/Standalone NT Account Database**,* type the Windows NT Standalone **Server Name**. Select additional options using the check boxes. We recommend that you **select all three** additional options.

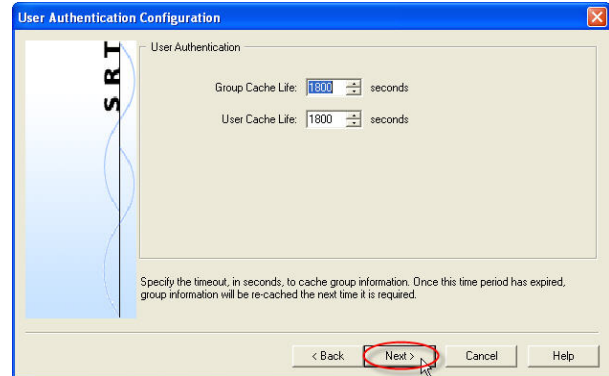


If you select **Use Global/Domain NT Account Database**.* Type the Windows NT **Domain Name**. Type the Windows NT Domain **Controller Name**. Select additional options using the check boxes. We recommend that you **select all three** additional options. When you are finished, click **Next**.



*A special NT User Account must be created on the Primary Domain Controller (PDC). Please see [Appendix A](#).

8. Set the Group Cache Life* using the up/down arrows. Click **Next**.



* GroupDrive Collaboration Server will cache user and group information to increase performance and decrease the load on your back-end database. The number of seconds that GroupDrive caches this information is controlled by the User Cache Life and Group Cache Life values. The Group Cache Life value is used by GroupDrive to determine how long to wait before refreshing the group information and also the list of members of that group. Once the cache life has expired, GroupDrive will flag the cached group information as “stale” and the next time GroupDrive needs that group information it will reload the group properties (and the list of members of the group) from the remote database. This means that if you modify the membership of the group by adding new users, or deleting users from the group, those changes will not appear in GroupDrive until the Group Cache Life value has expired and GroupDrive can reload that information. Therefore, if you have a dynamic system where the users/groups change frequently, set the Group Cache Life value to a short value, such as 300 seconds (5 minutes).

The same applies to the User Cache Life setting. If you make a change to a user account in the back end database, these changes will not appear in GroupDrive until the User Cache Life value has expired on that user account. The exception to the rule is the user’s password. GroupDrive never caches user passwords so any changes to the user’s password in the NT SAM user database will take effect immediately.

Warning: Avoid setting the Cache Life values too small. If you set the values too small, the performance could degrade because GroupDrive will be spending too much time flushing and reloading the user/group information from the database.

If you add and delete users frequently, change the Group Cache to 300 seconds.

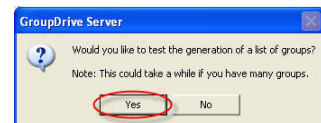
- Click **Test** to test the configuration and ensure that you are able to communicate with the user authentication server.



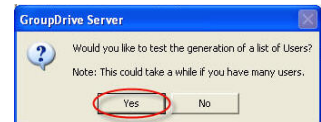
- If GroupDrive Collaboration Server can successfully communicate with the database the message that displays is Success. Click **OK**. (If an error is displayed, either GroupDrive was not able to connect to the database, or there was a problem with the back-end database.)



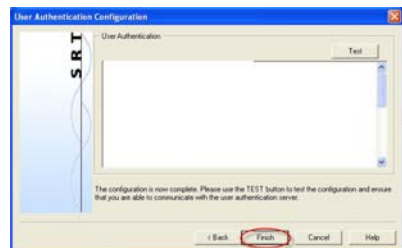
- After GroupDrive successfully connects to the database, GroupDrive will attempt to generate a list of groups. Click **Yes** to test the generation of a list of groups.



- Click **Yes** to test the generation of a list of Users.



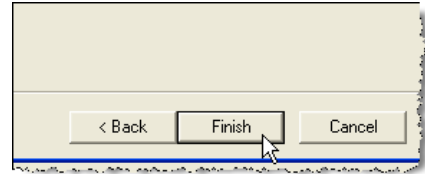
- Click **Finish**.



- You are now returned to the *GroupDrive New Server Wizard*. Click **Next**.



- The wizard will walk you through the steps to configure your **SMTP Mail Server** and your **Administrator Account**. Click **Finish** to create the server.

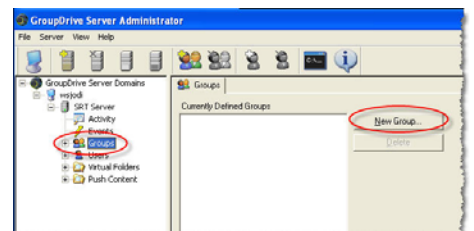


- Once the server is created, the server starts and appears in the main GroupDrive Administrator window. A green icon appears to indicate that the server is running. At this point, there are no external groups or users mapped to GroupDrive Collaboration Server.*

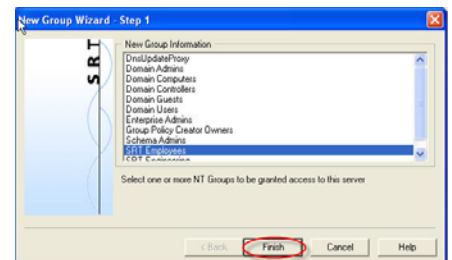


***PLEASE NOTE:** All GroupDrive Server users must belong to a group. Before any users can access the system, you must add one or more groups to the server. Because GroupDrive Collaboration Server uses the NT SAM user database, groups that will participate in the GroupDrive Server must be selected/mapped into GroupDrive Collaboration Server from the NT SAM database. To do this, you must run the *New Group Wizard* to add a new group to the GroupDrive Server.

