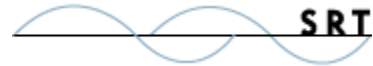




**GroupDrive Collaboration Server
Version 5.00
Administrator User's Guide**

July 2008



Copyrights

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 and GroupDrive are registered 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.
179 Admiral Cochrane Drive
Suite 110
Annapolis, Maryland 21401
USA
Telephone: 410-266-0667
Fax: 410-266-1191
www.southrivertech.com

Table of Contents

Copyrights.....	i
Table of Contents	2
What's New in GroupDrive 5	5
Getting Started	6
System Requirements	6
Installation	8
Uninstalling GroupDrive Server.....	9
GroupDrive Server Program Group Items	10
Starting GroupDrive Server.....	12
Launching the Administrator	13
Desktop Client Installation	15
Administration Terminology	16
Domain Configuration	19
Domain Overview	19
Server configuration	21
Servers Overview	21
Local Administration Tab	23
Creating New Servers	25
Creating a New Server—Tutorial	26
Step 1—Choosing an IP address and Port number.....	26
Creating a New Server—Tutorial Step 2.....	27
Creating a New Server—Tutorial Step 3.....	28
Creating a New Server—Tutorial Step 4.....	30
Creating a New Server—Tutorial Step 5.....	31
Creating a New Server—Tutorial Step 6.....	32
Creating a New Server—Tutorial Step 7.....	32
Deleting Servers.....	33
Server Settings.....	34
General Server Settings Tab	34
Advanced Server Settings Tab.....	36
Server Directories Tab.....	37
Authentication Server Settings Tab	38
User Authentication Wizard	40
Security Settings (SSL) Tab	41
Server Directory Quotas Tab	42
Server IP Access Restrictions Tab	42
Server Connection Settings Tab.....	43
User Rights Tab	44
Email Server Tab	47
Flood Protection/DoS Tab	47
UNC Accounts Tab	48
DMZedge Tab.....	49
Server Logging Settings	50
Server Log Tab.....	50
Server Log Settings Tab	51
Server Client Log Settings Tab	52
Statistics Tracking Tab	53
Server Activity Settings.....	54
Sessions Tab.....	54

Statistics Tab	55
Event Management.....	56
Event Management Overview	56
Event Handlers Tab.....	58
Event Handler Wizard	59
Event Handler Wizard Overview.....	59
Event Handler Wizard-Set Events	60
Event Handler Wizard-Set Conditions	62
Event Handler Wizard-Set Actions.....	63
Flagged Events Tab.....	65
Group Configuration	66
Groups Overview	66
Creating New Groups	67
Deleting Groups	68
Adding Users to Groups.....	69
Removing Users from Groups.....	69
Group Settings.....	70
General Group Settings Tab	70
User Configuration	71
User Configuration Overview.....	71
Creating New Users	72
Deleting Users	73
User Settings.....	74
General User Settings Tab	74
User Group Membership Tab	75
User IP Access Restrictions Tab	76
User Connection Settings Tab.....	76
SSL Tab	77
File System Settings.....	78
File System Overview.....	78
File System Permissions	80
Sharing	82
Linking to Shared Files and Folders.....	83
User Directory Quota	84
Virtual Folders	85
Virtual Folders Overview.....	85
Virtual Folders Tab.....	86
Push Content.....	87
Push Content Virtual Folders tab.....	87
Push Content Permissions Tab.....	88
Advanced Topics	89
User Authentication Overview	89
SSL Support.....	92
Creating a Special NT Account.....	93
Database Schema Column Descriptions	96
Advanced Features	99
Cache User & Group Information	99
UNC Paths—Overview	101
Desktop Client Access.....	104
Desktop Client Access	104
GroupDrive Desktop Client for Windows	105
Built-in MAC OS X Client.....	106
Goliath Desktop Client For MAC.....	109

Microsoft WebFolders	111
Contact Information	114
Troubleshooting	115
SRT Knowledgebase.....	115
Reporting Problems	115
Index.....	116

What's New in GroupDrive 5

GroupDrive version 5.00 was released on April 2, 2008. We've updated support and added new features to increase functionality, security, and ease of use.

Here's what's new in GroupDrive 5:

- **Added:** Support for 64-bit editions of Windows Server 2003, Windows Vista.
- **Added:** Support for 32 and 64-bit editions of Windows Server 2008.
- **Added:** Support for ODBC (Open Database Connectivity) [user authentication](#).
- **Added:** [Event Management](#), used for triggering actions based on conditions and events.
- **Added:** Enhanced support for Windows Active Directory [user authentication](#).
- **Added:** Enhanced support for LDAP (Lightweight Directory Access Protocol) [user authentication](#).
- **Added:** Support for Local NT [user authentication](#) with a stand-alone computer. GroupDrive can now be installed on a stand-alone NT based computer and use the local NT accounts database for authentication, impersonation, and home directories.
- **Added:** Enhanced support for NT home directories when used in conjunction with NT/Active Directory authentication.
- **Added:** Enhanced support for NT impersonation when used in conjunction with NT/Active Directory authentication.
- **Added:** [Email server](#) configuration options at the server level. These are used by Event Management and other notification subsystems.
- **Added:** [Logging](#) features to control the level of detail that is recorded in the logfile.
- **Added:** [Anti-hammering/D.O.S.](#) (Denial of Service) feature that prevents too many connection attempts in a brief period.
- **Added:** Support for [DMZedge Server](#).
- **Added:** [Password Complexity feature](#). GroupDrive can now force passwords to adhere to standard complexity rules.
- **Updated:** [SSL Engine](#) to OpenSSL v0.9.8g.

Getting Started

System Requirements

The GroupDrive Collaboration Suite has various components that can run on various platforms. The core component of the GroupDrive Collaboration Suite is the GroupDrive Server. The GroupDrive Server is used to host and serve the files that will be accessed by users by using a Web browser interface or a special desktop client application.

GroupDrive Server

GroupDrive Collaboration Server is a multi-threaded, dynamic WebDAV Server for the Windows operating system. GroupDrive utilizes multi-processor systems to full advantage. While it is designed to handle an unlimited number of user connections and servers, it is limited by the resources of the machine; most notably, those limitations imposed by the Windows Sockets (WINSOCK) Library. The GroupDrive Server application is a native Windows application and is supported under the following operating systems.

- Windows Server 2008 (32-bit and 64-bit editions).
- Windows Server 2003 (32-bit and 64-bit editions).
- Windows Vista Ultimate, Business, Enterprise (32-bit and 64-bit editions).
- Windows 2000 Advanced Server.
- Windows 2000 Server.

The following minimum hardware requirements are required to support the GroupDrive Server:

- **CPU** - Pentium class processor executing at 2GHz or faster.
- **RAM** - 512MB RAM is required. 2GB RAM is recommended.
- **Disk** - 50MB free disk space for the actual GroupDrive Server program. An additional 50MB of disk space, per-server, is also required. Additional temporary storage should be available to support the Zip Download feature.
- **Display** - Minimum VGA (640x480) resolution is required, although the Administrator program looks much better under SVGA in 800x600 mode.




Before installing GroupDrive, make sure the latest official service pack for your operating system is currently installed. Also run Windows Update to ensure that all hot-fixes and patches are installed.

GroupDrive Web Browser Interface

Files stored on the GroupDrive Server can be accessed using a Web browser. The GroupDrive Web browser interface is written using industry standard HTML and JavaScript and should run properly on most browsers. However, due to the minor differences in how various browsers interpret HTML, some graphics and features may not display correctly.

Operating System	Browser
<ul style="list-style-type: none"> ● Windows NT v4 ● Windows 2000 ● Windows XP ● Windows 2003 Server ● Windows Vista ● Windows Server 2008 	<ul style="list-style-type: none"> ● Microsoft Internet Explorer v6.0 or later ● Firefox v2.0 or later ● Netscape Navigator v8.0 or later
<ul style="list-style-type: none"> ● Apple Macintosh OS X 	<ul style="list-style-type: none"> ● Safari v2.0 or later ● Firefox v2.0 or later
<ul style="list-style-type: none"> ● Linux 	<ul style="list-style-type: none"> ● Firefox v2.0 or later



- Be sure that all service packs and security fixes are up-to-date.
- Any computer hardware capable of running your browser is sufficient to access your GroupDrive; however, minimum 800x600 resolution display is recommended.

GroupDrive Desktop Client Access

You can access your GroupDrive from anywhere, anytime, using a Web browser. If you would like to integrate GroupDrive directly into the desktop of your operating system, GroupDrive supports various desktop clients, giving you maximum flexibility and usability.

For more information, see the [Desktop Client Access](#) topic.

Installation

Installing GroupDrive Server

1. GroupDrive Server must be installed under an account that has **full administrative privileges**. Download the GroupDrive installation self-extracting installer to your computer. Alternatively, if you have the GroupDrive CD, insert the GroupDrive CD into your CD-ROM drive.
2. Double-click the GroupDrive installation file to start the installation process.
3. Follow the instructions outlined during the installation process. For most installations, the default values are acceptable for installation.
4. Once the installation process has completed, you must restart the computer. If you have not previously installed GroupDrive on the computer, you **must** restart the computer so that the GroupDrive Service can be properly registered as a valid Service.
5. After the computer has been restarted, the GroupDrive Service will be running and available for use. The GroupDrive Service runs as a system service and starts when the operating system loads. You can use the GroupDrive Server tray icon to start or stop the GroupDrive Service, or open the GroupDrive Server Administrator. You can also use the tray icon to configure GroupDrive Server **Run at Startup** options. We recommend that the GroupDrive Server service be configured to start automatically so that in the event of a power failure, or accidental system restart, the GroupDrive Server will automatically come back online.
6. Once GroupDrive Server has been installed, you can begin to configure your servers. This is done using the GroupDrive Administrator program located in the GroupDrive Server program group.

Uninstalling GroupDrive Server

Use the following procedure to completely uninstall GroupDrive Server from your computer:

1. From the Windows **Start** menu, select **Settings>Control Panel** to open the Windows Control Panel.
2. Double-click the **Add/Remove Programs** icon in the Control Panel.
3. Select **GroupDrive Collaboration Server**.
4. Follow the instructions on the dialog screens to remove GroupDrive from your computer.
5. Close the **Add/Remove Programs** applet.



You must **restart Windows** to completely remove GroupDrive from your computer.

GroupDrive Server Program Group Items

The GroupDrive Server Installation program will install GroupDrive Server on the local computer. As part of the installation process, the GroupDrive Server Program Group will be created. A standard GroupDrive Server installation produces a program group containing the following entries:

Documentation - The GroupDrive Documentation folder provides shortcuts to:

- GroupDrive Administrative Online Help
- GroupDrive Web User Interface (UI) Online Help
- GroupDrive Quick Start Guides
- GroupDrive Administrative User's Guide (PDF)
- GroupDrive Web User Interface User's Guide (PDF)

Administrator - Launches the GroupDrive Server Administrator program. This is the main program used to configure and administer all aspects of the GroupDrive Server. Using the Administrator, you can connect to the GroupDrive Service, add/delete/modify or monitor servers. The Administrator program is also used to configure groups, users, permissions, and access options. A shortcut to the Administrator program is also added to the Windows Desktop by the GroupDrive Installer.

Check for Program Update - Allows you to go online and check for a new release of GroupDrive.

GroupDrive Server Homepage - Launches your browser and opens the GroupDrive Server home page.

GroupDrive Tray Applet - Installs the GroupDrive icon in the system tray. This provides quick access to the GroupDrive Administrator program.


Pricing - Launches your browser and opens the GroupDrive pricing and purchasing area of the South River Technologies Web site.

Release Notes - Launches the Release Notes. Please review the Release Notes each time you install a new/upgrade build of GroupDrive Server. The Release Notes contain important information about bug fixes, known issues, and other information not found in the online Help.

Technical Support - Launches your browser and opens the GroupDrive technical support area of the South River Technologies Web site.

Uninstall GroupDrive Server - Launches the GroupDrive Server Uninstaller. This program will uninstall GroupDrive and remove all components from your computer. The GroupDrive user data is not deleted.

Version History - Launches your browser and opens the complete version history for GroupDrive Server. This page shows the various versions and which features/fixes appeared in those versions.

 A small icon of a red pushpin with a silver fastener, indicating a pinned or important note.	<ul style="list-style-type: none">• GroupDrive Server must be installed under an account that has full administrative privileges to the computer on which GroupDrive is being installed.• If you plan to use GroupDrive in conjunction with User Accounts on an existing NT Domain or Active Directory, please review the associated configuration information found on our Website.• We recommend that you run Check For Program Update regularly to ensure that you have the most recent version of the GroupDrive Server.
--	--

Starting GroupDrive Server

The GroupDrive Server is designed to run as a system service. You can configure GroupDrive Server so that it starts when Windows starts or you can configure it to be started manually. We recommend that you configure the Server Service to start automatically so that in the event of a power failure or accidental system restart, GroupDrive Server will automatically come back online.

Once you have installed GroupDrive you can use the GroupDrive Server tray icon to start or stop the GroupDrive Service or to open the GroupDrive Server [Administrator](#). You can also use the GroupDrive Server tray icon to configure GroupDrive Server **Run at Startup** options.



GroupDrive Server
Tray Icon

About GroupDrive Server - Right-click the tray icon to see GroupDrive Server version information.

Start Service/Stop GroupDrive Server Service - Right-click the tray icon to configure this option. **Note:** If you stop the GroupDrive Server Service, all GroupDrive Server instances will be shut down and any user connections will be terminated.

Run at Startup - Right-click the tray icon to configure this option. A check mark appears when this option is activated. When this option is activated, GroupDrive starts automatically when Windows starts. If this box is not selected, GroupDrive will not start until you start it manually start it. We recommend that you enable this option.

Open Administrator - Double-click the tray icon or right-click the tray icon and select **Open Administrator**.

Close Tray Application - Select this option to remove the tray icon. If you would like to retrieve the tray icon, select **GroupDrive Server>GroupDrive Tray Applet** from your Windows Start menu.



By default, the GroupDrive Service will run under the context of the **LocalSystem** or **Local Service** user account. When you create a GroupDrive Server configuration, the account that is used by the GroupDrive Service must have full access to the underlying file system where GroupDrive will store its files.

Launching the Administrator

The GroupDrive Server Administrator program is used to configure [servers](#), [groups](#), and [users](#).

The Administrator program can be started by double-clicking the GroupDrive Administrator icon in the GroupDrive Program Group. There is also a shortcut to the Administrator program on your Windows desktop.

The first time the Administrator is executed, the [Local Domain Wizard](#) will be launched. The Local Domain Wizard is used to ensure that your computer is properly configured. Among other things, you must specify the username and password that you will use for local administration. Save this information because each time you run the Administrator program and connect to the Local Domain, you will be prompted for the username and password for authentication.

Each time that you launch the GroupDrive Server Administrator the **Administer Domain** window will appear. Use the Administer Domain window to confirm or change your Authentication Credentials:

- **Host Address** - The host IP address. The GroupDrive Server Administrator communicates with the GroupDrive Server Service using a connection on the localhost (127.0.0.1) loopback address.
- **Administration Port** - The administration port number. The Local Administration Port specifies the port number to be used with the loopback address to be used by the GroupDrive Server Service for listening for the Administrator.
- **Administrator Username** - The administrator username that will be used to log in to the Local Domain. This username can be any combination of letters/numbers, but cannot contain spaces. The maximum limit for the administrator username is 128 characters. This username is case sensitive.
- **Administrator Password** - The administrator password that will be used in conjunction with the Administrator Username to confirm access to the Local Domain. The password can be any combination of letters/numbers, but cannot contain spaces. The maximum limit for the password is 128 characters. The Administrator password is case sensitive.

The Administrator program is designed as a standard Windows application containing a split screen with two panes separated by a vertical resizing bar. The left pane of the screen, or **treeview** pane, displays the overall hierarchy of **Domains, Servers, Groups, and Users**. The right pane of the screen, or **tab pane**, displays configuration information based on the current selection within the treeview pane. By scrolling through the various items in the treeview pane, the tab pane will update and one or more dialog tabs will be displayed. Each dialog tab will display information pertinent to the selected item.

Apply & Revert

Many of the dialog tabs in the Administrator program have two buttons located at the bottom of the screen. These two buttons, labeled **Apply** and **Revert**, provide the ability to apply the settings or revert to the last saved settings. Whenever a configuration option has been modified on a dialog tab, the **Apply** and **Revert** buttons are enabled. To save changes made on the dialog tab, click **Apply**. If you have made any changes that should be discarded, click **Revert** and the current tab will be reloaded with the currently saved settings. **Note:** If you make changes on any of the dialog tabs, and then switch to a different tab (or select a different item in the treeview pane), those changes will be saved automatically.



Real Time Effectiveness

Please note that in most cases, any modifications made at the server, group, or user level become effective once the **Apply** button has been clicked and the changes have been saved. When a configuration option at any level has been modified, the GroupDrive Service is notified that the configuration has been modified and will reload that information at the next available opportunity.

Navigation

The Administrator program uses standard Windows navigation keys for moving throughout the application.

Menu Bar - To access the menu options in the Administrator, hold down the **<ALT>** key to activate the menu bar, and then click the underlined letter of the desired menu item.

Toolbar - The toolbar has buttons for some of the more common features of the GroupDrive Server Administrator. As you scroll through the list of items in the tree pane, various toolbar buttons become enabled and disabled depending upon the availability of options for the selected item. The commands associated with the tools on the toolbar can also be accessed from the main menu bar.

Context Menus - You can use the main menu and toolbar to gain access to commands and you can also gain access to the various commands for a tree item by right-clicking that item. When you right-click an item in the treeview pane, a context menu is presented that will contain actions specific to the selected item.

Switching Panes - **<F6>** will cause focus to switch between the treeview pane and the tab pane; you can also use your mouse to click on the desired pane.

Switching Tabs - To switch between the various tabs in the tab pane, set focus to the pane using **<F6>** and use the left and right arrow keys on your keypad to activate the various tabs.

System Menu - The Administrator program has the Windows standard minimize, maximize, restore, and close functionality built into the System menu. Some of the configuration dialogs, such as the Server Configuration dialog, have many tabs, so it may be easier to maximize the Administrator so that all of the tabs are visible.

Desktop Client Installation

Users can install the GroupDrive Desktop Client by logging in to their GroupDrive account, and then by navigating to the Utilities area where the GroupDrive Desktop Client can be downloaded.

