User Manual

Table of Contents

List of Figures

INTRODUCTION

What Is FileReplicationPro

FileReplicationPro ("FRP") is your solution for file replication, file synchronization, and file backup. It is the best way to automate file copy operations and file distribution.

FRP is written in Java. It will work on any operating system that supports Java 1.4.1. This includes any Windows operating system, any flavor of UNIX including Linux, Sun Solaris, Novell Netware, and Mac OS X.

FRP is a pure TCP/IP application. This means that any two computers that are connected via a LAN, WAN or the Internet can use FRP.

FRP allows a user to move, copy, and synchronize directories and files by creating jobs. A job is a listing of the source path, destination path and the file operation you want to perform such as move, copy, one-way mirror, or two-way mirror. Once you create a job, you create a schedule for the job. Schedules range from run immediate, run once at a specified time, run on an interval, or run continuously. Schedules can be quite complex yet flexible.

Advanced features such as filters to include or exclude files and/or directories, bandwidth throttling, encryption, file compression and initialization procedures to comply with firewall rules are also available.

FRP is a "set it and forget it" operation. Once you configure it, the engine continues working under the hood. It creates summary and detail log files, which are configurable, and marks each success and failure. Email alerts are available to notify the user when jobs do not run correctly or to monitor that jobs are running correctly.

FRP provides a lot of value at a reasonable cost. Our licensing scheme is simple and provides all the features for one price. You get multi-threading, bit level replication, real-time OS hooks, bandwidth throttling, and auto-detection all for one low price. New features are always being added and they come free with the purchase of the maintenance and support bundle.

What Makes FRP Smart

FRP is smart about how it copies by using differential replication to skip files that haven't changed since the last replication and by using bit-level comparison technologies to transfer over only the portions of the file that have changed. With real time enabled, operating system hooks inform FRP within milliseconds of file additions, deletions, or changes. This is very useful when you have hundreds of thousands of files you need to keep in sync.

FRP doesn't just copy files; it also copies the permissions from both Windows and UNIX computers. In Mac OS X it copies the files' resource forks as well. FRP makes sure you get the complete file you need with all its associated permissions.

For the advanced user, FRP has include and exclude filters, and firewall friendly ports and IP addressing so that you can get the files you need where ever you may need them.

If a replication problem arises, FRP will retry replication and continue from where it left off. Log files are always available and FRP can send out email alerts to notify you when there is a problem.

What Makes FRP Easy

During installation and configuration on a local network, FRP detects its own installations enabling all your servers to show up on a single configuration screen. You can immediately begin defining jobs and schedules without having to know the server's IP addresses.

Job configuration is intuitive. Because all the servers have been automatically detected, you only need to provide the source and destination directory information. Add a schedule to the job and let it run. If a job fails, or a transfer was incomplete, you will receive email alerting you to the problem. From the central management console, you can view the log and status information for all your servers.

What Makes FRP Secure

FRP takes security very seriously and has created a number of safeguards to ensure that your files are secure.

If you choose to encrypt your file transmission, we use the Advanced Encryption Standard at 128 bit. This is the Federal information processing standard for advanced encryption used by US Government organizations to protect sensitive information.

For two computers to participate in the replication they must exchange and match encrypted licenses. All licenses are embedded and encrypted within the software. This prevents an un-trusted server from participating in the replication. In addition, FRP will only transfer data in the context of preconfigured scheduled jobs from "known" servers and will reject any "open-ended" communications attempt.

FRP runs in the application layer (although it functions as a service) and is subject to the security framework of its host server. In addition, we also allow the owner of each and every server that participates in the replication to set a replication password, if he so chooses to control replication access to the servers.

Entry to the configuration console is also password protected. This password ensures that only individuals assigned as administrators can access the jobs and schedules.

By using Java based FRP running as a pure TCP/IP application instead of a Windows based solution; you are also eliminating many known and unknown risks. Shared folders and Windows Networking are well known for their vulnerabilities. FRP offers several state of the art technologies to ensure the security of your replication, synchronization, and backup.

Features and Benefits

Installation

Simple installation and configuration on most computers.

LAN Auto Detection

Computers on a Local Area Network are detected automatically by utilizing UDP multicast technology.

IP Address & Port Is All You Need

For computers not on a LAN, servers are added simply filling in an IP address and port number.

Any Operating System

FRP will run on any operating system that runs Java 1.4. Here is list of Java Ports.

OS	CPU	Company / Organization	Description
AIX		IBM	Java for AIX
DG/UX 4.2	Intel	Data General Corporation	JDK for DG/UX
DIGITAL OpenVMS	Alpha	Digital Equipment Corporation	JDK for DIGITAL OpenVMS
DIGITAL Unix	Alpha	Digital Equipment Corporation	JDK for DIGITAL Unix
HP-UX		Hewlett-Packard	JDK for HP-UX
IRIX		Silicon Graphics	Java for Silicon Graphics
MacOS		Apple	MacOS Runtime for Java
NetWare		Novell	JNDI, NSI, JITand Java VM for IntranetWare.
OS/2	i386	IBM	Java for OS/2
OS/390, OS/400		IBM	Java for OS/390, OS/400
SCO	i386	SCO	JDK for SCO
UnixWare	i386	SCO	JDK for SCO

VxWorks		Wind River Systems	Java VM on VxWorks, an embedded RTOS
Windows NT	Alpha	Digital Equipment Corporation	JRE for Windows NT Alpha

Centralized Web Based Configuration

The FRP management console is a complete web based application provided to configure and monitor the replications, synchronizations, and backups. With the proper security, an administrator can access the management console from any browser providing ease of use, portability and a common interface.

The management console will automatically distribute any changes or updates to all your servers. Once you have configured your servers and entered jobs at the management console, there are no additional steps to take.

Centralized Logs

The management console also provides a centralized view of all your server's activities. Watch in real time, upon job completion or simply examine the summary logs. There is no need to visit each server in the replication and hunt for their logs. For greater efficiency, the management console can send email to you upon job completion or alert you to error conditions.

Servers, Jobs and Logs

The management console lets you view your servers, view your jobs, or examine your logs. Views can be filtered allowing you to manage cross-platform environments with consistency and ease.

Advanced Configuration Features

FRP is simple to use, yet powerful. The advanced features allow you to:

- Include only files/Folders/Exclude files/Folders
- Bandwidth Throttling
- Pre & Post Commands and Batch Files
- File Compression
- Encryption using 128 bit Advanced Encryption Standard or 128 bit Blowfish
- Set which server should initiate connection for firewall or NAT rules

Configuration Security

Multiple levels of security are available to you. All configurations are encrypted and all communication can be via SSL.

FRP runs in the application layer as a service and is subject to the security framework of its host server. Replication access to the servers can be controlled by assigning server passwords.

To ensure administrator only access, the management console is also controlled by a password.

Organize Your Servers

The following is a list of possible scenarios where FRP has delivered working solutions for a wide range of clients.

- Central server updating distributed servers
- Office server updating individual clients
- Many servers backing up to a central server
- Central server gathering data from distributed office servers
- Office servers gathering data from individual PCs and laptops
- Cascading Replication and Synchronization
- Web server updating many mirror sites
- Replicating over VPN, leased lines, WAN and LAN
- Backup to Network Attached Storage
- Cross Platform Distribution
- Offsite Backup to multiple locations
- Disaster Recovery mirroring
- Database Image and Log File Backup

TCP/IP Protocols

By using TCP/IP as the base protocol, all your serves can communicate with each other and transfer data on a schedule using FRP

Changed Files Only

Instead of replicating every file, FRP only replicates any files have changed.

Bit Level Copy

For files 10Mb or larger, FRP uses Bit Level technology to copy only the changed portion of the file. Transfer block sizes are determined by the file size and type allowing for improved matching and less data transferring. Transferred data is further compressed to improve transfer speed. This technology not only reduces the amount of bandwidth, but also the number of "round trips" required to accomplish the copy, making it particularly attractive for replication over WANs and the Internet

Real Time Event-Driven Replication

With Real-Time Operating System hooks for Windows and Linux, the operating system informs FRP within milliseconds of any file creation, change, or deletion. With Access Control List (ACL) real time triggering enabled, ACL changes will also trigger a replication.

Scalability

By utilizing advanced memory and CPU techniques, FRP takes up a small footprint. While large amounts of changed data as well as a large number of servers replicating simultaneously may affect the computer CPU and memory requirements, these techniques make the requirements quite manageable and allow for unlimited scaling.

Permissions

Copying and preserving file permissions for windows and UNIX are supported including full NTFS descriptors for windows and full UID, GUID for UNIX. FRP ensures that your data operations are performed intelligently, using the minimum amount of resources possible.

Replication Scenarios

LAN ONLY

Definition:

LAN Only refers to a situation where there are a series of computers situated on the same Local Area Network

Scenario:

The General Manager of the local division of a large national organization wants to keep a backup of all sales activities of its main office on a central Server. There are currently 12 sales representatives, each with their own computer connected together by a LAN.

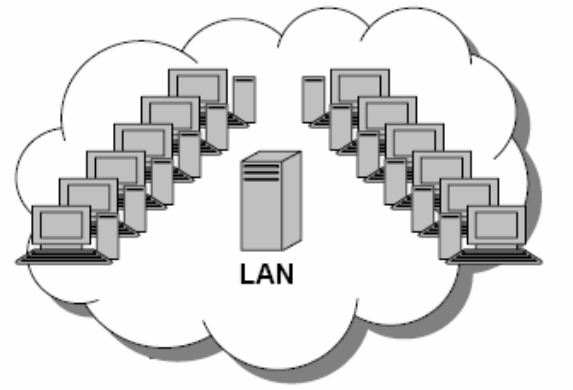


Figure 1 - LAN Only

Procedure:

FRP Replication Server needs to be installed and running on all computers. One computer would be selected and configured as the management server, while the rest are left as Replication Servers.

The management server automatically detects all Replication Servers. Using the management server, the General Manager would set up a Copy Replication job to include the Sales folders. This job could be scheduled to run daily after hours so as to not interfere with the daily operations of the company. The next day, the General Manager could then peruse the current sales information from one computer.

WAN ONLY

Definition:

WAN Only refers to a situation where there are a series of computers that are not situated on the same Local Area Network, but can access each other by way of a WAN (Wide Area Network).

Scenario:

Three branches of a national chain need to share data in real-time.

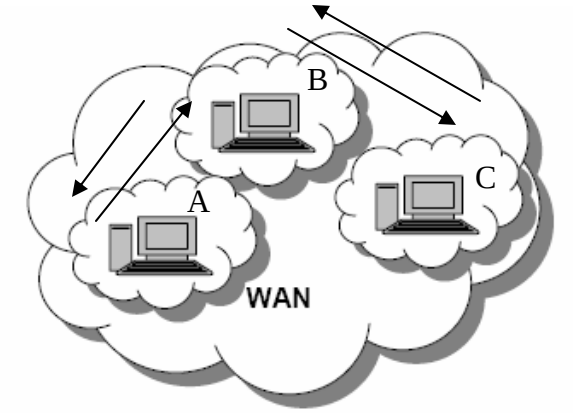


Figure 2 - WAN Only

Procedure:

A FRP Replication Server would need to be installed and running on all three computers. One computer would be selected and configured as the management server and Replication Server, while the other two are left as Replication Servers only.

The Replication Servers would need to be manually added to the management server's Server Overview screen. Then, the management server would be used to create several two-way mirror replication jobs scheduled for real-time, that would mirror the main directories of office A to B and office B to C. (Note: office A to C mirroring is accomplished by default via office B)

LAN & WAN

Definition:

LAN & WAN refers to a situation where there are a series of computers that are situated on the same Local Area Network, that can access another series of computers by way of a WAN.

Scenario:

An international company supports a website in the US and Europe. The developers are located in India.

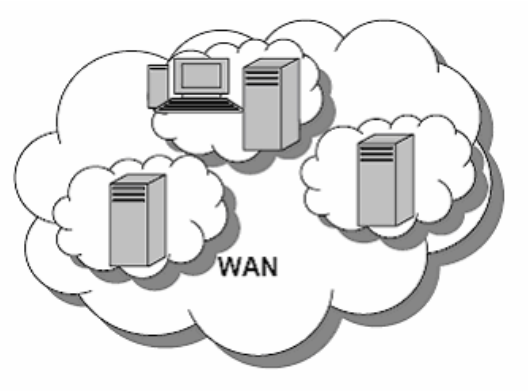


Figure 3 - LAN & WAN

Procedure:

FRP Replication Server would need to be installed and running on all the computers. One computer within the LAN would be selected and configured as the management server, while the others are left as Replication Servers. The Replication Servers would need to be manually added to the management server's Server Overview screen.

The management server would be used to create several scheduled jobs to run sequentially. The first job would be a one-way mirror replication from the developer's computer to the stage server. The second job (scheduled to run after the first job) would be a daily one way mirror from the stage server in India to the live servers in the USA and Europe.

TWO LANS

Definition:

Two LANs refers to a situation where there are a series of computers that are situated on two separate Local Area Networks, and can access each other by way of a WAN.

Scenario:

Two main offices, one in San Francisco and one in New York, need to be informed of each other's daily sales.

