Digital Payments
for a Trusted World

WORLDLINE

SFT User Manual FTPS

Secure File Transfer with FTP over TLS

Author:	Worldline Financial Services
Version:	3.0
Document date:	1 December 2021
Classification:	Public

Table of contents

1 Introduction

This manual provides information regarding Worldline Secure File Transfer services, in particular the FTP over TLS connection type.

1.1 Maintenance of this document

This document is managed and maintained by Worldline Middleware team. Amendment and publication of this document may be carried out solely by this team.

We would be grateful for any feedback regarding any unclear or incorrect information found in this manual. Please send your response to the department Client Services Desk of Worldline (for contact details, see chapter 12, Support processes: questions and changes).

1.2 Target groups

This manual is primarily intended for network specialists, functional and technical designers and administrators, ICT architects and FTP programmers who are involved in the implementation and use of the FTP over TLS connection.

Please note:
Worldline has given the file transfer platform the name: Secure File Transfer (SFT).
The FTP over TLS (FTPs) connection with SFT is not to be confused with SFTP (file transfer using the SSH protocol).

1.3 Test versus Production environment

Worldline Secure File Transfer has two separate environments: a Test/Acceptance environment and a Production environment. The credentials for Test/Acceptance are different from the credentials for the Production environment.

On the test/acceptance environment NO production data is allowed. You should test using test/dummy data.

1.4 Structure of this manual

This manual is divided into three sections in which the following is explained:

- Configuration of the connection with FTP over TLS
- How to make a connection
- Recurring procedures.

The first section describes how Worldline has configured the connection with FTP over TLS and comprises chapters 2 to 5, which contain the following information:

- Network variants via which you will be able to connect to our File Transfer system
- How the security works
- The way the system will route your data to its destination based on file names
- How Worldline has set up the backup and fall-back.

The second section explains in detail the one-off procedure you must perform in order to carry out future submissions of your data using FTP over TLS. This section comprises chapters 6 to 8, which contain the following information:

- The technical aspects of the connection (organisation of your network)
- Requesting and installing a certificate
- Testing your connection

The third section explains in detail the activities that recur. This section comprises chapters 9 to 12, which contain the following information:

- How to change your password
- How to send files
- How to collect files
- How to handle compressed files
- How to submit questions and/or changes

As each FTP client works differently, we are not able to provide a commonly used description. Therefore we provide an example of the WS_FTP client in annex 1.

2 FTP over TLS network variants and infrastructure

FTP over TLS provides a secure option through the strong level of data encryption.

2.1 Two network variants

Two network variants can be used for FTP over TLS:

- FTP over TLS via internet
- FTP over TLS via a private E-Line

With a connection via the internet is there is no guaranteed availability and bandwidth by Worldline, but it has the advantage of cost effective high-speed transfers. Furthermore, if you already have an internet connection, the costs will naturally be lower.

If you opt for a more robust connection, then the private E-Line is a good solution, although this will involve additional costs ensuing from the management of the E-Line by the connection provider.

The two network variants will be discussed in the subsequent sections.

2.2 FTP over TLS via internet

This network variant is the preferred choice of both Worldline and the majority of users. Its characteristics are as follows:

- The file transfer speed will depend on the internet connection bandwidth. Please note: As a rule, the available bandwidth cannot be guaranteed in the event of internet use.
- Securing your internet-linked infrastructure will be your responsibility, in addition to which Worldline strongly recommends using firewalls.

2.3 FTP over TLS via E-Line

For banks and large corporations, Worldline offers the option of connecting via an E-Line.
E-lines are based on a dedicated network and are therefore separate from the internet. One of the advantages of an E-line is that, service level agreements can be made with the connection provider with regard to guaranteed bandwidth and connection availability (up to 99,999%). As a result, such connections are more robust and have a higher level of security. The E-Line connection can be scaled from 2MB/second up to 100 MB/second. This type of connection can also be useful if you exchange multiple types of traffic with Worldline.
From a technical point of view, this type of connection is very similar to an internet connection.
Given the fact that these connections are always tailor-made, please contact the Technical Support department for additional information. This will not be discussed in any further detail in this manual.

3 Security

This chapter describes how the security of your data and the continuity of services will be guaranteed.

3.1 Introduction

Agreements and technical facilities will ensure that Secure File Transfer secures your data at all times. The security aspects are as follows:

Authenticity

Authenticity will be ensured by means of the following:

- Certificate verification and validation
- Username and password checks
- Whitelisting source IP-address

Confidentiality

Confidentiality regarding public and internal connections will be guaranteed through the use of FTP with Transport Layer Security (TLS), also known as FTP over TLS or FTPS.

Integrity

The integrity of the data that is to be transported will be guaranteed via the TLS hashing mechanism (digital signature).

Authorisation

Authorisation will be granted by means of the following:

- Username/password combination
- Contract conclusion checks (processing contracts)

3.2 Encrypted file transmission via TLS

FTP over TLS provides security by authentication and encryption to exchange files that contain confidential information. In use, FTP with TLS will be very similar to standard FTP. The important difference is that all confidential information will be encrypted via TLS and a strong encryption algorithm as AES. The client and server will automatically carry this out for you. This encryption will be applied to both the username and password required to log in, as well as to the files sent via FTP with TLS.
By default the following cipher suites are acceptable by Worldline unless agreed otherwise:

- ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_RSA_WITH_AES_128_GCM_SHA256
- RSA_WITH_AES_256_GCM_SHA384*
- RSA_WITH_AES_128_GCM_SHA256
- RSA_WITH_AES_256_CBC_SHA256
- RSA_WITH_AES_256_CBC_SHA

3.3 Authentication by means of certificates

An important aspect of the FTP over TLS infrastructure is the use of digital certificates. Both the FTP over TLS client and FTP over TLS server are equipped with certificates for the purpose of authentication. This authentication is based on the client and server only accepting one another's certificates when they have been signed by the correct (Worldline) Certificate Authority.

A Public Key Infrastructure (PKI) service will be used to issue certificates. Worldline has set up a private CA (Certificate Authority). Private, in relation to this matter, means that this CA will only issue certificates for the Secure File Transfer services.

Worldline will have full control over issuing of certificates and will determine which certificate applications will be accepted or rejected via a RA function. Worldline will also be able to revoke previously approved certificates when, for example, a security risk has been determined or when the contract expires.
More details on certificates can be found in the Worldline Certificate Policy (downloadable from our website: www.financial-service.worldline.com (Contact & Support – User downloads).

In case your security policy does not allow the usage of the Worldline PKI certificates, please contact the department Client Service Desk of Worldline.

You will find more information on how to obtain an Worldline certificate in a separate document: ‘Request WL Client Certificate’.

3.4 Access with usernames and passwords

Only you will have access to your Worldline files.

Your files will not only be secured during transmission to and from Worldline, but also at Worldline. Worldline guarantees that its customers only have access to their own details/data/files. This will be made possible by the fact that each user will have to enter their own username and password in order to gain entry to their mailbox.

Extra-secure password usage will be ensured as follows:

- The contact person receives a combination of a username and an initial password from Worldline in a secured envelope. Worldline will not activate a username and password until it has received a written confirmation of receipt signed by the contact person.
- The contact person has to change the initial password promptly at the first login. After the initial password has been changed passwords must be changed thereafter at least every 35 days. Please refer to chapter 9 ‘Changing the password’ for additional information.
- In the event a password is lost, only the (authorised) contact person will be able to request a new password (through the department Client Service Desk).

Please note:
Worldline will regard the contact person as authorised if his/her name and signature is registered via the Service Request form. The contact person is responsible not to share the password and is responsible for the proper use of the certificate and username/password combination on the customers system(s).

3.5 Username and password management

The registered contact person is responsible for the management of the username and password within their organisation. Access to FTP over TLS will only be possible with a username and valid password. Only a limited number of persons within the organisation should be authorised to use FTP over TLS, each having their individually assigned user name. Worldline will not allow the sharing of a single user name and password between multiple individuals. This will prevent unauthorised use and internal fraud. Additional user names and passwords can be requested via the 'Secure FTP’ form. This form can be downloaded from: www.financial-service.worldline.com (Contact & Support – User downloads).