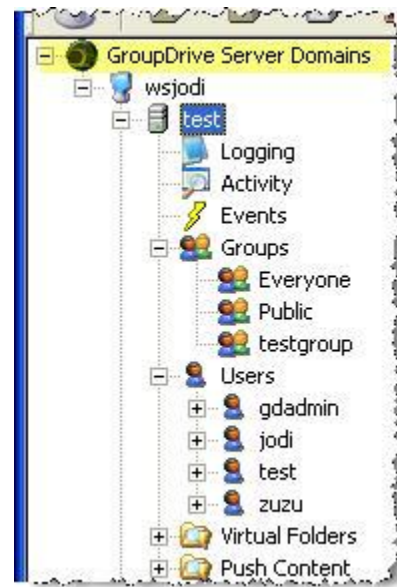
The GroupDrive Administrator can access the installer from the local computer. When GroupDrive is installed, the GroupDrive Desktop Client installer is copied to the installation directory. By default this folder is **c:\Program Files\GroupDrive Server\Downloads\gdClient.exe**.

Run the desktop client setup program and follow the on-screen instructions. An overview of the GroupDrive desktop client is available [in this help system](#). For more detailed information, the GroupDrive desktop client includes a separate [help file](#) that describes how to use the desktop client.

Administration Terminology

Administrator - The GroupDrive Server Administrator program allows you to configure all aspects of a GroupDrive server. Installed as part of a standard GroupDrive Server installation, you can use the GroupDrive Server Administrator program to view and configure options and settings for each **Domain, Server, Group, and User**. The Administrator program can be used to configure servers on local domains only.

DMZedge Server - The DMZedge Server enables you to close inbound ports on your firewall, reducing the risk of network intrusion and enabling the highest level of security for both data storage and transfers. When combined with GroupDrive Collaboration Server, the DMZedge Server uses a two-way connection originating from the GroupDrive Server that is inside of the firewall on your corporate LAN (Local Area Network). The DMZedge works as a communication proxy, shielding your internal network from unsecure inbound connections. For more information about DMZedge, see the [DMZedge User's Guide](#).



GroupDrive Server Service - The main program/service/daemon that runs on the computer and manages GroupDrive server instances. In the graphic to the right, the GroupDrive Server Service is represented by the root/top node in the tree, labeled **GroupDrive Server Domains**.

Groups - For each server instance, GroupDrive Server provides the ability to define one or more groups. Groups are a way to categorize users who share common attributes. First, you define a group, and then add users to the group. Groups are most useful when defining access permissions to files and folders. You can define a set of access [permissions](#) for a group to a specific folder and then you can manage access to the folder by simply adding or removing a user from a group. By default, each server instance is pre-configured with a general group called **Everyone**. This is a system level group and cannot be deleted. All Users are members of the **Everyone** group, so use caution when adjusting the permissions given to the **Everyone** group. The **Public Access** group is used to assign permissions to public users (non-named users). If you assign public access to a folder or file object, then no [authentication](#) to that folder/file is required. This is useful, for example, for sharing photos in a folder with friends over the Internet, you can simply email a link to the file.

Domain - A domain is defined as the physical computer on which the GroupDrive Server Service is running. The GroupDrive Server Administrator program can connect to the local Domain. For each domain, you can define zero or more server instances. Each server instance is identified by a unique IP/Port combination. In the graphic at the right, the domain is represented by the blue computer monitor located directly under the **GroupDrive Server Domains** node in the tree.

Local Domain - The local computer on which the GroupDrive Server Service is running. In most cases, the GroupDrive Server Administrator operates on the local domain. In the graphic, the local domain is the blue computer monitor located directly under the **GroupDrive Server Domains** node in the tree. There will only be one local domain listed; in our example, the Local Domain is called **wsjodi**.

Permissions - **Permissions** are different from **User Rights**. Permissions generally pertain to the level of access granted to a specific system resource, such as level of access a user has to a file or folder object. Permissions can be set by the System Administrator or the owner of the file or folder object. User rights are authorized by the System Administrator and generally refer to system actions, such as the ability of a user to share or download file and folder objects.

Push Content - Use the Push Content Virtual Folders tab to place a virtual folder in a user's directory space. When you use the Push Content feature, the server will "push" the virtual folder into the user's directory space without the user having to link to it.

Server - The GroupDrive Server Service manages the various server instances that are defined within the local domain. Each server instance is identified by a unique IP/Port combination, providing the ability to have multiple WebDAV Servers all running at the same time. For example, you can configure a production server to be listening on IP address **192.168.1.1 (Port 80)**, and also have a staging server, or test server, listening on **Port 8080**. If your computer has multiple NIC interfaces (**192.168.1.1 and 205.1.2.3**), you can set up a server to listen on **192.168.1.1:80** and set up another server instance to listen on **205.1.2.3 Port 80**. In the graphic, the local domain has one server instance configured and running under the name of **test**.

UNC Paths - 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.

User Rights - **User Rights** are different from **Permissions**. User rights are authorized by the System Administrator and generally refer to system actions, such as the ability of a user to share or download file and folder objects. Permissions generally pertain to the level of access granted to a specific system resource, such as level of access a user has to a file or folder object. Permissions can be set by the System Administrator or the owner of the file or folder object.

Users - For each server instance, the GroupDrive Server Administrator program provides the ability to define one or more users who can access the server. The GroupDrive Server Administrator has the ability to add new users, and to configure the access rights granted to these users.

Virtual Folders - Virtual folders are folders that can be mapped into a server's data directory and are used to link or map external folders into a user's directory space. This is useful for giving access to files on another disk drive, CD-ROM, or even a network drive. In a Virtual folder it appears as if the data resides within the folder structure; however, the data is actually stored somewhere else. If you are a Windows user, you can think of a Virtual Folder as a Windows Shortcut. The link appears in one location and the data lives in another location. For UNIX users, Virtual Folders are very similar to Symbolic Links.

WebDAV - Acronym for Web-based Distributed Authoring and Versioning protocol, an extension to the HTTP protocol that many servers are now supporting on the Internet. WebDAV extensions allow users to read, write, and share documents over the Internet.

Domain Configuration

Domain Overview

GroupDrive uses the term **domain** to denote a physical computer on which GroupDrive has been installed. A primary use of the domain is to provide a grouping for the actual GroupDrive server or servers that will be running on the physical computer. In order to configure the various GroupDrive servers, you must use the [GroupDrive Server Administrator](#) program to connect to the domain that houses the servers.

The first time the Administrator is executed, the **Local Domain Wizard** is launched. The Local Domain Wizard is used to ensure that your computer is properly configured. Among other things, you must specify the user name and password to be used for local administration. **Save this information** because each time you run the Administrator program and connect to the Local Domain, you will be prompted for the username and password for authentication.

Domain Properties

Local Domain Name - This name represents the local domain. By default, this is the same name as the computer. However, you can change this name to be any readable text name. The local domain is not displayed to the client.

Local Domain Description - A text phrase to further describe the domain.

Data Directory - The **Domain Data Directory** setting defines the default location where all server data will be stored. This value will be used to prime the Server Data Directory entry in the Server Wizard. For each new server, the Domain Data Directory and the new server name will be concatenated to produce the full path to the data directory where the server data files will be stored. This value can be either a fully qualified path such as **C:\Mydata** or a UNC name such as **\\Server\Share\MyData**.

Log Directory - The **Domain Log Directory** setting defines to default location where server logs will be stored. This value will be used to prime the Server Log Directory entry in the Server Wizard. For each new server, the Domain Log Directory and the new server name will be concatenated to produce the full path to the log directory where the server logs will be stored. This value can be either a fully qualified path such as **C:\MyLogs** or a UNC (Universal/Uniform Naming Convention) name such as **\\Server\Share\MyLogs**.

Start Service when Windows Starts - This option allows you to configure whether or not the GroupDrive **Server Service** will automatically start when Windows starts. If this option is enabled, the GroupDrive **Server Service** will start automatically when Windows starts. Once the Service has started, any servers that are configured to start when the Service starts will be launched. We recommend that you enable this option.

Run Tray Applet when Windows Starts - This option allows for the automatic launching of the Tray Applet used to display, start, and stop the Server Service.

Administrator Username - Type the **username** that will be used to log in to the local domain. This username can be any combination of letters/numbers, but cannot contain spaces. The maximum limit for the Administrator Username is 128 characters. This username is **case sensitive**.

Administrator Password - Type the password that will be used in conjunction with the Administrator Username to confirm access to the local domain. The password can be any combination of letters/numbers, but cannot contain spaces. The maximum limit for the password is 128 characters. The Administrator Password is **case sensitive**.

Local Administration IP Address/Port - The GroupDrive Server Administrator communicates with the GroupDrive Server Service using a connection on the localhost (**127.0.0.1**) loopback address. The Local Administration Port specifies the port number to be used with the loopback address to be used by the GroupDrive Server Service for listening for the Administrator.



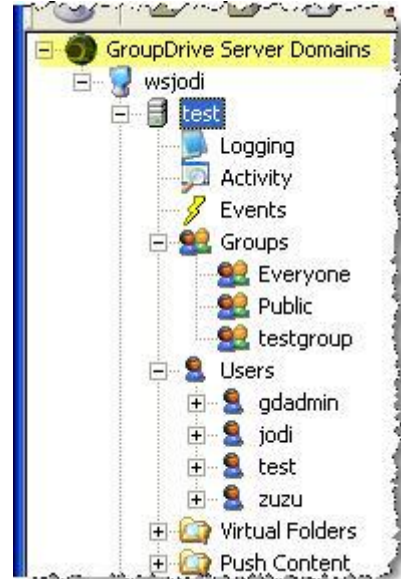
The Data Directory and Log Directory can be customized on a per-server basis; therefore, it is not required that all data be stored under the Domain Data Directory. This setting is primarily used to prime the individual Server Data Directories.

Server configuration

Servers Overview

GroupDrive supports the ability to configure multiple server instances under a single domain or physical computer. Each server instance listens on its own distinct IP address/Port combination, which provides the ability to have an unlimited number of servers running simultaneously.

Each server can be configured to store data in its own separate data directory; either on your local hard drive or on a shared network drive. GroupDrive Server supports both standard DOS path syntax and UNC paths.

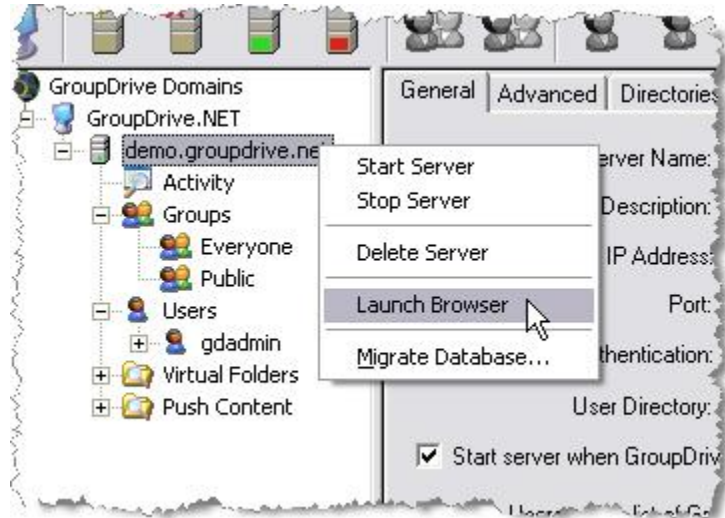


Creating new servers is easy; simply launch the New Server Wizard from either the main menu, toolbar, or via the right-click context menu for the domain under which you want the server to reside. The New Server Wizard walks you through the steps to configure your server. Once the New Server Wizard has completed, your new server will be created and you can start using it immediately. For more information about how to use the New Server Wizard, see the [Creating a New Server tutorial](#).

The **New Server Wizard** helps you to set up the initial configuration for your server and there are many more features and configuration options available once the server is created. Use the GroupDrive **Server Administrator** to modify server properties as necessary. Launch the GroupDrive **Server Administrator**, connect to the domain, and select the **server** in the treeview pane. Once the server has been highlighted in the tree pane, a list of dialog tabs are displayed in the tab pane. Numerous configuration options are grouped under various tabs; select the tab and make the necessary changes. Once you have made the configuration changes, click **Apply** to save the changes. The GroupDrive **Server Administrator** will save the configuration changes and notify the GroupDrive **Server Service** that it must reconfigure the server with the new settings.

Once the server has been created, its configuration information is displayed in the GroupDrive Administrator treeview pane.

If you have chosen to automatically start the server, the server icon in the tree will be illuminated green. You can easily test to see if the server is running: right-click the **server** item in the tree pane,



and then select **Launch Browser** from the context menu. This will launch your default browser and take you to the IP address for which the server has been configured. If the server is running and that address is available, you will see the default GroupDrive login screen.

You can also use the Administrator program to [Delete Servers](#). You cannot delete a server if it is running; you must stop the server before deleting it. To stop the server, right-click the **server** in the tree pane, and select **Stop Server**. Once the server has been deleted, all associated groups and users will also be deleted from the system.

Note: In order to protect from any possible data loss, the GroupDrive Server Administrator program will **not** delete the contents of the Server Data Directory or the Logfile Directory. If you no longer need the contents of the Server Data Directory or the Logfile Directory, you must manually delete that information.

Local Administration Tab

The **Local Administration** tab displays local Administration Settings.

To access the **Local Administration** tab, in the tree pane, select the **Domain**. The **Local Administration** tab is displayed in the tab pane.

The first time the Administrator is executed, the **Local Domain Wizard** is launched. The Local Domain Wizard is used to ensure that your computer is properly configured. Among other things, you must specify the user name and password to be used for local administration. **Save this information** because each time you run the Administrator program and connect to the Local Domain, you will be prompted for the user name and password for authentication. After the Local Domain Wizard has completed you can use the **Local Administration** tab to change various configuration options and settings. Some configuration settings cannot be changed, such as **Administration IP Address** and **Administration Port**.

Local Administration Settings

Administration IP Address - Displays the IP address that the GroupDrive Server Administrator uses to communicate with the GroupDrive Server Service using a connection on the localhost (**127.0.0.1**) loopback address.

Administration Port - The local Administration Port specifies the port number to be used with the loopback address to be used by the GroupDrive Server Service for listening for the Administrator.

Administrator Username - Type the username that will be used to log in to the local domain. This username can be any combination of letters/numbers, but cannot contain spaces. The maximum limit for the Administrator Username is 128 characters. This username is **case sensitive**.

Administrator Password - Type the password that will be used in conjunction with the Administrator Username to confirm access to the local domain. The password can be any combination of letters/numbers, minimum four characters, and cannot contain spaces. The maximum limit for the password is 128 characters. The Administrator Password is **case sensitive**.

Domain Name - This is the name represents the local domain. By default, this is the same name as the computer. However, you can change this name to be any readable text name. The local domain is not displayed to the client.

Domain Description - A text description used to further describe the domain.

Data Directory - The domain Data Directory setting defines the default location where all server data will be stored. This value will be used to prime the Server Data Directory entry in the New Server Wizard. For each new server, the Domain Data Directory and the new server name will be concatenated to produce the full path to the data directory where the server data files will be stored. This value can be either a fully qualified path such as **C:\Mydata** or a UNC (Universal/Uniform Naming Convention) name such as **\\Server\Share\MyData**.

Logfile Directory - The domain Logfile Directory setting defines to default location where server logs will be stored. This value will be used to prime the Server Log Directory entry in the New Server Wizard. For each new server, the domain Logfile Directory and the new server name will be concatenated to produce the full path to the log directory where the server logs will be stored. This value can be either a fully qualified path such as **C:\MyLogs** or a UNC name such as **\\Server\Share\MyLogs**.

Start GroupDrive Server Service when Windows Boots - This option allows you to configure whether or not the GroupDrive Server Service will automatically start when Windows starts. When this option is enabled, the GroupDrive Server Service starts automatically when Windows starts. Once the GroupDrive Server Service has started, any servers that are configured to start when the Server Service starts will be launched. We recommend that you enable this option.

Start GroupDrive Server Tray Applet when Windows Boots - This option allows for the automatic launching of the Tray Applet used to display, start, and stop the Service.



The Data Directory and Log Directory can be customized on a per-server basis; therefore, it is not required that all data be stored under the Domain Data Directory. This setting is primarily used to prime the individual Server Data Directories.

Creating New Servers

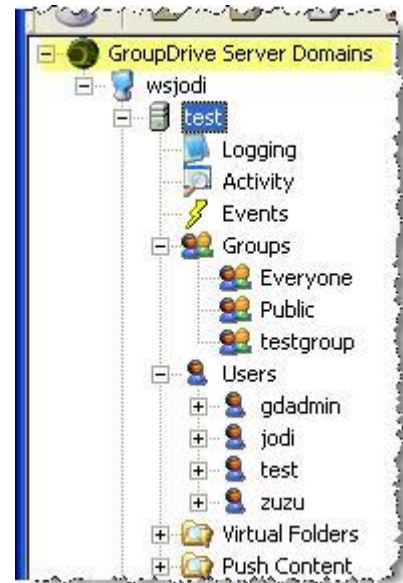
New servers can be configured at any time using the **New Server Wizard**.

The **New Server Wizard** can be launched from within the Administration program:

Right-click the Local or Remote **Domain** icon in treeview pane of the GroupDrive Server Administrator and select **New Server Wizard** from the context menu.

or

From the main menu, select **Server** then **New Server Wizard**.



The **New Server Wizard** will help you to configure a new server and set it online. Once the server has been created, you can go back and change server configuration options.

The **New Server Wizard** has built in QuickHelp that appears at the bottom of each page when focus is set to each control. To get QuickHelp on the **New Server Wizard**, click the desired control and the help text will appear at the bottom of the dialog.

For more information about configuration options available in GroupDrive Server, see the [Creating a New Server](#) tutorial.

Creating a New Server—Tutorial

This tutorial is designed to give step-by-step instructions for creating a new GroupDrive Server using the GroupDrive Administrator program.

Step 1—Choosing an IP address and Port number

The first thing that you must do before you create a new server is to select an IP address and port number for your new GroupDrive server to use. Most computers have a single IP address that can be accessed by other users. If you do not know the IP address of your computer, you can open a command prompt (DOS box) and type the command **IPCONFIG**. This command will display the IP address of your computer. This IP address can be used for your Server. You should also make sure that you have a **static** IP address for your computer. If you access the internet through a dial-up account, you most likely have a **dynamic** IP address. If you have a dynamic IP address, then during the setup process you must select **Any Available IP Address** when you are prompted, instead of selecting an actual IP address.

For each IP address, there are many **ports** that can be used to access the computer. If you think of the IP address as your house, a port is similar to a door that can be used to gain access to your home. TCP/IP defines standard port numbers for various protocols. For example, when you connect to a Web site using your browser, you are usually connecting over port 80, the port reserved for HTTP access. Port 80 is the default port for GroupDrive; however, you are free to choose a different port. Port 443 is commonly used for HTTPS traffic.

