



STCP OFTP Server Enterprise/Lite

Version 4.0.0

Content

About the STCP OFTP Server	4
OFTP (ODETTE File Transfer Protocol)	5
Where to use the STCP OFTP Server	5
Advantages	5
Technical Features	6
Software and Hardware requirements	6
How to configure the STCP OFTP Server	15
Configuration of the transfer interface of the STCP OFTP Server Enterprise/Lite for SSL3 communication	106
Directory structure	109
How to use the STCP OFTP Server	110
How to execute the STCP OFTP Server through the command line	111
Messages and Error Codes	112
Codes of events generated in the message file	113
General error codes	121
Transfer error codes of the Odette protocol	122
Session error codes of the Odette protocol	122
Transfer error codes	123
Generic error codes of the communication interface	124
Error codes of the TCP/IP (RAS) communication interface	124
Error codes of the TCP/IP communication interface	127
Error codes of the TCP/IP (Native Encryption) communication interface	129
Error codes of the X.25 communication interface	129
Error codes of the Serial communication interface	130
Error codes of the TCP/IP (Proxy) communication interface	131
Error codes of the TCP/IP (Encryption SSL3) communication interface	132
Audit file	134
Audit file format	135
Security	136
User application by the application (ODETTE ID)	137
Encryption	137
Message Digests	137

STCP OFTP Server

www.riversoft.com.br

Digital Signature	137
Certificate	138
Certification Authority (CA)	138
Secure Socket Layer (SSL)	138
Encryption in STCP OFTP Server	139
Native Encryption	139
SSL3 encryption in STCP OFTP Server	139
Architecture STCP OFTP Server	140
The supported algorithms in communication	140
Why OpenSSL implementation	144
OpenSSL License	145
References	148

About the STCP OFTP Server

About the STCP OFTP Server

The STCP OFTP Server is a safe file transfer Server for e-business and exchange of corporative trade information, based on the OFTP specification (ODETTE File Transfer Protocol).

OFTP (ODETTE File Transfer Protocol)

This protocol was specified by the Work Group number 4 of ODETTE (Organization for Data Exchange by Tele Transmission in Europe) in the 80's. The OFTP was developed to support the European Automotive Industry and to serve as a standard for the communication among different companies in the Supply-Chain.

OFTP was first specified under OSI model using network service recommended by CCITT X.25 standards.

ODETTE has incorporated the TCP/IP protocol due to the increase of OFTP use in different platforms (mainframes and PCs) by different sectors (banks, trade, governments, etc.).

Document RFC 2204 (Request for Comments) outlines the use of OFTP on TCP/IP networks.

Where to use the STCP OFTP Server

STCP OFTP Server can be used to:

- Information exchange
- Systems integration through file transferring
- Banking integration
- Shipping and Production Integration (Car Assembling Companies)
- Exchange of credit information (Trade Associations)
- Purchase Order Integration (Wholesalers)
- VANS integration
- Other applications

Advantages

STCP OFTP Server offers:

- Integration facility with existing applications
- Automation of files Sending/Receiving Process
- Task Scheduling
- Safe file transfer

- Compatible to products under OFTP (RFC2204) especification

Technical Features

STCP OFTP Server features:

- OFTP transfer protocol (ODETTE File Transfer Protocol)
- OFTP protocol authentication
- Authentication by Digital Certificate X.509 (SSL3)
- RSA, 3DES, DES, AES Cryptography (SSL3)
- Multiprotocol Communication TCP, SSL3, X.25, PAD and Dial-up
- Unlimited files transfer
- Audit Log Registers (billing) and events
- Recovery of interrupted transfer
- Communication via HTTP, SOCKS4 or SOCKS5 Proxy
- OFTP or GZIP standard compression
- Unlimited transfer sessions (Enterprise Version) or ten (10) transfer sessions (Lite Version)
- Unlimited number of users (Enterprise Version) or ten (10) users (Lite Version)
- Windows NT/2000/2003/XP compatible

Software and Hardware requirements

STCP OFTP Server requires:

- Processor 500MHz x86, x64 or superior
- 1Gb memory or superior
- 10 Mbytes Hard Disk space.
- CD-ROM Drive.
- Windows 2000/XP/2003/Vista/2008
- Net Open Wan Connect X.25*
- Database (SQL Server, MySQL, Oracle, Sybase, SQLite) **
- Driver ODBC to connect to Database

* Optional X.25 communication

** Optional

How to install the STCP OFTP Server

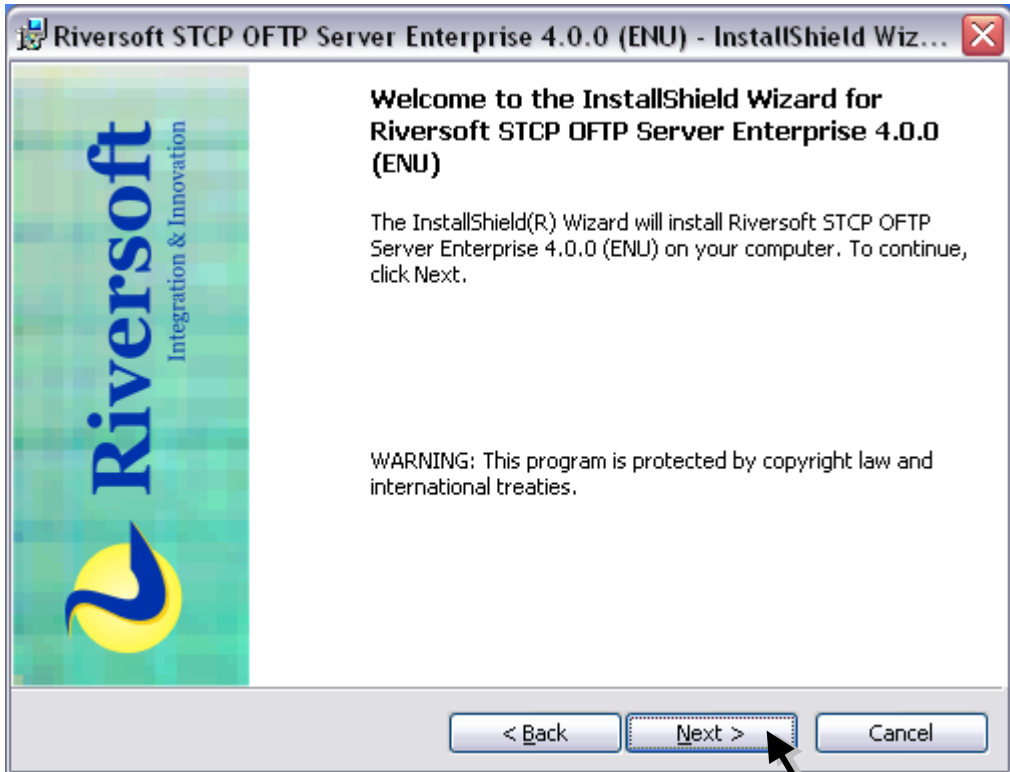
The STCP OFTP Server is distributed through a CD ROM, where SETUP.EXE program is found, the following steps must be executed to start installation:

1. Insert the CD media in the CD-ROM drive.
2. On **Start** menu choose the option **Execute**.
3. Use **Find** button, and select the CD-ROM unit.
4. Find and select **SETUP.EXE** file.
5. To run the program click the **OK** button.
6. The installation screen will be displayed.
7. This is the Welcome screen. To continue, click the **Next** button.



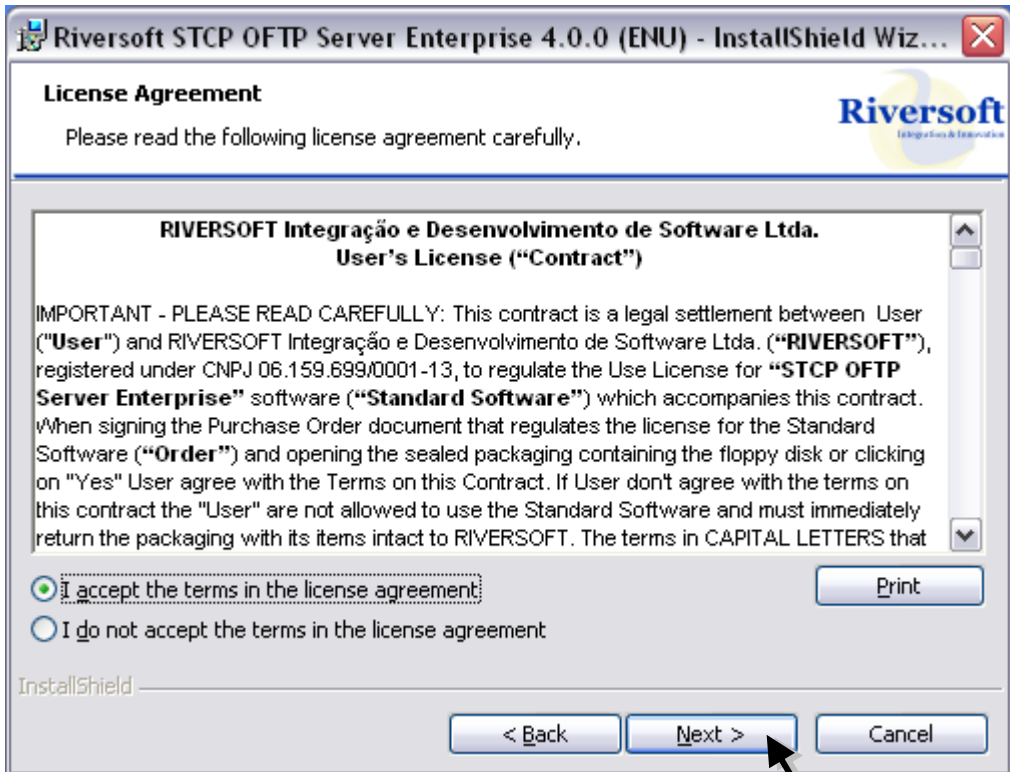
8. This is the Welcome screen, click the **Next** button to continue the installation.

Press **Back** to return to the previous screen or **Cancel** to stop the installation process.



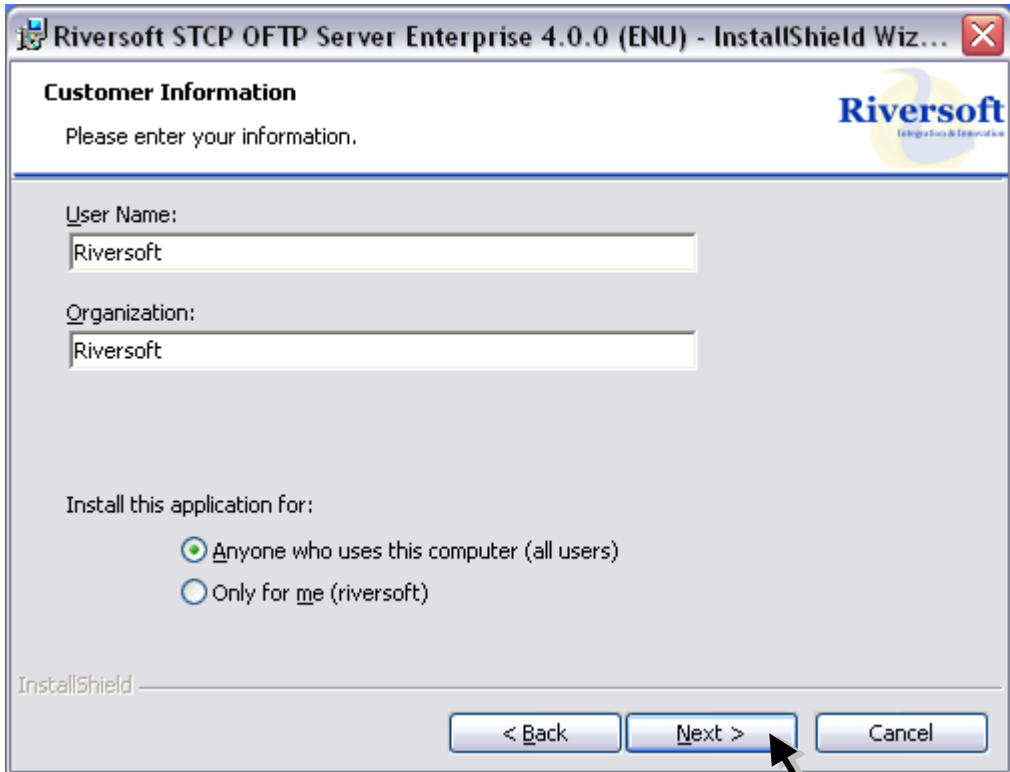
9. In this screen you should carefully read the Use License. If you agree with the contract terms, select **I agree** and click the **Next** button to continue the installation.

Press **Back** to return to the previous screen or **Cancel** to stop the installation process.



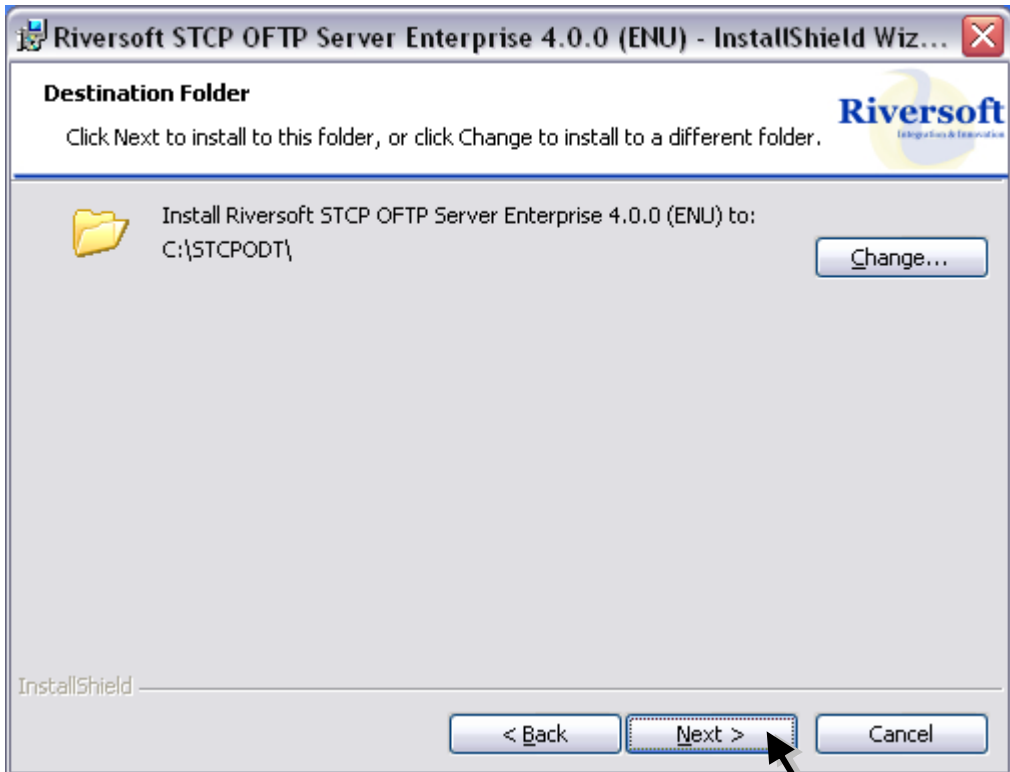
10. The **Customer Information** screen is displayed. You should inform the User Name and Organization.
11. Click the **Next** button to continue the installation

Press **Back** to return to the previous screen or **Cancel** to stop the installation process.



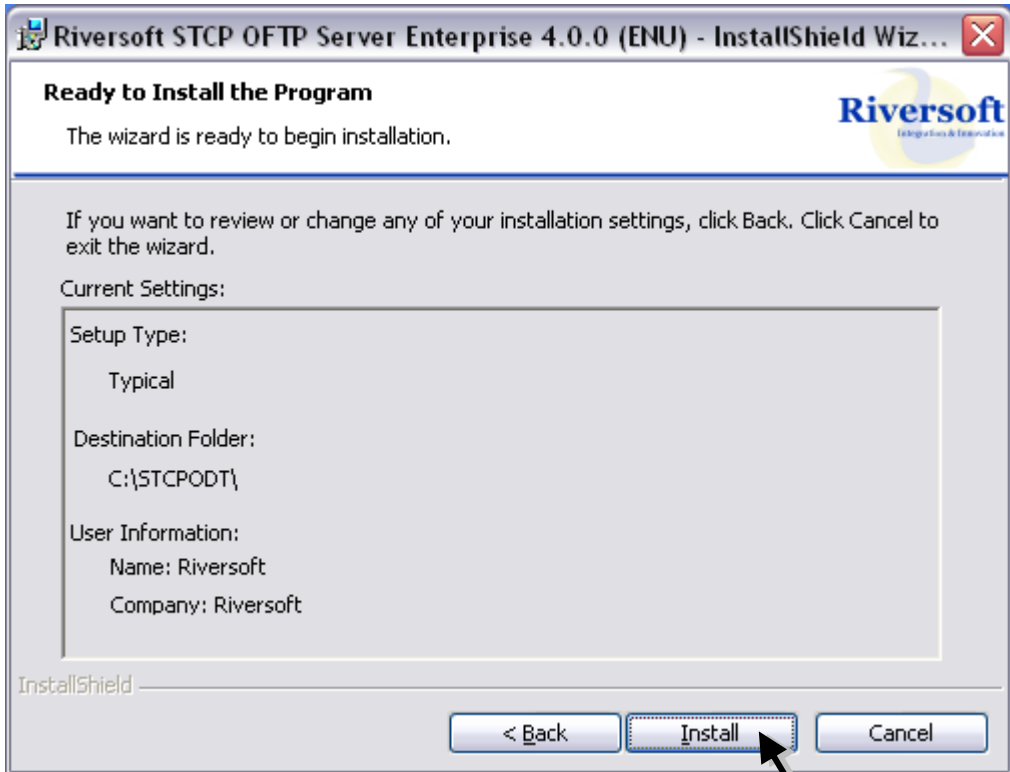
12. The screen **Destination Folder** is displayed. Click the **Next** button to install in the regular directory and click the **Change** button to select or create another directory.

Press **Back** to return to the previous screen or **Cancel** to stop the installation process.

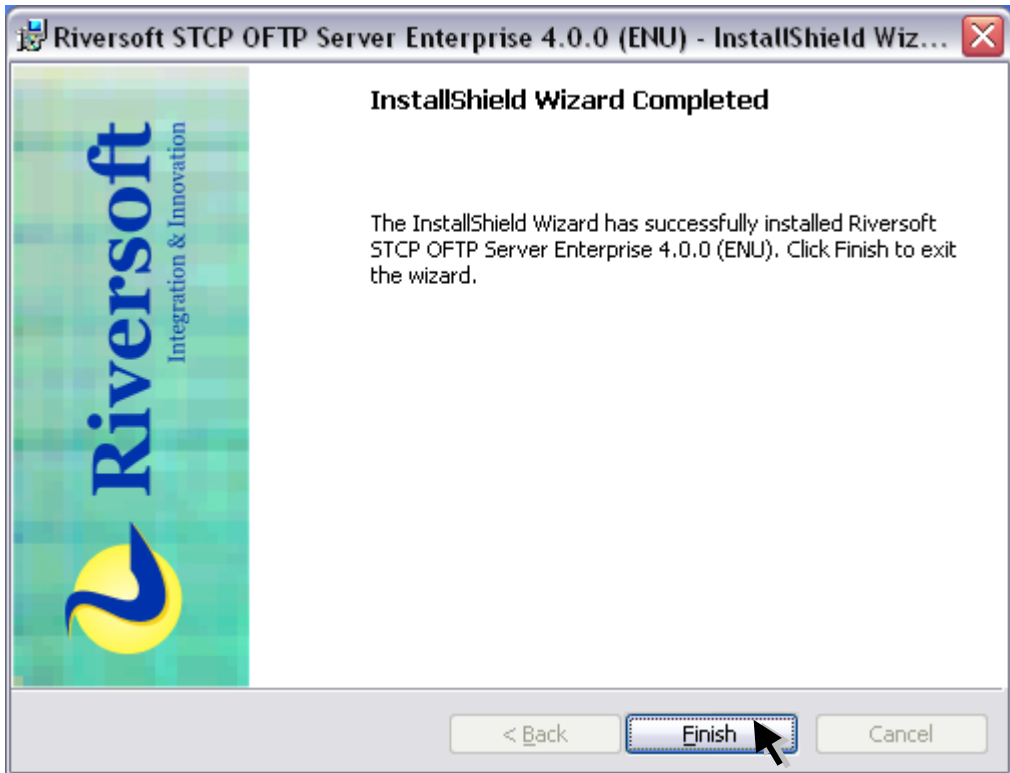


13. The screen **Ready to Install the Program** is displayed. Certify the configuration you chose is correct and click the **Install** button to continue the installation.

Press **Back** to return to the previous screen or **Cancel** to stop the installation process.



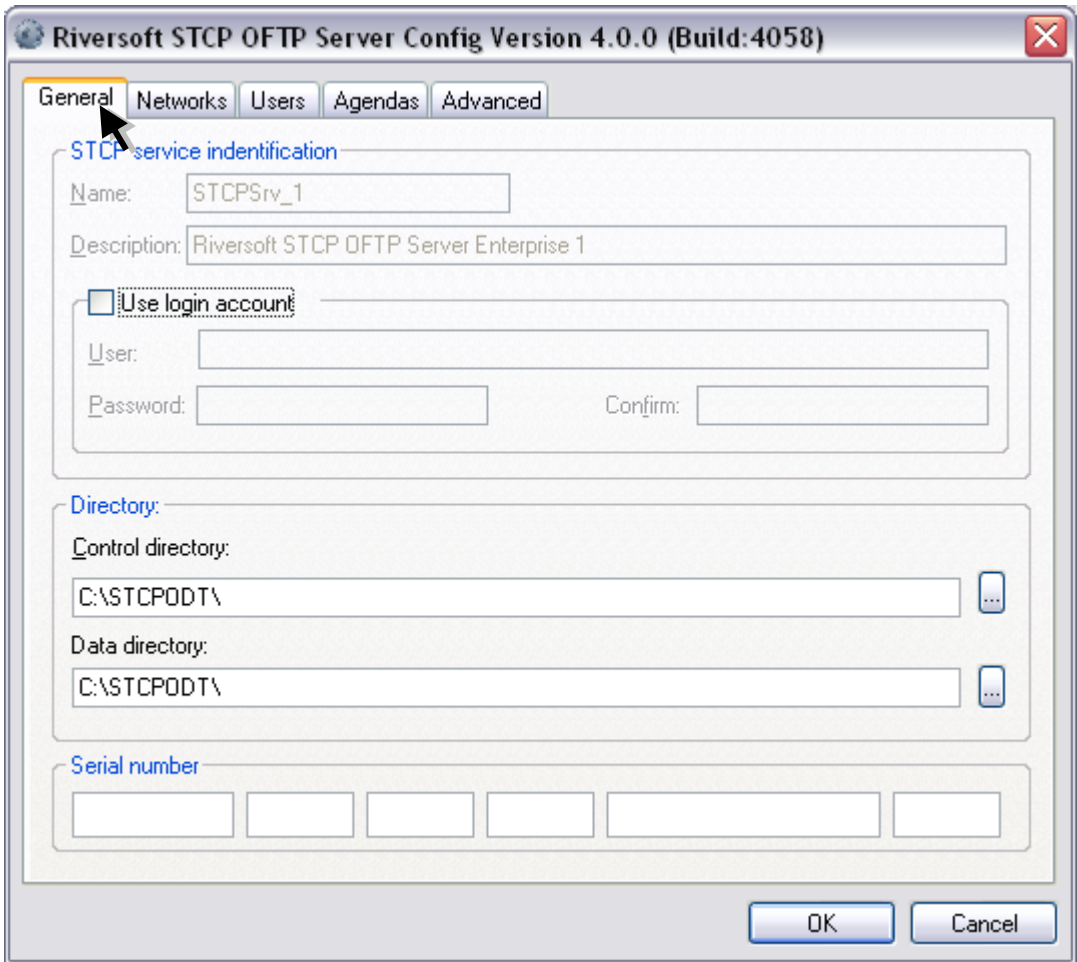
14. The screen **InstallShield Conclusion** is displayed. Click the **Finish** button to quit.



How to configure the STCP OFTP Server

The configuration program for STCP OFTP Server has been installed in the selected directory. Now it can be accessed through **Start** menu. If you have not modified yet the standard directory, follow the steps below:

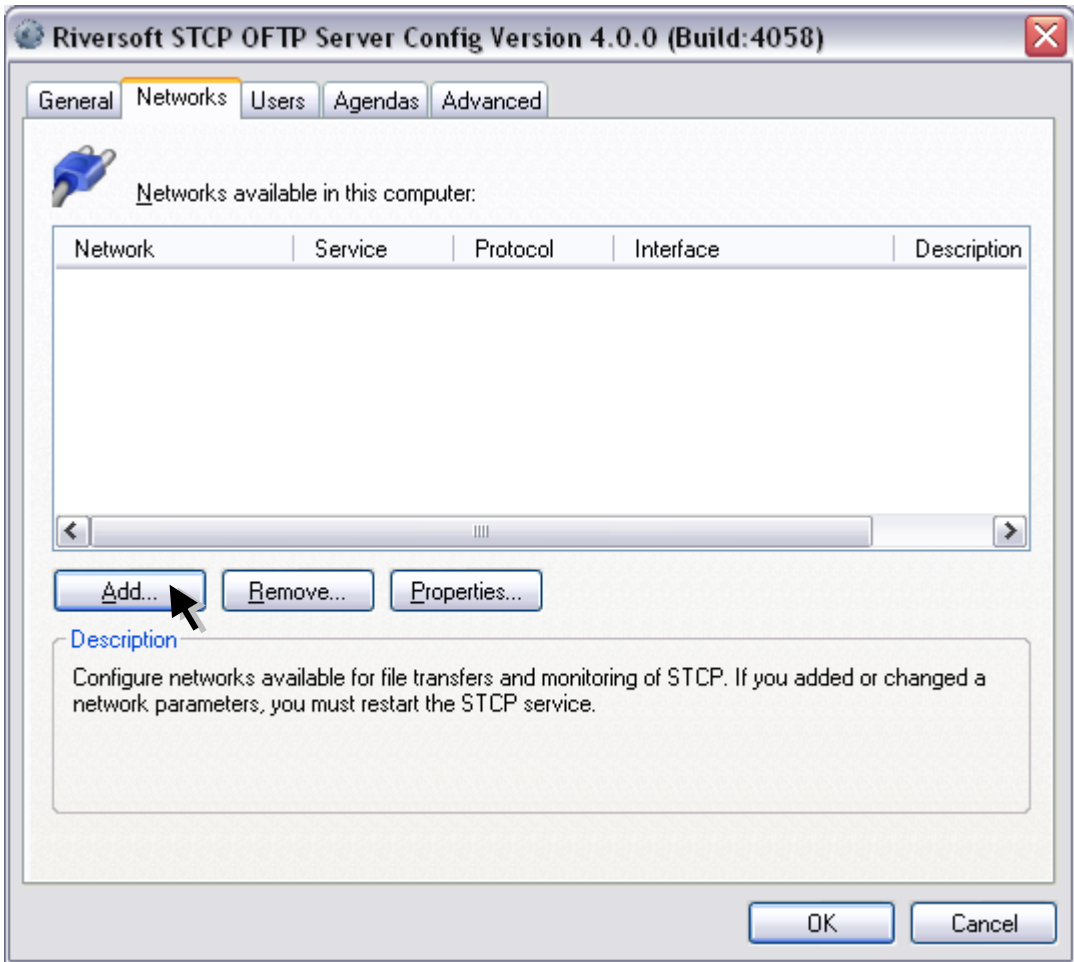
1. On **Start** menu, **All Files**, select **Riversoft STCP OFTP Server (Enterprise/Lite) 4.0.0**.
2. Click **Riversoft STCP OFTP Server Config**.
3. On the **General** tab, fill the fields with the information described below.



Fields	Description
Name	Inform the name of the STCP OFTP Server service.
Description	Inform the description of the STCP OFTP Server service.
Use login account	This option enables or disables the use of an operating system account by the service STCP OFTP Server. Note: Where the data directory selected is a network drive, this option should be enabled.
User	Fill this field with the user name to be used by the STCP OFTP Server service.

Password	Fill this field with the user password used by the STCP OFTP Server service.
Confirm	Fill this field with the user password to validate.
Control directory	Inform the installation directory name of STCP OFTP Server where user configuration, logs and communication debugging files. Note: For the version STCP OFTP Server, this parameter cannot be modified.
Data directory	Fill this tab with the directory name where the structure directory to send and receive files for each user should be created. Note: This configuration must be altered before creation of the users.
Serial number	Fill this tab with the serial number indicated on the Use license or on the CD case. Note: This field is required.

4. On the **Networks** tab you can add, remove or modify the parameters of the network interface controlled by the STCP OFTP Server service.
5. Press **Add** button.



STCP OFTP Server allows multiple network interface configuration with different communication protocols (**TCP/IP, SSL3, X.25, PAD, SERIAL** and etc.).

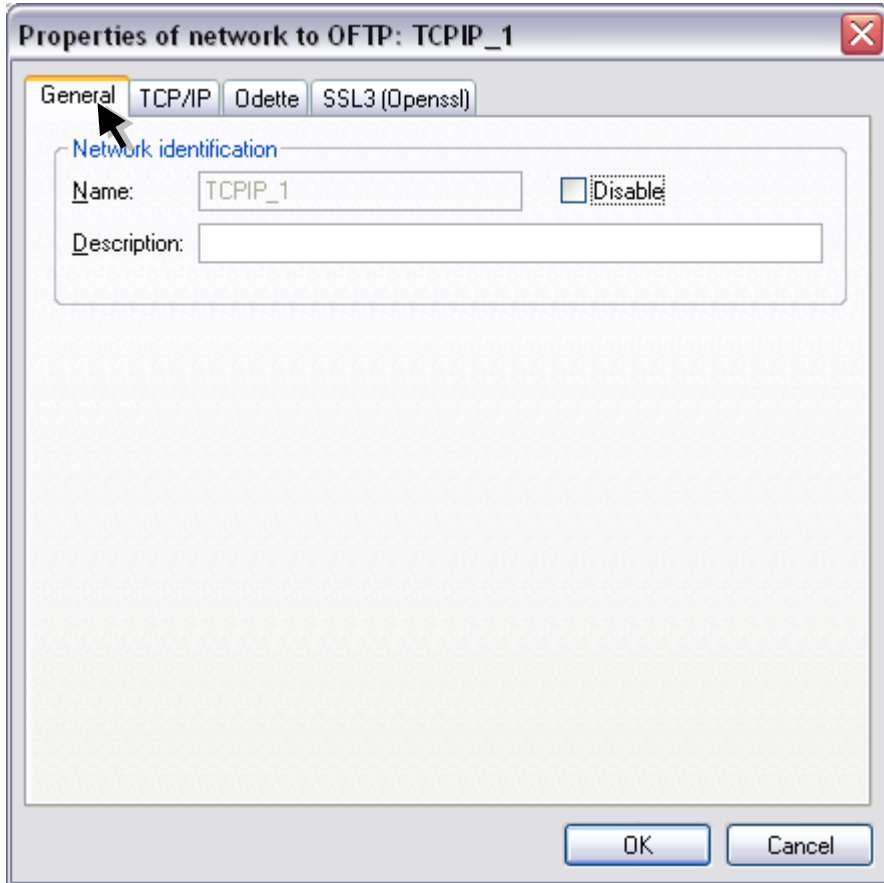
Note: Network configuration is used only for inbound connections.

6. Select a network service and press **OK** button.



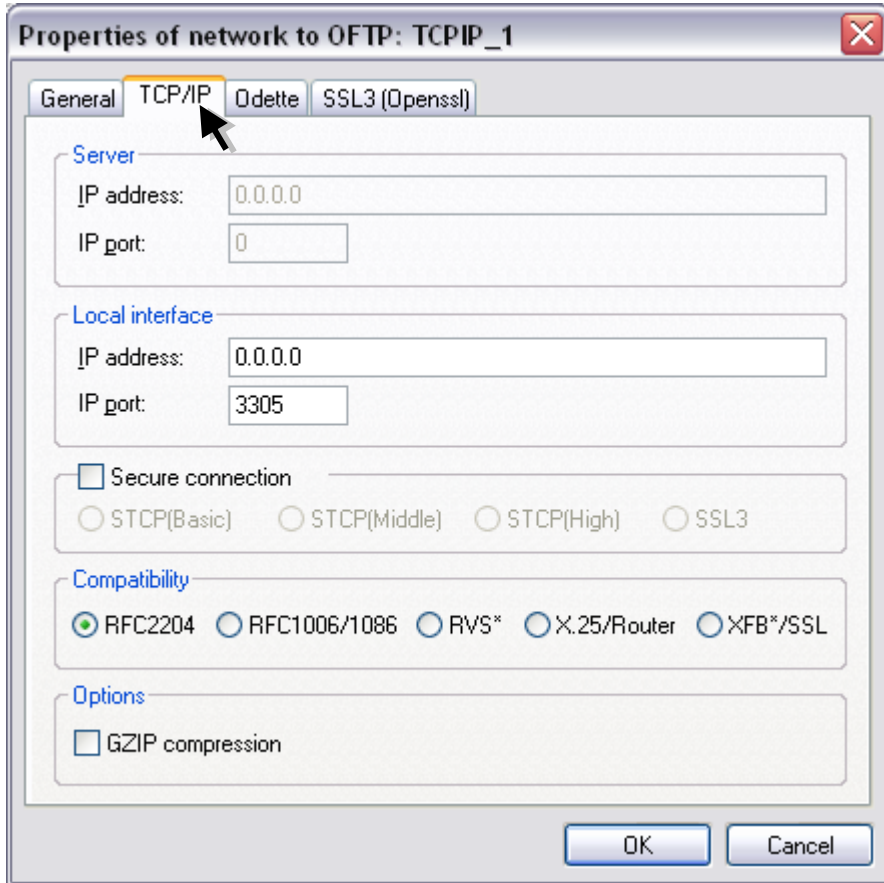
Protocol	Description
OFTP - TCP/IP	Configures the STCP OFTP Server to use the protocol of communication TCP/IP.
OFTP – X.25	Configures the STCP OFTP Server to use the protocol of communication X.25. Note: To use this option you must have installed a communication card WCK2000 provided by Net Open (www.netopen.com.br).
OFTP – SERIAL – DISCADO	Configures the STCP OFTP Server to use a serial port with a modem or a Fax /Modem card. Note: This option does not use TCP/IP protocol.
OFTP – PAD	Configures the STCP OFTP Server to use the protocol of communication PAD (X.28).
Monitor – TCP/IP	Enables the network for the STCP monitoring through the TCP/IP protocol.
Monitor X.25	Enables the network for the STCP monitoring through the X.25 protocol.
Monitor – SERIAL – DISCADO	Enables the network for the STCP monitoring through the SERIAL – DISCADO protocol.
Monitor - PAD	Enables the network for the STCP monitoring through the PAD protocol.
OFTP – SERIAL	Configures the STCP OFTP Server to use a serial port directly. Note: This option do not use protocol TCP/IP.

7. On the **General** tab fill the following configuration options for the protocol **OFTP – TCP/IP**.



Fields	Description
Name	Field with the name of the network interface configured.
Description	Fill this Field with the description of the network interface.
Disable	This option disables/enabled the network interface.

8. On the **TCP/IP** tab set the following options for the protocol OFTP - TCP / IP.

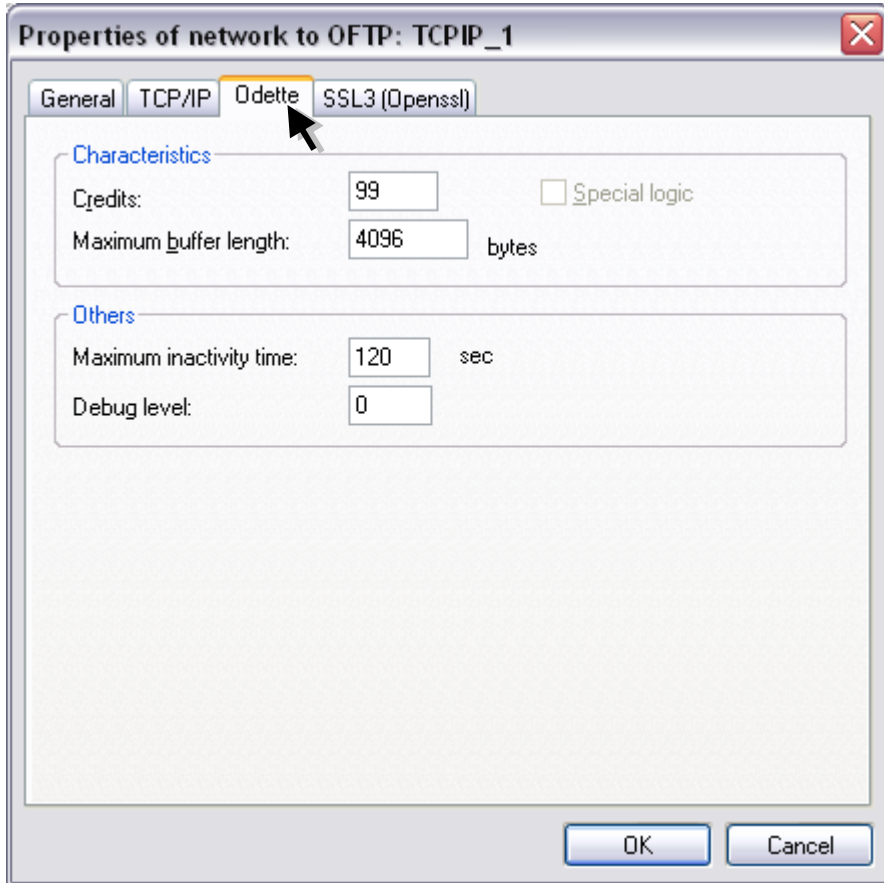


Fields	Description
IP Address	Fill this field with the TCP/IP address or name (DNS) of the local interface to which the STCP OFTP service must be available. Obs.: Use the address 0.0.0.0 to enable the service on all the network interfaces.
IP Port	Fill this field with IP port of the local interface to which the STCP OFTP Server service must be available. Note: The default port of the service is 3305.
Secure Communication	This option enables or disables the use of the encryption in communication with the STCP OFTP Server, you can choose between the option Native or SSL3. Note: Before you enable this option, read the chapter about Security.
Native (Basic)	Configures a secure communication with encryption basic level of security. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.

Native (Medium)	Configures a secure communication with encryption with medium level of security. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
Native (High)	Configures a secure communication with encryption with high level of security. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
SSL3	Sets a secure communication with encryption and digital certification, with the use of definite standard in RFC2246 (TLS1/SSL3). The TLS1/SSL3 is commonly found in servers of secure sites (HTTPS) and offers the highest level of security currently available. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
Compatibility	This option allows to compatible the STCP OFTP Server with different products currently on the market.
RFC2204	This compatibility option allows the communication of the STCP OFTP Server with other products that follow the RFC2204 recommendation.
RFC1006/RFC1086	This compatibility option allows the communication of the STCP OFTP Server through communication gateways TCP-IP/X.25, following the RFC1006/1086 recommendation.
RVS*	This compatibility option allows the communication of the STCP OFTP Server with the product RVS*. Note: This option should not be enabled when the server RVS* is a version of the mainframe (large).
X25/Router	This compatibility option allows the communication of the STCP OFTP Server through routers with support for X.25 communication via socket. Note: See Riversoft about this setting if you are in doubt.
XFB*/SSL	Enables the compatibility of the STCP with the XFB in SSL secure connections.
Compression GZIP	This option enables or disables the use of the compression GZIP on-the-fly (during the transfer). Note: Before you enable this option, confirm that the server you want to communicate supports this feature.