4 File naming convention and routing mechanism

When you wish to exchange files with Worldline via FTP over TLS, the file names must comply with a specific naming convention.

Files sent in will be routed to the appropriate processing system on the basis of the file name. We will not be able to route sent files if their name differs from the naming convention and will therefore be unable to process them. In such cases you will receive an error message by e-mail.

4.1 Standard file name convention

The following standard will apply within FTP over TLS with regard to the structure of file names:

```
<SENDER>.<DESTINATION>.<TYPE>.<REFERENCE>.<EXTENSION>
```

The separate fields are defined as follows:

Field	Format	Length	Description
<SENDER>	UPPERCASE, alpha-numeric	1-8	The ID (router address) of the submitting party. This will be assigned by Worldline and made known to the customer.
<DESTINATION>	UPPERCASE, alpha-numeric	1-8	The ID (router address) of the destination. Use 'SFT' unless another specific value has been assigned by Worldline.
<TYPE>	UPPERCASE, alpha-numeric	1-8	The ID of the file type being exchanged. The file type determines the type of processing by Worldline. The file types to be used will be assigned by Worldline.
<REFERENCE>	UPPERCASE, alpha-numeric	1-8	A unique alpha-numeric file reference ID assigned by the submitting party. The field must be unique for the submitting party within a time frame of at least 35 days.
<EXTENSION>	UPPERCASE, alpha-numeric	1-8	The file name suffix, assigned by the submitting party indicating the format of the file. Important extensions include the following: TXT ('readable'/ASCII data) DAT (binary) PDF (Adobe Acrobat Reader format, binary) XLS (Microsoft Excel format, binary) XML (Extensible Mark-up Language format, binary) ZIP (compressed files, binary)

Specifications:

- Each field is mandatory with a dot '.' as separator

Below is an example of a complete file name for a file sent from <SENDER> R0001234 to <DESTINATION> SFT:

R0001234.SFT.PACS008.C1234567.XML

4.1.1 Receipt of different file types

A customer will be able to receive numerous file types via Secure File Transfer. Each type will be processed by a specific application on the side of the customer.
The customer must have a mechanism that ensures that each file type is routed to the correct application on the basis of the field `<TYPE>`.

4.1.2 Multiple destination id's (optional)

Worldline can only issue multiple <DESTINATION> id's (router addresses) to a customer in complex cases (for example, if a group has numerous offices, all of which process the same file types and also share the same connection). The customer will then be able to route internally on the basis of the <DESTINATION> id in the file name.
Additional <DESTINATION> id (router address) requests can be subject to extra charges, please contact the department Client Service Desk of Worldline for more information.

4.2 Custom file name convention

However we prefer the standard naming convention, we can agree on a custom specific naming convention. Please contact the department Client Service Desk of Worldline for additional information if you are unable to comply to the standard naming convention.

5 Fall-back and backup facilities

Worldline will have two identical environments; a primary location and a secondary location, both with a backup facility. Under normal circumstances each customer will have a FTP connection with the primary location.

In the event of a network failure at the primary location the system will automatically use the network infrastructure at the secondary location. With the exception of a brief hiccup, the customer will not notice a difference.

In the event of a total failure at the primary location, a procedure will be started in order to summon the secondary location as the fall-back location.
A number of procedures will ensure that the FTP traffic for the different network variants is routed to the secondary location. During these procedures it will not be possible to connect to Worldline. The customer will not notice a difference after activation of the fall-back location and does not need to make any changes.

6 Configuration of your network

This chapter explains the procedure for connecting to Secure File Transfer at network level. Once the connection has been made it will be possible to use FTP commands and programmes at transportation level.

Two network variants can be used for FTP over TLS:

- FTP over TLS via internet
- FTP over TLS via E-Line

The specifications for these network variants are described in chapter 2 ‘FTP over TLS network variants and infrastructure’.

6.1 Configuration of your firewall

In order to be able to connect to the Worldline Secure File Transfer system, you will need to open some TCP ports in your firewall.

The technical details for the configuration will be provided during the on-boarding process.

6.2 Configuration of the FTP client in your environment

The FTP client can be used in two different ways, i.e. interactively via GUI screens or by means of batches, usually via a script. You should consult the instruction manuals of your FTP client on how to configure it for the use of FTP over TLS and the installation and use of certificates.

The FTP server is configured for FTP Passive Mode and explicit SSL/TLS. Please refer to the documentation of your FTP client for more details.

As each FTP client works differently, we are not able to provide a commonly used description. We provide an example of a commonly used FTP client (WS-FTP) in Annex 1.

7 Testing your connection

It is advisable to first check whether the connection is functioning correctly and whether the files are being forwarded in the required manner. You can test this easily by sending a file to yourself. This connection test and file transfer test can simply be carried out in the Worldline production environment.

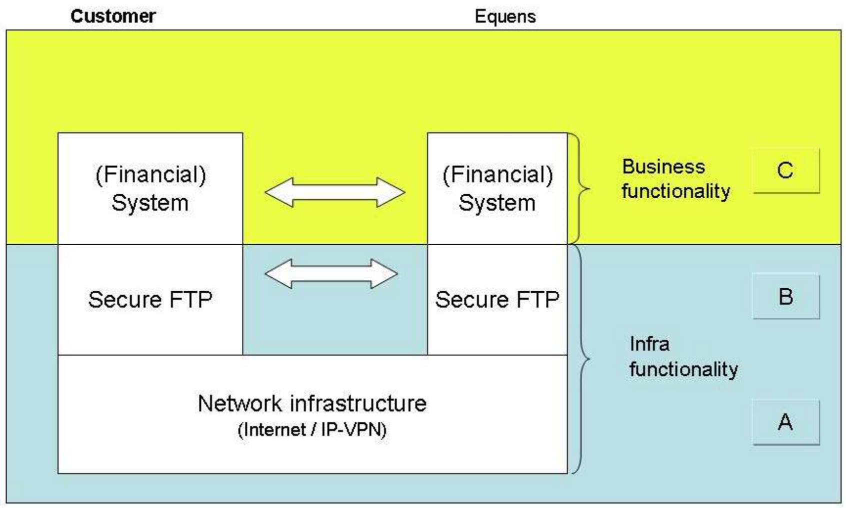
Please note:
If you also wish to carry out processing tests, you must carry these out in the test/acceptance environment (!). These processing tests must be scheduled at least one week in advance in consultation with the department Client Service Desk of Worldline and the relevant business unit.

7.1 Difference between three test types

Tests can be carried out at three levels:

- Level A: connection test
- Level B: file transfer tests
- Level C: processing tests (application level)

The level A and B tests relate specifically to the FTP over TLS connection.
The level C tests are not related to the connection type.
The following figure shows the levels at which the tests should be carried out.



Testing can only commence if the following conditions have been met:

- All relevant data must have been entered in the various Worldline databases
- You must have installed a FTP over TLS client
- You must have installed both the client and CA root certificates

7.2 Connection test

Connection test features and conditions

Feature	Description
Subject	The connection with FTP over TLS. This involves aspects such as: The ability to log in with FTP + TLS Changing a password
Objective	Checking whether the FTP over TLS specifications have been properly implemented at the customer's side
Conditions	You do not need to contact Worldline in order to carry out this test
Importance	Recommended
Environment	Production or test/acceptance environment

Connection test execution

You can use your FTP client in the production or test/acceptance environment to test whether a connection can be established. Please refer to the documentation of your FTP client for setting up a connection. Changing the password is a good way to test the connection. The procedure is explained in section 8.4 ‘Password changing procedure’.

7.3 File transfer test

File transfer test features and conditions

Feature	Description
Subject	Routing to and from yourself
Objective	Checking whether file transfers between Worldline and the customer via FTP over TLS are successful
Conditions	You do not need to contact Worldline in order to carry out this test
Importance	Recommended
Environment	Production or test/acceptance environment. On the test/acceptance environment NO production data is allowed. You should test using test/dummy data.

