

# **Integration Objects'**

## **Solution for Secure File Transfer**

**File Tunneller**  
Version 1.1. Rev0

**USER GUIDE**

Integration Objects' File Tunneller User Guide Version 1.1 Rev.0  
Published September 2016

Copyright © 2014-2016 Integration Objects. All rights reserved.

No part of this document may be reproduced, stored in a retrieval system, translated, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Integration Objects.

Windows®, Windows NT® and .NET are registered trademarks of Microsoft Corporation.

# TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>9</b>
<b>1. Overview .....</b>	<b>9</b>
<b>2. Features .....</b>	<b>10</b>
<b>3. System Requirements.....</b>	<b>10</b>
<b>GETTING STARTED.....</b>	<b>11</b>
<b>1. Pre-Installation Considerations .....</b>	<b>11</b>
<b>2. Installing And Running .....</b>	<b>11</b>
<b>3. Start-up .....</b>	<b>17</b>
<b>4. Log Files .....</b>	<b>17</b>
<b>5. Removing the File Tunneller .....</b>	<b>17</b>
<b>USING FILE TUNNELLER.....</b>	<b>19</b>
<b>1. Main Interface Overview .....</b>	<b>19</b>
1.1. Manage file transfers.....	20
1.2. Manage Connections .....	20
1.3. Monitor Transfers .....	21
<b>2. Managing administrator account .....</b>	<b>21</b>
2.1. Login Into File Tunneller.....	21
2.2. Edit Administrator Credential .....	22
<b>3. File Tunneller Functionalities.....</b>	<b>23</b>
3.1. Add Shared Folders .....	23
3.2. Configure Server Settings .....	27
3.2.1. Communication Parameters .....	27
3.2.2. Security Settings .....	29
3.2.3. User Management.....	31
3.2.4. Display.....	34
3.2.5. Log Settings .....	35

3.3. Configure Connections.....	35
3.4. Connection Properties.....	37
3.5. Transfer Operations .....	38
3.5.1. Upload File .....	38
3.5.2. Download File .....	40
3.5.3. Bridge File Transfer.....	42
3.5.4. Schedule File Transfer .....	43
3.6. Transfer Properties .....	45
<b>4. Step by Step Procedure to Use File Tunneller.....</b>	<b>47</b>
<b>5. License Authorization .....</b>	<b>53</b>

## TABLE OF FIGURES

Figure 1: File Tunneller Architecture.....	9
Figure 2: Installation Welcome Dialog .....	12
Figure 3: License Agreement Dialog.....	13
Figure 4: Customer Information Dialog .....	14
Figure 5: Choose Destination Folder Dialog .....	15
Figure 6: Installation Dialog .....	16
Figure 7: File Tunneller Start Menu .....	17
Figure 8: Uninstall the File Tunneller .....	18
Figure 9: File Tunneller Main View .....	19
Figure 10: Home menu.....	20
Figure 11: Connections Context Menu .....	20
Figure 12: Available Connections .....	21
Figure 13: Server Context Menu.....	21
Figure 14: Current File Transfers.....	21
Figure 15: Enter Admin Credential .....	22
Figure 16: Edit Admin Credential.....	22
Figure 17: Shared Folders.....	23
Figure 18: Add shared folder .....	24
Figure 19: Edit Shared Folder.....	24
Figure 20: Manage folder .....	25
Figure 21: Add extension.....	25
Figure 22: File Filter .....	26
Figure 23: Set users' permissions.....	26
Figure 24: Configure Server Security Mode.....	29
Figure 25: Add Trust.....	30
Figure 26: Configure a Trust.....	30
Figure 27: Trusted Accounts Configuration.....	31
Figure 28: Add User .....	32
Figure 29: Set User's Password .....	32
Figure 30: Add Application Authentication .....	33
Figure 31: Change Password .....	33
Figure 32: Set a New Password .....	34
Figure 33: Change display settings.....	34
Figure 34: Configure log settings.....	35
Figure 35: Add connection.....	36
Figure 36: Add connection with authentication .....	36
Figure 37: Remove connections .....	37
Figure 38: Connection properties .....	37
Figure 39: Server properties.....	38
Figure 40: Current transfer menu .....	38
Figure 41: Set destination folder.....	39

Figure 42: Add file or folder .....	39
Figure 43: Upload files.....	40
Figure 44: Browse remote machine's files .....	41
Figure 45: Download file.....	42
Figure 46: Add new bridge .....	43
Figure 47: Select destination folder .....	43
Figure 48: Add new schedule send .....	44
Figure 49: Configured scheduled transfers .....	45
Figure 50: Scheduled transfer options .....	45
Figure 51: Scheduled transfer general options .....	45
Figure 52: Current transfer .....	46
Figure 53: Open containing folder .....	46
Figure 54: Main interface.....	47
Figure 55: Server settings .....	48
Figure 56: Set security mode.....	49
Figure 57: Configure shared folders .....	49
Figure 58: User's access rights .....	50
Figure 59: Manage filters.....	50
Figure 60: Add new connection .....	51
Figure 61: Connections tree view .....	51
Figure 62: Choose the destination folder .....	52
Figure 63: Upload your files.....	52
Figure 64: License authorization tool.....	53
Figure 65: Registration dialog.....	54
Figure 66: Valid license .....	54

## TABLE OF TABLES

Table 1: Communication Settings.....	28
--------------------------------------	----

# PREFACE

## ABOUT THIS USER GUIDE


This guide:

- Portrays the need for Integration Objects' File Tunneller, describes its main offered features, and lists the system requirements for installing and running File Tunneller.
- Explains how to install and run File Tunneller components following a typical configuration.
- Explains how to use, configure, and run File Tunneller for different scenarios.
- And recapitulates the main steps and instructions to follow in order to successfully configure and run the File Tunneller application.

## TARGET AUDIENCE

This document is intended for Integration Objects' File Tunneller users who need to securely transfer files between networks and domains.

## DOCUMENT CONVENTIONS

Convention	Description
<b>Bold</b>	Click/selection action required
Monospaced type	Indicates a file reference
	Information to be noted

## CUSTOMER SUPPORT SERVICES

Phone	Email
<b>Americas:</b> +1 713 609 9208  <b>Europe-Africa-Middle East</b> +216 71 195 360	Support: <a href="mailto:customerservice@integrationobjects.com">customerservice@integrationobjects.com</a>  Sales: <a href="mailto:sales@integrationobjects.com">sales@integrationobjects.com</a>  Online: <a href="http://www.integrationobjects.com">www.integrationobjects.com</a>



# INTRODUCTION

## 1. Overview

Several products available today on the market offer file transfer features between machines, but most of these software do not encrypt their communications on the network and therefore are not secure. Using a non-secure transfer makes your network vulnerable for multiple attacks during the transfer of data, such as:

- Bounce attacks
- Spoof attacks
- Brute force attacks
- Packet sniffing
- User name protection
- Port sealing

File Tunneller is an Integration Objects' solution providing you with a secure method to exchange files over TCP-based network.

File Tunneller is firewall friendly software that ensures fast, reliable, and secure remote communication to transfer files between different domains, through both LAN and WAN networks.

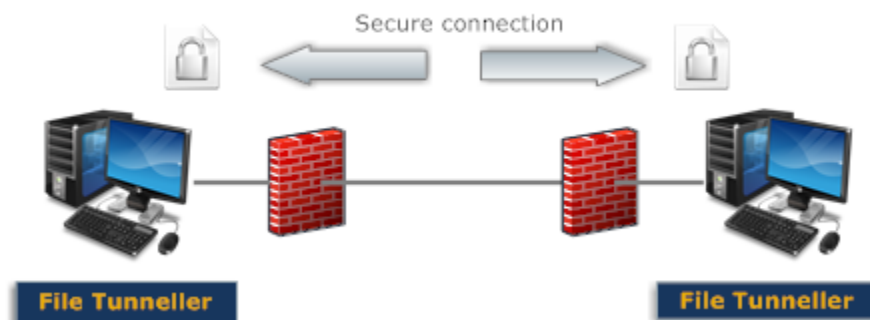


Figure 1: File Tunneller Architecture

Integration Objects' File Tunneller should be installed on both machines involved in the files transfer. Each machine acts as both server and client and securely communicates with the remote machine through TCP.

The machine will act as a server when it shares folders and files to be downloaded/uploaded. Any other machine that connects to the server and access the shared folders will act as a client.

## 2. Features

Integration Objects' File Tunneller features include:

- Easy-to-use user interface: A simple and interactive graphical interface is made available for the end users allowing them to quickly create and manage their file transfers.
- Multiple connections and transfers: The user can add multiple connections to different remote machines where the File Tunneller is installed and set up simultaneous uploads and downloads.
- User authentication: To avoid unauthorized access, the file transfers are protected with user authentication feature. The user can also configure the application to either use application based authentication or integrate with an existing active directory.
- Secure remote communications: Track and encrypt client/server communications and so ensuring data integrity and enhancing the security of the systems in order to protect assets, critical applications and the information confidentiality of the network.
- Limiting the number of open ports within your firewalls to a single TCP port to minimize security holes.
- Uploading and downloading any file's format or size: File Tunneller does not present limitations on the transferred file format or size.
- Robustness against network disruptions (automatic reconnection): File Tunneller automatically reconnects file transfer operations after a broken network connection and resume the transfer.
- User profiles management: File Tunneller allows the application administrator to set up different access rights to access the shared folders
- Scheduling files transfer operations: The user can schedule transfers of any file or folder to run automatically at the specified time and per the specified configuration.

## 3. System Requirements

File Tunneller was successfully installed and executed under the following operating systems:

- Windows 2003 SP2
- Windows XP SP3
- Windows Server 2008
- Windows 7
- Windows 8
- Windows Server 2012
- Windows 10

# GETTING STARTED

## 1. Pre-Installation Considerations

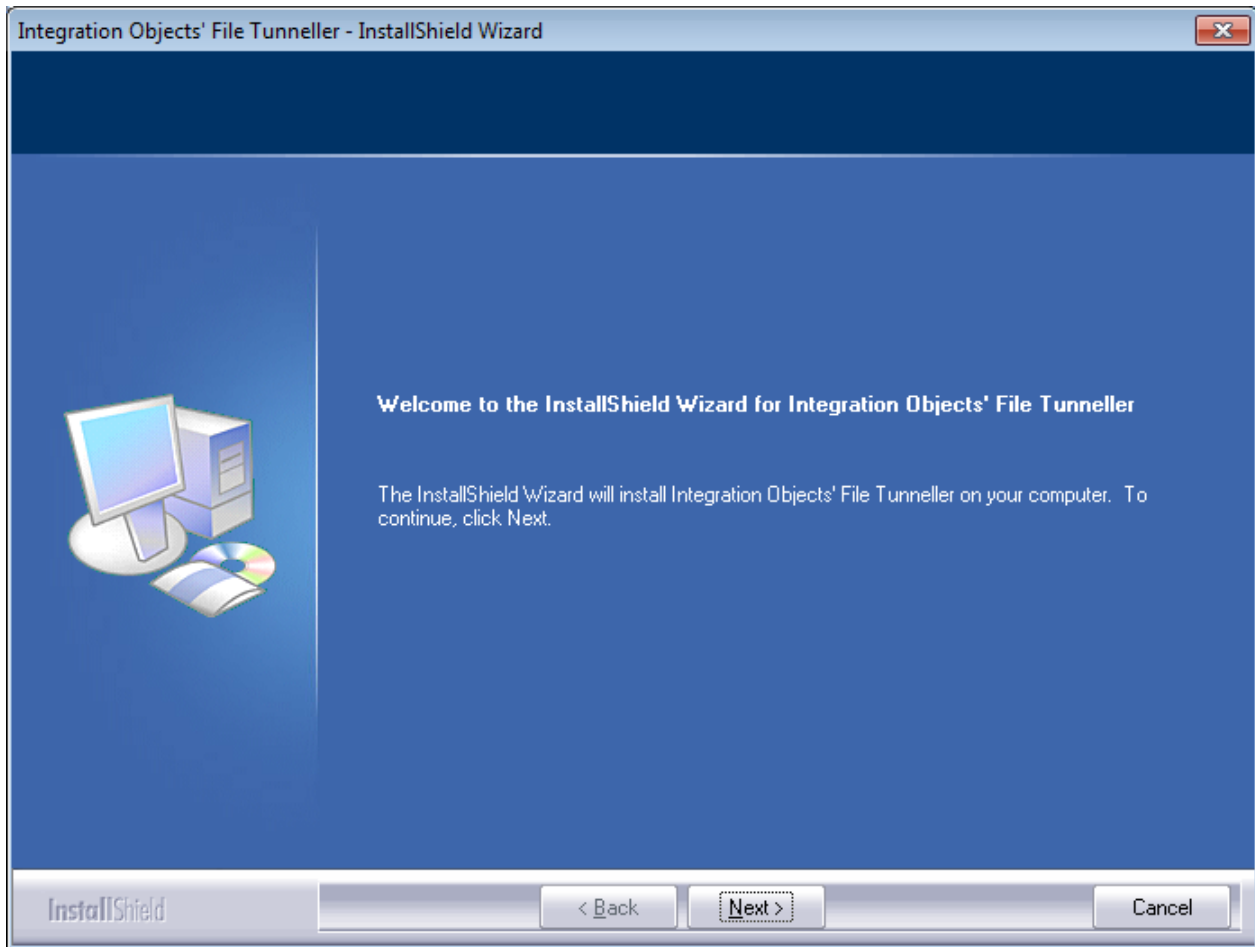
In order to properly run File Tunneller, install these software components on both the Server and Client computers:

- Microsoft .NET Framework ([Microsoft .NET Framework 4](#)) or higher.

## 2. Installing And Running

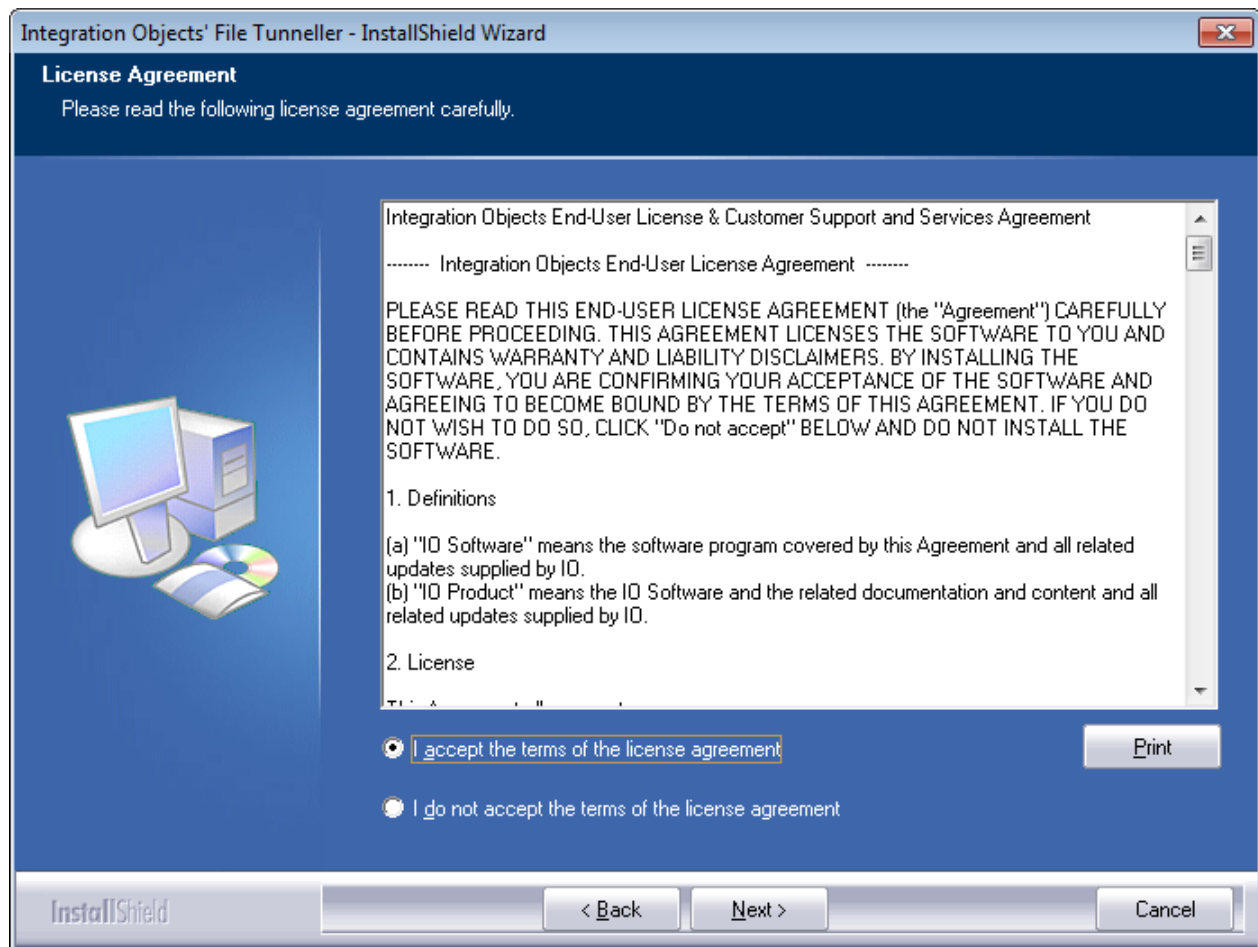
To install the File Tunneller:

1. Double click on the **Integration Objects' File Tunneller.exe**. The installation welcome dialog box will appear.



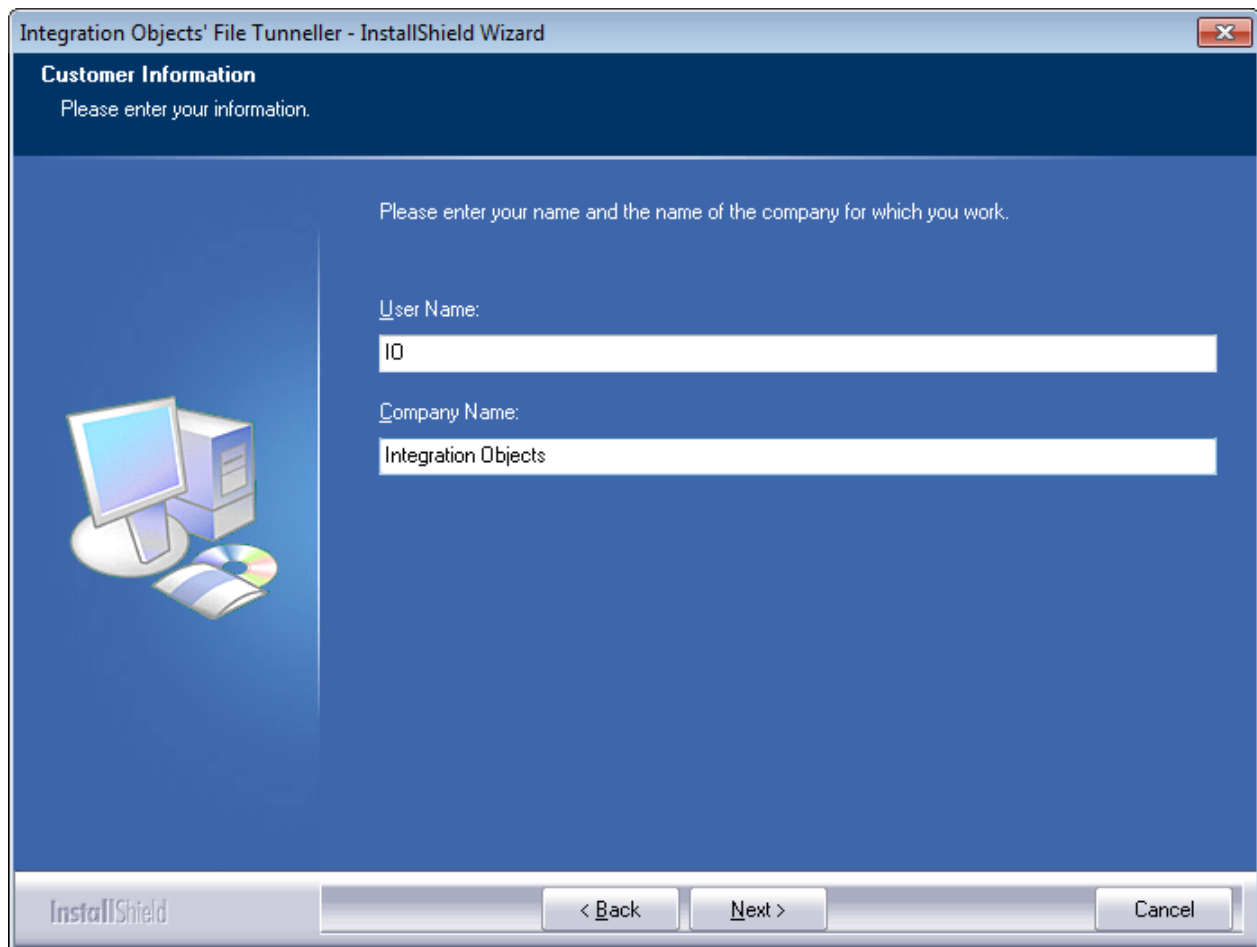
**Figure 2: Installation Welcome Dialog**

2. Click the **Next** button. The license agreement (Figure below) will be displayed



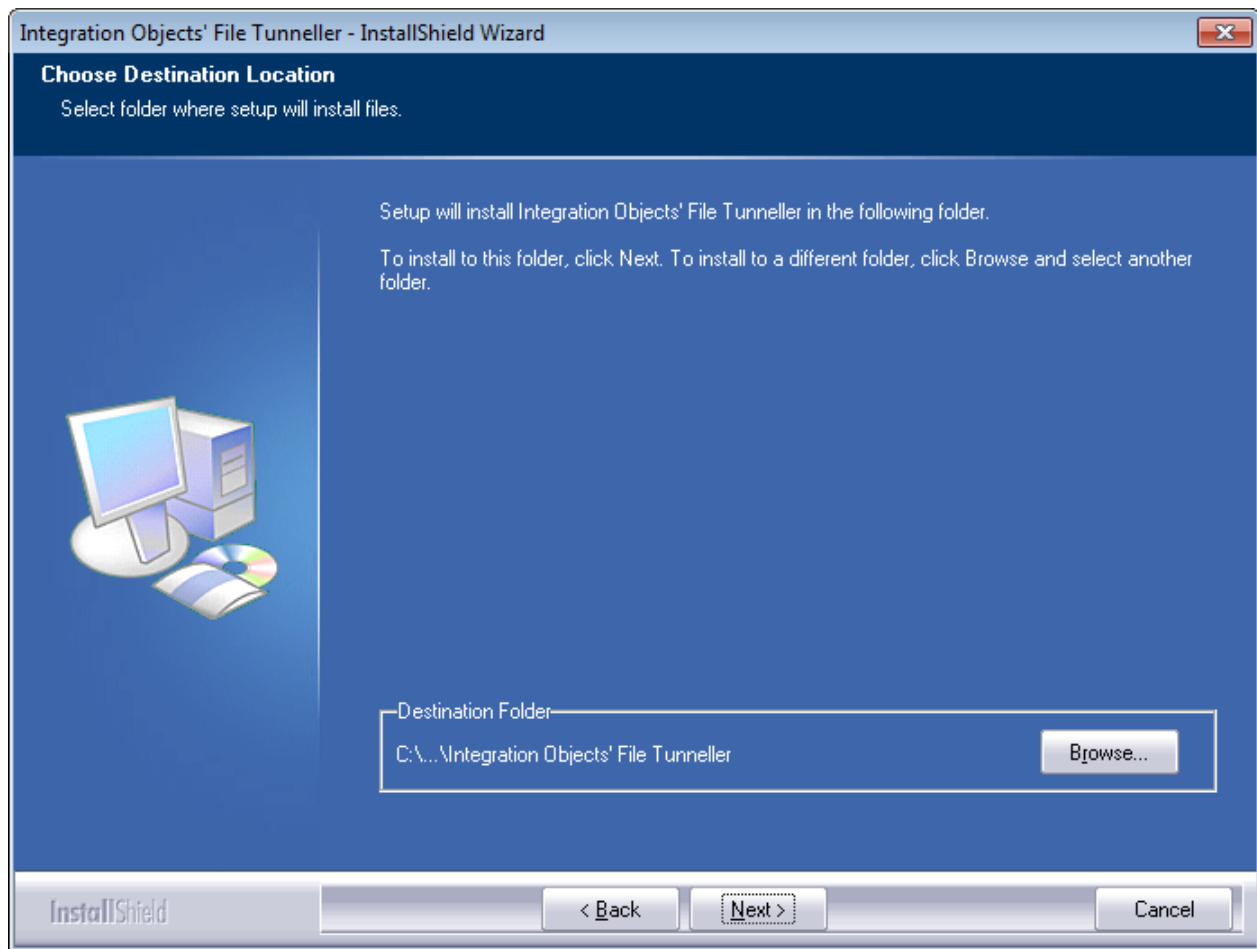
**Figure 3: License Agreement Dialog**

3. By proceeding, you are accepting all of the license agreement terms. Otherwise, you can cancel the installation. Next, the customer information dialog will appear.



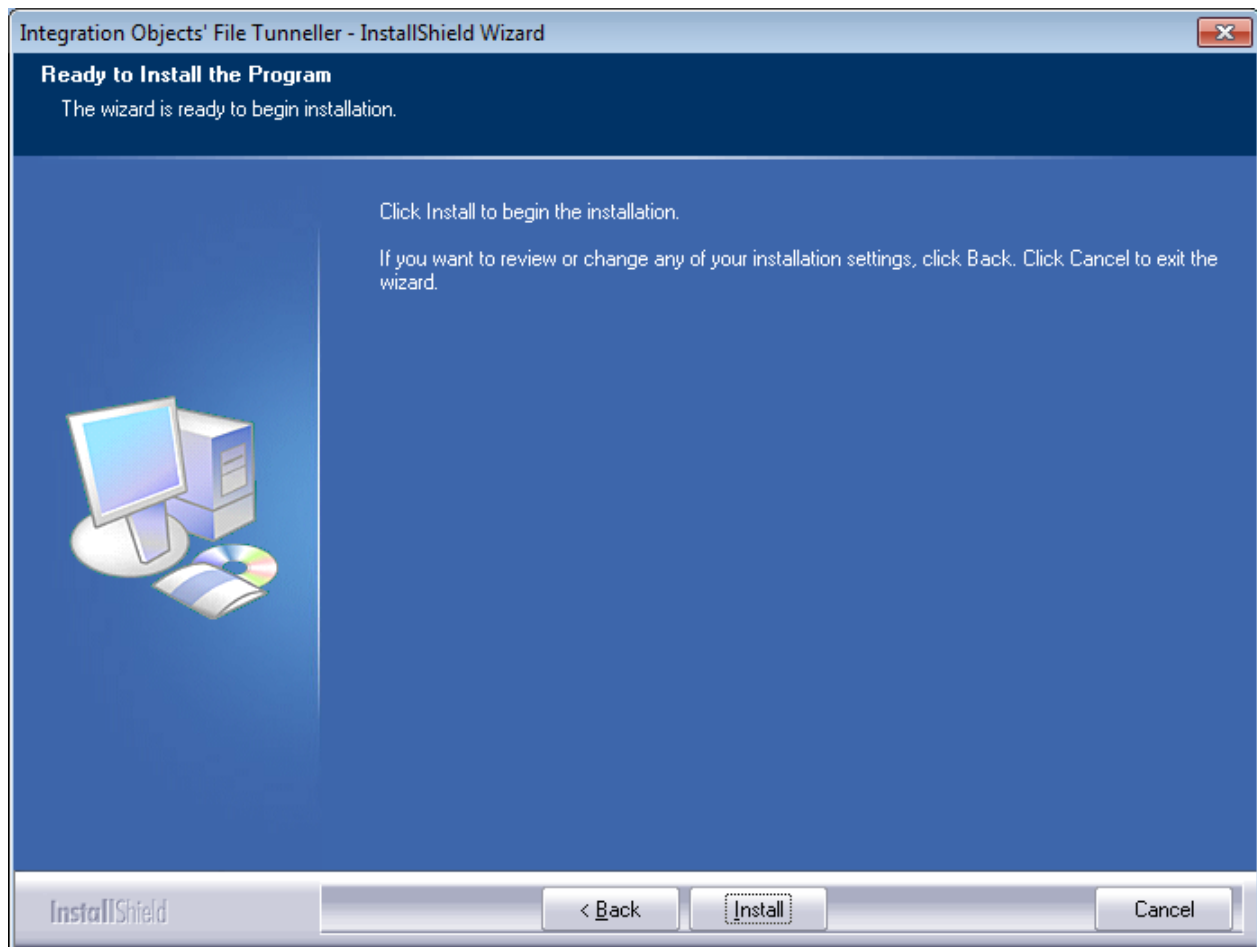
**Figure 4: Customer Information Dialog**

4. Enter user name and company name and then click the **Next** button. The dialog box for choosing the destination folder (Figure below) will be displayed.



**Figure 5: Choose Destination Folder Dialog**

5. Click the **Next** button to continue the installation, or the **Browse** button to select a different destination folder. The installation dialog box (Figure below) will then appear.



**Figure 6: Installation Dialog**

6. Click the **Install** button to start installation.

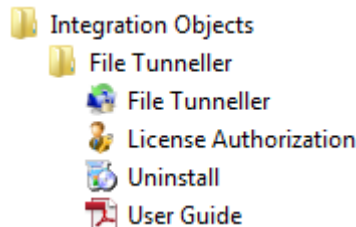
The setup will then:

- Copy the necessary files to the selected target folder,
  - Create shortcut icons to launch the File Tunneller and Authorization License executable from the start menu and the desktop,
  - And make an un-installation entry in the Add/Remove Programs in the Control Panel.
7. Click **Finish**.



### 3. Start-up

To manually start the File Tunneller graphical user interface, click on **Start → Programs → Integration Objects → File Tunneller → File Tunneller**



**Figure 7: File Tunneller Start Menu**

### 4. Log Files

The file transfer service produces the `FileTunnellerService.log` default log file under the File Tunneller installation folder.

The main GUI interface executable generates the `FileTunnellerApp.log` default log file also located under the installation folder.

These files record information, errors and debugging messages for respectively the service and the graphical user interface.

If any difficulties occur with the File Tunneller application, these recorded messages can be extremely valuable for troubleshooting.

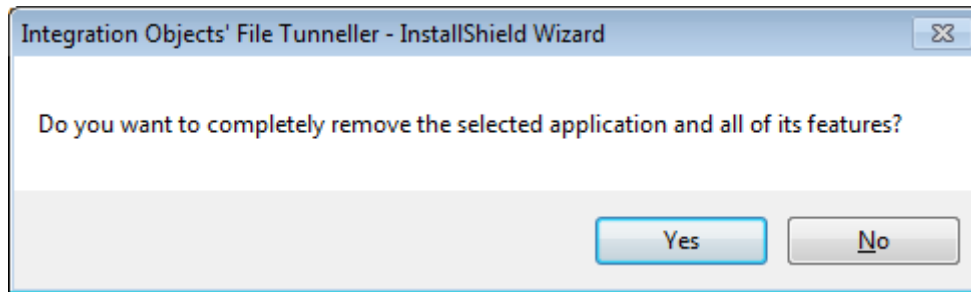
Logging parameters can be changed using both the `ServiceConfig.ini` and `GUIConfig.ini` configuration files or using the log settings after starting the application.

### 5. Removing the File Tunneller

To uninstall the File Tunneller, you need to follow the steps below:

1. Click the Uninstall shortcut icon available in the start menu.

The following dialog box will appear:



**Figure 8: Uninstall the File Tunneller**

2. Click **Yes** to start uninstalling.
3. The wizard will take you through the removal steps. Click **Finish** when the un-installation is complete.