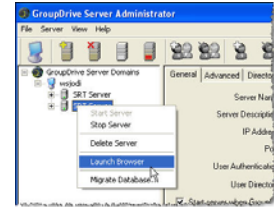
- Expand the server menu and click **Groups**. Click **New Group** to launch the *New Group Wizard*.



- Select one or more NT Groups to be granted access to this server. Click **Finish**.



19. It is now time to test the server. To test the server, right-click on the Server in the *GroupDrive Administrator* and select *Launch Browser*. Then log in with the credentials.

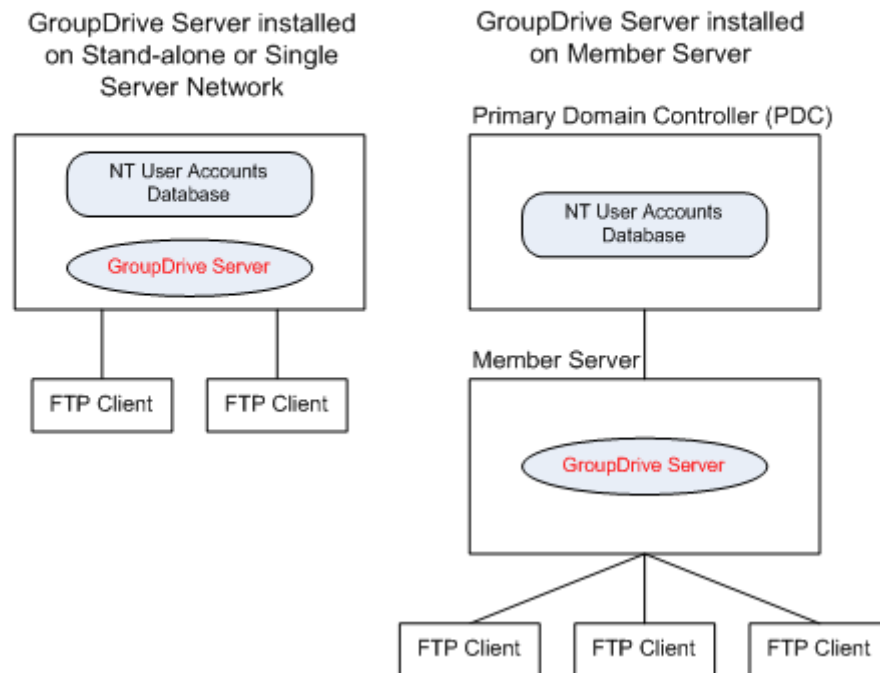


Appendix A: Create a special NT User Account

If you would like to use Windows NT SAM (Security Accounts Manager) for user authentication with GroupDrive Collaboration Server, a special NT User Account must be created. The special NT User Account will be used by the GroupDrive Server to authenticate GroupDrive clients when they connect to the system (it will **not** be used by the GroupDrive clients to connect to the server). This special NT User Account will be given certain rights not usually available to other NT User accounts. The GroupDrive Server service will also need to be modified to use this new NT User account that will be created.

GroupDrive Collaboration Server must be able to access the Windows NT SAM User Accounts Database whether GroupDrive Collaboration Server is installed on a standalone or single server network, or on a multi-server network. There can be other servers on the network, but GroupDrive Collaboration Server will only interact with the server that stores the Windows NT SAM User Accounts database.

Using GroupDrive Collaboration Server with Windows NT SAM Authentication



If GroupDrive Collaboration Server is installed on the PDC, use the following steps to create the new NT User 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 *newuser* as the username and *newpass* 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 *newuser* 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 *newuser* 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.
5. Open the *Services Control Panel Applet* and scroll down to the *GroupDrive Server service*. Right-click on the *GroupDrive Server service* and select **Properties**.
6. Modify the *Log on As:* section so that the GroupDrive Server Service will log on using the *newuser/newpass* account that was created.
7. **Stop** then **Restart** the GroupDrive Server Service.

If GroupDrive Server is not being installed on the PDC, then the PC on which GroupDrive Collaboration Server is installed must be a Member Server of the domain:

1. On the **PDC**, create a new **Domain User Account** and make note of the username and password. For our example, we will use *newuser* as the username and *newpass* 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 *newuser* 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 *newuser* is granted the right to **Access Computer From The Network** and **Act As Part Of Operating System**.
4. On the **Member Server**, create a new **Local User Account** using the same username and password as the user in step 1. Make this user a member of the **Power Users** group.
5. Open the **Local Security Policy** applet on the **Member Server** and under the **Security Settings -> Local Policies -> User Rights Assignments** make sure that *newuser* is granted the right to **Log on as a Service**.
6. Install GroupDrive Server on the **Member Server** and restart the **Member Server**.
7. Open the **Services** Control Panel Applet on the **Member Server** and scroll down to the **GroupDrive Server** Service. Right-click on the **GroupDrive Server** service and select **Properties**.
8. Modify the **Log on As:** section so that the GroupDrive Service will log on using the *newuser/newpass* account that was created.
9. **Stop** then **Restart** the GroupDrive Service.

GroupDrive Collaboration Server is now configured to use the special NT User Account that has the proper rights necessary to query the PDC User Accounts Database during the authentication of a GroupDrive client session. When a GroupDrive client attempts to connect to a GroupDrive Server that has been set up to use NT SAM Authentication, GroupDrive sends the GroupDrive client's username and password over to the PDC User Accounts Manager asking if the GroupDrive client username/password are valid. If they are valid, then GroupDrive Collaboration Server will allow the GroupDrive client to connect.