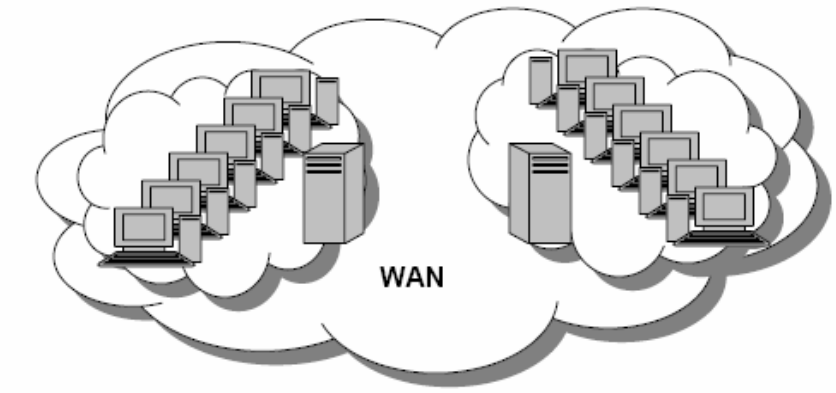


Figure 4 - Two LANs

Procedure:

FRP Replication Server would need to be installed and running on all the computers. One computer would be selected and configured as the management server. For our example, we will configure a server in New York as the management server. The remaining computers at both locations are left as Replication Servers only.

The New York Replication Servers would be automatically detected and added to the Server Overview screen. The San Francisco Replication Servers would need to be manually added to the management server's Server Overview screen.

The management server would be used to create several scheduled jobs. First, a Copy Replication job would be scheduled to run nightly; from all the local workstations (LAN) in each office to a specified sales directory on its corresponding central server. Second, a two-way mirror replication of the Sales folder would be set up between the two central servers. This job would be configured to run after the first job.

INSTALLATION

First Time Set-Up

To Set up FRP on your network you must create a management server and at least one Replication Server. These two Servers must have access to each other by way of a LAN or a WAN.

Management Server

The management server is used to create and schedule jobs, view logs, and manage the replication process. Before installation it is important to select a management server. Ideally, the management server must have two-way communications with all other Servers via port 9100. In a **LAN Only** situation, any Server can be the management server.

Note: Once the jobs have been defined and scheduled, the management server does not need to remain online for replication to take place if the management server is not part of the replication process.

Replication Server

All computers that are going to be involved in the replication process are replication servers. They need to have an installed and running version of FRP Replication Server.

Note: Replication will only take place when all computers involved in the replication process are turned on, and running FRP Replication Server. In order to ensure that scheduled jobs are run; it is strongly recommended that FRP services are set to start automatically, when the computer is turned on.

Installation

To install FRP:

1. Download FRP from the FRP Website http://www.filereplicationpro.com/

Click on Download then click on the appropriate installation.

2. Click the Open Button; to begin the download and installation...
3. After the download has completed, the installation will begin automatically.

The following screen will appear:

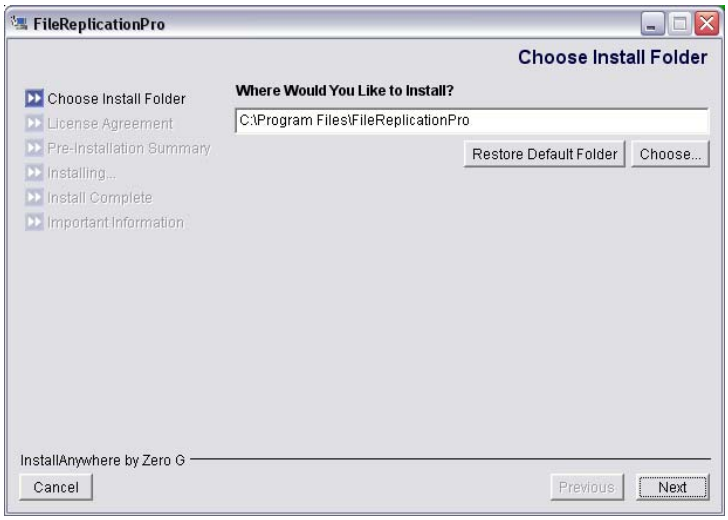


Figure 5 - Choose Install Folder

4. Select the folder that will be used to install FRP. Click on the **Choose** Button to browse, or type the path directly into the field.
5. Click on the **Next** Button; the **License Agreement** screen opens.
6. Scroll down and read the agreement and select the radio button beside the Acceptance statement.
7. Click the **Next** Button; the **Pre-Installation Summary** screen opens.

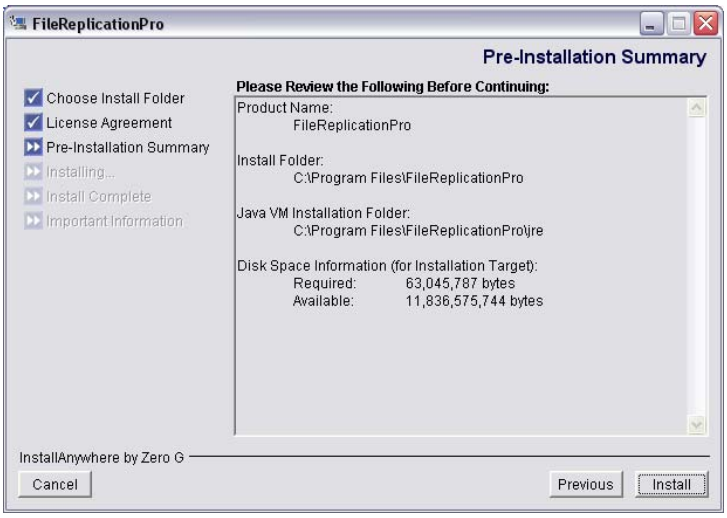


Figure 6 - Pre-Installation Summary

8. Review the installation information to ensure that it is correct and click the **Install** Button; installation begins and the following screen appears.

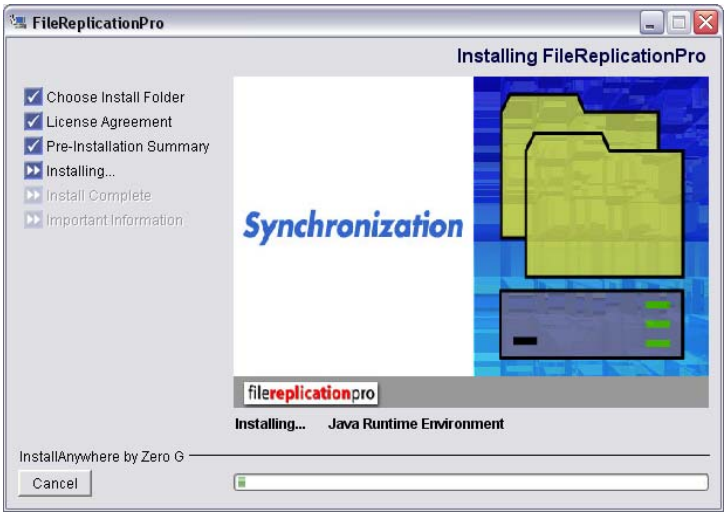


Figure 7 - Installation

9. Follow the onscreen instructions. The last installation screen provides detailed information about the installation as well as instructions on starting up FRP services

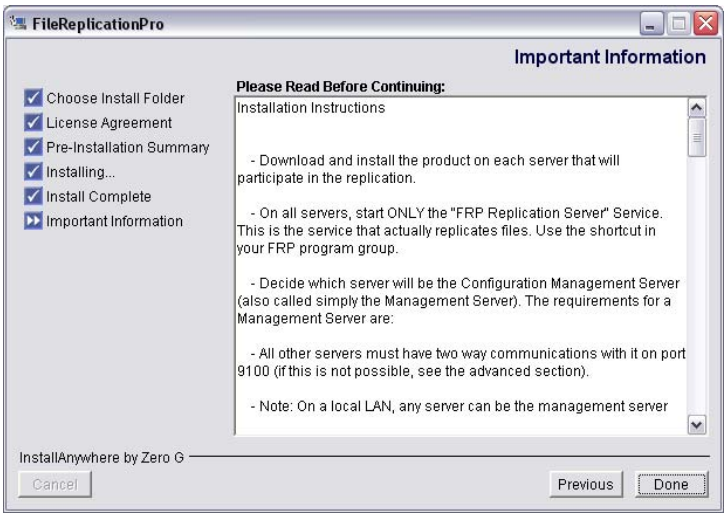


Figure 8 - Installation Important Information

10. When installation is complete, click the **Done** Button to quit the installer.

Auto-Start

Windows98 and ME

In order for FRP to run at startup, FRP needs to be added to the Windows Startup Directory.

To add FRP to Startup:

1. Right Click on the Windows **Start** Button.

2. Select **Explore** from the menu; a Windows Explorer will open, with the **Start Menu** Directory selected.
3. Double Click the **Startup** Folder in the **Program Files** Folder that is in the **Start Menu** Directory
4. Select File > New >Shortcut.
5. A create shortcut window will open. Click browse. Browse to the location of FRP executables (FRP home directory). Select FRPRep.exe click next and name it FRP Replication Server. Repeat this process for the FRPHelp.exe file. If the server will also act as a management console, repeat this process for the FRPMgmt.exe file.

Windows 2000, Windows XP, and Windows 2003

1. To set FRP Services to automatically start:
2. From the Start Menu Select Settings > Control Panel; the Control Panel Window opens.

3. Double click on the Administrative Tools Icon; the Administrative Tools Window opens.
4. Double Click on the Services Icon; the Services Window Opens.

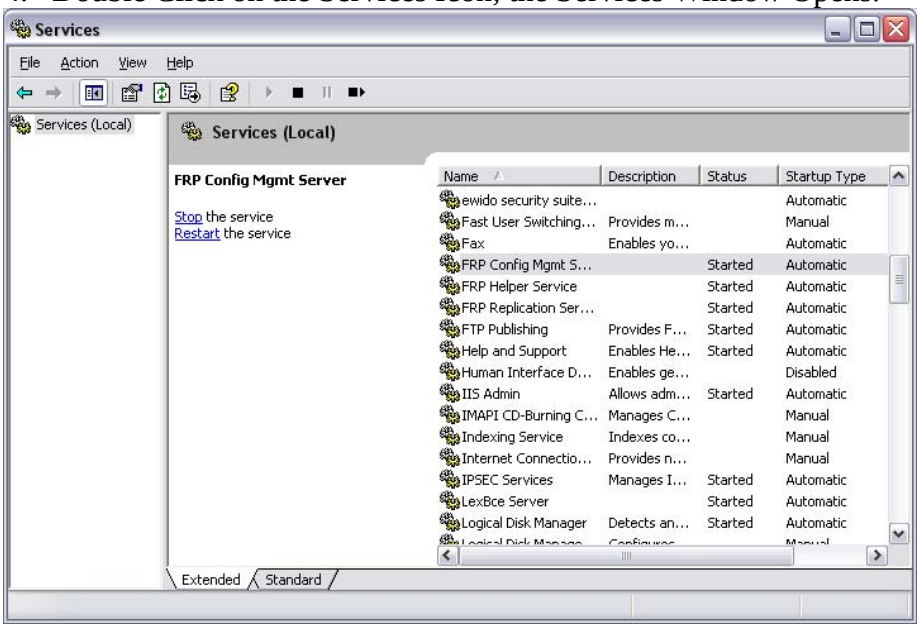


Figure 9 - Services Window

5. Scroll down and Double Click on the FRP Replication Server; the FRP Replication Server Properties Window opens.

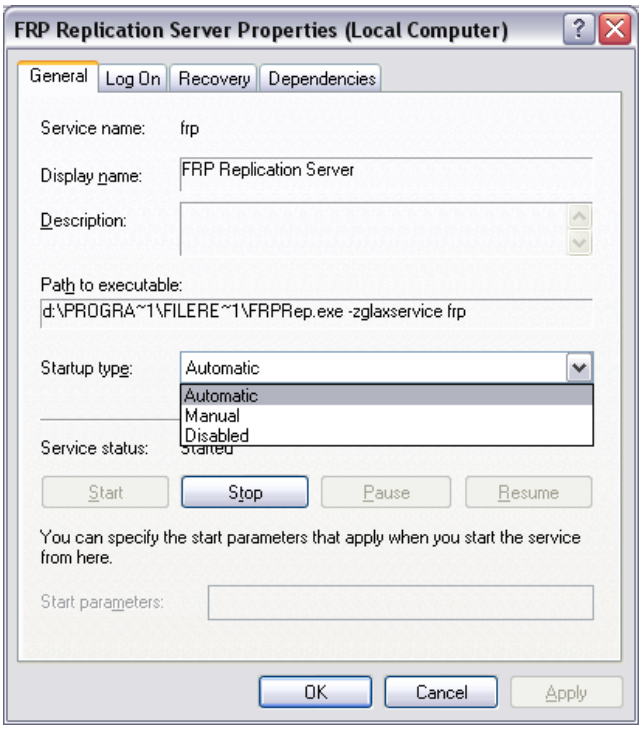


Figure 10 - FRP Replication Server Properties

6. Select **Automatic** from the **Startup type:** Drop-down list.
7. Click the **Apply** Button.
8. Click the **Start** Button in the **Service Status:** Section.
9. On the management server repeat all the above steps for the FRP management server Service.

Non-Windows Servers

Users should follow the specific operating system installation instructions shown on the filereplication website.

In general, the Linux and UNIX installer is a file named frpro.bin that needs to be downloaded, saved, changed with user executable permissions, and then executed from the command line (e.g. $ ./frpro.bin).