*** The trademarks are property of their respective owners.**

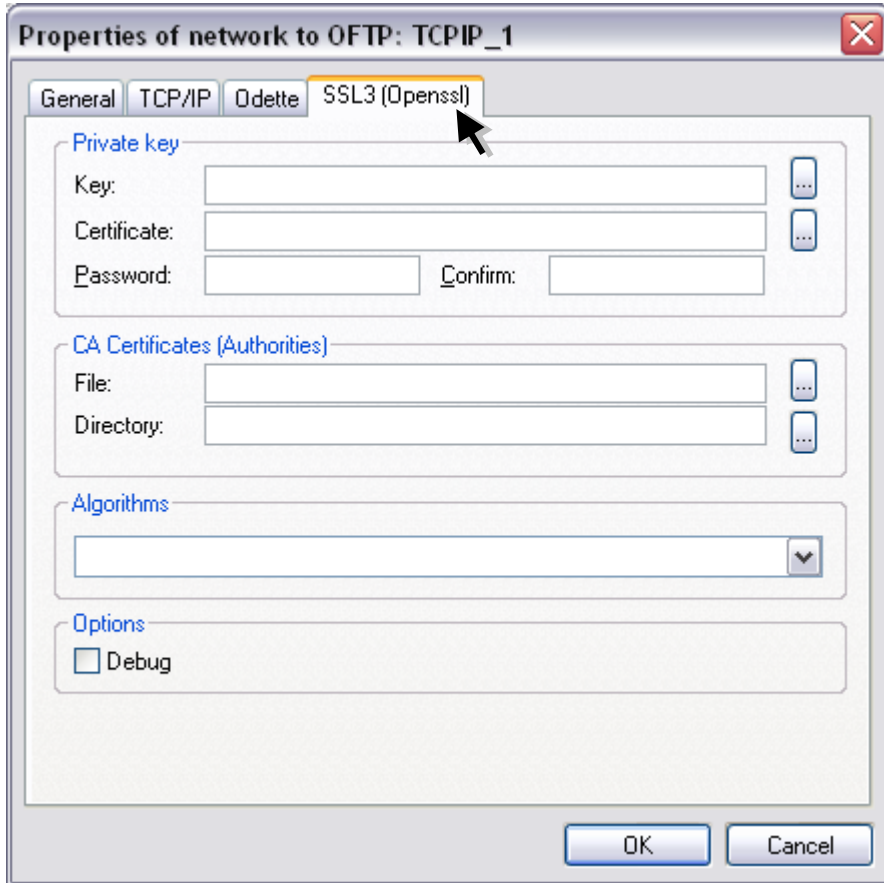
9. On the **Odette** tab set the following options for the protocol TCP-IP.



Fields	Description
Characteristics	The options defined in this group are used by STCP OFTP Server in communication with the server Odette. Note: Do not modify these features without reading carefully each of them and making sure you really want to do it.
Credits	Fill this field with the amount of data blocks to be transferred to wait a new permission to send. The valid range is 1 up to 99.
Special Logic	This option enables or disables the system control for special logic communication. This option should only be enabled for communication through the PAD or SERIAL protocol. Note: Do not enable this option when the PAD or SERIAL protocol is not used.
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is 1 up to 65535.
Others	The options defined in this group will be used locally by STCP OFTP Server to control the downtime and the file generation of communication debug.

Maximum inactivity time	Fill this field with the maximum downtime of communication between the STCP OFTP Server and the remote computer.
Debug level	Fill this field with the level of information details to be recorded in the debug file. To obtain the information of the different levels in the same debug file, please complete this field with the sum of desired levels. Note: See table of the debug levels on the configuration of users.

10. On the **SSL3** tab set the following options for the **OFTP – TCP/IP** protocol.

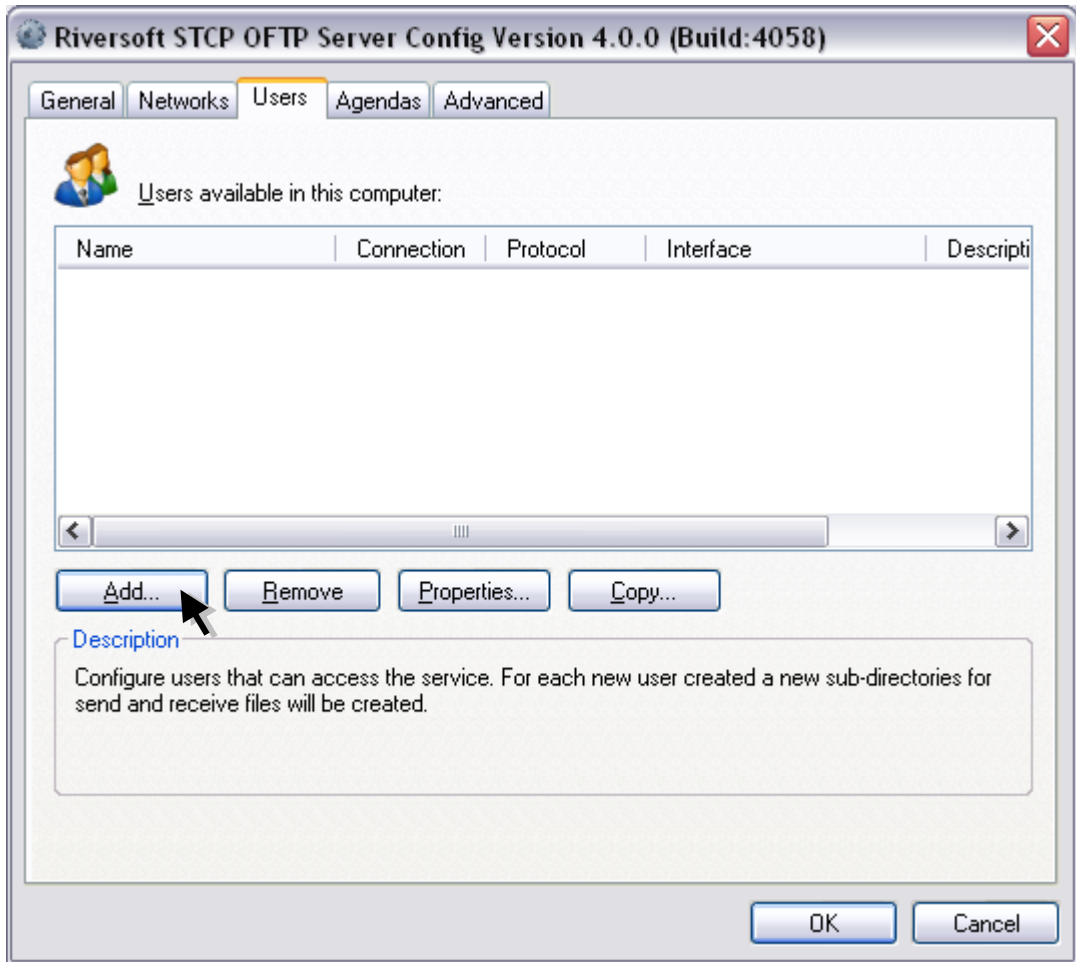


Fields	Description
Private Key	The options in this group are related to public and private keys, used by TLS1/SSL3 protocol for authentication and data encryption. Note: The file of private key must be in PKCS # 12 format and the certificates, in DER or PEM format.
Key	Fill this field with the file name (full path) where the private key is installed.
Certificate	Fill this field with the file name (full path) where the digital certificate (X509) is installed, associated with the private key.
Password	Fill this field with the password that protects the file of private key.
Confirm	Fill this field with the password supplied in the password field for validation.
Certificates CA (Authority)	The options in this group are related to digital certificates of certification authorities (CA) that will serve to validate the authenticity of the certificate presented by the Server. Note: The file of private key must be in PKCS # 12 format and the

	certificates, in DER or PEM format.
File	Fill this field with the file name (full path) where the digital certificate (X509) is installed containing the public key that signs the certificate presented by the server.
Directory	Fill this field with the directory name (full path) where the digital certificates (X509) are installed containing the public key that signs the certificate presented by the server.
Algorithms	Fill this field with the names of supported algorithms for digital signature, hashing, and data encryption. Note: If this field is not configured, TLS1/SSL3 the protocol is automatically selected. See also page 95.
Debug	This option allows generating a debug file in the Debug folder of the installation directory of the STCP.

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

11. On **Users** tab you can add, remove, modify or copy the configuration parameters of a STCP OFTP Server service user.
12. Click the **Add** button.



To a new user automatically a subdirectory structure for sending and receiving files will create within the **Data Directory** that was previously configured on the **General** tab.

13. Fill the fields with the information described below and click the **OK** button.



Add User

Identification

Name:

Password:

Confirm:

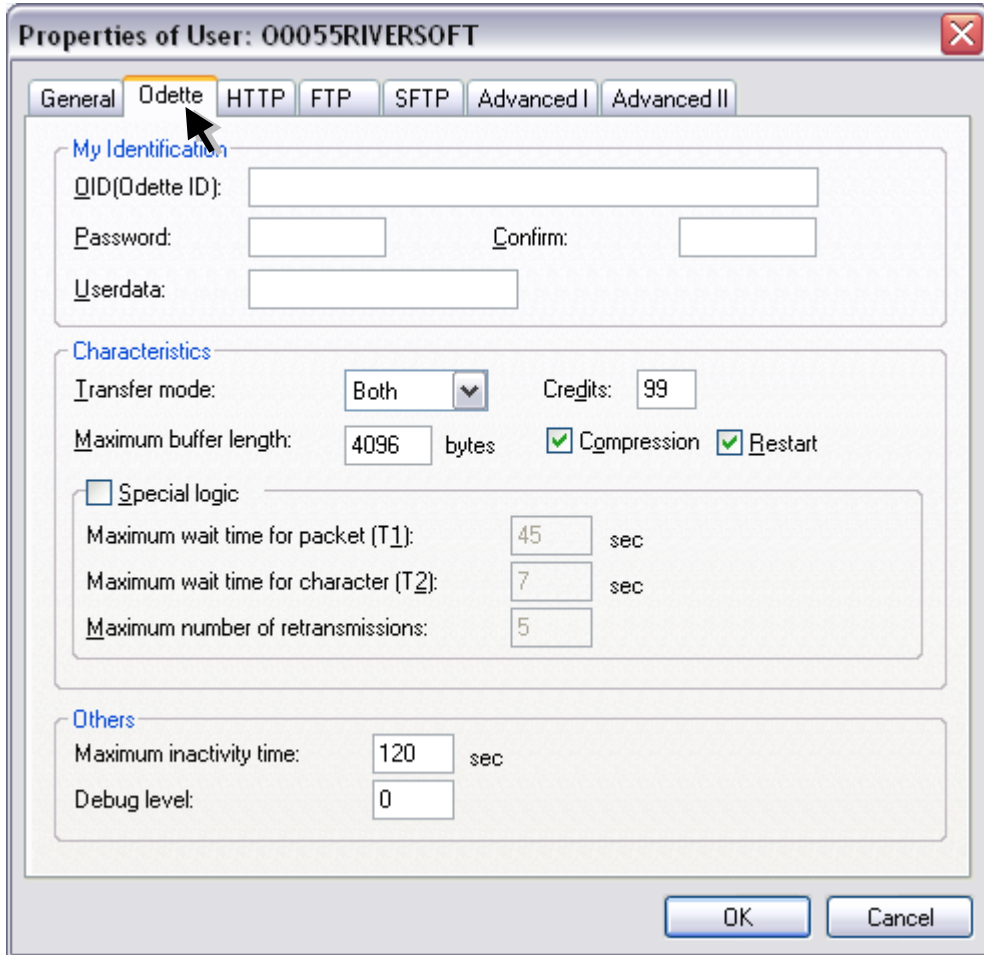
Description

The new user must be a partner for transfer.

Fields	Description
Name	Fill this field with the desired name for this User, which matches Odette ID (OID) of the partner. Note: Do not use special characters.
Password	Fill this field with the password associated with User. Note: Maximum size of eight (8) characters.
Confirm	Fill this field with the password associated with User for validation.
Description	Fill this field with the description of choice.

Press **OK** button to save the settings or **Cancel** to abandon without changing the settings.

14. On the **Odette** tab fill the fields with the information described below.



Fields	Description
OID (Odette ID)	Fill this field with the Odette ID associated with this User. This field can have a maximum of 25 (twenty five) characters.
Password	Fill this field with the password associated with the Odette ID. This field can have a maximum of eight (8) characters.
Confirm	Fill this field with the typed password in the Password field for validation.
Userdata	Fill this field with the extra data associated with Odette ID informed. Note: Complete this field only if requested by the server.
Characteristics	The options defined in this group are used by STCP OFTP Server in the communication with the server Odette. Note: Do not modify these features without carefully reading each of them and making sure you really want to do it.
Transfer mode	This option allows selecting the transfer mode to be used for

communication with the server, they are: Both (transmit and receive files), Sender (only file transmission) and Receiver (only receiving files).

Credits	Fill this field with the amount of data blocks to be transferred to wait a new permission for transfer. The valid range is 1 up to 99.
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is 1 up to 65535.
Compression	This option enables or disables the data compression (default Odette) of a transfer.
Restart	This option enables or disables the control of automatic recovery in an interrupted transfer. With this option enabled, the STCP OFTP Server will retrieve the transfer of the breakpoint.
Special Logic	This option enables or disables the system control for special logic communication. It should only be enabled for communication via the protocol PAD or SERIAL. Note: Do not enable this option when the protocol PAD or SERIAL is not used.
Maximum waiting time of packet (T1)	Maximum time to detect timeout of process.
Maximum waiting time of character (T2)	Maximum time to detect errors in the reception of individual characters.
Maximum number of retransmissions	Maximum number of retransmissions using the system control for special logic communicating.
Others	The options defined in this group will be used locally by STCP OFTP Server to control the timeout and file generation of debug communication.
Maximum inactivity time	Fill this field with the maximum timeout for communication between the STCP OFTP Server and the remote computer.
Debug level	Fill this field with the level of details of information to be recorded in the debug file. To obtain the information of the different levels in the same debug file, please complete this field with the sum of desired levels.

For each connection attempt, a new file in the subdirectory DEBUG will be created, with the following syntax:

ODTDEB.<Protocol>.<User>.YYMMDDhhmmssnnn.

Protocolo	TCPIP, X25, SERIAL ou PAD
Usuário	Filename used
YYYY	Year
MM	Month
DD	Day
hh	Hour
mm	Minute

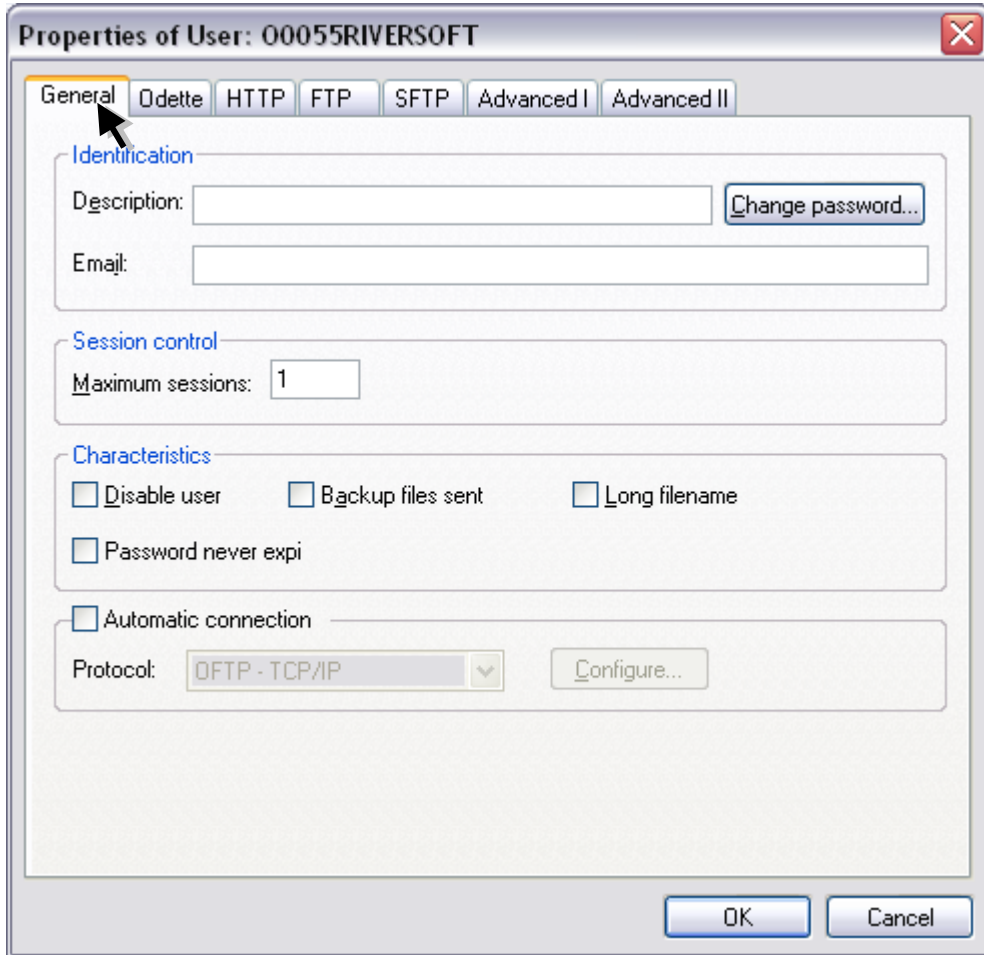
ss	Seconds
nnn	Milliseconds

The following table contains the relationship between the level of detail and information that will be generated.

Level	Description
0	It does not save the debug file.
1	It saves in and out information of subroutines.
2	It saves information of changes of the protocol state.
4	It saves information of the packets received and sent, formatted by field.
8	It saves information of the packets received and sent, formatted in hexadecimal.
16	It records information of the events.
32	It writes information from underreporting.

Note: Only enable this option when prompted by specialized personnel.

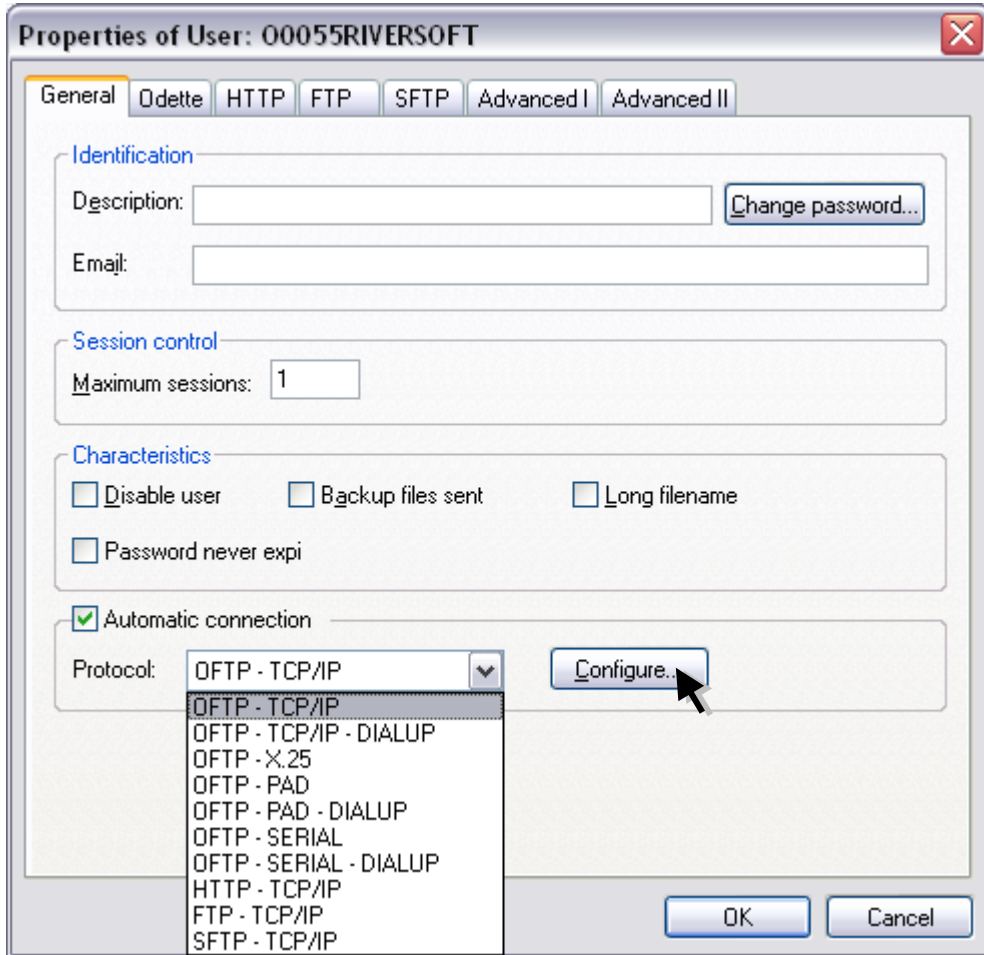
15. On the **General** tab set the following options.



Fields	Description
Description	Fill this field with the description of your choice.
Change password	This option allows you change the password of User created.
Email	This email should be linked to Mailbox and serves for the notification system.
Maximum sessions	This field reports the maximum number of simultaneous sessions of transfer can be activated.
Disable user	This option disables temporarily this User to perform the transfer operations when checked.
Backup files sent	This option enables or disables temporarily this User to move the files successfully transmitted to the backup subdirectory. Note: The files moved to the backup directory contain an extension at the end of the name with the following feature: YYYYMMDDHHMMSS, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm is the seconds of the end of

	transfer.
Long filename	This option enables or disables temporarily this User to transfer files with name longer than 26 (twenty six) positions. Note: Do not enable this option if you are not absolutely sure that the remote partner is another STCP OFTP Server and is also with this feature enabled.
Password never expires	This option prevents the password expires.
Automatic connection	This option enables or disables that this User can start a connection.
Protocol	This field selects the type of communication protocol that this User will use to connect. Once selected, press the Configure button to access the screen of specific configuration of the communication protocol.

16. Select the option of **Protocol** desired and click the **Configure** button.



Protocol	Description
OFTP - TCP/IP	Sets the STCP OFTP Server to use the TCP/IP communication protocol through a local network.
OFTP - TCP/IP - DISCADO	Sets the STCP OFTP Server to use the TCP/IP communication protocol through a dial-up access network (dial-up).
OFTP - X.25	Sets the STCP OFTP Server to use the X.25 communication protocol through a dedicated access network. Note: To use this option, you must have installed a WCK2000 communication card provided by Net Open (www.net-open.com.br).
OFTP - PAD	Sets the STCP OFTP Server to use the PAD (X.28) communication protocol through a dedicated access network.
OFTP - PAD - DISCADO	Sets the STCP OFTP Server to use the PAD (X.28) communication protocol through a dial access network.
OFTP - SERIAL	Sets the STCP OFTP Server to use straight a serial port

Note: This option do not use TCP/IP protocol.

OFTP – SERIAL – DISCADO	Sets the STCP OFTP Server to use a serial port with a modem or Fax/Modem card.
-------------------------	--

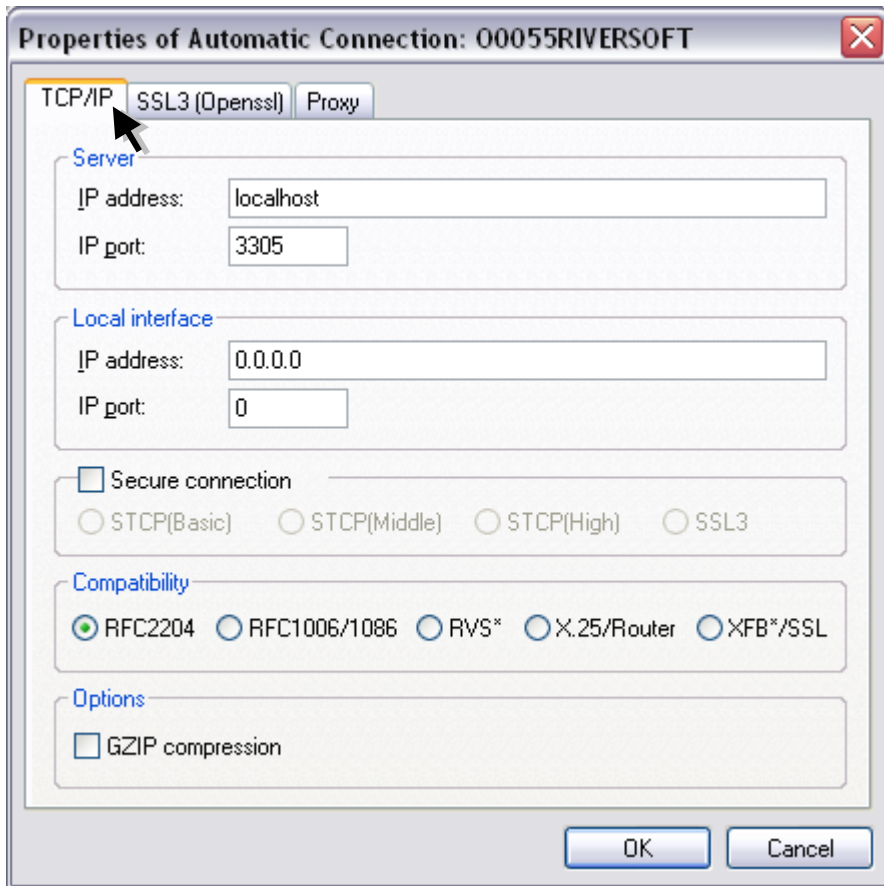
Note: This option do not use TCP/IP protocol.

HTTP – TCP/IP	Sets the STCP OFTP Server to use the HTTP communication protocol.
---------------	---

FTP – TCP/IP	Sets the STCP OFTP Server to use the FTP communication protocol.
--------------	--

SFTP – TCP/IP	Sets the STCP OFTP Server to use the SFTP communication protocol.
---------------	---

17. If the protocol selected is **OFTP – TCP/IP**, set the following options on the **TCP/IP** tab.

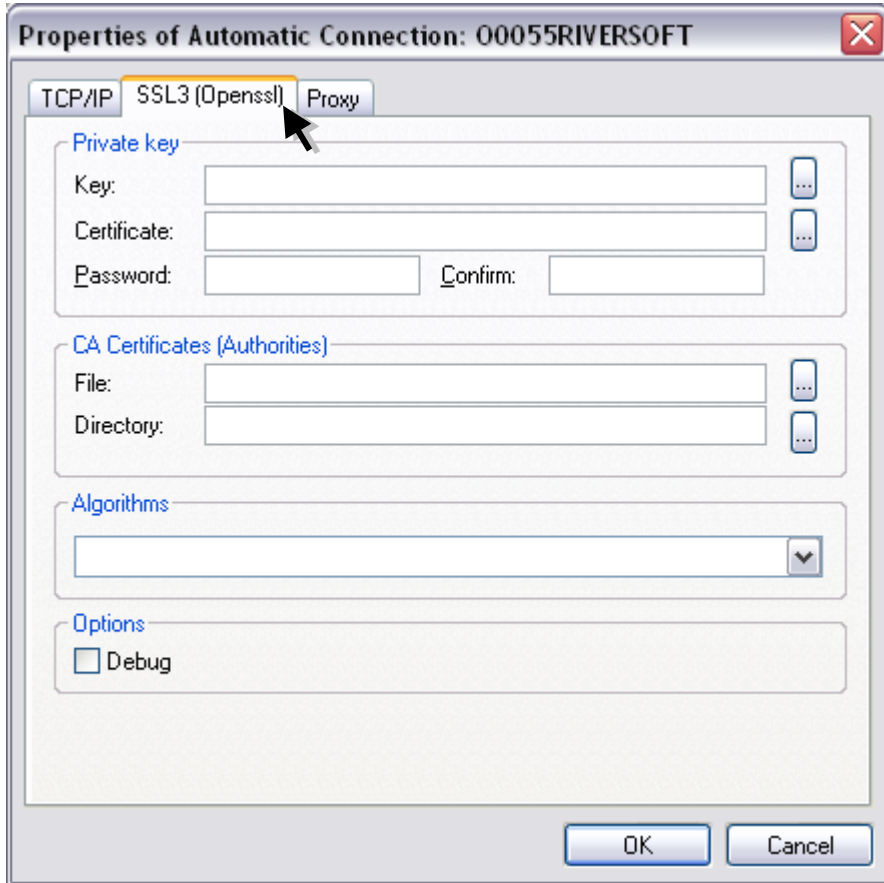


Fields	Description
IP address	Fill this field with the TCP/IP address or name (DNS) of the server STCP OFTP Server.
IP port	Fill this field with the TCP/IP port of the STCP OFTP Server.
Secure connection	This option enables or disables the use of encryption in communication with the STCP OFTP Server. You can choose between the Native option and SSL3. Note: Before you enable this option, read the chapter about Security.
STCP (Basic)	Sets the secure communication with encryption of basic security level. Note: Before you enable this option, confirm if the server you want to communicate supports this feature.
STCP (Middle)	Configura a comunicação segura com criptografia com nível de segurança médio. Sets secure communication with encryption of medium security level.

Note: Before you enable this option, confirm if the server you want to communicate supports this feature.

STCP (High)	Sets secure communication with encryption of high security level. Note: Before you enable this option to confirm if the server you want to communicate supports this feature.
SSL3	Sets secure communication with encryption and digital certification, using the standardization defined in RFC2246 (TLS1/SSL3). The TLS1/SSL3 is commonly found in servers of secure sites (HTTPS) and offers the highest level of security currently available. Note: Before you enable this option to confirm if the server you want to communicate supports this feature.
Compatibility	This option allows to compatible the STCP OFTP Server with different products currently on the market.
RFC2204	This compatibility option allows the communication of STCP OFTP Server with other products that follow the RFC2204 recommendation.
RFC1006/RFC1086	This compatibility option allows communication of STCP OFTP Server through TCP-IP/X.25 communication gateways that follow the recommendation RFC1006/1086.
RVS*	This compatibility option allows communication of STCP OFTP Server with the RVS* product. Note: This option should not be enabled when the RVS * server is a version of the mainframe (large). * The trademarks are property of their respective owners.
X25/Router	This compatibility option allows the communication of STCP OFTP Server through routers with support for X.25 communication via socket. Note: See Riversoft about this setting if you are in doubt.
XFB*/SSL	Enables the compatibility of the STCP with the XFB in SSL secure connections.
Compresion GZIP	This option enables or disables the use of GZIP compression on-the-fly (during transfer). Note: Before you enable this option to confirm if the server you want to communicate supports this feature.

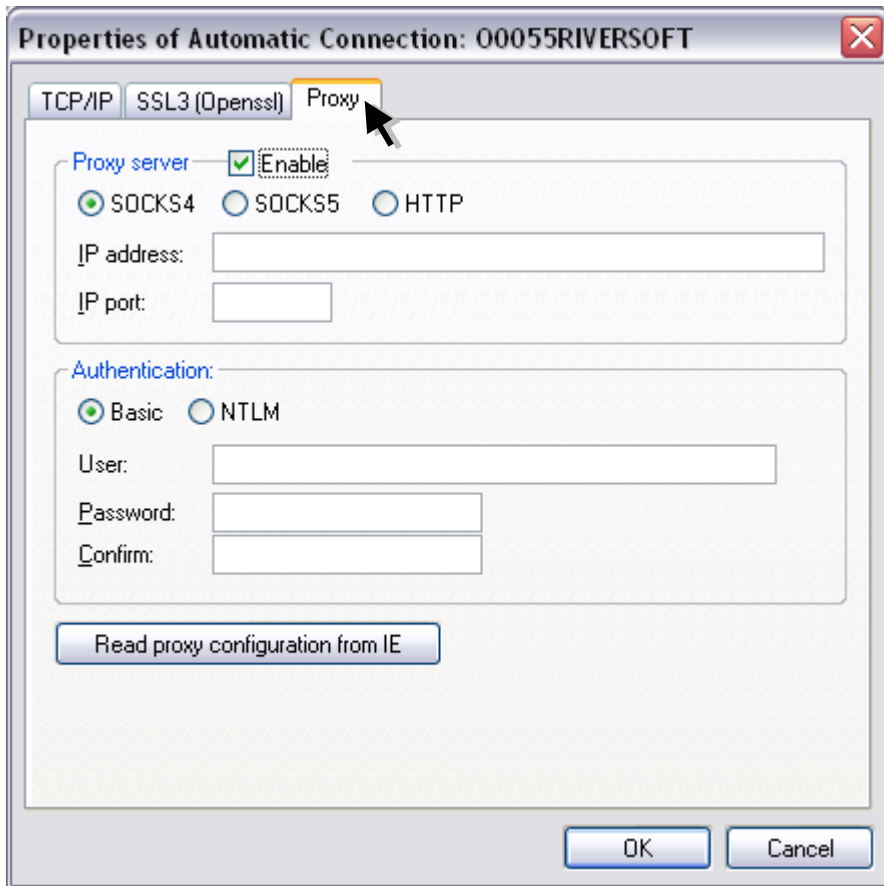
18. On the **SSL3** tab set the following options for the **OFTP – TCP/IP** protocol.



Fields	Description
Private Key	The options in this group are related to public and private keys, used by TLS1/SSL3 protocol for authentication and data encryption. Note: The file of private key must be in PKCS#12 formats and the certificates, in DER or PEM format.
Key	Fill this field with the file name (full path) where the private key is installed.
Certificate	Fill this field with the file name (full path) where is the digital certificate (X509) installed, associated with the private key.
Password	Fill this field with the password that protects the file of private key.
Confirm	Fill this field with the supplied typed in the Password field for validation.
CA Certificates (Authority)	The options in this group are related to digital certificates of certification authorities (CA) that will serve to validate the authenticity of the certificate presented by the server. Note: The file of private key must be in PKCS#12 formats and the

	certificates, in DER or PEM format.
File	Fill this field with the file name (full path) where the digital certificate (X509) is installed containing the public key that signs the certificate presented by the server.
Directory	Fill this field with the directory name (full path) where the installed digital certificates (X509) are installed containing the public key that signs the certificate presented by the server.
Algorithms	Fill this field with the names of supported algorithms for digital signatures, hashing, and data encryption. Note: If this field is not configured, the TLS1/SSL3 protocol will be automatically selected.
Debug	This option allows generating a debug file in the Debug folder of the installation directory of the STCP.

19. On the **Proxy** tab set the following options for the **OFTP – TCP/IP** protocol.

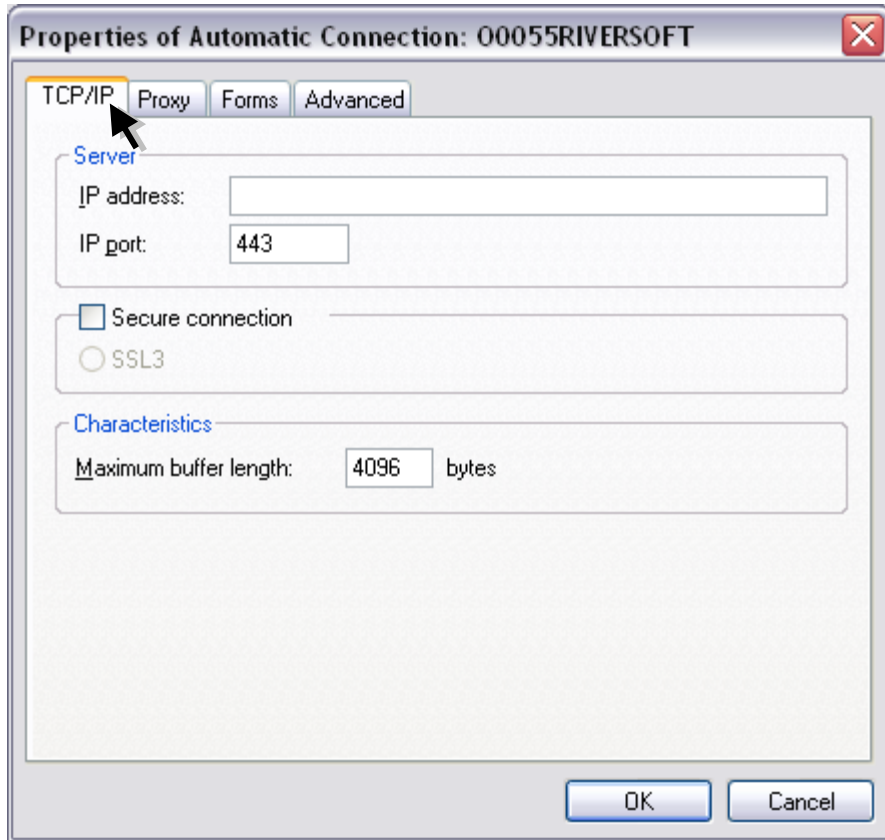


Fields	Description
Proxy Server	The options in this group allow the communication setup through a Proxy server.
Enable	This option enables the use of a Proxy Server when checked.
SOCKS4	This option enables the use of a Proxy server in accordance with the SOCKS4 specification.
SOCKS5	This option enables the use of a Proxy server in accordance with the RFC1928 (SOCKS5) and RFC1929 recommendation. Note: The authentication process used is defined in RFC1929.
HTTP	This option enables the use of a Proxy server in accordance with the RFC2817 recommendation (HTTP). Note: The authentication process used is Basic.
IP Address	Fill this field with the TCP/IP address or name (DNS) of STCP Proxy server.
IP Port	Fill this field with the TCP/IP proxy server.
Authentication	The options in this group allow the user setup and password that will be reported to the Proxy server.

Basic	Check this option if your Proxy server supports Basic authentication mode.
NTLM	Check this option if your proxy server supports the NTLM authentication mode. If you use Proxy servers of Microsoft, this should be the preferential option.
User	Fill this field with the username authorized to use the Proxy service.
Password	Fill this field with the password of the user authorized to use the Proxy service.
Confirm	Fill this field with the supplied password in the Password field for validation.
Read proxy configuration from IE	Press this button to read the Proxy settings configured in Internet Explorer. Note: The authentication information will not be read from IE.

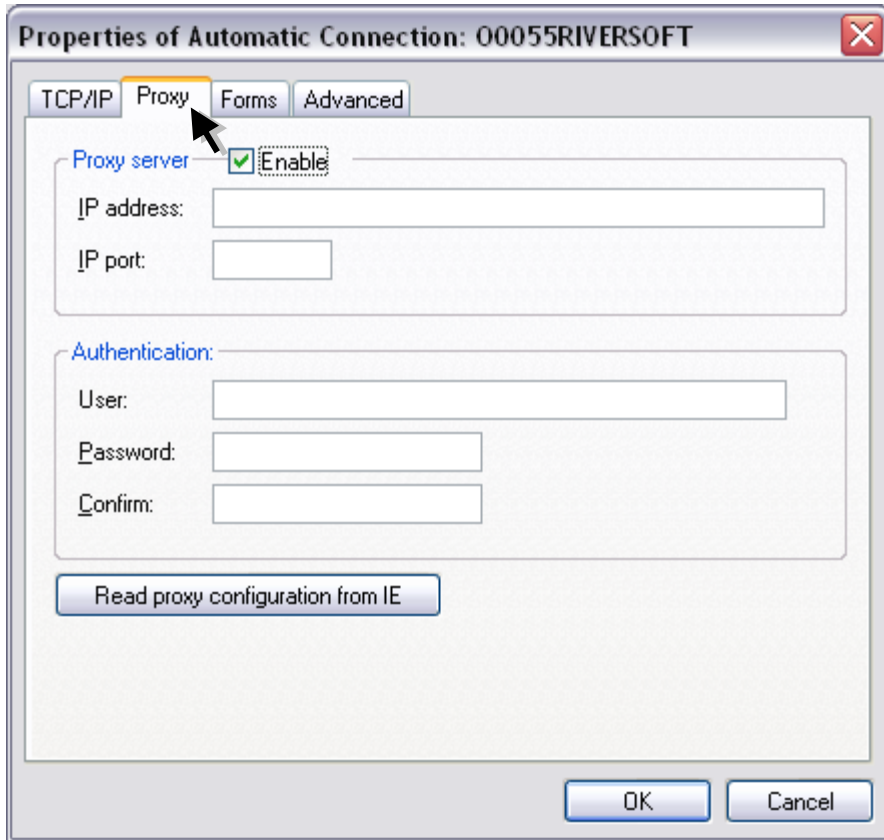
Press **OK** button to continue or **Cancel** to abandon without changing the settings.