7.4 File transfer test execution

File transfer tests consists of sending a file to yourself.
Please do this in the following manner:

Prepare a test file and change its name according to the naming convention.

- For <DESTINATION> enter the same as for <SENDER>
- Enter the SELFTEST value for <TYPE>

Example filename for FTP over TLS:
R0001234.R0001234.SELFTEST.TEST1234.TXT

- Start your FTP over TLS client
- Connect to sft.equens.com (or sftacc.equens.com for test/acceptance)
- Give the AUTH TLS command
- Log in with your username and password
- Submit the file to the server
  Please refer to chapter 10 ‘File sending’ for additional information.
  The file will be fully processed at Worldline. This means the file will be routed to the <DESTINATION>, in this case yourself. The file will ultimately be made available for collection as an output file.
- Wait for at least 2 minutes and collect the file (time needed for routing purposes)
  Please refer to chapter 11 ‘File retrieval’ for additional information.

The test has been completed successfully once you have collected the file.

7.5 FTP-commands

The FTP commands that are used in FTP over TLS sessions are described below. Graphical FTP applications generate these commands automatically.
If a command line FTP application is used then these commands must be entered manually. The FTP server is configured for FTP Passive Mode only and for explicit SSL/TLS. Please refer to the manual of your FTP client for details.

The FTP commands and responses from the server are stored in the logs of the FTP clients. It is important to know the meaning of the commands when analysing problems that might occur. Examples of logs (correct and error situations) are given in the configuration description for the WS_FTP client in the annex of this document.

This is not a complete overview of all the commands that can occur in a FTP session, only the most important commands are described.

7.5.1 Setting up a session

- AUTH TLS: Set up a session in *Explicit TLS* mode. This **must** be the first command given
- USER, PASS: With these commands the *username* and *password* are given, usually directly after the AUTH TLS command

7.5.2 Changing the password

- SITE CPWD <new password>: With this command the *password* is changed.

7.5.3 Data transfer

- PASV: With this command the data connection is set to *passive FTP-mode*
- DIR or LS: Request an overview of all available files
- GET or RETR: Receive a file
- PUT or STOR: Send a file
- NOOP: If a data transfer takes longer than 10 minutes a time-out may occur which could terminate the FTP session before the data transfer has been completed. To prevent a time-out you could use the 'NOOP' command to keep the FTP session alive.
- BYE: Ending a session

8 Changing the password

According to Worldline specifications you must change the initial password. This is done by means of the FTP command SITE CPWD <new password>
The username and initial password is sent to the contact person of your organisation specified on the FTP over TLS Service Request form.

8.1 Password specifications

A password must comply with the following specifications:

- A password must comprise of letters and digits (case sensitive)
- A password must comprise of a minimum of seven and a maximum of twenty characters
- A password that has already been used cannot be used for the following twenty password changes
- Your account will be locked after three incorrect logins (log in using an incorrect password). In case you have forgotten the correct password you will need to request a new password. The contact person will need to contact the department Client Service Desk of Worldline to request a new password form

8.2 Password period of validity

The first time you log in you will need to change your initial password immediately. You will subsequently have to change your password at least every 35 days. Naturally you could also do this during every FTP over TLS session.
If you do not change your password within 35 days, your account will be blocked and you will be unable to log in. To unblock your account, the contact person will need to contact the Technical Support department to request a form for a new password request.

The new password request form needs to be filled in and returned to Worldline (follow the instructions on the form). Only the contact person can request a new password. To register a new contact person a Service Request Form FTP over TLS needs to be send to Worldline requesting a change of contact person.

If you have received a new password you have to change it immediately after logging in. The initial password is only valid for a very limited amount of time after it has been issued.

Please note:
You will **not** receive a warning when your password is about to expire.

8.3 Password changing procedure

The possibility to change the password for a specific FTP username has not been described within a general RFC.
Consequently, Worldline has decided to opt for the most common type of implementation, i.e. the implementation procedure based on the SITE CPWD command.

Please change your password as follows:

- Start your FTP over TLS client software
- Connect to the FTP over TLS server
- Log in using your username and password
- Use the possibility your client provides to give special commands
- Give the following command: SITE CPWD <new password> where <new password> will be your new password
  - The configuration description of the WS_FTP client includes information on using the SITE CPWD command

If return code 200 appears, your password has been successfully changed.
If a different code appears, an error has occurred.

The FTP over TLS server can give the following return codes:

Return code	Message	Explanation
200	CPWD successful	Password changed successfully
500	CPWD no authorization	The password cannot be changed. Please contact the Client Service Desk of Worldline.
501	SITE unknown option	After the command SITE CPWD no password is entered. Please correct this.
503	Invalid sequence of commands	Configuration error of the FTP client. You used a 'clear command channel', this is not permitted.
530	Not logged in	You need to be logged in to be able to change the password
550	Requested action not taken	The password does not comply with the specifications, please see section 8.2

9 File sending

You can send files to Worldline using commands in your FTP over TLS client. When sending files you will need to initiate the transfer. You can also send compressed data files. Please refer to chapter 12 ‘Using compressed files’ for additional information.

Please note:
The maximum file size for FTP over TLS is 2 GB (uncompressed).

9.1 Manual file sending

The procedure for sending files to Worldline comprises the following steps:

- Correctly name the files in accordance with the following convention:
  <SENDER>.<DESTINATION>.<TYPE>.<REFERENCE>.<EXTENSION>

  Please refer to section 4.2 “FTP over TLS file name convention” for the correct specifications.
  In the event a file is sent to Worldline:
  - Enter 'SFT' in the file name in the <DESTINATION> field
    The file will be routed to the processing unit. The internal destination will be derived from the entry made for <TYPE>.
  - Enter the correct value in the file name in the <TYPE> field
  - Also fill in the remaining fields. These fields are mandatory
- Start your FTP over TLS client
- Connect to Worldline
  - Give the AUTH TLS command if this is not done automatically
  - Log on using your username
  - Enter your password
- Check if the connection is set up successfully
  This is the case if the following criteria are met:
  - You see the content of your Worldline directory
  - No error messages appear in the log window
- Send the data file
- Check whether the file has been sent successfully
  This is the case when the following criteria are met:
  - Directly after sending the file is in your Worldline directory
  - In the log window 'Transfer completed successfully', or something similar, is shown
- After two minutes, check if the file has disappeared from the directory
  (Worldline processes files within two minutes after they have been received)
- If the sent file does not disappear from the directory:
  - If an incorrect file name has been used, please remove the file
    An error message will be sent to the e-mail address you have given for the connection
  - Correct the filename, enter a different <REFERENCE> and resend the file
- Close the connection
- Close the FTP-client

9.2 Automatic file sending

Most FTP over TLS clients have the possibility to send files automatically. The client can be set up in such a way that it will check the local system directory for waiting files. If this is the case, the files will be sent to Worldline without any further action being required from the user. If the files are sent successfully, the client can remove the files.
You will be responsible for the automation, as Worldline does not provide support for this.

9.3 Binary file sending

Some file types, such as files with the extension .ZIP, .DAT, .PDF or .BIN must be sent in binary mode. In order to do this you must give the BIN command in a text-based FTP over TLS client before sending the files.

Please note:
Some FTP clients will interpret the file name extension. For example, they will always send files with the .DAT extension in binary mode.
If you send a binary file as a non-binary file, it may arrive corrupted at the destination.

10 File retrieval

You can retrieve files from Worldline using commands in your FTP over TLS client. Retrieving the files from Worldline will be your responsibility.
To do this you need to access your personal client directory in the Worldline system. (Also called the mailbox). The CWD (Change Directory) command will not be required.
After retrieving the files they will be automatically moved to the subdirectory 'ARCHIVE' in your mailbox. Previously retrieved files can be downloaded from the 'ARCHIVE' directory for a limited period of time, after which they will be deleted.