The File Tunneller can also be manually removed as follows:

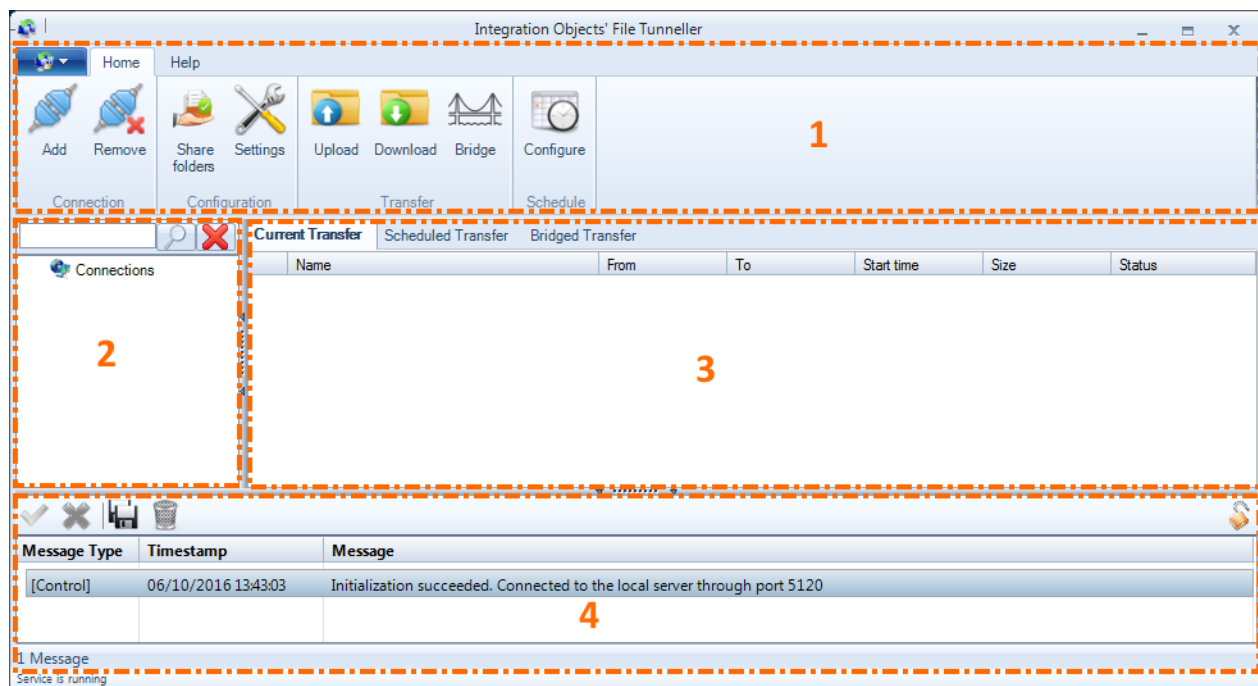
1. Go to the **Control Panel**.
2. Click **Add/Remove** Programs.
3. In the **Add/Remove Programs** dialog screen, select **Integration Objects' File Tunneller**.
4. Click **Change/Remove** then **OK**.

# USING FILE TUNNELLER

In this section, you will find an overview of the File Tunneller user interface as well as the required steps to configure and use this product.

## 1. Main Interface Overview

The File Tunneller user interface allows you to configure the local server, connect to remote machines, download, upload files and schedule file transfer.



**Figure 9: File Tunneller Main View**

There are four parts in the main user interface, as highlighted above:

- Menu bar (1): This part contains the Home menu and the Help menu. These menus provide quick access to functions that help the user interact with the application.
- Connections (2): This part contains the list of server the File Tunneller is connected to.
- Transfer operations (3): This control contains 3 tabs, which are:

- Current Transfer: list all current transfers.
- Scheduled Transfer: list all the transfers that have been scheduled.
- Bridged Transfer: list of all configured bridged transfers.
- Log messages browser (4): This part displays log messages. The most recent messages are displayed at the top of the messages list.

## 1.1. MANAGE FILE TRANSFERS

Using the different buttons in the main menu:

- You can add a new connection to a remote machine using the **Add** button.
- You can remove an existing connection by click in the **Remove** button.
- The **Share Folders** action allows you to add shared folders. Only these folders will be accessible from the client side.
- The **Settings** actions will enable you to manage your connection parameters, log and security settings
- By clicking on the **Access rights** button, you can manage access to your shared folders.
- You can upload files to a remote machine using the **Upload** option.
- To download files from a shared folder configured in a remote server, use the **Download** option.
- Click **Configure** to schedule files in order be sent in a specific date or time

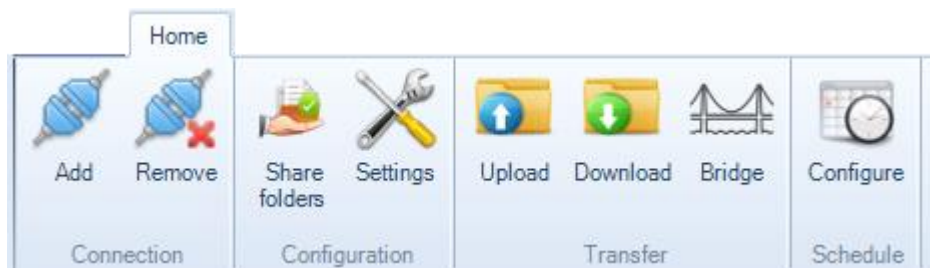


Figure 10: Home Menu

## 1.2. MANAGE CONNECTIONS

To add a new connection, you can either use the **Add** button in the Home menu or use the **Add connection** action by right click on the **Connections** node in the left tree view.

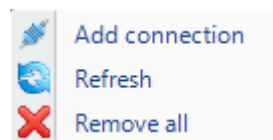
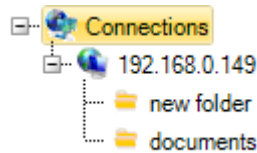


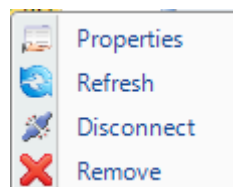
Figure 11: Connections Context Menu

You can check the available servers as well as their respective shared folder below the **Connections** node.



**Figure 12: Available Connections**










Right click on any added server and the following menu will be displayed:



**Figure 13: Server Context Menu**

### 1.3. MONITOR TRANSFERS

You can monitor the current transfers and their statuses in the main interface (see figure 14). You can also check and manage the scheduled and bridged transfers by consulting respectively the **Scheduled transfer** and the **Bridged Transfer** tab.

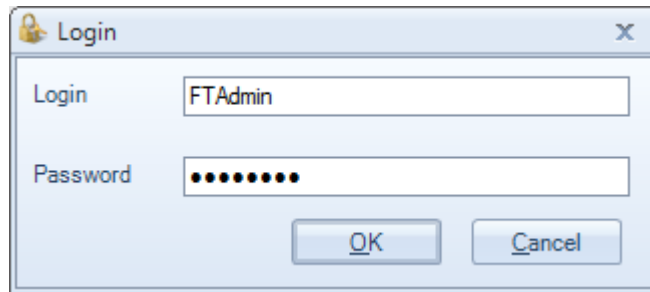
Current Transfer	Scheduled Transfer	Bridged Transfer					
Name	From	To	Start time	Size	Status		
 license.io	192.168.0.124	192.168.0.133	Friday, June 10, 2016 13:28:19	496B	Completed		
 Integration Objects' OPC EasyArchiver.exe	192.168.0.124	192.168.0.133	Friday, June 10, 2016 13:28:19	38.7MB	Completed		
 Crypted\	192.168.0.124	192.168.0.133	Friday, June 10, 2016 13:28:19	19.9MB	Completed		
 Configuration.zip	192.168.0.133	192.168.0.124	Friday, June 10, 2016 13:29:05	404.6MB	3.00 %		
 SLicense.io	192.168.0.133	192.168.0.124	Friday, June 10, 2016 13:29:05	21.4KB	Completed		
 c:\users\administrator\desktop\TCPView	192.168.0.133	192.168.0.124	Friday, June 10, 2016 13:29:05	543.4KB	Completed		
 license.ofa	192.168.0.133	192.168.0.124	Friday, June 10, 2016 13:29:05	1.2KB	Completed		
 myExcel.xlsx	192.168.0.124	192.168.0.133	Friday, June 10, 2016 13:30:13	5.6KB	Completed		
 Integration Objects' OPC UA Wrapper.exe	192.168.0.133	192.168.0.124	Friday, June 10, 2016 13:30:34	10.5MB	71.99 %		

**Figure 14: Current File Transfers**

## 2. Managing administrator account

### 2.1. LOGIN INTO FILE TUNNELLER

The administrator logon is disabled by default. When this option is enabled, the File Tunneller will prompt the for admin logon credentials on start-up.



**Figure 15: Enter Admin Credential**

The default login is:

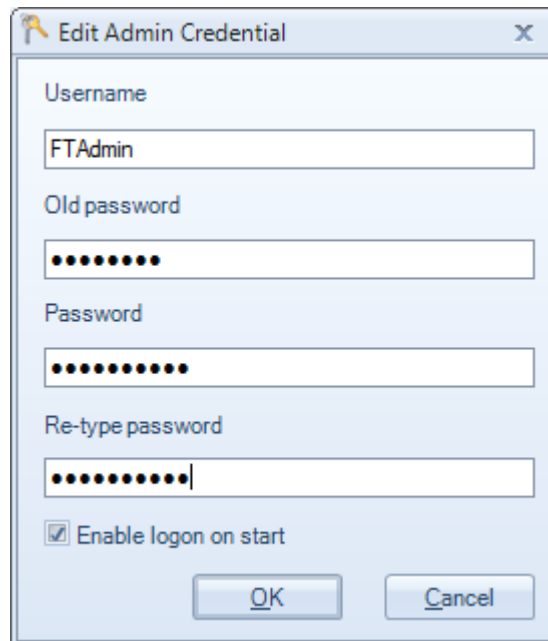
- Login: FTAdmin
- Password: FT5@dmin



**It is recommended that users change the default password once they complete the installation.**

## 2.2. EDIT ADMINISTRATOR CREDENTIAL

You can edit your login credential using the following windows:



**Figure 16: Edit Admin Credential**

You can change your user name as well as your password.

## 3. File Tunneller Functionalities

### 3.1. ADD SHARED FOLDERS

This interface enables the end user to select the folders from where files will be downloaded or to be uploaded.

To do so, click the **Share Folders** button in the menu bar.

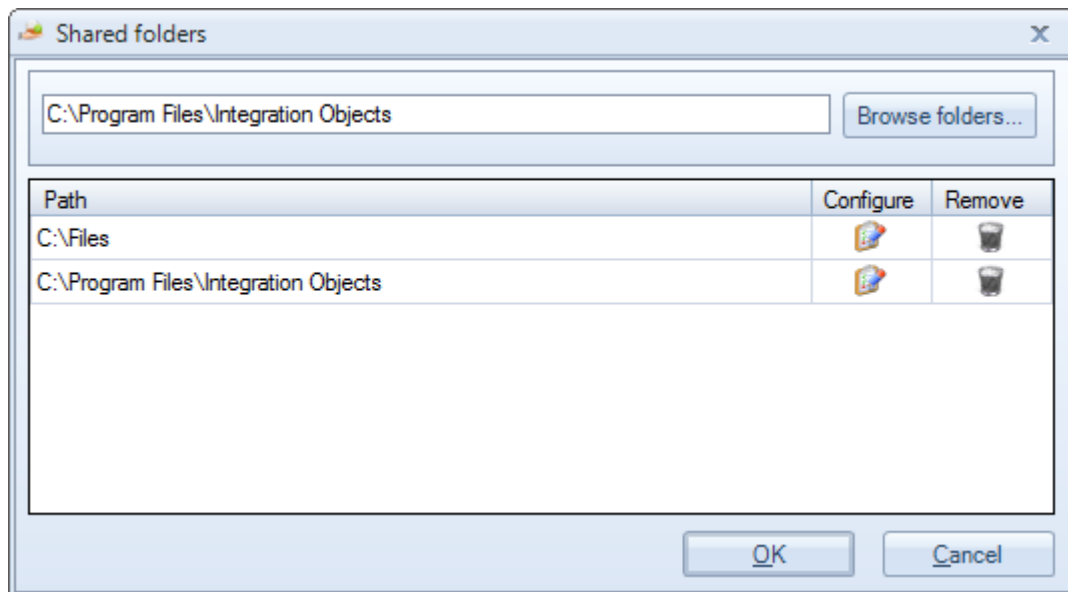
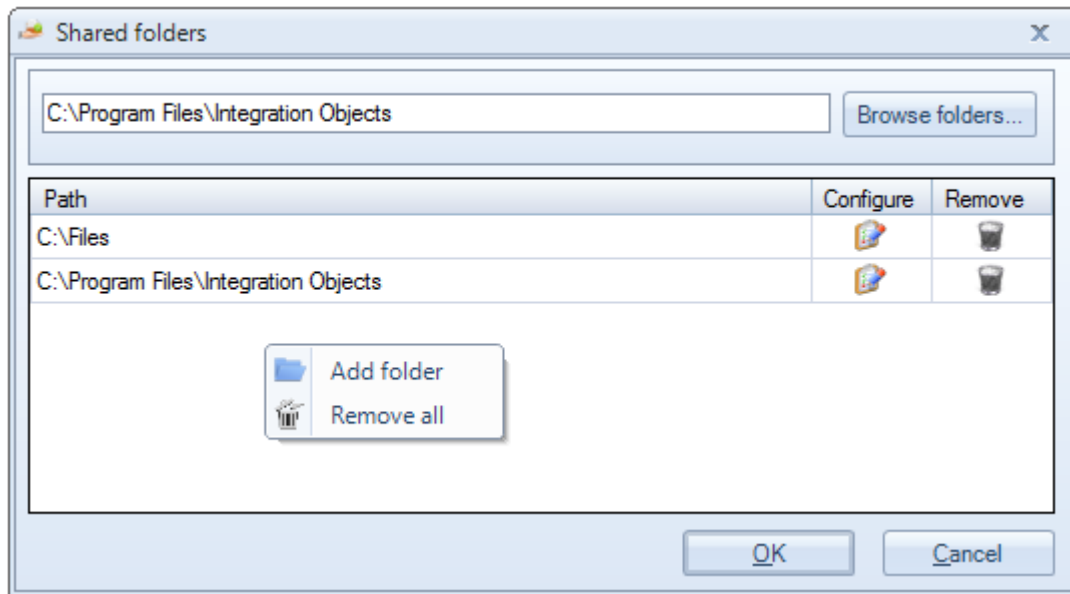


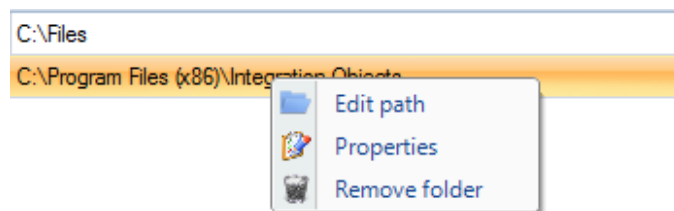
Figure 17: Shared Folders

You can browse the folder name using the **Browse Folders** button or just enter the folder path in the respective entry. You can also add them by simply right click on the blank area and select the **Add folder** option.



**Figure 18: Add shared folder**

To remove a shared folder, right click on the folder you want to remove and select **Remove folder** from the displayed menu.

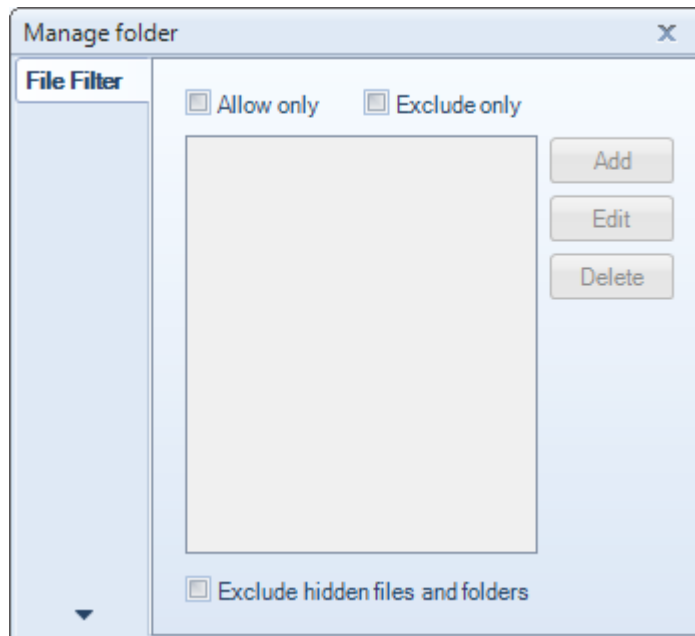


**Figure 19: Edit Shared Folder**

The **Edit path** option enables you to change the path of the selected folder.  
File

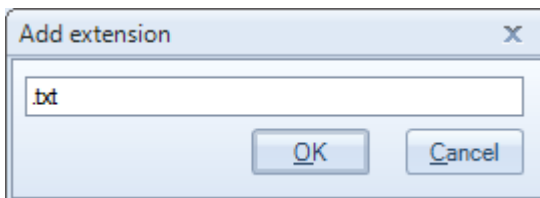
When selecting properties, you can manage the shared folder properties such as the allowed extensions.