Before you set up the server, you should check to see if any other program is currently using port 80 on your computer. To see which ports are being used on your computer, open a command prompt and type the command:

netstat -a -n -p TCP

This command will display a list of IP addresses and ports that are currently in use on your computer. If **ipconfig** revealed that your IP address was **192.168.1.100**, then the **netstat** command may print information such as:

Protocol	Local Address/Port	Foreign Address	State
TCP	192.168.1.100:80	0.0.0.0:0	Listening
TCP	192.168.1.100:990	0.0.0.0:0	Listening

The **Local Address/Port** column displays a list of IP/ports that are currently in use. If you see an entry which has **:80** after the IP address in the Local Address column, then your default port is currently being used by some other application. If you do not see **:80**, then the HTTP port is available for use.

If **port 80** is currently in use, another HTTP or web server may be active on your computer. You can either choose another port, such as **port 8080**, or you can make **port 80** available by closing the application that is using **port 80**. There are over 32000 ports per IP address on your computer. You can use any port that is available for your server. TCP/IP usually reserves ports 1 through 1024 for special uses (such as **port 21** for **FTP** and **port 80** for **HTTP**), so if you are not using port 80, you should choose a port number above 1024 for your Server.

Creating a New Server—Tutorial Step 2

Choose a location for your data

Your Server will "serve" files to users who connect using a browser or one of the supported [Desktop Clients](#). When users connect to your server, they will usually want to download existing files or upload new files. The files that your Server "serves" will be stored either on the local disk drive, or on a network drive that has been shared for use by the GroupDrive server.

Usually you do not want to provide users with the ability to access all of your files, so you should choose a location, for example, an individual subdirectory, that will house the files that users will be able to access. This directory, along with all subdirectories and files within those subdirectories, is known as the **namespace** for the GroupDrive server. By default, GroupDrive will create a base domain data directory on your computer named **\srtData**, which is the primary namespace where GroupDrive will store all of the data for all GroupDrive servers that are configured. If you create a sever named **demo**, then GroupDrive will create a directory named **\srtData\demo** that will be used as the primary namespace for all files accessible to users connecting to **demo**.

Note: During the process of creating the new server, you will have an opportunity to customize the directory name for the server.

Once you have selected an **IP address**, a **Port number**, and a **Data Directory** location for your new server, you are ready to create your new server.

In many instances, you will have an existing network file server that contains user data that will be accessed by GroupDrive. If this is the case, GroupDrive will be able to access that remote file server using a UNC share such as **\\Server\share\demo**.

File Permissions for the Data

File access rights are required by the GroupDrive Server to access the data; and this is a very important concept to keep in mind when you are configuring GroupDrive. The GroupDrive 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, this may not always be the case. 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, they will not usually 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 New Server—Tutorial Step 3

Launching the New Server Wizard

Launch the GroupDrive **Server Administrator** to create a new server. You can access the GroupDrive Administrator by double-clicking on the **Administrator** icon in the GroupDrive Server **Program Group**.

Once the Administrator program is running, select **Server** then **New Server Wizard** from the main menu to launch the New Server Wizard.



The New Server Wizard is a dialog driven process designed to help you quickly create a new GroupDrive server. The GroupDrive server is highly configurable; however, the New Server Wizard only requires a few key configuration settings to create the server. Once the server is created, you can use the GroupDrive Administrator at any time to change settings for the server.

Basic Server Information—Wizard Step 1

The New Server Wizard will prompt you for basic information to uniquely identify the server on this domain.

Server Name - A short name that uniquely identifies the server on your system. By default, this name is also used as the name of the directory on your local computer where the server data files will reside. For example, **BetaServer1** might be a name given to a server that will be used to house beta versions of software.

Server Description - A longer text description for the server. For example, **My Internal Beta Server** may be a description for the **BetaServer1** server. This description is displayed when the user logs in to GroupDrive using the browser.

IP Address - This drop-down list box contains a list of all IP addresses that are currently registered on your computer. You can choose any of the IP addresses that are listed, or you can select Any **Available IP Address** that instructs GroupDrive to dynamically determine the IP address at runtime. This is useful in an environment where the computer may have multiple IP addresses configured and GroupDrive must listen on all of the IP addresses. If you have a **dynamic** IP address, you must select **Any Available IP Address**

Port Number - Enter the port number that the server will use to listen for incoming connections from clients. By default, TCP/IP reserves **port 80** for HTTP traffic, so you may want to use this port if it is available. If not, you can choose another port. If port 80 is not available, it is customary to choose a port between 1024 and 32000, such as port 8080 or port 8888.

Start Server When GroupDrive Server Service Starts - Select this option if you want this server to automatically start when the GroupDrive Service starts. The GroupDrive Service usually starts when Windows boots, so enabling this feature ensures that this server automatically starts and is available when Windows starts. This is beneficial because if the computer loses power for some reason, or Windows needs to restart, your server will automatically come back online.



- The Server Description will be displayed in the Browser when the user connects to GroupDrive. If you omit the Server Description, the word **GROUPDRIVE** will be displayed as the server name when a user logs in to GroupDrive using the browser.
- Each Wizard page has a **QuickHelp** area just above the **Back/Next** buttons. This area will display a short help message relating to the control that currently has focus.

Creating a New Server—Tutorial Step 4

New Server Wizard—Directory Locations

This step of the New Server Wizard allows you to configure the location where your user files and logs will be stored. By default, each server is given its own directory under the main Data Directory for the domain. You can customize this location and enter any fully qualified path on your local computer or network.

User Data Directory - Specify the fully qualified path to the directory that will be used to store all of the files and folders accessible by users who connect to your GroupDrive server. **Note:** each user can have a custom specified directory. This value will be used as the default for all new users who are given access to the GroupDrive server.

Logfile Directory - Specify the fully qualified path to the directory where all of the server log files will be stored. This location should NOT be the same as the Data Directory since you usually do not want users to be able to gain access to your log files. Log files can become rather large, so we recommend that this location be on a drive that has at least 100MB of free space.

Temporary Cache Directory - Specify the fully qualified path to a directory that will be used for temporary files. This folder is primarily used during the Zip Download feature that allows users to zip the contents of a folder and download that zip file to their computer. GroupDrive will zip the requested files and folders and store the zip file temporarily in this folder during the download process. We recommend that this location be on a drive that can handle the zipping of a user's directory.

System Database Directory - Specify the fully qualified path to the directory where GroupDrive will store a database containing system configuration information. We recommend that this location be on a drive with at least 100MB of free space.

SSL Certificate Store Directory - Specify the fully qualified path to the directory where GroupDrive will store server and user certificates when running in HTTPS mode. We recommend that this location be on a drive with at least 100MB of free space.



- Do not use a **Mapped Network Drive** for storage since mapped drives are not normally available to NT services such as GroupDrive. The GroupDrive Administrator will replace any mapped drive specifications with the UNC path instead.
- The **NT account** specified by the GroupDrive Service **must** have full access granted to every directory/path specified on this page. GroupDrive will not function correctly if it does not have full read/write/delete/create access to these directories.
- For more information about **SSL Certificates**, see the GroupDrive SSL Public Key [Quick Start Guide](#).

Creating a New Server—Tutorial Step 5

New Server Wizard—Server Database Configuration

GroupDrive uses an internal database to store configuration, user, and runtime information.

NOTE: When you create an ODBC datasource to be used by GroupDrive Server, the datasource must be defined as a **System/Machine** datasource to that the GroupDrive Server Service can make use of that datasource.

ODBC Datasource - Enter the name of the ODBC datasource for your production server. the "... " button can be used to launch the ODBC Administration utility to select the datasource.

DB Username - Enter the username used to access the production database server.

DB Password - Enter the password used to access the production database server.

Database Name - Enter the name of the database on the production database server used to store the GroupDrive server information.

Test - Click **Test** to test access to the production database server. It is highly recommended that you test the connection to the database server before continuing to the next step.

GroupDrive currently supports access to the following database engines:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2005 Express
- Microsoft SQL Server 2000
- Microsoft SQL Server 2000 Desktop Engine (MSDE)
- MySQL v5.0
- Microsoft Access 2000 (*)




- *The **default database** that is provided in GroupDrive Server is a **Microsoft Access database**. Depending on your needs, you may require a more robust database for back up, performance, or scalability.
- While GroupDrive is built on standard relational database concepts and data types, not all **ODBC compliant database servers** are created equally. If you are unsure if GroupDrive can be used with your ODBC compliant database server, please contact our [support staff](#).

Creating a New Server—Tutorial Step 6

New Server Wizard—User Authentication Options

GroupDrive Server supports various methods of user authentication:

- **Native GroupDrive Server User Authentication**
- **Windows NT/SAM User Authentication**
- **Windows Active Directory (ADSI)**
- **Standard LDAP User Authentication**
- **ODBC Data Source User Authentication**

	<ul style="list-style-type: none"> • For more information about user authentication, read the User Authentication Overview topic or see the GroupDrive Quick Start Guide for your specific user authentication method.
	<ul style="list-style-type: none"> • Once you select a User Authentication Database option in GroupDrive, you cannot change to a different method after the server wizard has completed.

Creating a New Server—Tutorial Step 7

New Server Wizard—Server Administration Account

The final step in configuring your GroupDrive server is to create an account that will be used for user/group administration. This account will allow you to create users and groups from the Web browser, eliminating the need to sit down at the GroupDrive Administrator console each time you need to create a new user account.

Admin Full Name - The name of the user who will be assuming the role of Administrator for this server.

Username - The username assigned to this user. By default, the username will be **gdadmin**, but any username is acceptable. Usernames are **case-sensitive**.

Password - The password assigned to this user account. Passwords are case-sensitive and must contain a minimum of four characters.

Confirm Password - Confirm the password by typing it again.

	<p>For more information about server configuration options, see the GroupDrive Quick Start Guide for your specific server configuration.</p>
---	--

Deleting Servers

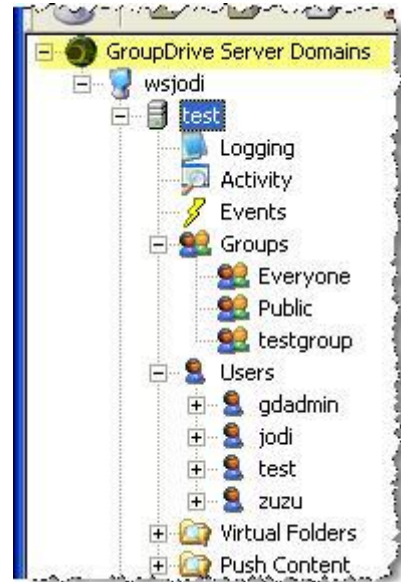
Servers can only be deleted if they are not running. Make sure that you have stopped the server before attempting to delete it from the system.

To delete an existing server using the GroupDrive Server Administrator:

Right-click the **Server** in left pane (tree pane) of the GroupDrive Server Administrator and select **Delete Server** from the menu. You will be prompted to confirm the deletion of the server.

or

Click the **Server** in the left pane of the GroupDrive Server Administrator. From the main menu, select **Server** then **Delete Server**. You will be prompted to confirm the deletion of the server.



Deletion of a server is **permanent**. We recommend that you delete a server only if you are absolutely sure that you will no longer be using it. Once you delete a server, all associated groups and user information is removed.

Server Settings

General Server Settings Tab

Use the server **General Settings** tab to manage basic configuration options for the server.

To access the **General Settings** tab, in the tree pane, select the **Server**. In the tab pane, select the **General Settings** tab. When you are creating a new server, the [New Server Wizard](#) is used to initially configure most of these options.

Server Name - Displays the name of the server.

Server Description - Displays the text description for the server.

IP Address - Displays the [IP Address](#) that the server will listen on. You can type a specific IP address, or you can select **Any Available IP Address**. You must select **Any Available IP Address** if your computer has a dynamic IP addressing scheme.

Port - The [port](#) that the server will listen on.

User Authentication - Displays the [user authentication method](#). Once the [New Server Wizard](#) has completed you cannot change to a different user authentication method.

User Directory - The relative path to the server data directory where user data directories will be created. By default, the User Directory is set to **\User**, so if the Server Data Directory is set to **c:\srtData\MyServer** then a user whose name is **john** would store his files in the **c:\srtData\MyServer\User\john** folder. The user folder will be created when the user first logs onto the GroupDrive server. To change the location of a User Directory use the Server **Directories** tab.

Start Server when Service Starts - When enabled, the server will automatically be started when the GroupDrive Server starts.

Allow Users to see list of Group names - When enabled, this option allows users to view the list of Group names when a user is sharing a file or folder and wants to grant permissions to specific Groups.

Allow Users to see list of Usernames - When enabled, this option allows users to view the list of user names when a user is sharing a file or folder and wants to grant permissions to specific Users.

Allow "Public" Group Access - When selected, this option enables the use of the **Public** group which allows users to give access to files or folders in their user directories to the general public without requiring authentication to that specific file or folder. This is useful for sharing a folder of pictures and being able to e-mail the link to the folder or files to anyone who could then view them in a browser without the need to authenticate to the GroupDrive server.

Session Timeout - Displays the timeout in minutes for a GroupDrive session. Each time a user logs in to the GroupDrive server a session is created for that user. If no activity occurs with this session for the specified timeout value, then GroupDrive will delete the session, which forces the user to log in the next time he tries to access the GroupDrive server.

Client Session Timeout - Displays the timeout in minutes for the GroupDrive Client Session. Similar to the **Session Timeout** value above; however, this setting only applies to the GroupDrive Client.

Advanced Server Settings Tab

Use the server **Advanced** tab to configure advanced settings for this server.

To access the **Advanced** tab, in the tree pane, select the **Server**. In the tab pane, select the **Advanced** tab.

Allow Users to change password - When enabled, this option allows users to change their password using the Web user interface.

Dormant file timeout - Set the inactivity timeout in minutes. This will indicate the amount of time that will elapse before a file handle that is opened by the desktop client will be considered dormant and will be closed automatically by the server. When editing a document by a desktop application, the application will open the file handle and generally read data from the file. Even if the application opens a file and reads data from it, but then does not close the file handle, the desktop client software will automatically periodically send a keep-alive request to the server so that it will not close the file handle. Generally, this timeout is useful only if, for some reason, a desktop client opened a file but then the user turned off power on the computer so that the client could not send keep-alive requests. If this does occur, then the server will close the file handle after the timeout period expires.

O'CLOCK Acknowledge timeout - Set the time to wait in seconds for a desktop client to acknowledge an **O'CLOCK** acknowledge. **OPLOCKS** are "opportunity locks" that the desktop client will take out on a file so that it can cache file data. If another user opens the same file that another user has already opened and it has an **OPLOCK** on it, then the server will "break" the **O'CLOCK** with the first user. Before returning a file handle to the second user, the server will wait for an acknowledgement from the desktop client for the first user. If the desktop client does not respond in this "timeout" period, then the server will break the **OPLOCK** and allow the second user to continue.

Server Directories Tab

Use the server **Directories** tab to manage the location of various server directories.

To access the server **Directories** tab, in the tree pane, select the **Server**. In the tab pane, select the **Directories** tab.

Use the browse "... " button to change the location of a directory.

User Data Directory - The relative path to the server data directory where user data directories will be created. By default, the User Directory is set to User, so if the Server Data Directory is set to **c:\srtData\MyServer** then a user whose name is john would store his files in the **c:\srtData\MyServer\User\john** folder. The user folder will be created when the user first logs onto the GroupDrive server.

Logfile Directory - The relative path to the location where the log files will be stored.

System Database Directory - The base directory where all file data will be stored. Note: The GroupDrive Server runs as an NT Service that, by default, does not have access to shared network resources or mapped drive letters because these are based on the currently authorized NT user. If you are configuring your Server Data Directory to be a network resource, you must manually reconfigure the GroupDrive Server Service/Daemon so that it "Logs In" using an NT User account that has access to network resources. The default NT Service account, Local System, does not have access to network resources.

Temporary Cache Directory - The relative path to the location where the temporary cache will be stored.

SSL Certificate Store Directory - The relative path to the location where SSL certificates will be stored.

Authentication Server Settings Tab

Use the server **User Authentication** tab to configure settings for the authentication method to be used for GroupDrive users for this server. If you are configuring a new server, use the [New Server Wizard](#) to configure your authentication method.

We recommend that you read the [User Authentication Overview](#) topic.

To access the server **User Authentication** tab, in the tree pane, select the **Server**. In the tab pane, select the **User Authentication** tab.

Authentication Database - Displays the user authentication method that is used by this server. **NOTE:** Once you select a user authentication database option in GroupDrive, you cannot change to a different method once the server wizard has completed.

Authentication Server Setup... - Launches the [User Authentication Configuration Wizard](#). GroupDrive currently supports the following user authentication methods:

- **Native GroupDrive Server User Authentication**
- **Windows NT/SAM User Authentication**
- **Windows Active Directory User Authentication**
- **Standard LDAP User Authentication**
- **ODBC Data Source User Authentication**

Use NTFS Permissions and ACLs for User Rights - If you are using Windows NT authentication, enable this feature to have GroupDrive use existing NTFS file permissions and ACLs (Access Control Lists) for GroupDrive user rights.

Enable Digest Authentication - Enables the Digest HTTP authentication method. Web browsers and the GroupDrive desktop client support Digest authentication. Digest authentication is more secure than basic authentication but not as secure as Integrated Windows authentication.

Enable Basic Authentication - Enables Basic HTTP Authentication. Basic authentication is the least secure authentication scheme, however some browsers or DAV clients might not support Digest or Windows authentication. If security is a concern, you can use SSL to secure the connection.

Integrated Windows Authentication - Enables the Windows NTLM/Negotiate challenge response authentication scheme. This is only available when using Windows user authentication. To use this option the GroupDrive server must also be running on the machine that hosts the NT user database. The GroupDrive desktop client will use Windows authentication to the GroupDrive server if this setting is enabled.



For more information about configuring user authentication, see the GroupDrive [Quick Start Guide](#) for your specific user authentication method.

User Authentication Wizard

To access the **User Configuration** wizard for an existing server, in the tree pane, select the **Server**. In the tab pane, select the **User Authentication** tab and then click the **Authentication Server Setup** button. If you are configuring a new server, use the **New Server Wizard**.

We recommend that you read the [User Authentication Overview](#) topic.

The GroupDrive Server User Configuration wizard allows you to configure various user authentication options for the following user authentication methods:

- Native GroupDrive User Authentication
- Windows NT/SAM User Authentication
- Windows Active Directory User Authentication
- Standard LDAP User Authentication
- ODBC Data Source User Authentication



- Once you select a User Authentication Database option in GroupDrive, you cannot change to a different method once the server wizard has completed.
- For more information about configuring user authentication, see the GroupDrive [Quick Start Guide](#) for your specific user authentication method.

Security Settings (SSL) Tab

Use the server **HTTPS/SSL** tab to manage SSL settings for the server.

To configure HTTPS/SSL settings for a new server, use the [New Server Wizard](#). To access the server **HTTPS/SSL** tab to manage HTTPS/SSL settings, select the **Server** in the tree pane, and in the tab pane, select the **HTTPS/SSL** tab.