For Novell Netware, the installer is a file name frpro.jar, that should be downloaded, saved, and then executed using the command line: "java -jar frpro.jar"

In all these cases, the command will start the FRP GUI installer as described in the Windows Installation section.

Startup script and Auto-Start for Linux, UNIX and Netware

- UNIX/Linux: See knowledgebase article no. 3
- Novel Netware: See knowledgebase article no. 24

Please note that FRP also supports silent and console mode installation See Appendix C – Optional Installer Modes.

UNINSTALL/UPGRADE

Windows Based Servers

To uninstall FRP:

1. From the Start Menu select **Settings**>**Control Panel**.
2. Double click on the **Add/Remove Programs** icon.
3. Select FRP from the list of programs.
4. Click the **Add/Remove** Button.
5. When performing a major update or full uninstall, manually delete the FRP home directory. When performing a minor upgrade and you want to retain your jobs and configuration information, do not delete the FRP home directory.

MANAGEMENT CONSOLE OPERATION

FRP is managed using a web browser, and can be managed by any computer that has access to the management server using the specified management port. FRP is platform independent.

Login

FRP provides two methods for logging in to the FRP management console window:

1. Directly from a browser window (Recommended method)
2. Running the Connect_to_FRP_MS executable (Figure 13)

Directly from a browser window

1. On the FRP management server, open a browser window.
2. Enter the following (path) in the address window:
   http://<local host name or IP address>:9100/ to open the **management console Login** screen (Figure 11)

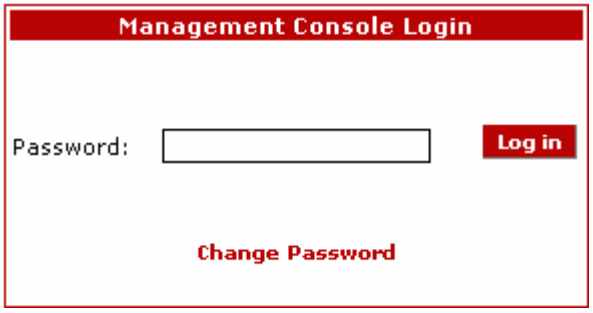


Figure 11 - Login screen

Note: It is possible to access the management server from any other computer that has access to the management server's IP address and the Management port. The management console Login screen appears with the host name in the top left corner. Example: http://mycomputer:9100/

---

3. Enter admin into the **Password** Field on the **management console Login** screen, and click the **Log in** Button to open the **management console screen** (Figure 12)**.**

Changing the Login Password

The default login password for FRP is 'admin'. It can be changed when logging into the **management console**.

To change the Login Password:

1. Click on the **Change Password** Link beneath the **Password** Field on the **management console Login** screen to open the **Change Password** screen.
2. Enter the current password ('admin') in the **Current Password** Field.
3. Enter a new password in the **New Password** and **Re-enter New Password** Fields.
4. Click the **Change Password** Button to create the new password. Or Click the **Cancel** Button to clear all information and return to the **management console Login** screen.

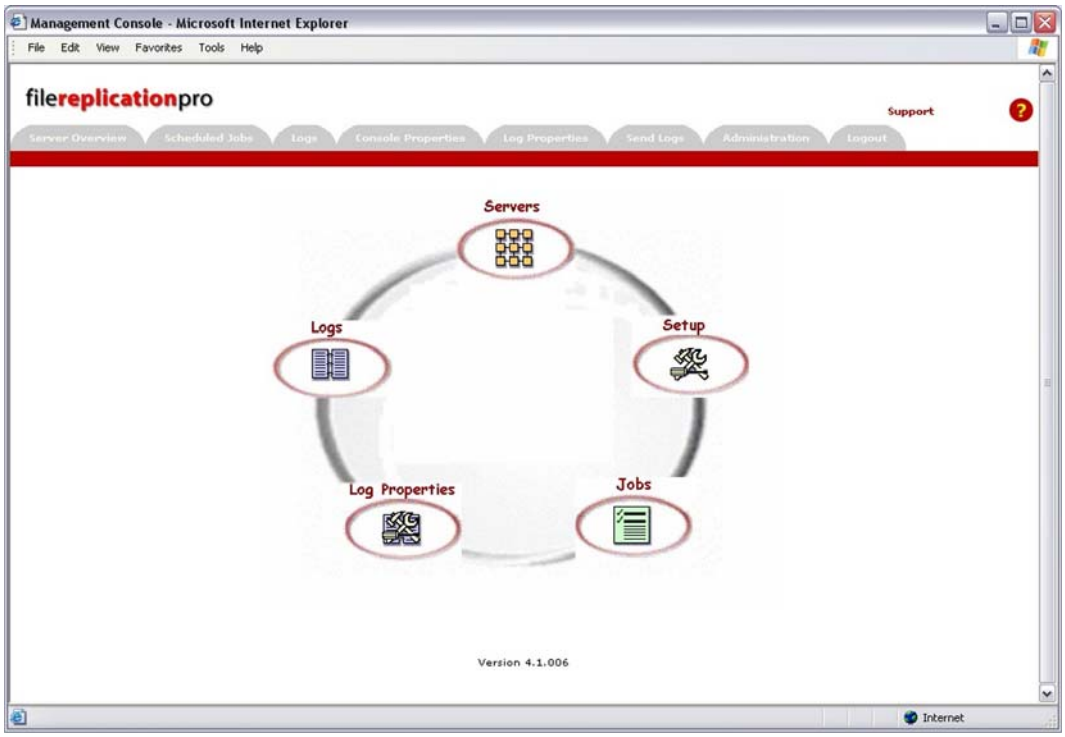


Figure 12 – management console screen

Connect_ to_FRP_MS

If the user is unsure how to start the configuration manager from the browser, FRP provides a small utility named Connect_to_FRP_MS which can be used to launch the configuration manager.

1. From the start menu, click All Programs\FileReplicationPro\Connect_to_FRP_MS
2. Select the appropriate URL for your configuration management server.
3. Click on Launch URL to open the **management console Login** screen (Figure 11)

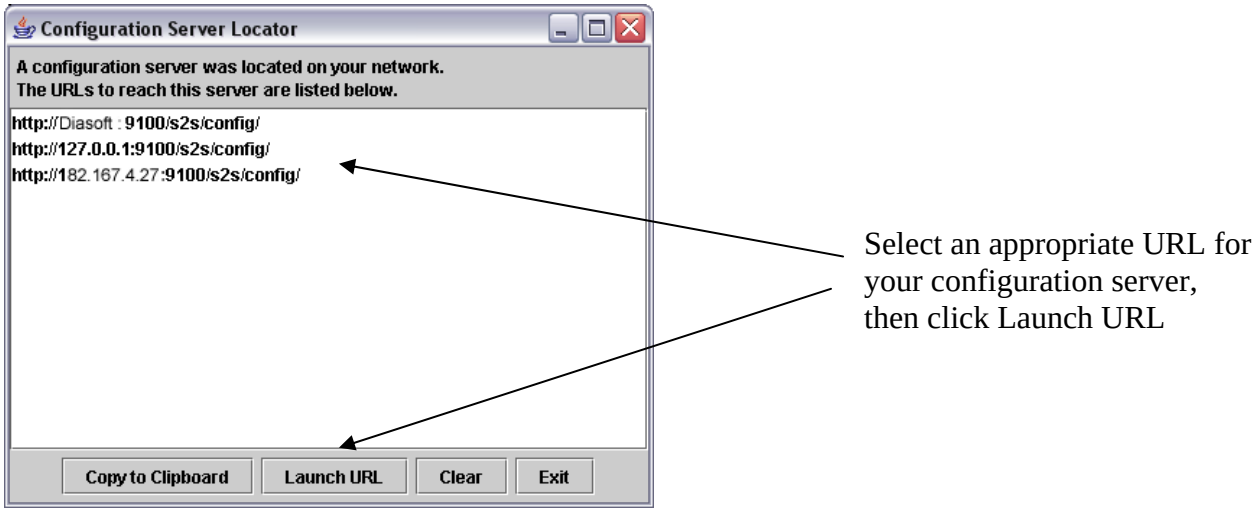


Figure 13 - Configuration Sever Locator

SERVER OVERVIEW

Overview

The server overview window is used to view your server's status, add/delete servers manually, and edit server properties such as its port number, password, or license.

There are two types of FRP servers:

- Management servers.
- Replication Servers

A management server manages replication servers and replication jobs. The management console enables the adding and editing of replication servers and managing replication jobs. All replication servers that are associated with a specific management server are part of that management server's management group.

A replication server is a server that is configured to perform FRP replication jobs.

FRP recognizes two categories of replication servers:

- Fully-Accessible Servers
- Partially-Accessible Servers.

Local Servers

These servers include all auto-detected replication servers on the management servers LAN, and any manually added replication servers on a WAN that has two-way connectivity over port 9100 (or user defined) to the management server.

Remote Servers

These servers include replication servers that are a part of another management group and that have sufficient connectivity to allow for replication with Fully-Accessible Servers. These replication servers do not have two-way connectivity to the management server and are typically on another LAN.

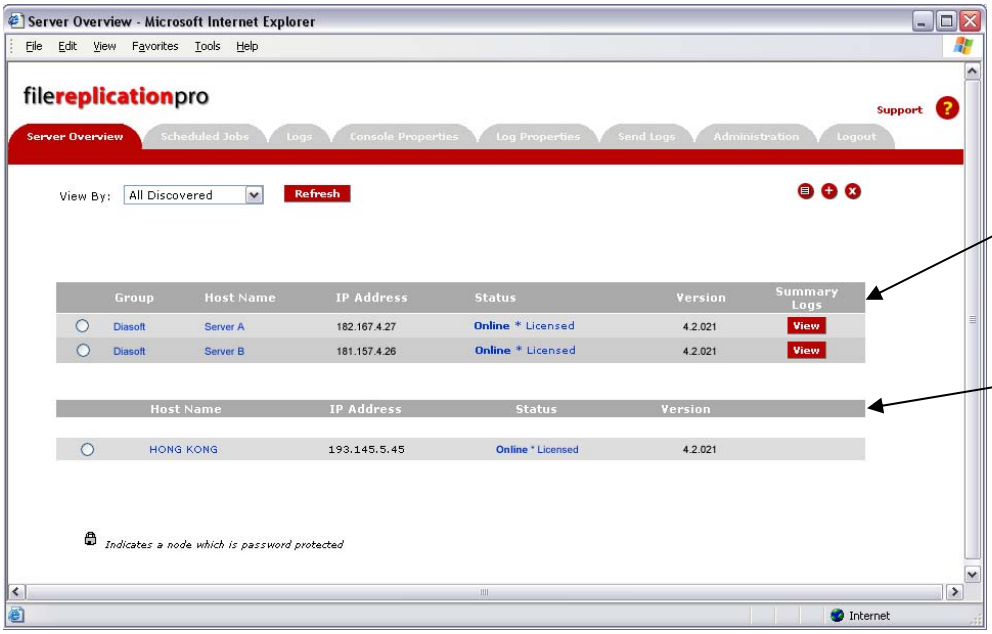
FRP uses **Auto-Detection** to locate and display all FRP replication servers that are on the same LAN as the management server, and support UDP. The management server broadcasts UDP packets over the LAN, and any replication server that can hear them responds. UDP is a standard part of every network. It will be present unless it has been intentionally disabled. The management server then creates a list of detected replication servers which are displayed on the **Server Overview** screen. The auto-detect procedure is performed frequently to maintain system accuracy.

Viewing Servers

The **Server Overview** screen displays all servers that have been automatically discovered by the FRP management server, or manually added to the management group. These servers are listed on the **Server Overview** screen (Figure 14).

Note: The first time the **Server Overview** screen is accessed, only Replication Servers that have FRP Replication Server installed and running, will be auto-detected and visible. (*see* INSTALLATION *Page 13*)

To view the Servers:
From the **Main Console** screen, click on the **Server Overview** Link. The **Server Overview** screen will open and display a list of servers found by the management service.
OR
From any screen click on the **Server Overview** Link at the top of the screen; The **Server Overview** screen opens displaying the list of servers.



Local servers & remote servers with bi-directional connectivity

Remote servers with none or unidirectional connectivity (the management server can connect to it but it can not connect to the management server)

Figure 14 - Server Overview screen

Filtering Servers

The **View By:** Drop-down List selects which servers are to be displayed in the **Local Servers** list. The options are:

- **All Discovered** – This is the default setting. All detected servers will be listed.
- **All FRP Configured** - Shows all the servers that have jobs assigned to them.
- **Unlicensed Servers** - Shows all the servers that do not have a legally purchased license. Servers with trial licenses will also be listed.

To filter Servers:
Select an option from the **View By:** Drop-down List and click the **Refresh** Button.

Replication Server Properties

The following properties are listed for each replication server:

- Group - A Group is made up of all replication servers that are managed by a single management console. This is set automatically and cannot be changed.
- Host Name - This is the server's host name. Each replication server must have a unique host name.
- IP Address - This is the server's IP Address.
- Status - This field indicates the server's current status; either online or offline and if the server is licensed or a trial version.
- Version – The currently installed and running FRP version.
- Summary Logs - Clicking on this button will open the logs screen for the specific Replication Server (*see* LOGS *Page 39).*

Add Server

The first step in adding a replication server is to install the FRP on the new server. If the new replication server is located on the same LAN as the management server, it will be automatically detected, and appear on the **Fully-Accessible Server** list on the **Server Overview** screen.