20. If the protocol selected is **HTTP - TCP / IP**, set the following options in the **TCP/IP** tab.



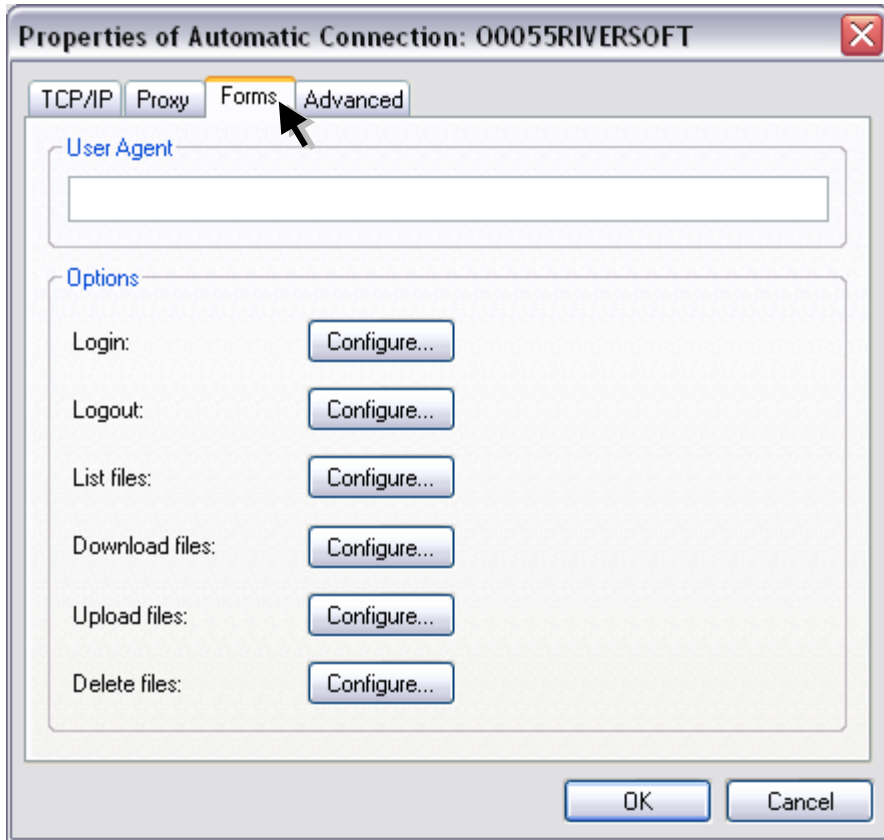
Fields	Description
IP address	Fill this field with the TCP/IP address or name (DNS) of the server STCP OFTP Server.
IP port	Fill this field with the TCP/IP port of the server STCP OFTP Server.
SSL3	Sets a secure communication with encryption and digital certification, with the use of definite standard in RFC2246 (TLS1/SSL3). The TLS1/SSL3 is commonly found in servers of secure sites (HTTPS) and offers the highest level of security currently available. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is from 1 up to 65535.

21. On the **Proxy** tab set the following options.



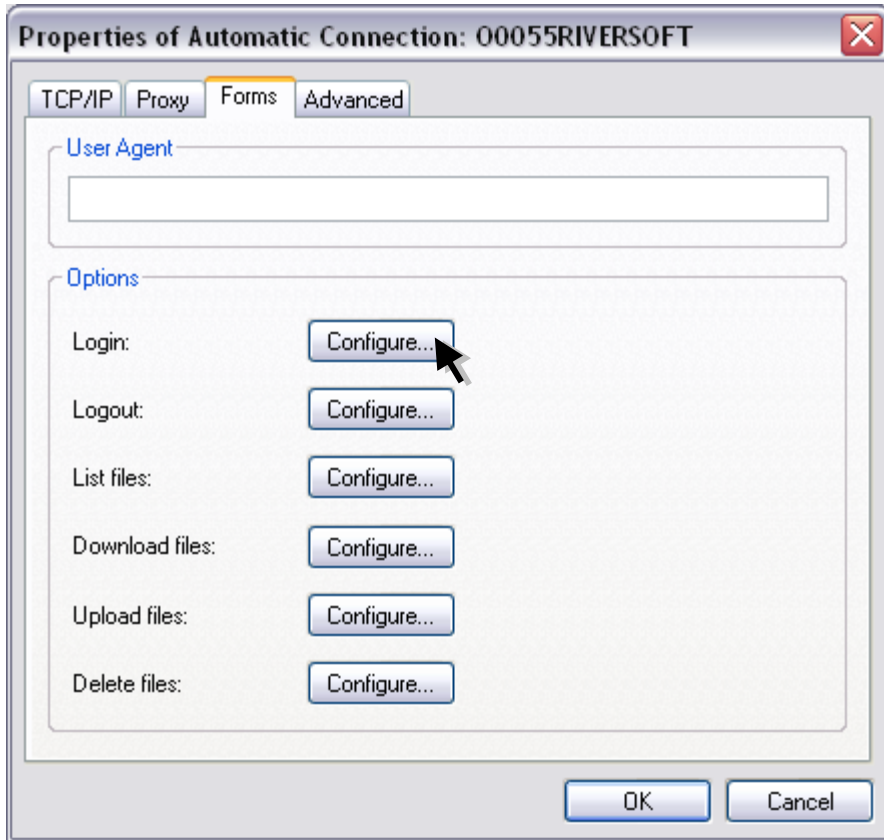
Fields	Description
Enable	This option enables the use of a Proxy server when checked.
IP address	Fill this field with the TCP/IP address or name (DNS) of the STCP Proxy server.
IP port	Fill this field with the TCP/ IP port of the Proxy server.
User	Fill this field with the username authorized to use the Proxy service.
Password	Fill this field with the password of the user authorized to use the Proxy service.
Confirm	Fill this field with the specified password in the Password field for validation.
Read Proxy configuration from IE	Press this button to read the Proxy settings configured in Internet Explorer. Note: The authentication information will not be read from IE.

22. On the **Forms** tab set the following options.

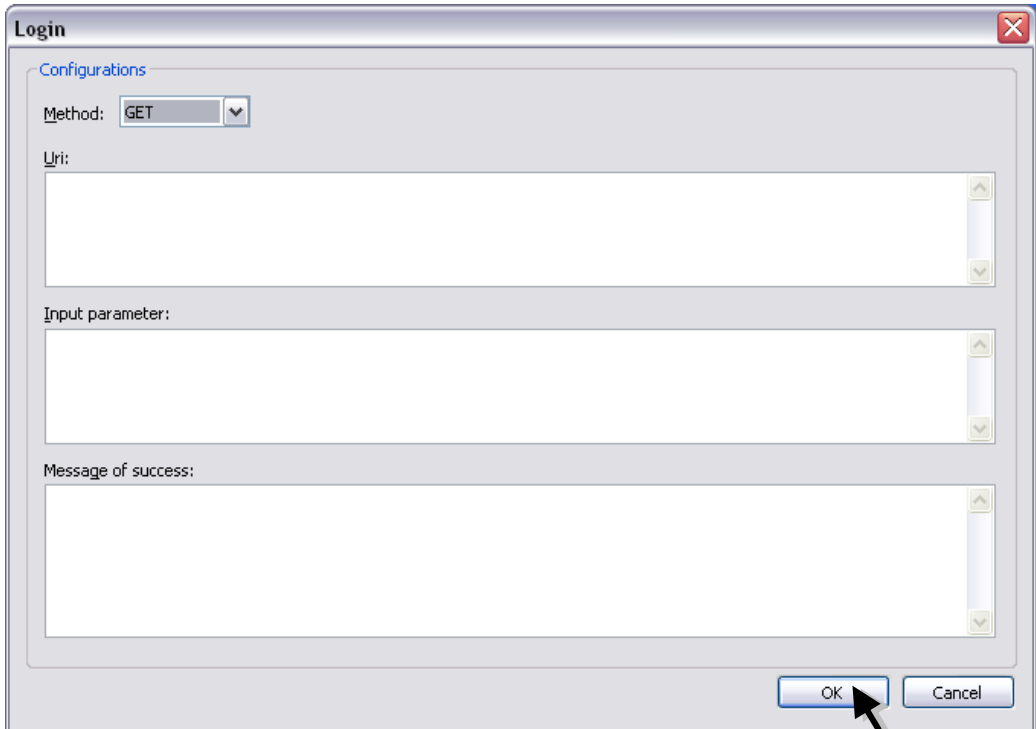


Fields	Description
User Agent	User Agent is a string that indicates the application name, version, operating system and some characteristics of the computer.
Login	Configuration parameter in the login form on the site.
Logout	Configuration parameter in the logout form on the site.
List files	Configuration parameters of the form for listing the contents of the Mailbox.
Download files	Configuration parameters of the form to receive files.
Upload files	Configuration parameters of the form to send files.
Delete files	Configuration parameters of the form for removing files.

23. Click the **Configure** button to access the Login options.



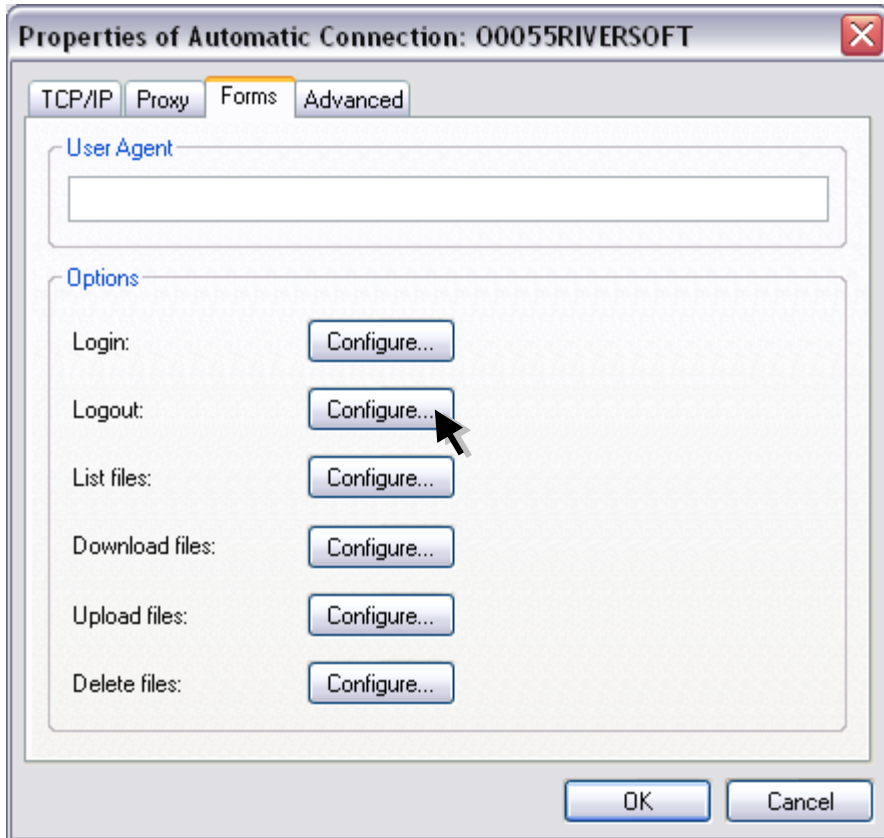
24. Set the following fields.



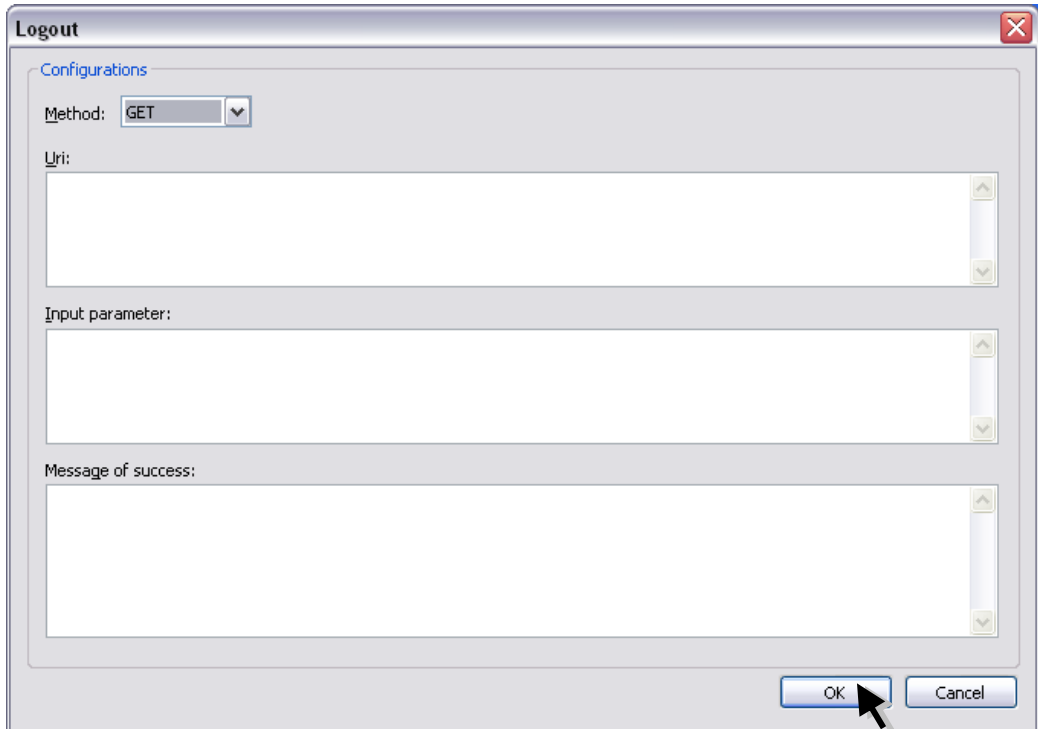
Fields	Description
Method	These data are part of the configuration parameters of the form for HTTP access. Through these data the STCP integration is done with a remote site in order to automate the Transmission and/or Reception of files via HTTP protocol.
Uri	
Input parameter	
Message of success	

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

25. Click the **Configure** button to access the Logout options.



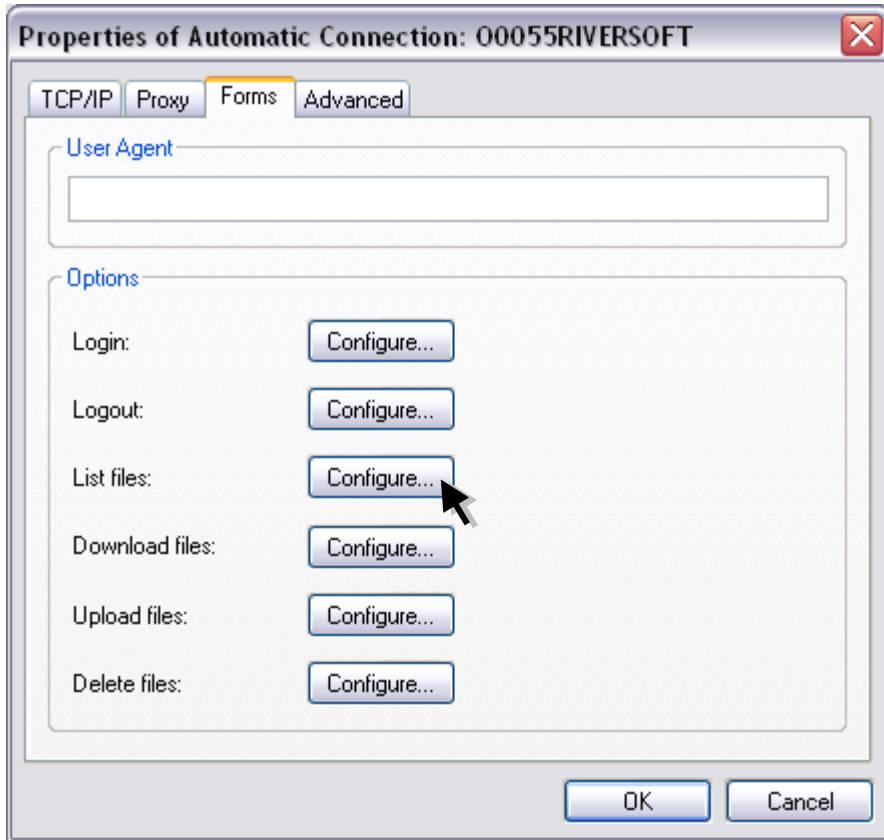
26. Set the following fields.



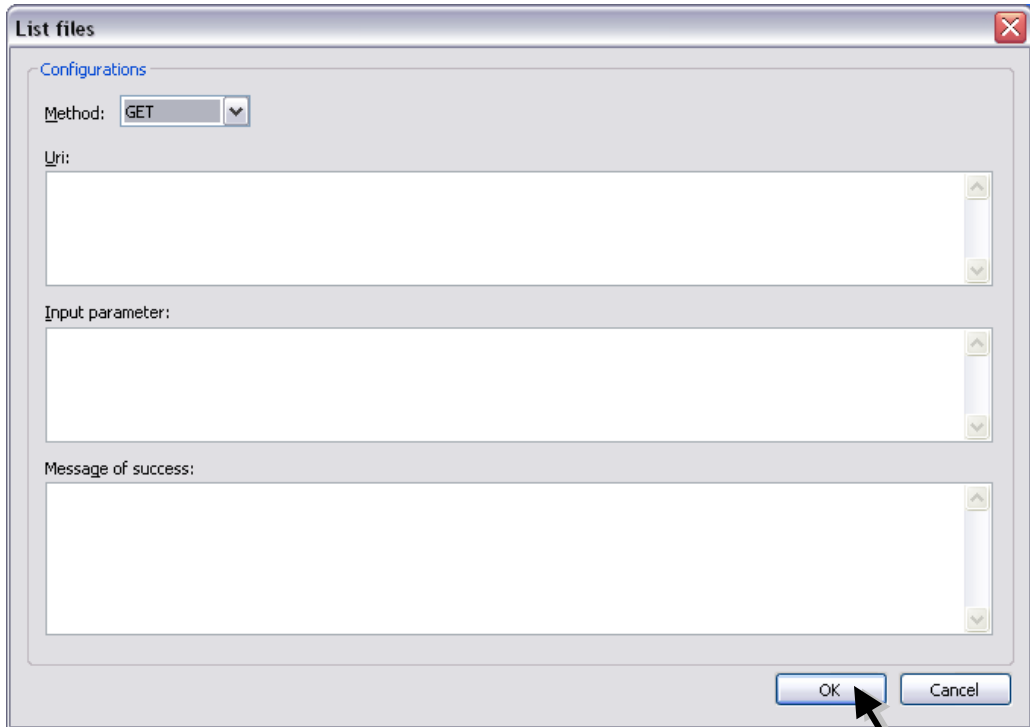
Fields	Description
Method	These data are part of the configuration parameters of the form for HTTP access. Through these data the STCP integration is done with a remote site in order to automate the Transmission and/or Reception of files via HTTP protocol.
Uri	
Input parameter	
Message of success	

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

27. Click the **Configure** button to access the List files parameters.



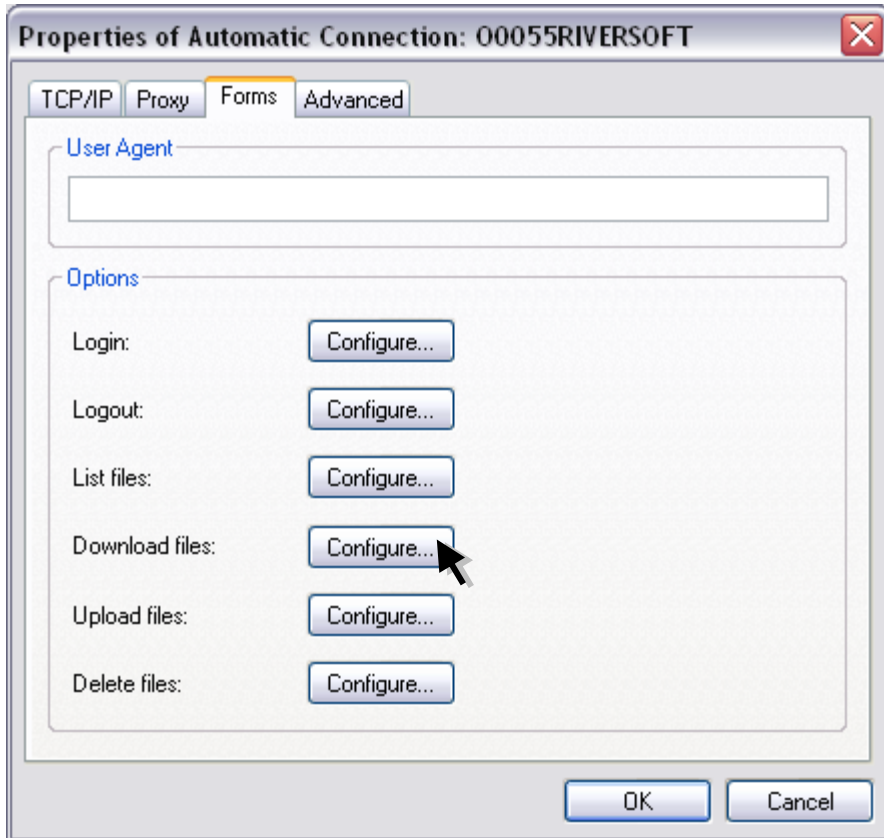
28. Set the following fields.



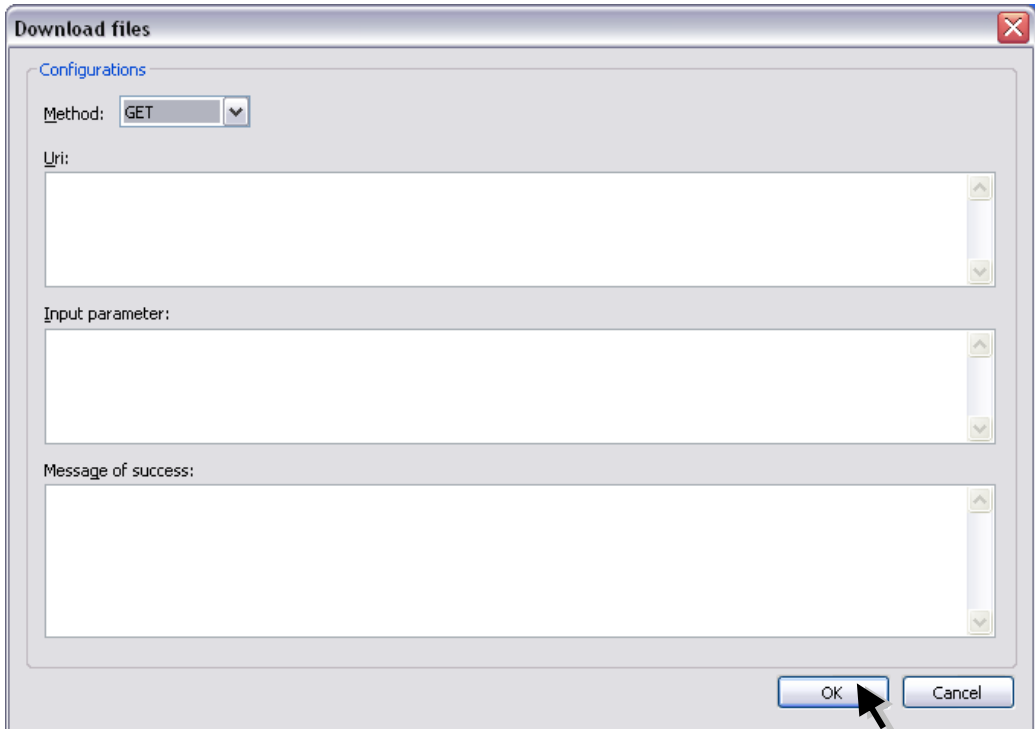
Fields	Description
Method	These data are part of the configuration parameters of the form for HTTP access. Through these data the STCP integration is done with a remote site in order to automate the Transmission and/or Reception of files via HTTP protocol.
Uri	
Input parameter	
Message of success	

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

29. Click the **Configure** button to access the Download files parameters.



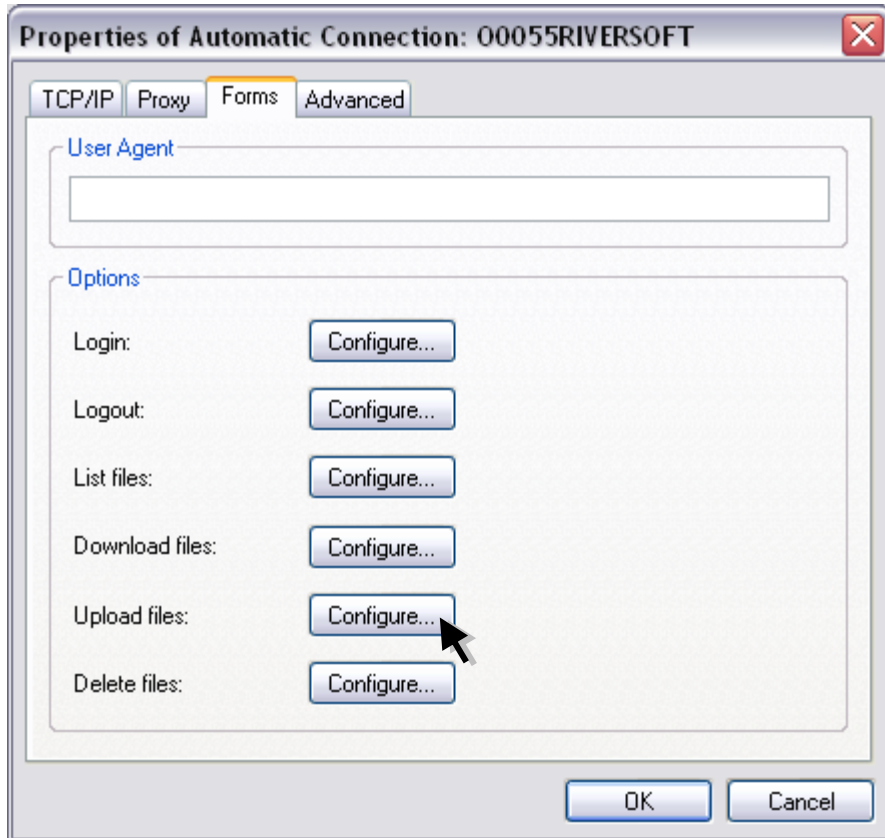
30. Set the following fields.



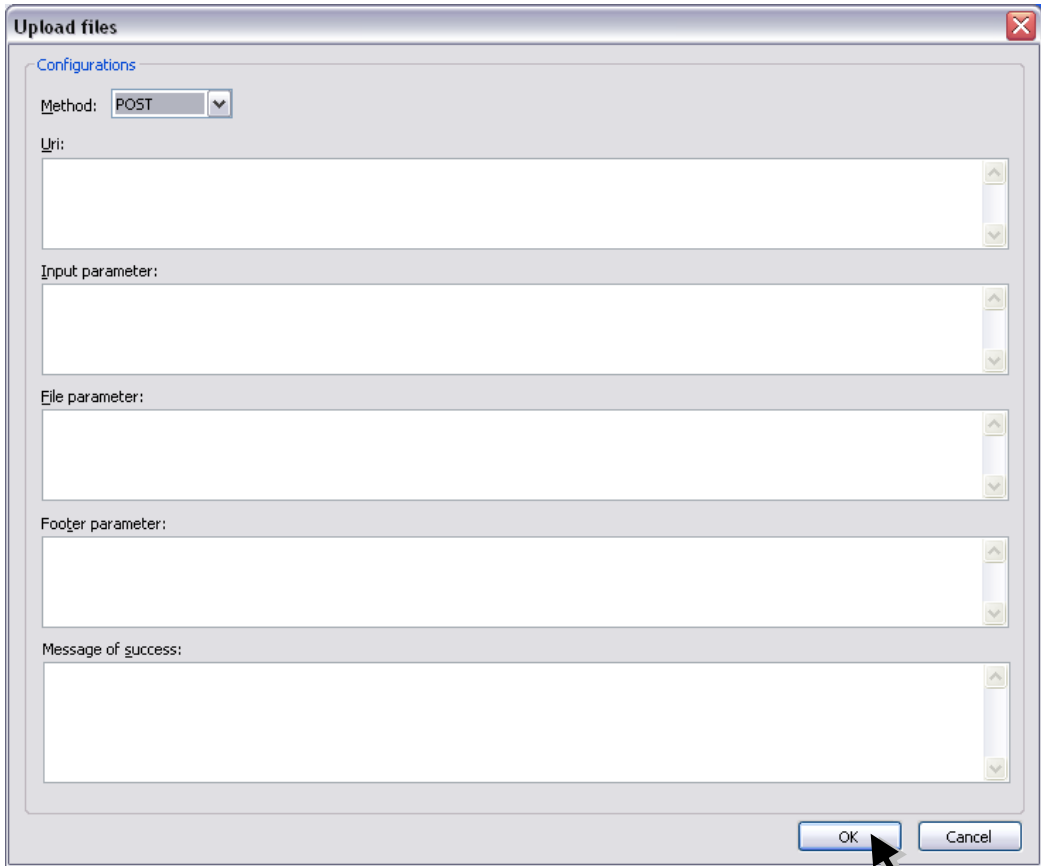
Fields	Description
Method	These data are part of the configuration parameters of the form for HTTP access. Through these data the STCP integration is done with a remote site in order to automate the Transmission and/or Reception of files via HTTP protocol.
Uri	
Input parameter	
Message of success	

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

31. Click the **Configure** button to access the Upload files parameters.



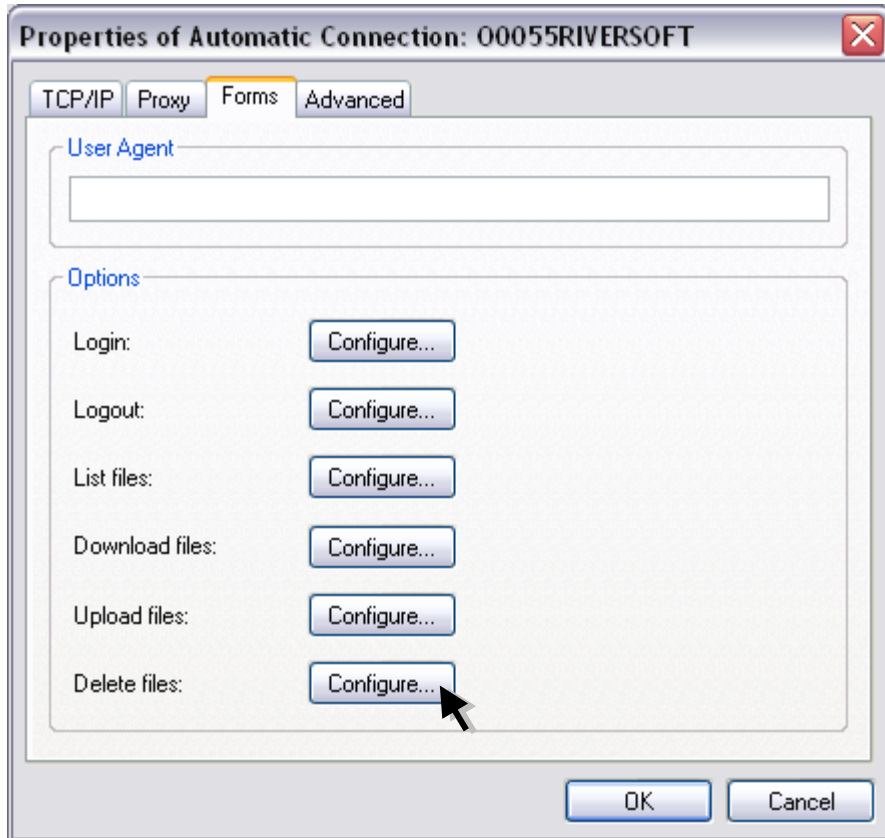
32. Set the following fields.



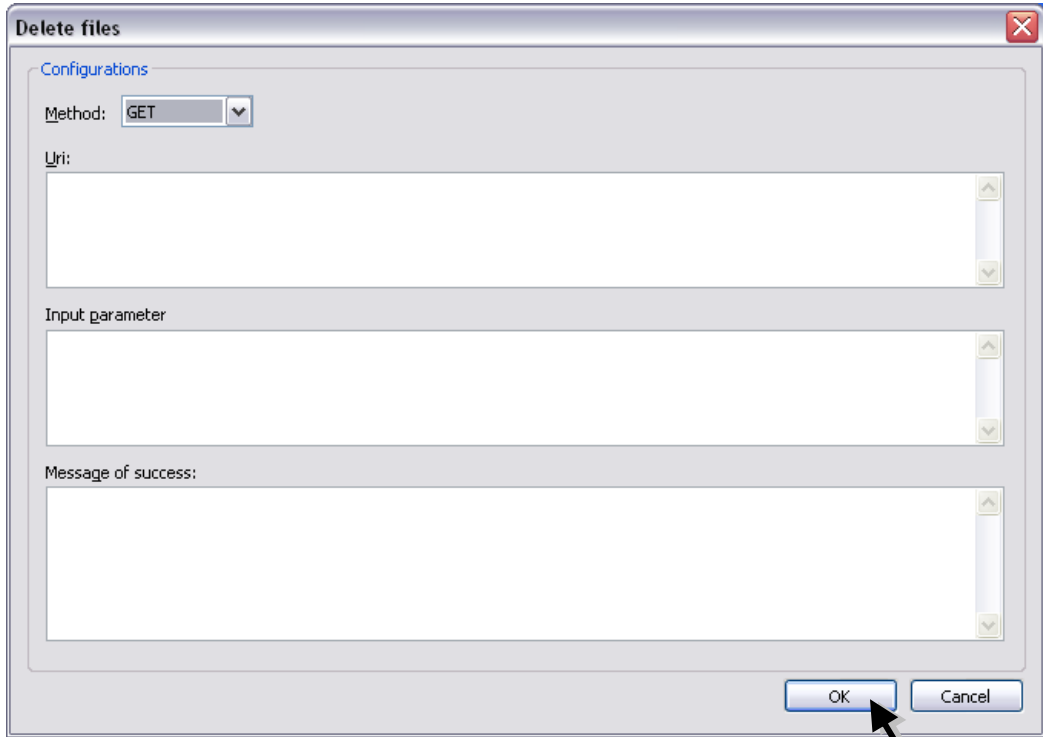
Fields	Description
Method	These data are part of the configuration parameters of the form for HTTP access. Through these data the STCP integration is done with a remote site in order to automate the Transmission and/or Reception of files via HTTP protocol.
Uri	
Input parameter	
File parameter	
Footer parameter	
Message of success	

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

33. Click the **Configure** button to access the Delete files parameters.



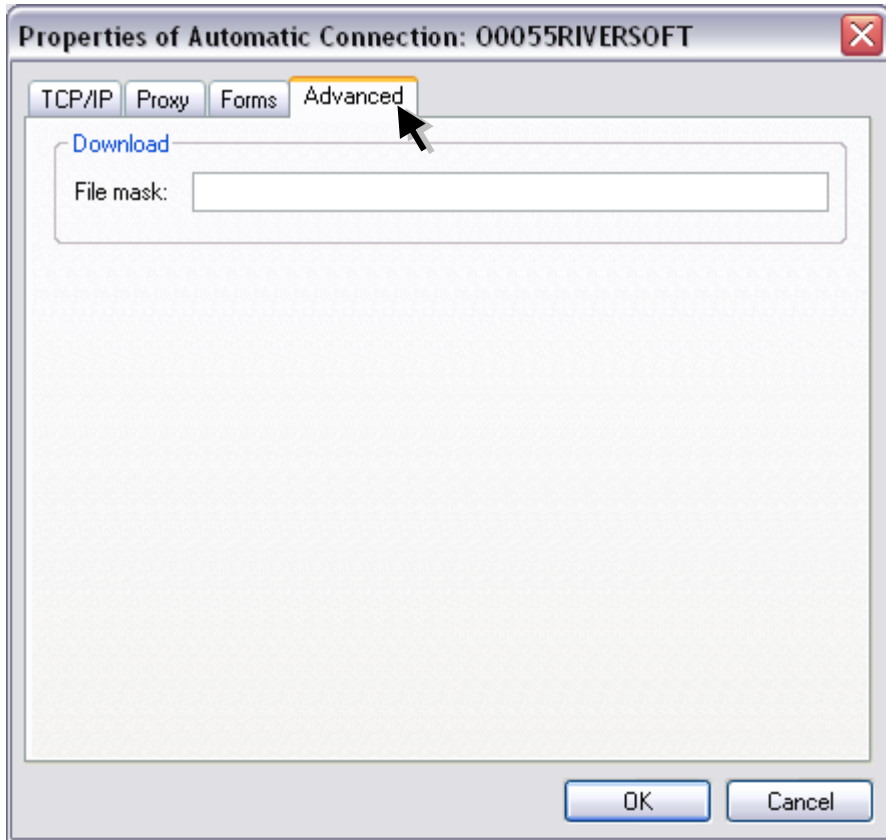
34. Set the following fields.



Fields	Description
Method	These data are part of the configuration parameters of the form for HTTP access. Through these data the STCP integration is done with a remote site in order to automate the Transmission and/or Reception of files via HTTP protocol.
Uri	
Input parameter	
Message of success	

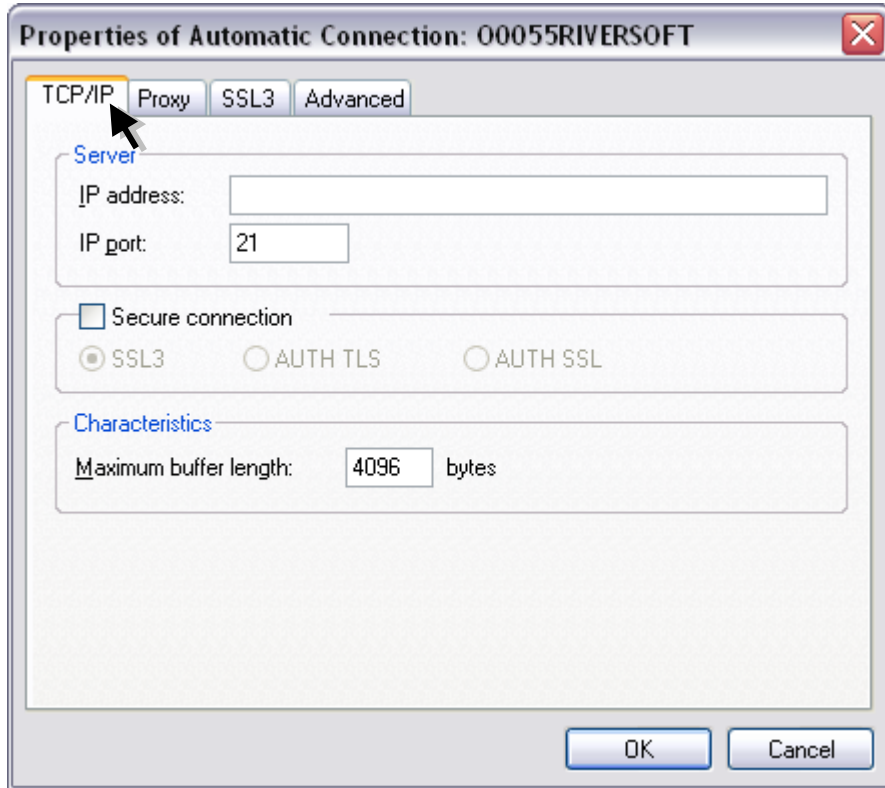
Press **OK** button to continue or **Cancel** to abandon without changing the settings.

35. On the **Advanced** tab set the following parameters.



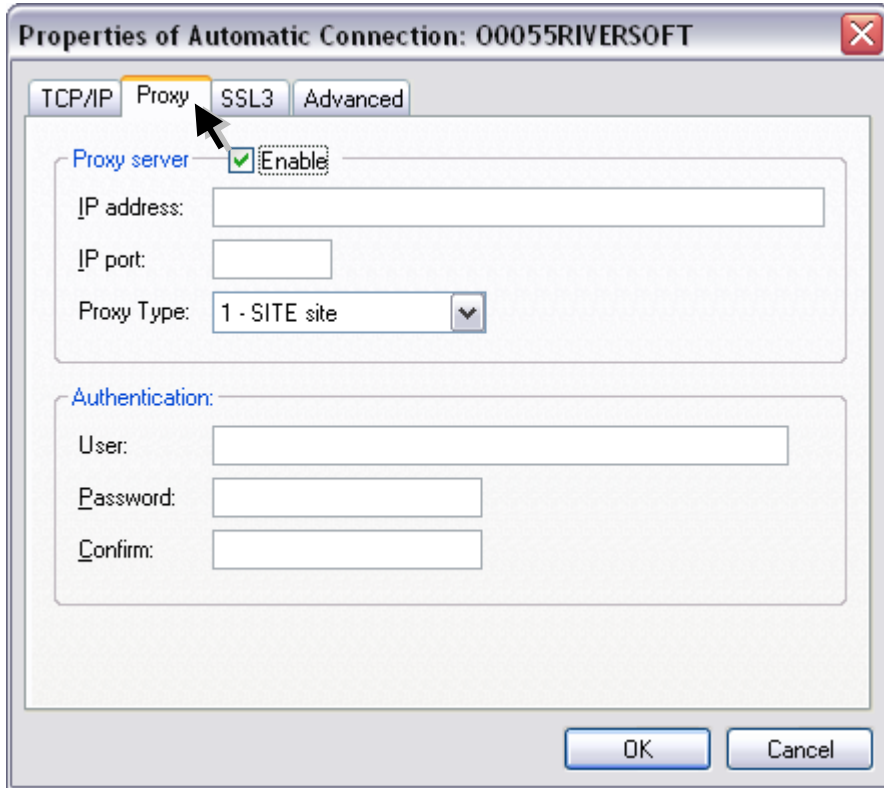
Fields	Description
File mask	Through regular expression, this option is used to filter what you want to download.