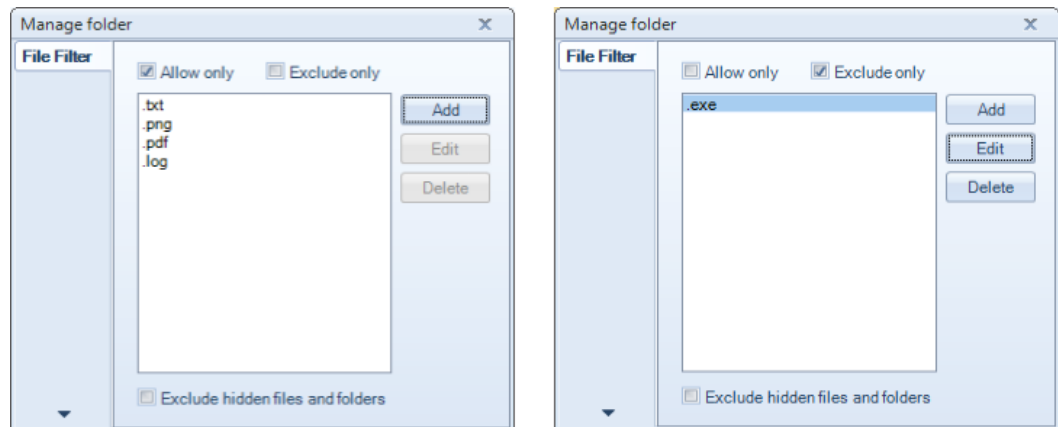


**Figure 20: Manage Folder**

You can allow or exclude specific extensions by checking the Allow only\Exclude only check box and hit the **Add** button.

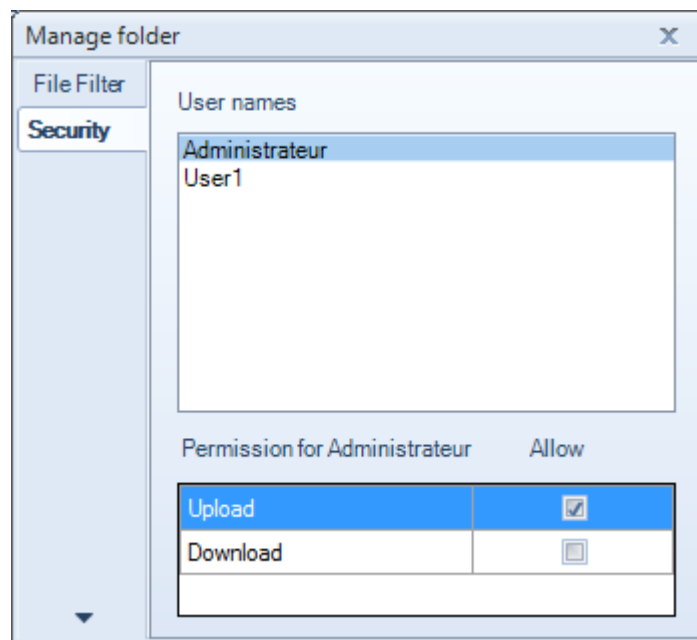


**Figure 21: Add File Extension**



**Figure 22: File Filter**

You can manage the users' access rights to the shared folders by using the security tab. This tab is only available in the **With encryption and authentication** mode.



**Figure 23: Set Users' Permissions**

This interface will display the configured users in the user management dialog. When using one of the configured accounts to connect, the remote machine can only upload or download files to/from the allowed shared folders.

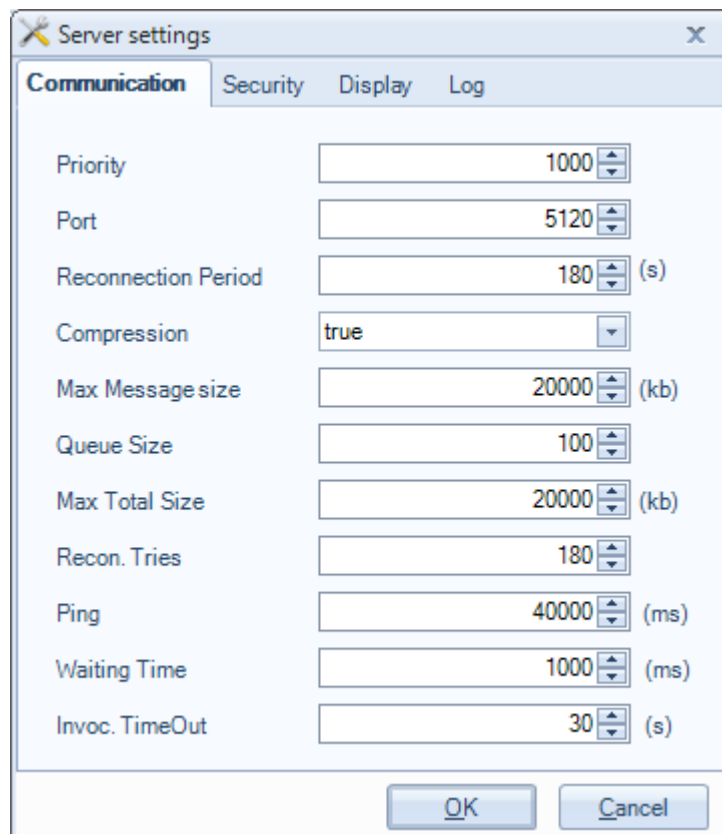
## 3.2. CONFIGURE SERVER SETTINGS

The Server side should be configured before adding a new connection to this end. To configure the server, click the **Settings** button in the menu bar.

After the configuration, the user must click **OK** to save the changes. Otherwise, the changes will be lost.

### 3.2.1. Communication Parameters

The communication settings are used to configure the server's connection parameters.



Parameter	Value	Unit
Priority	1000	
Port	5120	
Reconnection Period	180	(s)
Compression	true	
Max Message size	20000	(kb)
Queue Size	100	
Max Total Size	20000	(kb)
Recon. Tries	180	
Ping	40000	(ms)
Waiting Time	1000	(ms)
Invoc. TimeOut	30	(s)

Figure 13: Configure Server Communication Settings

For more explanation about the different communication settings, please refer to the table below:

Communication Setting	Description	Default Value
<b>Priority</b>	An integer value representing the priority assigned to this connection. The higher the priority is, the higher is the chance for this connection to be established first.	100
<b>Port</b>	This is the port on which the Server will listen to connected clients	5120
<b>Reconnection Period</b>	When the client connection through the TCP channel is broken, it is expected to re-establish the connection within the specified time interval. Otherwise, the Server declares the connection as closed.	180 (seconds)
<b>Compression</b>	To enable compression on the server side, set this flag to true.  Possible options: <ul style="list-style-type: none"> <li>• True: Enable compression</li> <li>• False: Disable compression</li> </ul>	true
<b>Max Message Size</b>	The maximum size of a transmitted message.	20000 (kilobytes)
<b>Queue Size</b>	The total number of queued messages.	100
<b>Max Total Size</b>	The maximum total size of queued messages.	20000 (kilobytes)
<b>Recon. Tries</b>	The number of reconnection attempts before declaring that the connection as lost.	180
<b>Ping</b>	The client sends ping messages to the server within this ping time period.	40000 (milliseconds)
<b>Waiting Time</b>	The waiting time after every reconnection failure.	1000 (milliseconds)
<b>Invoc. TimeOut</b>	The request is recognized as failed when the client does not receive a response from the server within this time period.	30 (seconds)

**Table 1: Communication Settings**

### 3.2.2. Security Settings

Select **Security** in the server settings dialog to configure security options. You will then get the following screen:



**Figure 24: Configure Server Security Mode**

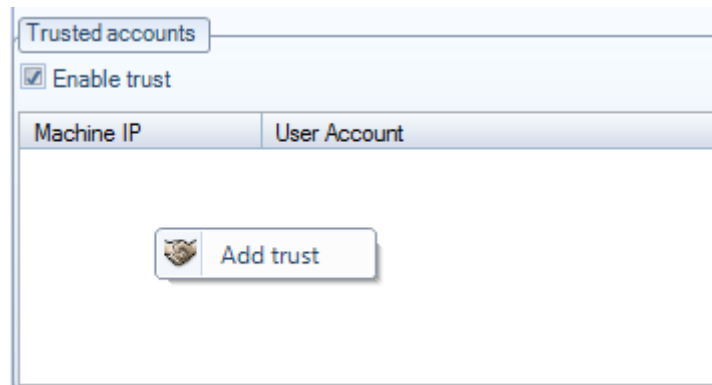
The server can be accessed using one of the three security modes:

- Without encryption: This mode is not recommended because it disables the data encryption for the network communications. But it may be used for testing or troubleshooting purposes.
- With encryption: This is the default mode which enables using data encryption.
- With encryption and authentication: This is the most secure mode enabling both data encryption and user authentication in order to ensure both data integrity and confidentiality.

You can also strengthen your data confidentiality scheme by adding another authentication layer to your communications. To do so, you can configure a trust between the server and the client machines by checking the **Enable trust** check box

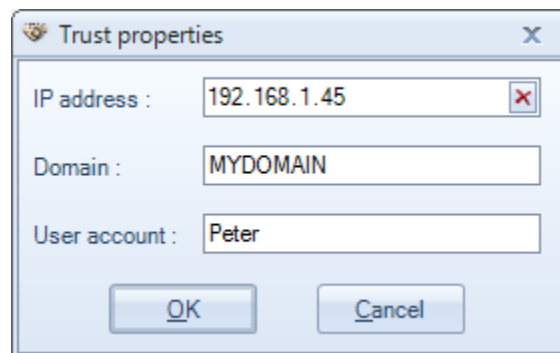
and adding the machines and users you trust. This option works with the three connection modes listed above. Only the configured users in the trust can access this server.

Right click on the **Trusted accounts** table in the **Security Settings** window and select **Add trust** from the displayed menu.



**Figure 25: Add Trust**

The window shown in the figure below should appear. The end user should enter the IP address of the trusted client machine and the authorized user account information:



**Figure 26: Configure a Trust**

The security settings window will be updated and the configured user accounts will be added as shown in the figure below:



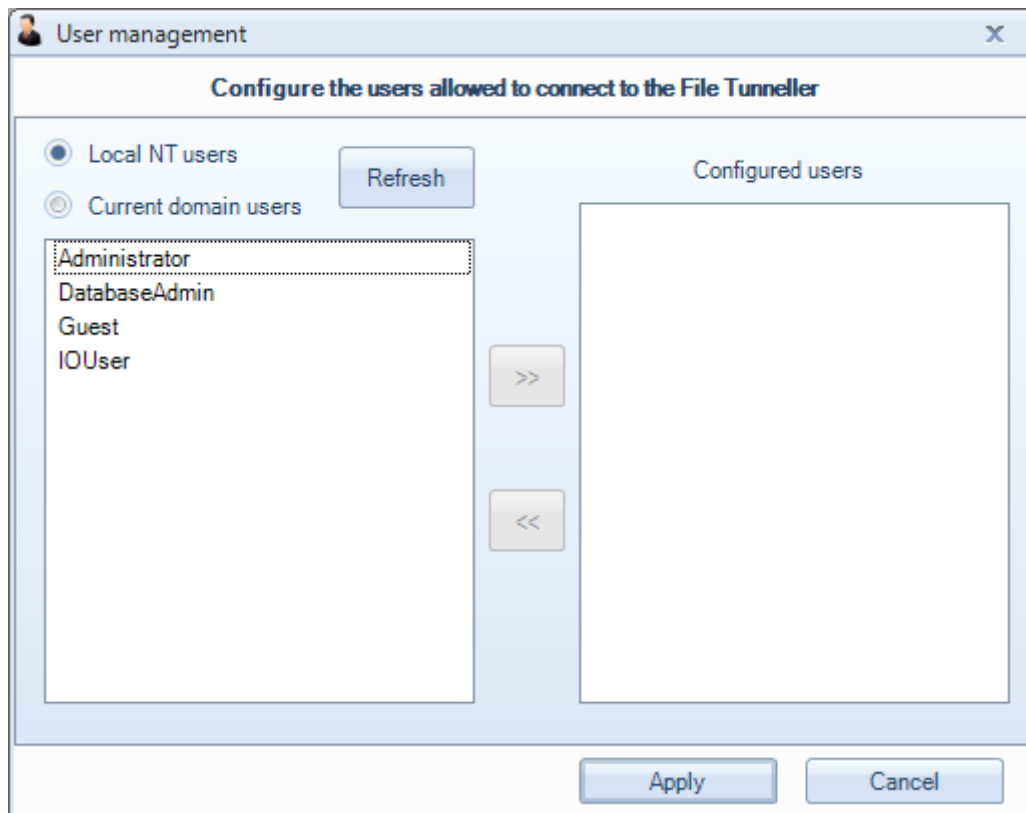
**Figure 27: Trusted Accounts Configuration**

If you enable the trust, only the configured machines can have access to the server. When adding a machine with an empty user accounts, all users having access to that machine have permission to add a connection to the server.

### 3.2.3. User Management

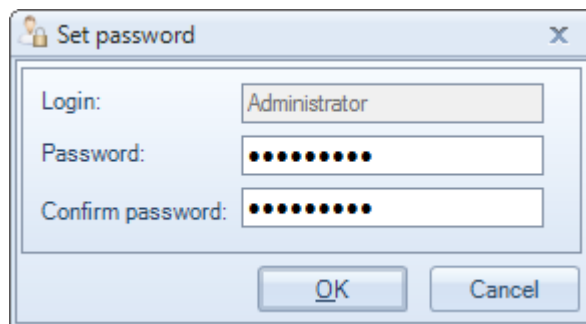
User configuration is required for secured communication. This tool manages user accounts configured on the server machine. Also, it manages the client accounts when using the **With encryption and authentication** mode.

Select the server side account from the **Available Users** List and then click the **>>** button to add one server user to the list of **Configured Users**.



**Figure 28: Add User**

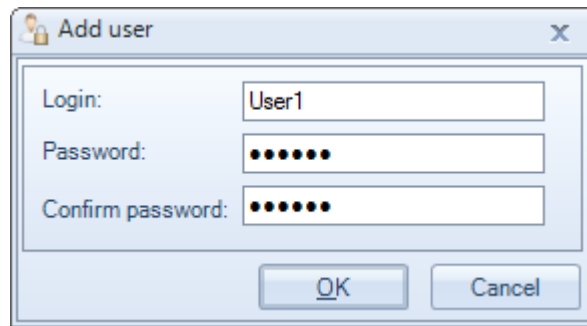
You will be asked to set the password and confirm it: you can enter the NT user account password or a custom password. An empty value is not permitted. Then, click the **OK** button.



**Figure 29: Set User's Password**

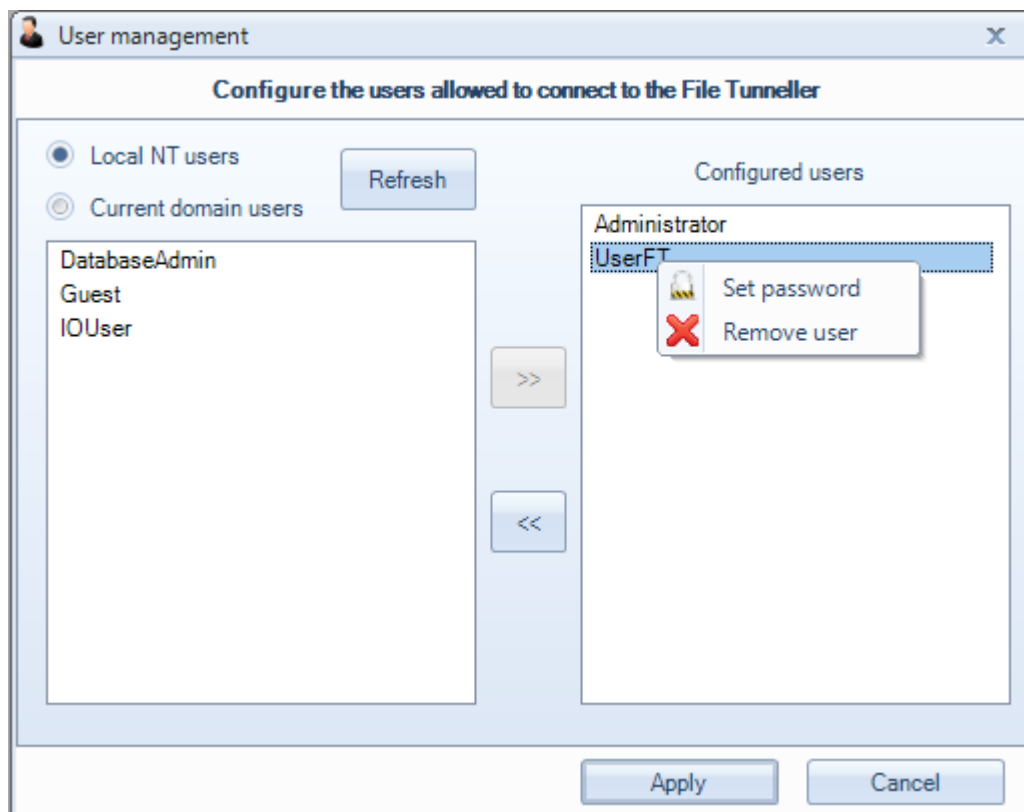
To add a custom user, right click on an empty field on the configured user list and click the **Add user** button.