10.1 Manual file retrieval

The procedure for retrieving files comprises the following steps:

- Start your FTP over TLS client
- Connect to Worldline
    - Give the AUTH TLS command if this is not done automatically
    - Log on using your username
    - Enter your password
- Check if the connection is set up successfully
  This is the case if the following criteria are met:
    - You see the content of your Worldline directory
    - No error messages appear in the log window
- Retrieve the data file
- Check whether the file is retrieved successfully
  This is the case when the following criteria are met:
    - Directly after retrieving the file, it is located in your local directory
    - In the log window 'Transfer completed successfully' or something similar is shown
        - Retrieved files are automatically deleted from the Worldline directory. Worldline will transfer them to the subdirectory 'ARCHIVE' in your own directory. If you wish to retrieve a file again, you will be able to retrieve it from this directory.
- Close the connection
- Close the FTP-client

10.2 Automatic file retrieval

Most FTP over TLS clients can also be automated for file retrieval. For example, the client will be able to connect to Worldline and retrieve the available files.
You will be responsible for the automation, as Worldline does not provide support of this nature.

10.3 Binary file retrieval

Most file types, such as files with the extension .ZIP, .DAT, .PDF or .BIN must be sent in binary mode.
In order to do this you must give the BIN command in a text-based FTP over TLS client before retrieving the files.

Please note:
Some FTP clients will interpret the file name extension. For example, they will always retrieve files with the .DAT extension in binary mode.
If you send a binary file as a non-binary file, it may arrive corrupted at the destination.

10.4 Output notification by e-mail

For the connection type FTP over TLS it is possible to receive a notification by e-mail once a file is placed in your mailbox. This e-mail will contain an output notification and the name of the file you can retrieve.

If you would like to use this output notification by e-mail, you can indicate this on the Service Request Form FTP over TLS.

11 Using compressed files

Files can be compressed (zipped) in order to reduce their size and therefore the amount of time that it takes for them to be transmitted. If your connection has sufficient bandwidth then compression will not be necessary and we advise against using it.

Compression programme conditions

- Your compression programme must be compatible with PKZIP version 2.04g
- Acquisition and use of compression software will be your own responsibility
- Please refer to your compression programme manual for information regarding file compression and decompression

Binary file transmission

You must use binary transmission in order to both send and retrieve compressed files. In order to do this you must give the BIN command in a text-related FTP over TLS client before sending or retrieving the files, please see section 10.4, ‘Binary file sending’.

11.1 Sending and receiving compressed files

Conditions

- You will be able to send both compressed and uncompressed files. There is no need to specify this on the Service Request Form.
- Compressed files must be indicated with the <EXTENSION> 'ZIP'
- In case you would like to receive compressed files you must specify this on the Service Request Form.
- The compressed file that you wish to send must not contain more than one data file. The compressed file will be unzipped by Worldline before it is routed to the <DESTINATION> and can be zipped again by Worldline, depending on the configuration of the <DESTINATION>.
- Although the file name *in* the archive does not need to comply with the naming convention, this is advisable.
  This is also more convenient because the majority of compression programmes use the name of the file being compressed in the archive file name. For example: If you were to compress the file R0001234.SFT.PACS008.A1234567.XML, the compressed file will be named R0001234.SFT.PACS008.A1234567.ZIP by default.

11.2 Retrieving compressed files

Conditions

If you wish to receive compressed output from Worldline, then please specify this on the Service Request form.

Features:

If you have stated you wish to receive compressed files, the following rules will apply:

- *All* files you receive from Worldline are compressed, it is not possible to compress specific file types
- The names of both the ZIP archive and the archived file will comply with the naming convention
  For example: the archive MFC.R0001234.VERWINFA.A1234567.ZIP would contain the file MFC.R0001234.VERWINFA.A1234567.TXT

12 Support processes: questions and changes

12.1 FTP over TLS availability

Secure File Transfer will be available 24/7.
Maintenance will be scheduled between Saturday 7:00a.m. and Sunday 4:00p.m.

12.2 Contact information Client Service Desk

Support for File Transfer products will be provided by the department Client Service Desk:

Telephone (local rate)	0900 – 0660
Telephone from abroad	+31 (0)88 385 6860
Business days	Monday to Friday
Trading hours	08.00 AM - 06.00 PM
E-mail	clientservicedesk-fs-nl@worldline.com

The support will encompass the following:

- Answering questions by telephone and e-mail
- Dealing with incidents
- Processing new password requests
- Monitoring the file exchange and any underlying network connections

Please note:
The support that Client Service Desk will provide is intended for situations involving a standard connection to FTP over TLS. In other instances, Client Service Desk will not provide any support for matters relating to the client's domain.

12.3 Information on the Worldline Financial Services website

On www.financial-service.worldline.com (Contact & Support – User downloads) you will find the following information regarding Secure File Transfer and the various connection types:

- Manuals
- Forms

12.4 Changing connection specifications

You can use the 'Service Request Form FTP over TLS' to do the following:

- Submit a request for:
  - A username and password for the production environment
  - An additional username and password for the production environment
  - A username and password for the test environment
- Register a contact person. In case of an existing FTP over TLS connection the contact person will be replaced by the new contact person
- Change contact details:
  - Organisational information
  - Telephone number and/or e-mail address of the contact person
- Change service specifications:
  - Whether you want to receive compressed files
  - Whether you want to receive output messages
    (e-mail messages stating an output file is ready for retrieval)
  - At which e-mail address you would like to receive error messages
    (i.e. e-mail messages that inform you of a file that could not be processed, for example, because using an incorrect file name has been used)

You must fill in and send a separate copy of the form for each request and/or change! This form can be downloaded from our website: www.financial-service.worldline.com (Contact & Support – User downloads). This Service Request Form only concerns the *transport* of files/data. For the *processing* of data files you are sending/receiving, you will need to make agreements with the appropriate (processing) department of Worldline.

12.5 Changing connection type

If you wish to deliver data using a connection type other than FTP over TLS, please contact the Technical Support department.

12.6 Terminating the connection

The FTP over TLS agreement must be terminated by means of a written request. Please use the Service Request Form to request a termination of the FTP over TLS agreement.
When terminating the connection you must ensure that all streams you use with FTP over TLS are migrated in a timely fashion. This means that the relevant processing agreements must be amended.

12.7 Changing processing agreements

You must arrange changes or termination of your processing agreements with your bank and the Worldline business unit that carries out the processing activities, in accordance with the relevant procedures.

Annex 1 Instructions for WS_FTP client

The information in this annex is based on WS_FTP Pro version 12. These screenshots may differ from more recent versions and are provided for reference only. Worldline does not support nor specify use of any particular FTP-client software.

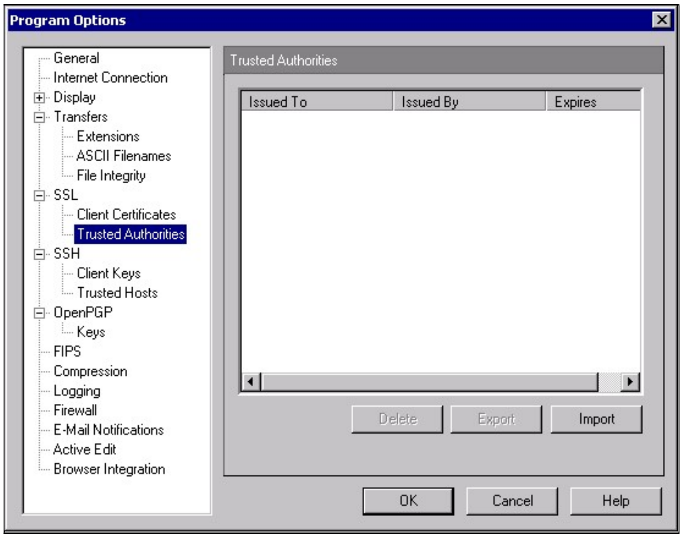
Configuring WS_FTP PRO

Configuring WS_FTP PRO consists of 2 steps:

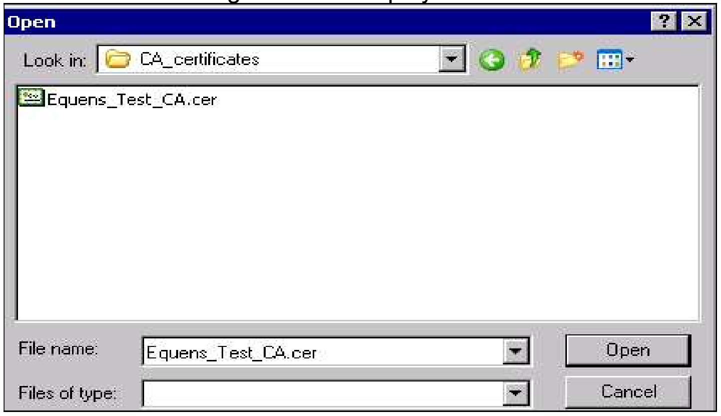
- Importing the certificates
- Creating the connection

1.1 Importing the certificates

- Start WS_FTP PRO via: 'Start, Programs, Ipswitch WS_FTP Pro, WS_FTP Pro', or via the icon on the desktop
- Go to 'Tools, Options' or click the 'Options' icon
- The following screen is displayed



- Click in the left menu 'Trusted Authorities'
- Click 'Import'
- The following screen is displayed



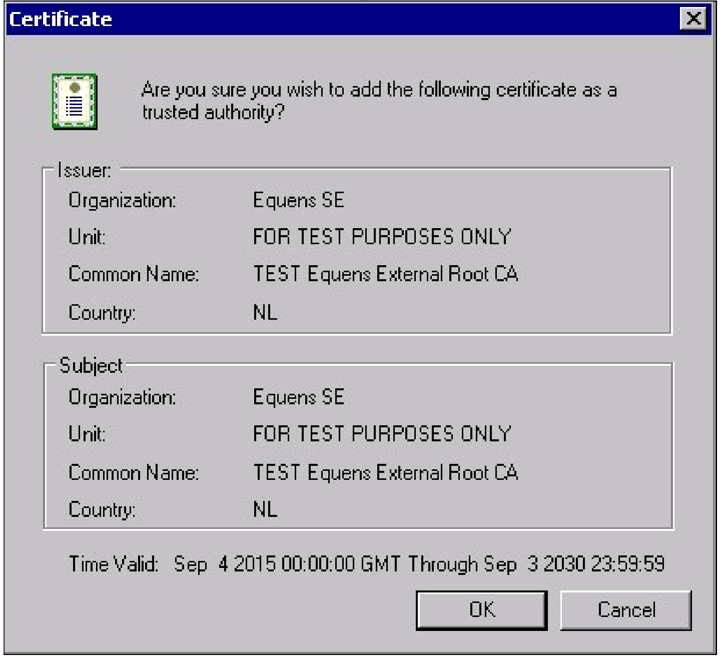
Look in: CA_certificates

Equens_Test_CA.cer

File name: Equens_Test_CA.cer

Files of type:

- Navigate to the directory where the CA root Certificate is located (in this example named 'Equens_Test-CA-Cert.cer')
- Click the certificate
- Click 'Open'
- You will see the message below
- Check if this is the right certificate (Equens External SE test or production)
- Click 'OK'
- The following screen is displayed
- The certificate is now imported



Certificate

Are you sure you wish to add the following certificate as a trusted authority?

Issuer:

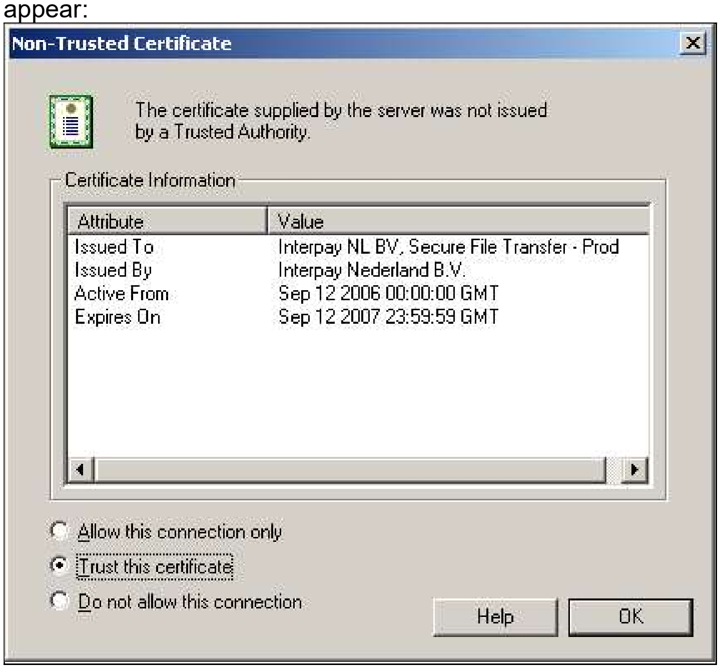
Organization:	Equens SE
Unit:	FOR TEST PURPOSES ONLY
Common Name:	TEST Equens External Root CA
Country:	NL

Subject

Organization:	Equens SE
Unit:	FOR TEST PURPOSES ONLY
Common Name:	TEST Equens External Root CA
Country:	NL

Time Valid: Sep 4 2015 00:00:00 GMT Through Sep 3 2030 23:59:59

When you first set up a connection with the Worldline production environment the following pop-up will appear:



Non-Trusted Certificate

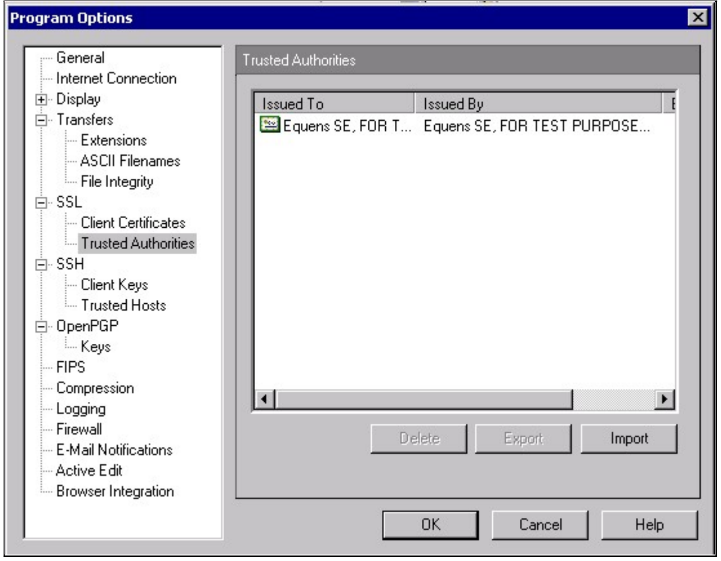
The certificate supplied by the server was not issued by a Trusted Authority.

Certificate Information

Attribute	Value
Issued To	Interpay NL BV, Secure File Transfer - Prod
Issued By	Interpay Nederland B.V.
Active From	Sep 12 2006 00:00:00 GMT
Expires On	Sep 12 2007 23:59:59 GMT

○ Allow this connection only
● Trust this certificate
○ Do not allow this connection

- This message appears because the CA root certificate is not correctly imported.
- If you click 'Trust this certificate' and 'OK', the session will be started and the next time it will be setup without the pop-up. At the current time the certificate needs to be accepted again when a new server certificate is implemented. (This may change when the problem is solved within WS_FTP).