A server would need to be added manually if:

- The server to be added is located on a LAN that does not support UDP.
- The server to be added is not located within the same LAN as the management server.

Note: FRP services must be installed and running on all servers to be added to the management console.

Verify Services

To verify that FRP services are running:
In a browser window, enter http://<hostname>:9200/ on the address line.

A similar message to the following should appear:
FRP Node Ready F4a9EBF0CD4B63 OK

If FRP services are not running, an error will appear.

Adding a Replication Server in a Standard LAN

To Add a **Replication Server** (in a LAN with UDP support):

1. Install FRP on the new server.
2. Start the replication services on the new server.
3. On the management server, open the management console
4. Open the **Server Overview screen.** The **Local Server** List will display all auto-detected Replication Servers, including the new server.

Manually Adding a Replication Server

To manually add a Replication Server:

1. Install FRP on the new server.
2. Start the replication services on the new server.
3. On the management server, open the management console
4. Open the **Server Overview** screen**.**
5. Click the **Add Server** button.
6. Enter the server information into the appropriate fields.
7. Click **Add**.
8. FRP will process the information and determines if FRP services are running on the new server, return to the server overview screen, and update the screen with the newly added server.

Note: The Replication Password default to blank. This password is only needed when adding an existing password protected server.

Add Server Fields

Host Name

The new server's host name. The true host name does not have to be used; a symbolic name can be entered here. Only the IP address is used for identification purposes.

IP Address

The new server's IP Address.

Port #

The port number to be used for replication between the servers. The default port is 9200.

Replication Password

If the new server is password protected, enter the password in this field.

Edit Server

Each Replication Server can be selected from the Server Lists to edit its properties. The current Replication Jobs for each Replication Server can also be viewed from the **Server Properties** screen (Figure 15).

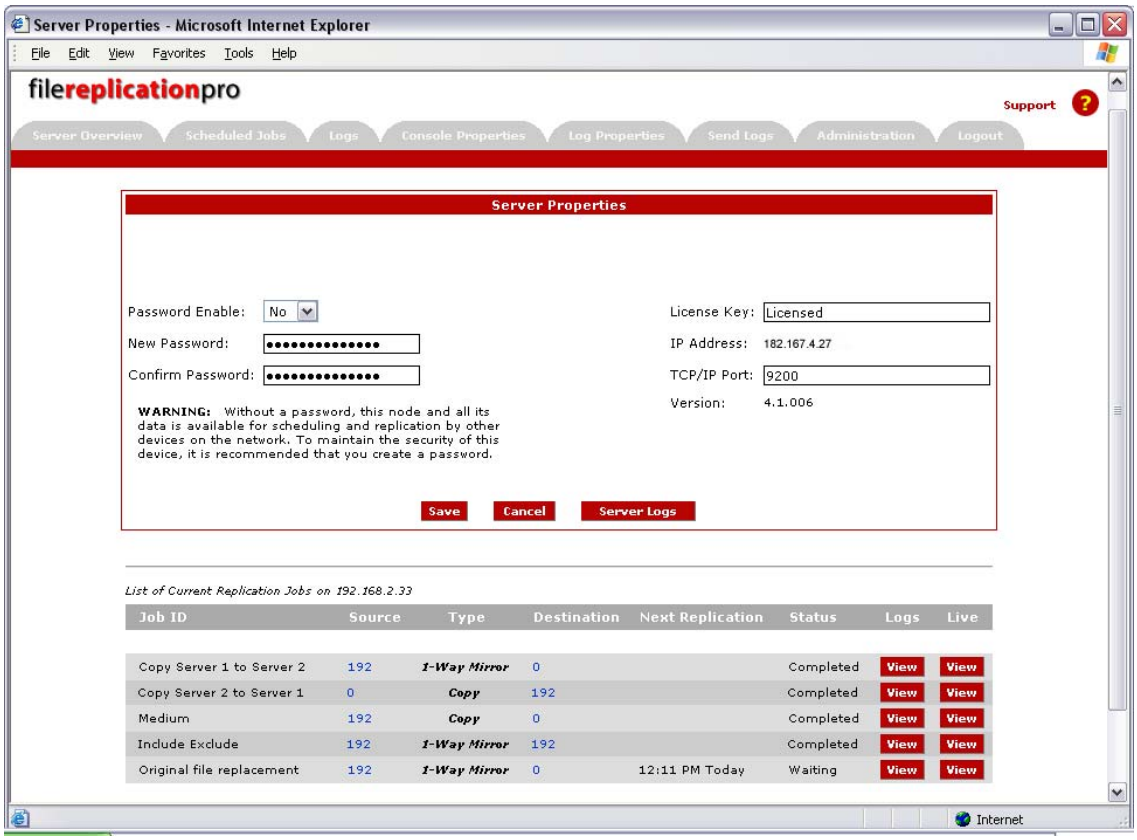


Figure 15 - Server Properties screen

To Edit a Server:

1. Select a server from the **Fully-Accessible Server** list by clicking the radio button next to the server name.
2. Click the **Edit** Button. (The Server Password screen opens, if the Server has been password protected)
3. Enter the password in the **Server Password** field, and Click **OK** to open the **Server Properties** screen.
   OR
   The **Server Properties** screen opens for the selected server.
4. Edit the available fields and Click **Save**.

Password Protection

To maintain the security of data on the Replication Servers, it is strongly recommended to create an FRP password. Without a password, this FRP Server and all its data is available for scheduling and replication by other servers on the network.

To create a password:

1. Select **YES** from the **Password Enable** Drop-down List.
2. Enter the password in the **New Password** Field.
3. Enter the password again in the **Confirm Password** Field
4. Click **Save**.

License Key

FRP initially comes with a 45-day trial license. To continue using FRP after the trial period requires purchasing a license key for each Server. To ensure uninterrupted FRP service, be sure to obtain the necessary licenses before the trial expiration date.

After receiving your license keys, they must be entered in the license field for each server.

Local Servers

To update Licensing information:

1. Copy the License Key from the Email.
2. Open the **Edit Server** screen for the appropriate Server.
3. Paste the License Key into the **License Key** field.
4. Click **Save**; the License Key is updated.

Remote Servers

On each server, there is a file named .key which contains the license key. It is located in the <frp home>\etc folder. Create the file and open it in a text editor. Copy the License Key from the email and paste it into this file. Save the file and place it in the etc folder on the remote server.

TCP/IP Port

The **TCP/IP** Port field indicates the port number through which the replication will take place. The default Replication Port number is 9200.

The Replication Port Number may need to be changed due to firewall requirements.

To change the port number

1. Enter a new port number in the **TCP/IP Port** field.
2. Click **Save**; the port number has been changed.

Current Replication Jobs

This section shows a list of jobs associated with the currently viewed server.

Delete Server

This feature allows the user to remove a server from the management group.

To delete a Server:

1. Select a server from a server list by clicking the radio button next to the server name.
2. Click the **Delete** Button.

Note: You can only delete a server that is offline.

View Summary Logs

Selecting this feature presents the **Logs** screen (Also see Page 39) with the selected server's logs displayed in reverse chronological order. A sample log entry is shown in Figure 16. The log listing shows a history of what replications have transpired for the selected server.

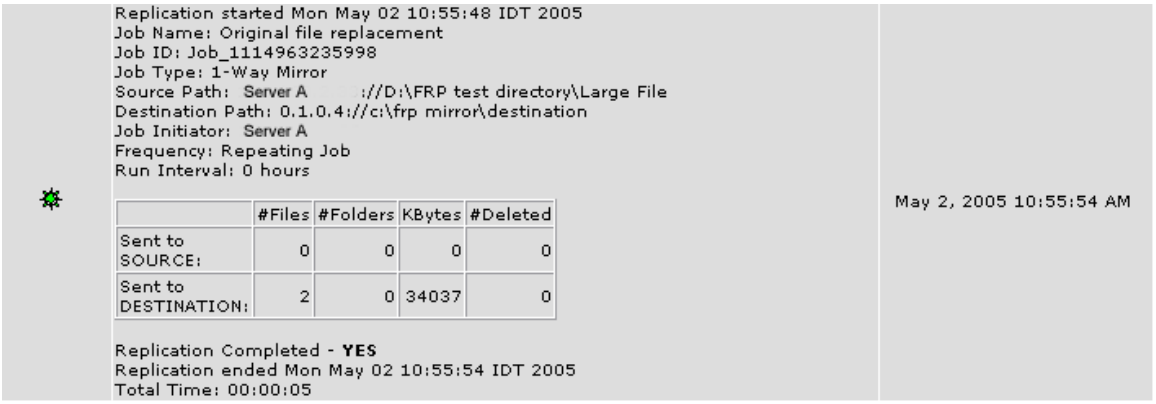


Figure 16 - Sample Log Entry

SCHEDULED JOBS

Overview

Once replication servers have been setup, defining and scheduling jobs are the next step in achieving replication.

Jobs are defined based on the data to be replicated from a source to a destination. The source can be one or a series of files, folders, or directories. Once a source is specified, some files or directories may be excluded from the list and/or other files and directories may be included from outside the defined path.

Once the source and destination has been specified, the job needs to be scheduled. Jobs can be set to run on specific days, dates, and times. They can be set to run once or repeatedly. There are settings for exception dates and times. These are the times in which the job should never run.

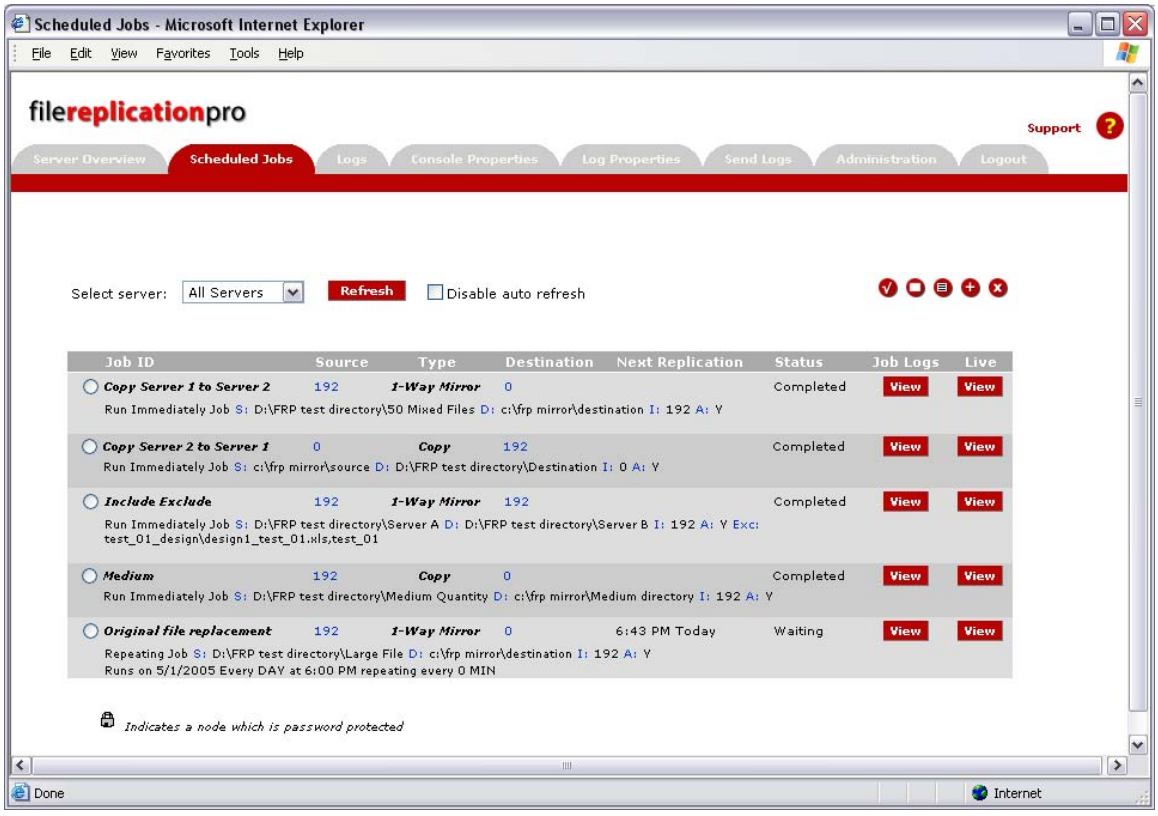


Figure 17 - Scheduled Jobs screen

Select Server

This is a drop down list to filter which jobs are displayed in the jobs screen. Jobs can be viewed by:

- All Servers – All configured server's jobs are displayed.

- Individual servers – Only the jobs associated with the selected server will be displayed.

Disable Auto-Refresh

Selecting this checkbox disables the **Scheduled Jobs** screen automatic refresh. When this feature is disabled, you can refresh the screen anytime by clicking the **Refresh** button.

Job Window Details

The following properties are listed for each Job:

Job ID

The job name.

Source

The source server's host name.

Type

The selected replication type – Move, Copy, One-way Mirror, or Two-way Mirror

Destination

The destination server's host name.

Next Replication

The time the next replication is scheduled to run. A blank field indicates that the job is not scheduled to run again.

Status

This is the current status of the Job – Initializing, Waiting, Replicating, Completed, Aborting, or Failed

Job Logs View

Click this button display a reverse chronological job history log for the associated job.

Live View

Clicking this button opens a window which displays the current job status. See Figure 18.