Enable SSL on this server - When enabled, the server will be able to conduct secure transfers using SSL.

SSL Port - The port to use for SSL connections.

Allow non-SSL connections to this server - Clients are still allowed to use the standard non SSL port.

Require Trusted Certificates - When enabled, requires clients that connect securely to the server to supply a certificate.

Server Certificate Settings - Displays the current public key certificate in use by the server. In order to use SSL, you **must** have a valid server certificate.

Certificate Manager - Launches the Certificate Manager to create or import certificates for this server. User certificates can be imported into the certificate store so that the server can validate client side certificates.

Certificate Store - Select the folder to use for the certificate store for this server.



- For more information about configuring SSL & public key certificate-based authentication, see the [SSL Support](#) topic and the GroupDrive SSL & Public Key Certificate-based Authentication [Quick Start Guide](#).

Server Directory Quotas Tab

The server **Quota** tab is used to configure directory quota limits for the server.

To access the server **Directory Quota** tab, select the **Server** in the tree pane. In the tab pane, select the **Quota** tab.

Enable Directory Quotas - When enabled, the server will process Quota limits on directories.

Set Default user Quota for new Users - Select this check box to set a directory quota for new users.

Default user Quota limit - Specify the default quota amount in bytes for new users. The default amount is 2,000 MB.

Server IP Access Restrictions Tab

The **IP Access** tab is used to configure TCP/IP Access restrictions for the server.

To access the server **IP Access** tab, select the **Server** in the tree pane. In the tab pane, select the **IP Access** tab.

Enable IP Access Restrictions - When enabled, IP Access restrictions will be applied to this server whenever a user attempts to connect.

Grant/Deny access to all IP Addresses by default - Select the default action that will be applied to this server when a connection attempt is made.

Exception List - Type a list of IP addresses which will be the exception to the default rule. For example, you can **Deny Access to all IP Addresses by default** and then enter a single IP address. This will then be the only IP address that the user will be permitted to connect from. When you use GroupDrive Collaboration Server Event Management to ban an IP address, the IP address will appear on this list once the IP address has been banned. Use the **Add, Edit, Remove** buttons to manage this list.

Server Connection Settings Tab

Use the server **Connections** tab to configure various connection settings for this server.

To access the server **Connections** tab, select the **Server** in the tree pane. In the tab pane, select the **Connections** tab.

Disabled account after X bad password attempts - When enabled, the user account will be disabled after X number of consecutive incorrect password attempts.

Idle TCP connection timeout - When enabled, socket connections that are idle for the specified number of minutes will be automatically disconnected.

Max concurrent connections - Enable this option to set the maximum number of simultaneous socket connections. Once this limit is reached, connections will be refused until a connection is closed. **Note:** this setting should not be confused with the maximum number of concurrent **users** that could be supported. HTTP sessions do not require that an active socket connection be maintained.

Max Keep-Alive requests - When enabled, this option will limit the number of commands that will be allowed on a HTTP Keep-Alive socket connection. HTTP clients can request that the connection be kept open "alive" after processing a command so that another command can be sent without having to establish a new connection. The ability to keep the connection open between requests can greatly increase performance. In general, for the best performance, it is best that you do not enable this setting or that you set it to a very high number of requests.

User Rights Tab

Use the **Rights** tab to set administrative privileges for users and groups.

Rights vs. Permissions

GroupDrive Server user **rights** are not the same as GroupDrive file system [permissions](#). User rights are authorized by the System Administrator and generally refer to **system actions**, such as the ability of a user to **share** or **download** file and folder objects. Permissions pertain to the **level of access** granted to a specific shared resource, such as the level of access a user has to a file or folder object. Permissions can be set by the System Administrator or the owner of the file or folder object.

User Rights Tab

To access the server user **Rights** tab, select the **Server** in the tree pane. In the tab pane, select the **Rights** tab.

For each specific right there is an **Allow right to** and a **Deny right to** list to control the rights of users. The deny list takes precedence over the allow list.

Share files and folders - Allows user to share files and folders with other users. If this right is enabled then the user is also allowed to set/get permissions on file objects. Default setting: **Allow right to Everyone**.

Set/Get permissions on file objects - Allows users to view and set permissions on file objects. Default setting: **Allow right to Everyone**.

Link to shared files and folders - Allows users to link to shared objects. Default setting: **Allow right to Everyone**.

E-mail links to files and folders - Allows users to email links to files and folders. Default setting: **Allow right to Everyone**.

Set quota limits on folders - Sets a quota limit on the files that can be uploaded to the server. Default setting: **Allow right to Everyone**.

Open folders as picture slide shows - Opens folders as slide shows. Default setting: **Allow right to Everyone**.

Download files/folders as ZIP files - Allows users to download files/folders as ZIP files. Default setting: **Allow right to Everyone**.

Create user accounts - Allows users to create user accounts. Default setting: **Deny right to Everyone**.

Delete user accounts - Allows users to delete user accounts. Default setting: **Deny right to Everyone**.

View user account settings - Allows users to view user account settings. Default setting: **Deny right to Everyone**.

Modify user account settings - Allows users to modify user account settings. Default setting: **Deny right to Everyone.**

Create groups - Allows users to create groups. Default setting: **Deny right to Everyone.**

Delete groups - Allows users to delete groups. Default setting: **Deny right to Everyone.**

View group settings - Allows users to view group settings. Default setting: **Deny right to Everyone.**

Modify group settings - Allows users to modify group settings. Default setting: **Deny right to Everyone.**

Create server configurations - Allows users to create server configurations. Default setting: **Deny right to Everyone.**

Delete server configurations - Allows users to delete server configurations. If a server is deleted all user/group information is deleted. Deletion of a server is **permanent**. Default setting: **Deny right to Everyone.**

View and modify server configurations - Allows users to view and modify server configurations. Default setting: **Deny right to Everyone.**

Start and stop servers - Allows users to start and stop servers. Default setting: **Deny right to Everyone.**

Modify general server settings - Allows users to modify general server settings. Default setting: **Deny right to Everyone.**

View general server settings - Allows users to view general server settings. Default setting: **Deny right to Everyone.**

Modify advanced server settings - Allows users to modify advanced server settings. Default setting: **Deny right to Everyone.**

View advanced server settings - Allows users to view advanced server settings. Default setting: **Deny right to Everyone.**

Modify server authentication settings - Allows users to modify server authentication settings. Default setting: **Deny right to Everyone.**

View server authentication settings - Allows users to view server authentication settings. Default setting: **Deny right to Everyone.**

Modify server certificate information - Allows users to modify server certificate information. Default setting: **Deny right to Everyone.**

Modify server security settings - Allows users to modify server security settings. Default setting: **Deny right to Everyone.**

View server security settings - Allows users to view server security settings. Default setting: **Deny right to Everyone.**

Modify server logging settings - Allows users to modify server logging settings. Default setting: **Deny right to Everyone.**

View server logging settings - Allows users to view server logging settings. Default setting: **Deny right to Everyone.**

Modify server quota settings - Allows users to modify server quota settings. Default setting: **Deny right to Everyone.**

View server quota settings - Allows users to view server quota settings. Default setting: **Deny right to Everyone.**

Modify server IP access settings - Allows users to modify server IP settings. Default setting: **Deny right to Everyone.**

View server IP access settings - Allows users to view server IP access settings. Default setting: **Deny right to Everyone.**

Modify server connection settings - Allows users to modify server connection settings. Default setting: **Deny right to Everyone.**

View server connection settings - Allows users to view server connection settings. Default setting: **Deny right to Everyone.**

Modify server rights settings - Allows users to modify server rights settings. Default setting: **Deny right to Everyone.**

View server rights settings - Allows users to view server rights settings. Default setting: **Deny right to Everyone.**

Modify server statistics settings - Allows users to modify server statistics settings. Default setting: **Deny right to Everyone.**

View server statistics settings - Allows users to view server statistics settings. Default setting: **Deny right to Everyone.**

View server session activity - Allows users to view server session activity. Default setting: **Deny right to Everyone.**

View server statistics activity - Allows users to view server statistics activity. Default setting: **Deny right to Everyone.**

View server log activity - Allows users to view server log activity. Default setting: **Deny right to Everyone.**

Access server file system settings - Allows users to access server file system settings. Default setting: **Deny right to Everyone.**

Access server virtual folder settings - Allows users to access server virtual folder settings. Default setting: **Deny right to Everyone.**



- For more information about **setting permissions for files/folders**, see the [File System Permissions](#) topic.

Email Server Tab

Use the **Email Server** tab to configure mail server settings.

To access the **Email Server** tab, in the tree pane, select the **Server**. In the tab pane, select the **Email Server** tab.

SMTP Server IP or Hostname - Type the name of the SMTP server or the Hostname.

Mail Server Username - Type the mail server username.

Mail Server Password - Type the mail server password.

Test Connection - Click Test Connection to test the mail server connection.

Flood Protection/DoS Tab

Use the server **Flood Protection/DoS** tab to configure flood protection (DoS/Hammering) settings.

To access the **Flood Protection/DoS** (Denial of Service) tab, in the tree pane, select the **Server**. In the tab pane, select the **Flood Protection/DoS** tab.

Enable Flood Protection (DoS/Hammering) - This option is enabled by default. Clear this check box to disable Flood Protection.

X connections received from an IP address within X seconds - Set the number of connections received from an IP Address within X amount of time, measured in seconds. The default is 200 connections received within 5 seconds.

Action - Use the radio button to select Ban IP Address Forever or Ban IP Address for X minutes. The default is 60 minutes.

UNC Accounts Tab


Use the **UNC Accounts** tab to set the list of logins for UNC (Universal/Uniform Naming Convention) shares and other restricted resources. Use the UNC Accounts tab 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. Since GroupDrive Service usually runs under the context of a Local System NT Account that is defined for the local computer, 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.

To access the **UNC Accounts** tab, in the tree pane, select the **Server**. In the tab pane, select the **UNC Accounts** tab.

Username - Type the Username. The Username can be simply a user name or **<username@domain>** or **<domain/username>**.

Password - Type the Password. The password will be used for authentication against the remote UNC share.

UNC Account List - Displays the list of usernames for users who are allowed to access the UNC shares.

	<ul style="list-style-type: none">• 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.• For more information about configuring UNC shares, see the GroupDrive Collaboration Server Using UNC Paths for Data Storage & Scalability Quick Start Guide.
---	--

DMZedge Tab

Use the **DMZedge** tab to configure DMZedge server settings. The DMZedge Server enables you to close inbound ports on your firewall, reducing the risk of network intrusion and enabling the highest level of security for both data storage and transfers. When combined with GroupDrive Collaboration Server, the DMZedge Server uses a two-way connection originating from the GroupDrive Server that is inside of the firewall on your corporate LAN (Local Area Network). The DMZedge works as a communication proxy, shielding your internal network from unsecure inbound connections.

To access the **DMZedge** tab, in the tree pane, select the **Server**. In the tab pane, select the **DMZedge** tab.

Server URL - Type the Server URL that will contact the DMZedge Server.

Server Port - Type the Server Port to use to contact the DMZedge Server. The default port is port 45000.

DMZedge should accept DAV/HTTP connections - Select this check box to allow DMZedge to accept DAV/HTTP connections.

DAV/HTTP Listening Port - Type the DAV/HTTP Listening Port. The default listening port is port 80.

DMZedge should accept HTTPS connections - Select this check box to allow the DMZedge to accept HTTPS (secure) connections.

HTTPS Listening Port - Type the HTTPS (secure) Listening Port. The default listening port for secure connections is port 443.



For more information about DMZedge, see the [DMZedge User's Guide](#).

Server Logging Settings

Server Log Tab

Use the **Server Log** tab to view the entire logfile.

To access the **Server Log** tab, in the tree pane, expand the **Server** and click **Logging**. In the tab pane, select the **Server Log** tab.

Auto-refresh list every: x Seconds - Select this check box to enable auto-refresh of the logfile list. The default is one second.

Refresh - Click **Refresh** to immediately refresh the logfile window.

View Entire Logfile - Opens the logfile in Windows Notepad.

Clear Log Window - Clears the log window.

Server Log Settings Tab

Use the **Server Log Settings** tab to configure the logging options for the server.

To access the **Server Log** settings tab, in the tree pane, expand the **Server** and click **Logging**. In the tab pane, select the **Server Log** tab.

Enable Logging to file - Select this option to enable logging to a disk file. This is HIGHLY recommended.

Enable Logging to screen- Select this option to enable logging to the **Activity screen** in the GroupDrive Server Administrator program.

Log Directory - Specifies the location where log files will be stored. Use the browse "... " button to change the location.

Explore Log Directory - Launches Windows Explorer so that you can browse the contents of the Log Directory for this server.

Logfile Format- Select the output format for the server log file.

- **Plain Text Format** - Select this format to have log entries dumped in plain text format (default).
- **W3C Extended Log File Format** - Select this formation to have log entries dumped in a format compatible with the W3C standard.

Log Fields - Select the fields that you like to include in the log file: **Date, Time, ServerID/Socket#, Message**.

Information Level - Select the Information Level that you would like to include in the log file: **General, Verbose/Detailed, Debug**.

Word wrap log text - Select this check box to enable word wrap for the log text.

Log Rotation - Select the rotation schedule for log files. This option dictates how often a new log file is created. Selecting **Never** is highly discouraged because the log files can become very large.

Server Client Log Settings Tab

Use the **Client Log Settings** tab to set the settings for the desktop client file I/O (input/output) log.

To access the **Client Log Settings** tab, in the tree pane, expand the **Server** and select **Logging**. In the tab pane, select the **Client Log Settings** tab.

Desktop Client File I/O Logging - Specifies the type of Desktop Client operations that will be logged. Logging all desktop client I/O can slow down the server and consume log file space.

All File I/O - Enable this option to log all file I/O.

To enable file logging for any of the following options, select the check box.

- **Open/Close File**
- **Read File**
- **Write File**
- **Lock/Unlock record**

Enable Web Interface Verbose Logging - Select the check box to enable verbose (highly detailed) logging for Web interface activity.

Statistics Tracking Tab

Use the **Statistics Tracking** tab to configure statistics options in GroupDrive Server. To access the **Statistics Tracking** tab, in the tree pane, expand the **Server**, and click **Logging**. In the tab pane, select the **Statistics Tracking** tab.

GroupDrive Statistics Tracking allows you to log actions to a database through ODBC (Open Database Connectivity). By default, GroupDrive uses a Microsoft Access Database; however, you can configure GroupDrive to use any database through an ODBC Datasource. When users upload/download/delete files, the actions will be recorded into the **Statistics Database**. The Web interface has a **History** page that allows users to query the database for past actions on files or folders. For reports that are more detailed you can open the database with any standard database reporting tool and create your own queries.

Enable Statistics Tracking - Select the check box to enable Statistics Tracking.

ODBC Datasource - Use the browse "..." button to browse to your ODBC datasource. Click **Test** to make sure the datasource is valid.

Prune/Purge old statistics every - Allows you to delete old statistics so that the database does not become bloated.

Archive old statistics before pruning - If this option is enabled, the contents of the statistics table will be backed up to an archive table before the statistics table is pruned.

Statistics to track - select **Check All** to track all statistics or select the check box for specific statistics that you would like to track:

- | | |
|---|---|
| <input type="checkbox"/> File Uploads | <input type="checkbox"/> Client Disconnects |
| <input type="checkbox"/> File Downloads | <input type="checkbox"/> Directory Listings |
| <input type="checkbox"/> User Login Attempts | <input type="checkbox"/> Delete Files |
| <input type="checkbox"/> User Logout Attempts | <input type="checkbox"/> Delete Folders |
| <input type="checkbox"/> Client Connection Attempts | <input type="checkbox"/> Create Folders |



- ODBC must be installed on your system before you can use the statistics tracking features of GroupDrive. When Statistics Tracking is enabled, a database will be created in the server data directory under the **\database** directory.
- Please note that in many cases creating an **Event Handler** is a helpful approach to tracking and responding to server events. See [Event Management](#) for more information.

Server Activity Settings

Sessions Tab

Use the **Sessions** tab to view current session activity for users.

To access the **Sessions** tab, in the tree pane, expand the **Server** and select **Activity**. In the tab pane, select the **Sessions** tab.

Auto refresh user list every: X Seconds - Select the check box to enable this option. Enter the amount of time, in seconds, that you would like the list to refresh. The default is one second.

Refresh Now - Click Refresh Now to immediately refresh the list.

Session Id - Displays the current Session Id for the user.

Username - Displays the username for the current session.

IP Address - Displays the IP Address for the current session.

Created - Displays the date and time that the current session was created.

Idle Time - Displays the amount of time that has elapsed since the current session has had activity.

Statistics Tab

Use the **Statistics** tab to view the current activity and statistics for the server.

To access the **Statistics** tab, in the tree pane, expand the **Server** and click **Activity**. In the tab pane, select the **Statistics** tab.

Auto refresh user list every X Seconds - When this option is enabled, the user list will be refreshed every X seconds. This option is enabled by default.

Refresh Now - Click Refresh Now to immediately refresh the user list.

Is Online - Indicates if the server is online.

Server Start Time - Displays what time the server was started.

Running Time - Displays the total running time since the server was started.

Active Connections - Displays the total number of active connections.

Active SSL Connections - Displays the total number of active SSL (secure) connections.

Active Sessions - Displays the total number of active sessions.

Active Public Sessions - Displays the total number of active public sessions.

Open file handles - Displays the total number of file transfers in process.

Transactions/last second - Displays the total number of transactions during the last second. Click Refresh Now to immediately update this value.

Transaction Total - Displays the total number of transactions that have taken place since the server was started.

Total Bytes Received - Displays the total bytes received, in KB, since the server was started.

Total Bytes Sent - Displays the total bytes sent, in KB, since the server was started.

Total File Transfer Bytes Received - Displays the total file transfer bytes received, in KB.

Total File Transfer Bytes Sent - Displays the total file transfer bytes sent, in KB.



Please note that in many cases creating an **Event Handler** is a helpful approach to tracking and responding to server events.

Event Management

Event Management Overview

You can utilize the event management functions in GroupDrive Collaboration Server in a variety of ways, from automating processes to thwarting hacking attempts. You can also use event management for statistics tracking or notification purposes. For example, so that you will know when files have been uploaded or downloaded.

A few more examples of what the Event Handling system can be used for include:

- Notify the administrator every time the server is started.
- Create an event log that logs every event that occurs on the server.
- Create user accounts that expire after a single use.
- Send an e-mail when a user account is near expiration.
- Create custom log files for each user account.
- Move/off-load a file on the server after it has been uploaded.
- Constrain certain users/groups to a limited command set.
- Create a directory log for each shared folder, so that whenever anything happens in that folder, an entry is added.
- Create command logs for every command entered.
- Kick any lower-class users (members of a less privileged group) if the number of connections to the server reaches a certain threshold.
- Send an e-mail to the administrator every hour showing the current status of the server.