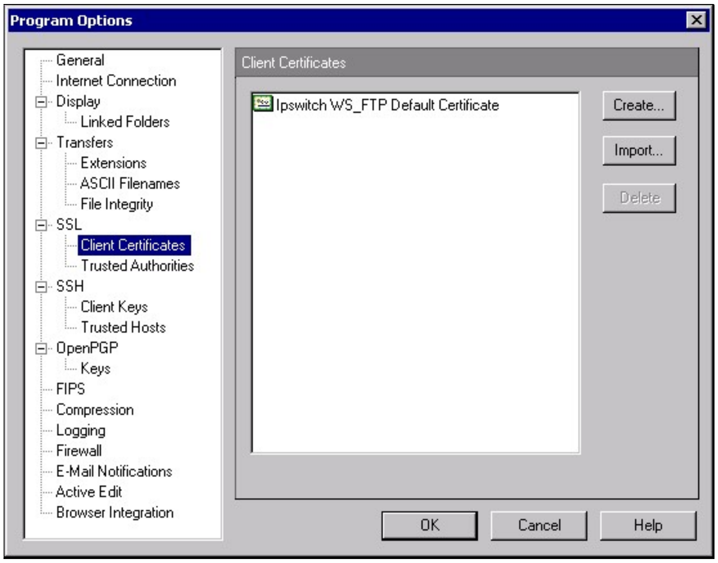


Program Options

Trusted Authorities

Issued To	Issued By
Equens SE, FOR T...	Equens SE, FOR TEST PURPOSE...

- Click in the left menu 'Client Certificates'
- The following screen is displayed
- Click 'Import'

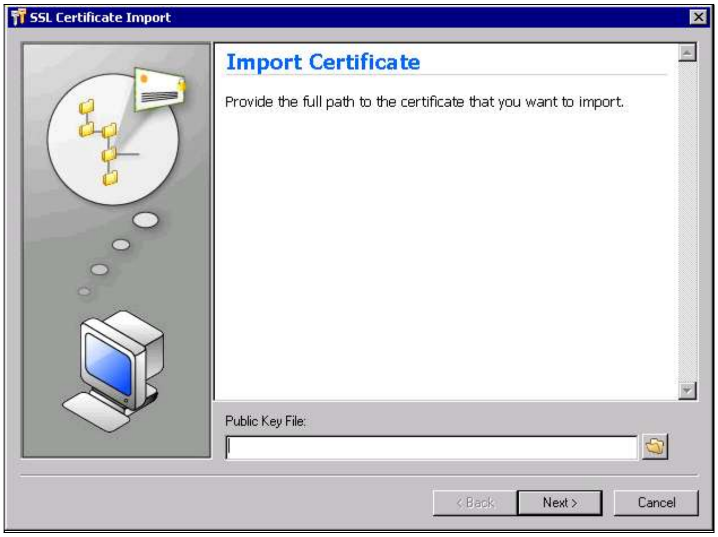


Program Options

Client Certificates

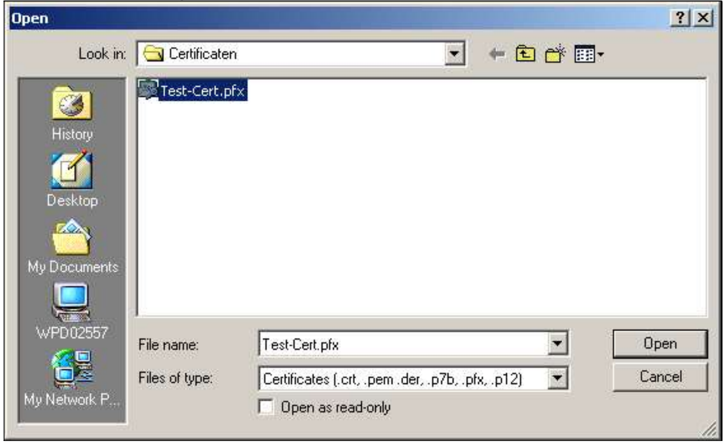
Ipswitch WS_FTP Default Certificate

- The following screen is displayed
- Click the Folder Icon



Go to the directory with the Client Certificate

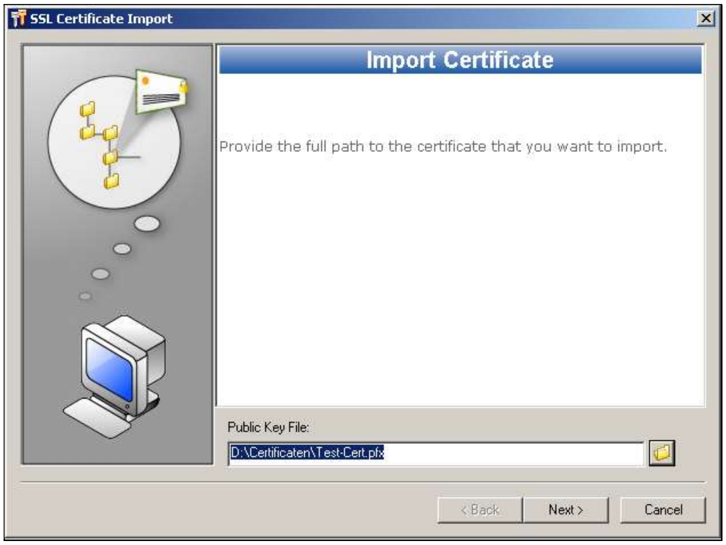
- The following screen is displayed
- Click the Client Certificate (in this example Test-Cert.pfx)
- Click 'Open'



File name: Test-Cert.pfx

Files of type: Certificates (.crt, .pem .der, .p7b, .pfx, .p12)

- The following screen is displayed
- Click 'Next'

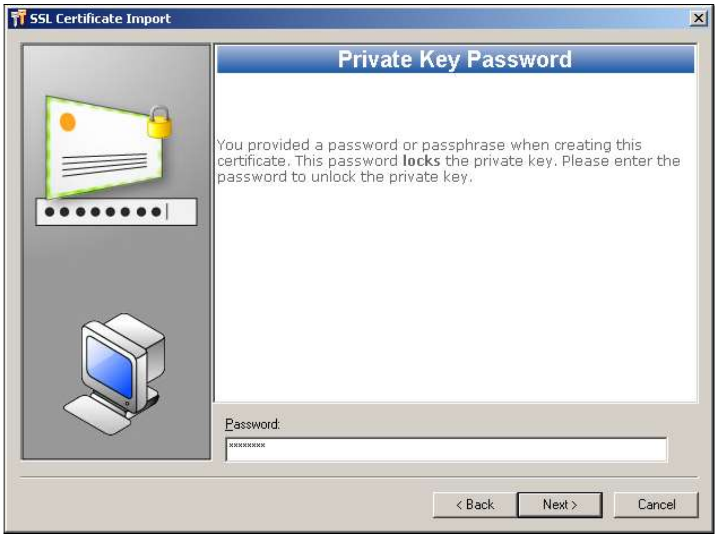


Import Certificate

Provide the full path to the certificate that you want to import.

Public Key File: D:\Certificaten\Test-Cert.pfx

- The following screen is displayed
- Type the password you have entered when you exported the certificate from your browser
- Click 'Next'

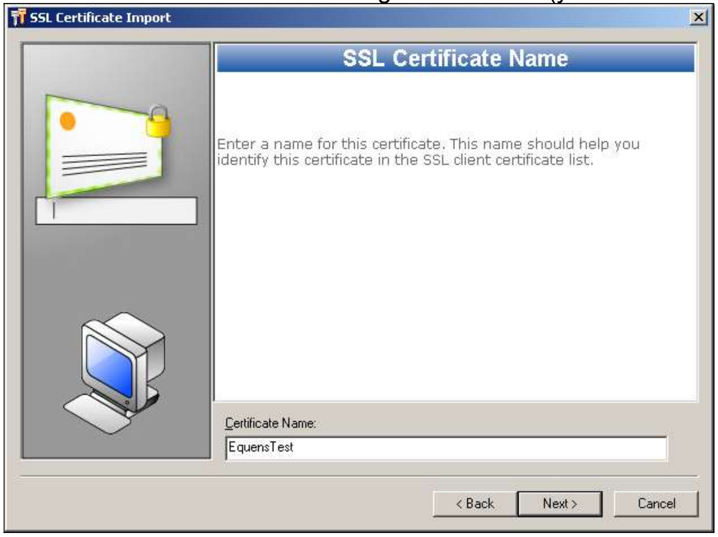


Private Key Password

You provided a password or passphrase when creating this certificate. This password **locks** the private key. Please enter the password to unlock the private key.