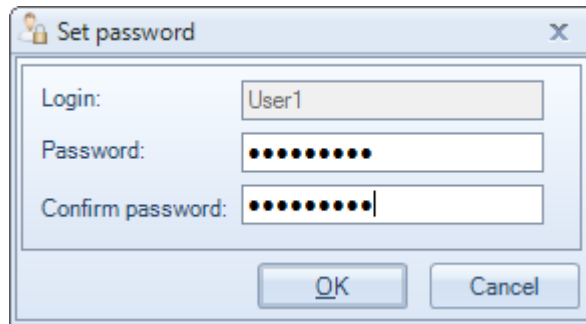
**Figure 30: Add Application Authentication**

To change a configured user password, select one user from the configured user list and then click on **Set password** button.



**Figure 31: Change Password**

The dialog below will be displayed. Enter the new password and click **OK** to confirm.

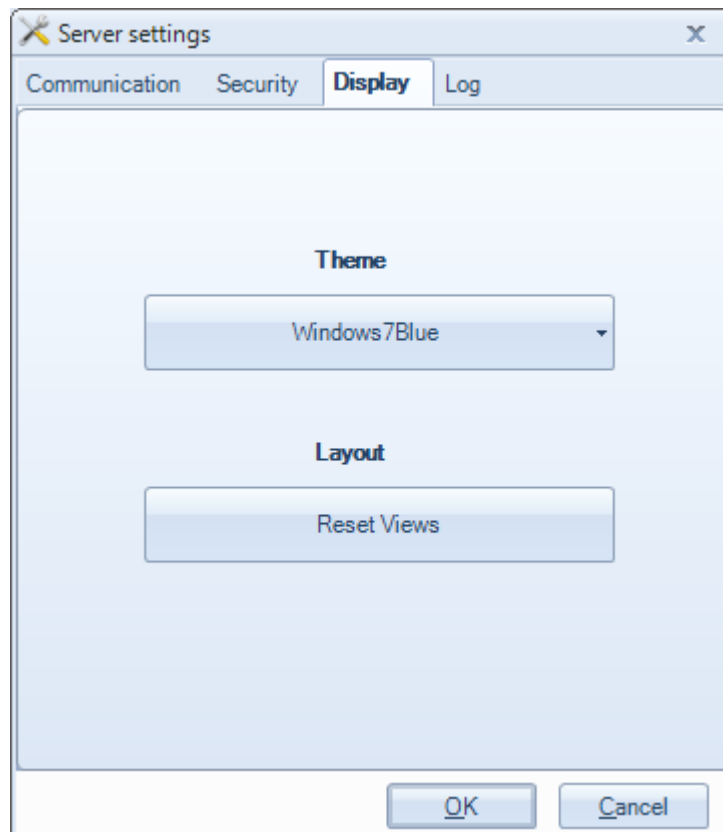


**Figure 32: Set a New Password**

Click the **Apply** button to save the configuration.

### 3.2.4. Display

This tab allows users to change the File Tunneller theme. The default theme is Windows7Blue.



**Figure 33: Change display settings**

### 3.2.5. Log Settings

Select the **Log** tab from the server settings window to configure log options. This tab contains the configuration of both the File Tunneller service and the application log files.

The below window will appear:

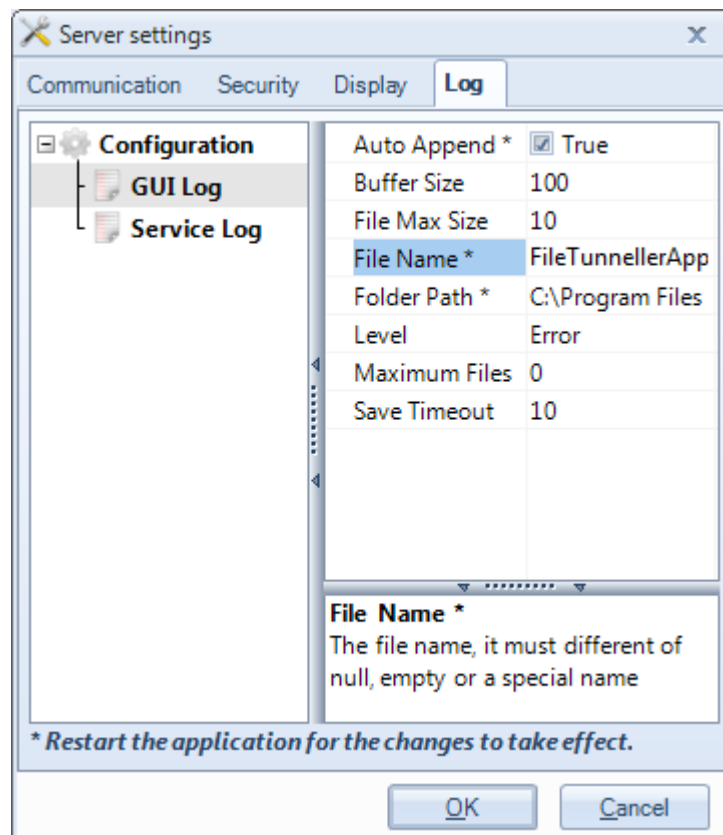
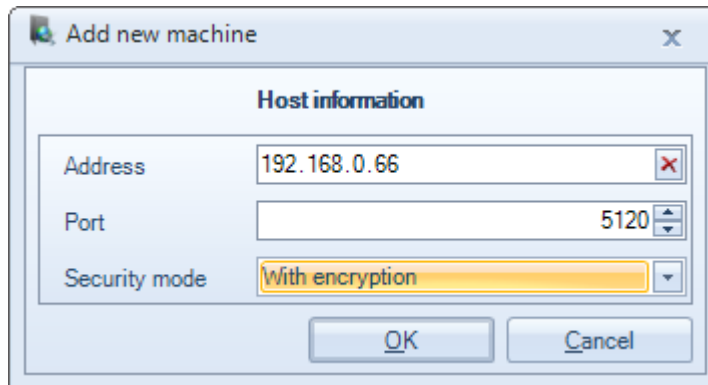


Figure 34: Configure Log Settings

## 3.3. CONFIGURE CONNECTIONS

Using the File Tunneller, you can connect to different machines. The connection dialog is shown in the figure below:



The dialog box is titled "Add new machine". It contains a section titled "Host information" with the following fields:

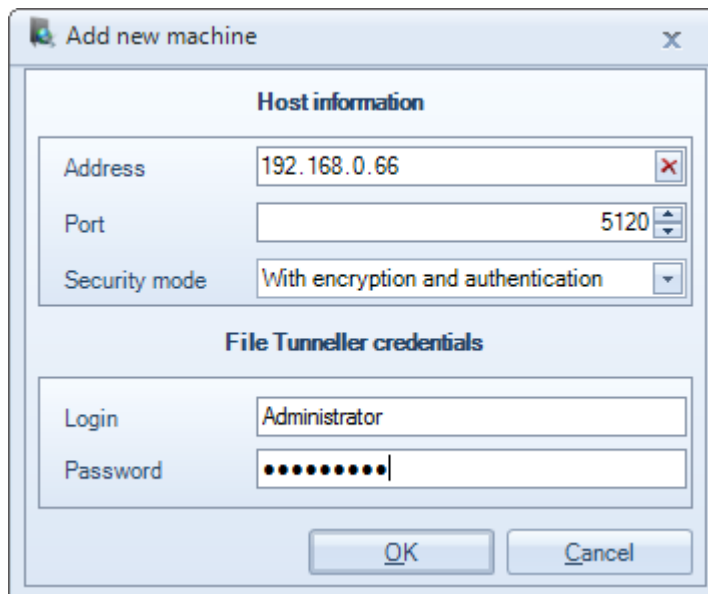
- Address: 192.168.0.66
- Port: 5120
- Security mode: With encryption

Buttons for "OK" and "Cancel" are located at the bottom of the dialog.

**Figure 35: Add Connection**

Enter the IP address of the remote machine and the port configured in the server. You have the choice between three different connection modes (**Without Encryption**, **With Encryption** and **With Encryption and Authentication**).

When selecting the **With Encryption and Authentication** mode, the following dialog will appear where you can enter the login and the password of the authorized user.



The dialog box is titled "Add new machine". It contains a section titled "Host information" with the following fields:

- Address: 192.168.0.66
- Port: 5120
- Security mode: With encryption and authentication

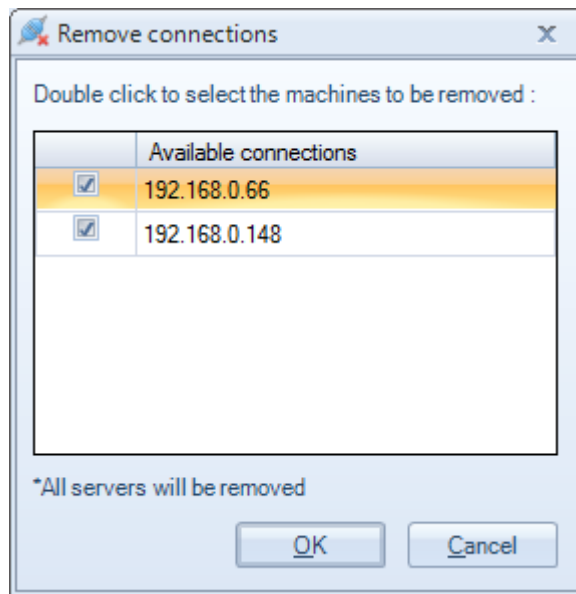
Below the "Host information" section is a section titled "File Tunneller credentials" with the following fields:

- Login: Administrator
- Password: [Masked]

Buttons for "OK" and "Cancel" are located at the bottom of the dialog.

**Figure 36: Add Connection with Authentication**

To remove a connection, click the **Remove** button in the connection tab of the main user interface. Select the servers you want to disconnect from and then click "**OK**".

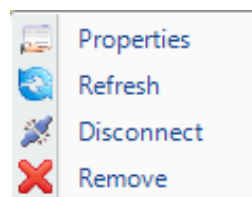


**Figure 37: Remove Connections**

The connection will be destroyed and you can no longer download or upload files from/to this location.

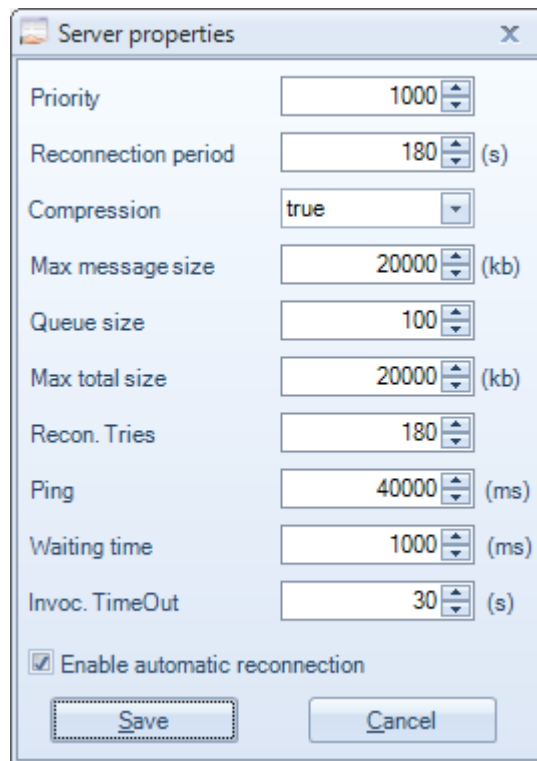
### 3.4. CONNECTION PROPERTIES

When right clicking on a connection from the left tree view, you can check the connection properties by selecting the **Properties** button from the displayed menu.



**Figure 38: Connection Properties**

The **Refresh** button will refresh the connection of the respective shared folders list.  
The **Disconnect** button will allow to disconnect from the remote machine but enables you to reconnect when needed.



**Figure 39: Server Properties**

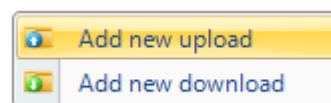
You can also refresh or remove all connections by selecting the respective option and by right clicking on the connections node.

## 3.5. TRANSFER OPERATIONS

### 3.5.1. Upload File

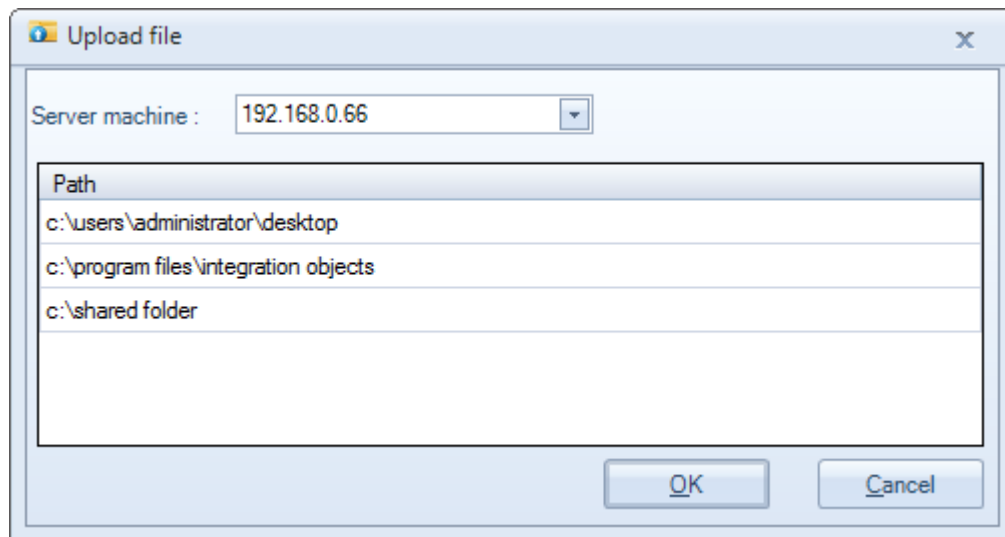
To upload a file:

1. Click on the **Upload** button from the transfer menu or right click on the current transfer grid and select **Add new upload**



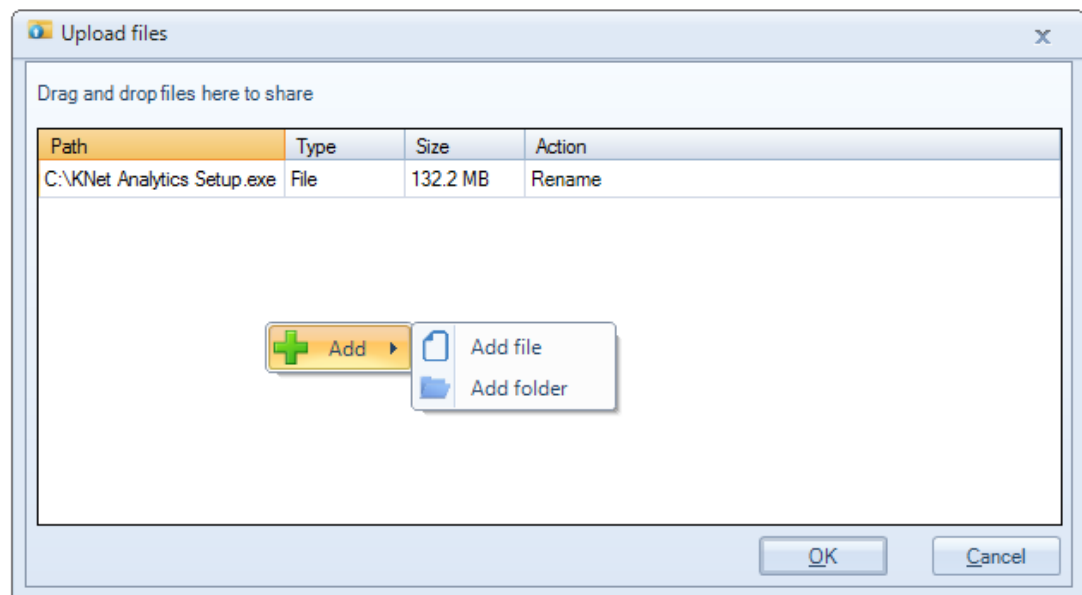
**Figure 40: Current Transfer Menu**

2. Choose the remote machine. The configured shared folders in that machine will be listed.
3. Select the destination folder from that list and click **OK**