Figure 18 - Live View

The following list shows some of the messages displayed in live view:

- Starting REAL-TIME Replication…
- Replicating Directory + directory name
- Failed Replication of + path
- Replication Waiting
- Job aborted due to an invalid license key for one of this job's servers
- Replication started + current time
- Job Succeeded

Run Now

There may be times when a job is scheduled for a specific time, but you want to run the job now. This feature is used to start the selected replication job immediately.
To run a job:

1. Click on the radio button next to the job you want to run.
2. Click the **Run Now** Button; a status message will appear on the screen.
3. The status of the replication is updated in the **Status** column.

Note: You can only run a job now if the job is not inactive.

Stop Job

This feature will stop a currently replicating job. This button has no effect if the job is not replicating.

To stop a job:

1. Click on the radio button next to the job you want to stop.
2. Click the **Stop Job** Button to abort the job.
3. The status of the replication is updated in the **Status** column.

Edit Job

To edit a Job:

1. Click on the radio button beside a job to select a Job from the Job List.
2. Click the **Edit** Button; the **Edit Job** screen opens.
3. Edit the appropriate fields.
4. Click the Advanced button to edit advanced features.
5. Click the Schedule button to edit the scheduling fields.

Add Job

Overview

There are three main steps to adding a job.

1. Add basic information
2. Setup advanced features (optional)
3. Setup a schedule

Basic

Figure 19 - Add Job screen

Basic Details

Job Name

Enter a unique meaningful name to identify the job.

Source

Select from the drop down list, the source server.

Source Path

Enter the source server's path here. i.e. c:\data\monthly. You can also select the source server's path by using the remote browser feature (Figure 20). Click the Browse button to

open the remote browser. Click on the arrows starting from the drive letter or sharename and traverse the directory structure. When you get to the directory you want, click on the directory name and FRP will automatically insert the proper path in the source path field.

Figure 20 - Remote Brower

Password
If a password is required to access the source server, enter it here.

Make this Job Active
Check this box to make this job active. Clear this check box to disable the job but save the settings in case you want to re-activate and run the job at a later time.

Destination
Select from the drop down list, the destination server.

Destination Path
Enter the destination server's path here. i.e. c:\backup\data. You can also select the destination server's path by using the remote browser feature (Figure 20). Click the Browse button to open the remote browser. Click on the arrows starting from the drive letter or sharename and traverse the directory structure. When you get to the directory you want, click on the directory name and FRP will automatically insert the proper path in the destination path field.

Password
If a password is required to access the destination server, enter it here.

Replication Types
There are four replication types that can be assigned:

- Move
- Copy
- One-way Mirror
- Two-way Mirror.

Move

The FRP Replication Type **Move** will copy the specified files or folders from the **Source** Server to the **Destination** Server. It then deletes the specified files from **Source** Server.

Example

A web developer would use a **Move** Replication Type to publish to a website from a development computer. The developer would specify a folder on the development computer that he wanted to replicate. Then he would specify the path on the Destination Server where he wants to place the files.

Copy

The FRP Replication Type **Copy** will copy the specified files or folders from the **Source** Server to the **Destination** Server. This does not effect or change the files on the **Source** Server.

Example

The manager wants to review the work of all entry-level programmers. The manager would specify a folder per programmer, on his own computer. He would then set a **Copy** Type Replication job to run twice a day, in order to follow their progress.

One-Way Mirror

The FRP Replication Type **One-way Mirror** will copy the specified files or folders from the **Source** Server to the **Destination** Server. All changes made on the **Source** Server are reflected on the **Destination** Server but changes made on the **Destination** Server are not reflected on the **Source** Server.

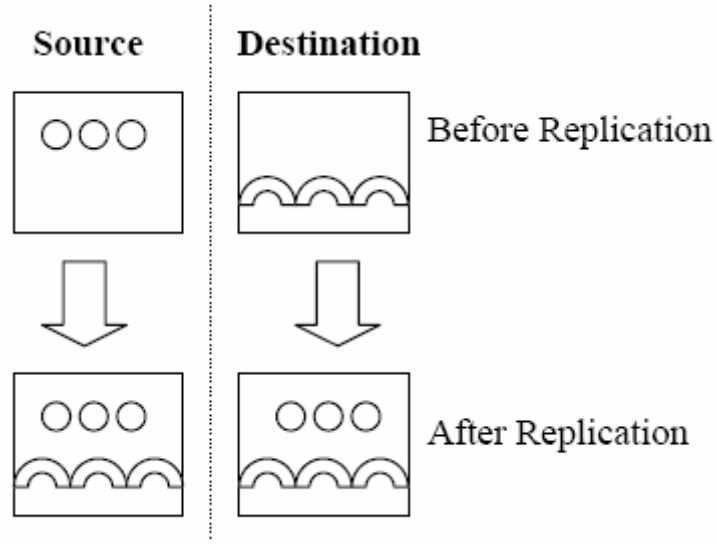
The end result is identical Servers, which ‘mirror’ the **Source** Server. No changes were made to the **Source** Server.

Example

A student lab would perform a nightly **One-way** replication from a default Server to all of its lab computers. The job would specify all of the directories to be replicated, and the replication type would be set to **One-way**. It would be scheduled to run nightly, after all the students were done for the day. This would ensure that all computers were identical, and in working order, for the morning classes.

Two-Way Mirror

The FRP Replication Type **Two-way Mirror** will copy the specified files or folders from the **Source** Server to the **Destination** Server. It deletes any files/folders/directories that do not exist on the **Source** Server, from the **Destination** Server and visa versa. The end result is identical content on each Server, which ‘mirrors’ each other.



Example

A businessperson would use a **Two-way** Replication Type to ensure his home and office computers reflect the exact same information. He would need to select the directories, folders, and files that he wanted to keep updated in both places. He then would need to set a repeating job that would run twice a day; once, after he completed work at home, and once when he completed the workday in the office.

Advanced

The advanced screen (See Figure 21) provides the user with the following additional features:

- Include/Exclude
- Replication initiator
- Bandwidth throttling
- File compression
- File encryption

The **Edit Job – Advanced** screen is opened by clicking the **Advanced** button from the **Edit Job – Basic** screen.

Clicking the **Schedule** button returns the user to the **Edit Job – Schedule** screen.
Clicking the **Basic** button returns the user to the **Edit Job – Basic** screen.
Clicking the **Finish** button saves all job changes and returns the user to the **Schedule Jobs** screen.
Clicking the **Cancel** button disregards all job changes and returns the user to the **Schedule Jobs** screen.

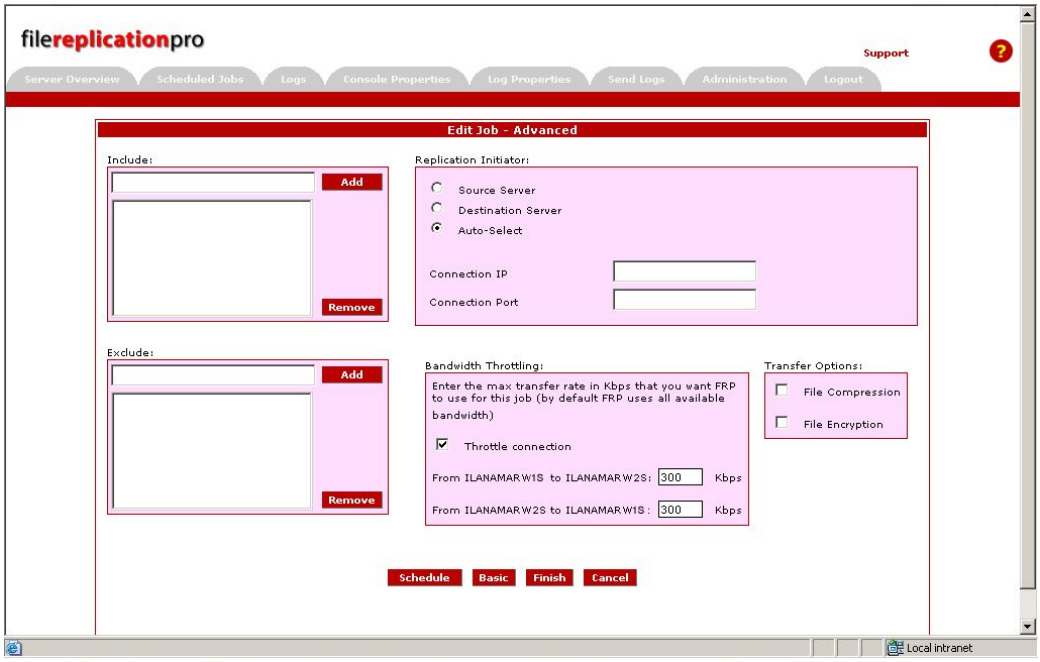


Figure 21 - Edit Job - Advanced screen

Exclude/Include

Exclusion/Inclusion Rules

Exclusion/Inclusion rules are used to specify files, folders, directories and even file types that are to be excluded or included from a replication. The Exclusion/Inclusion fields accept entries using either basic wild card patterns "*" or "?" or more sophisticated patterns using Regular Expressions (REGEX). The default pattern language is basic wild card patterns. To user REGEX, see Appendix B – Exclude/Include Filtering Options.

Exclusion

Exclusion rules allow the user to exclude specific files or directories from the replication source path. Users may enter one or more exclusion rules.

Inclusion

Inclusion rules allow a user to only include the files or directories from the replication source path. Users may enter one or more inclusion rules.

FRP provides the ability to filter data based on full or relative paths, folders, files or both or to use basic wild card patterns or Regular expressions.

The default settings are:
Relative path – filtering is applied relative to the source path
Filter All – filtering is applied against files and directories
Wild card expressions – Use basic wild card patterns

For examples on changing and using these options, see Appendix B – Exclude/Include Filtering Options.

Setting Exclusion/Inclusion Rules

To set rules:

1. Enter items to include or exclude using regular expressions or wildcards in their respective windows.
2. Click the **Add** Button to add the Item to the list.

To remove an Item from the exclude or include list:

1. Select the Item to be deleted.
2. Click the **Remove** Button.

Bandwidth Throttling

This option enables the user to limit the bandwidth available to FRP during replication. Normally FRP uses all the available bandwidth. There may be times where you require bandwidth for a different application; you therefore need to limit the bandwidth used by FRP. The numeric entries set the maximum bandwidth available to FRP in kilo-bits per second. Bandwidth throttling is set individual for each job. The default setting is no throttling, maximum bandwidth available.

To set Bandwidth Throttling:

1. Check the Throttle Connection checkbox.
2. Enter the limiting replication speed for each direction.

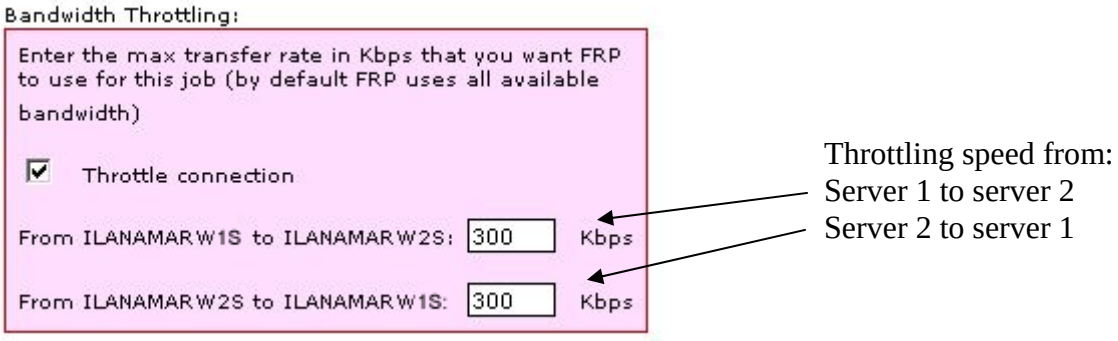


Figure 22 - Bandwidth throttling

Replication Initiator

Replication initiator determines which server initiates the replication job. The default setting is **Auto-Select**, which enables FRP to make the decision as to which Server initiates the replication.

The Replication Initiator would need to be specified when the Destination and Source Servers are not Fully-Accessible to each other. An example of this is when you have a server behind a router and it only has a local IP (not public) and you are interfacing the server with

a different server that has a public IP. You would set the server behind the router as the initiating server.

To set the Replication Initiator, select the appropriate radio button in the **Replication Initiator.**

File Compression

When this option is selected FRP compresses the files before replicating them. Enabling Compression reduces the required bandwidth to accomplish the replication. It will also increase the CPU utilization for the task. Enabling Compression may also increase the replication time. In a low bandwidth environment this setting can be used to decrease the bandwidth that FRP uses, although it would increase CPU usage. In a high bandwidth environment, file compression is not recommended. The default file compression setting is off.

Check the **File Compression** Checkbox in the **Transfer Options** Box to enable file compression.

File Encryption

When this option is selected FRP encrypts the files before replicating them. When this setting is selected, FRP uses AES encryption with Java 1.4.2 and above. With lower versions it uses Blowfish Encryption. This will increase the security level of the replication. It also may increase the Replication time, and increase the percentage of CPU utilized for the task. The default setting for **File Encryption** is off.

Check the **File Encryption** checkbox in the **Transfer Options** box to enable file encryption.

Schedule

The last step in defining a job is to assign a schedule to it.