Password: ********

- The following screen is displayed
- Give the certificate a recognizable name (you will need this when making a connection).



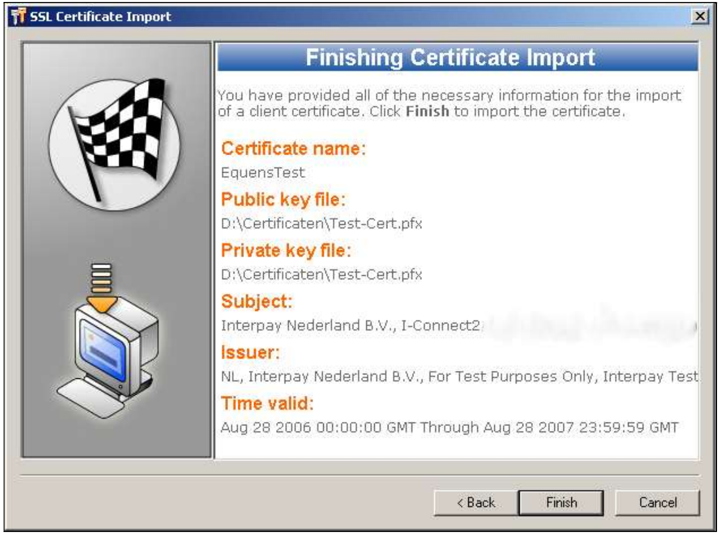
SSL Certificate Import

SSL Certificate Name

Enter a name for this certificate. This name should help you identify this certificate in the SSL client certificate list.

Certificate Name: EquensTest

- The following screen is displayed
- Check the given information
- If correct, click 'Finish'



SSL Certificate Import

Finishing Certificate Import

You have provided all of the necessary information for the import of a client certificate. Click **Finish** to import the certificate.

Certificate name:
EquensTest

Public key file:
D:\Certificaten\Test-Cert.pfx

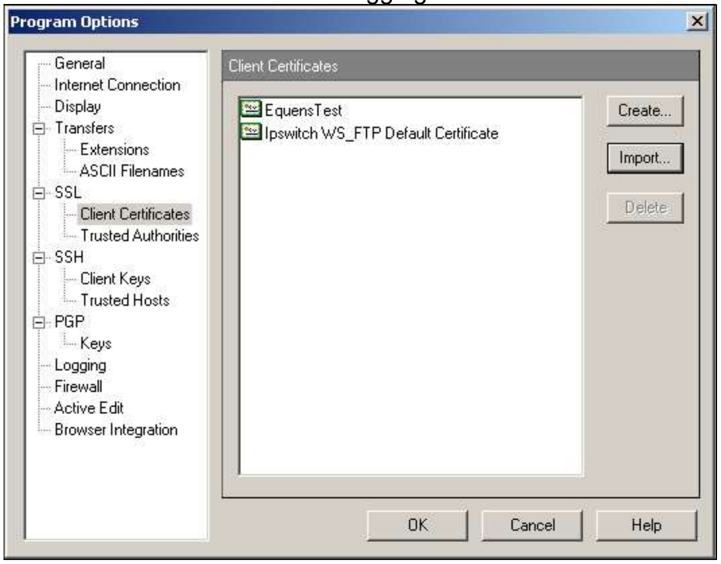
Private key file:
D:\Certificaten\Test-Cert.pfx

Subject:
Interpay Nederland B.V., I-Connect2 [redacted]

Issuer:
NL, Interpay Nederland B.V., For Test Purposes Only, Interpay Test

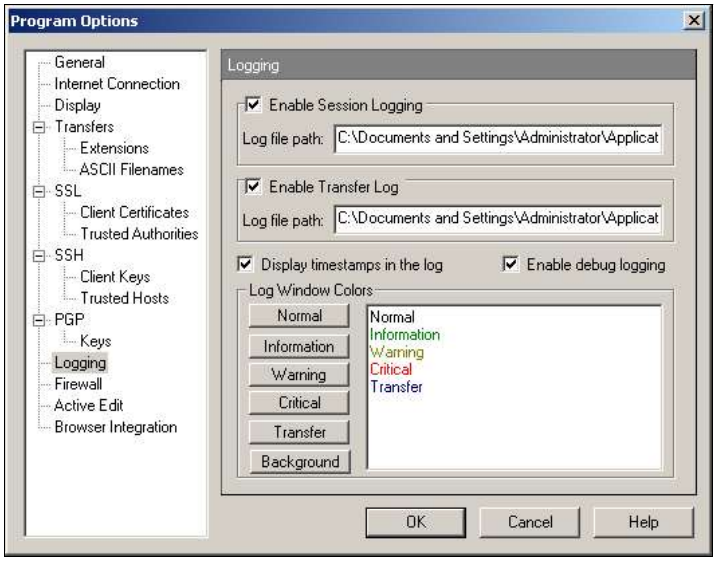
Time valid:
Aug 28 2006 00:00:00 GMT Through Aug 28 2007 23:59:59 GMT

- The following screen is displayed where you see the client certificate is available
- You can optionally set a number of options for logging
- Click in the left menu 'Logging' for this.



EquensTest
Ipswitch WS_FTP Default Certificate

- The following screen is displayed
- If desired tick 'Display timestamps in the log' (highly recommended) and/or 'Enable debug logging' (You can optionally change the location of the log files if desired)
- The options are now set
- Click 'OK'



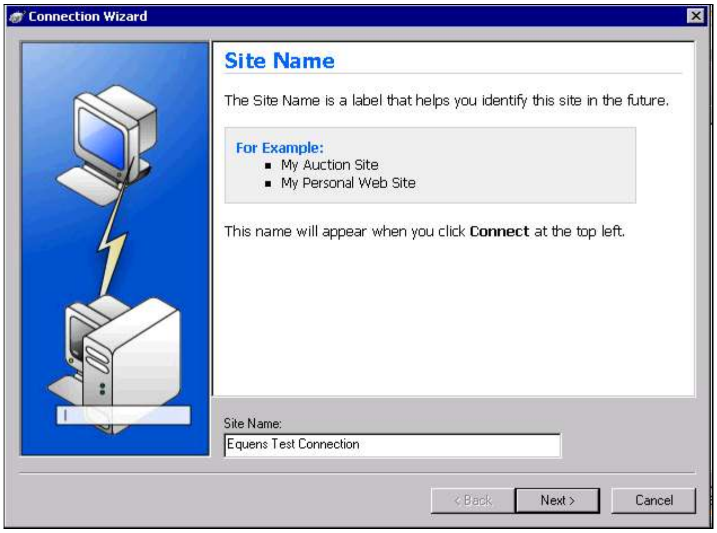
☑ Enable Session Logging
Log file path: C:\Documents and Settings\Administrator\Applicat

☑ Enable Transfer Log
Log file path: C:\Documents and Settings\Administrator\Applicat

☑ Display timestamps in the log ☑ Enable debug logging

1.2 Creating the connection

- Go to the 'Connection Wizard' through one of the following ways:
- 'File', 'Connect', 'Connection Wizard'
- The Connection Wizard button
- The following screen is displayed
- Choose a name for the connection, for example 'SFT Production' of 'SFT Test'
- Click 'Next'



Site Name

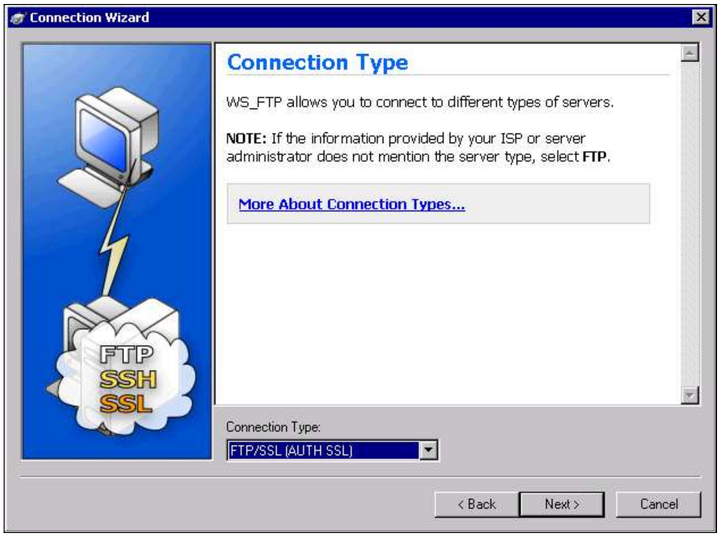
The Site Name is a label that helps you identify this site in the future.