36. If the protocol selected is **FTP – TCP/IP**, set the following options on the **TCP/IP** tab.



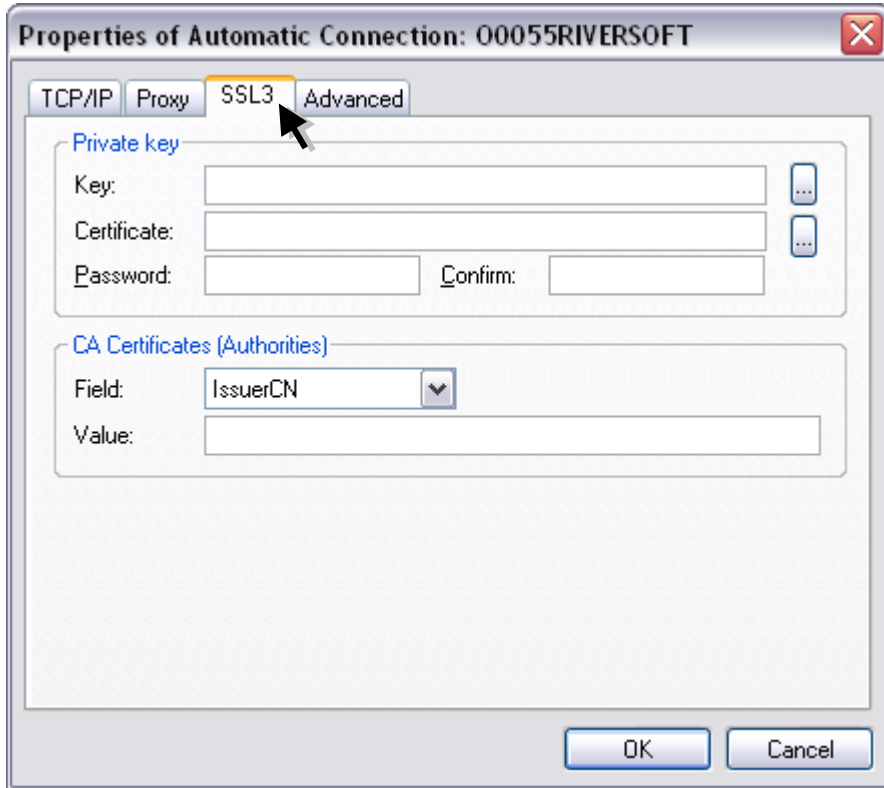
Fields	Description
IP address	Fill this field with the TCP / IP address or name (DNS) of the server STCP OFTP Server.
IP port	Fill this field with the TCP/IP port of the STCP OFTP Server. Note: The default port of the service is 21.
SSL3	Sets a secure communication with encryption and digital certification, with the use of definite standard in RFC2246 (TLS1/SSL3). The TLS1/SSL3 is commonly found in servers of secure sites (HTTPS) and offers the highest level of security currently available. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
AUTH TLS	Enables the encrypted authentication process, ensuring security in password exchange.
AUTH SSL	Enables the sending of an explicit command to the FTP server to use the SSL security.
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is from 1 up to 65535.

37. On the **Proxy** tab set the following options.



Fields	Description
Enable	This option enables the use of a Proxy Server when checked.
IP address	Fill this field with the TCP/IP address or name (DNS) of STCP Proxy server.
IP port	Fill this field with the TCP/IP proxy server.
Proxy Type	Parameter used to manage the Firewall settings if it is used in the FTP connection.
User	Fill this field with the username authorized to use the Proxy service.
Password	Fill this field with the password of the user authorized to use the Proxy service.
Confirm	Fill this field with the specified password in the Password field for validation.

38. On the **SSL3** tab set the following options.



Fields	Description
Private key	The options in this group are related to public and private keys, used by TLS1/SSL3 protocol for authentication and data encryption. Note: The file of private key must be in PKCS # 12 format and the certificates, in DER or PEM format.
Key	Fill this field with the file name (full path) where the private key is installed.
Certificate	Fill this field with the file name (full path) where the digital certificate (X509) is installed, associated with the private key.
Password	Fill this field with the password that protects the file of private key.
Confirm	Fill this field with the password supplied in the password field for validation.
CA Certificates (Authorities)	The options in this group are related to digital certificates of certification authorities (CA) that will serve to validate the authenticity of the certificate presented by the Server. Note: The file of private key must be in PKCS # 12 format and the certificates, in DER or PEM format.
Field	IssuerCN: Certificate issuer. IssuerDN: Details about the issuer.

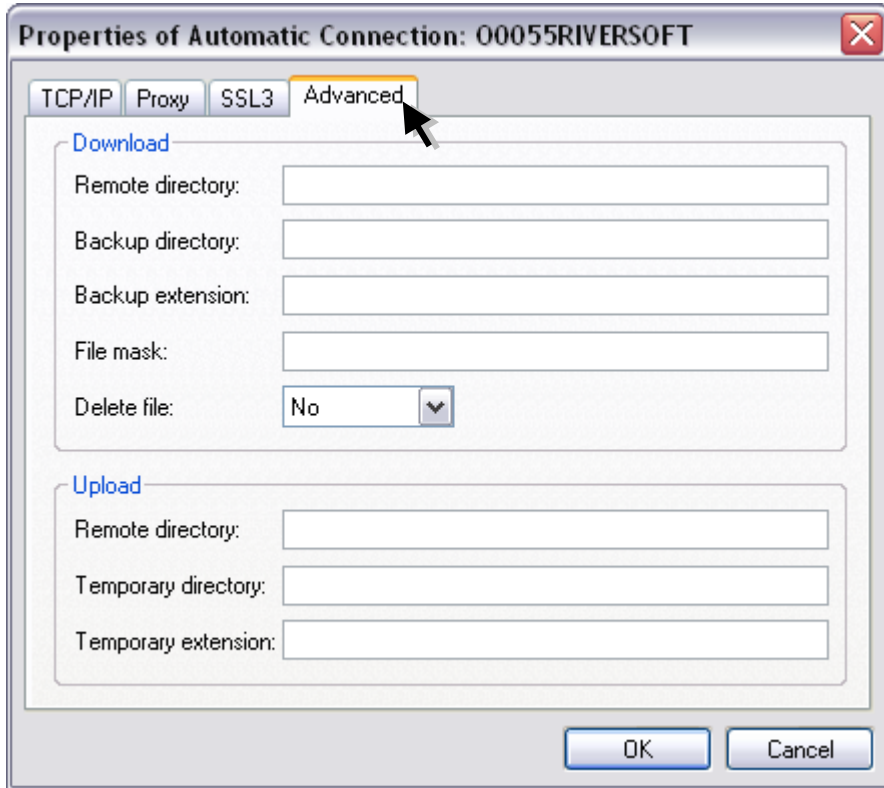
SubjectCN: Certificate owner.

SubjectDN: Details about the certificate owner.

Value

The value of this field is related to the digital certificates of certificate authorities (CA) that will serve to validate the authenticity of the certificate presented by the FTP server.

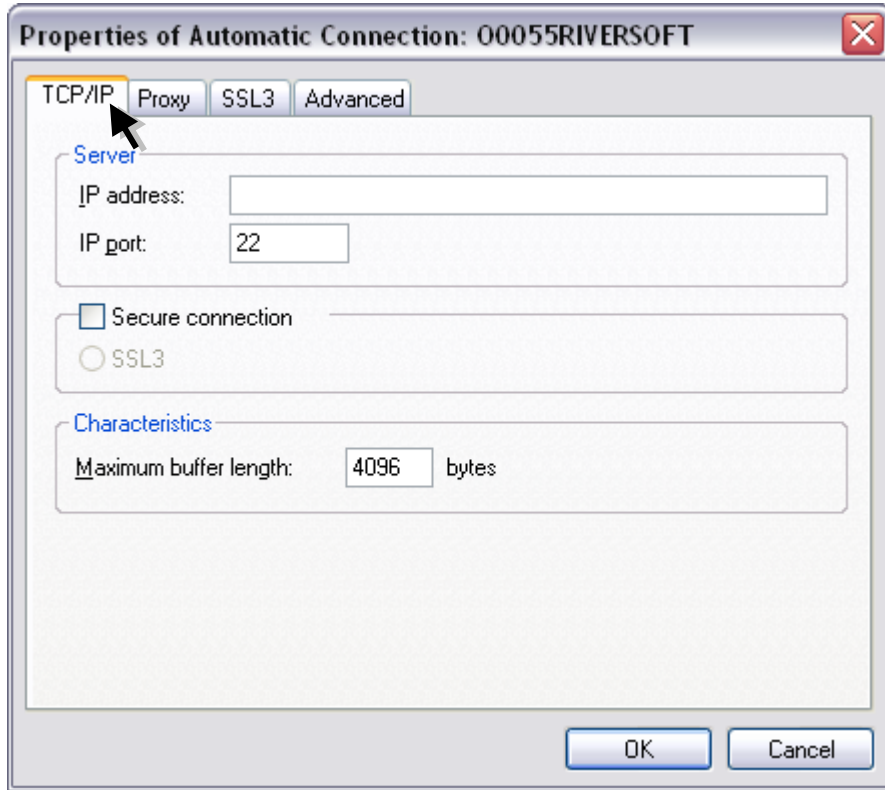
39. On the **Advanced** tab set the following options.



Fields	Description
Remote directory	Sets the remote directory where you want to download the file.
Backup directory	Sets the backup directory, which controls the download process and becomes effective, avoiding duplication of files.
Backup extension	Sets extension for backup file on the remote server (FTP).
File mask	Through regular expression, this option is used to filter what you want to download.
Delete file	This option allows or not removing the file of the directory on the FTP server.
Remote directory	Sets the remote directory where you want to upload the file.
Temporary directory	Sets the temporary directory, which guarantees the integrity of the files during the upload.
Temporary extension	Sets a temporary extension to file on the remote server (FTP).

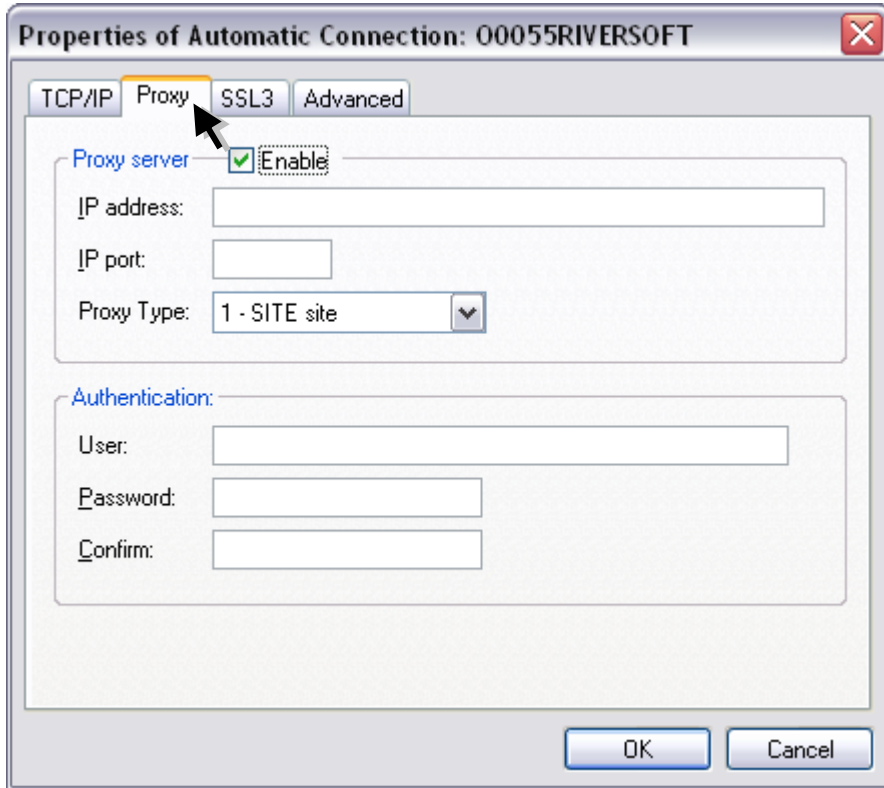
Press **OK** button to continue or **Cancel** to abandon without changing the settings.

40. If the protocol selected is **SFTP – TCP/IP** set the following options on the **TCP/IP** tab.



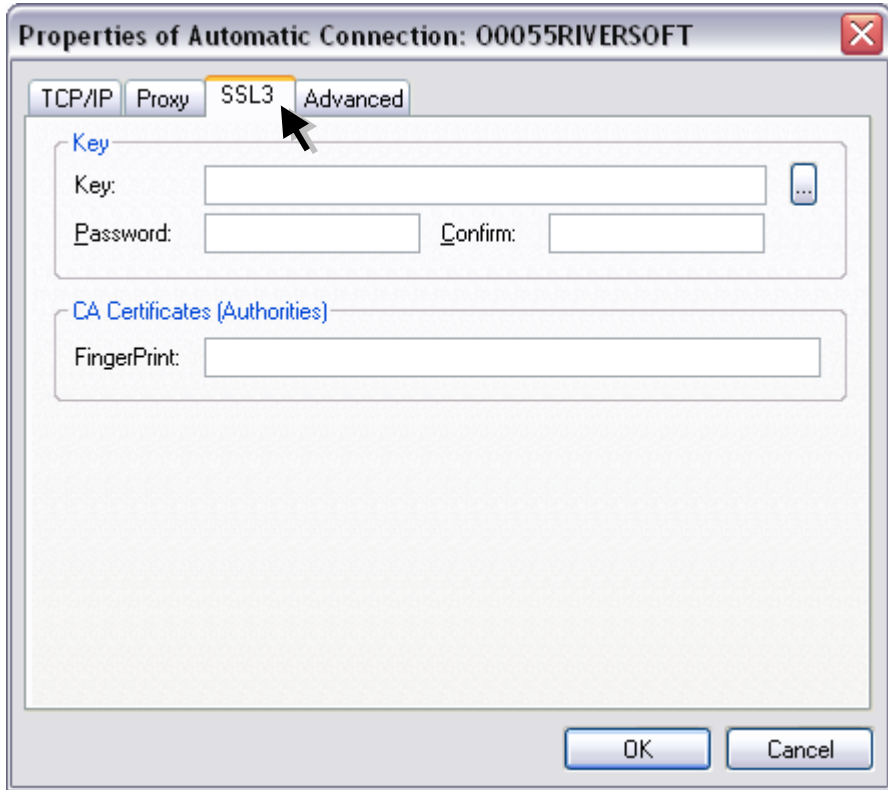
Fields	Description
IP address	Fill this field with the TCP/IP address or name (DNS) of the server STCP OFTP Server.
IP port	Fill this field with the TCP/IP port of the server STCP OFTP Server.
SSL3	Sets a secure communication with encryption and digital certification, with the use of definite standard in RFC2246 (TLS1/SSL3). The TLS1/SSL3 is commonly found in servers of secure sites (HTTPS) and offers the highest level of security currently available. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is from 1 up to 65535.

41. On the **Proxy** tab set the following options.



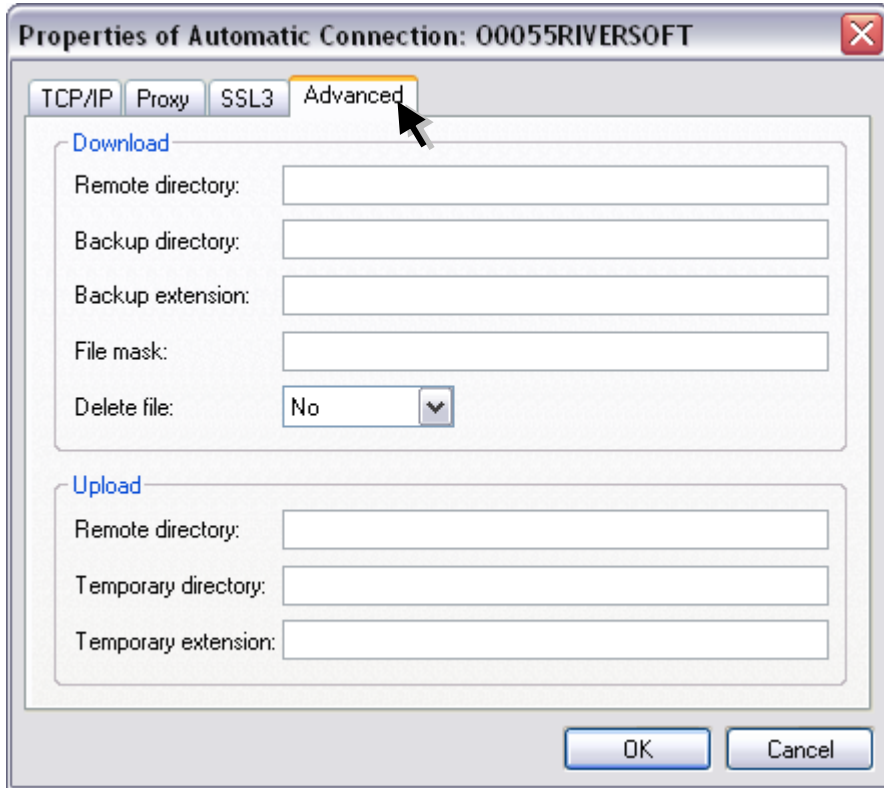
Fields	Description
IP address	Fill this field with the TCP/IP address or name (DNS) of the server STCP OFTP Server.
IP port	Fill this field with the TCP/IP port of the server STCP OFTP Server.
SSL3	Sets a secure communication with encryption and digital certification, with the use of definite standard in RFC2246 (TLS1/SSL3). The TLS1/SSL3 is commonly found in servers of secure sites (HTTPS) and offers the highest level of security currently available. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is from 1 up to 65535.

42. On the **SSL3** tab set the following options.



Fields	Description
Key	Fill this field with the filename (full path) where the private key is installed.
Password	Fill this field with the password that protects the private key file.
Confirm	Fill this field with the specified password in the Password field for validation.
FingerPrint	Digital signature of the private key.

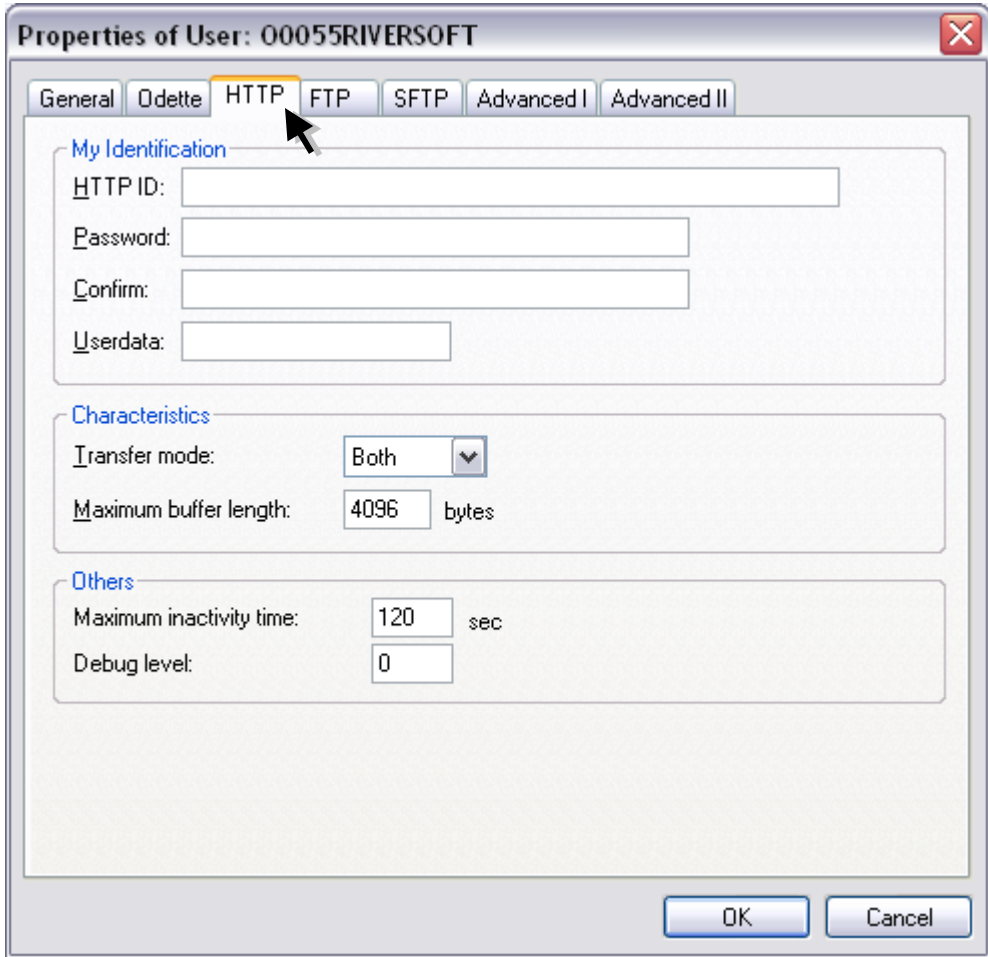
43. On the **Advanced** set the following options.



Fields	Description
Remote directory	Sets the remote directory where you want to download the file.
Backup directory	Sets the backup directory, which controls the download process and becomes effective, avoiding duplication of files.
Backup extension	Sets extension for backup file on the remote server (SFTP).
File mask	Through regular expression, this option is used to filter what you want to download.
Remove file	This option allows or not removing the file of the directory on the FTP server.
Remote directory	Sets the remote directory where you want to upload the file.
Temporary directory	Sets the temporary directory, which guarantees the integrity of the files during the upload.
Temporary extension	Sets a temporary extension to file on the remote server (SFTP).

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

44. On the **HTTP** tab set the following options.



Fields	Description
HTTP ID	Identification and authentication used to access the site.
Password	Password used to authentication and access to the site.
Confirm	Fill this field with the specified password in the Password field for validation.
Userdata	Fill this field with the extra data associated with Odette identification informed. Note: Fill this field only if it is requested by the server.
Transfer mode	This option allows to select the transfer mode to be used for communication with the server, they are: Both (transmit and receive files), Sender (only file transmission) and Receiver (only receiving files).
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is 1 up to 65535.
Maximum inactivity time	Fill this field with the maximum timeout for communication

between the STCP OFTP Server and the remote computer.

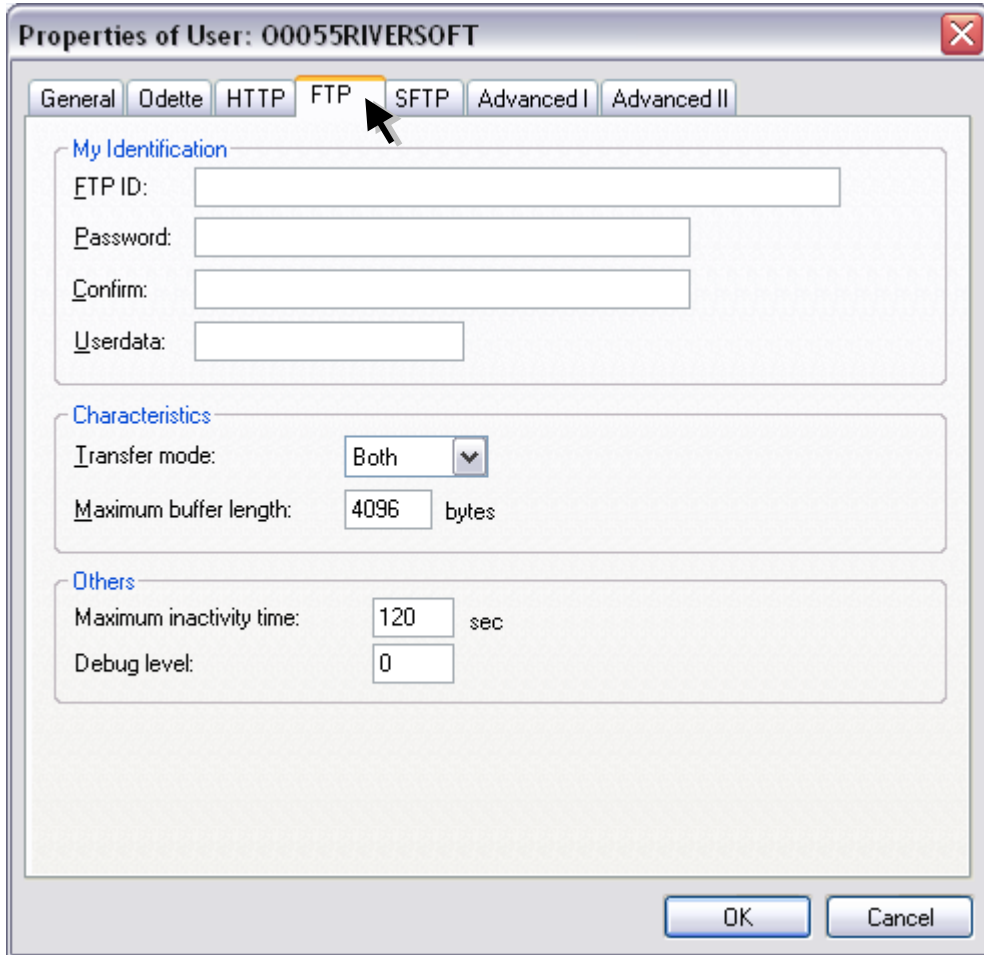
Debug level

Fill this field with the level of details of information to be recorded in the debug file.

To obtain the information of different levels in the same debug file, fill this field with the sum of desired levels.

Note: See table of debug levels in configuration of users.

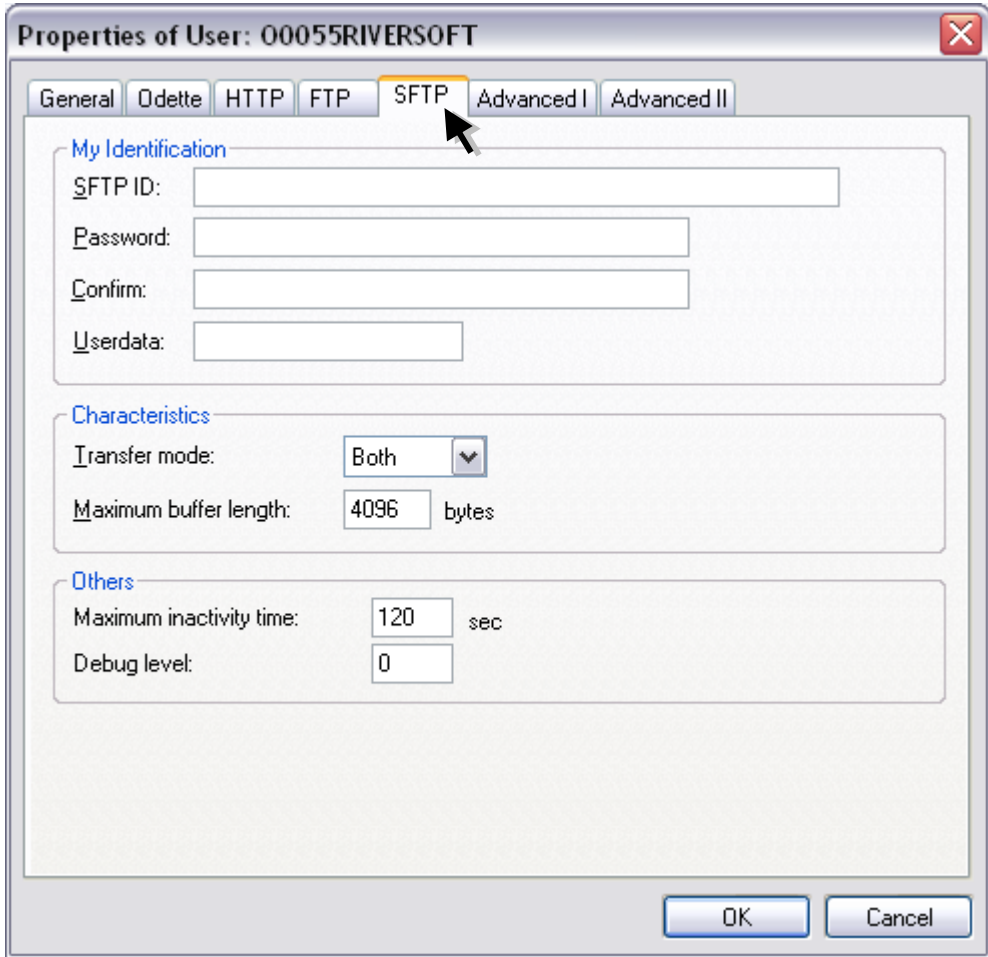
45. On the **FTP** tab set the following options.



Fields	Description
FTP ID	Identification to access the FTP.
Password	Password to access the FTP.
Confirm	Fill this field with the specified password in the Password field for validation.
Userdata	Fill this field with the extra data associated with Odette ID informed. Obs.: Preencha este campo somente se for requerido pelo servidor. Note: Fill this field only if requested by the server.
Transfer mode	This option allows to select the transfer mode to be used for communication with the server, they are: Both (transmit and receive files), Sender (only file transmission) and Receiver (only receiving files).
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is from 1 up to 65535.

Maximum inactivity time	Preencha este campo com o tempo máximo de inatividade de comunicação entre o STCP OFTP Server e o computador remoto. Fill this field with the maximum downtime for communication between the STCP OFTP Server and the remote computer.
Debug level	Fill this field with the level of details of information to be recorded in the debug file. To obtain the information at different levels in the same file debug, fill this field with the sum of desired levels. Note: See table of debug levels in configuration of users.

46. On **SFTP** tab set the following options.



Fields	Description
SFTP ID	Identification of access to SFTP.
Password	Password to access the SFTP.
Confirm	Fill this field with the specified password in the Password field for validation.
Userdata	Fill this field with the extra data associated with Odette ID informed. Note: Fill this field only if it is requested by the server.
Transfer mode	This option allows selecting the transfer mode to be used for communication with the server, they are: Both (transmit and receive files), Sender (only file transmission) and Receiver (only receiving files).
Maximum buffer length	Fill this field with the maximum size of data blocks to be transferred. The valid range is from 1 up to 65535.
Maximum inactivity time	Fill this field with the maximum downtime of communication between the STCP OFTP Server and the remote computer.

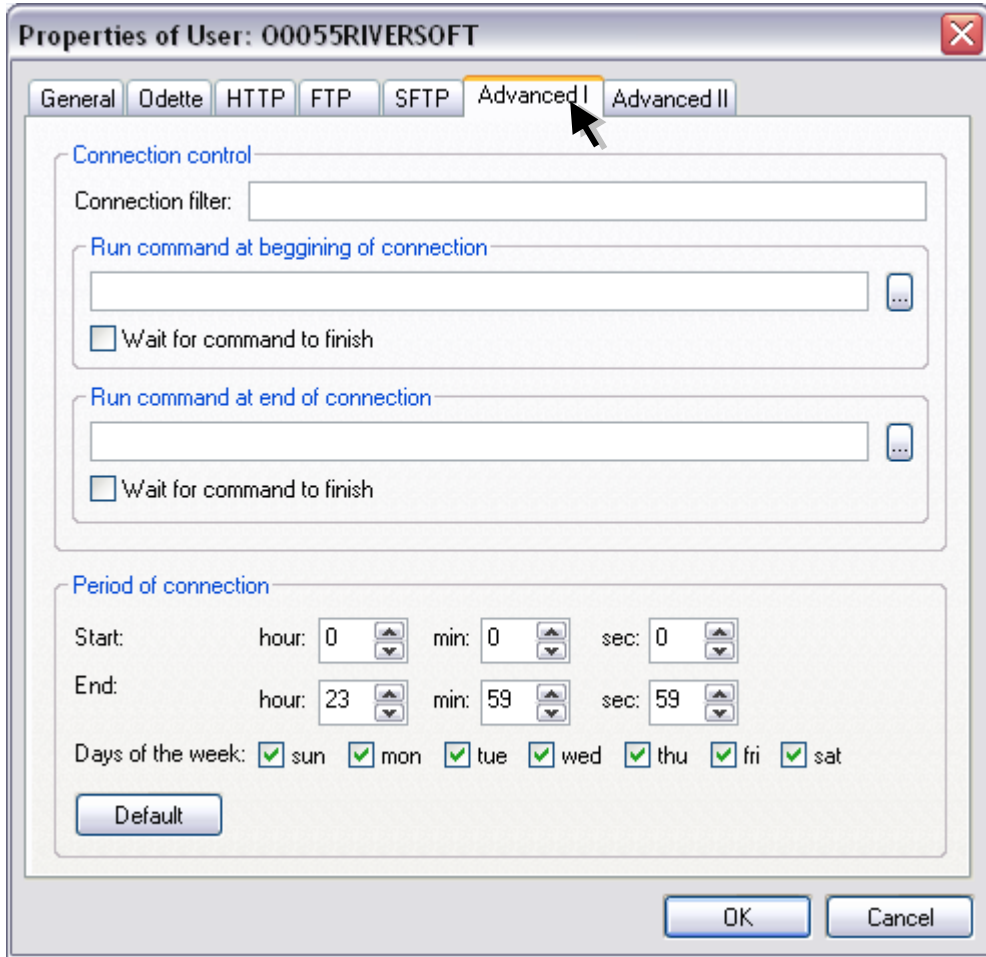
Debug level

Fill this field with the level of details of information to be recorded in the debug file.

To obtain the information of different levels in the same debug file, fill this field with the sum of desired levels.

Note: See table of debug levels in configuration of users.

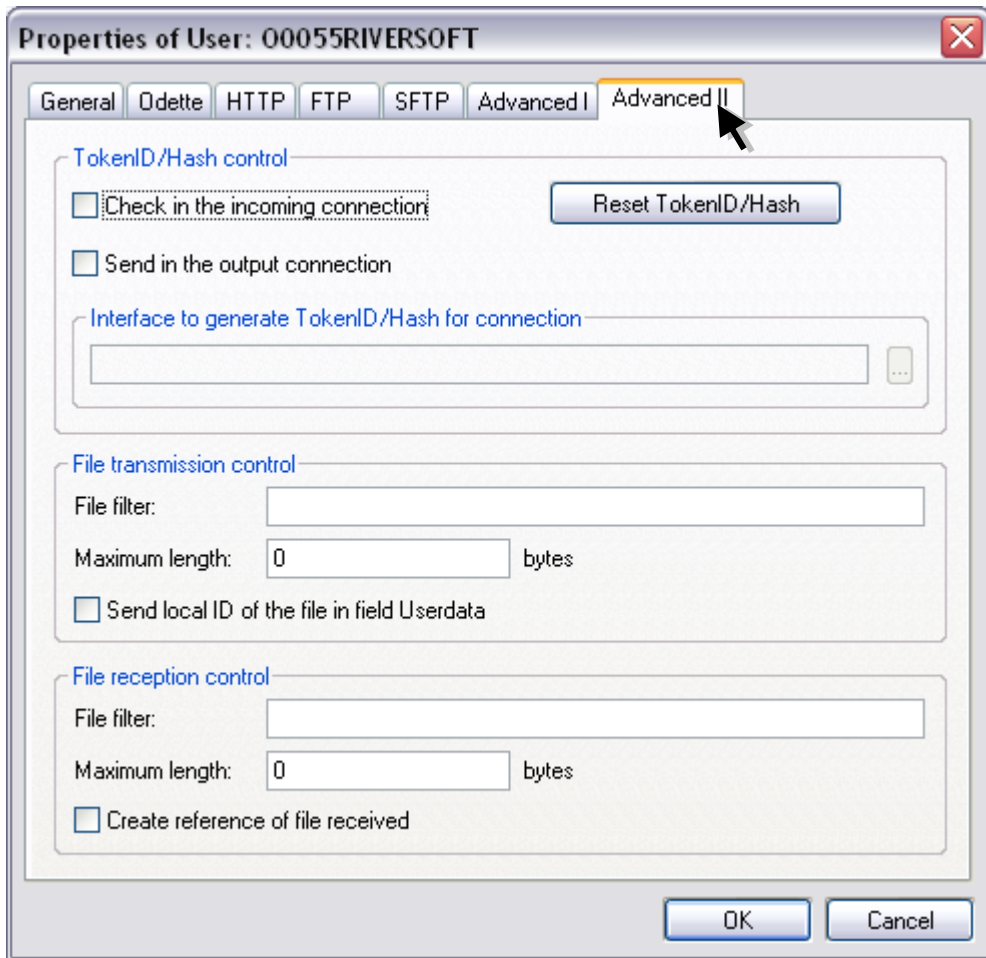
47. On the **Advanced I** set the following options for the user.



Fields	Description
Connection control	The options defined in this group will be used by STCP OFTP Server to validate the connection information (IP address, port, X.25 address, SSL3 certificate etc.).
Connection filter	Fill this field with a regular expression to validate the connection information.
Run command at beginning of connection	Fill this field with the name of an external command (program or bat) that must be executed at the beginning of the connection immediately after the user ID and before file transfer (sending or receiving).
Wait for command to finish	This option enables or disables the STCP OFTP Server to wait until the end of the external command when checked. If the application needs to perform complex operations, keep this option disabled.
Run command at end of	Fill this field with the name of an external command (program or

connection	bat) that must be executed at the end of the connection.
Wait for command to finish	This option enables the STCP OFTP Server to wait until the end of the external command when checked. If the application needs to perform complex operations, keep this option disabled.
Period of connection	Start and end of a connection.
Start	Beginning of the period range of connection.
End	End of the period range of connection.
Days of the week	Reports the days of the week that the connection may occur.
Default	Restores default settings for the connection period.

48. On the **Advanced II** tab set the following options for the user.



Fields	Description
Check in the incoming connection	Validates the Hash information of the machine control at connection of entry.
Send in the output connection	This option enables the sending of TolkenID/Hash information and is configured when using the STCP OFTP Server with automatic connection enabled.
Reset TokenID/Hash	Deletes the TolkenID information or Hash of machine control.
Interface to generate TolkenID/Hash for connection	Parameter that provides the library used to generate the TolkenID/Hash information for the connection.
File transmission control	The options defined in this group will be used by STCP OFTP Server in the treatment of transmission and reception of files.
File filter	Fill this field with a regular expression to validate the filename.
Maximum length	Fill this field with the maximum size that a file may have to be transferred.
Send local ID of the file in field	This option enables the sending of a sequential to the file.