From the **Edit Jobs – Basic** or **Advanced** screens, click the **Schedule** button to open the **Edit Job – Schedule** screen (Figure 23).

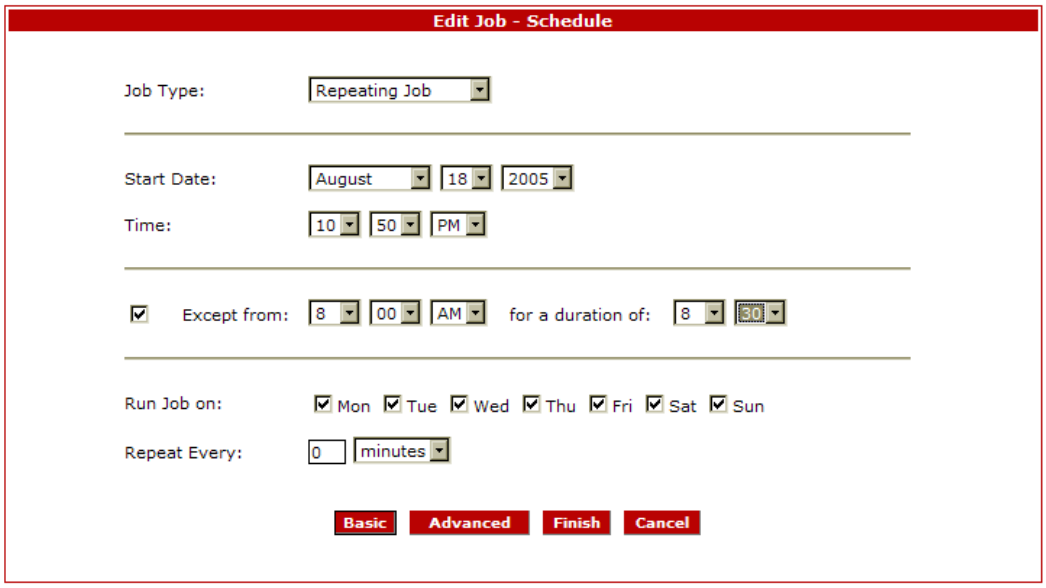


Figure 23 - Edit Job Schedule

Scheduling Job Properties

Job Type

There are three job types available:

- **Run Immediately –**The job is run immediately. When this job type is chosen, no other fields need to be filled in.
- **Run Once –**The job is scheduled to run once at a selected date and time. Only the **Start Date** and **Time** Section are available, and must be filled in.
- **Repeating Job** –The job is scheduled to recur at a specified interval from a selected start date. All other fields are available and may be filled in.

Start Date

This is the date on which the job will begin to run.

Time

This is the time of day at which the job will begin to run.

Except from

These fields can be used to specify time periods when the job will not run.

Run Job on

Use this section to select the days on which the job will be run.

Repeat Every

Use this section to set this is the interval of time that specifies how often the job is run. It can be specified in increments of hours or minutes.

A setting of 0 enables real-time mode. In this mode, the job sits in a wait condition. When a real-time event such as file change, file add, file delete, ACL change occurs, FRP will start replicating the changed file(s).

Delete Job

To delete a Job:

1. Click on the radio button beside a job to select a Job from the job List.
2. Click the **Delete** Button; the job is deleted and removed from the job list.

LOGS

FRP provides several log views which provide information about replications that have occurred and to view management console information.

A common method to view log records is to view the records for a specific job. Accessing log information for a specific replication job is accessed by clicking the job logs view button in the Scheduled Jobs screen (Figure 24).

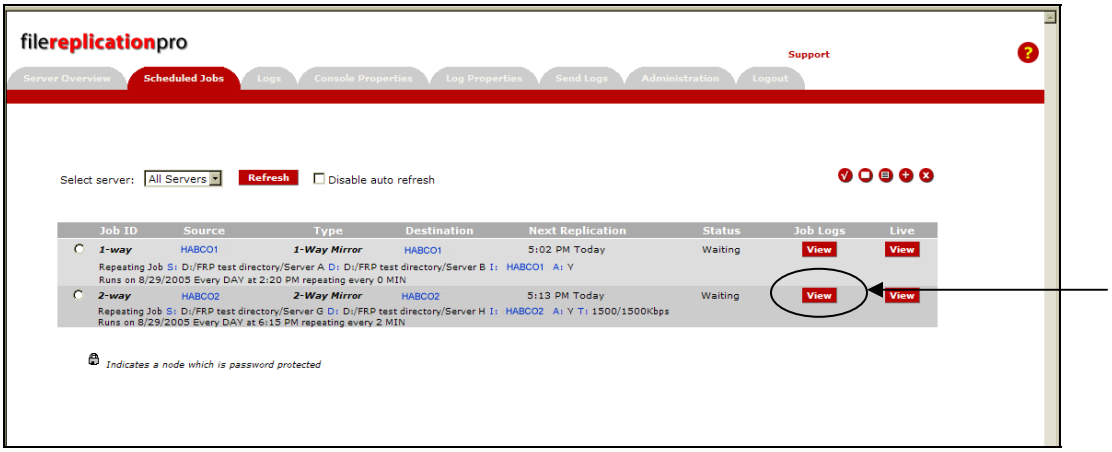


Figure 24 - Scheduled Jobs Screen

Clicking the job logs view button opens the Log screen and displays the log records for the specified job (Figure 25).

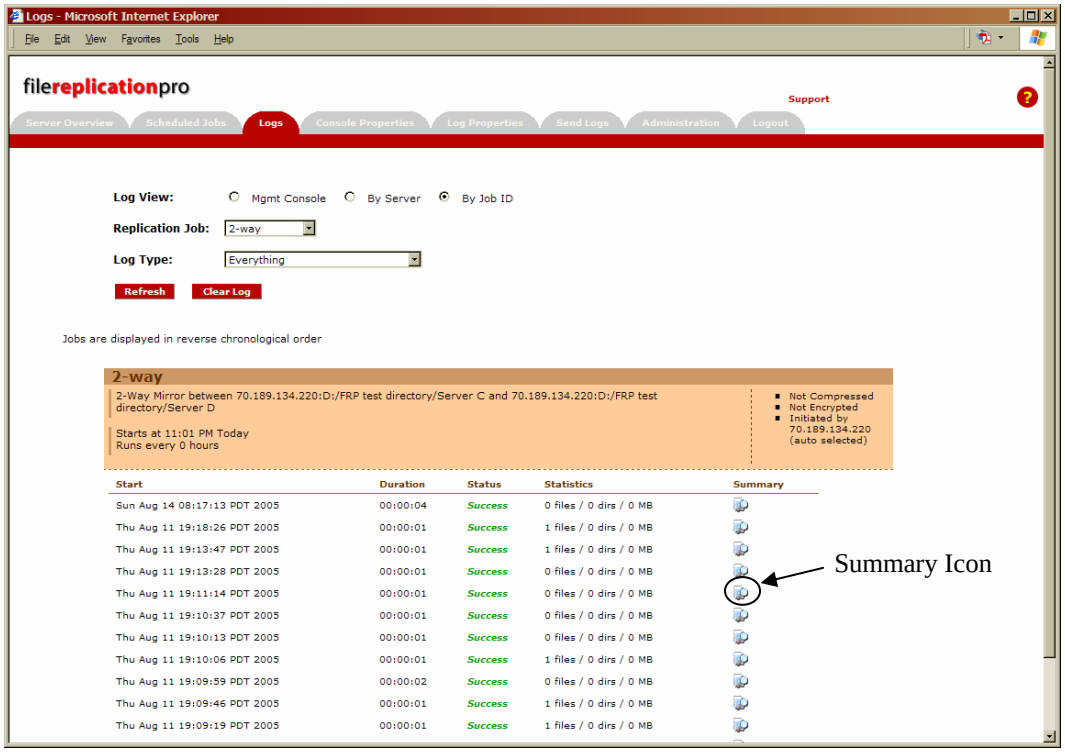


Figure 25 - Log Screen

The log screen displays general job information in the colored box area and one line for each replication performed for the specified job. Information shown includes the replication date and time, replication duration, status, replication statistics, and a summary icon link.

Values for the Status indicator are:

- Success – Replication took place correctly
- Errors – Some type of error(s) occurred. Click the summary icon for more information
- Warning – Replication occurred correctly, but some type of change event occurred during replication. Click the summary icon for more information.

The statistics column displays the number of files and folders that were replicated and the number of bytes transferred.

Click the summary icon link at the end of the replication record to open the summary screen (Figure 26) for the specific record.

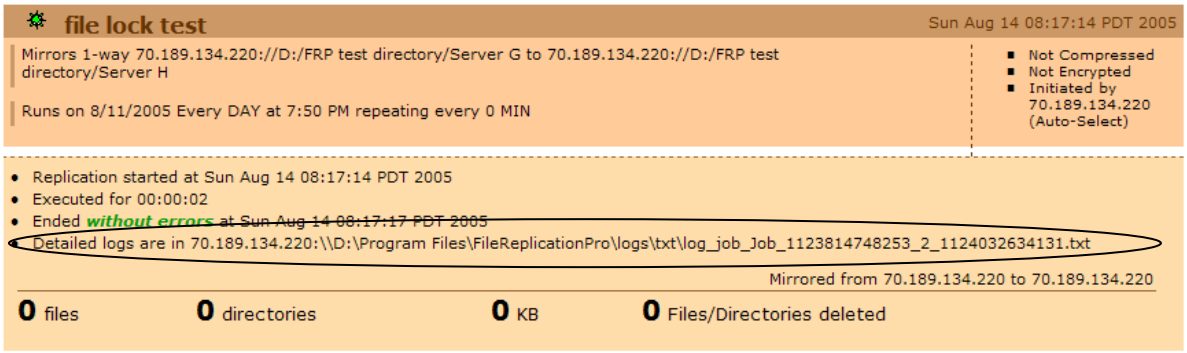
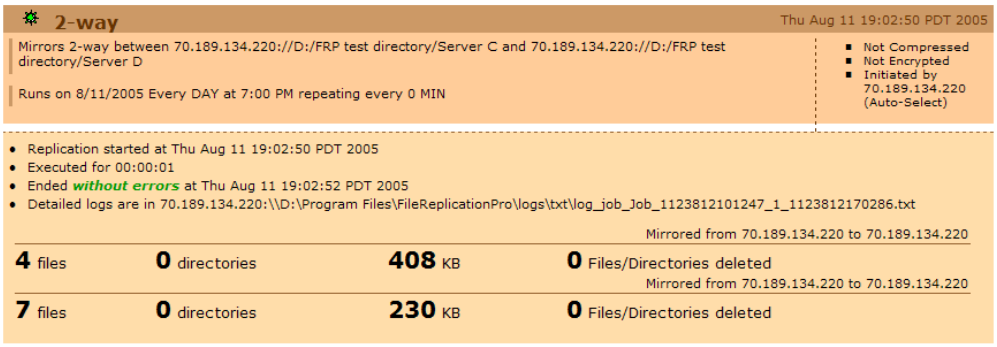


Figure 26 - Summary Screen

The summary screen presents general job information in the top section, replication start date and time, execution duration, end time and status, the path to the log summary text file and statistical information are displayed in the bottom section.

For users who want additional information about the replication record, the detailed logs text file path is presented in the summary screen. Users can open this file using any text editor to view all record details including FRP internal messages. The detailed logs text file provides the user with more specific information such as the names of all files/directories that were replicated, replication mode (real time or directory scan), exact timestamps, and error information if FRP encountered any errors during replication.

If the job is a 2-way replication, the summary screen (Figure 27) adds one extra line which shows the transfer information from the destination server to the source server.



Source -> Destination

Destination -> Source

Figure 27 - Summary Screen 2-Way replication

Log view can also be entered by clicking the Logs tab from the main FRP screen. Clicking the Logs tab enters log view with the Console Manager Radio button selected.

Regardless of the method used to access the logs screen, the user can change how logs are displayed by selecting different options (Figure 28).

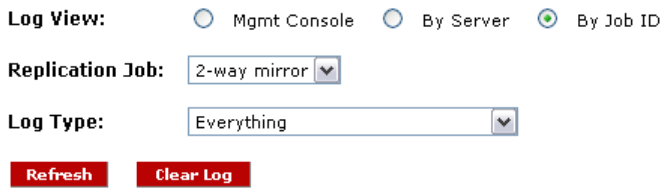


Figure 28 - Log screen Options

- Click the By Server radio button and select a server from the drop down list to display a list of replication records grouped by jobs for a specific server.
- Click the By Job ID radio button and select a replication job from the drop down list to display a list of replication records for the selected job (or all jobs).
- Select what log records to display from the Log Type drop down list. Options are:
  - Everything – All data in the associated log file is displayed.
  - Error – Display log information filter by errors only.
  - Error + Warning - Display log information filter by errors and warnings only.
  - Error + Warning + Informational
- Click the Refresh button to update the record list with the most current replications.
- Click the Clear Log button to clear all the currently displayed record logs from the system.

Verbose Mode

When Log View by server is selected, an optional checkbox named Verbose is displayed. Click this checkbox to display a verbose list of messages related to the selected server (Figure 29).