Server events are managed by Event Handlers. Event Handlers are used to trigger customized actions based on specific events and conditions. Events are fired whenever anything of importance occurs on the server, such as a user logging in or a file being uploaded. Multiple Event Handlers can be configured for each server, depending on your needs. The GroupDrive Collaboration Server Event Wizard is used to create the Event Handler. Event Handlers are triggered depending upon the specifications that the you set up using the Event Wizard.

An Event Handler consists of the Event, the Condition, and the Action.

Event - The event triggers the Event Handler Action depending upon a specified Condition. For example, if a login attempt fails or if a file is downloaded.

Condition - The condition specified for the event. Depending on the condition set for the event, an Action will be triggered. For example, if a user or group name does or does not match an authorized list of users or a file name does or does not match a specified file. You can also select All Conditions so that the specified action will take place every time that event takes place.

Action - The action that will take place for an event if it meets the specified conditions. For example, kick user or send e-mail.

Performance

The Event Handler system was designed for efficient performance, but it is possible to design an Event Handler that will slow down the server. Therefore, care must be taken to ensure that system performance is not adversely affected.

Logging

When creating a custom log, ensure that the file is periodically rotated or renamed to prevent large file sizes. Appending to large files (1MB+) will cause a noticeable delay, especially if the log is being updated frequently.

Flag for admin review

The Flag for admin review action was not designed to be triggered frequently. Overuse of this action will cause the Flagged Events list to become bloated. As this list grows, especially beyond a few hundred entries, performance will deteriorate.

Send e-mail

Depending on your e-mail system, sending e-mail frequently could slow performance. In addition, many e-mail servers have spam countermeasures, which may block e-mails or even blacklist the sender.

Event Management Best Practices

Regardless of the event and action configuration for each event, whenever you create new events it is a good idea to send an email notification to the system administrator, especially if you have defined an action that bans someone from accessing the system. Although rare, on occasion, a valid user may misspell his user name or some other error may occur that causes a valid user to be banned from the system.

Using Events to Thwart Hackers

One of the most common server problems involves unauthorized users or hackers attempting to guess user names and passwords in order to gain access to the server.

GroupDrive Collaboration Server Event Management can help thwart hacking attempts by detecting invalid user attempts. GroupDrive will kick that connection from the server and ban future access from the client IP address.



For more information about configuring an Event Handler to thwart hackers, see the [GroupDrive Collaboration Server Using Events to Thwart Hackers Quick Start Guide](#).

Event Handlers Tab

Use the Event Handlers tab to add, modify, or view an Event Handler. The Event Handlers tab is used to view, create, modify, and delete Event Handlers. Event Handlers are used to trigger customized actions based on events and conditions. We recommend that you read the [Event Management Overview](#) before you configure an Event Handler in GroupDrive Server.

To access the **Event Handlers** tab, in the tree pane, expand the **Server** and click **Events**. In the tab pane, select the **Event Handlers** tab.

Add - Click **Add** to add a new Event Handler for this server. This will launch the Event Handler Wizard.

Edit - Click **Edit** to edit an existing Event Handler. This will launch the Event Handler Wizard.

Enable/Disable - To enable or disable one or more Event Handlers, select the **Event Handler** and click **Enable** or **Disable**. Enabled Event Handlers will appear in black text, while disabled Event Handlers will appear in gray text.

Remove - To remove one or more Event Handlers, select the **Event Handler** and click **Remove**.

Event Handler Wizard

Event Handler Wizard Overview

Use the **Event Handlers** tab to manage and create Event Handlers in GroupDrive Server. Multiple Event Handlers can be configured for each server, depending on your needs.

We recommend that you read the [Event Management Overview](#) before configuring an Event Handler in GroupDrive Collaboration Server.

To access the **Event Handler Wizard**, in the tree pane expand the **Server** and click **Events**. In the tab pane select the **Event Handlers** tab and click **Add** to add a new Event Handler. If you would like to edit an Event Handler, select the **Event Handler**, and click **Edit**. The Event Handler Wizard will launch.

An Event Handler consists of the **Event**, the **Condition**, and the **Action**.

Event - The event triggers the Event Handler Action depending upon a specified Condition. For example, if a login attempt fails or if a file is downloaded.

Condition - The necessary condition specified for the event. Depending on the condition set for the event, an Action will be triggered. For example, if a user or group name does or does not match an authorized list of users or a file name does or does not match a specified file. You can also select All Conditions so that the specified action will take place every time that event takes place.

Action - The action that will take place for an event if it meets the specified conditions. For example, kick user or send e-mail.

The Event Handler Wizard will prompt you to select one or more **events**, one or more **conditions**, and one or more **actions** for the Event Handler. Depending on what you select, the Event Handler Wizard will prompt you for the necessary information. You will also be prompted to name the Event Handler.

Event Handler Wizard-Set Events

Events are organized into a relational hierarchy that provides a mechanism to handle events generically. For example, you can select specific events or you can select the **All events** event, which can be used as a basis to handle every server event. You can then modify the action for that event trigger by setting a condition for the event.

All Events - Encompasses every server event listed below.

Scheduled event - Use this event to set up a one-time or repeatable event that will run based on the current time. This event type must have a corresponding Scheduled time elapsed Condition.

Server events - This is the parent event for any server-specific events.

Server start succeeded - This event fires every time the server starts.

Server start failed - This event fires when the server fails to start because of any of the specific failures listed below. This event can be used as a "catch all" event to trap any server start failure.

Server start failed -- Statistics failed - The server failed to start correctly because the Statistics subsystem failed to initialize.

Server start failed -- HTTP failed - The server failed to start correctly because the HTTP subsystem failed to initialize. This often indicates a port conflict.

Server start failed -- HTTPS failed - The server failed to start correctly because the HTTPS subsystem failed to initialize. This often indicates a port conflict.

Server stopped - The server has stopped. This event is triggered if the server is stopped or if the server is restarted, in which case, a Server start event would immediately follow.

Server log rotated - The server log has been rotated. This occurs every time the server starts, any time the log rotation period expires, or any time the Administrator manually rotates the log.

Connection attempt failed - A client connection attempt has failed.

Connection attempt failed -- Banned IP address - A client connection attempt has failed because the IP address is banned at the server level.

Connection attempt failed -- Server Hammering - A client connection has failed because the IP address has been banned at the server level (per the [Flood Protection/DoS Hammering settings](#)).

User events - This is the parent event for any user-specific events.

User login attempt successful - A user has successfully logged in.

User login attempt failed - A user login attempt has failed.

User login attempt failed -- Bad username - The username specified does not exist.

User login attempt failed -- Bad password - The password specified does not match the correct password for the supplied username.

User login attempt failed -- Password expired - A user login attempt failed because the user's password is expired. Expired passwords are always disabled.

User login attempt failed -- Account disabled -- Account expired - A user login attempt failed because the specified username is expired. Expired accounts are always disabled.

User account created - A user account has been created.

User account deleted - A user account has been deleted.

File events - This is the parent event for any file-specific events.

File download/read - This is the parent event for any file download/read events.

File download/read -- Download/read successful - A file has been successfully downloaded.

File download/read -- Download/read failed - A file download has failed.

File upload/write - This is the parent event for any file upload/write events.

File upload/write -- Upload/write successful - A file has been successfully uploaded.

File upload/write -- Upload/write failed - A file upload has failed.

File delete - This is the parent event for any file delete events.

File delete -- Delete successful - A file has been successfully deleted.

File delete -- Delete failed - A file delete has failed.

File rename - This is the parent event for any file rename events.

File rename -- Rename successful - A file has been successfully renamed.

File rename -- Rename failed - A file rename has failed.

Directory events - This is the parent event for any directory-specific events.

Directory created - This is the parent event for any directory created events.

Directory created -- Directory create successful - A directory has been successfully created.

Directory created -- Directory create failed - A directory created has failed.

Directory removed - This is the parent event for any directory removed events.

Directory removed -- Directory remove successful - A directory has been successfully removed.

Directory removed -- Directory remove failed - A directory remove has failed.

Event Handler Wizard-Set Conditions

Depending on the condition set for the event, an action will be triggered. A condition modifies when the action will occur in accordance with the event. The condition is an important prerequisite for the action to take place. For example, if a user or group name does or does not match a previously defined authorized list of users or if a file name does or does not match a previously defined specified file, then the action will not take place. Select conditions to fine-tune Event Handler definitions to handle specific cases. Different conditions apply to each event type. When you are creating an Event Handler, be careful not to create conditions that are never satisfied.

All Conditions - Not available in the current version of GroupDrive Server.

User name - Use this condition to specify one or more usernames. If any of the specified usernames match the username of the account that caused the event to be triggered, the condition will be satisfied. Wildcards can be used, for example, specifying "*z*" in the list would cause the condition to be satisfied for any username which contains a "z".

User group membership - Use this condition to specify one or more groups. If any of the specified groups match the group membership of the account that caused the event to be triggered, the condition will be satisfied. Wildcards can be used, for example, specifying "grp*" in the list would cause the condition to be satisfied for any group names that begin with "grp".

User account expiration date - Use this condition to specify a time range for account expiration date values. The time range can either be less than or greater than a set number of days/hours/minutes/seconds. If the account that caused the event to be triggered has a valid expiration date within the specified range, the condition will be satisfied. For example, specifying Less than and 20 days means that the condition will be satisfied if the user account is expiring within the next 20 days. This condition is very useful to remind users and administrators that an account will soon be expiring.

User enabled - Use this condition to specify whether or not an account is expired. If the account that caused the event to be triggered matches this specified value, the condition is satisfied.

IP address - Use this condition to specify one or more IP addresses. If any of the specified IP addresses match the IP address of the account that caused the event to be triggered, the condition will be satisfied. Wildcards can be used, for example, specifying "123.*.*" in the list would cause the condition to be satisfied for any IP address that starts with "123".

Connection time - Use this condition to specify a time range for the connection time. The time range can either be less than or greater than a set number of days/hours/minutes/seconds. If the connection that caused the event to be triggered has a connection time that is within the specified range, the condition will be satisfied. For example, specifying More than and 1 days means that the condition will be satisfied if the connection has been alive for more than one day.

Scheduled time elapsed - Use this condition in conjunction with the Scheduled event. For a one-time scheduled event, simply specify the date/time you wish the event to occur. This one-time condition is satisfied if the current system time is beyond the First occurrence time. For a repeatable scheduled event, specify the date/time of the first occurrence, and the repeat interval. The repeatable condition is satisfied if the current system time is beyond the First occurrence time and it has been at least Repeat Interval units of time since the condition was last satisfied. The repeatable condition will keep track of the last time the condition was satisfied so that it does not repeat more than once in any Repeat Interval units of time.

Event Handler Wizard-Set Actions

Actions are used to implement the server's response to a specific event. The action will take place for an event if it meets the specified conditions. For example, **kick user** or **send e-mail**.

All Actions - This action is not available in the current version of GroupDrive Server.

Do not process command - This action is not available in the current version of GroupDrive Server.

Send email - Causes an e-mail to be sent, provided you have a SMTP mail server that will handle the request. SMTP mail server configuration is set at the Server level on the **E-Mail Server** tab. The following fields may be set for the Send email action:

- **From** - Specifies the email address from which the email will be sent.
- **To** - Specifies the email address to which the email will be sent. For instance, you could specify the **%USEREMAIL%** variable in the case where a user-triggered event has occurred and you wish to notify that user. Use the Show Variables button to see a list of variables. You can send the email to more than one person by separating addresses with a semicolon. For example, **bob@abc.com; joe@abc.com**
- **Subject** - Specifies the text that will go into the email subject line.
- **Body** - Specifies the text that will go into the body of the email.

Flag for admin review - Causes a Flagged Event to be created, which will appear on the Flagged Events tab. The **Flag for admin review** action was not designed to be triggered frequently. Overuse of this action will cause the Flagged Events list to become bloated. As this list grows, especially beyond a few hundred entries, performance will deteriorate.

Run file/script - Launches a file/script with optional command line parameters. The following fields may be set for the Run file/script action:
File/script - Specifies the location of the file/script to be run.

Parameters - Specifies any command line arguments to the file. Add each parameter to the parameter list in the order in which they should be passed to the file/script. Any parameters that could contain a space should always be wrapped in double quotes.

Examples:

C:\long file name.txt

%FILEPATH%

Write to custom logfile - Writes a message to a log file. The following fields may be set for the **Write to custom logfile** action:

- **Logfile** - Specifies the location of the file that the message will be written to.
- **Log text** - Specifies the message that will be written to the log file.

Ban IP address - Bans an IP address. The following field may be set for the Ban IP address action:

- **IP address** - Specifies the IP address to ban.

Kick user - Kicks a user from the server. The following field may be set for the Kick user action:

- **Username** - Specifies the username of the account you wish to kick from the server.

Disable user account - Disables a user account. The following field may be set for the Disable User account action:

- **Username** - Specifies the user name of the account you wish to disable on the server.



The **Flag for admin review** action was not designed to be triggered frequently. Overuse of this action will cause the Flagged Events list to become bloated. As this list grows, especially beyond a few hundred entries, performance will deteriorate.

Flagged Events Tab

The **Flagged Events** tab displays a list of events triggered by your Event Handler that are **Flagged for Admin Review**.

To access the **Flagged Events** tab, in the tree pane, expand the **Server** and click **Events**. In the tab pane, select the **Flagged Events** tab.

The **Flagged Events** tab displays the name of the event and the date and time that the event occurred.

Once you have reviewed there event, it you can delete it from the list. To delete the event, select the event in the list and click **Remove From List**.

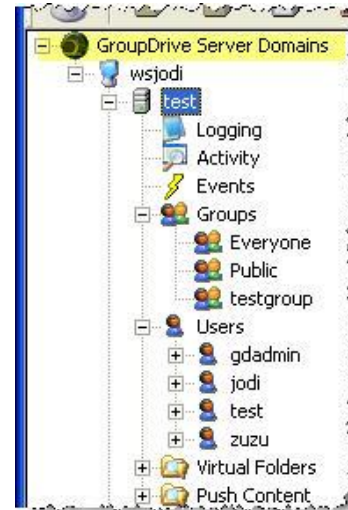
The **Flag for admin review** action was not designed to be triggered frequently. Overuse of this action will cause the Flagged Events list to become bloated. As this list grows, especially beyond a few hundred entries, performance will deteriorate.

Group Configuration

Groups Overview

Groups provide the ability to associate multiple users with similar characteristics. You can use groups as a convenient and efficient way to set file system access [permissions](#) that will apply to all members of the group.

By default, GroupDrive Server will generate a global system group called **Everyone**. The **Everyone** group cannot be deleted. All users are members of the **Everyone** group, so keep this in mind, and use discretion when you adjust the access permissions for this group. **NOTE:** The **Everyone** group is not created when using Windows NT Authentication, use the NT user manager to create or manage an **Everyone** group.



The GroupDrive server also generates a global system group called **Public** that applies to users that do not require authentication to the GroupDrive server. If a user grants read permissions to the group **Public Access** for one of his files or folders, then the user will be able to e-mail a hyperlink to the folder or file and anybody can access the folder or file using the hyperlink without authentication. This is very useful for sharing pictures or documents to non-GroupDrive users. You can still assign limited read-only access to the document when using the **Public Access** group.

You can setup an unlimited number of Groups for each server. Each Group can have zero or more Users. You can also add the same user to multiple groups.



- **All GroupDrive Server users must belong to a group.** If you are using a user authentication method other than native GroupDrive Server user authentication, we recommend that you read the [User Authentication Overview](#) topic.
- For more information about configuring **user authentication**, see the GroupDrive [Quick Start Guide](#) for your specific user authentication method.

Creating New Groups

In the GroupDrive Server [Administrator](#), expand the server in the tree pane, right-click the **Groups** icon and select **New Group**. The **New Group Wizard** will launch.


or

From the main menu, select **Server>Groups>New Group Wizard**.

or

Click the **Groups** icon in the left pane (tree pane) of the Administration program. This will cause a list of groups to be generated and displayed in the right pane (tab pane). Click the **New Group** button in the tab pane to launch the **New Group Wizard**.

The Wizard has built-in **QuickHelp** that appears at the bottom of each Wizard Page when focus is set to each control. To get QuickHelp on the New Group Wizard, Click or use the tab key to move to the desired control and the help text will appear at the bottom of the dialog.

	<ul style="list-style-type: none">• All GroupDrive Server users must belong to a group. If you are using a user authentication method other than native GroupDrive Server user authentication, we recommend that you read the User Authentication Overview topic.• For more information about configuring user authentication, see the GroupDrive Quick Start Guide for your specific user authentication method.
---	--

Deleting Groups

User groups can be deleted directly within the [Administration program](#). When you delete a group from the system, all users who are members of that group are removed from the group and their Directory Access Permissions are updated.

Right-click the desired group in left pane (tree pane) of the Administration program and select **Delete Group** from the menu. You will be prompted to confirm the deletion of the group.

or

Click the desired group in the left pane of the Administration program. From the main menu, select **Server>Groups>Delete Group**. You will be prompted to confirm the deletion of the group.

or

Click the **Groups** icon in the left pane (tree pane) of the Administration program. This will cause a list of groups to be generated and displayed in the right pane (tab pane). Select the desired group in the list of available groups and click the **Delete** button in the tab pane. You will be prompted to confirm the deletion of the group.

Adding Users to Groups

All GroupDrive Server users must belong to a group. Users can be added to an unlimited number of groups.

To add users as members of a group using the GroupDrive [Administrator](#), expand the **Server**, select the **Group**, and then click the **Group General** tab.

Make the appropriate changes to Group Membership and then click **Apply** to save the changes.

Note: If a user is a member of multiple groups, the user will inherit the sum or culmination of the Directory Access [Permissions](#) for the various groups. For example, if **User A** is a member of **Group 1** and **Group 2**, and **Group 1** has **Read** permissions to **folder /F/**, and **Group 2** has **Write** permissions to **folder /F/**, then **User A** will have **Read AND Write** permissions to **folder /F/**.



- **All GroupDrive Server users must belong to a group.** We recommend that you read the [Groups Overview](#) before you add groups to GroupDrive Server.
- See [File System Permissions](#) for more information about **inheritance** and **group permissions**.

Removing Users from Groups

Users can be removed from all groups except for the **Everyone** Group. Removing a user from a specific group also deletes any Directory Access [Permissions](#) that they may have had by being a member of the group.

To delete a user from a group using the GroupDrive Server [Administrator](#), in the tree pane, expand the **Server** and select the **Group**. In the tab pane, click the **Group General** tab.

Make the appropriate changes to the membership of the group and then click **Apply** to save the changes.