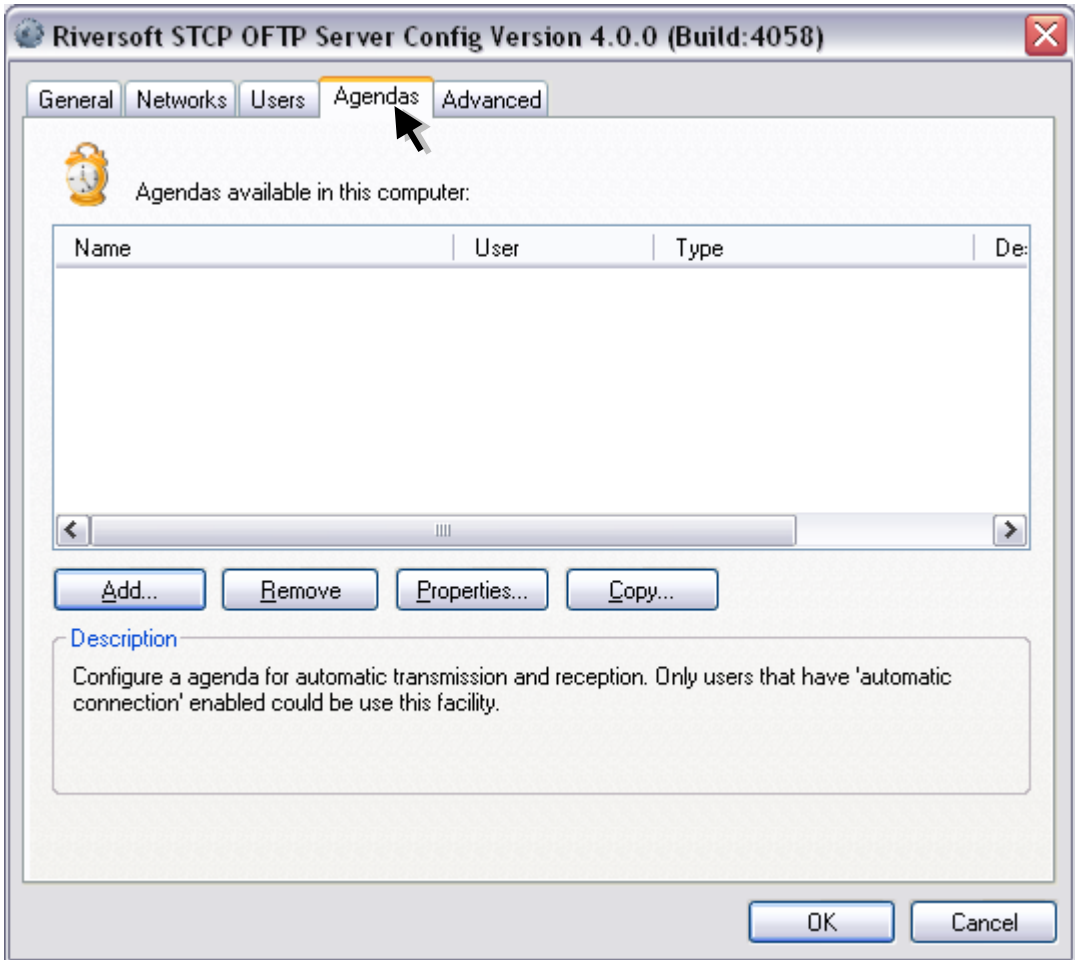
Userdata

File reception control	The options defined in this group will be used by STCP OFTP Server to validate the connection information (IP address, port, address, X.25, SSL3 certificate etc.).
File filter	Fill this field with a regular expression to validate the filename.
Maximum length	Fill this field with the maximum size that a file may have to be transferred.
Create reference of the file received	This option controls the file duplicate, creating a file reference in the directory Restart.

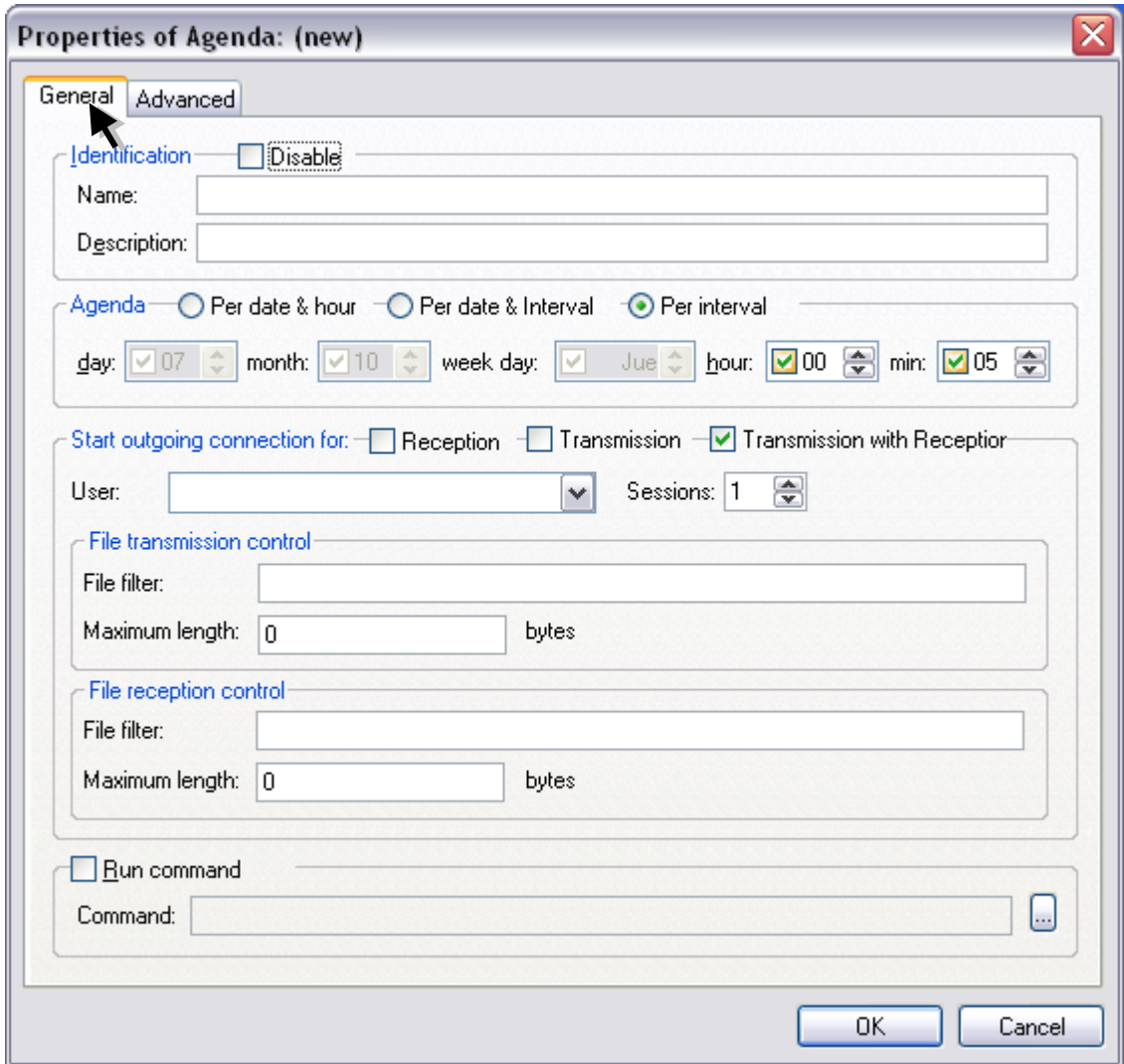
Press **OK** button to continue or **Cancel** to abandon without changing the settings.

On the **Schedule** tab you can add, remove, modify or copy the configuration parameters of a schedule of STCP OFTP Server service.

49. Click the **Add** button.



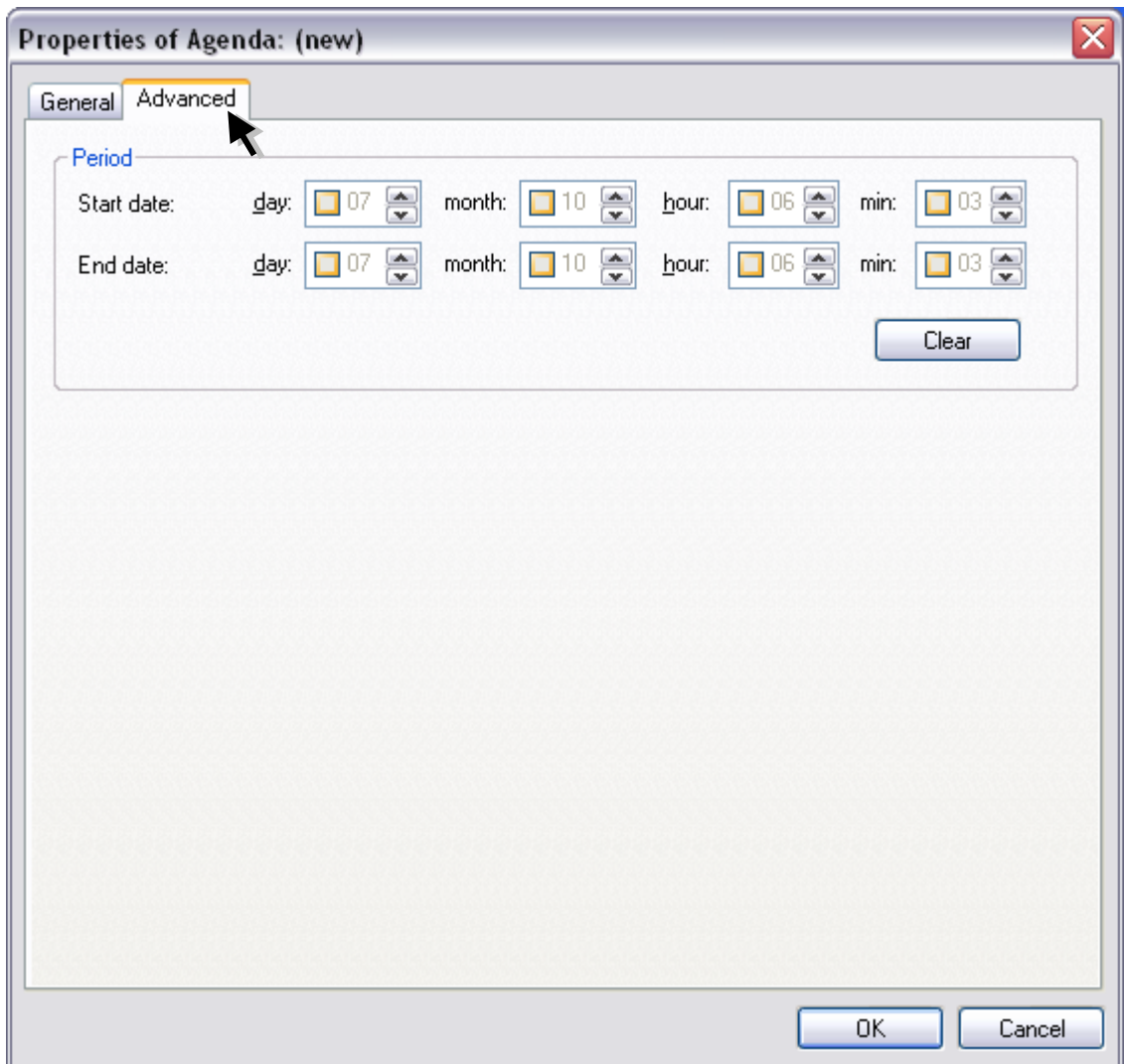
50. On **Properties of schedule**, fill in the fields with the information described below.



Fields	Description
Disable	This option disables the agenda execution when checked.
Name	Fill this field with the desired name for the new schedule.
Description	Fill this field with the description for the new schedule.
Agenda	This group of options allows selecting the operating mode of the schedule. Note: You can enable the fields that are not needed to use in the desired mode.
Per date & time	This option enables the operating mode of the schedule for the date and time specified.
Per date & interval	This option enables the operation mode set of the schedule for the specified date and continuous time interval.

Per interval	This option enables the operation mode of the schedule only for continuous time interval.
Start outgoing connection for:	This group of options allows selecting the operation mode of the connection for transfer. Note: A connection will only be started for the User who have enabled and configured the automatic connection.
Reception	This option enables or disables the reception of files during the execution of the schedule. Note: If this option is enabled, a connection will be established to check for new file to receive.
Transmission	This option enables or disables the transmission of files during the execution of this schedule. Note: If this option is enabled and there is no file to send, the connection is not established.
Transmission with reception	This option enables or disables the transmission and reception of files during the execution of this schedule. Note: If this option is enabled and there is no file to send, the connection is not established.
User	Select this field the User associated with the schedule of the outgoing connection.
Sessions	Fill this field with the amount of transfer sessions to be activated. Note: This amount should be less than or equal to the number of sessions configured for the User.
File transmission control	The options defined in this group are used by STCP OFTP Server in the treatment of transfers (transmission and reception) of this schedule. Note: These settings will override those set for the User.
File filter	Fill this field with a regular expression to validate the filename.
Maximum length	Fill this field with the maximum size that a file may have to be transferred.
Run command	This option enables or disables the execution of a external command (executable or bat).
Command	Fill this field with the application name (executable or bat) to be executed by this Schedule.

51. On the **Advanced** tab set the period of agenda.



Fields	Description
Start date	Check the start time of the agenda execution.
End date	Marque a opção de hora de término da execução da agenda. Check the end time of the agenda execution.
Clean	Click the Clean button to disable the options of start and end date of agenda execution.

Definition of internal variables of the STCP OFTP Server

The internal variables of STCP OFTP Server can be used as parameters to external commands.

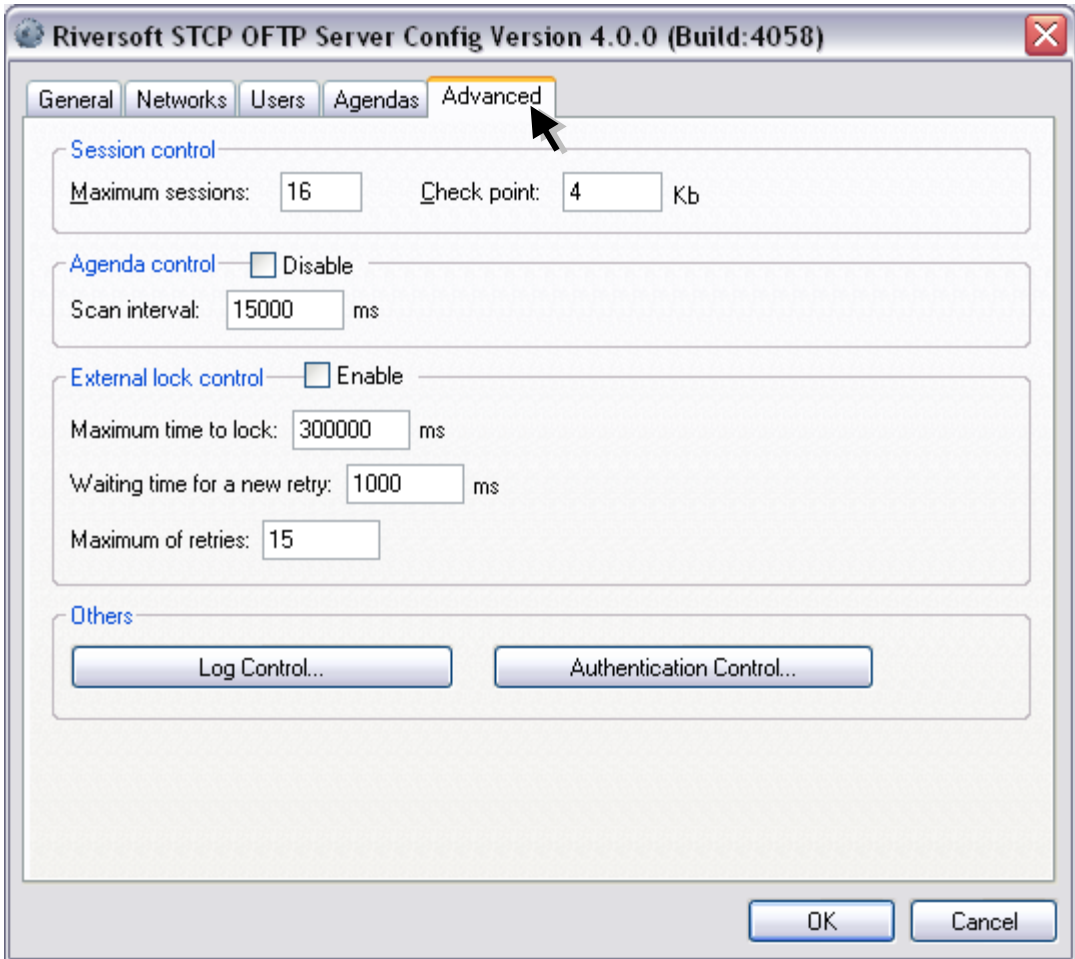
Variable	Description
\$DEFPARAM	Variable that contains the default value for the external command.
\$DIRSYS	Variable that contains the directory name of control.
\$DIRDATA	Variable that contains the name of the data directory.
\$LUSERID	Variable that contains the user name.
\$LFNAME	Variable containing the full name of the local directory.
\$OFNAME	Variable that contains the ODETTE filename.
\$OFTYPE	Variable that contains the record type of the ODETTE file.
\$OFRECLEN	Variable that contains the record size of the ODETTE file.
\$OFSIZE	Variable that contains the approximate size of the ODETTE file.
\$OFDATE	Variable that contains the ODETTE file date.
\$OFTIME	Variable that contains the time of the ODETTE file.
\$OFUSERDATA	Variable that contains the userdata of the ODETTE file.
\$OFORIGINATOR	Variable that contains the origin of the ODETTE file.
\$OFDESTINATION	Variable that contains the destiny of the ODETTE file.

Definition of the default value of the parameter

Execute command to:	Default value of parameter.
Start of connection	Directory name of user data.
End of connection	Directory name of user data.
End of file transmission	Full name of the file.
Read the file	Full name of the file.
Save the file	Full name of the file.
Schedule	Name of the Schedule.
Events (LOG)	Line with the event details

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

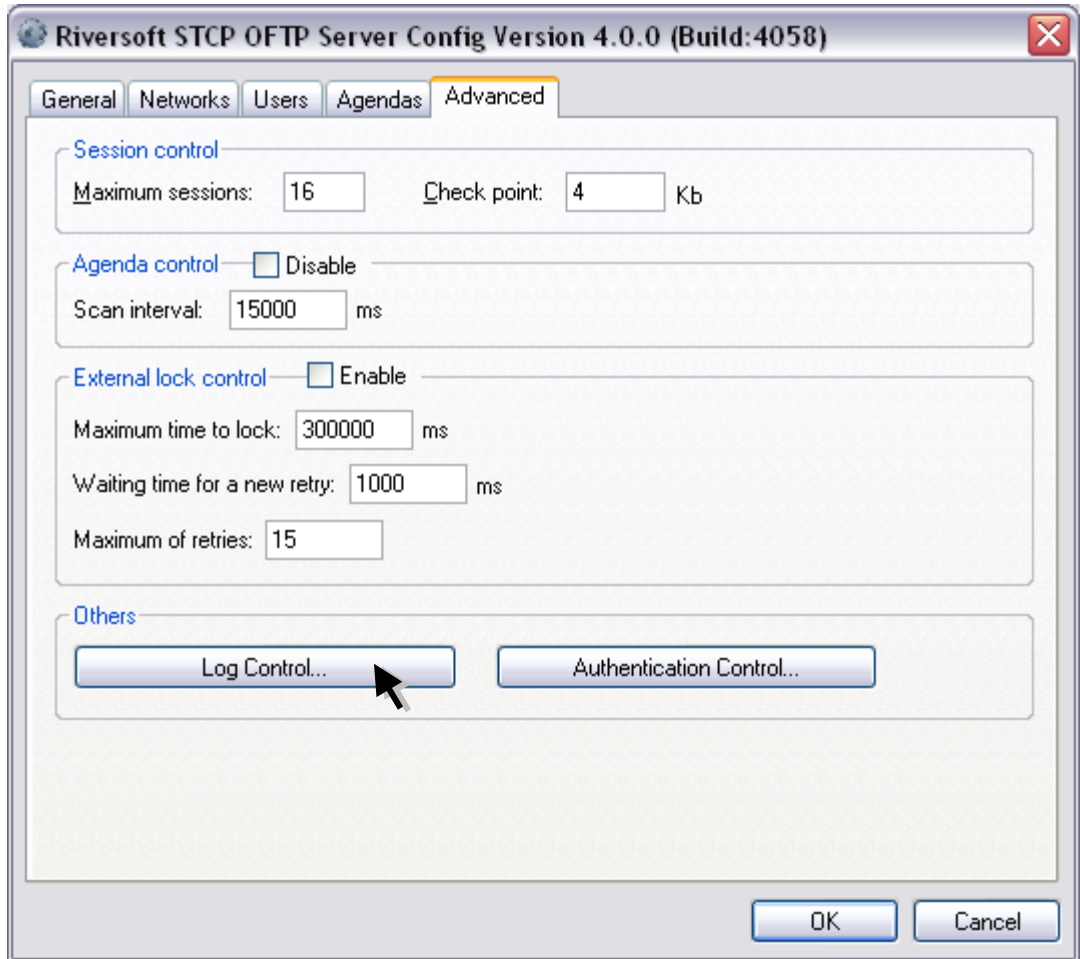
52. On **Advanced** tab fill the fields with the information described.



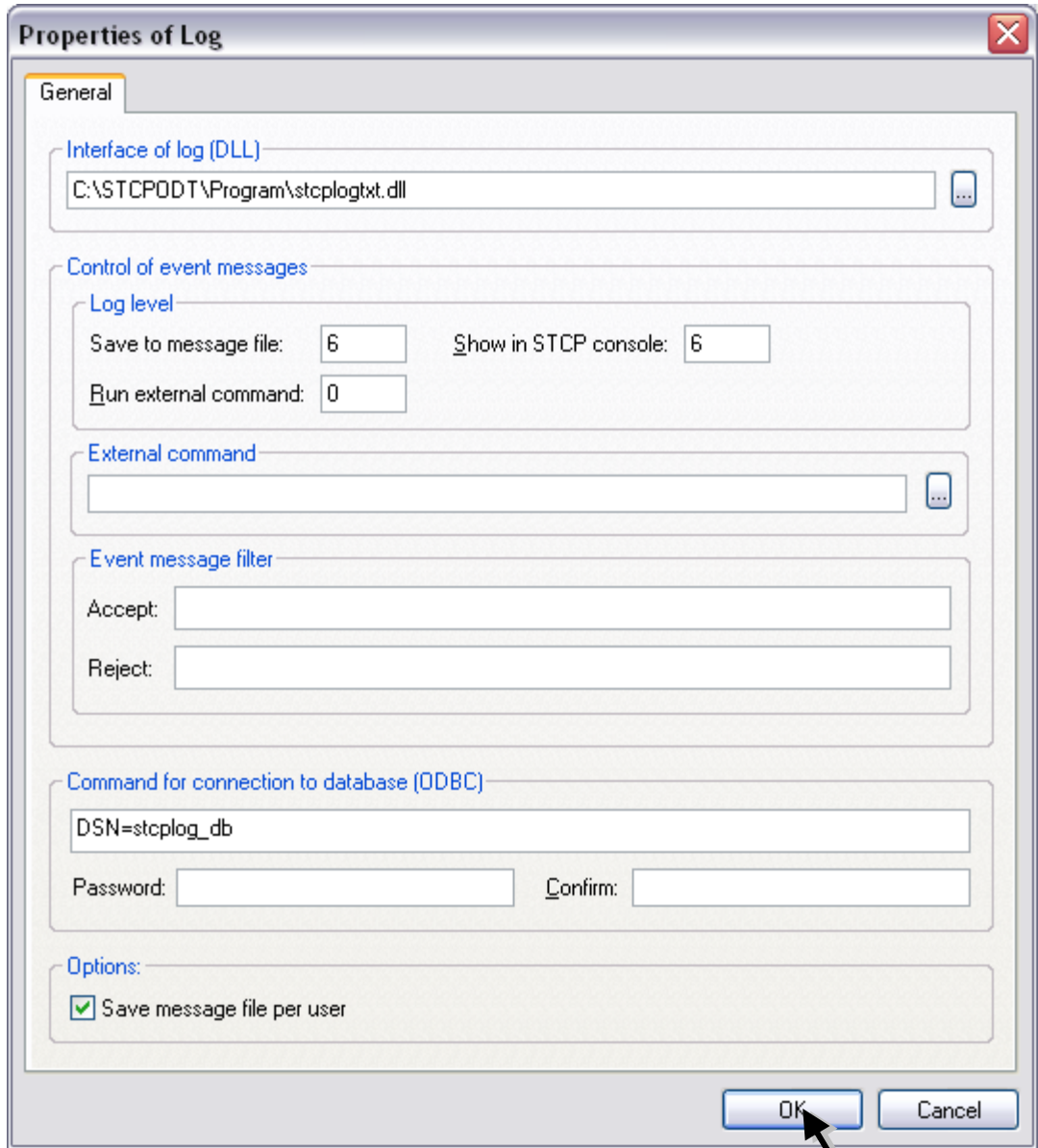
Fields	Description
Maximum sessions	This field reports the maximum number of concurrent sessions of transfer that can be activated by the service. Note: Limited to ten (10) concurrent sessions in the STCP OFTP Server Lite version.
Check Point	Fill this field with the multiple of the amount of data received to the STCP OFTP Server force a physical write of the file. In the case of an interruption of the transfer, the recovery will occur after the last check point position correctly recorded.
Agenda control	Check "Disable" or leave unchecked.
Disable	Cancels the Agenda.
Scan interval	Fill this field with the minimum time interval of the agenda processing in milliseconds.
Enable	Enables control of external lock when checked.
Maximum time to lock	Maximum time that the file remains locked.

Waiting time for a new retry	Waiting time for another attempt to process the file.
Maximum of retries	Number of attempts to process the file.
Log control	The options in this group control the configuration properties of the system logs.
Authentication control	The options in this group control the type of authentication used by STCP OFTP Server to validate a User. The authentication is available by Operating System Note: We recommend the use of STCP authentication.

53. Then click the **Log Control...** button.



54. On the **General** tab of the Properties of the Log fill the fields described below.



Fields	Description
Interface of log (DLL)	Writes to text file if the DLL selected is stcplogtxt.dll or writes to database if the DLL is logodbc.dll.
Save to message file	Fill this field with the level of event that will be stored in the message.
Show in STCP Console	Fill this field with the level of event that will be shown in the message window of the STCP OFTP Server.
Run external command	Fill this field with the level of event that will trigger an external command (program or bat).

External command	Fill this field with the name of the external command (program or bat).
Accept	Records in the log files or database of STCP.
Reject	No records in the log files or database of STCP.
Command for connection to database (ODBC)	Connection string for ODBC data source. Tell DSN, UID (username) and PWD (password).
Password	Enter the password to access the database.
Confirm	Fill this field with the specified password in the Password field for validation.
Save message file per user	This option enables or disables the generation of the message file of the events individually for each User. Note: The message file is generated in the LOG subdirectory for each user.

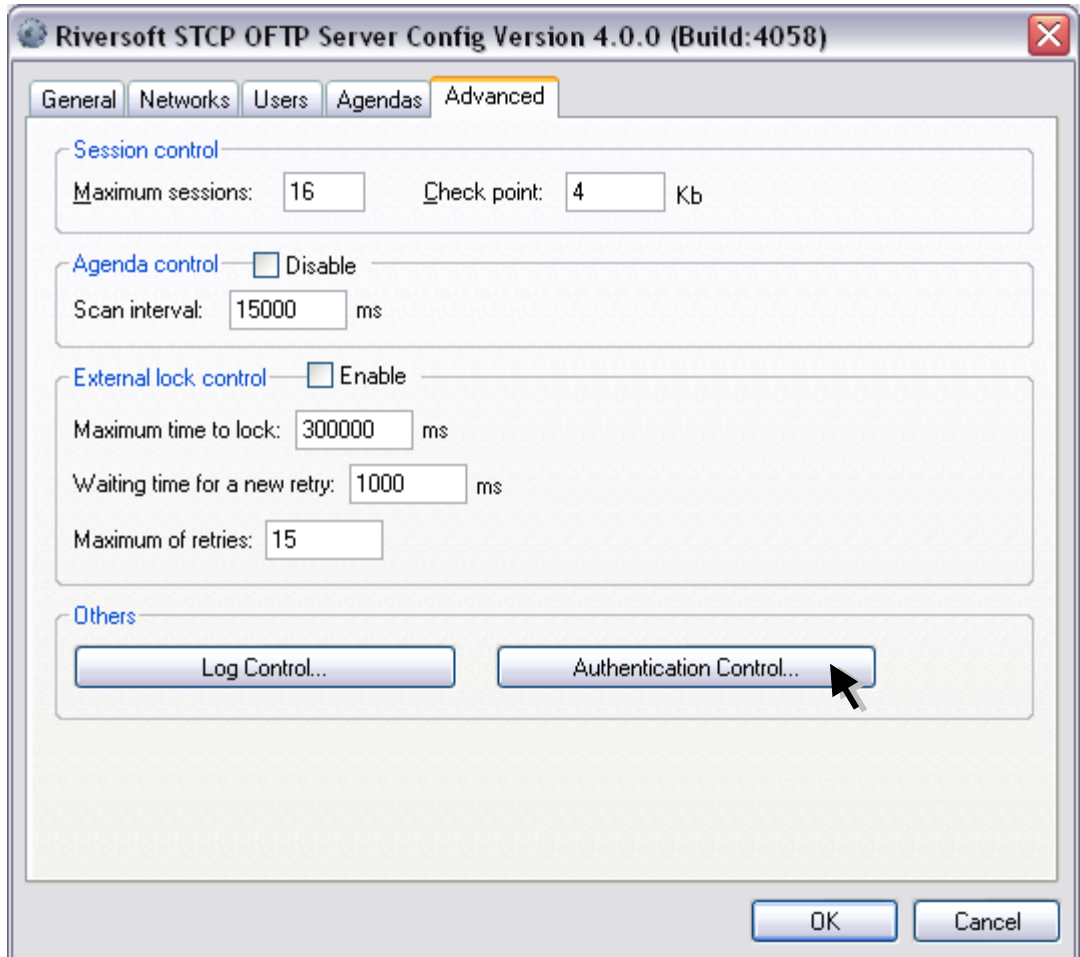
Table describing the Level of the event

Level of the event	Description
0	The events of start and end of the application.
1	The events that contain any errors.
2	The events of end of the operation of cancellation of waiting for a connection.
3	The events of start and end of cancellation of the connections.
4	The events of start and end of connection, start and end of session, start and end of transmission or start and end of reception with success.
5	Not defined.
6	Not defined.
7	The events of start and end of the processing unit (threads).
8	The events of start and end of the schedule.

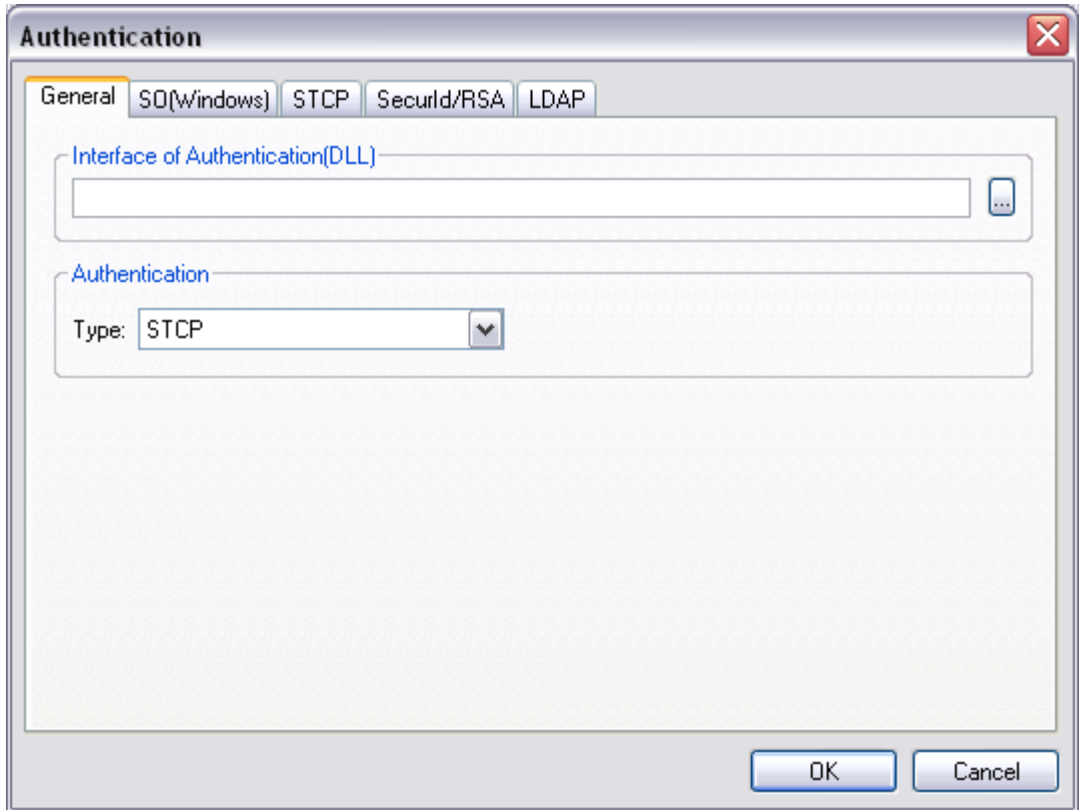
Note: The events associated with a level less than or equal to the selected will be processed.

Press **OK** button to continue or **Cancel** to abandon without changing the settings.

55. Click the **Authentication Control...** button.

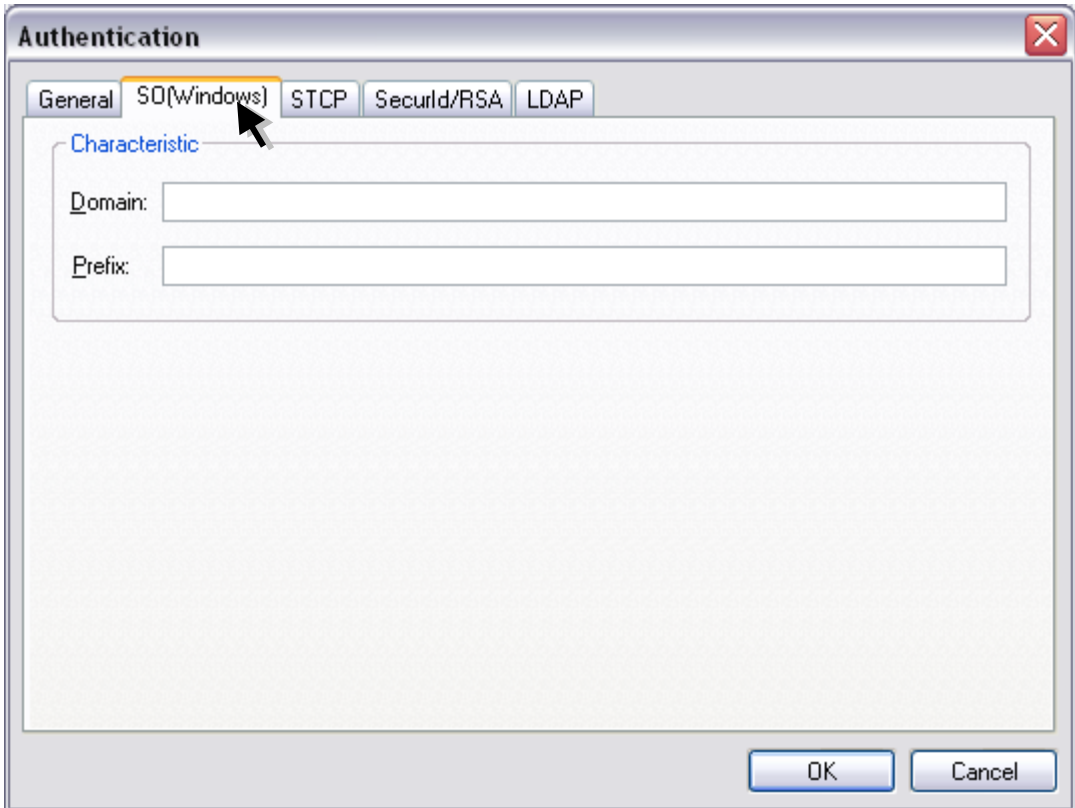


56. On the **General** tab of the Properties of the Log fill the fields described below.



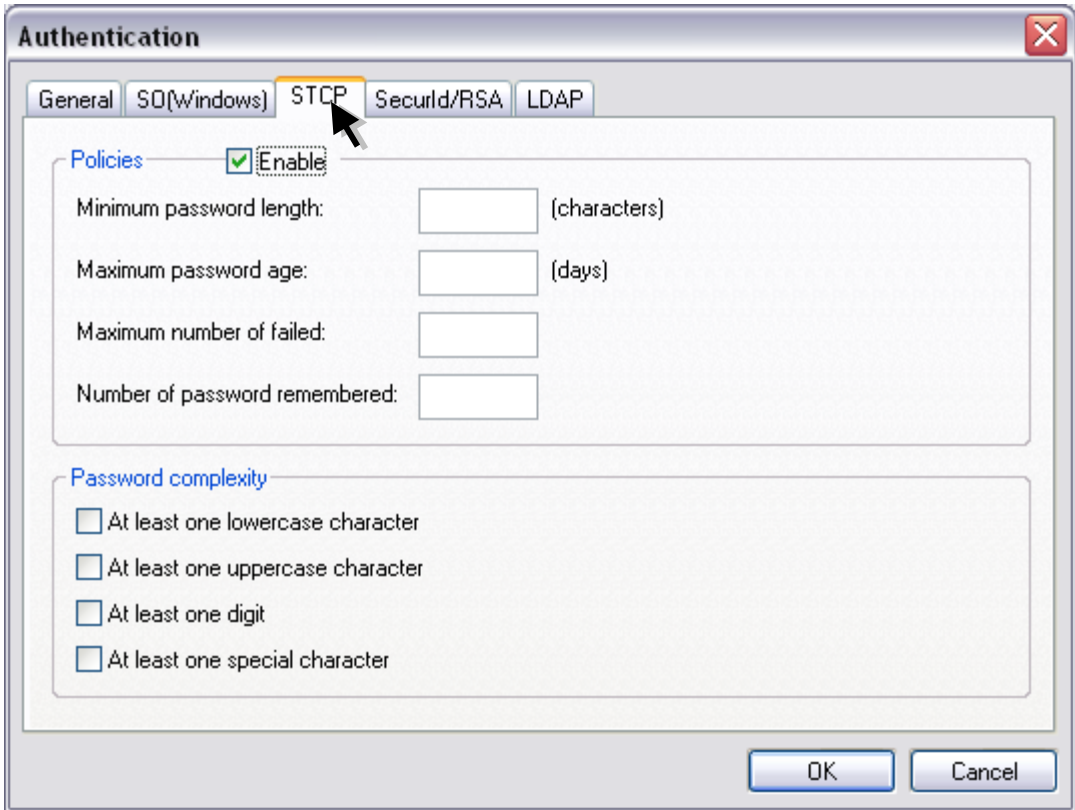
Fields	Description
Interface of Authentication (DLL)	Parameter provides the library used to configure the authentication interface of STCP.
Type	Authentication types supported by STCP OFTP Server: SO(Windows), STCP (Native Authentication of the application), SecurId/RSA, LDAP.

57. On the **SO(Windows)** tab fill the following fields.



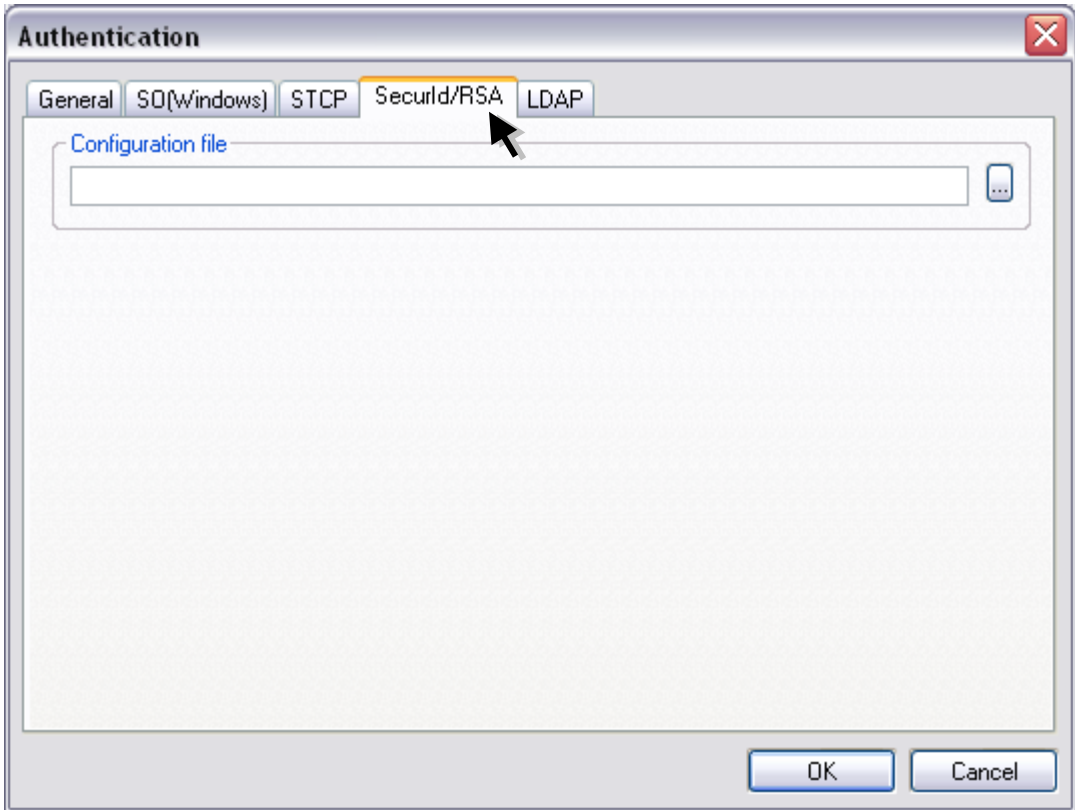
Fields	Description
Domain	Domain of the operating system.
Prefix	Prefix for mask for the user.