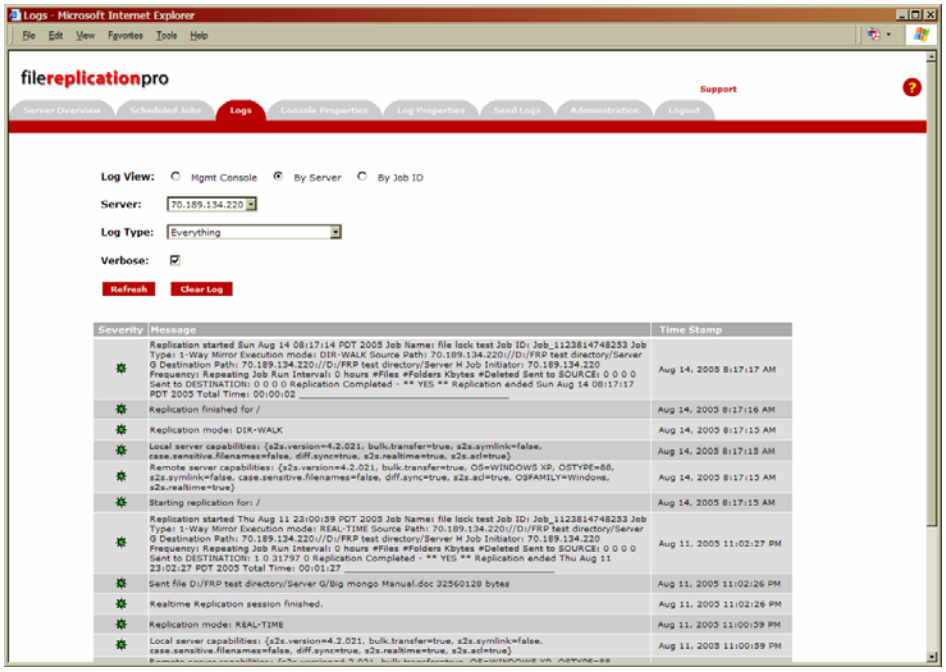


Figure 29 - Job log Verbose mode

The verbose display shows more information including a severity icon and detailed messages with time stamping.

CONSOLE PROPERTIES

Overview

The console properties screen enables the user to setup email alerts from the console. The purpose of the email is to alert the user when a specific replication condition occurs. Alerts are sent based on the alert level setting. The user can choose whether to send an alert when a job fails to run, when it runs but with errors or when the job runs successfully.

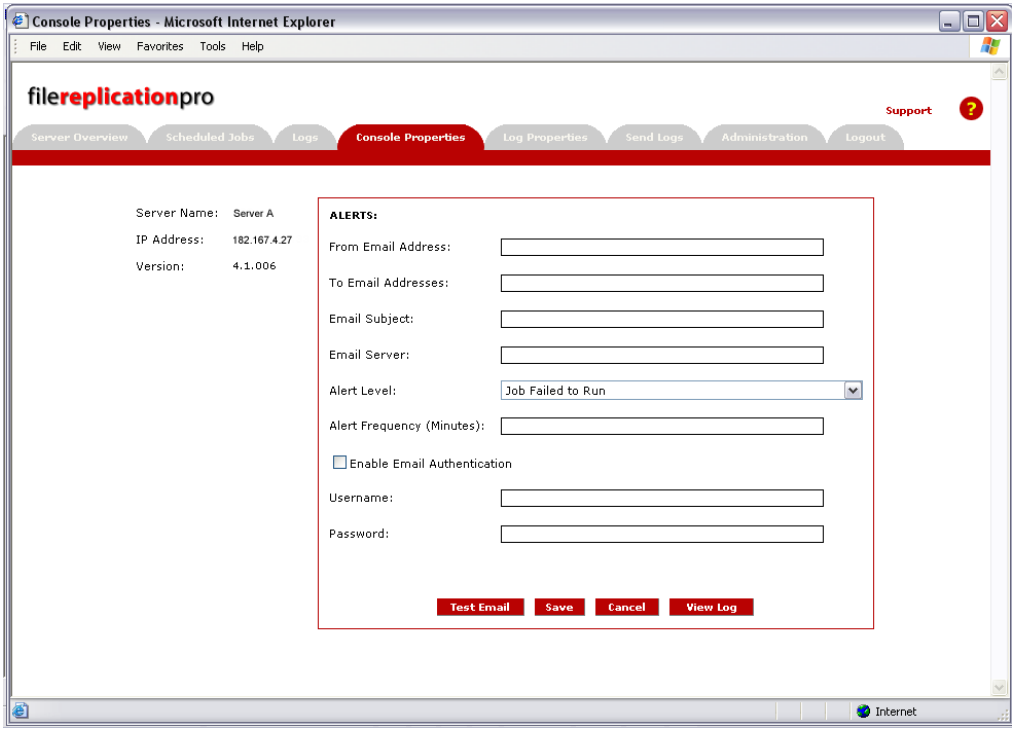


Figure 30 - Console Properties

Server Name
The name of the management server that the email alerts will be sent about.

IP Address
The IP address of the management server.

Version
The version of FRP running on the management server.

From Email Address
This field is used to set the email Address that will appear in the “From” field of the Alert email. howard@diasoft.net

To Email Addresses
This field is used to set the email addresses to which the Alert email will be sent.

Email Subject
This field is used to set the subject that will appear in the “Subject” field of the email.

Email Server
This field is used to set the email server from which the email will be sent. The email server field may be an address described either as a hostname (e.g. mail.diasoft.net or IP - 192.200.197.8) of the SMTP server

Alert Level
This field is used to set which emails will be sent out as alerts, based on Alert Level. There are three Alert Levels:

- **Job Failed to Run:** Email is sent only if a job fails.

- **Job Failed to Run + with Errors:** Email is sent if a job fails or if errors occurred while running a job.
- **Job Failed to Run + with Errors + Job Successful:** Email is sent if a job fails or if errors occurred while running a job and for each successful job.

Alert Frequency (minutes)

This field is used to set the send email time interval in minutes. Any emails generated within this time interval will be consolidated into one email and sent at the end of the interval period..

Note: The fields must be filled in before sending a test email, or leaving the screen, otherwise the fields will be cleared.

Email authentication

Use these fields if your email requires SMTP Authentication.
Check the Enable Email Authentication checkbox and enter a username and password to utilize this feature.

Sending a Test Email

To send a Test Email:

1. Click on the **Test Email** Button on; a test email is sent with the following message:
   `This is a test email sent from the FRP configuration management console. It confirms that the email settings you configured in FRP are correct.`

Save

Click the save button after entering the field information to save the configuration.

LOG PROPERTIES

This function allows the user configure the log file setting for each server.

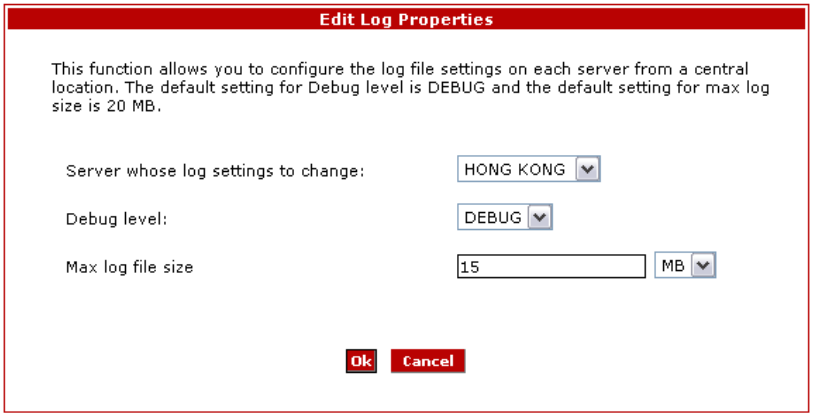


Figure 31 - Edit Log Properties

1. Select a specific server or all servers from the Server drop down list.
2. Select a debug level of:
   - WARN
   - INFO
   - DEBUG
3. Enter a maximum log size either in MB or KB.
4. Click **OK** to save your settings or **Cancel** to ignore any changes.

Default settings are:

- Debug level = DEBUG
- Max log size = 20MB

SEND LOGS

This function allows the user to send log files to FileReplicationPro support, with questions and comments. This allows the support team to analyze the user's log files and provide a solution.

1. Select a specific server or all servers whose logs you wish to send
2. Enter your email address
3. Write out your questions or comments to help the support department analyze your situation.
4. Click **OK** to send the log files.

ADMINISTRATION

Clicking this tab allows the user to change the management console's password.

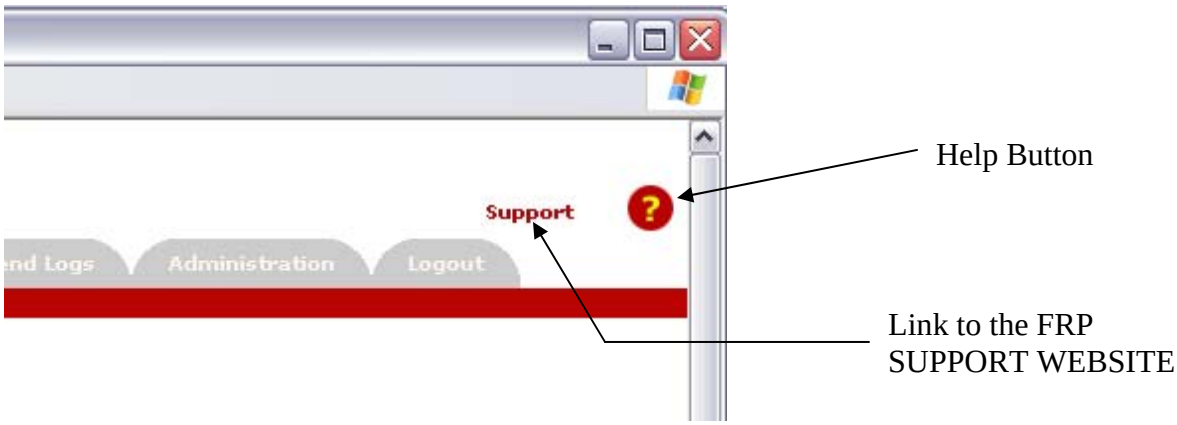
LOGOUT

Clicking this tab, logs the user out from the management console. All active jobs will continue to run in the background.

HELP

Help is available for all console screen tabs by clicking the questions mark.

Additional information, numerous Knowledge Base articles, and this manual may be found at the FRP website. Click the support link to go directly to the FRP SUPPORT WEBSITE.



Appendix A – Licensing

Managing Licenses

- Licenses are sent via email upon purchase.
- You need to purchase one license per server.
- Licenses are not node locked and may be used on any server; one server at a time.
- Licenses are not transferable.

Appendix B – Exclude/Include Filtering Options

S2s.properties Fullpath

Setting this value to true enables the include/exclude advanced features to specify filters using a full path definition. False enables the include/exclude advanced features to specify filters relative to the specified source directory.

S2s.properties Filetype

The s2s.filter.filetype can accept the following three values:

- FILTER_ALL - allows filtering to apply to both directories and files
- FILTER_FILE - allows filtering to apply files only
- FILTER_DIR allows filtering to apply to directories only

Example:

S2s.properties conditions		
Filetype=FILTER_FILE	Fullpath=false	Regex=false

A source directory contains
2000 files of which 150 are text files and you want to replicate all the files except the 150 text files. In the exclude window, add an exclude expression of *.txt. The replication would replicate all the files except the 150 text files.

Example:

S2s.properties conditions		
Filetype=FILTER_DIR	Fullpath=false	Regex=false

A source directory contains
50 files plus 35 directories. Some of the directory names contain the text “Financial” followed by a month (i.e. Financial_01, Financial_02) other directory names are a mix of

different text. You want to replicate all the data except for the financial information. In the exclude window, add an exclude pattern of Financial*.

Example:

S2s.properties conditions		
Filetype=FILTER_ALL	Fullpath=false	Regex=false

A source directory contains a mixture of file and directories. Some of the directory names contains the text “A Testdata_010205”, “B Testdata_040604” etc. Some of the files names also contain the text “Testdata”. You want to replicate all the data in all the directories except for the Testdata directories and any files that have names containing “Testdata”. In the exclude window, add an exclude pattern of *Testdata* (Note that filtertype=FILTER_ALL).

Example:

S2s.properties conditions		
Filetype=FILTER_FILE	Fullpath-false	Regex=false

A source directory contains 1,000 files of which 56 files are text files and you only want to replicate the 56 text files. In the include window, add an include expression of *.txt. The replication would only replicate the 56 text files to the destination.

Example:

S2s.properties conditions		
Filetype=FILTER_FILE	Fullpath-false	Regex=true

A source directory contains files, which some are special operations files named op1cyt.doc, op22cyt.doc, op666cyt.doc. There are also some files named op22cyt.lib, op22cyt.lib etc. You only want to replicate the opXXXcyt.doc files. In the include window, add an include expression of op.+\.doc. The replication would only replicate the selected doc files to the destination.

Appendix C – Optional Installer Modes

Replication from a Command Line

There may be times when a user wants to start a replication session from an external scheduler or from a text based window. FRP provides a command line utility named FrpShell which allows users to launch FRP replication jobs using an external scheduling system (e.g. UNIX crontab).

In order to use FrpShell to launch a job without using FRP Management UI, you first must have the job’s unique ID and an additional FRP identification called connection ID. By default the command is setup to be used on the machine hosting the FRP Management Server. You can also setup the command to run from a remote system that has no FRP installation.

Setup:

The command FrpShell can be found at <FRP home directory>\utils.