Group Settings

General Group Settings Tab

The **Group General** tab is used to manage the membership of users to the group.

To access the **Group General** tab, in the tree pane expand the **Server**, expand **Groups**, and then select the **Group**. In the tab pane, select the **Group General** tab.

Members List - Lists the member of the currently selected group. By being a member of a group, users adopt all of the [permissions](#), [rights](#), and restrictions assigned to the group.

Non-Members List - Lists users who are not currently members of the selected group.

User Configuration

User Configuration Overview

GroupDrive Server currently supports the following methods of [User Authentication](#):

- **Native GroupDrive Server User Authentication**
- **Windows NT/SAM User Authentication**
- **Windows Active Directory User Authentication**
- **Standard LDAP User Authentication**
- **ODBC Data Source User Authentication**



- **All users must be a member of a group.** Before you add users to GroupDrive Server, we recommend that you read the [Groups Overview](#) topic.
- Once you select a **User Authentication Database** option in GroupDrive, you cannot change to a different method once the server wizard has completed.
- For more information about configuring **user authentication**, see the [User Authentication Overview](#) topic or the GroupDrive [Quick Start Guide](#) for your specific user authentication method.

Creating New Users

If your server is configured for native GroupDrive User Authentication, new user accounts can be created directly within the GroupDrive [Administration](#) program.

To create a new user using the Administration program:

In the tree pane, expand the **Server**, right-click the **Users** icon and select **New User**. The New User Wizard will launch.

Or

Select the **Server** and then from the main menu, select **Server>Users>New User**. The **New User Wizard** will launch.

Or

Click the **Users** icon in the left pane (tree pane) of the Administration program. This will cause a list of users to be generated and displayed in the right pane (tab pane). Click the **New User** button in the tab pane to launch the **New User Wizard**.

The Wizard has built-in **QuickHelp** that appears at the bottom of each Wizard Page when focus is set to each control. To get QuickHelp on the wizard, click or use the tab key to move to the desired control and the help text will appear at the bottom of the dialog.



- **All users must be a member of a group.** Before you add users to GroupDrive Server, we recommend that you read the [Groups Overview](#) topic.
- For information about configuring **user authentication**, read the [User Authentication Overview](#) topic or see the GroupDrive [Quick Start Guide](#) for your specific user authentication method.

Deleting Users

If your server is configured for standard GroupDrive [Authentication](#), then users can be deleted directly within the [Administration](#) program.

To delete an existing user using the Administration program:

Right-click the user in left pane (tree pane) of the Administration program and select **Delete User** from the context menu. You will be prompted to confirm the deletion of the user.

or

Click the user in the left pane of the Administration program. From the main menu, select **Server>Users>Delete User**. You will be prompted to confirm the deletion of the user.

or

Click the **Users** icon in the left pane (tree pane) of the Administration program. This will cause a list of users to be generated and displayed in the right pane (tab pane). In the tab pane, Select the user from the list of available users and click **Delete**. You will be prompted to confirm the deletion of the user.



Deleting a user is permanent.

User Settings

General User Settings Tab

Use the **User General** tab to manage basic configuration options for the user.

To access the **User General** tab, expand the **Server** in the tree pane, expand **Users**, and then select the **User**. In the tab pane, select the **User General** tab.

Account Enabled - When selected, the user account is enabled and available for use. If you clear this check box, the account is disabled and the user will not be permitted to log in to the server.

Username - The user's unique name used to log on to the system. Usernames are unique per server.

Password - The user's password used to log in to the system. The user's password is not displayed in the GroupDrive Server Administrator for security reasons. **Note:** Passwords are case sensitive and must be at least four characters in length.

Force Complex Password Rules - When enabled, the user's password must meet the following complexity requirements:

- Password must be at least eight characters long.
- Must contain one or more Latin uppercase letters (A through Z).
- Must contain one or more Latin lowercase letters (a through z).
- Must contain one or more digits (zero through nine).
- Must contain one or more non-alpha characters ('!', '#', '\$', '^', '&', '(', ')', '-', '+', '=').

NOTE: When the **Force Complex Password Rules** feature is not enabled, there are no password requirements other than the requirement that the password be at least four characters in length.

Confirm Password - Type the user's password a second time to verify that it is correct. **Note:** Passwords are case sensitive.

User's Full Name - Contains the user's full name. Used for informational purposes only.

Home Directory - Displays the root/home directory for the user. The user's home directory is relative to the Server Data Directory specified in the General Server Settings tab. For example, if the user's Home Directory is `\User\test1\` and the Server Data Directory is `c:\data\`, then the user's actual home directory will be `c:\data\User\test1\`.

Email Address: Type the user's e-mail address.

Account Expires On - Enable this feature to specify a date on which the user account will expire. Once this date is reached, the account becomes disabled and the user will no longer be permitted to log in to the system.

User Group Membership Tab

Use the **Groups** tab to manage the groups to which this user belongs.

To access the **Groups** tab, in the tree pane expand the **Server**, expand **Users**, and select the **User**. In the tab pane, select the **Groups** tab.

Member Of - Contains a list of all groups to which this user is a member. By being a member of a group, the user adopts all of the [permissions](#) and [rights](#) and restrictions assigned to that group.

Not a Member Of - Contains a list of the groups that the user is NOT a member of.



- **All users must be a member of a group.** Before you add users to GroupDrive Server, we recommend that you read the [Groups Overview](#) topic.

User IP Access Restrictions Tab

Use the **IP Access** tab to configure IP access restrictions for this user. To access the **IP Access** tab, in the tree pane expand the **Server**, expand **User**, and then select the **User**. In the tab pane, select the **IP Access** tab.

Note: many of these configuration options are also available at the Server level. **User level configuration options override** the same options at the **Server level**. When check box values are **Grayed out**, this indicates that the **Server level** setting will be used instead of the User Level Setting. If a check box option is selected, this means that the option is enabled at the **User level**. If a check box is cleared, that indicates that this option is disabled at the **User level** and this value overrides any value that has been set at the Server level. **Unchecked = disabled, Checked = enabled, Grayed = Use SERVER setting.**

Enable IP Access Restrictions - When enabled, IP Access restrictions will be applied to this user whenever they attempt to log in to the system.

Grant/Deny access by default - Select the default action that will be applied to this user when they access the server.

Except those addresses listed below - Type a list of IP addresses that will be the exception to the default rule. For example, you can **Deny Access by default** and then enter a single IP address. This will be the only IP address that the user will be permitted to connect from.

User Connection Settings Tab

Use the user **Connections** tab to configure various connection settings for this user. To access the user **Connections** tab, in the tree pane expand the **Server**, expand **Users**, and then select the **User**. In the tab pane, select the **Connections** tab.

Note: Many user configuration options are also available at the **Server level**. **User level** configuration options **override** the same options at the Server level. When check box values are **Grayed** out, this indicates that the **Server level setting** will be used instead of the User Level Setting. If a check box option is selected, this means that the option is enabled at the **User level**. if a check box is cleared, this indicates that this option is disabled at the **User level** this value overrides any value that has been set at the Server level. **Unchecked = disabled, Checked = enabled, Grayed = Use SERVER setting.**

Disabled account after X bad password attempts - When enabled, the user account will be disabled after X number of consecutive invalid password attempts.

SSL Tab

Use the user **SSL** tab to manage SSL settings for this user.

To access the **SSL** tab, in the tree pane expand the **Server**, expand **Users**, and select the **User**. In the tab pane, select the **SSL** tab.

User Certificate Settings

Trust the following certificate for this user - Displays the current public key certificate in use by this user.

Certificate Manager - Launches the Certificate Manager to create or import certificates for this user. User certificates can be imported into the certificate store so that the server can validate client side certificates.

Certificate Store Folder - Displays the location of the user's certificate.



- See the [SSL Support](#) topic for more information about using SSL with GroupDrive Server.
- For more information about configuring SSL & public key certificate-based authentication, see the [GroupDrive SSL & Public Key Certificate-based Authentication Quick Start Guide](#).

File System Settings

File System Overview

Each GroupDrive Server stores its files under the Data Directory that is specified for each server, for example **c:\srtData\My Server**. Typically each user is assigned his own directory under this root directory where the user's files are stored, for example, **c:\srtData\My Server\Users\john**. When a client connects to the server with a specific username and password, the root directory would be the files under **c:\srtData\My Server\Users\john**. A user does not have access to files outside of his root directory unless another user specifically grants [shared access](#) to one of his file objects.

Shared Files and Folders

The GroupDrive Server has the capability to allow users to share folders or files with other users who are outside of the user's directory space. To share a file object with another user, the file object must be configured to allow [sharing](#). To enable sharing for a file object within the GroupDrive client, right-click a file and select **Properties**. From the property page, select the **Share** tab and enable sharing for the file or folder. In addition to enabling sharing, you must define an [access control list](#) for the share to determine which users or groups have access to the file object.

Linking to Shared Files and Folders

In order to access a shared file object, a [link to](#) the shared object is defined by the user. The name of the link is chosen by the user and can be placed anywhere in the user's name space.

Here is a typical example of how a user would share a folder with another user:

1. User **John** has a folder in his name space called **Vacation Pics** and it is located under the relative root **\Personal\Vacation Pics**. John wants to share this folder with user **Nicole**, so he enables sharing for the folder **\Personal\Vacation Pics** and sets the [permissions](#) to allow user **Nicole** access to this folder.

2. User **Nicole** wants to see the files under the shared folder defined by **John**. To do this, user **Nicole** creates a link to the shared folder in a directory of her choosing. Using the GroupDrive client, user **Nicole** navigates to the directory that she wants to place the link into and then right-clicks in Explorer and selects **Create Link**. A dialog box is presented to user **Nicole**, listing all the shared objects that she has access to. She selects the desired object and creates a link to it. For example, she could create a link to the shared **Vacation Pics** folder under her directory of **\Misc\Photos\Johns Vacation**. The folder **Johns Vacation** is a virtual folder which is simply a link to the actual folder **\Users\John\Personal\Vacation Pics**.

Virtual Folders

Virtual folders are used to give access to directory structures that are not rooted under the Data Directory for the server. This is useful for giving access to folders on another disk drive, CD-ROM, or even a network drive. Virtual folders can only be configured using the GroupDrive Server [Administrator](#) program. Using the Administrator program, you can define a [virtual folder](#) and specify the access [permissions](#) for it. Users can access the virtual folder by linking to it, the same way that they normally [link to](#) a shared file object, and they would be unaware that it is a virtual folder or what path it actually points to.

File System Permissions

Access Control List/Access Control Entry/Permissions

GroupDrive **Access control** is the process of granting users and groups access privileges to folder and file objects. Key concepts that make up access control are permissions, ownership of files, inheritance of permissions, [user rights](#), and [sharing](#) and [linking to](#) files or folders.

In GroupDrive Server you set **Permissions**, using an **access control entry**, to specify the user's level of access to files. For example, you can set permissions on a file to let one user read the contents of a file, let another user make changes to the file, and prevent all other users from accessing the file. **NOTE:** It is a good practice to assign permissions to groups because it improves system performance when verifying the user's access to files.

Every folder object and every file object in the GroupDrive file system has an **access control list** (ACL) associated with it that defines which users or groups have access to these objects. An access control list is comprised of one or more **access control entries** (ACE) that define the access permissions for a specific user or group.

You can allow users to **inherit** access control lists (permissions) by creating parent/child relationships. Inheritance makes it easy to assign and manage permissions because this feature automatically causes child objects to inherit all inheritable permissions from its parent object. For example, when you use **Inherit**, once you set the permissions for a folder, any new files created within that folder automatically inherit the permissions that are set for that folder. Each file object in the system can have its own individual access control list associated with it or it can inherit the access permissions of its parent, but only permissions marked to be inherited will be inherited. Using inherited permissions is not only easier to manage but it is also the most efficient method.

Typically, an access control list is defined at the root directory of a user's file space and then all objects under this directory simply inherit the permissions of the root directory. GroupDrive client users have the ability to define the permissions for any file object under their directory tree to allow other users access to a specific directory or file. Users can assign permissions to their own file objects using either the Web interface or the Desktop Client. The Administrator application also has the ability to set permissions for any file object.

GroupDrive Server Administrator—Set or Change Permissions

You can use the GroupDrive Server Administrator to set or change the permissions on a folder or file object. To access the **Permissions** tab, expand the **Server** in the tree pane, expand **Users**, and then select the **User**. Select the **folder** or **file** on which you would like to set permissions. In the tab pane, select the **User**.

Add - Add an access control entry (ACE) to the access control list for this file object. After selecting **Add** a dialog box is displayed that allows you to select a list of users or groups to add to this access control list.

Remove - Removes the selected access control entry from the access control list.

Inherit permissions from parent - When enabled, the access control list for this file object also contains the permissions from the parent directory in addition to the specific permissions defined for this access control list.

Replace permission on all child objects with entries shown here - When selected, and you click **Apply**, then any specific access control lists that are defined under this directory will be replaced with this list of permissions.

File/Folder Permissions

- **Read/Download Files** - Allow read access to the file object.
- **Write/Upload New Files** - Allow write access to the file object.
- **Append/Replace Files** - Allow modify access to the file object.
- **Delete Files** - Allow delete access to the file object.
- **Rename Files** - Allow rename access to the file object.
- **Create Subdirectories** - Allow create directory access.
- **Remove Subdirectories** - Allow remove directory access.
- **Can View Directory Listing** - Allow browsing of folders.
- **Apply Rights to Subdirectories** - Allow permissions to be inherited.
- **Read Permissions** - Allow for reading of access permissions.
- **Write Permissions** - Allow for writing of access permissions.



GroupDrive Server user **rights** are not the same as GroupDrive file system permissions. User rights are authorized by the System Administrator and generally refer to **system actions**, such as the ability of a user to **share** or **download** file and folder objects. Permissions pertain to the **level of access** granted to a specific shared resource, such as the level of access a user has to a file or folder object. Permissions can be set by the System Administrator or the owner of the file or folder object. See the GroupDrive **Rights tab** topic for more information.

Sharing

To share a file or folder object with another user, the object must be configured to allow sharing. You can configure file or folder objects for sharing by using the GroupDrive Server Administrator **Sharing** tab, or by using the GroupDrive Web interface or Desktop client.

Sharing Files and Folders using the GroupDrive Server Administrator

The GroupDrive Server Administrator has the capability to allow users to share folders or files with other users. To access the **Sharing tab**, in the tree pane expand **Server>Users>User's Data Directory** and then select the **Folder or File**. In the tab pane, select the **Sharing** tab. **NOTE:** In addition to enabling sharing, you must define an [access control list](#) for the share to determine which users or groups have access to the file object. Use the Permissions tab to define the access control list.


The GroupDrive Server Administrator **Sharing** tab is used to enable/disable the sharing of a file object.

Do not share this object - Sharing is disabled.

Share this object - Sharing is enabled for the selected file object.

Share Owner - Name of the person who created the file object. Use the drop-down arrow to change the file owner.

Comment - A comment/description for the shared file object.

	<ul style="list-style-type: none">• In general, GroupDrive Server User Rights are different from file system permissions because user rights usually apply to user accounts, and permissions are usually attached to files and folders, although there is some overlap. See the GroupDrive Rights tab topic for more information.• For information about linking using the Desktop client or Web interface, see the GroupDrive Desktop Client User's Guide or the GroupDrive Web Interface User's Guide.
---	---

Linking to Shared Files and Folders

In order for a user to access a [shared](#) file object, that user must define a link to the shared object. The user who wants to access the shared object will create the link in the user's own directory space. The link is named by that user and can be placed anywhere in the user's name space.

Here is a typical example of how a user would share a folder with another user:

1. User **John** has a folder in his name space called **Vacation Pics** and it is located under the relative root **\Personal\Vacation Pics**. John wants to share this folder with user **Nicole**, so he enables [sharing](#) for the folder **\Personal\Vacation Pics** and sets the permissions to allow user **Nicole** access to this folder.
2. User **Nicole** wants to see the files under the shared folder defined by **John**. To do this, user **Nicole** creates a **link** to the shared folder in a directory of her choosing. Using the GroupDrive client, user **Nicole** navigates to the directory that she wants to place the link into, and then right-clicks in Explorer and selects **Create Link**. A dialog box is presented to user **Nicole** for all the shared objects that she has access to. Nicole selects the desired object and creates a link to it. For example, she could create a link to the shared **Vacation Pics** folder under her directory of **\Misc\Photos\Johns Vacation**. The folder **Johns Vacation** is a virtual folder which is simply a link to the actual folder **\Users\John\Personal\Vacation Pics**.

In the GroupDrive Server Administrator, the **Link To** tab can be used to define a link to a shared file object. To access the **Link To** tab, in the tree pane expand **Server>Users>User>User's Data Directory** and then select the **folder or file** object. In the tab pane, select the **Link to** tab.

The link is placed in the currently selected folder in the tree pane. You can link to files or folders. Select the [Shared object](#) to link to, define a **Name** for the link, and click **Add**.

Link Name - The name for the link. This name will be used for the directory name if linking to a shared folder, or the file name if linking to shared file.



- In addition to enabling [sharing](#), you must define an [access control list](#) for the share to determine which users or groups have access to the file object. Use the Permissions tab to define the access control list.
- For information about **linking** using the Desktop client or Web interface, see the [GroupDrive Desktop Client User's Guide](#) or the [GroupDrive Web Interface User's Guide](#).

User Directory Quota

The **Directory Quota** tab is used to configure quotas on a specific directory.

To access the **Quota** tab, in the tree pane select the **Server>Users>User>User Directory**. In the tab pane, select the **Quota** tab.

Enable Quotas for this Directory - Enables quota checks on this directory and all directories under it. When a limit is set for a directory then the users will not be allowed to upload any new files into this directory once the quota limit has been reached.

Current Quota Usage - The total number of bytes in use under this directory.

Quota Limit - The quota limit for this directory and all directories underneath it.

Virtual Folders

Virtual Folders Overview

Virtual folders are folders that can be mapped into a server's data directory and are used to link or map external folders into a user's directory space. This is useful for giving access to files on another disk drive, CD-ROM, or even a network drive. In a Virtual folder it appears as if the data resides within the folder structure; however, the data is actually stored somewhere else. If you are a Windows user, you can think of a Virtual Folder as a Windows Shortcut. The link appears in one location and the data lives in another location. For UNIX users, Virtual Folders are very similar to Symbolic Links.

Virtual folders can only be configured using the GroupDrive Server Administrator program. Using the Administrator program, you can define a Virtual folder and specify the access permissions for it. Virtual folders can be added at the Server, Group, or User level. Users can access the virtual folder by linking to it, in the same way that they normally link to a shared file object, and they would be unaware that it is a virtual folder or what path it actually points to.

Group level virtual folders allow data to be shared with all users of a given group. In a group level virtual folder, all users can share the same data and have Directory Access Rights to that data. Virtual folders added at the group level can be made accessible to all users in the group, depending on the Directory Access Permissions that are set for that group. Virtual folders added at the User Level are limited to that specific user.