58. On the **STCP** tab enable or disable the following options.



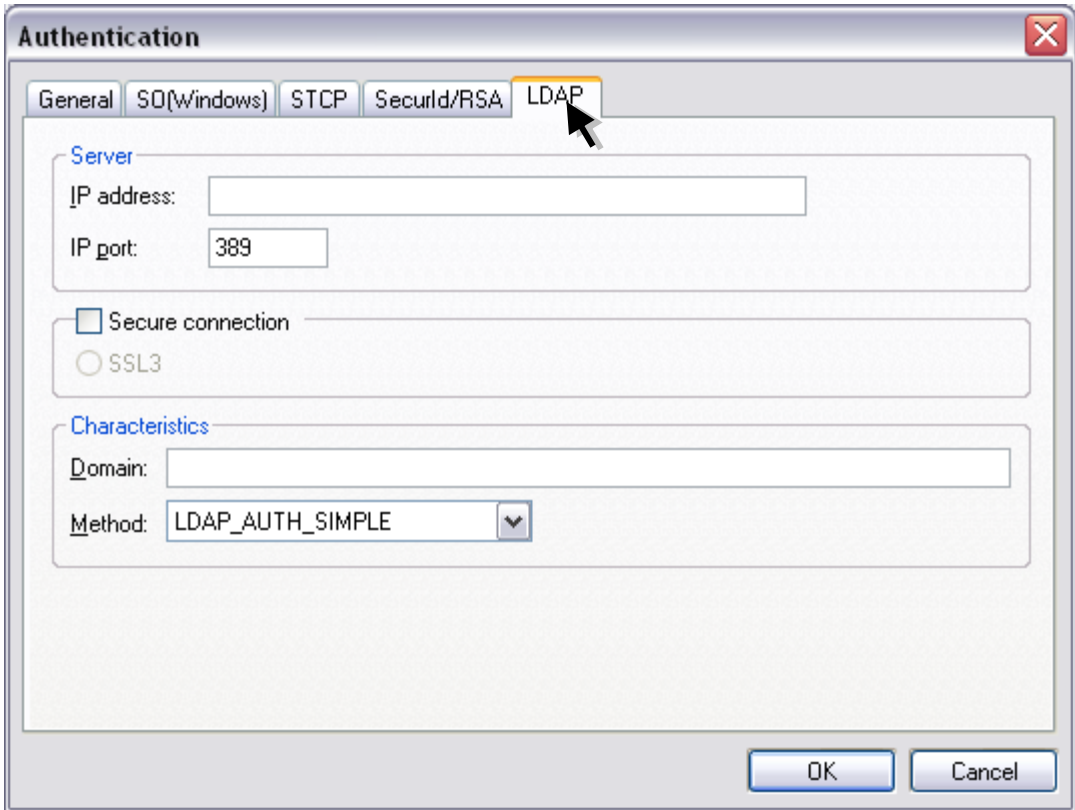
Fields	Description
Enable	This option enables the policy options and complexity of the password when checked.
Minimum password length	Minimum number of characters for a password.
Maximum password age	Maximum number of days for a password expires.
Maximum number of failed	Maximum number of authentication retries.
Number of password remembered	Number of passwords that can be stored by STCP.
At least on lowercase character	This option forces the creation of passwords with at least one lowercase character.
At least uppercase character	This option forces the creation of passwords with at least one uppercase character.
At least one digit	This option forces the creation of passwords with at least one numeric character.
At least one special character	This option forces the creation of passwords with at least one special character.

59. On the **SecurId/RSA** tab fill the following field.



Fields	Description
Configuration file	Parameter that provides the settings for SecurId/RSA authentication.

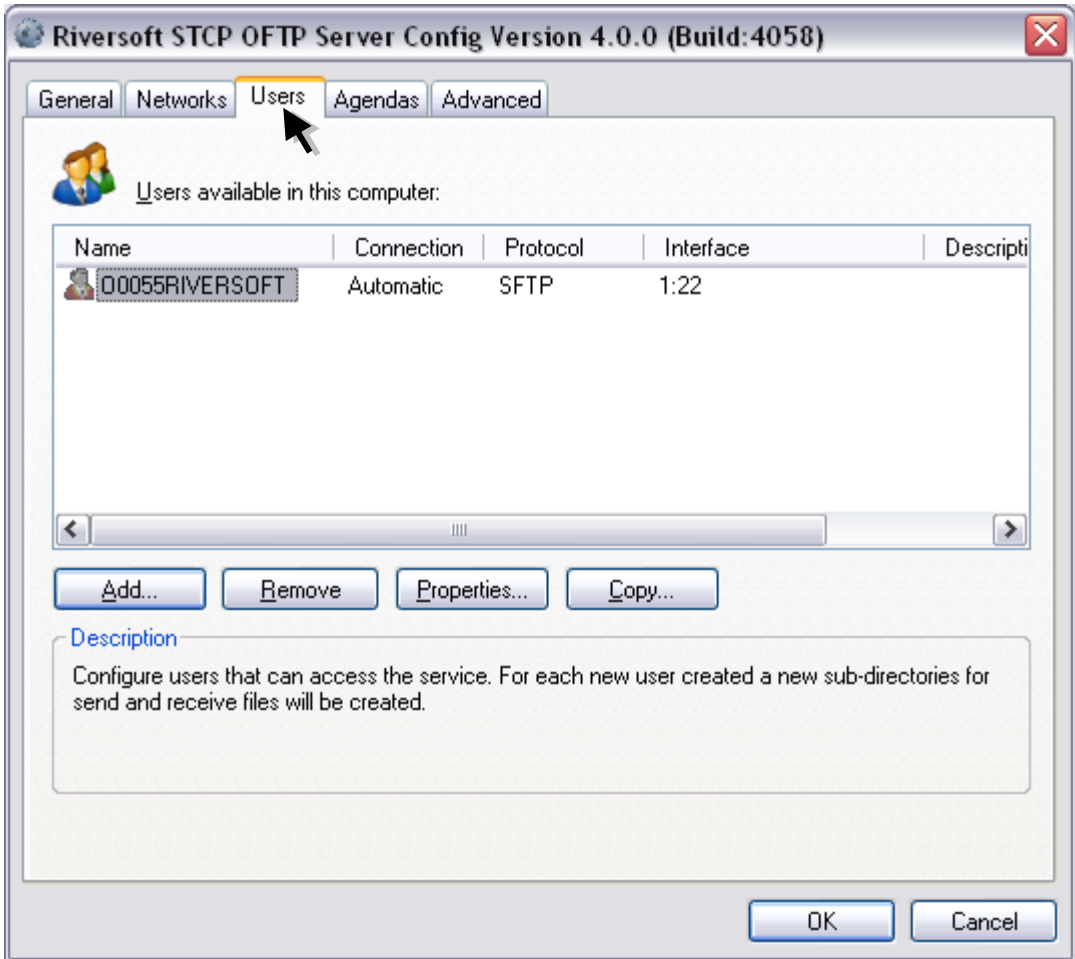
60. On the **LDAP** tab fill the following field.



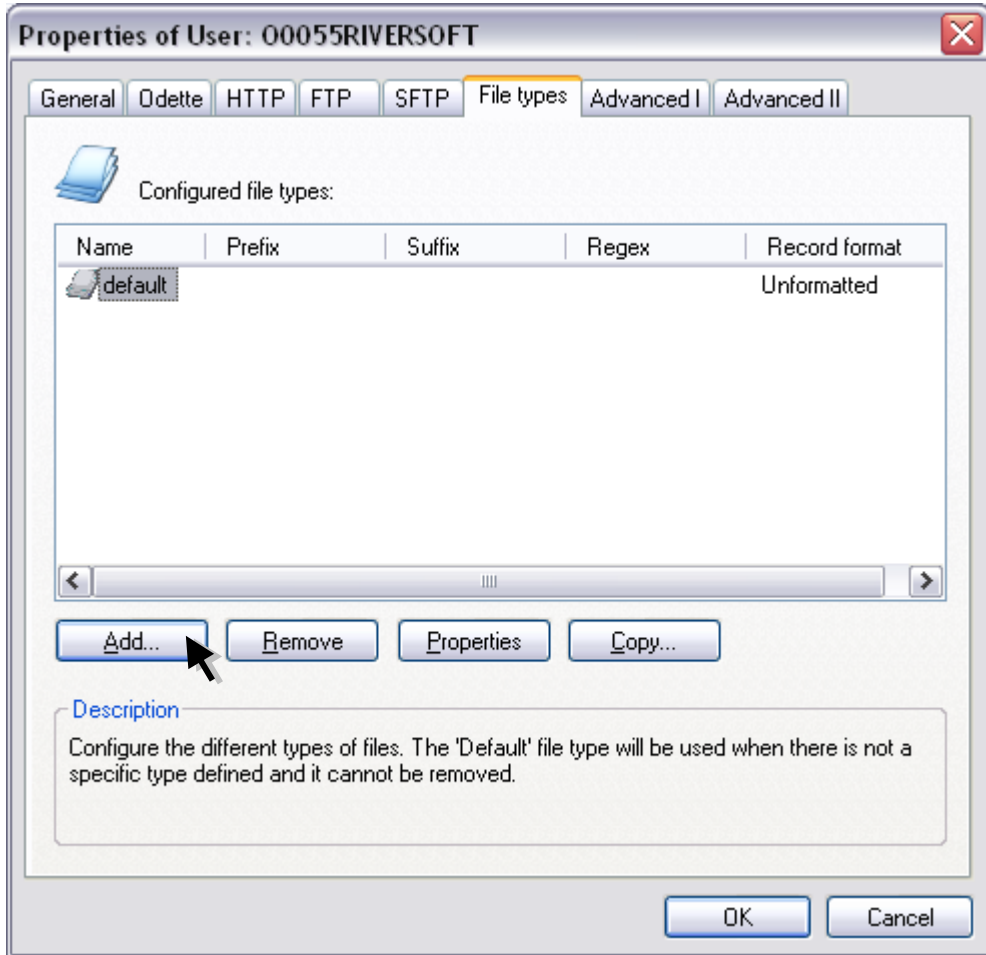
Fields	Description
IP address	Fill this field with the TCP / IP address or name (DNS) of the server STCP OFTP Server.
IP port	Fill this field with the TCP/IP port of the STCP OFTP Server. Note: The default port of the service is 389.
Secure communication	This option enables or disables the use of the encryption in communication with the STCP OFTP Server, you can choose between the option Native or SSL3. Note: Before you enable this option, read the chapter about Security.
SSL3	Sets a secure communication with encryption and digital certification, with the use of definite standard in RFC2246 (TLS1/SSL3). The TLS1/SSL3 is commonly found in servers of secure sites (HTTPS) and offers the highest level of security currently available. Note: Before you enable this option, confirm that the server you want to communicate supports this feature.
Domain	Domain of the authentication server.
Method	Methods used by protocol LDAP: LDAP_AUTH_SIMPLE, LDAP_AUTH_DIGEST, LDAP_AUTH_DPA, LDAP_AUTH_MSN, LDAP_AUTH_NEGOTIATE, LDAP_AUTH_NTLM, LDAP_AUTH_SICILY, LDAP_AUTH_SSPI

Click the **OK** button to continue or **Cancel** to abandon without changing the settings.

61. On the **Users** tab select the user and click the **Properties** button.



62. On the **File Types** tab click the **Add** button.



The setting of a File Type enables to change some features in the transfer of the file, such as converter name or file format, data encoding, start an application or bat and others.

The type Default exists and should always be used in cases where there is a specific type defined for the transfer in progress.

The association between a File Type and file itself can be established in three distinct ways:

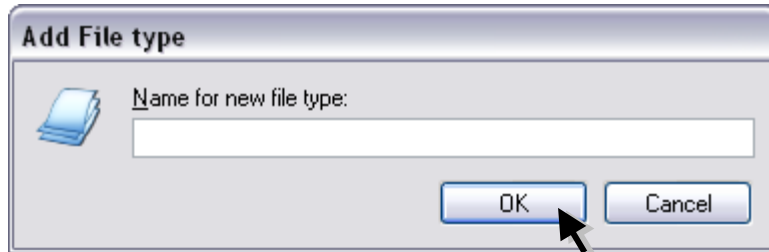
Type	Description
1	Through the file name and the type name.
2	Part of the file name and values defined in the Prefix and Suffix properties of the type.
3	The filename and values defined in a regular expression.

Note: For more detailed information about regular expression (RegEx), visit www.pcre.org.

The table below shows the association of the filename with the specific type:

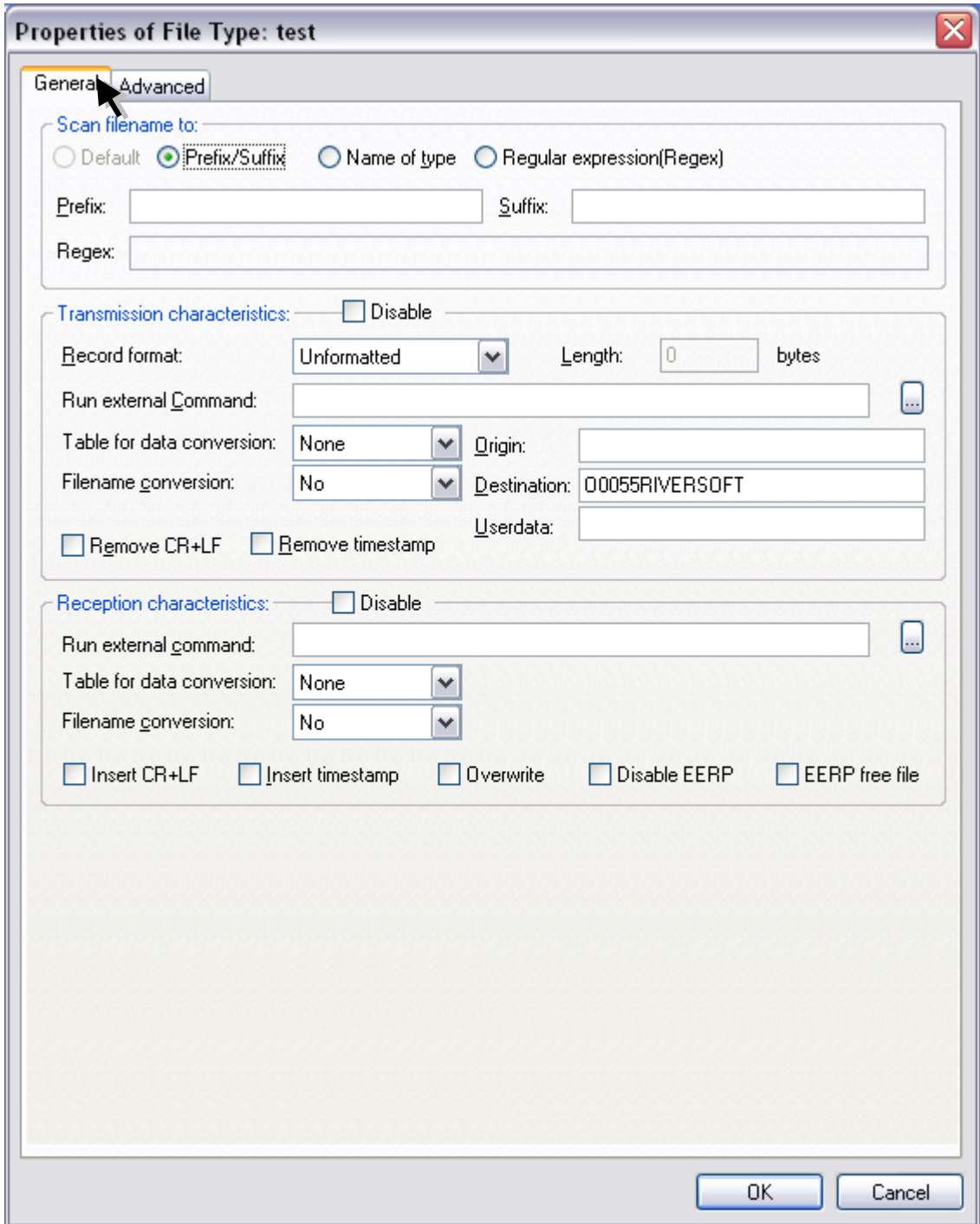
Name Type	Type	Prefix	Suffix	RegEx	Filename	Association
TEST.0	1	—	—	—	TEST.0	Yes
					TEST.TXT	No
TEST.1	2	TEST	—	—	TEST.TXT	Yes
					TXT.TEST	No
TEST.2	2	—	TEST	—	TXT.TEST	Yes
					TXT.TXT	No
TEST.3	3	—	—	T.T	TXT.TXT	Yes
					TXTTXT	No
Default	—	—	—	—	TXTTXT	Yes

63. Enter the name of the **Name of the new file type** and click the **OK** button.



Fields	Description
Name of the new file type	Fill this field with the desired name for the new type. Note: Do not use special characters or blanks.

64. On **Properties of the file type**, configure the following options.



Fields

Description

Scan filename to:

The options defined in this group are used by STCP OFTP Server to define how to associate file name to type: Standard (Default),

Prefix/Suffix, type name, Regular Expression.

Note: The type name associates the name of the file name of the file type created.

Prefix	Fill this field with the prefix of the file name to be associated with this type.
Suffix	Fill this field with the suffix of the file name to be associated with this type.
Regular Expression	Fill this field with the regular expression that should be associated with this type.
Transmission characteristics	The options defined in this group are used by STCP OFTP Server to define the characteristics of the file transmission.
Disable	This option disables the characteristics of the transmission.
Record format	This option allows to select the format of the file record, they are: Not Formatted, Fixed and Variable. Note: Only use Fixed or variable when the server Odette is a version of mainframe (large) and this feature is enabled.
Length	Fill this field with the amount of characters (bytes) that make up the record. Note: Only use this option when the record format is Fixed or Variable.
Run external command	Fill this field with the name of an application or batch file (bat) to be executed after sending the file successfully.
Table for data conversion	This option allows to select the table of conversion of the data in the transmission, they are: None, ASC2EBC.TAB (converts from ASCII to EBCDIC) and EBC2ASC.TAB (converts from EBCDIC to ASCII).
Origin	Fill this field with the Odette ID (OID) of origin of the file. Note: When the User is created, this field contains the local identification.
Filename conversion	This option allows selecting the conversion of the file name before sending, they are: No, uppercase or lowercase.
Destination	Fill this field with the the Odette ID (OID) of the file destination. Note: When the user is created, this field contains the remote identification.
Userdata	Fill this field with the extra data associated with Odette ID informed. Note: Complete this field only if requested by the server.
Remove CR+LF	This option allows enabling or disabling the removal of the characters CR (Carriage Return) and LF (Line Feed) in the transmission of the file. Note: Only use this option when the record format is Fixed or Variable.
Remove Timestamp	This option allows enabling or disabling the removal of the external timestamp of the file name.
Reception characteristics	The options defined in this group are used by STCP OFTP Server to define the characteristics of the file at the reception.

Disable	This option disables the characteristics of the transmission.
Run external command	Fill this field with the name of an application or batch file (bat) to be executed after receiving the file successfully.
Table for data conversion	This option allows selecting a conversion table in the reception of data, they are: None, ASC2EBC.TAB (converts from ASCII to EBCDIC) and EBC2ASC.TAB (converts from EBCDIC to ASCII).
Filename conversion	This option allows selecting the conversion of the file name before sending, they are: No, uppercase or lowercase.
Insert CR+LF	This option lets you enable or inhibit the insertion of the characters CR (Carriage Return) and LF (Line Feed) on receipt of the file. Note: Only use this option when the record format is Fixed or Variable.
Insert Timestamp	This option lets you enable or disable the insertion of external timestamp on the filename.
Overwrite	This option enables or disables the overlap of the file when there is already a file with the same name.
Disable EERP	This option disables the sending of the EERP Odette command (End to End Response) at the end of receiving the file successfully. Note: Only use this option if the server supports this feature.
EERP free file	This option allows enabling or disabling the treatment of the file received only after sending the Odette EERP (End to End Response). Note: Only use this option if the server supports this feature.

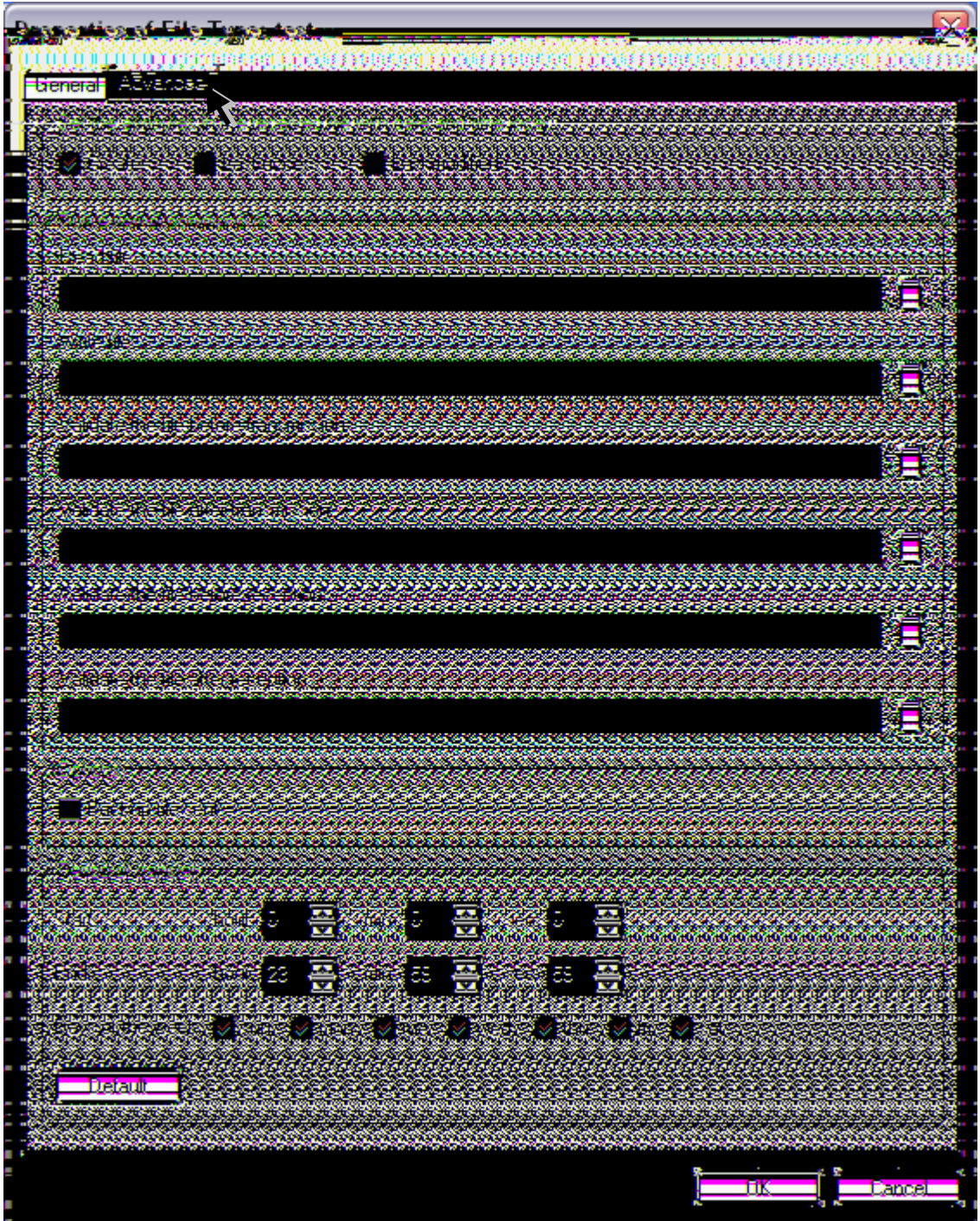
Format of the external Timestamp of the file

The use of external timestamp of the file has the following format:

<filename>.YYYYMMDDhhmmssnnn

<filename>	File name without spaces or special characters.
YYYY	Year
MM	Month
DD	Day
Hh	Hour
mm	Minute
ss	Seconds
nnn	Miliseconds

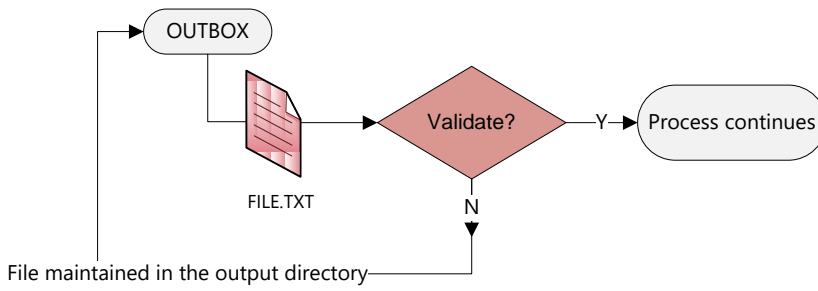
65. On the **Advanced** tab set the following options to the type of file.



Fields	Description
Set the attributes in the received file with date and time local:	This option enables or disables the insertion of local date and time the file received for the corresponding attributes. Note: The date and time of the Odette protocol will be used in attributes disabled.
Read file	Fill this field with the name of an external program that runs for reading the file.
Write file	Fill this field with the name of an external program that will run to perform the recording file.

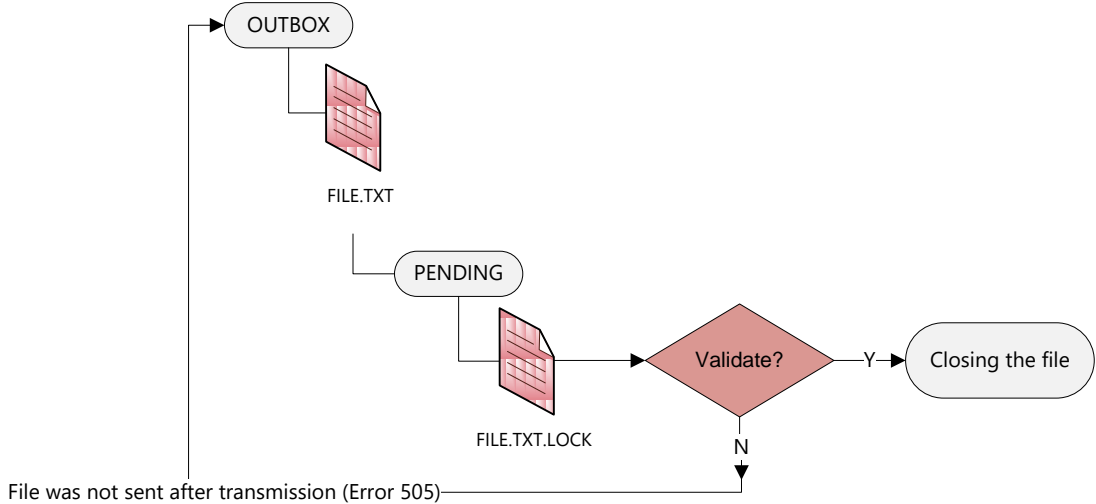
Validate the file before transmission

Executes an external command to validate the file before transmitting. On success (Return code 0), the transmission process is executed.



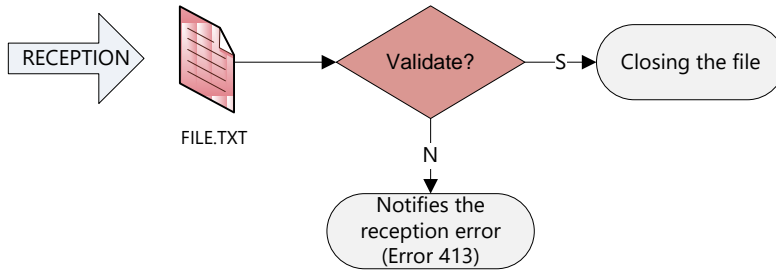
Validate the file after transmission

Executes command to validate the file after transmitting. On success (return code 0), the transmission process is executed.



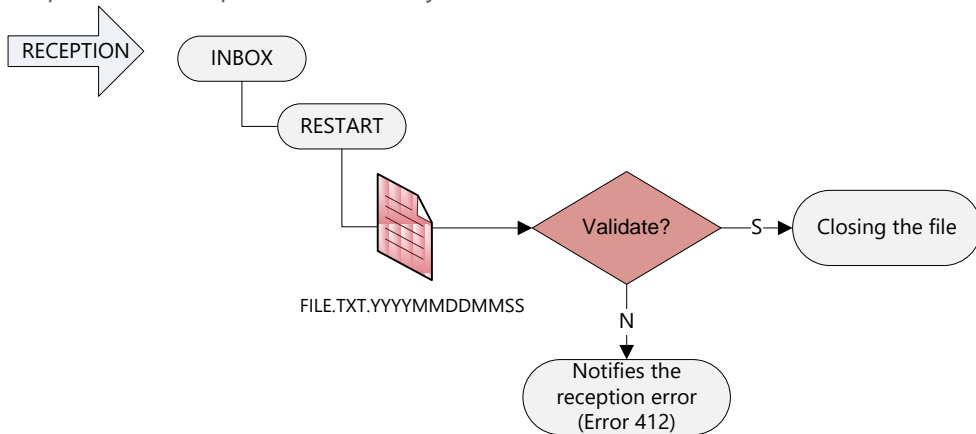
Validate the file before reception

Executes an external command before receiving the file. On success (Return code 0), the file is closed and the reception ended successfully.



Validate the file after reception

Executes an external command after receiving the file, before closing the file. On success (Return code 0), the process is completed successfully.



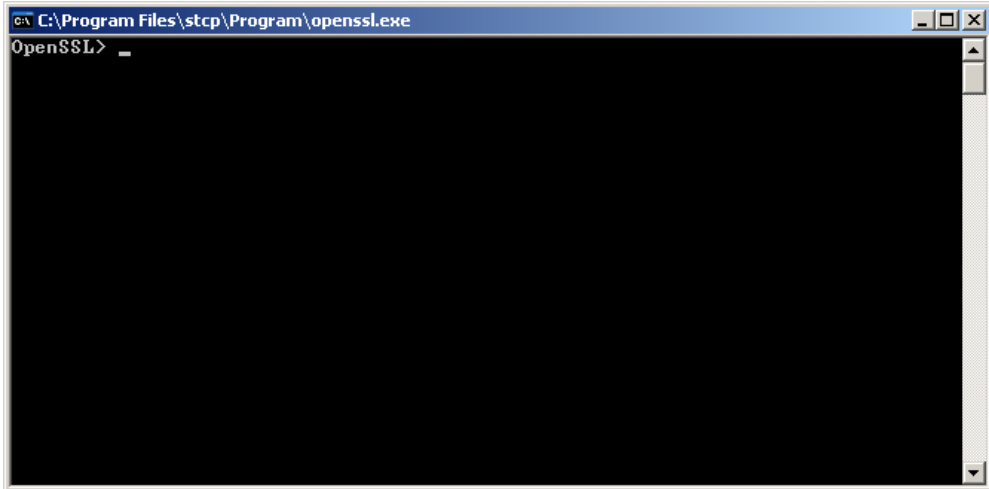
Backup file sent	This option enables or disables the backup of the files transmitted to this type.
Period of transfer	Start and end of a transfer.
Start	Start of the interval of the transfer period.
End	End of the interval of the transfer period.
Days of the week	Reports the days of the week that the transfer may occur.
Padrão	Restores default settings for the transfer period.

Press the **OK** button to save the settings or **Cancel** to abandon without changing the settings.

Generation of private key and certificate of SSL3 authentication

The following procedures should be executed to generate the private key and digital certificate to be used in communication SSL3.

1. At the command prompt, run the application openssl.exe (e.g. C:\STCPODT\Program\openssl.exe) to start the process of generation of asymmetric key pair (private/public).

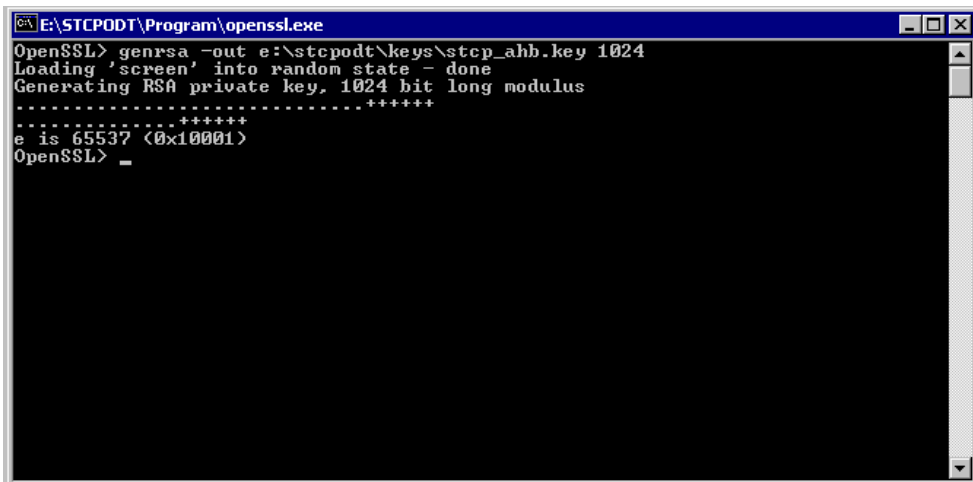


2. Use the following command to generate the private key that is used for encryption of the connection.

```
genrsa -out[unidade_disco][diretorio_instalação_stcp]\keys\[nome_da_chave].key 1024
```

Example:

```
genrsa -out c:\stcpodt\keys\stcp_abcde.key 1024
```



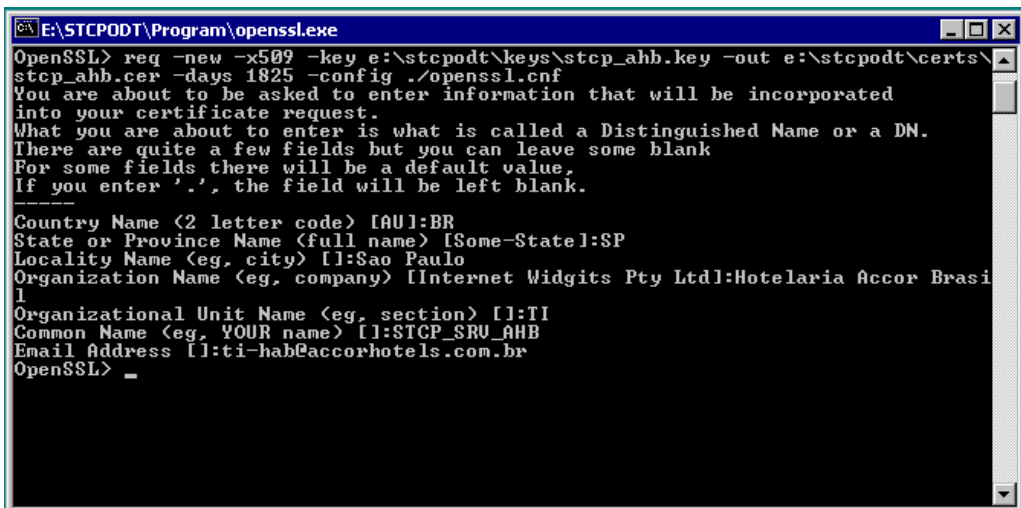
3. The next step is to generate the digital certificate associated with the previously generated key for this use the command below.

```
req -new -x509 -key [unidade_disco][diretório_instalação_stcp]\keys\[nome_da_chave].key -out [unidade_disco][diretório_instalação_stcp]\certs\[nome_do_certificado].cer -days 1825 -config ./openssl.cnf
```

Example:

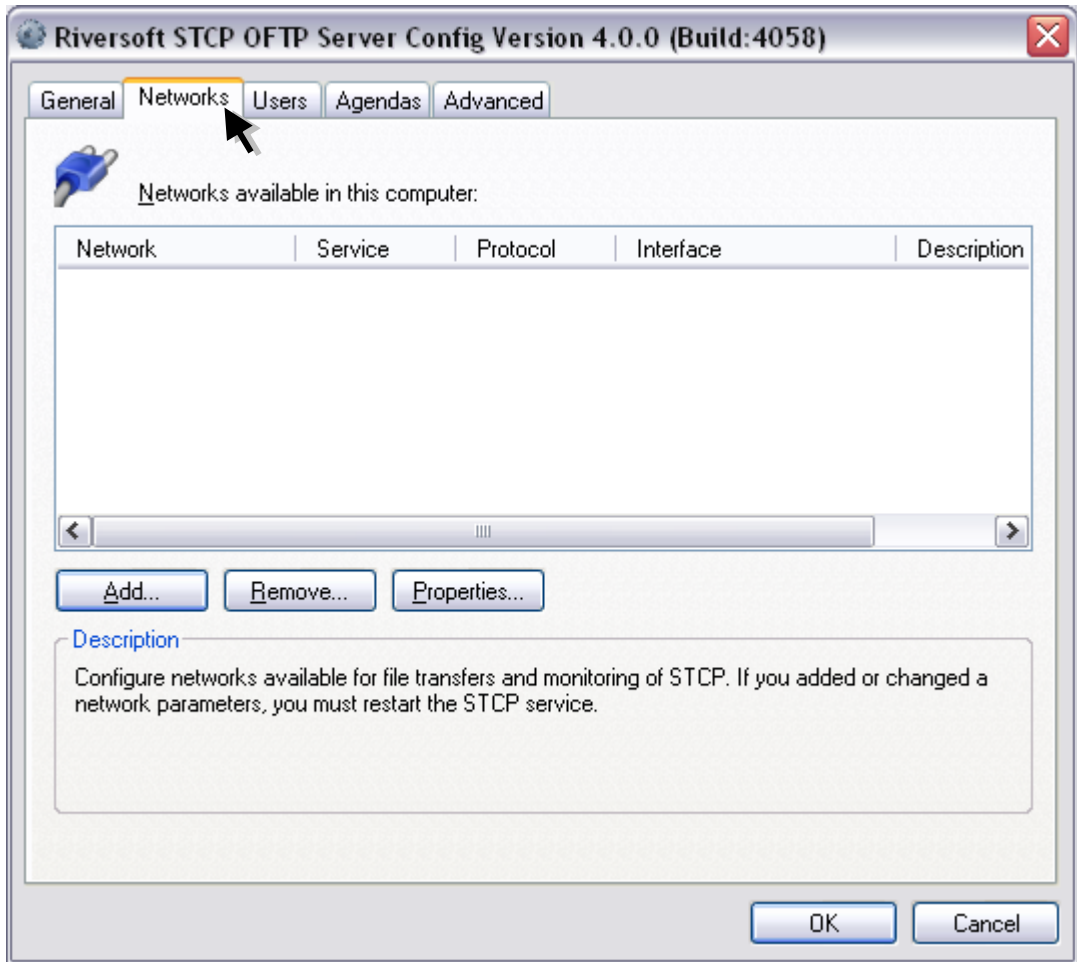
```
req -new -x509 -key c:\stcpodt\keys\stcp_interprint.key -out c:\stcpodt\certs\stcp_abcde.cer -days 1825 -config ./openssl.cnf
```

4. Fill the information requested to complete the process of generation of the Digital Certificate:



Configuration of the transfer interface of the STCP OFTP Server Enterprise/Lite for SSL3 communication

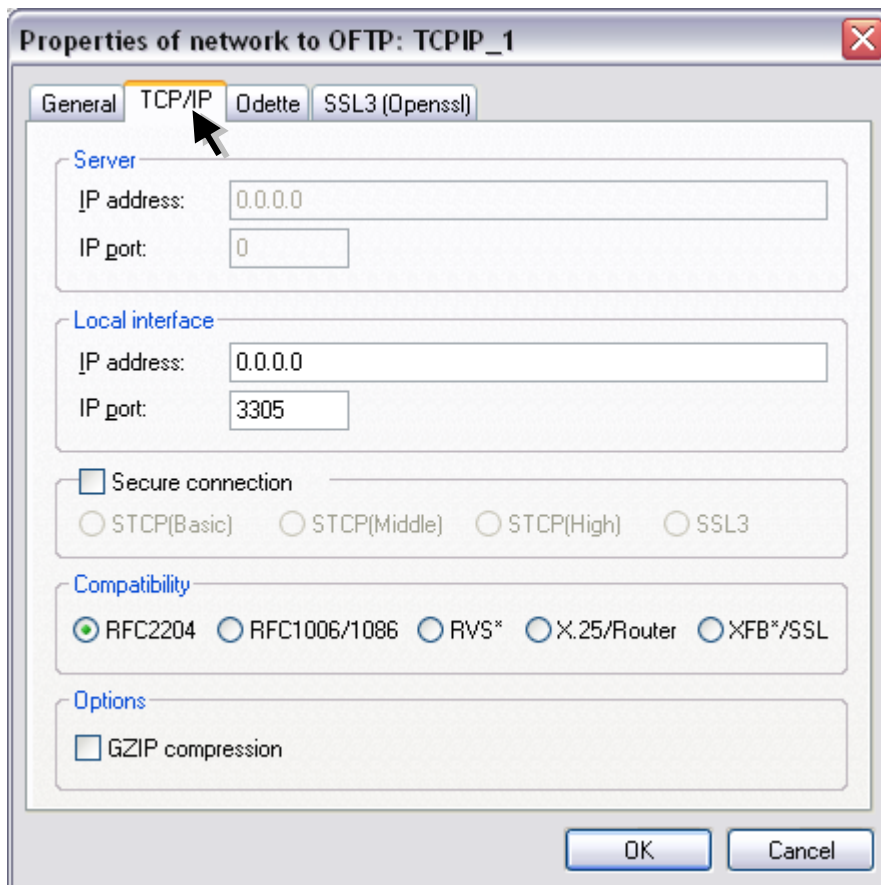
1. To access the STCP OFTP Server Enterprise/Lite configurator, click **Start** and then, click **Riversoft STCP OFTP Server Config**.
2. Access the **Network** tab to add the interfaces that will be available for transfer service and then add a transfer service interface.