To use the FrpShell from a machine that has no FRP installation (but has a Java runtime), copy to that machine the folder <frp home>\utils. Also create the folder <frp home>\lib and copy the file diasoft_utils.jar to this folder.

You may need to edit file frpshell.sh (UNIX) or frpshell.bat (Windows) to setup the correct IP or FRP Management Server and FRP Admin password.

Usage:

$ frpshell COMMAND ARGUMENT 1 .. ARGUMENT n

Currently the only command supported by frpshell is runJobNow.

To start a job now, use the following command:

$ frpshell runJobNow <CONNECTION_ID parameter> <JOB_ID parameter>

This sends a message for the FRP management server to run a job identified by CONNECTION_ID and JOB_ID.

Most probably you know your job by name and not by Ids. The easiest way to find the CONNECTION_ID and JOB_ID associated with a specific job is to:
Open FRP configuration file <FRP-HOME>/etc/configuration.xml
Search for the job name.
CONNECTION_ID and JOB_ID should be listed prior to <JobName> element.

Usage Example:

$ ./frpshell.sh runJobNow Connection_1101118401337 Job_1101118333648

In order to run this job from an external scheduling system, you will need to configure the scheduling system to activate this shell command in this manner.

Appendix D – System Properties

S2s.properties File

The S2S.properties file is a text file used to setup certain default parameters and other configuration information for FRP operation. This file is located at <frp home>\lib.

Group	Property	Description
2-Way Mirror	s2s.2way.max_sys_time_diff	Max time difference between servers to allow a 2-way mirror
2-Way Mirror	s2s.2way.enable_deletes	Enable/disable 2-way mirror deletions

2-Way Mirror	s2s.2way.exclude	File list to exempt from 2-way mirror delete prohibition
2-Way Mirror	s2s.2way.enforce_sys_time_sync	Enable/disable 2-way mirror time sync check
File	s2s.log.days	Duration to maintain log files
File	s2s.jetty.home	Jetty web server home directory
File	s2s.data.dir	Data directory location
File	s2s.dir	FRP working directory
File	s2s.log.size	Default log file size
File	s2s.log.dir	Log files directory
File	s2s.send.log.url	URL location when sending log files
General	s2s.dsync.threshold	Minimum file size for differential synchronization
General	s2s.dsync.max	Maximum file size for differential synchronization
General	s2s.crypto	Encryption algorithm type
General	s2s.symlink	Symbolic link copy enable flag
General	s2s.acl	ACL replication enable flag
Include/Exclude	s2s.filter.filetype	Include/Exclude filter selector
Include/Exclude	s2s.filter.fullpath	Include/exclude fullpath enable flag
Include/Exclude	s2s.filter.regex	Include/exclude regular expressions enable flag
Internal	s2s.realtime.events_read_ interval	Internal FRP use only
Internal	s2s.pipeline.url	Internal FRP use only.
Real-time	s2s.realtime.dir_walk_interval	Interval between full directory scans
Real-time	s2s.realtime	Real-time enable flag
Real-time	s2s.realtime.acl	ACL real-time replication trigger enable flag
Real-time	s2s.realtime.max_job_interval	Max real-time job repeating interval
Real-time	s2s.realtime.dir_walk_interval	Interval time between safety directory scan replications
Real-time	s2s.realtime.events_buffer_ size	Real-time events buffer size
Real-time	s2s.realtime.network_drives_ events_buffer_size	Real-time events buffer size for Windows network/shares drives
Real-time	s2s.realtime.events_threshold	Real-time events threshold
Real-time	s2s.realtime.trace_events	Enables additional logging of real-time event triggers
Real-time	s2s.realtime.event_write_interval	Write delay for real-time events to the database (obsolete).
Real-time	s2s.realtime.silent_before_trigger	Silent period (no real-time events) required before replication starts.
Real-time	s2s.realtime.max_trigger_delay	Max time to wait for silent period.

Real-time	s2s.realtime.max_events_per_ replication	The batch size for reading from the events database.
TCP	s2s.tcp.exclude_ips	List of excluded IP addresses
TCP	s2s.buffer.size	Buffer size TCP communication.
TCP	s2s.tcp.response_timeout	TCP protocol socket connection timeout.
TCP	s2s.tcp.connect_timeout	Max time to establish a connection with a peer server.
TCP	s2s.tcp.session_inactivity_timeout	Timeout for closing an inactive replication session.

Group : 2-Way Mirror

s2s.2way.enable_deletes

Function
Enable or disable deletions to take place during a 2-way mirror.

Default
s2s.2way.enable_deletes=false

s2s.2way.exclude

Function
This parameter lists files (wildcards allowed) that the user wants to exempt from the delete prohibition. This list should contain the names or types of temporary files created by user applications that the user want to be deleted during a 2-way replication even if 2-way mirror deletes are not allowed.

Default
s2s.2way.exclude=*.tmp,~$*.doc

s2s.2way.enforce_sys_time_sync

Function
Enable or disable system time differential check during a 2-way mirror. When set to true, FRP will check that the system times between the source and destination servers are within the time specified by the s2s.2way.max_sys_time_diff parameter. If the system times are within the limits, the 2-way replication will take place.

Default
s2s.2way.enforce_sys_time_sync=true

s2s.2way.max_sys_time_diff

Function
This parameter sets the maximum allowable differential time between the source and destination server system clocks for 2-way replication to take place. If the system time differential exceeds this parameter, 2-way replication will not take place. s2s.2way.enforce_sys_time_sync must be set to true to enable this function. The value is set in seconds.

Default
s2s.2way.max_sys_time_diff =10000

Group : File

s2s.log.days

Function
The number of days FRP keeps the log files in the <frp-home>\logs\txt directory.

Default
s2s.log.days=10

s2s.jetty.home

Function
Home directory for Jetty web server used to host the FRP console web application.

Default
s2s.jetty.home= .

s2s.data.dir

Function
Data directory location relative to the FRP installation directory.

Default
s2s.data.dir=./data

s2s.dir

Function
FRP working directory location relative to the FRP installation directory.

Default
s2s.dir=.

s2s.log.size

Function
This parameter defines the maximum file size for the replication execution logs.

Default
s2s.log.size=300KB

s2s.log.dir

Function
Log files directory location relative to the FRP installation directory.

Default
s2s.log.dir=./logs

s2s.send.log.url

Function
This parameter defines the Web location URL to where FRP sends the log files when the user initiates the send log feature.

Default

s2s.send.log.url=http\://filereplicationpro.com/ LogService/LogService

Group : General

s2s.dsync.threshold

Function
This parameter sets the minimum file size for differential synchronization to take place.

Default
s2s.dsync.threshold=10000000

s2s.dsync.max

Function
This parameter sets the maximum file size for differential synchronization to take place.

Default
s2s.dsync.max=10000000000

s2s.crypto

Function
This parameter is the encryption algorithm used by FRP to encrypt control data between servers and also to encrypt file data if encryption was selected for the job. Possible encryption values supported by Java version 1.4 are:

- DES
- DESede
- AES (with Java 2 SDK, v 1.4.2)
- Blowfish
- PBEWithMD5AndDES
- PBEWithMD5AndTripleDES
- Diffie-Hellman key agreement among multiple parties
- HmacMD5
- HmacSHA1

Default
s2s.crypto=Blowfish

s2s.symlink

Function
Used for UNIX/Linux to enable replicating symbolic links.
Value of true enables the replication of symbolic links.
Value of false replicates the file referenced by the link.

Default
s2s.symlink=true

s2s.acl

Function
Enable/Disable replication of file security information (Windows ACL or file ownership/permission bits in Unix/Linux). True enables ACLs to be replicated. False – ACLs

will not be replicated with the file or directory which means the replicated file will keep the values assigned by the destination operating system.

Default
s2s.acl=true

Group : Include/Exclude

s2s.filter.filetype

Function
Specifies how the include/exclude parameters in the advanced job features are applied. The include/exclude parameters can be applied to files only, directories only or to both.
Value of FILTER_ALL filters the include/exclude parameters against files and directories.
Value of FILTER_FILE filters the include/exclude parameters against files only.
Value of FILTER_DIR filters the include/exclude parameters against directories only.

Default
s2s.filter.filetype=FILTER_ALL

s2s.filter.fullpath

Function
This parameter enables or disables using a full path for include/exclude filtering.
Value of true enables the include/exclude features to specify filters using a full path definition.
Value of false enables the include/exclude features to specify filters based on the specified source directory.

Default
s2s.filter.fullpath=false

s2s.filter.regex

Function
This parameter enables or disables the use of regular expressions filtering in the include/exclude values.
Value of true enables using regular expressions to specify include or exclude values.
Value of false disables the use of regular expressions and enables using Windows wildcard filtering in the include/exclude values.

Default
s2s.filter.regex=false

Group : Internal

s2s.realtime.events_read_ interval

Function
Internal FRP use only (version 4.2 and higher)

Default
s2s.realtime.events_read_interval=0

s2s.pipeline.url

Function
Internal FRP use only.

Default
s2s.pipeline.url=http\://{0}/s2s/config

Group : Real-time

s2s.realtime

Function
This parameter enables or disables using real-time replication.
Value of true enables real-time replications to be performed. Real-time events such as adding, deleting, changing, or renaming a file will trigger an immediate replication.
Value of false disables real-time event triggering. When disabled, FRP works on directory scanning and comparisons.

Default
s2s.realtime=true

s2s.realtime.acl

Function
This parameter enables a change in the ACL (Windows) or permissions (UNIX/Linux) to trigger a replication.
Value of true enables ACL changes to trigger a real-time replication.
Value of false disables ACL changes from triggering a real-time replication.

Default
s2s.realtime.acl=true

s2s.realtime.max_job_interval

Function
If a job repeating interval is set higher than this value, replication will be based on directory scans only even if real-time is enabled. The value is set in minutes.

Default
s2s.realtime.max_job_interval=120

s2s.realtime.dir_walk_interval

Function
This is the interval time in which FRP will perform a safety directory scanning replication. Even though real-time is enabled, a directory scan will be performed based on the interval setting. The value is set in minutes.

Default
s2s.realtime.dir_walk_interval=1440 (1440 minutes=24 hours)

s2s.realtime.events_buffer_ size

Function
This is a buffer size used to collect real-time file system changes from the operating system. This number may be increased if the replication base is characterized by many changes during short time intervals. The value is in Kb.

Default
s2s.realtime.events_buffer_size=1024

s2s.realtime.network_drives_ events_buffer_size

Function
This parameters is the same as the s2s.realtime.events_buffer_size but is specific to Windows network/shares drives. The value is in Kb.

Default
s2s.realtime.network_drives_events_buffer_size=64

s2s.realtime.events_threshold

Function
If the operating system reports a number of real-time events that exceed this threshold, FRP will switch to directory scan replication instead of real-time replication. This prevents the condition where the O/S could overload the available memory due to an excessively large number of real-time events.

Default
s2s.realtime.events_threshold=5000

s2s.realtime.trace_events

Function
Controls logging additional trace logs for the FRP real-time module.
When set to true, FRP logs each file system change event as notified by the operating system and each event read from the events database. When set to false, additional logging is not performed.

Default
s2s.realtime.trace_events=true

s2s.realtime.event_write_interval

Function
Permits a time delay before writing real-time events to the database. This parameter is obsolete.

Default
s2s.realtime.event_write_interval=0

s2s.realtime.silent_before_trigger

Function
This parameter is used to hold off file replication (real-time) while there are constant changes to the source. FRP will not start replicating files until the silent period (no more real-time changes to the source folder for the specified time) has been reached. This minimizes multiple replication sessions and its associated performance degradation. In the case where a silent period is not reached, the parameter s2s.realtime.max_trigger_delay (see below) takes over. The value is in milli-seconds.

Default
s2s.realtime.silent_before_trigger=1500

s2s.realtime.max_trigger_delay

Function
This parameter is the maximum time to wait for a silent period (see above) when constant changes are made to the source in real-time mode. Replication will take place after this delay has been reached. The value is in milli-seconds.

Default
s2s.realtime.max_trigger_delay=15000

s2s.realtime.max_events_per_replication

Function
This parameter defines the batch size when reading from the events database. The set value prevents a potential OutOfMemory exception in situations where a large number of events are waiting to be read from the events database.

Default
s2s.realtime.max_events_per_replication=10000

Group : TCP

s2s.tcp.exclude_ips

Function
(v4.2 and higher) This is an optional comma separated list of IP addresses for FRP to ignore during server auto-detect. This is useful for customers that have many virtual IPs and want FRP to ignore them. Values may be listed by IP or by host name.

Default
s2s.tcp.exclude_ips=

s2s.buffer.size

Function
This parameter is the default buffer size used by FRP for server to server TCP communication. The value is in Kb.

Default
s2s.buffer.size=64000

s2s.tcp.response_timeout

Function
The maximum waiting time for a response from a peer server. May need to be increased if communication is over a slow WAN. The value is in seconds.

Default
s2s.tcp.response_timeout=30

s2s.tcp.connect_timeout

Function
The maximum waiting time to establish a tcp connection with a peer. May need to be increased if communication is over a slow WAN. The value is in seconds.

Default
s2s.tcp.connect_timeout=15

s2s.tcp.session_inactivity_timeout

Function

Time before closing an inactive replication session. There may be cases where an initiator is disconnected from the network during a replication session. This parameter allows the receiving side to close the tcp session with the initiator. The value is in seconds.

Default

s2s.tcp.session_inactivity_timeout=300