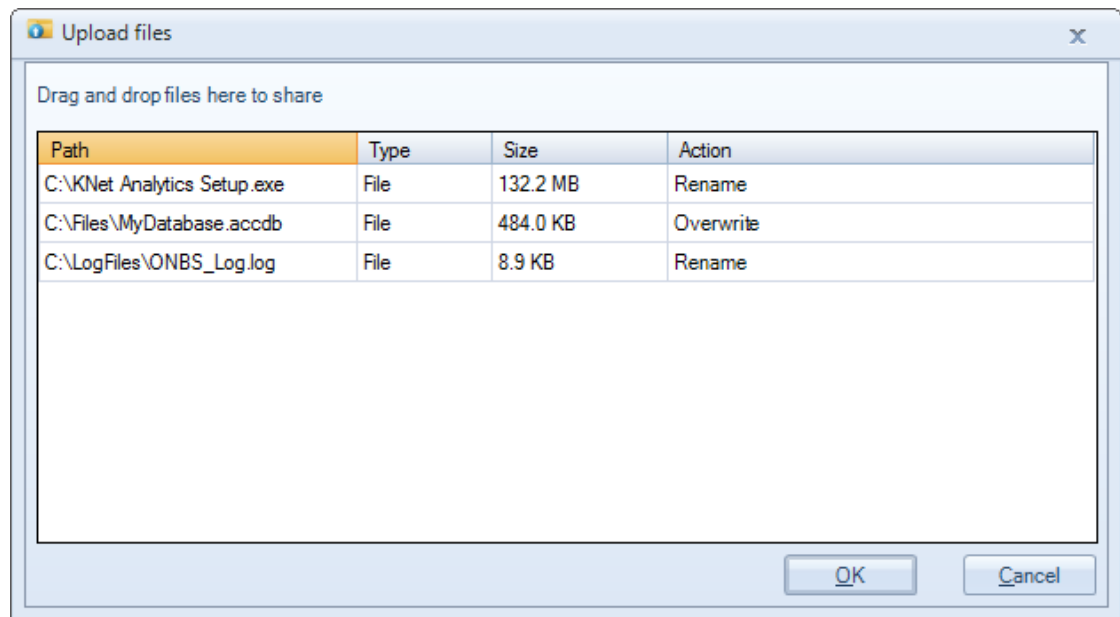
**Figure 41: Set Destination Folder**

4. Add the files or folders to be sent to the destination machine by either drag and drop them into the upload list or by right click and select the **Add** action.



**Figure 42: Add File or Folder**

5. If the file already exists in the destination machine's shared folder, select either rename or overwrite it, then click **OK**.



**Figure 43: Upload Files**

If the file already exists in the remote folder:

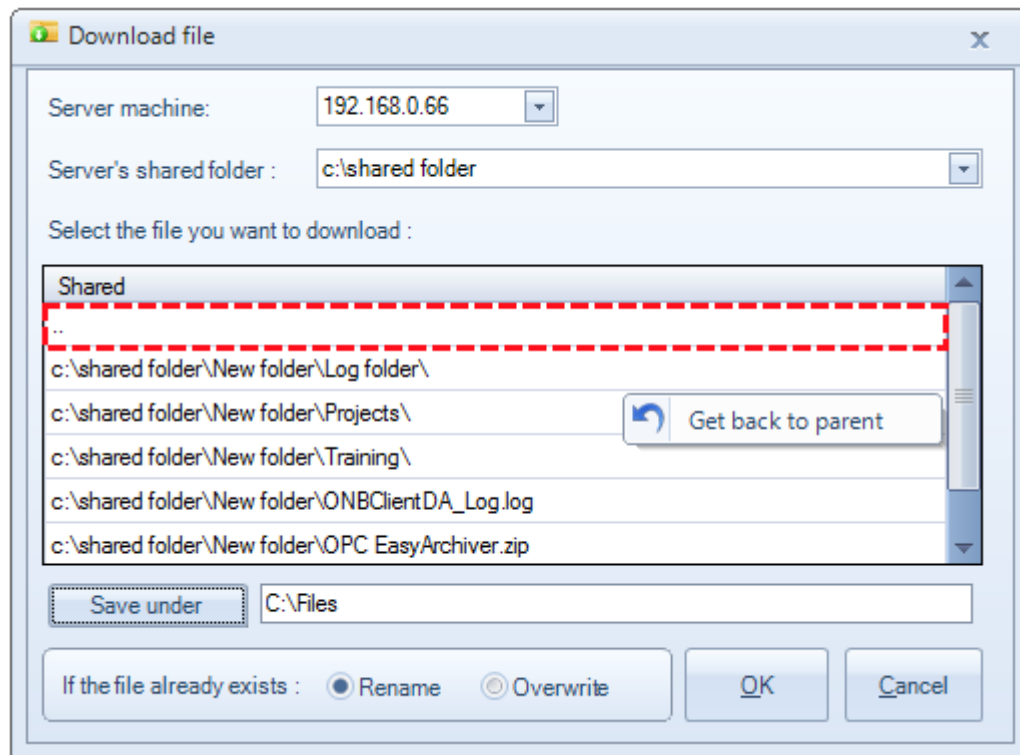
- The default action is to rename it. The new file name will show the time of reception at the end of the file's name
- When you choose the **Overwrite** option, the older file will be removed.

### 3.5.2. Download File

To download a file:

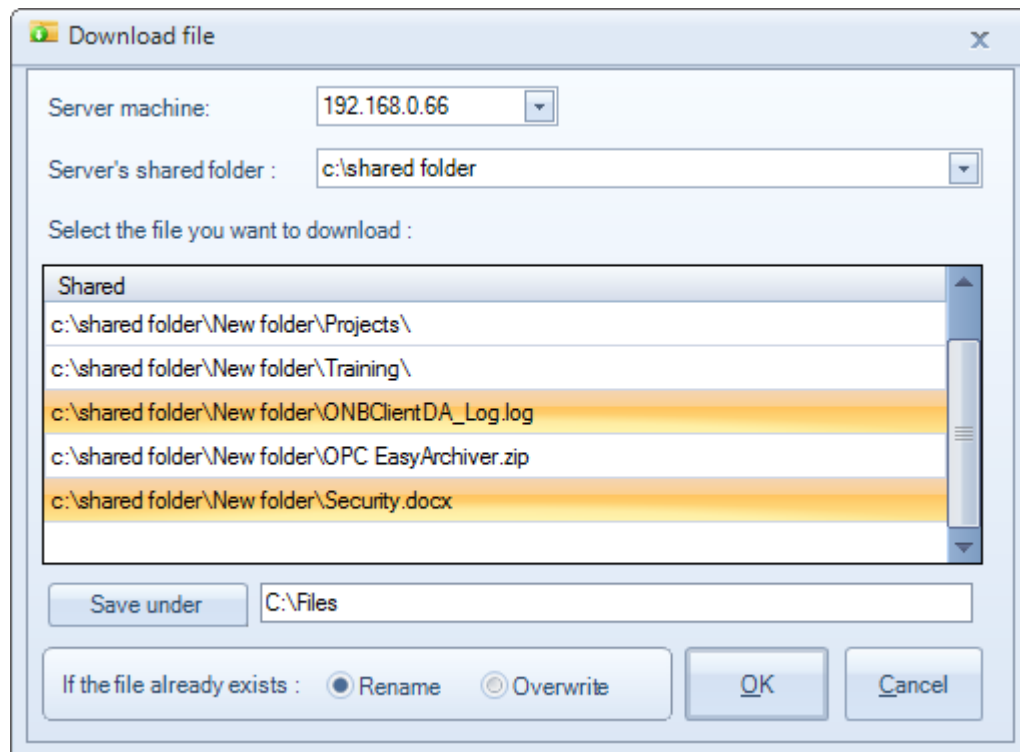
1. Click the **Download** button from the transfer menu in the main user interface.
2. Select the destination machine.
3. Select the shared folder containing the files you are interested in. You can browse the shared subfolders by double clicking on them. You can go back to the main folder by right clicking on the subfolder and selecting the **Get back to parent** from the displayed menu or by clicking on the first row in the subfolder.





**Figure 44: Browse Remote Machine's Files**

4. After that, you have to specify where the folder will be saved in your machine using the **Save under** field.

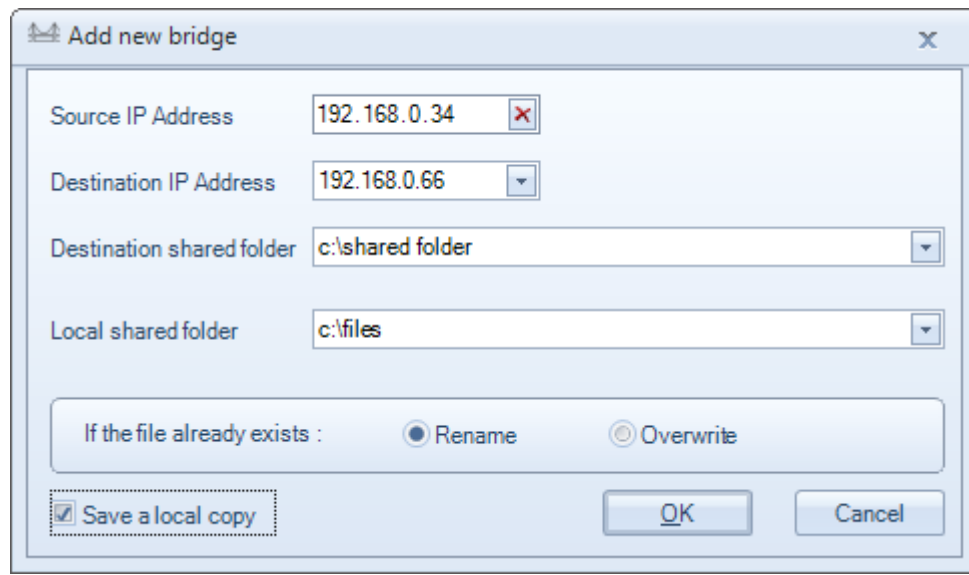


**Figure 45: Download File**

5. Select the files to be downloaded.
6. Specify the action to take if the file already exists.
7. Click **OK**.

### 3.5.3. Bridge File Transfer

To configure a bridge file transfer, click the **Bridge** button from the transfer bar in the main user interface or right click on the bridged transfer grid and select **Add bridge**. Whenever you receive a transfer from the **Source IP Address** and in the configured **Local shared folder**, the File Tunneller will automatically transfer the received file to the configured destination folder in **Destination IP Address**.



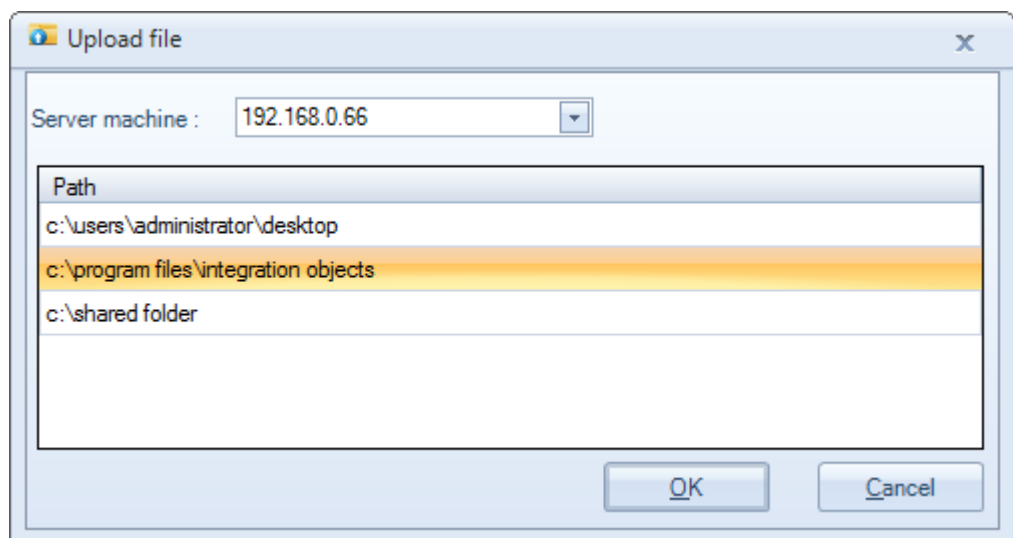
**Figure 46: Add New Bridge**

### 3.5.4. Schedule File Transfer

To configure a scheduled file transfer, click the **Configure** button from the schedule bar in the main user interface or right click on the schedule transfer grid and select **Add schedule**.

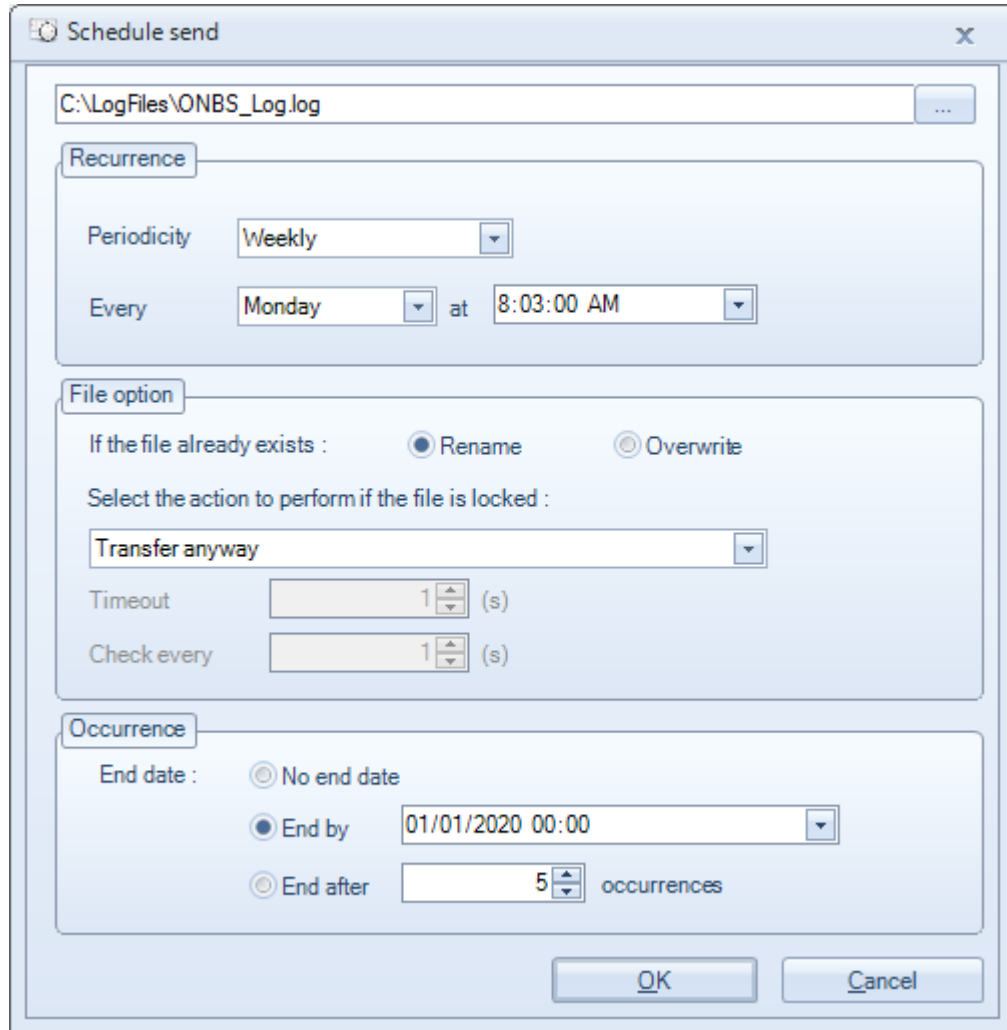
Then, you will have to:

1. Choose the remote machine. The configured shared folders in that machine will be listed.
2. Select the destination folder from that list and click **OK**



**Figure 47: Select Destination Folder**

3. Browse and select the file\folder that will be sent
4. Specify the time when the operation will be executed
5. Choose what to do if the file already exists.