When you add a Virtual folder to a GroupDrive Server configuration, the default Directory Access Permissions will be set to Read Only. Read Only permissions means that users are allowed to browse the folder, and download information, but cannot modify the contents or upload files. You can modify the standard Directory Access Permissions after the virtual folder has been added to the configuration.

One of the benefits of virtual folders is that you can access network shares from the GroupDrive Server through the use of virtual folders. GroupDrive Server supports the ability to add a UNC (Universal Naming Convention) path into the name space. For example, if you have a share on your network called `\\MyServer\My Music\` you can use virtual folder support to map that into your Server Data Directory as `/pub/My Music/` or `/usr/joe/My Music/`

If you attempt to create a virtual folder for a mapped network drive, GroupDrive will replace the drive mapping with the actual UNC name. This is because the GroupDrive Service does not have access to mapped drives, only to UNC shares. Under Windows, GroupDrive Server runs as an NT Service that, by default, does not have access to shared network resources because shared network resources are based on the authorized NT user. If you are mapping a UNC share, you must make sure that the account under which the GroupDrive Service is running has access to the UNC. Otherwise, you must enter the appropriate username and password under the UNC Accounts tab.

Virtual Folders Tab

The **Virtual Folders** tab is used to define Virtual folders that can be [linked to](#) by each user. The Virtual File can be either a directory or a file that is on a hard disk, CD-ROM, or Network share.

To access the **Virtual Folders** tab, expand the **Server** in the tree pane and click **Virtual Folders**. In the tab pane, select the **Virtual Folders** tab. To add a virtual folder, click **Add**.

Add - Click **Add** to add a virtual folder. The **New Folder Wizard** will launch. A dialog is displayed allowing you to choose a **Physical path**, a **Name**, and **Permissions** for the folder.

Remove - Click **Remove** to remove the selected Virtual File.



Use the Virtual Folders **Permissions** tab to change Permissions on the virtual folder.

Push Content

Push Content Virtual Folders tab

You can use the **Push Content Virtual Folders** tab to place a virtual folder in a user's directory space. When you use the Push Content feature, the server will "push" the virtual folder into the user's directory space without the user having to link to it.

To access the **Push Content Virtual Folders** tab, in the tree pane expand the **Server** and then select **Push Content**. In the tab pane, select the **Virtual Folders** tab.

Add - Click **Add** to add a virtual folder. The New Folder Wizard will launch. A dialog is displayed allowing you to choose a Physical path, a Name, and [Permissions](#) for the folder.

Remove - Click **Remove** to remove the selected Virtual File.

Use the **Push Content Permissions** tab to change [Permissions](#) on the virtual folder.

Push Content Permissions Tab

The **Push Content Permissions** tab can be used to set or change the permissions on push content.

To access the **Push Content Permissions** tab, expand the **Server** in the tree pane, expand **Push Content**, and then select the **Folder**. In the tab pane, select the **Permissions** tab.

Add - Add an [access control entry \(ACE\)](#) to the access control list for this folder object. After you select **Add**, a dialog box is displayed that allows you to select a list of users or groups to add to this access control list.

Remove - Removes the selected access control entry from the access control list.

Inherit permissions from parent - When enabled, the access control list for this folder object also contains the permissions from the parent directory in addition to the specific permissions defined for this access control list.

Replace permission on all child objects with entries shown here - When selected, and you click **Apply**, any specific access control lists defined under this directory will be replaced with this list of permissions.

File/Folder Permissions

- **Read/Download Files** - Allow read access to the file object.
- **Write/Upload New Files** - Allow write access to the file object.
- **Append/Replace Files** - Allow modify access to the file object.
- **Delete Files** - Allow delete access to the file object.
- **Rename Files** - Allow rename access to the file object.
- **Create Subdirectories** - Allow create directory access.
- **Remove Subdirectories** - Allow remove directory access.
- **Can View Directory Listing** - Allow browsing of folders.
- **Apply Rights to Subdirectories** - Allow permissions to be inherited.
- **Read Permissions** - Allow for reading of access permissions.
- **Write Permissions** - Allow for writing of access permissions.

Advanced Topics

User Authentication Overview

GroupDrive Server currently supports the following methods of User Authentication:

Native GroupDrive Server User Authentication - When you use GroupDrive Authentication, the server administrator will create, manage, and delete user accounts from within the GroupDrive Administration program. User accounts created in the GroupDrive Administration program can access only the GroupDrive server for which they are defined. These user accounts will not permit users to access other areas of your network.

Windows NT/SAM User Authentication - When using Windows NT/SAM (Security Accounts Manager) Authentication, the server administrator will create and delete user accounts using the Windows NT User Manager. The GroupDrive Server administration program can then be configured to include one or more NT Groups from the Windows SAM database. All NT User Accounts from the selected NT Group or Groups will then appear in the valid user list for GroupDrive. GroupDrive will need to know the name of the Domain and/or Computer that contains the User Accounts database. Usually this will be the domain name and computer name of your domain controller. This has the benefit of providing your NT users with a single username/password that they can use to access both the NT domain and the GroupDrive server. **NOTE:** If you use NT authentication, and GroupDrive is running on Windows NT/2K/XP, you must modify the user account that GroupDrive uses in the Service Manager. By default, GroupDrive will use the LocalSystem account when it runs, but the LocalSystem account does not usually have access to query the NT User Accounts database. Therefore, you should [create an account](#) on your NT Domain Controller that has the proper permissions, and then update the GroupDrive Service properties so that GroupDrive uses this new account when it runs.

Windows Active Directory User Authentication – GroupDrive can be configured to work in conjunction with an existing Active Directory network. In this mode, GroupDrive will be configured to allow members of one or more Active Directory Security Groups or OrgUnits access to the GroupDrive Server. All management/maintenance of the Active Directory Users, Groups, and Organizational Units will still be performed by the Active Directory Administrator, GroupDrive will simply access the existing data from the Active Directory. **NOTE:** GroupDrive must be configured with the proper search strings in order to locate user and group information in the Active Directory (AD). For most AD installations, the default values can be used and will return the proper user and group information from your AD. However, there are some instances where these values may need to be enhanced to allow GroupDrive to find the user information in the AD.

Standard LDAP User Authentication - GroupDrive can be configured to work in conjunction with an existing LDAP based network. In this mode, GroupDrive will be configured to allow members of one or more Directory Groups or Organizational Units access to the GroupDrive Server. All management/maintenance of the Directory Users, Groups, and Organizational Units will still be performed by the LDAP Administrator, GroupDrive will simply access the existing data from the LDAP Directory. **NOTE:** GroupDrive must be configured with the proper search strings in order to locate user and group information in LDAP. For most LDAP installations, the default values can be used and will return the proper user and group information from your Active Directory (AD). However, there are some instances where these values may need to be enhanced to allow GroupDrive to find the user information in LDAP.

ODBC Data Source User Authentication – GroupDrive Server can be configured to use any industry standard ODBC (Open Database Connectivity) compliant database to store and manage users and groups. When configured for ODBC based user authentication, GroupDrive will create and maintain database tables containing a list of valid users and groups. System administrators can use the GroupDrive administration program to manage users, groups, and membership. Changes to the users and groups list will be written out to the ODBC database. The ODBC data source configuration options vary based on your specific ODBC database. A configuration of a MS Access data source and a SQL Server data source is included with GroupDrive Server. If you are using a database other than MS Access or SQL Server, see your database's ODBC help system for instructions on configuring an ODBC data source for that database. See the [GroupDrive Collaboration Server Open Database Connectivity \(ODBC\) User Authentication Quick Start Guide](#) for configuration information and a [schema example](#).



- All users must be a member of a group. Before you add users to GroupDrive Server, we recommend that you read the [Groups Overview](#) topic.
- Once you select a User Authentication Database option in GroupDrive, you cannot change to a different method after the server wizard has completed.
- For more information about user authentication, see the GroupDrive [Quick Start Guide](#) for your specific user authentication method.

SSL Support

GroupDrive Collaboration Server provides support for the industry standard Secure Sockets Layer (SSL). You can use the GroupDrive Desktop client with SSL to encrypt communications as well as other WebDAV clients such as Microsoft's WebFolders.

To configure **HTTPS/SSL** options in a new server, use the **New Server Wizard**. To manage **HTTPS/SSL** options in an existing server use the **Server HTTPS/SSL** tab.

Public Key Authentication Best Practices

Each entity in a secure environment, both the client and the server, should generate its own key pair. This key pair will have a public key and a corresponding private key. Never share or send your private key to anyone as this will compromise the integrity of your key pair. It is always a good practice to password protect your private key, and GroupDrive requires this. Each GroupDrive client's public certificate must be provided to the GroupDrive server administrator to be installed on the GroupDrive Server. While it is possible to use the Certificate Management features in GroupDrive to export your private key, it is highly discouraged unless it is for backup purposes because it is difficult to ensure the integrity of the private key during the physical transfer of the key file. If it is necessary to export the private key, we recommend that the transfer be performed over a secure medium. Export the keys to an encrypted USB drive, or encrypt the files onto a DVD/CDROM. However, never e-mail the private key. E-mail is natively insecure and there is no way to ensure the integrity of the files during electronic transfer.



For more information about configuring SSL & public key certificate-based authentication, see the GroupDrive SSL & Public Key Certificate-based Authentication [Quick Start Guide](#).

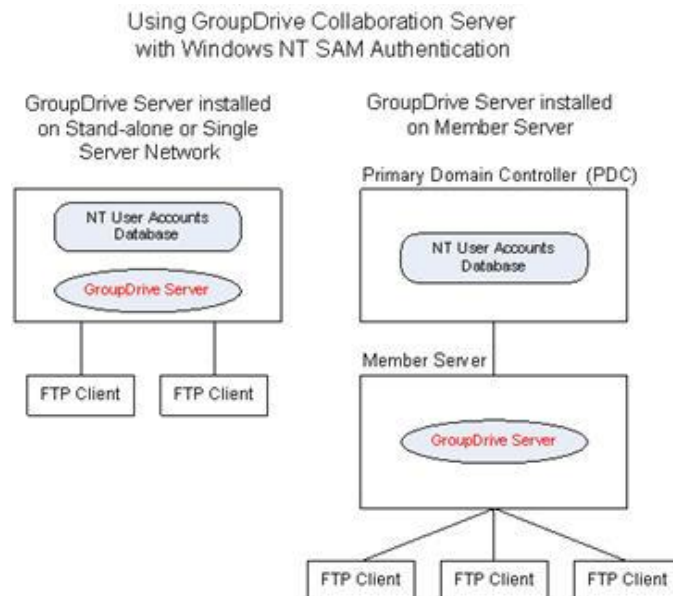
Creating a Special NT Account

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 but 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 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 data.

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.



See the following examples to configure GroupDrive Collaboration Server to use a special NT User Account that has the proper rights necessary to query the PDC (Primary Domain Controller) User Accounts Database during the authentication of a GroupDrive client session.

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 into 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. From **Control Panel > Administrative Tools**, open **Services**. Scroll down to the **GroupDrive Daemon**. Right-click the **daemon** 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 into 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. From **Control Panel > Administrative Tools**, open **Services**. Scroll down to the **GroupDrive Daemon**. Right-click the **daemon** 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.

Database Schema Column Descriptions

Table: sr_uagroups

Name	Type	Size
groupid	Long Integer	4
gname	Text	132
gdesc	Text	132

Table: sr_uusers

Name	Type	Size
userid	Long Integer	4
uname	Text	132
upass	Text	132
ufullname	Text	132
uhomedir	Text/Memo	1024
uenabled	Long Integer	4

Table: sr_uamembers

Name	Type	Size
groupid	Long Integer	4
userid	Long Integer	4

Table: sr_uagroups

This table stores the group lists that GroupDrive accesses by way of the GroupDrive [Administration](#) utility.

groupid – This is a 4-byte numeric value that uniquely identifies each group in the system. Group ID’s must be numbers only, must be unique, and must be within the range of 100-999.

gname – This is a text field that stores a human readable name associated with the group. This field must contain alpha-numeric printable/readable ASCII characters only. The maximum length of a group name in GroupDrive Collaboration Server is 131 characters.

gdesc – This is a text field that stores a human readable description associated with a group. This field must contain alpha-numeric printable/readable ASCII characters only. The maximum length of a group description in GroupDrive Collaboration Server is 131 characters.

Table: sr_uusers

This table stores the list of users who can be granted access to the GroupDrive server. Since GroupDrive is a "group" based server, only users who are members of a group included in GroupDrive Collaboration Server will be permitted to access the server.

userid – This is a 4-byte numeric value that uniquely identifies each user in the system. User ID's must be numbers only, must be unique, and must be within the range of 1000-2,000,000.

uname – This is a text field that stores the user name for a user. This field must contain alpha-numeric printable/readable ASCII characters only. No spaces are permitted in a user name. User names are not case sensitive; however, using only lowercase characters in a user name is recommended. The maximum length of a user name in GroupDrive is 131 characters.

upass – This text field contains either the user's password, or a hash of the user's password depending on the type of password masking that has been chosen in the GroupDrive Administrator during the setup process. GroupDrive currently supports Plaintext, MD5, SHA-1, RIPE-MD-160, and SHA-256 hashing algorithms for passwords.

ufullname – This text field contains the user's full name. This field must contain alpha-numeric printable/readable ASCII characters only. This field allows a maximum length of 131 characters.

uhomedir – This text field contains the fully qualified path for the user's home directory. This can be a local path or a UNC (Universal Naming Convention) that points to a remote data location. **Note:** do not use a mapped drive letter. GroupDrive runs as a system service so it does not have access to mapped drives that are "user" based. Use a [UNC](#) instead.

uenabled – This Boolean field tells GroupDrive if the user account is enabled or disabled. If this value is 1, then the user will be permitted to log on to the GroupDrive server. If this value is 0, the user will not be permitted to log on to the GroupDrive server even if they specify a valid password.

Table: sr_uamembers

This table stores a mapping of Users to Groups. Since GroupDrive Collaboration Server is a Group based server, users must belong to a group that has been included in the GroupDrive Administrator.

groupid – This field contains the unique Group ID for the group that will be allowed to access the GroupDrive server.

userid – This field contains the unique User ID for the user that will be a member of the group accessing GroupDrive.



For information about configuring ODBC user authentication, see the [GroupDrive Server ODBC User Authentication Quick Start Guide](#).

Advanced Features

Cache User & Group Information

To access the Group Cache Life and the User Cache Life settings for an existing server, select the Server in the tree pane. In the tab pane, select the **User Authentication** tab, and then click **Authentication Server Setup**. If you are creating a new server, use the [New Server Wizard](#).

Group Cache Life and User Cache Life settings are available to the following user authentication methods:

Windows NT/SAM User Authentication

Windows Active Directory User Authentication

Standard LDAP User Authentication

ODBC Data Source User Authentication

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.

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 reloads that information.

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 ODBC 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.



For more information about configuring group and user cache life values and user authentication, see the GroupDrive [Quick Start Guide](#) for your specific user authentication method.

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.

UNC 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

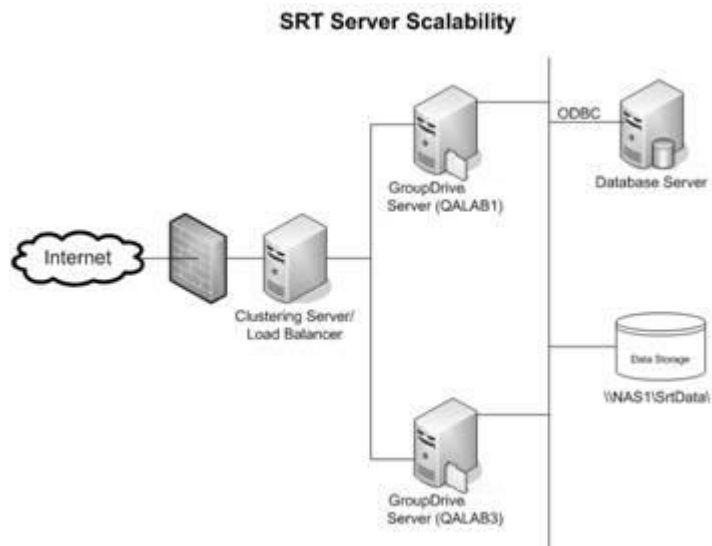
The main benefit to using UNC's to refer to data storage locations is scalability. GroupDrive Collaboration Server supports the ability to be deployed in a scalable environment, meaning that one or more servers can run in parallel and can access the same back end data storage to service the same front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

If you intend to scale your GroupDrive Collaboration Server to multiple boxes, you must 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. Right-click 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**.

NOTE: 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.

So that GroupDrive can access the data:

You can 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. (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.

Or

You can **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. 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. If you use the UNC Accounts tab, 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.

NOTE: 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.

UNC Accounts Tab

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.

Since GroupDrive Service usually runs under the context of a Local System NT Account that is defined for the local computer, 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.

Instead of using the UNC Accounts tab, you could alternately [create special NT account](#) for GroupDrive Collaboration server.

Update 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.

If you are reconfiguring an existing server, you must **update the user data directory**.

If you are reconfiguring an existing server, GroupDrive will ask you if you would like to migrate the data. If you did not change the physical location of the user data, **DO NOT** migrate the data; select **NO**.

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.



For more information, see the GroupDrive Collaboration Server [Using UNC Paths for Data Storage & Scalability Quick Start Guide](#).

Desktop Client Access

Desktop Client Access

You can access your GroupDrive from anywhere, anytime, using a Web browser. If you would like to integrate your GroupDrive directly into the desktop of your operating system, GroupDrive supports various desktop clients, giving you maximum flexibility and usability with your GroupDrive.

GroupDrive Desktop Client For Windows - The GroupDrive Desktop Client integrates directly into your Windows Operating System, allowing you to access your workspace through a mapped drive letter or from within other applications that you are using. The GroupDrive Desktop Client offers some significant advantages over the browser interface. Real-time file collaboration is facilitated by enabling multiple users to edit the same file at the same time without being locked out of a file and without the risk of overwriting each other's changes. In addition, you can create shortcuts on your Windows desktop to different directories within your workspace, giving you quick access to frequently used folders.

The following desktop clients are supported:

Goliath Desktop Client for Macintosh - Goliath is an open-source application that runs on the Apple Macintosh and allows users to access files on a WebDAV enabled server (GroupDrive supports WebDAV). Goliath exposes functionality similar to that of Microsoft WebFolders.

Macintosh OS X Support - Macintosh OS X and later includes native support for accessing files stored on a WebDAV server such as GroupDrive. Using the native WebDAV support, users can upload, download, edit, and even stream movies/music directly from GroupDrive.