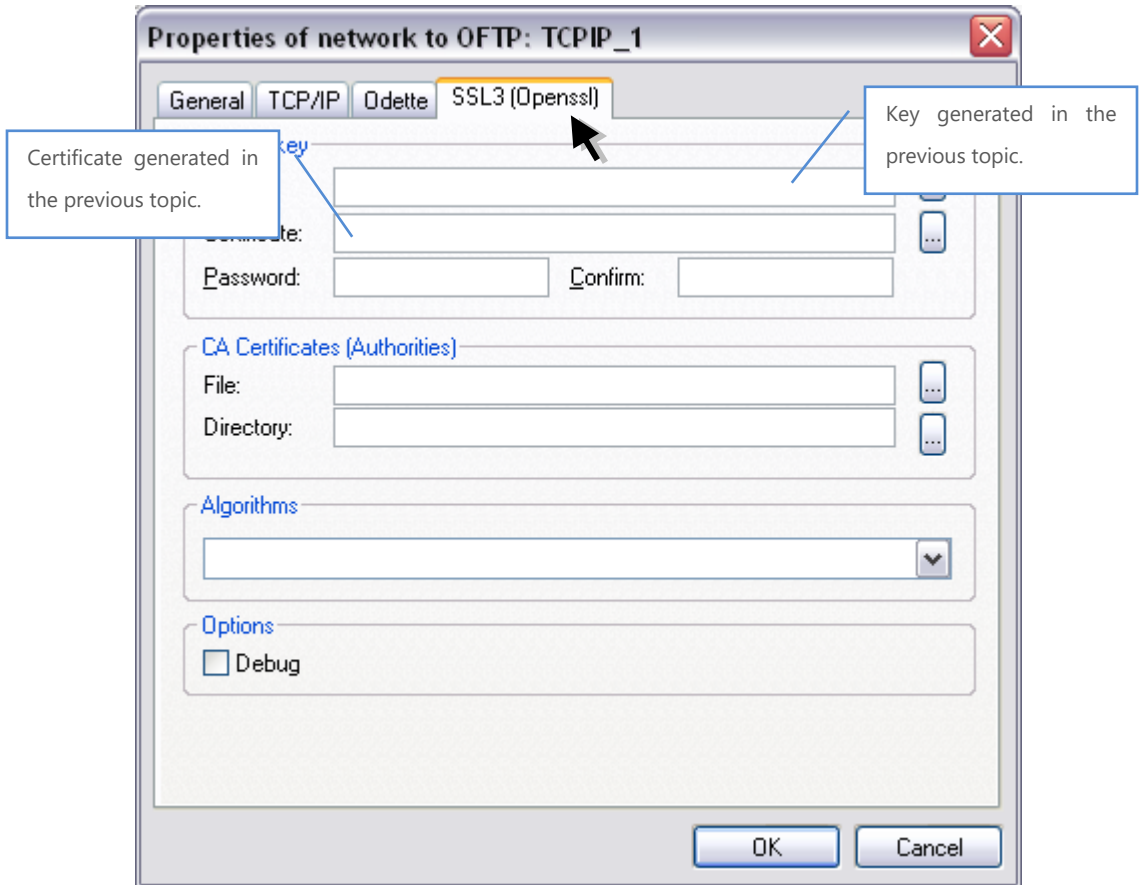
3. Click the **Add** button and select the OFTP – TCP/IP protocol.



4. On the **TCP/IP** tab set the following parameters.

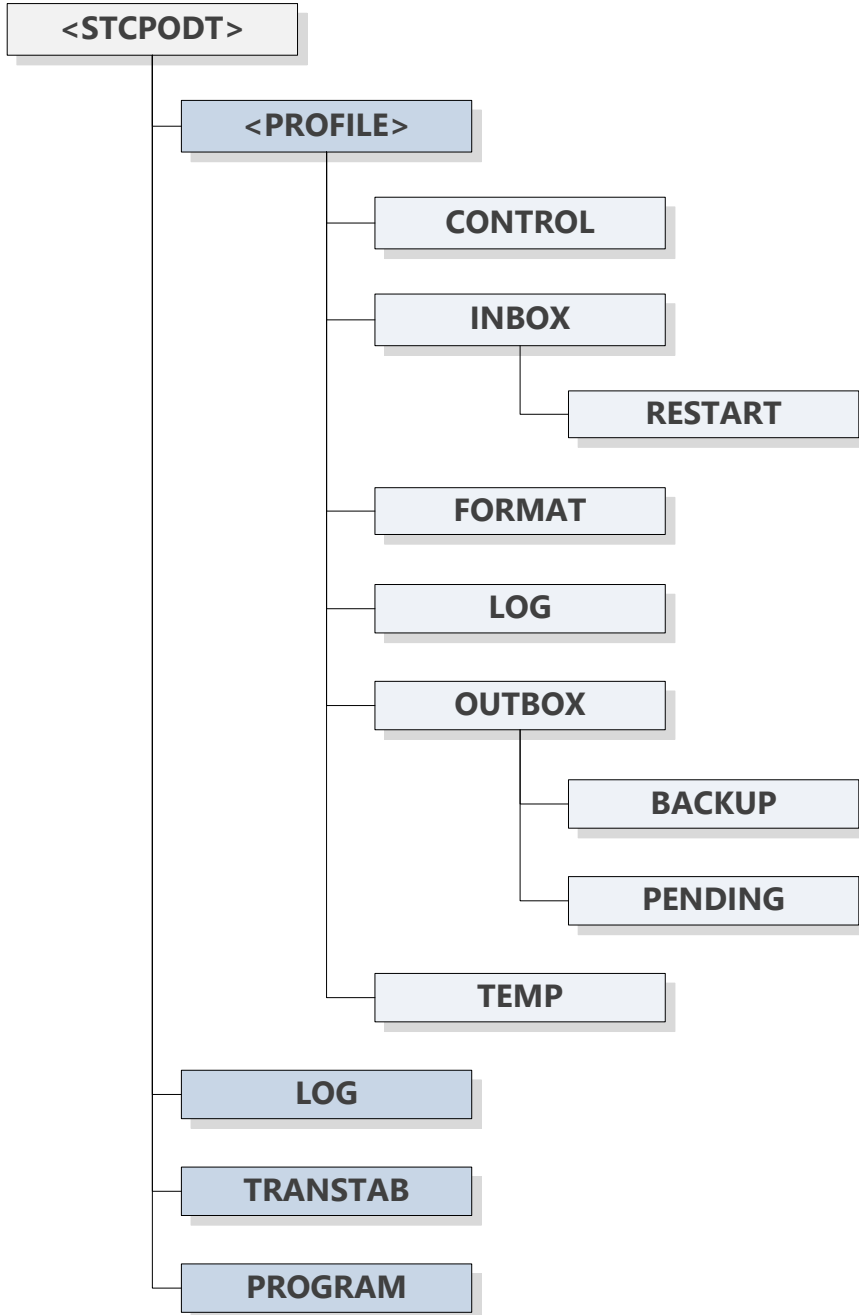


- On the **SSL3** (Openssl) tab set the parameters presented below and press the **OK** button to finish.



Directory structure

After the installation and configuration of the STCP OFTP Server, it will create the following directory tree, where the information of configuration, logs and control will be stored.



How to use the STCP OFTP Server

The STCP OFTP Server, for each User configured in the service, creates an individual set of subdirectories for control of transfers and integration with external applications:

<Data Directory>\	Subdirectory of data configured.
<User Directory>\	Individual subdirectory of the User.
CONTROL	Subdirectory of the application control.
INBOX\	Subdirectory where the files successfully received will be available.
RESTART	Subdirectory where the files that are in process of reception are stored temporarily.
FORMAT	Subdirectory that contains the definitions of the types of files.
LOG	Subdirectory where the files of events and record transfers are stored.
OUTBOX\	Subdirectory where the files to be sent should be available.
BACKUP	Subdirectory where the files successfully sent will be stored if the backup option of the User is enabled.
PENDING	Subdirectory where the control file of the transmission will be stored temporarily.
TEMP	Subdirectory of general use.

To transfer, the files should be available in the subdirectory "**OUTBOX**" and received files are in subdirectory "**INBOX**".

How to execute the STCP OFTP Server through the command line

The syntax to run the STCP OFTP Server through the command line is as follows:

CTCPSVC.EXE <Configuration file> [-addservice]-delservice]-noservice]

Parameter	Description
<configuration file>	Defines the installation configuration filename "CTCP.INI" with the full path.
-addservice	Adds the STCP OFTP Server as an operating system service.
-delservice	Removes the STCP OFTP Server as an operating system service.
-noservice	Executes the STCP OFTP as an application.

Example:

C:\STCPODT\CTCPSVC.EXE C:\STCPCLT\CTCP.INI -noservice

In the above example will run the STCP OFTP Server as an application.

Messages and Error Codes

STCP OFTP Server generates for each event of the system a set of messages that can be stored in a diary file and the error codes are described in the following tables:

Codes of events generated in the message file

Message	Description
MSG0001	[MSG0001] %s - %s - Error: to configure characters conversion '%s' [code:%u]
MSG0002	[MSG0002] %s - %s - Error: to configure characters conversion '%s' [code:%u]
MSG0003	[MSG0003] %s - %s - Error: duplicate file '%s'
MSG0004	[MSG0004] %s - %s - Error: to remove file '%s' [code:%u]
MSG0005	[MSG0005] LOCAL - <STCP> - NOT DEFINED
MSG0006	[MSG0006] %s - %s - Error: to remove file '%s' [code:%u]
MSG0007	[MSG0007] %s - %s - Verified the restart for reception file '%s'
MSG0008	[MSG0008] LOCAL - <STCP> - Error: to create object ODETTE
MSG0009	[MSG0009] LOCAL - <STCP> - Error: to allocate UCB for user
MSG0010	[MSG0010] LOCAL - <STCP> - Exceeded the limit of '%d' connections for the user '%s'
MSG0011	[MSG0011] %s - %s - File already being transmitted '%s'
MSG0012	[MSG0012] %s - %s - Error: to open the pending directory '%s' [code:%u]
MSG0013	[MSG0013] %s - %s - Error: to remove file from pending directory '%s' [code:%u]
MSG0014	[MSG0014] %s - %s - Error: to move file to backup directory '%s' '%s' [code:%u]
MSG0015	[MSG0015] %s - %s - Error: to configure transmission parameters maxrecsize '%d' origin '%s' destination '%s' [code:%u]
MSG0016	[MSG0016] LOCAL - <STCP> - NOT DEFINED
MSG0017	[MSG0017] %s - %s - Error: to configure characters conversion '%s' [code:%u]
MSG0018	[MSG0018] %s - %s - Error: to get file size '%s' [code:%u]
MSG0019	[MSG0019] %s - %s - Beginning of transmission '%s'
MSG0020	[MSG0020] %s - %s - Error: timestamp format incorrect '%s'
MSG0021	[MSG0021] %s - %s - End of transmission with error '%s' [code:%u]
MSG0022	[MSG0022] %s - %s - Error: filename size exceeded '%s'
MSG0023	[MSG0023] %s - %s - End of transmission with error '%s' [code:%u]
MSG0024	[MSG0024] %s - %s - End of transmission with error '%s' [code:%u]
MSG0025	[MSG0025] %s - %s - Error: file does not exist in pending directory '%s'
MSG0026	[MSG0026] %s - %s - Successfully confirmed transmission '%s'
MSG0027	[MSG0027] %s - %s - Error: execution of command line '%s' [code:%u]
MSG0028	[MSG0028] %s - %s - End of transmission with error '%s' [code:%u]

MSG0029	[MSG0029] %s - %s - Error: to create reference in pending directory '%s' [code:%u]
MSG0030	[MSG0030] %s - %s - Error: to remove file '%s' [code:%u]
MSG0031	[MSG0031] %s - %s - End of transmission successfully '%s' bytes sent '%u'
MSG0032	[MSG0032] %s - %s - NOT DEFINED
MSG0033	[MSG0033] LOCAL - <STCP> - NOT DEFINED
MSG0034	[MSG0034] %s - %s - Error: execution of command line '%s' [code:%u]
MSG0035	[MSG0035] %s - %s - Beginning of reception '%s'
MSG0036	[MSG0036] %s - %s - End of reception with error '%s' [code:%u]
MSG0037	[MSG0037] %s - %s - Error: to remove file '%s' [code:%u]
MSG0038	[MSG0038] %s - %s - Error: to move file from '%s' to '%s' [code:%u]
MSG0039	[MSG0039] %s - %s - End of reception successfully '%s' bytes received '%u'
MSG0040	[MSG0040] %s - %s - Error: execution of command line '%s' [code:%u]
MSG0041	[MSG0041] LOCAL - <STCP> - Beginning the process for cancellation of connections
MSG0042	[MSG0042] LOCAL - <STCP> - Error: in the process of cancellation of connections
MSG0043	[MSG0043] LOCAL - <STCP> - End of service '%s' for '%s - Version %s'
MSG0044	[MSG0044] LOCAL - <STCP> - Beginning of the service '%s' for '%s - Version %s'
MSG0045	[MSG0045] LOCAL - <STCP> - Error: to allocate memory for users
MSG0046	[MSG0046] LOCAL - <STCP> - Started logging to server '%s'
MSG0047	[MSG0047] LOCAL - <STCP> - Error: in logging to server '%s' [code:%u]
MSG0048	[MSG0048] LOCAL - <STCP> - Success in logging to server '%s'
MSG0049	[MSG0049] LOCAL - <STCPAGENDA> - Verified directory of transmission for user '%s' condition '%d'
MSG0050	[MSG0050] LOCAL - <STCP> - NOT DEFINED
MSG0051	[MSG0051] LOCAL - <STCP> - NOT DEFINED
MSG0052	[MSG0052] %s - %s - Error: to configure object ODETTE [code:%u]
MSG0053	[MSG0053] %s - %s - Error: to configure object ODETTE extra parameters [code:%u]
MSG0054	[MSG0054] %s - %s - Error: trying outgoing connection [code:%u]
MSG0055	[MSG0055] %s - %s - Beginning of outgoing connection - '%s'
MSG0056	[MSG0056] %s - %s - Error: outgoing connection [code:%u]
MSG0057	[MSG0057] %s - %s - Beginning of thread for outgoing connection - %08X - %08X
MSG0058	[MSG0058] %s - %s - Error: user is blocked for connection
MSG0059	[MSG0059] %s - %s - Error: to configure characters conversion '%s' [code:%u]
MSG0060	[MSG0060] %s - %s - End outgoing connection with error '%s' [code:%u]
MSG0061	[MSG0061] %s - %s - Error: access rejected in local logon for outgoing connection [code:%u]
MSG0062	[MSG0062] %s - %s - End of outgoing connection with error '%s' [code:%u]
MSG0063	[MSG0063] %s - %s - Beginning of outgoing session '%s'
MSG0064	[MSG0064] %s - %s - End of outgoing session '%s'
MSG0065	[MSG0065] %s - %s - End of outgoing connection '%s'
MSG0066	[MSG0066] %s - %s - End of thread for outgoing connection %08X - %08X
MSG0067	[MSG0067] LOCAL - <STCPCLI> - NOT DEFINED
MSG0068	[MSG0068] LOCAL - <STCPCLI> - NOT DEFINED
MSG0069	[MSG0069] LOCAL - <STCPCLI> - NOT DEFINED
MSG0070	[MSG0070] LOCAL - <STCPAGENDA> - Verifying automatic agenda '%s' type '%d' mode '%d' agenda '%d/%d-%d-%d:%d' at '%d/%d-%d-%d:%d'

MSG0071	[MSG0071] LOCAL - <STCPCLI> - Error: to create thread (stcpCliService)
MSG0072	[MSG0072] %s - %s - Reading format configuration file '%s', section '%s'
MSG0073	[MSG0073] LOCAL - <STCP> - NOT DEFINED
MSG0074	[MSG0074] LOCAL - <STCPLOG> - %s - %s - Error: to open log file '%s'
MSG0075	[MSG0075] %s - <STCPMON> - User '%s' was authenticated for monitoring '%s'
MSG0076	[MSG0076] %s - <STCPMON> - Error: user '%s' was not authenticated for monitoring '%s'
MSG0077	[MSG0077] %s - <STCPMON> - Error: reception of monitoring [code:%u, %u] '%s'
MSG0078	[MSG0078] %s - <STCPMON> - Timeout in the reception of monitoring '%s'
MSG0079	[MSG0079] %s - <STCPMON> - Cancellation or error when waiting connection for monitoring [code:%u]
MSG0080	[MSG0080] %s - <STCPMON> - Beginning of connection for monitoring '%s'
MSG0081	[MSG0081] %s - <STCPMON> - End of connection for monitoring '%s'
MSG0082	[MSG0082] %s - <STCPMON> - Beginning of thread for monitoring %08X - %08X
MSG0083	[MSG0083] %s - <STCPMON> - End of thread for monitoring %08X - %08X
MSG0084	[MSG0084] %s - <STCPSRV> - Error: to configure object ODETTE [code:%u]
MSG0085	[MSG0085] %s - <STCPSRV> - Error: to configure object ODETTE extra parameters [code:%u]
MSG0086	[MSG0086] %s - <STCPSRV> - Cancellation or error when waiting incoming connection %08X - %08X [code:%u]
MSG0087	[MSG0087] %s - %s - Beginning of incoming connection '%s'
MSG0088	[MSG0088] %s - %s - Error: rejected access, user already connected
MSG0089	[MSG0089] %s - %s - Error: rejected access, user is blocked
MSG0090	[MSG0090] %s - %s - Error: to configure object ODETTE [code:%u]
MSG0091	[MSG0091] %s - %s - Error: to configure characters conversion '%s' [code:%u]
MSG0092	[MSG0092] %s - %s - Error: access rejected in local logon for incoming connection [code:%u]
MSG0093	[MSG0093] LOCAL - <STCP> - NOT DEFINED
MSG0094	[MSG0094] %s - %s - Beginning of incoming session '%s'
MSG0095	[MSG0095] %s - %s - End of incoming session '%s'
MSG0096	[MSG0096] %s - %s - End of incoming connection '%s'
MSG0097	[MSG0097] %s - <STCPSRV> - Beginning of thread for incoming connection %08X - %08X
MSG0098	[MSG0098] %s - %s - End of incoming connection with error '%s' [code:%u]
MSG0099	[MSG0099] %s - <STCPSRV> - End of thread for incoming connection %08X - %08X
MSG0100	[MSG0100] LOCAL - <STCPSRV> - NOT DEFINED
MSG0101	[MSG0101] LOCAL - <STCP> - NOT DEFINED
MSG0102	[MSG0102] LOCAL - <STCPSRV> - Error: to allocate UCB for network '%s'
MSG0103	[MSG0103] LOCAL - <STCPSRV> - Error: to create thread (stcpSrvServer) for network '%s'
MSG0104	[MSG0104] %s - <STCPSRV> - End of incoming connection with error '%s' [code:%u]
MSG0105	[MSG0105] %s - <STCPSRV> - Error: rejected access, user '%s' not registered in database
MSG0106	[MSG0106] %s - <STCPSRV> - Error: rejected access, user '%s' is invalid for '%s'
MSG0107	[MSG0107] LOCAL - <STCP> - %s - Error: to allocate memory for debug filename '%s'

MSG0108	[MSG0108] LOCAL - <STCP> - %s - Error: to open debug file '%s' [code:%u]
MSG0109	[MSG0109] LOCAL - <STCP> - End of cancellation process for the connections
MSG0110	[MSG0110] LOCAL - <STCP> - Error: configuration file CTCP.INI/CTCP.AUX does not exist
MSG0111	[MSG0111] LOCAL - <STCPAGENDA> - Initiate agenda '%s' for user '%s' mode '%c' sessions '%d' filter '%s' command '%s'
MSG0112	[MSG0112] %s - %s - Error: automatic connection is disabled
MSG0113	[MSG0113] LOCAL - <STCP> - Configuration '%s' maximum sessions '%d'
MSG0114	[MSG0114] LOCAL - <STCP> - Demo version limited by '%d' simultaneous sessions
MSG0115	[MSG0115] %s - %s - Error: invalid file name '%s'
MSG0116	[MSG0116] LOCAL - <STCPAGENDA> - Error: to open transmission directory '%s' for user '%s' [code:%u]
MSG0117	[MSG0117] %s - %s - Error: to open transmission directory '%s' [code:%u]
MSG0118	[MSG0118] %s - %s - Error: to open formats directory '%s' [code:%u]
MSG0119	[MSG0119] %s - %s - Error: reception of file '%s' blocked by the filter '%s'
MSG0120	[MSG0120] %s - %s - Error: reception of file '%s' blocked by the size '%d' > '%d'
MSG0121	[MSG0121] LOCAL - <STCPAGENDA> - Error: execution of command line '%s' for agenda '%s' [code:%u]
MSG0122	[MSG0122] LOCAL - <STCP> - Error: to compile regular expression '%s' [code:%u]
MSG0123	[MSG0123] %s - %s - Error: transmission of file '%s' blocked by the filter '%s'
MSG0124	[MSG0124] %s - %s - Error: transmission of file '%s' blocked by the size '%d' > '%d'
MSG0125	[MSG0125] %s - %s - Error: connection was blocked '%s' for the filter '%s'
MSG0126	[MSG0126] LOCAL - <STCPCLI> - Error: rejected access, user '%s' not registered in database
MSG0127	[MSG0127] %s - %s - Error: execution of command line '%s' [code:%u]
MSG0128	[MSG0128] %s - %s - Error: execution of command line '%s' [code:%u]
MSG0129	[MSG0129] LOCAL - <STCP> - Error: to load the configuration program %s - [code:%u]
MSG0130	[MSG0130] %s - %s - %s '%s'
MSG0131	[MSG0131] %s - <STCPMON> - Error: to modify password for '%s', user or password are invalid - '%s'
MSG0132	[MSG0132] %s - <STCPMON> - Error: command not defined '%d' - '%s'
MSG0133	[MSG0133] %s - <STCPMON> - Error: invalid parameters - '%s'
MSG0134	[MSG0134] LOCAL - <STCP> - Error: serial number is blank or incorrect '%s'
MSG0135	[MSG0135] LOCAL - <STCP> - Serial number: '%-.8s-%-.4s-%-.4s-%-.4s-%-.12s-%-.4s' - ID: '%-04X-%-04X'
MSG0136	[MSG0136] LOCAL - <STCPAGENDA> - Error: to create thread (stcpSchedService)

MSG0137	[MSG0137] LOCAL - <STCP> - Error: in function SetConsoleCtrlHandler
MSG0138	[MSG0138] LOCAL - <STCP> - Error: to create semaphore (sema_usu)
MSG0139	[MSG0139] LOCAL - <STCP> - Error: to create semaphore (sema_filename)
MSG0140	[MSG0140] LOCAL - <STCP> - Do you wish to end the service '%s'?
MSG0141	[MSG0141] LOCAL - <STCP> - Do you wish to restart service '%s'?
MSG0142	[MSG0142] LOCAL - <STCP> - Do you wish to start connection '%s'?
MSG0143	[MSG0143] LOCAL - <STCP> - Invalid user
MSG0144	[MSG0144] LOCAL - <STCP> - Invalid password
MSG0145	[MSG0145] LOCAL - <STCP> - User must be administrator or \nMember of group CONADMIN
MSG0146	[MSG0146] LOCAL - <STCP> - User or password invalid
MSG7001	[MSG7001] LOCAL - <STCPREN> - Error: invalid number of parameters - '%d'
MSG7002	[MSG7002] LOCAL - <STCPREN> - Error: invalid filename - '%s'
MSG7003	[MSG7003] LOCAL - <STCPREN> - Error: rules file '%s' does not have definition for file '%s'
MSG7004	[MSG7004] LOCAL - <STCPREN> - Error: log service not opened
MSG7005	[MSG7005] LOCAL - %s - Error: rule '%s' with invalid parameter in file '%s'
MSG7006	[MSG7006] LOCAL - %s - Beginning of the STCPREN for file '%s'
MSG7007	[MSG7007] LOCAL - %s - Error: to copy file from '%s' to '%s' [code:%u]
MSG7008	[MSG7008] LOCAL - %s - Copied file from '%s' to '%s' destination '%s'
MSG7009	[MSG7009] LOCAL - %s - Copied file from '%s' to '%s' origin '%s'
MSG7010	[MSG7010] LOCAL - %s - Error: to remove file '%s' [code:%u]
MSG7011	[MSG7011] LOCAL - %s - Error: execution of command line '%s %s'[code:%u]
MSG7012	[MSG7012] LOCAL - %s - Error: execution of command line '%s %s'[code:%u]
MSG7013	[MSG7013] LOCAL - <STCPREN> - Error: connecting resource '%s' [code:%u]
MSG7014	[MSG7014] LOCAL - <STCPREN> - Error: disconnecting resource '%s' [code:%u]
MSG8001	[MSG8001] LOCAL - <STCPCFG> - File Type name not informed
MSG8002	[MSG8002] LOCAL - <STCPCFG> - Profile name not informed
MSG8002	[MSG8002] LOCAL - <STCPCFG> - User name not informed
MSG8003	[MSG8003] LOCAL - <STCPCFG> - Password not informed
MSG8004	[MSG8004] LOCAL - <STCPCFG> - Password not confirmed
MSG8005	[MSG8005] LOCAL - <STCPCFG> - Trace filename of data sent not informed
MSG8006	[MSG8006] LOCAL - <STCPCFG> - Trace filename of received data not informed
MSG8007	[MSG8007] LOCAL - <STCPCFG> - Debug filename not informed
MSG8008	[MSG8008] LOCAL - <STCPCFG> - Modem dial string not informed
MSG8009	[MSG8009] LOCAL - <STCPCFG> - Modem init string not informed
MSG8010	[MSG8010] LOCAL - <STCPCFG> - Modem hangup string not informed
MSG8011	[MSG8011] LOCAL - <STCPCFG> - Connection message not informed
MSG8012	[MSG8012] LOCAL - <STCPCFG> - Confirmation message not informed

MSG8013	[MSG8013]	LOCAL - <STCPCFG> - Busy message not informed
MSG8014	[MSG8014]	LOCAL - <STCPCFG> - Error message not informed
MSG8015	[MSG8015]	LOCAL - <STCPCFG> - No dialtone, message not informed
MSG8016	[MSG8016]	LOCAL - <STCPCFG> - No carrier, message not informed
MSG8017	[MSG8017]	LOCAL - <STCPCFG> - PAD parameters not informed
MSG8018	[MSG8018]	LOCAL - <STCPCFG> - New password not confirmed
MSG8019	[MSG8019]	LOCAL - <STCPCFG> - Error: to create directory '%s' [code:%d]
MSG8020	[MSG8020]	LOCAL - <STCPCFG> - Command line not informed
MSG8021	[MSG8021]	LOCAL - <STCPCFG> - Invalid command line
MSG8022	[MSG8022]	LOCAL - <STCPCFG> - Error: to write file CTCP.INI
MSG8023	[MSG8023]	LOCAL - <STCPCFG> - Type 'default' cannot be removed
MSG8024	[MSG8024]	LOCAL - <STCPCFG> - Service name not informed
MSG8025	[MSG8025]	LOCAL - <STCPCFG> - Control directory not informed
MSG8026	[MSG8026]	LOCAL - <STCPCFG> - Data directory not informed
MSG8027	[MSG8027]	LOCAL - <STCPCFG> - Password confirmation is incorrect
MSG8028	[MSG8028]	LOCAL - <STCPCFG> - Control directory is different of the current one.\nCheck if STCP OFTP service is halted\nbefore making the changes.\n\nDo you want to continue?
MSG8029	[MSG8029]	LOCAL - <STCPCFG> - Data directory is different of the current one.\nCheck if STCP OFTP service is halted\nbefore making the changes.\n\nDo you want to continue?
MSG8030	[MSG8030]	LOCAL - <STCPCFG> - Invalid serial number
MSG8031	[MSG8031]	LOCAL - <STCPCFG> - OnButtonDirsys SHGetMalloc
MSG8032	[MSG8032]	LOCAL - <STCPCFG> - Invalid directory
MSG8033	[MSG8033]	LOCAL - <STCPCFG> - OnButtonDirdat SHGetMalloc
MSG8034	[MSG8034]	LOCAL - <STCPCFG> - Invalid sessions number
MSG8035	[MSG8035]	LOCAL - <STCPCFG> - Checkpoint cannot be equal to zero
MSG8036	[MSG8036]	LOCAL - <STCPCFG> - IP address not informed
MSG8037	[MSG8037]	LOCAL - <STCPCFG> - IP port not informed
MSG8038	[MSG8038]	LOCAL - <STCPCFG> - Remote X.25 address not informed
MSG8039	[MSG8039]	LOCAL - <STCPCFG> - DTE address not informed
MSG8040	[MSG8040]	LOCAL - <STCPCFG> - Customer identification number not informed
MSG8041	[MSG8041]	LOCAL - <STCPCFG> - Number to be dialed not informed
MSG8042	[MSG8042]	LOCAL - <STCPCFG> - ODETTE Id (OID) not informed
MSG8043	[MSG8043]	LOCAL - <STCPCFG> - IP port already configured in another section
MSG8044	[MSG8044]	LOCAL - <STCPCFG> - User for monitor not informed
MSG8045	[MSG8045]	LOCAL - <STCPCFG> - Password for monitor not informed
MSG8046	[MSG8046]	LOCAL - <STCPCFG> - Password for monitor not confirmed
MSG8047	[MSG8047]	LOCAL - <STCPCFG> - Initial size of buffer cannot be inferior to 128 or superior to 99999
MSG8048	[MSG8048]	LOCAL - <STCPCFG> - Credits cannot be inferior to 1 or superior to 999
MSG8049	[MSG8049]	LOCAL - <STCPCFG> - Error: dialup archive load
MSG8050	[MSG8050]	LOCAL - <STCPCFG> - It was not possible to open or to find library RAS
MSG8051	[MSG8051]	LOCAL - <STCPCFG> - Error: to load the remote access functions

MSG8052	[MSG8052] LOCAL - <STCPCFG> - Verification mode not informed
MSG8053	[MSG8053] LOCAL - <STCPCFG> - Prefix or suffix not informed
MSG8054	[MSG8054] LOCAL - <STCPCFG> - Regular expression not informed
MSG8055	[MSG8055] LOCAL - <STCPCFG> - Record length not informed
MSG8056	[MSG8056] LOCAL - <STCPCFG> - The informed directory '%s' does not exist.\n\nDo you wish to create it?
MSG8057	[MSG8057] LOCAL - <STCPCFG> - Odette password not informed
MSG8058	[MSG8058] LOCAL - <STCPCFG> - Odette password not confirmed
MSG8059	[MSG8059] LOCAL - <STCPCFG> - Buffer size cannot be inferior to 128 or superior to 99999
MSG8060	[MSG8060] LOCAL - <STCPCFG> - Timeout for packages cannot be equal to zero
MSG8061	[MSG8061] LOCAL - <STCPCFG> - Timeout for waiting packages cannot be equal to zero
MSG8062	[MSG8062] LOCAL - <STCPCFG> - Timeout for waiting character can not be equal to zero
MSG8063	[MSG8063] LOCAL - <STCPCFG> - Maximum number of attempts cannot be equal to zero
MSG8064	[MSG8064] LOCAL - <STCPCFG> - Remote address DTE not informed
MSG8065	[MSG8065] LOCAL - <STCPCFG> - PAD connection message not informed
MSG8066	[MSG8066] LOCAL - <STCPCFG> - Password not confirmed
MSG8067	[MSG8067] LOCAL - <STCPCFG> - IP address not informed
MSG8068	[MSG8068] LOCAL - <STCPCFG> - IP port invalid
MSG8069	[MSG8069] LOCAL - <STCPCFG> - Name not informed
MSG8070	[MSG8070] LOCAL - <STCPCFG> - Agenda name already exists
MSG8071	[MSG8071] LOCAL - <STCPCFG> - User not informed
MSG8072	[MSG8072] LOCAL - <STCPCFG> - Command not informed
MSG8073	[MSG8073] LOCAL - <STCPCFG> - IP address not informed
MSG8074	[MSG8074] LOCAL - <STCPCFG> - IP Port invalid
MSG8075	[MSG8075] LOCAL - <STCPCFG> - User not informed
MSG8076	[MSG8076] LOCAL - <STCPCFG> - X.25 board not informed
MSG8077	[MSG8077] LOCAL - <STCPCFG> - X.25 port not informed
MSG8078	[MSG8078] LOCAL - <STCPCFG> - Wait, connection string not informed
MSG8079	[MSG8079] LOCAL - <STCPCFG> - File type '%s' already exists
MSG8080	[MSG8080] LOCAL - <STCPCFG> - Nome do perfil '%s' já existe
MSG8080	[MSG8080] LOCAL - <STCPCFG> - User name '%s' already exists
MSG8081	[MSG8081] LOCAL - <STCPCFG> - Error: to modify system password [code:%u]
MSG8082	[MSG8082] LOCAL - <STCPCFG> - Error: file '%s' does not exist or it does not possess access permission
MSG8083	[MSG8083] LOCAL - <STCPCFG> - Service '%s' deactivated successfully
MSG8084	[MSG8084] LOCAL - <STCPCFG> - Service '%s' activated successfully
MSG8085	[MSG8085] LOCAL - <STCPCFG> - Are you sure to remove Profile '%s'\n and all its sub-directories?
MSG8085	[MSG8085] LOCAL - <STCPCFG> - Are you sure to remove User '%s'\n and his sub-directories?
MSG8086	[MSG8086] LOCAL - <STCPCFG> - Remove File Type '%s' ?

MSG8087	[MSG8087] LOCAL - <STCPCFG> - Remove Network '%s' ?
MSG8088	[MSG8088] LOCAL - <STCPCFG> - The user '%s' already exists
MSG8089	[MSG8089] LOCAL - <STCPCFG> - Remove profile '%s' ?
MSG8089	[MSG8089] LOCAL - <STCPCFG> - Remove user '%s' ?
MSG8090	[MSG8090] LOCAL - <STCPCFG> - It was not possible to create the directory '%s' [code:%d]
MSG8091	[MSG8091] LOCAL - <STCPCFG> - Error: %d to remove file '%s'
MSG8092	[MSG8092] LOCAL - <STCPCFG> - Error: %d to remove directory '%s'
MSG8093	[MSG8093] LOCAL - <STCPCFG> - Error: to create group STCPGRP [code:%u]
MSG8094	[MSG8094] LOCAL - <STCPCFG> - Error: to create user
MSG8095	[MSG8095] LOCAL - <STCPCFG> - Error: to create user %s [code:%u]
MSG8096	[MSG8096] LOCAL - <STCPCFG> - Error: to add user '%s' to group STCPGRP [code:%u]
MSG8097	[MSG8097] LOCAL - <STCPCFG> - Error: to remove user '%s' [code:%u]
MSG8098	[MSG8098] LOCAL - <STCPCFG> - Remove agenda '%s' ?
MSG8099	[MSG8099] LOCAL - <STCPCFG> - Agenda name '%s' already exists
MSG8100	[MSG8100] LOCAL - <STCPCFG> - Service '%s' already exists
MSG8101	[MSG8101] LOCAL - <STCPCFG> - The origin directory '%s' does not exist
MSG8102	[MSG8102] LOCAL - <STCPCFG> - Error: to add group [code:%d]
MSG8103	[MSG8103] LOCAL - <STCPCFG> - Error: to configure info into group [code:%d]
MSG8104	[MSG8104] LOCAL - <STCPCFG> - Error: to add user [code:%d]
MSG8105	[MSG8105] LOCAL - <STCPCFG> - Error: to add user into group [code:%d]
MSG8106	[MSG8106] LOCAL - <STCPCFG> - Error: to remove user [code:%d]
MSG8107	[MSG8107] LOCAL - <STCPCFG> - Error: to remove group [code:%d]
MSG8108	[MSG8108] LOCAL - <STCPCFG> - Service '%s' is active.\n\nDo you wish to deactivate it now ?\n
MSG8109	[MSG8109] LOCAL - <STCPCFG> - Service '%s' is not active.\n\nDo you wish to activate it now ?\n
MSG8110	[MSG8110] LOCAL - <STCPCFG> - A previous version of STCP OFTP is already installed in this machine.\nWe recommend that a security copy be made.\n\nDo you wish to continue with the update?
MSG8111	[MSG8111] LOCAL - <STCPCFG> - There are some files in inbox/outbox directories\n\nAre you sure to remove Profile '%s'\nand all its sub-directories?
MSG8111	[MSG8111] LOCAL - <STCPCFG> - There are some files in inbox/outbox directories\n\nAre you sure to remove User '%s'\nand all its sub-directories?
MSG8112	[MSG8112] LOCAL - <STCPCFG> - Service '%s' not removed correctly [code:%d].\n\nExecute the following command line:\n\n--> '%s %s -delservice' <--
MSG8113	[MSG8113] LOCAL - <STCPCFG> - Service '%s' not installed correctly [code:%d].\n\nExecute the following command line:\n\n--> '%s %s -addservice' <--
MSG8114	[MSG8114] LOCAL - <STCPCFG> - Error: to apply rights to group STCPGRP [code:%u]
MSG8115	[MSG8115] LOCAL - <STCPCFG> - New password not informed
MSG8116	[MSG8116] LOCAL - <STCPCFG> - Error: configuration file '%s' does not exist
MSG8117	[MSG8117] LOCAL - <STCPCFG> - User '%s' created successfully
MSG8118	[MSG8118] LOCAL - <STCPCFG> - Error: to create user '%s' [code:0x%X]
MSG8119	[MSG8119] LOCAL - <STCPCFG> - Error: to create user '%s', already exists
MSG8120	[MSG8120] LOCAL - <STCPCFG> - User '%s' removed successfully

MSG8121	[MSG8121] LOCAL - <STCPCFG> - Error: to remove user '%s' [code:0x%X]
MSG8122	[MSG8122] LOCAL - <STCPCFG> - Error: to remove user '%s' does not exist
MSG8123	[MSG8123] LOCAL - <STCPCFG> - User '%s' modified successfully
MSG8124	[MSG8124] LOCAL - <STCPCFG> - Error: to modify user '%s' does not exist
MSG8125	[MSG8125] LOCAL - <STCPCFG> - User '%s' modified successfully
MSG8126	[MSG8126] LOCAL - <STCPCFG> - Error: to modify password of the user '%s'
MSG8127	[MSG8127] LOCAL - <STCPCFG> - Error: to modify user '%s', user does not exist
MSG8128	[MSG8128] LOCAL - <STCPCFG> - Error: to create shortcut on desktop
MSG8129	[MSG8129] LOCAL - <STCPCFG> - Error: to remove shortcut from desktop
MSG8130	[MSG8130] LOCAL - <STCPCFG> - Error: to locate directory on desktop
MSG9001	[MSG9001] LOCAL - <STCPCTL> - Error: IP address not defined
MSG9002	[MSG9002] LOCAL - <STCPCTL> - Error: IP port invalid
MSG9003	[MSG9003] LOCAL - <STCPCTL> - Error: user not defined
MSG9004	[MSG9004] LOCAL - <STCPCTL> - Error: password not confirmed
MSG9005	[MSG9005] LOCAL - <STCPCTL> - Error: execution of command line '%s' [code:%d]
MSG9006	[MSG9006] LOCAL - <STCPCTL> - Error: invalid directory or undefined profile
MSG9007	[MSG9007] LOCAL - <STCPCTL> - Error: to remove directory %s [code:0x%X]
MSG9008	[MSG9008] LOCAL - <STCPCTL> - Error: program '%s' not authorized [code:0x%X]
MSG9009	[MSG9009] LOCAL - <STCPCTL> - Error: to remove file '%s' [code:0x%X]

General error codes

Code	Description
1	Operation not allowed conflict of permissions for the process. (EPERM)
2	File or directory selected does not exist. (ENOENT)
3	Process selected has not been found. (ESRCH)
4	Function interrupted. (EINTR)
5	Failure in access incoming/outgoing sessions. (EIO)
6	Failure to access device. (ENXIO).
7	Argument for execution exceeds maximum allowable limit. (E2BIG).
8	Invalid format for executable file. (ENOEXEC).
9	Descriptor used to Access file is invalid. (EBADF).
10	No child process. (ECHILD).
11	Resource temporarily unavailable. (EAGAIN).
12	Not enough memory available. (ENOMEM).
13	Failure on permission to desired operation. (EACCESS).
14	Invalid memory address. (EFAULT).
16	Resource already in use. (EBUSY).
17	File already exists. (EEXIST).
18	Failure to execute a link through files system. (EXDEV).
19	Type of device for operation requested is invalid (ENODEV).
20	File informed is not a directory. (ENOTDIR).
21	File informed is a directory. (EISDIR).