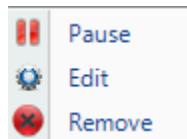
**Figure 48: Schedule Send**

You can view the scheduled operation by selecting **Configure** button in the schedule bar in the main user interface. This dialog offers you the needed information about the scheduled operations and enables you to pause, remove a scheduled operation or resume a paused one.

Current Transfer		Scheduled Transfer		Bridged Transfer	
Status	From	Destination IP	To	Type	Time
	C:\LogFiles\ONBS_Log.log.bt	192.168.0.148	c:\perflogs	Weekly	Monday at 8:00:00 PM
	C:\AllFiles\Configuration.zip	192.168.0.148	c:\shared folder	Specific time	25/03/2015 10:20
	C:\Program Files (x86)\Integration Objects\Integration Objects' OPCNet Broker Client Side\DA\ONBClientDA_Log.log	192.168.0.148	c:\shared folder	Daily	at 08:30:00
	C:\Executable\New folder	192.168.0.148	c:\shared folder	Hourly	at 5 minutes 5 seconds

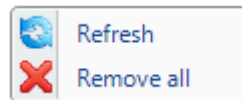
**Figure 49: Configured Scheduled Transfers**

To configure the available file transfer schedules, right click on the transfer and select to either stop, edit or remove it.



**Figure 50: Scheduled Transfer Options**

You can also refresh or remove all scheduled transfer by right clicking on the scheduled transfer tab empty area.



**Figure 51: Scheduled Transfer General Options**

### 3.6. TRANSFER PROPERTIES

When downloading or uploading files, the main interface will be updated to display the ongoing transfers along with their respective status in the status column:

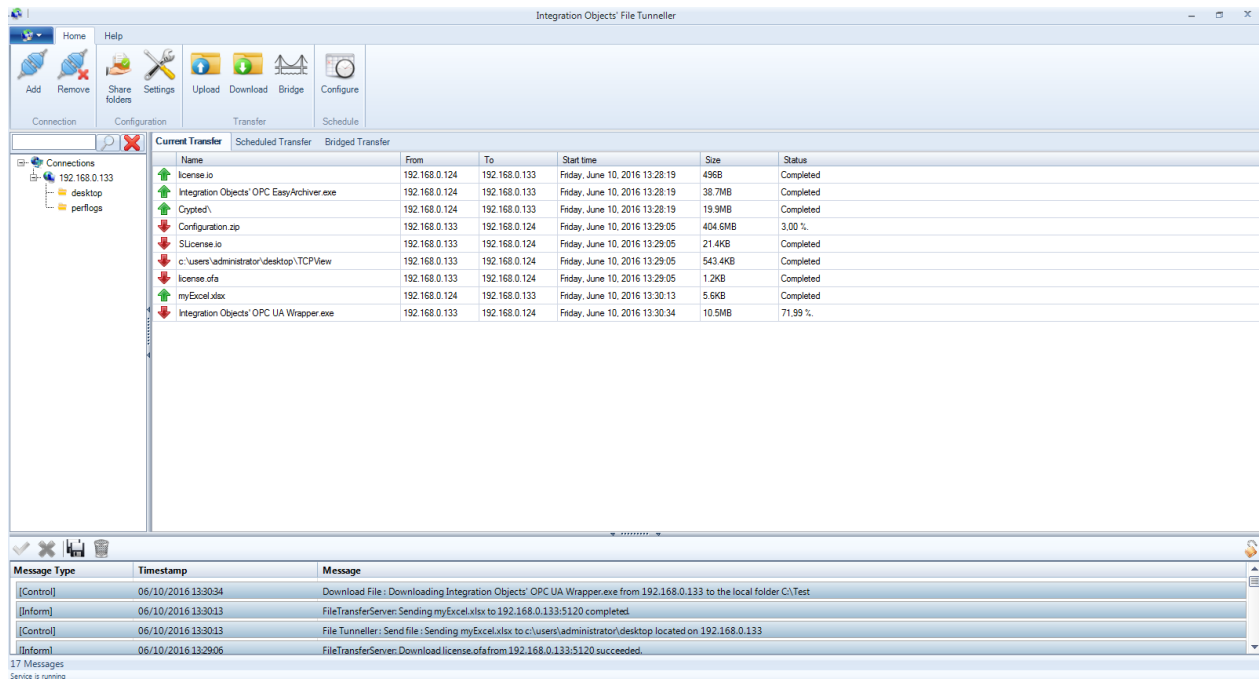


Figure 52: Current Transfer

You can clear the completed transfers by right clicking on the empty area in the **Current transfer** tab.

You can also check the file location by right clicking on the file as shown in the figure below:

Name	From	To
Integration Objects' OPC EasyArchiver.exe	192.168.0.24	192.168.0.148
OPCNet Broker.zip	192.168.0.24	192.168.0.148
Tag configuration.xlsx	192.168.0.24	192.168.0.148
Text.txt	192.168.0.24	192.168.0.148
LogFiles\	192.168.0.24	192.168.0.148
ONBClientDA_Log.log	192.168.0.148	192.168.0.24
ONBS_Log.log	192.168.0.148	192.168.0.24
OPCNet Broker Training.pdf	192.168.0.148	192.168.0.24
Copyright.png	192.168.0.24	192.168.0.148
KNet Analytics Setup.exe	192.168.0.148	192.168.0.24
archiverDatabase.accdb	192.168.0.148	192.168.0.24

Figure 53: Open Containing Folder

## 4. Step by Step Procedure to Use File Tunneller

When starting the main interface of the File Tunneller, and after logging into the application, you can see that the service is running and the graphical user interface has been successfully initialized.

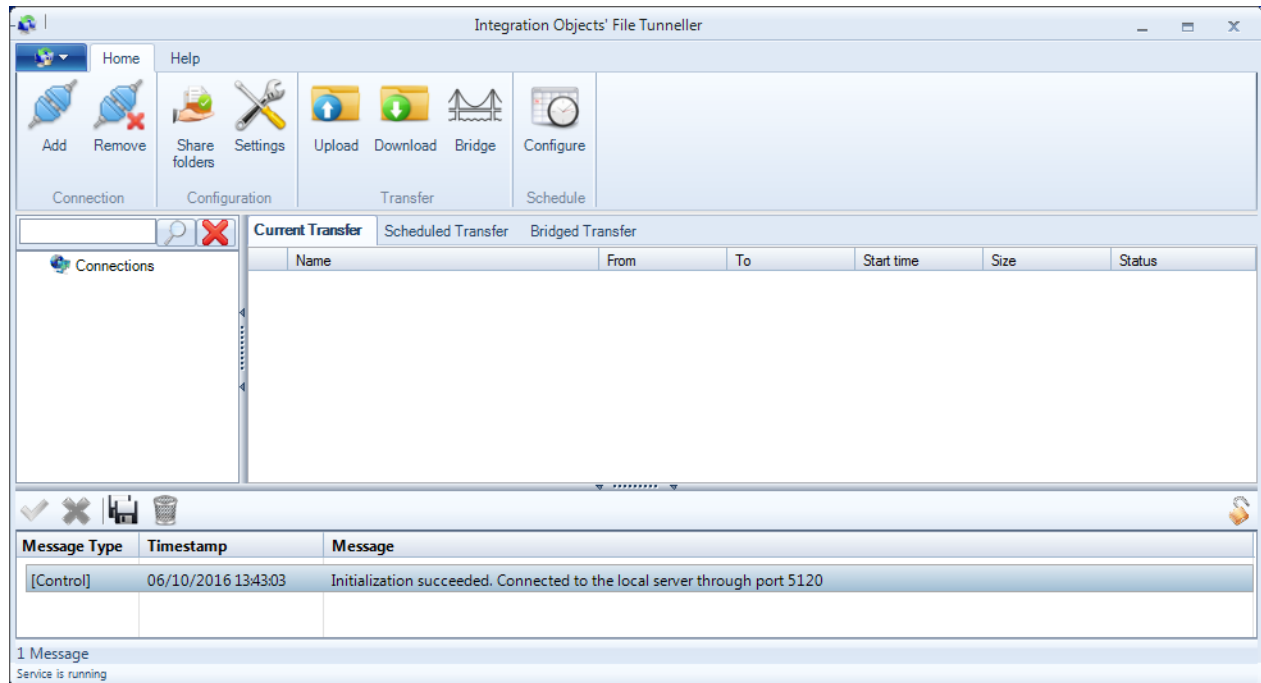
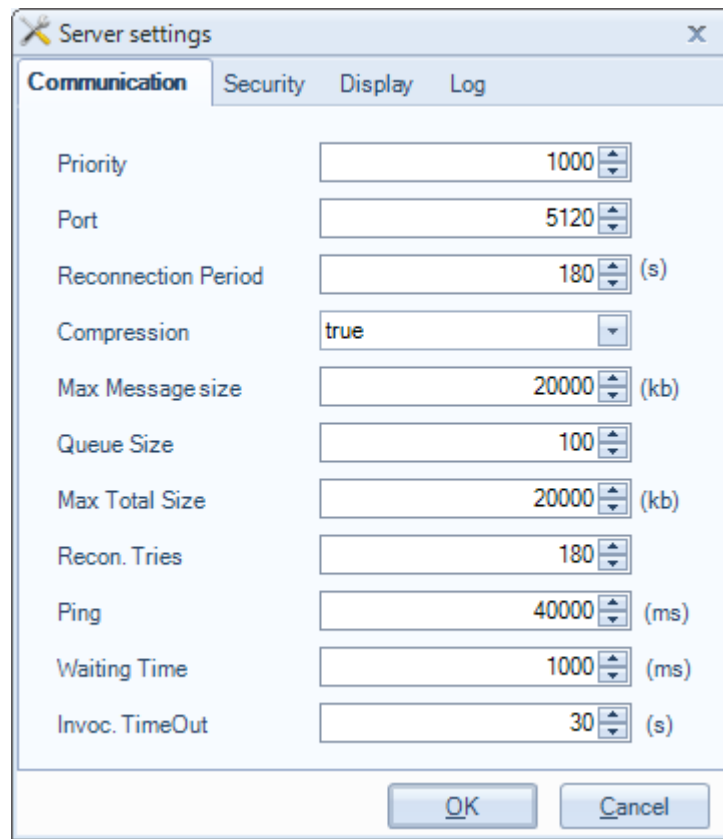


Figure 54: Main User Interface

First of all, if you are in the server machine, you need to configure the communication settings. Click on the **Settings** button, the following dialog shall appear:



**Figure 55: Server Settings**

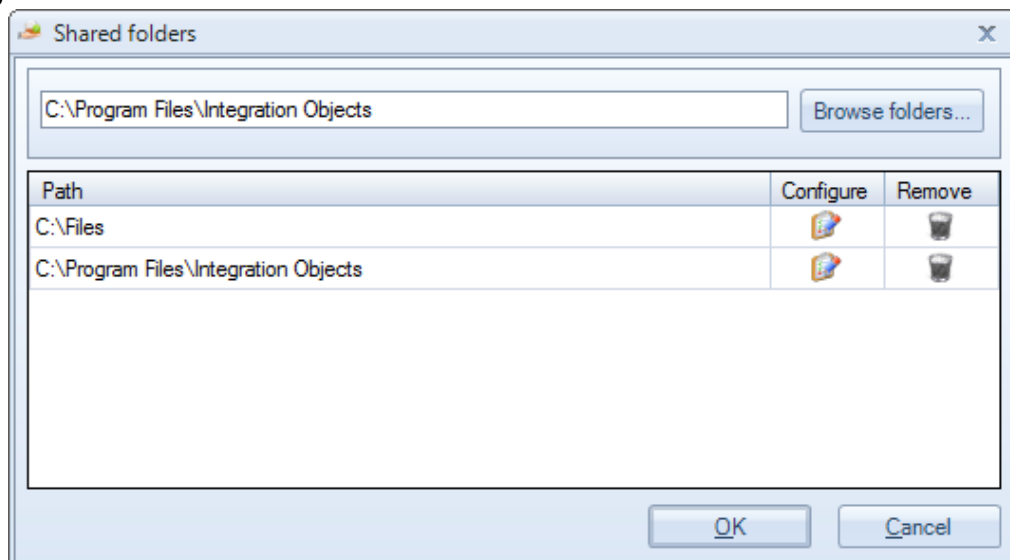
You can change these parameters to suit your needs. You can also modify the security mode you will be using for the remote communication by going to the security tab:





**Figure 56: Set Security Mode**

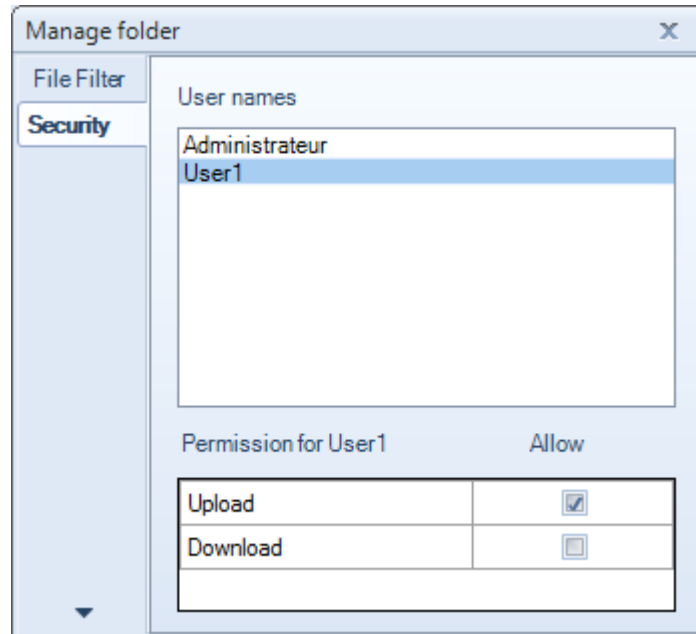
You need to select **Share Folders** button in the main user interface. To add folders, use the **Browse Folders** button or just copy/past the folder path in the appropriate field as shown in following tab:



**Figure 57: Configure Shared Folders**

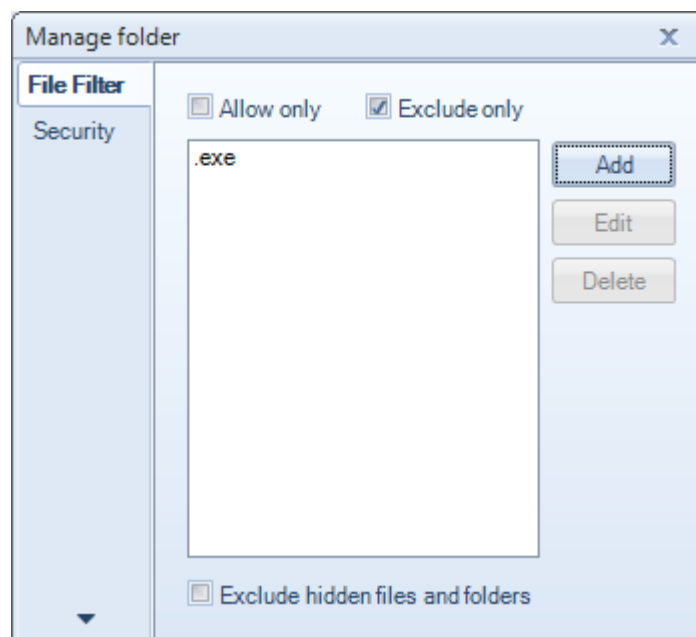
If you are using **With encryption and authentication** security mode, you should grant the configured users access rights to your shared folders to be able to exchange files.

To do so, click on the **Access rights** button in the main user interface, change and save the configuration as shown in the figure below:



**Figure 58: User's Access Rights**

You can also add your folder's file filter.