Microsoft WebFolders for Windows - WebFolders is Microsoft's interface for WebDAV servers. Accessible from My Network Places, WebFolders allows users to browse WebDAV file systems and servers.



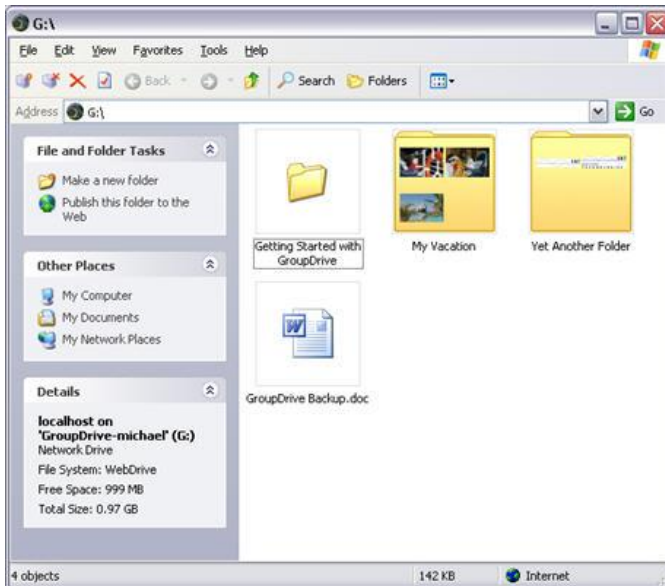
Help desk Support for Goliath, Macintosh OS X, and WebFolders is not provided by South River Technologies. Please contact the respective program vendor for support on these desktop clients.

GroupDrive Desktop Client for Windows

The GroupDrive Desktop Client integrates directly into your Windows operating system, allowing you to access your workspace through a mapped drive letter or from within other applications that you are using. The GroupDrive Desktop Client offers some significant advantages over the browser interface. Real-time file collaboration is facilitated by enabling multiple users to edit the same file at the same time without being locked out of a file and without the risk of overwriting each other's changes. In addition, you can create shortcuts on your Windows desktop to different directories within your workspace, giving you quick access to frequently used folders.

You can download the **GroupDrive Desktop Client for Windows** from the GroupDrive Web user interface Utilities>Desktop Client Download area.

GroupDrive displays your server connection as a mapped drive.



Please review the GroupDrive Desktop Client [Online Help System](#) for details about available features and configuration options.

Built-in MAC OS X Client

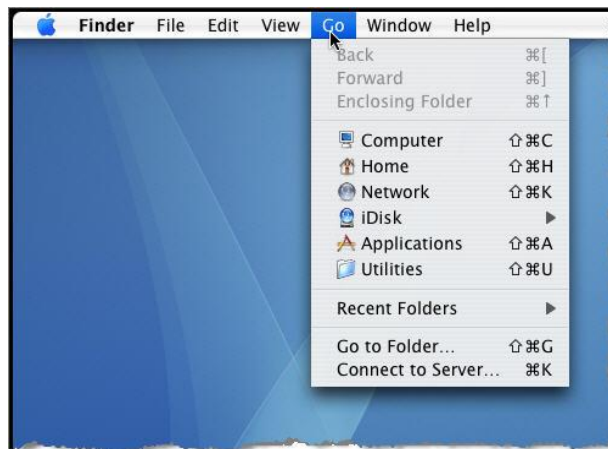
Macintosh OS X and later includes native support for accessing files stored on a WebDAV server such as GroupDrive. Using the native WebDAV support, you can upload, download, edit, and even stream movies/music directly from your GroupDrive.

There is no need to download or install any special software to access your GroupDrive account from a Macintosh with OS X, simply use the **Connect to Server** feature under the **GO** menu.

Configuring Macintosh OS X 10.4 and Later

Use the following procedure if you have OS X version 10.4 or above:

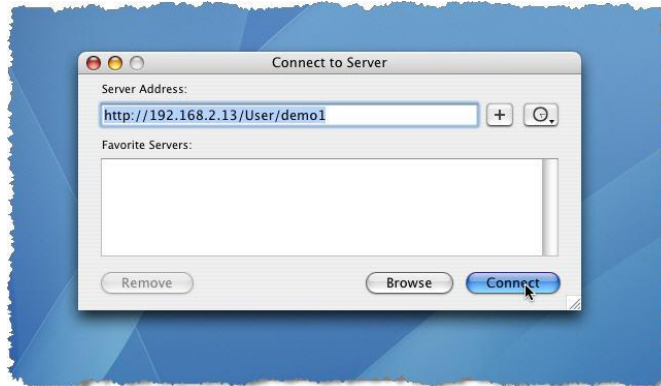
1. From the main **Finder** menu bar, click **GO**.



2. Select **Connect To Server**.



- When prompted, type the **GroupDrive URL** and your **user path**. Our sample server is named **192.168.2.13**, and our sample username is **demo1**, so the full URL is: **http://192.168.2.13/User/demo1/**.



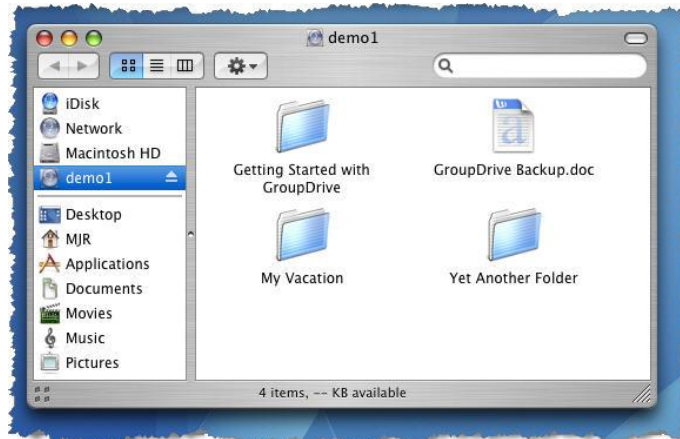
- Click **Connect**.



- When prompted, type your GroupDrive **username** and **password**. We recommend that you also select the option to **Remember this password in my keychain** so that you do not have to re-type your password during your GroupDrive session. Click **OK** to save this information.



6. Your GroupDrive desktop will be displayed.



More information about connecting to WebDAV enabled servers from your Macintosh is available on [Apple's Web site](#).

Goliath Desktop Client For MAC

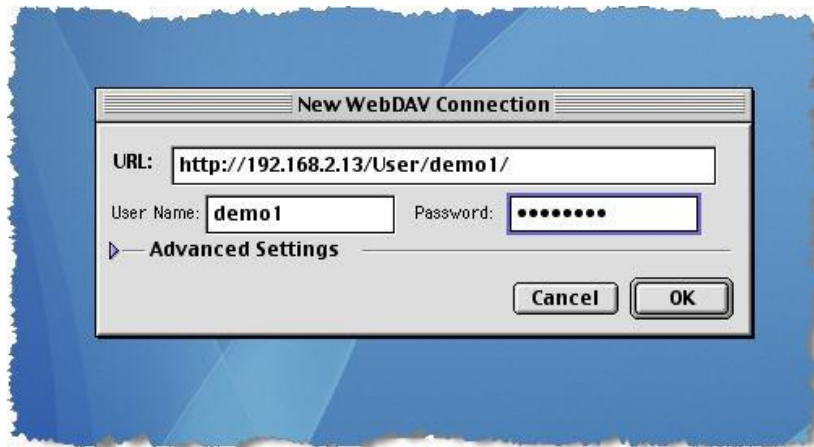
Goliath is an open-source application that runs on the Apple Macintosh and allows users to access files on a WebDAV enabled server (GroupDrive supports WebDAV). Goliath exposes functionality similar to that of Microsoft WebFolders. There are two versions of Goliath, one version for classic Macintosh OS 9 and one version for Macintosh OS/X and later.

You can download the Goliath Desktop Client from the GroupDrive Web user interface **Utilities>Desktop Client Download** area.

Configuring Goliath

Use the following procedure to configure Goliath for access to your GroupDrive:

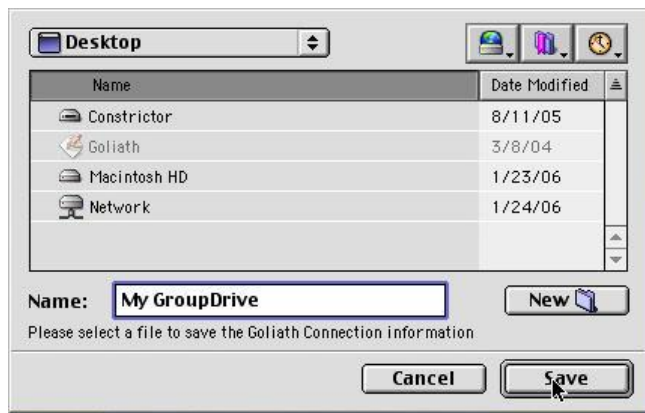
1. Install Goliath on your Macintosh operating system.
2. Launch the Goliath application. The **New WebDAV Connection** dialog will appear.
3. Type the GroupDrive **URL** and your **User Path**. Our sample server is named **192.168.2.13**, and our sample username is **demo1**, so the full URL is: **http://192.168.2.13/User/demo1/**. Type your GroupDrive **Username** and **Password**. Click **OK** to connect to your GroupDrive.



- You can browse your GroupDrive using Goliath. If you need to make changes to your files, drag the file from the Goliath application onto your Macintosh desktop. Edit the file on your local computer and then drag the modified document onto the Goliath window, and the file will be uploaded to your GroupDrive.



- Goliath also has the ability to save the GroupDrive Profile information.



- Save your GroupDrive profile to your Macintosh desktop, making it easy to reconnect to your GroupDrive later.

Microsoft WebFolders

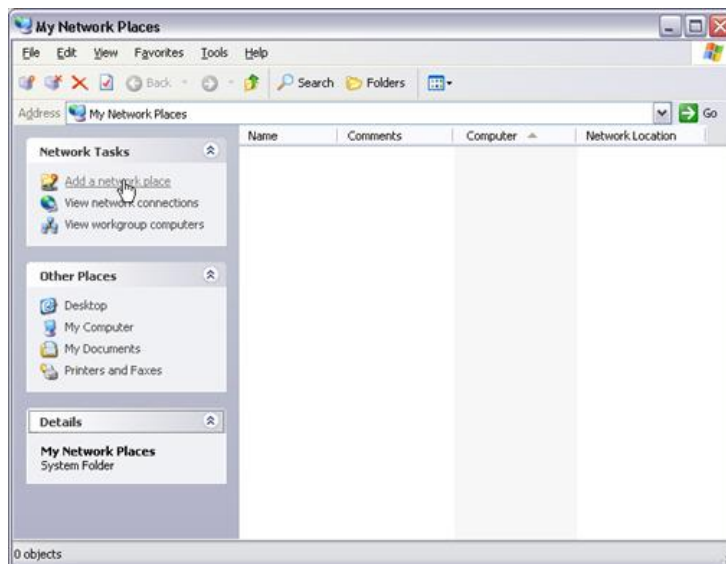
WebFolders is Microsoft's interface for WebDAV servers. Accessible from **My Network Places**, WebFolders allows you to browse WebDAV file systems and servers.

Note: You cannot edit files on your GroupDrive using Microsoft WebFolders. If you want to edit a file, drag the file out of the WebFolder and onto your local desktop where it can then be modified. Once you have modified the file, you can drag the file from your desktop to your WebFolder. We recommend that you use the [GroupDrive Desktop Client for Windows](#) instead of WebFolders.

Configuring WebFolders

Use the following procedure to configure Microsoft WebFolders to access your GroupDrive account.

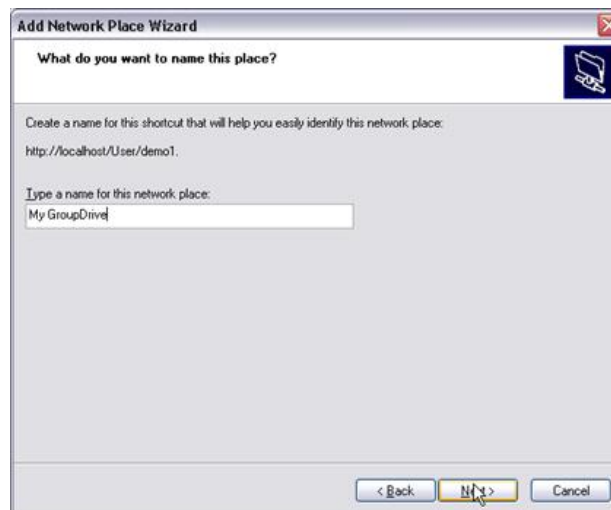
1. To start the configuration process, click the **My Network Places** icon on your Windows desktop.
2. Double-click **Add Network Place**.



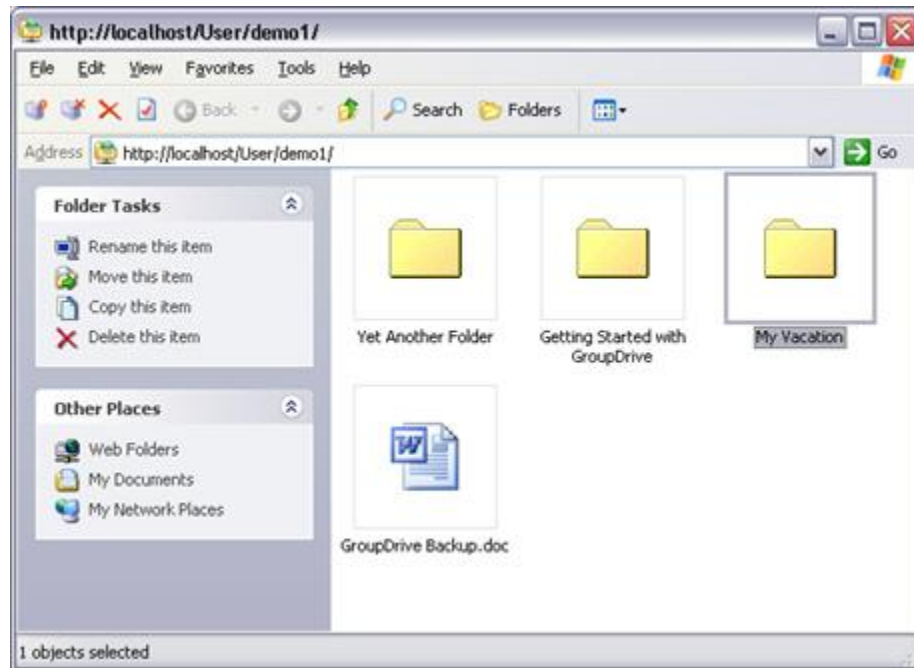
- The **Add Network Place** wizard will launch. When prompted, type the GroupDrive **URL** and your **User Path**. Our sample server is named **testdrive.groupdrive.net**, and our sample username is **demo1**, so the full URL is **http://testdrive.groupdrive.net/User/demo1/**.



- Click **Next**.
- When prompted, type your **Username** and **Password** and select the check box to **save password**. Click **OK**.
- After you have successfully typed your **Username** and **Password**, you will be prompted to type a user-friendly name to be associated with this WebFolder; you can choose any name, such as **My GroupDrive**.



- Click **Finish** to save the WebFolder configuration.



- If you receive the error **The folder you entered does not appear to be valid**, you should download the latest update to WebFolders from [Microsoft's Web site](#).
- File transfers using WebFolders are accomplished by dragging a file or folder from your local computer to the WebFolder.
- You can view a file on your GroupDrive using WebFolders by double-clicking the file. This will cause WebFolders to copy the file to your local Internet cache folder and then WebFolders will launch the default application associated with the file. **NOTE:** Any changes made to the local cached file will **NOT** be copied up to your GroupDrive. To edit the file using WebFolders, you must first drag the file to your Windows Desktop, then edit the file, then manually drag it back to your GroupDrive.

Contact Information

Corporate Headquarters Address:	South River Technologies, Inc. 179 Admiral Cochrane Drive Suite 110 Annapolis, Maryland 21401 USA
Main Telephone:	410.266.0667
Fax:	410.266.1191
Website:	http://www.SouthRiverTechnologies.com
Sales Inquiries Email:	sales@southrivertech.com
Telephone:	410.266.0667
Fax:	410.266.1191
Support Inquiries Website:	www.srthelpdesk.com

Troubleshooting

SRT Knowledgebase

Visit our [Knowledgebase](#) to read helpdesk articles and answers to frequently asked questions.

Reporting Problems

To report a problem, visit the GroupDrive support site at <http://www.SouthRiverTechnologies.com/support/>.

Please furnish our Support Engineers with the following information:

1. The Windows platform you are running.
2. The version of GroupDrive that you are using.
3. The [URL](#) of the server you were using when the problem occurred.
4. A detailed description of the problem. Include file name and complete sub-directory name, if applicable.
5. Attach a copy of the log file to your e-mail.

Index

A	
About GroupDrive Server	14
Access control.....	87
access control entries (ACE)	87
access control list (ACL)	87
Adding Users	75
Administration Port.....	15
Administrator Password	15
Administrator Username	15, 21
Authentication	77
C	
Close Tray Application.....	14
Connections tab	83
Creating New Users	79
D	
Data Directory	21
Deleting Groups	74
Deleting Users	80
Desktop Client Access.....	110
Desktop Client Installation.....	17
Directory Quotas	46
Domain.....	21
Domain Properties.....	21
F	
Force Complex Password Rules	81
G	
General Group Settings.....	76
General User Settings.....	81
Group Membership	82
GroupDrive Desktop Client Access	8
GroupDrive Desktop Client For Windows	110
Groups.....	70
H	
Host Address	15
I	
IP Access	83
IP Access Restrictions	46
L	
Launching the Administrator	15
LDAP User Authentication.....	77
Linking to.....	90
Local Administration IP Address/Port.....	21
Local Domain Description	21
Local Domain Name.....	21
Local Domain Wizard	15
Log Directory.....	21
Log Settings	46
N	
New Groups.....	74
New Server Wizard.....	23
O	
ODBC Data Source User Authentication.....	77
Open Administrator	14
R	
Removing Users	75
Rights.....	48
Run at Startup.....	14
Run Tray Applet when Windows Starts	21
S	
Security Settings (SSL).....	45
Server	46
Servers.....	23, 28, 37, 39, 46
Shared Files	85
Shared object	90
Sharing tab	89
SSL	i, 5
Start Service/Stop GroupDrive Server Service	14
Starting GroupDrive Server	14
Statistics	57
System Requirements.....	8
U	
user authentication.....	41, 77
User Connection Settings	83
User Rights	48
User Settings.....	81
V	
Virtual Files tab.....	92
Virtual Folders	85
W	
Web Browser Interface	8
WebDAV	112
WebDAV protocol	i, 5
Windows Active Directory User Authentication.....	77
Windows NT/SAM User Authentication.....	77