22	Invalid argument for the function. (EINVAL).
23	Too many files opened in the system. (ENFILE).
24	Excess of files opened in the process. (EMFILE).
25	Failure of operation for the device selected. (ENOTTY).
27	File too big. (EFBIG).
28	Not enough space in the device selected. (ENOSPC).
29	Invalid positioning operation (seek) on device. (ESPIPE).
30	Invalid Operation on Only Read device. (EROFS).
31	Exceeded number of reference for the same file. (EMLINK).
32	Pipe interrupted. (EPIPE).
33	Failure to execute a calculation function. (EDOM).
34	Failure of overflow or underflow. (ERANGE).
36	(EDEADLK)
39	Lock resource not available. (ENOLCK).
40	Function not implemented. (ENOSYS).
42	Failure on the decoding of a multi-byte character. (EILSEQ).
80	Arquivo duplicado ao executar função "COPY". Verificar arquivo duplicado na pasta de destino.
183	Arquivo duplicado ao executar função "MOVE". Verificar arquivo duplicado na pasta de destino.

Transfer error codes of the Odette protocol

Code	Description
400	Null.
401	Invalid file name.
402	Invalid Destination Parameter for Odette session.
403	Invalid Originator Parameter for Odette session.
404	Register Format not supported.
405	Size of register not supported.
406	File size exceeding maximum allowed.
410	Invalid register counter.
411	Invalid byte counter.
412	Failure on access method.
413	Duplicate file or directory RESTART do not exist.
499	Code not specified: an error has been detected but cannot be appropriately described by any of the codes available.

Session error codes of the Odette protocol

Code	Description
501	Invalid command for ODETTE package.
502	Protocol violation: command has specified an invalid function for the current state of

	operation.
503	User code not registered in the concentrator.
504	Invalid Password.
505	Error on local PC, end of communication.
506	Command has invalid data.
507	Invalid size of ODETTE package.
508	Exceeded maximum limit for user connections.
509	Exceeded time limit of inactivity.
510	Incompatible mode.
599	Code not specified: an error has been detected but cannot appropriately be described by any of the codes available.

Transfer error codes

Code	Description
1001	Operação não permitida, conflito de permissões para o processo (EPERM).
1002	O arquivo ou diretório selecionado não existe (ENOENT).
1003	O processo selecionado não foi encontrado (ESRCH).
1004	A função foi interrompida (EINTR).
1005	Falha de acesso de entrada ou saída (EIO).
1006	Falha de acesso ao dispositivo (ENXIO).
1007	Argumento passado para executar o processo excede o limite permitido (E2BIG).
1008	Formato inválido do arquivo executável (ENOEXEC).
1009	Descritor utilizado para acesso ao arquivo é inválido (EBADF).
1010	Não existe processo filho (ECHILD).
1011	Recurso temporariamente indisponível (EAGAIN).
1012	Não existe memória disponível (ENOMEM).
1013	Falha de permissão para a operação desejada (EACCESS).
1014	Endereço de memória inválido (EFAULT).
1016	Recurso está ocupado (EBUSY).
1017	Arquivo já existe (EEXIST).
1018	Falha para executar um link através do sistema de arquivos (EXDEV).
1019	O tipo de dispositivo para operação solicitada é inválido (ENODEV).
1020	O tipo de arquivo informado não é um diretório (ENOTDIR).
1021	O tipo de arquivo informado é um diretório (EISDIR).
1022	Argumento inválido para a função (EINVAL).
1023	Existe excesso de arquivos abertos no sistema (ENFILE).
1024	Existe excesso de arquivos abertos no processo (EMFILE).
1025	Falha de operação para o dispositivo selecionado (ENOTTY).
1027	Tamanho do arquivo excede o permitido (EFBIG).
1028	Não existe espaço disponível no dispositivo selecionado (ENOSPC).
1029	Operação inválida de posicionamento (seek) no dispositivo.
1030	Operação inválida em um dispositivo somente de leitura (EROFS).
1031	Excedido número de referências para o mesmo arquivo (EMLINK).

1032	Pipe interrompido (EPIPE).
1033	Falha para executar uma função matemática (EDOM).
1034	Falha de overflow ou underflow (ERANGE).
1036	O sistema ficou bloqueado (EDEADLK).
1039	Recurso de lock não disponível (ENOLCK).
1040	Função não implementada (ENOSYS).
1042	Falha na decodificação de um caractere multibyte (EILSEQ).
1100	File has invalid external timestamp extension. See option Remove Timestamp.
1101	O nome do arquivo excedeu o limite máximo de 26 (vinte e seis) caracteres. Verifique a opção <i>Nome longo para arquivos</i> . File name exceeded maximum of 26 (twenty-six) characters. See option Long file names.
1102	File name has invalid character or blank space.
1103	File name is blocked. See option File Filter.
1104	Size of file exceeded limit. See option Maximum File Size.
1203	Erro: conectar recurso.
1265	Null.

Generic error codes of the communication interface

Code	Description
6801	Failure on memory allocation.
6802	Parameter indicating the location of communication library (DLLName) was not informed on configuration file.
6803	Failure when loading communication library.
6804	Invalid or corrupted Communication Library.

Error codes of the TCP/IP (RAS) communication interface

Code	Description
9005	Access denied. Check user name and password.
9600	There is an operation pending.
9601	Invalid description of port.
9602	Port is already opened.
9603	Buffer is small.
9604	Error on information given.
9605	Impossible to configure information for the port.
9606	Port not connected.
9607	Invalid Event.
9608	Device does not exist.
9609	Type of device does not exist.
9610	Invalid Buffer.
9611	Path is unavailable.
9612	Path is not allocated.

9613	Compression specified is invalid.
9614	No buffers available.
9615	Port not found.
9616	Asynchronous requisition is pending.
9617	Port or device already disconnected.
9618	Port not opened.
9619	Port disconnected.
9620	No endpoints.
9621	Unable to open phone book file.
9622	Unable to load phone book file.
9623	Unable to find phone book inlet.
9624	Unable to write on phone book file.
9625	Invalid Information found on phone book file.
9626	Unable to load a string
9627	Key not found
9628	Port disconnected.
9629	Connection aborted by remote computer.
9630	Port disconnected due to hardware failure.
9631	Port disconnect by the user.
9632	Incorrect structure size.
9633	Port already in use or not configured for remote access.
9634	Unable to register your PC on remote network.
9635	Unknown Error.
9636	Wrong device related to the port.
9637	String cannot be converted.
9638	Exceeded time limit.
9639	Asynchronous network not available.
9640	NETBIOS Error.
9641	Server unable to allocate needed NETBIOS resources for customer.
9642	One of NETBIOS' names is already registered on the remote network.
9643	Failure of network adaptor.
9644	No messages from pop ups networks.
9645	Authentication Error.
9646	Account not allowed to login at this time.
9647	Account unavailable.
9648	Password has expired.
9649	Account has no permission for remote Access.
9650	Server for remote access is not answering.
9651	Your modem (or other device connected) reported an error.
9652	Not acknowledgement response from device.
9653	A macro requested by the device has not been found on the configuration file.
9654	A command or response from the device configuration file refers to an undefined macro.
9655	A macro has not been found on device configuration file.
9656	A macro on the device configuration file remains undefined.

9657	Configuration file for the device cannot be opened.
9658	Name of device on the configuration file is too long.
9659	Configuration file refers to an unknown device name.
9660	Configuration file for device has no response for the command.
9661	Configuration file is missing a command.
9662	Attempt to configure a macro which is not listed on configuration file.
9663	Configuration files relate to unknown type of device.
9664	Impossible allocate memory.
9665	Port is not configured for remote access.
9666	Modem (or other device connected) is not working.
9667	Unable to read the configuration file.
9668	Connection failure.
9669	Parameter 'usage' on configuration file is invalid.
9670	Unable to read name of configuration file session.
9671	Unable to read type of device on configuration file.
9672	Unable to read name of device on configuration file.
9674	Unable to read maximum speed of connection on configuration file.
9675	Unable to read maximum speed of carrier on configuration file.
9676	Line is busy.
9677	Someone answered instead of modem.
9678	No response.
9679	Carrier not detected.
9680	No phone service.
9681	General Error reported by device.
9691	Access denied due to invalid user and/or password.
9692	Hardware failure.
9699	Device response overloaded the buffer.
9701	Device speed not supported by COM driver.
9702	Device responded when not expected.
9703	Application does not allow interaction with User. Connection needs interaction with User to successfully end.
9708	Account expired.
9709	Error while changing password. Too short or already exists.
9710	Overrun errors on serial port detected during communication to modem.
9711	Initialization fails of RASMAN. Check event log.
9712	Biplex Port initializing. Wait a couple of minutes and redial.
9713	ISDN lines not available.
9714	ISDN channels not available for call making.
9715	Too many errors caused by poor quality transmission of line.
9717	IP's addresses not available on static IP's list for remote access.
9718	Timeout while awaiting a valid response from remote PPP.
9719	PPP ended by remote machine.
9720	No control protocol configured.
9721	Remote PPP not answering.
9722	PPP package is invalid.

9723	Phone number too long.
9724	Protocol IPX unable to dial-out because machine is IPX router.
9725	Protocol IPX cannot dial-out because IPX router is not installed.
9726	Protocol IPX cannot be used for dial-out by more than a port at a time.
9727	Unable to access TCPCFG.DLL file.
9728	Unable to find an IP adaptor for remote access.
9729	SLIP cannot be used unless protocol IP is installed.
9730	Computer register not complete.
9731	Protocol not configured.
9732	PPP negotiation not converging.
9733	Control Protocol PPP not available on Server.
9734	Control Protocol PPP ended.
9735	Address requested was rejected by Server.
9736	Remote computer ended control protocol.
9737	Loopback detected.
9738	Server did not relate an address.
9739	Authentication protocol requested by remote Server cannot use cryptographed password of Windows NT. Dial again and type in password.
9740	Invalid TAPI configuration.
9741	Local PC does not support type of cryptography
9742	Remote PC does not support type of cryptography required.
9743	Remote PC requests cryptography.
9744	Number of network IPX related by remote Server cannot be used. Check event log.
9745	Invalid SMM.
9746	SMM not initialized.
9748	SMM Timeout
9749	Wrong module.
9750	Módulo errado.
9751	Invalid callback number. Only characters 0 to 9, T, P, W, (,), -, @ e space are allowed.
9752	Syntax error found during script processing.
9753	Connection cannot be ended as it was set by Multi-Protocol Router.
9804	RAS connection not established.
9805	User in RAS authentication is not configured.

Error codes of the TCP/IP communication interface

Code	Description
10004	Function interrupted. (WSAEINTR)
10009	Descriptor used for access is invalid. (WSAEBADF).
10013	Failure on permission for desired operation. (WSAEACCESS).
10014	Invalid memory address. (WSAEFAULT).
10022	Invalid argument for the function. (WSAEINVAL).
10024	Too many sockets opened in the process. (WSAEMFILE).
10035	Resource temporarily unavailable. (WSAEWOULDBLOCK).

10036	Undergoing operation. (WSAEINPROGRESS).
10037	Undergoing operation. (WSAEALREADY).
10038	Operation requested on invalid handle. (WSAENOTSOCK).
10039	IP address requested. (WSAEDESTADDREQ).
10040	Message exceeds size limit. (WSAEMSGSIZE).
10041	Invalid Protocol for socket. (WSAEPROTOTYPE).
10042	Invalid option for protocol. (WSAENOPROTOOPT).
10043	Protocol not supported. (WSAEPROTONOSUPPORT).
10044	Type of socket not supported. (WSAESOCKTNOSUPPORT)
10045	Operation not supported. (WSAEOPNOTSUPP).
10046	Protocol family not supported. (WSAEPFNOSUPPORT).
10047	Address family not supported by protocol family. (WSAEAFNOSUPPORT).
10048	Address already in use. (WSAEADDRINUSE).
10049	Address not available. (WSAEADDRNOTAVAIL).
10050	Network down. (WSAENETDOWN).
10051	Network not reached. (WSAENETUNREACH).
10052	Network connection aborted by reset. (WSAENETRESET).
10053	Network connection aborted by software. (WSAECONNABORTED).
10054	Network connection aborted by remote PC. (WSAECONNRESET).
10055	Operation requested cannot be completed due low memory. (WSAENOBUFS).
10056	Connection requested on a socket already in use. (WSAEISCONN).
10057	Socket not connected, transmission/reception operation disabled. (WSAENOTCONN).
10058	Socket connected in shutdown, transmission/reception operation disabled (WSAESHUTDOWN).
10059	(WSAETOOMANYREFS).
10060	Connection request failed because remote PC has not answered in time due. (WSAETIMEDOUT).
10061	Connection request denied because remote PC does not provide the service requested. (WSAECONNREFUSED).
10062	(WSAELOOP).
10063	(WSAENAMETOOLONG).
10064	Operation failure because remote PC is inactive. (WSAEHOSTDOWN).
10065	Operation requested to unknown remote PC. (WSAEHOSTUNREACH).
10066	(WSAENOTEMPTY).
10067	Process limit exceeded. (WSAEPROCLIM).
10068	(WSAEUSERS).
10069	(WSAEDQUOT).
10070	(WSAESTALE).
10071	(WSAEREMOTE).
10091	Network subsystem not available. (WSASYSNOTREADY).
10092	Winsock.dll version not supported. (WSAVERNOTSUPPORTED).
10093	Winsock not initialized. (WSANOTINITIALISED).
10101	Shutdown command undergoing. (WSAEDISCON)
10801	Failure on the allocation of control memory.
10805	Failure on the creation of reception control semaphore.

10806	Failure on the creation of end of reception control semaphore.
10807	Failure on the allocation of reception buffer.
10808	Failure on the allocation of transmission buffer.
10809	Connection identifier already released or invalid.
10811	Communication library RAS not correct loaded.
10822	Connection ended.
10830	Invalid configuration of communication mode.
10831	Address of remote PC not configured.
10900	Data compression successfully done.
10901	Data decompression not concluded.
10902	Type of Proxy Server configured not supported.

Error codes of the X.25 communication interface

Code	Description
15001	Internal system error.
15002	Internal system error.
15004	Internal system error.
15005	Communication link inactive.
15007	Network has sent a reset, check if signal 104 is active on modem. If not, contact Network Provider.
15008	Invalid command for X.25 interface.
15009	All logic channels on circuit are busy.
15010	Operation chosen cannot be done.
15014	Level 2 of X.25 not active.
15015	Number of transmission or reception pending exceeded maximum limit of X.25 internal queues.
15016	Received confirmation package CLEAR in answer to a RESET.
15017	Message too large for buffer specified in the application.
15018	Received a message with qualified bit active. Nevertheless it does not interfere in use of application.
15019	User sent a disconnect signal to remote PC.
15020	Subscriber called, asked for disconnection or reinitialization.
15021	All logic channels of number called are busy.
15022	Received disconnection signal from remote PC, after establishing the connection.
15023	This facility does not exist.
15025	Network blocked. Try latter on.
15026	Number called is inactive.
15029	Number called is inactive.
15031	Number called belongs to a closed group.
15033	Number called does not exist.
15037	Received disconnect signal from remote PC.
15039	Network detected an error in the procedure of local subscriber.
15041	RPOA disconnected.

15045	Number called does not bear collect calls.
15053	Number called is invalid.
15061	Facility not found.
15070	User sent reset signal.
15073	Received reset signal from remote PC.
15075	Network detected an error on local subscriber.
15077	Network jammed. Try latter.
15079	Number called is inactive.
15085	Network sent a reset signal.
15087	Number called is invalid.
15090	No response to connection request.
15091	Restart signal sent.
15092	No response to reset command.
15093	No response to interruption command.
15094	Unable to allocate memory for reception compression dictionary.
15095	Unable to allocate memory for transmission compression dictionary.
15099	Number called is out of service.
15801 a	Internal error on APIX25
15808	
15809	Communication ended by remote PC.
15902	Error at package capsulizing.

Error codes of the Serial communication interface

Code	Description
17601	Not enough memory available
17602	Internal Error
17603	Error serial port opening
17604	Access denied to serial port
17605	Serial port not found
17606	Error on configuration of serial port
17607	Error on serial port while receiving
17608	Error on serial port while sending
17631	No number to dial
17632	(DTE) connection address not informed
17633	Error at memory allocation
17634	Invalid modem command (ERROR)
17635	Modem busy (BUSY)
17636	Modem with no carrier (NO CARRIER)
17637	Modem with no dial tone (NO DIAL TONE)
17638	Modem receiving a call (RING)
17639	Time limit exceed while awaiting a response from modem.
17640	Invalid serial port, cable to modem not connected or any invalid response from PAD or modem.

17661	Clear signal received from remote PC
17662	Invalid PAD command
17663	RESET sent by PAD
17664	PAD already connected (ENGAGED)
17665	Time limit exceeded while awaiting a response from PAD.
17671	MODEM signals down. Impossible transmit or receive.
17672	PAD inactive. Impossible transmit or receive.
17673	Process cancelled by the user.

Error codes of the TCP/IP (Native Encryption) communication interface

Code	Description
18001	Cryptography not concluded.
18002	Decrypt not satisfactorily concluded.
18003	Import of public key not satisfactorily concluded.
18004	Export of session key not satisfactorily concluded.
18005	Import of session key not satisfactorily concluded.
18006	Creation of cryptography context not satisfactorily concluded.
18007	Generation of public key not satisfactorily concluded.
18008	Generation of session key not satisfactorily concluded.
18009	Export of public key not satisfactorily concluded.
18900	Negotiation time limit for keys has expired.
18901	Keys negotiation cancelled.
18902	Internal failure.

Error codes of the TCP/IP (Proxy) communication interface

Code	Description
19001	Server reported a general error. (SOCKS5)
19002	Connection to requested address is blocked. (SOCKS5)
19003	Network not reached. (SOCKS5)
19004	Address requested not found. (SOCKS5)
19005	Connection request denied. (SOCKS5)
19006	TTL expired. (SOCKS5)
19007	Command requested is not supported. (SOCKS5)
19008	Type of address not supported. (SOCKS5)
19091	Request rejected or failed. (SOCKS4)
19092	Request rejected because Server SOCKS failed to communicate to identifier. (SOCKS4)
19093	Request rejected because Server SOCKS failed to communicate to identifier. (SOCKS4)
19256 a	User authentication not accepted. (SOCKS5)
19399	
19401	Request denied by proxy. (HTTP)
19402	This code is reserved for future use (HTTP).

19403	User/password not authenticated. (HTTP)
19404	The page requested was not found (HTTP).
19405	Access method is not allowed (HTTP).
19406	The resource has the features requested (HTTP).
19407	The proxy server requires authentication (HTTP).
19408	Timeout for the request (HTTP).
19409	The request cannot be processed because there is a resource conflict (HTTP).
19410	The requested resource is unavailable (HTTP).
19411	The server refused the request because it did not find the Content-Length (HTTP).
19412	The server refused the request because the pre-conditions field is invalid (HTTP).
19413	The server refused the request because the content exceeds the size limit (HTTP).
19414	The server refused the request because the URI field exceeds the limit (HTTP).
19415	The server refused the request because it has an unsupported format (HTTP).
19416	The server refused the request because the Range field has a value not supported (HTTP).
19417	The server refused the request because the Expect field has a value not supported (HTTP).
19500	The server found an internal error when trying to process the request (HTTP).
19501	The server does not support a required functionality (HTTP).
19502	The server cannot establish contact or failed to connect to another server (HTTP).
19503	The server is not available to process the request (HTTP).
19504	Timeout occurred in the communication between servers (HTTP).
19505	The server refused the request because the protocol version is not supported (HTTP).
19512	Version informed not supported. (SOCKS4, SOCKS5)
19513	Authentication method requested is not supported. (SOCKS5)
19514	Time limit for response has expired. (SOCKS4, SOCKS5, HTTP)
19515	Internal Failure.

Error codes of the TCP/IP (Encryption SSL3) communication interface

Code	Description
20001	Negotiation of protocol SSL3 not satisfactorily concluded.
20002	Protocol waiting for reading.
20003	Protocol waiting for writing.
20004	Protocol waiting certificate checking (X509).
20005	Protocol reported an error on TCP/IP pile.
20006	Protocol in operation.
20007	Protocol waiting CONNECT command.
20008	Protocol waiting ACCEPT command.
20851	Failed to allocate context for SSL3.
20852	List of invalid algorithms.
20853	Certificate invalid or not found.
20854	Private key file not found or invalid.
20855	Invalid certificate file for private key.

20856	Directory of files of CA certificates invalid or nonexistent.
20857	Directory of the certificate files does not exist or invalid.
20858	SSL3 connection context is invalid.
20859	Failed to configure the SSL3 connection descriptor.

Audit file

The STCP OFTP Server generates an audit log file, containing information corresponding to the beginning and end of the session, start and end of the transfer. Through these files you can create reports and statistics using the service.

The audit file is stored in the **LOG** subdirectory of control with the following nomenclature: **YYYYMMDD.log.txt**, each line of the file is a record of fixed format containing the information described below:

Audit file format

Sequenece	Size	Format	Description
1	14	N	Date and time of occurrence. (YYYYMMDDhhmmss)
2	4	N	Código da operação relacionada a este registro: Code of operation related to this item: 0000 – Login incoming 0001 – End of incoming session 0002 – Start of output session 0003 – End of output session 0004 – Start of file transmission 0005 – End of file transmission 0006 – Start of file reception 0007 – End of file reception
3	30	X	Filename
4	16	X	Name of the communication process
5	8	X	Process code
6	8	X	Código da thread Thread code
7	6	N	Result 000000 – Success
8	12	N	File size
9	256	X	Filename
10	128	X	General information

Security

The STCP OFTP Server implements the security at two levels: user authentication by the application and the data encryption.

User authentication by the application (ODETTE ID)

The user authentication is performed by application through the recognition of a user with up to 26 (twenty six) characters and password with up to eight (8) characters before the start of transfer.

Encryption

Encryption is the encoding of data in order to protect its contents from unwanted people. The mathematical algorithms used to protect data are called encoders.

There are two types of encoders: asymmetric (public key) and symmetric (conventional).

Asymmetrical encoders operate with a pair of keys: public and private. The key that encrypts the data is not the same decoding.

The encoders use a single symmetric key. The key that encrypts data is the same as decoding.

Symmetrical encoders are faster than asymmetric and so are used to encode large volumes of data, but the asymmetric encoders serve to maintain the privacy during the exchange of symmetric keys and digital signature.

Message Digests

The representation of a message of variable size in a small message of fixed length is called 'hash' or 'Message Digest'.

Algorithms 'hash' were designed so as to produce a single representation for each message and make it extremely difficult process of reconstruction of the message from your 'hash'.

Digital Signature

The Digital Signature is the process of encoding the 'hash' of a given message with the sender's private key. Anyone who receives a digitally signed message can, through the issuer's public key, decode the 'hash' and verify its origin.

Certificate

The Certificate is the association public key to the identification of its owner (individual name, address of the server or otherwise) issued and signed by a Certification Authority (CA).

The certificate also includes the information of the certification authority and its period of validity. Additionally more information (lengths) can be attached (serial number and others).

Certification Authority (CA)

The Certification Authority is the company responsible by the verification and processing of requests for certificate (certificate request), emission and maintenance. These companies maintain a list of procedures and requirements to ensure the authenticity of the key public.

It is possible to create your own certificate authority (CA), in general, to be used inside the network (Intranet).

Secure Socket Layer (SSL)

SSL is a protocol layer for use between the application and TCP/IP communication layer. SSL provides services for secure communication between the client application and server, allowing mutual authentication, digital signature (integrity) and encryption (privacy).

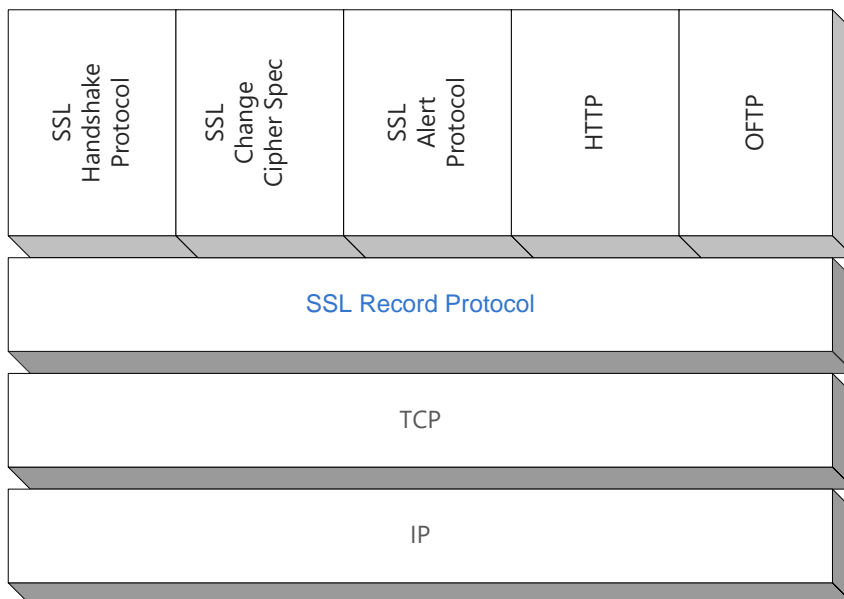


Figure 1 - Architecture SSL

SSL supports the specific choice of algorithms for encryption, 'hash' and digital signature. The selection of algorithms between the client and server is performed in the session establishment protocol.

SSL has different versions, adopted by STCP OFTP Server is version 3.0.

Encryption in STCP OFTP Server

The STCP OFTP Server uses encryption on the transport level where a secure tunnel is established between the client and server and all data traffic is encrypted. The choice of native or SSL3 encryption is performed on the product configuration.

Native Encryption

A "native encryption" is a proprietary implementation of key exchange and encryption of data using the algorithms of symmetric and asymmetric keys where the keys are dynamically negotiated. There are three (3) configuration options for encryption levels: Normal, Medium and High, with the following characteristics:

- Normal - Asymmetric key of 512 bits and symmetric key of 48 bits
- Medium - Asymmetric key of 1024 bits and symmetric key of 56 bits
- High - Asymmetric key of 2048 bits and symmetric key of 128 bits

SSL3 encryption in STCP OFTP Server

The STCP OFTP Server starts the process of secure communication with the request to the SSL3 layer opening a new session with the exchange of public key (asymmetric) followed by the exchange of session key (symmetric).

These are the steps for the key exchange:

1. The client requests to open a secure session with the server. The server has a certificate (X.509), containing the public key and private key.
2. The server sends a copy of your certificate containing the public key for the client.
3. The client generates a new symmetric key for the session.
4. The client encrypts the session key with the server's public key and sends the encrypted session key to the server.
5. The server uses its private key to decrypt the session key.

The STCP OFTP Server allows the configuration of the set of algorithms for encoding to be used for encryption, digital signature and hash.

Communication Architecture of STCP OFTP Server

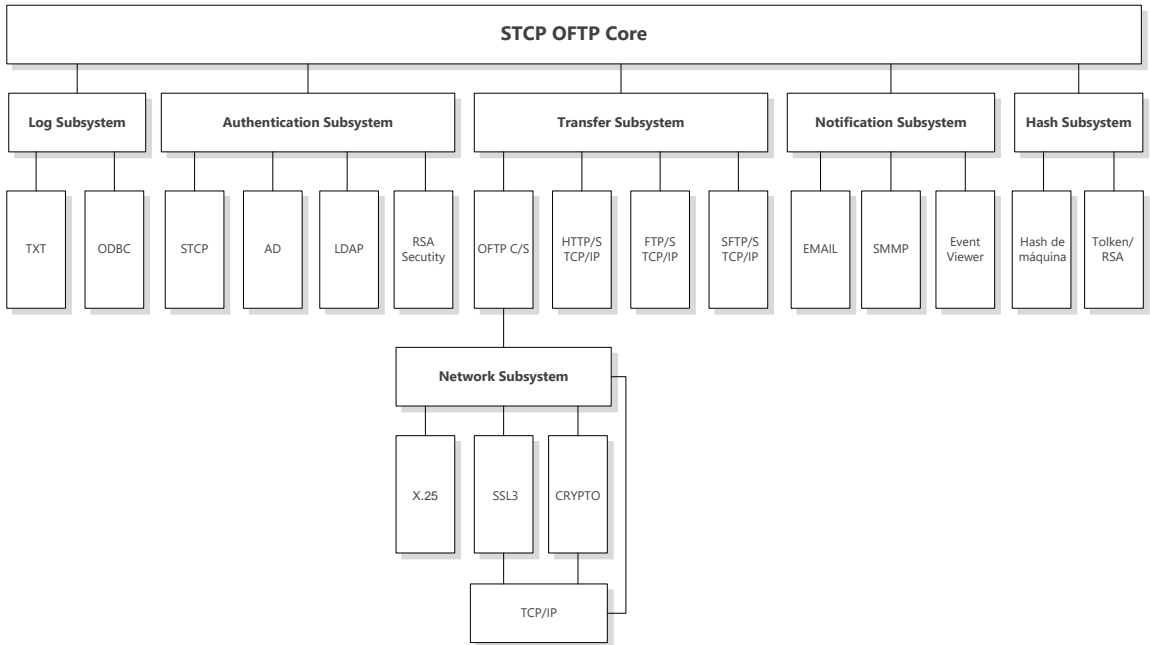


Figure 2 - Architecture of STCP OFTP Server

The STCP OFTP Server has a modular architecture and allows the configuration of different types of communication.

The supported algorithms in communication

The STCP OFTP Server allows the configuration of different algorithms and groups of algorithms for SSL3 communication, below the list and definitions:

Algorithms	Description
ALL	All algorithms.
HIGH	Encoders with more than 128 key bits.
MEDIUM	Encoders with key of 128 bits.
LOW	Encoders with key of 56 or 64 bits.
EXP EXPORT	Exportable encoders with 40 or 56 bits.
EXPORT40	Exportable encoders with 40 bits.
EXPORT56	Exportable encoders with 56 bits.
eNULL NULL	Without encoders (not recommended).
aNULL	Without authentication. It corresponds to the algorithm DH anonymous. This configuration is vulnerable to attack "man in the middle" (not

	recommended).
RSA	Encoders that use DH (Diffie Hellman) for validation of key and certificate signed by a CA DH with RSA key.
kEDH	Encoders that use EDH (Ephemeral Diffie Hellman) for key validation.
kDHr	Encoders that use DH (Diffie Hellman) for validation of key and DH certificate signed by a CA with RSA key.
kDHd	Encoders that use DH for validation of key and DH certificate signed by a CA with DSS key.
aRSA	Authentication RSA with certificate with RSA key.
aDSS DSS	Authentication DSS with certificate with DSS key.
aDH	Authentication DH with certificate with DSS key.
kFZA aFZA eFZA FZA	Encoders, authentication with algorithm FORTEZZA (not available).
DH	Encoders, authentication algorithm FORTEZZA (not available).
ADH	Encoders DH anonymous.
3DES	Encoders triple DES.
DES	Encoders DES (Data Encryption Standard).
RC4	Encoders RC4.
RC2	Encoders RC2.
IDEA	Encoders IDEA.
AES	Encoders AES (Advanced Encryption Standard).
MD5	MD5
SHA SHA1	SHA1

Set of Algorithms	Description
ADH-AES256-SHA	Exchange of keys = Diffie-Helman Authentication = No Encryption = AES with 256 bits Mac = SHA1
DHE-RSA-AES256-SHA	Exchange of keys = Diffie-Helman Authentication = RSA Encryption= AES with 256 bits Mac = SHA1
DHE-DSS-AES256-SHA	Exchange of keys = Diffie-Helman Authentication = DSS Encryption = AES with 256 bits Mac = SHA1
AES256-SHA	Exchange of keys = RSA Authentication = RSA Encryption = AES with 256 bits Mac = SHA1

ADH-AES128-SHA	Exchange of keys = Diffie-Helman Authentication = No Encryption = AES with 128 bits Mac = SHA1
DHE-RSA-AES128-SHA	Exchange of keys = Diffie-Helman Authentication = RSA Encryption = AES with 128 bits Mac = SHA1
DHE-DSS-AES128-SHA	Exchange of keys = Diffie-Helman Authentication = DSS Encryption = AES with 128 bits Mac = SHA1
AES128-SHA	Exchange of keys = RSA Authentication = RSA Encryption = AES with 128 bits Mac = SHA1
DHE-DSS-RC4-SHA	Exchange of keys = DH Authentication = DSS Encryption = RC4 with 128 bits Mac = SHA1
EXP1024-DHE-DSS-RC4-SHA	Exchange of keys = DH (1024) Authentication = DSS Encryption = RC4 with 56 bits Mac = SHA1
EXP1024-RC4-SHA	Exchange of keys = RSA (1024) Authentication = RSA Encryption = RC4 with 56 bits Mac = SHA1
EXP1024-DHE-DSS-DES-CBC-SHA	Exchange of keys = DH (1024) Authentication = DSS Encryption = DES with 56 bits Mac = SHA1
EXP1024-DES-CBC-SHA	Exchange of keys = RSA (1024) Authentication = RSA Encryption = DES with 56 bits Mac = SHA1
EXP1024-RC2-CBC-MD5	Exchange of keys = RSA (1024) Authentication = RSA Encryption = RC2 with 56 bits Mac = MD5
EXP1024-RC4-MD5	Exchange of keys = RSA (1024) Authentication = RSA Encryption = RC4 with 56 bits Mac = MD5
EDH-RSA-DES-CBC3-SHA	Exchange of keys = DH Authentication = RSA

	Encryption = 3DES with 168 bits Mac = SHA1
EDH-RSA-DES-CBC-SHA	Exchange of keys = DH Authentication = RSA Encryption = DES with 56 bits Mac = SHA1
EXP-EDH-RSA-DES-CBC-SHA	Exchange of keys = DH (512) Authentication = RSA Encryption = DES with 40 bits Mac = SHA1
EDH-DSS-DES-CBC3-SHA	Exchange of keys = DH Authentication = DSS Encryption = 3DES with 168 bits Mac = SHA1
EDH-DSS-DES-CBC-SHA	Exchange of keys = DH Authentication = DSS Encryption = DES with 56 bits Mac = SHA1
EXP-EDH-DSS-DES-CBC-SHA	Exchange of keys = DH (512) Authentication = DSS Encryption = DES with 40 bits Mac = SHA1
DES-CBC3-SHA	Exchange of keys = RSA Authentication = RSA Encryption = 3DES with 168 bits Mac = SHA1
DES-CBC-SHA	Exchange of keys = RSA Authentication = RSA Encryption = DES with 56 bits Mac = SHA1
EXP-DES-CBC-SHA	Exchange of keys = RSA (512) Authentication = RSA Encryption = DES with 40 bits Mac = SHA1
IDEA-CBC-SHA	Exchange of keys = RSA Authentication = RSA Encryption = IDEA with 128 bits Mac = SHA1
EXP-RC2-CBC-MD5	Exchange of keys = RSA (512) Authentication = RSA Encryption = RC2 with 40 bits Mac = MD5
RC4-SHA	Exchange of keys = RSA Authentication = RSA Encryption = RC4 with 128 bits Mac = SHA1

RC4-MD5	Exchange of keys = RSA Authentication = RSA Encryption = RC4 with 128 bits Mac = MD5
EXP-RC4-MD5	Exchange of keys = RSA(512) Authentication = RSA Encryption = RC4 with 40 bits Mac = MD5
ADH-DES-CBC3-SHA	Exchange of keys = DH Authentication = No Encryption = 3DES with 168 bits Mac = SHA1
ADH-DES-CBC-SHA	Exchange of keys = DH Authentication = No Encryption = DES with 56 bits Mac = SHA1
EXP-ADH-DES-CBC-SHA	Exchange of keys = DH(512) Authentication = No Encryption = DES with 40 bits Mac = SHA1
ADH-RC4-MD5	Exchange of keys = DH Authentication = No Encryption = RC4 with 128 bits Mac = MD5
EXP-ADH-RC4-MD5	Exchange of keys = DH(512) Authentication = No Encryption = RC4 with 40 bits Mac = MD5
NULL-SHA	Exchange of keys = RSA Authentication = RSA Encryption = No Mac = SHA1
NULL-MD5	Exchange of keys = RSA Authentication = RSA Encryption = No Mac = MD5

Why OpenSSL implementation

The Riversoft opted to use the implementation of SSL3 OpenSSL in its line of products as this is currently one of the most used on the world market (Apache, Squid, Tivoli, VPN-1 Firewall-1 among several other products) while allowing the access to its sources by the international community.

Adopting the OFTP global standardization and TLS1/SSL3 is a commitment of the Riversoft to ensure the interoperability of STCP OFTP Server product.

OpenSSL License

OpenSSL License

```
-----  
  
/*  
=====
```

===

- * Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
- *
- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:
- *
- * 1. Redistributions of source code must retain the above copyright
- * notice, this list of conditions and the following disclaimer.
- *
- * 2. Redistributions in binary form must reproduce the above copyright
- * notice, this list of conditions and the following disclaimer in
- * the documentation and/or other materials provided with the
- * distribution.
- *
- * 3. All advertising materials mentioning features or use of this
- * software must display the following acknowledgment:
- * "This product includes software developed by the OpenSSL Project
- * for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
- *
- * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
- * endorse or promote products derived from this software without
- * prior written permission. For written permission, please contact
- * openssl-core@openssl.org.
- *

* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:

* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.

=====
===

* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

*/

Original SSLey License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
```

- * "This product includes cryptographic software written by
- * Eric Young (eay@cryptsoft.com)"
- * The word 'cryptographic' can be left out if the routines from the library
- * being used are not cryptographic related :-).
- * 4. If you include any Windows specific code (or a derivative thereof) from
- * the apps directory (application code) you must include an acknowledgement:
- * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
- *
- * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
- * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
- * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
- * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
- * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
- * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
- * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
- * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
- * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
- * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
- * SUCH DAMAGE.
- *
- * The licence and distribution terms for any publically available version or
- * derivative of this code cannot be changed. i.e. this code cannot simply be
- * copied and put under another distribution licence
- * [including the GNU Public Licence.]
- */

References

www.openssl.org

www.modssl.org

<http://oss-institute.org/newspdf/OSSIFIPSRef.pdf>

www.odette.org

STCP OFTP Server
www.riversoft.com.br

www.oftp.net