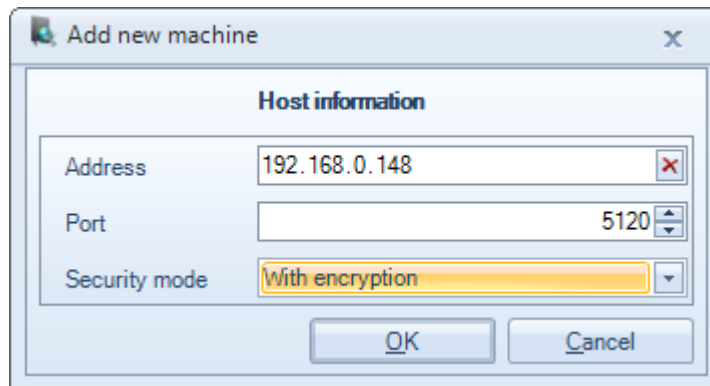
**Figure 59: Manage Filters**

The configuration of the server side is now completed.



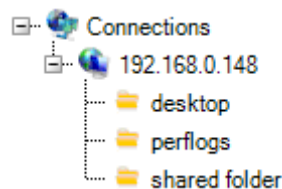
**Note that the File Tunneller acts as a server and client.**

From the client machine, select **Add**. You need to enter the IP address of the server side machine, the port and the security mode previously configured.



**Figure 60: Add New Connection**

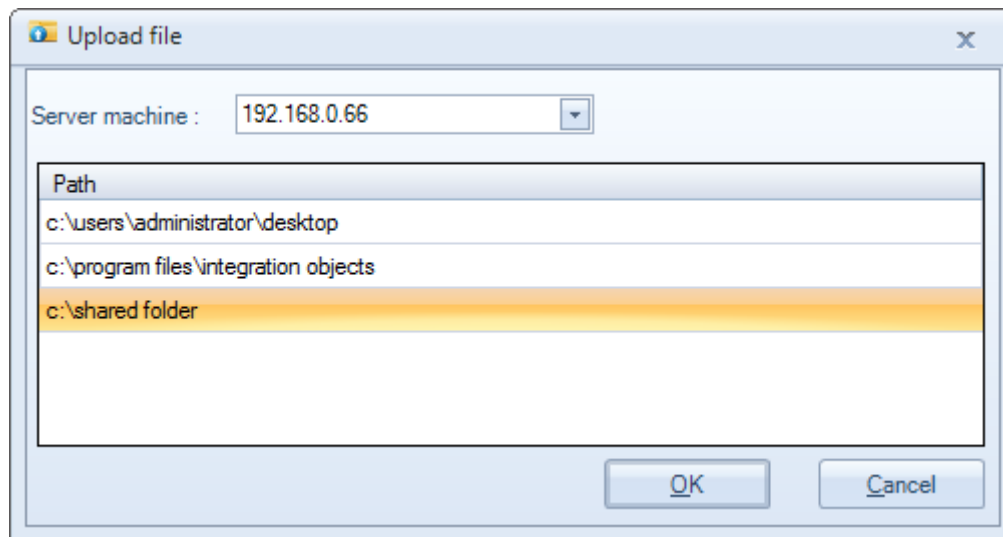
After establishing the connection, the server node along with its respective shared folders will be added to the connection tree view.



**Figure 61: Connections Tree View**

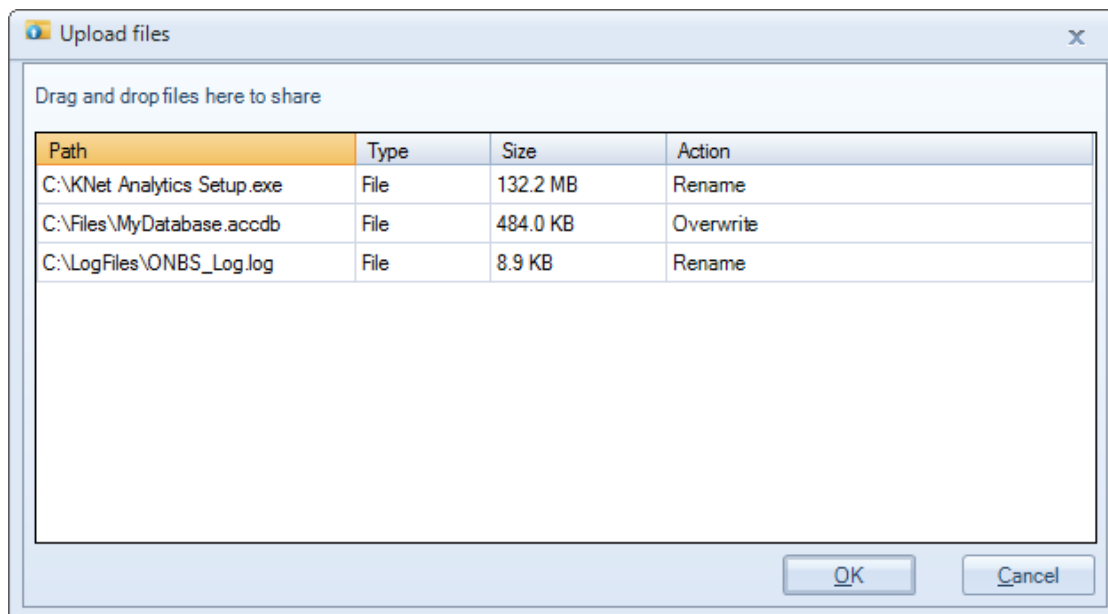
Now that the connection is established, you can download, upload and schedule files using the File Tunneller application.

When you select the upload option, you first need to set the destination folder.



**Figure 62: Choose Destination Folder**

After selecting the destination folder which is *c:\shared folder* in our case, you can add the files and folders you want to upload.

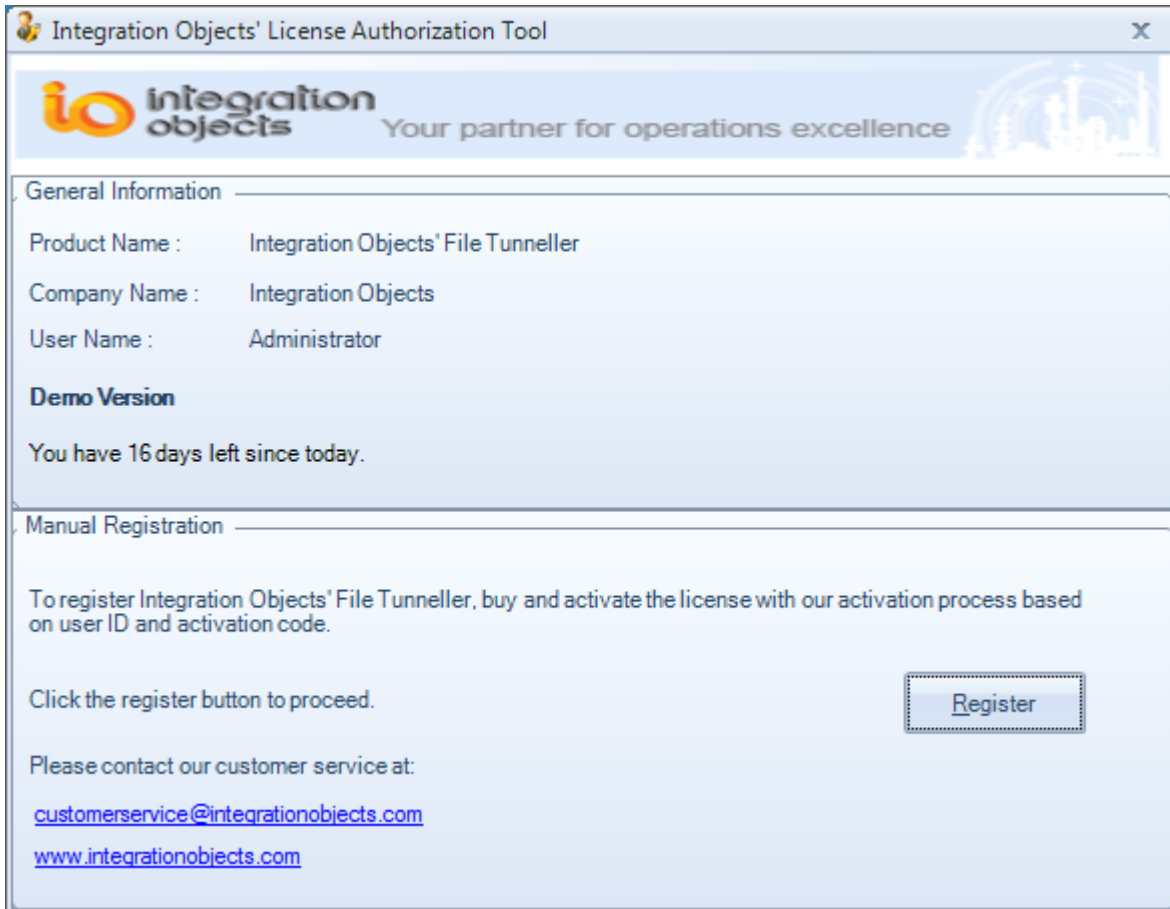


**Figure 63: Upload your Files**

## 5. License Authorization

Integration Objects provides a 16-day demo license by default allowing you to evaluate and test the product.

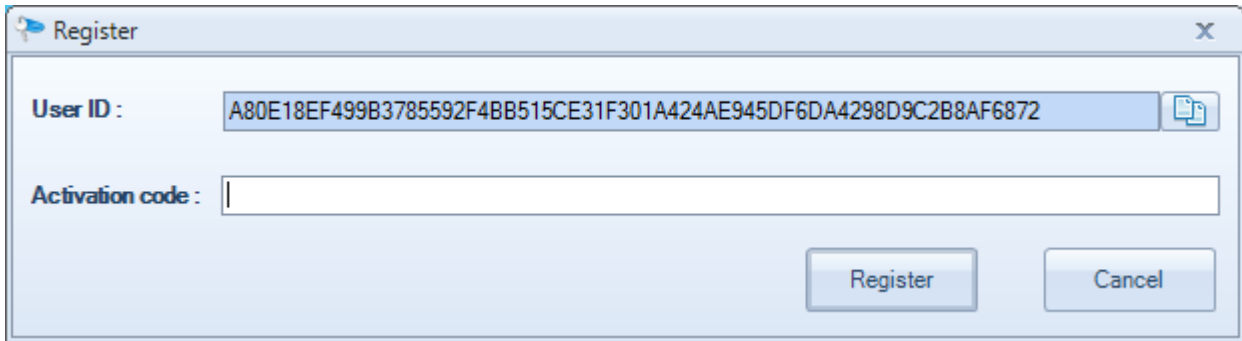
Once purchasing is completed, you need to register your license. Open the Integration Objects' License Authorization Tool from the start menu or the installation folder under the License management folder. The figure below will appear:



**Figure 64: License Authorization Tool**

In the company name and user name field you shall see the respective names that you have entered during the installation.

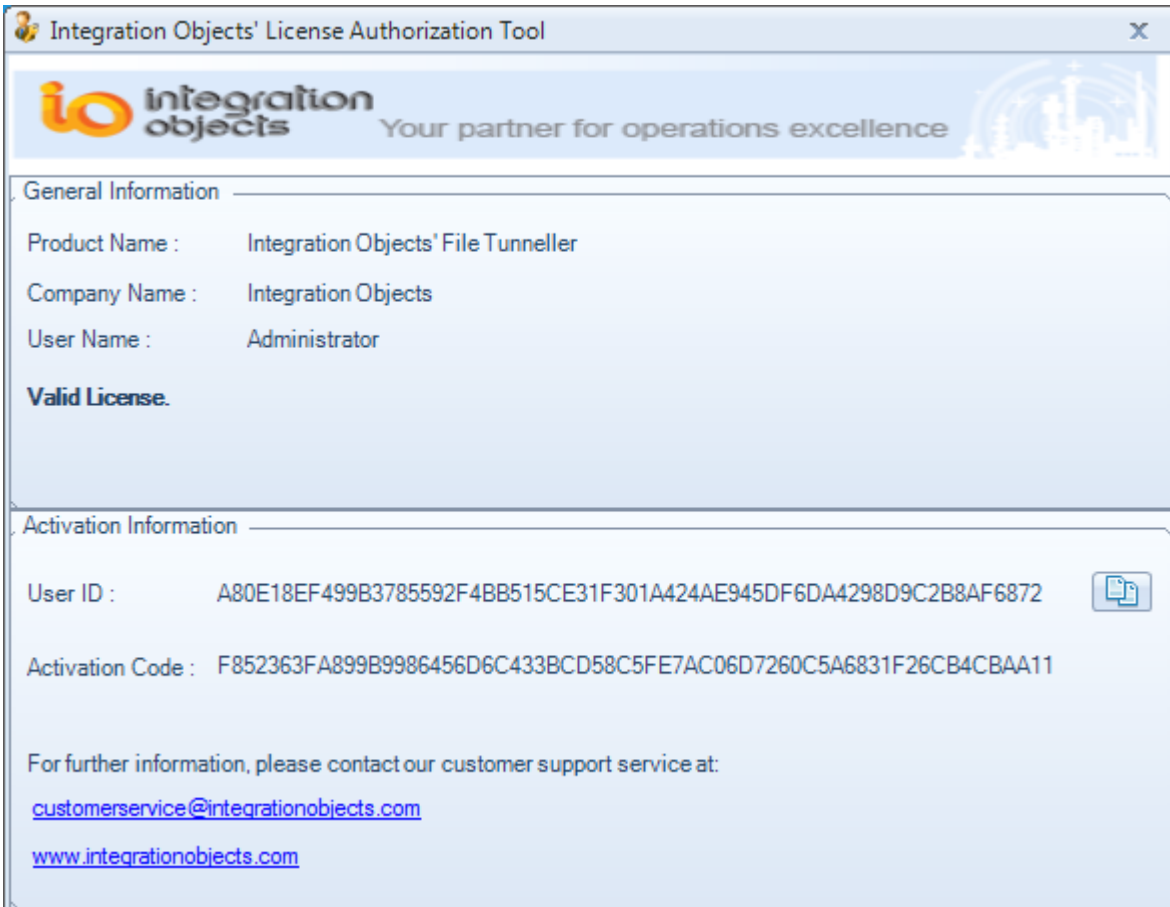
Now, click the **Register** button. The following registration dialog should appear:



The Registration Dialog window has a title bar with a minimize icon, a maximize icon, and a close icon. The main area contains two input fields: 'User ID' and 'Activation code'. The 'User ID' field is pre-filled with the alphanumeric string 'A80E18EF499B3785592F4BB515CE31F301A424AE945DF6DA4298D9C2B8AF6872' and has a copy icon to its right. The 'Activation code' field is empty. At the bottom right, there are two buttons: 'Register' and 'Cancel'.

**Figure 65: Registration Dialog**

To receive your activation key, copy the **User ID** then send it to Integration Objects' sales team and they will get back to you with the requested code.



The License Authorization Tool window has a title bar with a minimize icon, a maximize icon, and a close icon. The main area features the Integration Objects logo and tagline 'Your partner for operations excellence' at the top. Below this, there are two expandable sections: 'General Information' and 'Activation Information'. The 'General Information' section displays: Product Name: Integration Objects' File Tunneller, Company Name: Integration Objects, and User Name: Administrator. The 'Activation Information' section displays: User ID: A80E18EF499B3785592F4BB515CE31F301A424AE945DF6DA4298D9C2B8AF6872 (with a copy icon) and Activation Code: F852363FA899B9986456D6C433BCD58C5FE7AC06D7260C5A6831F26CB4CBAA11. At the bottom, there is a message: 'For further information, please contact our customer support service at: [customerservice@integrationobjects.com](mailto:customerservice@integrationobjects.com) [www.integrationobjects.com](http://www.integrationobjects.com)'.

**Figure 66: Valid Full License**

For additional information on this guide, questions or problems to report, please contact:

**Offices**

- Americas: +1 713 609 9208
- Europe-Africa-Middle East: +216 71 195 360

**Email**

- Support Services: [customerservice@integrationobjects.com](mailto:customerservice@integrationobjects.com)
- Sales: [sales@integrationobjects.com](mailto:sales@integrationobjects.com)

To find out how you can benefit from other Integration Objects products and custom-designed solutions, please visit our website [www.integrationobjects.com](http://www.integrationobjects.com).