For Example:
- My Auction Site
- My Personal Web Site

This name will appear when you click **Connect** at the top left.

Site Name: Equens Test Connection

- The following screen is displayed:
- Select the option (FTP/TLS (AUTH TLS))
- Click 'Next'



Connection Type

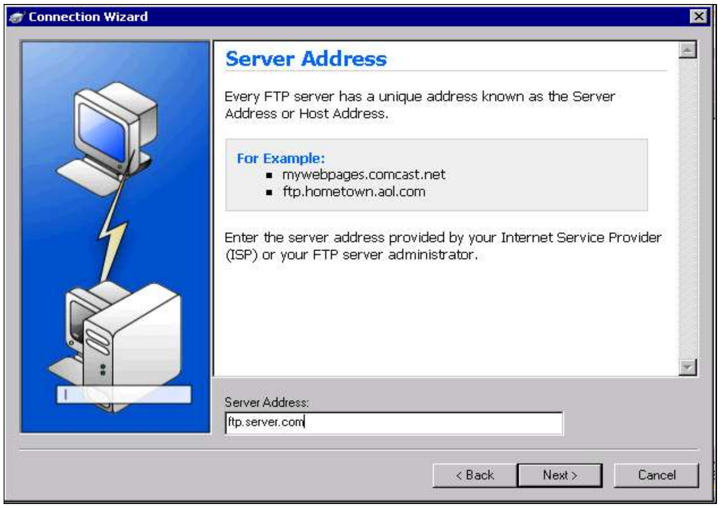
WS_FTP allows you to connect to different types of servers.

NOTE: If the information provided by your ISP or server administrator does not mention the server type, select **FTP**.

More About Connection Types...

Connection Type: FTP/SSL (AUTH SSL)

- The following screen is displayed
- Type the correct server address which is provided during the on-boarding process
- Click 'Next'



Server Address

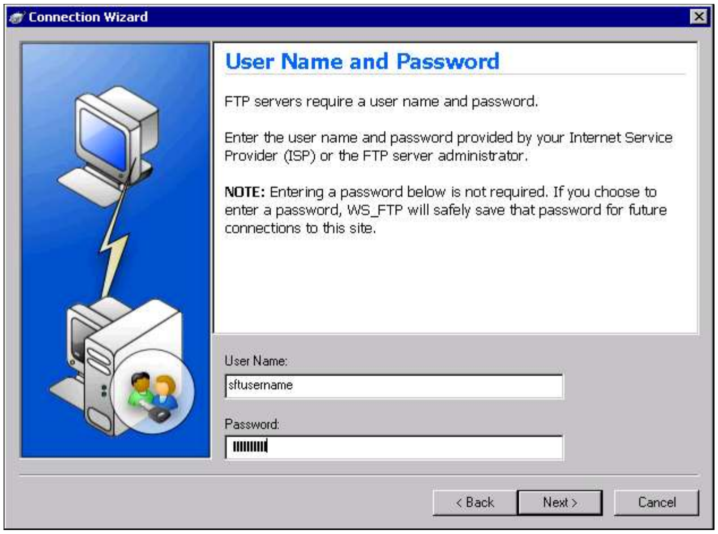
Every FTP server has a unique address known as the Server Address or Host Address.

For Example:
- mywebpages.comcast.net
- ftp.hometown.aol.com

Enter the server address provided by your Internet Service Provider (ISP) or your FTP server administrator.

Server Address: ftp.server.com

- Next you will see the screen below
- Type the username and password that are relevant for this connection
- Click 'Next'



User Name and Password

FTP servers require a user name and password.

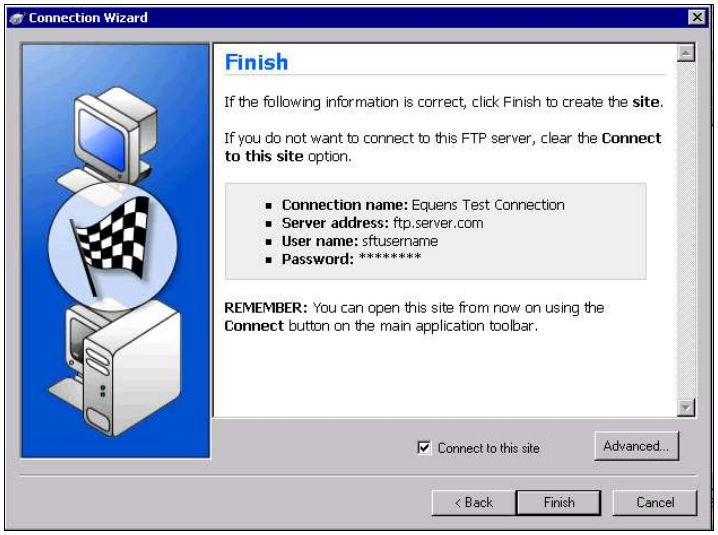
Enter the user name and password provided by your Internet Service Provider (ISP) or the FTP server administrator.

NOTE: Entering a password below is not required. If you choose to enter a password, WS_FTP will safely save that password for future connections to this site.

User Name: sftusername

Password: ||||||||||

- The following screen is displayed
- If desired remove the mark at 'Connect to this site'
- Click 'Advanced'



Connection Wizard

Finish

If the following information is correct, click Finish to create the **site**.

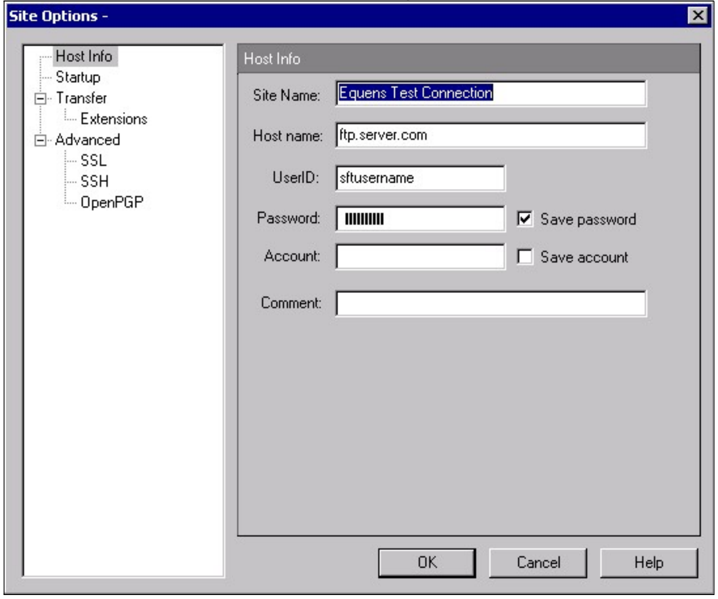
If you do not want to connect to this FTP server, clear the **Connect to this site** option.

- **Connection name:** Equens Test Connection
- **Server address:** ftp.server.com
- **User name:** sftusername
- **Password:** ********

REMEMBER: You can open this site from now on using the **Connect** button on the main application toolbar.

☑ Connect to this site

- The following screen is displayed
- Click in the left menu 'Host info'
- Remove if desired the mark at 'Save password', so the password needs to be entered manually each time a connection is made
- Click in the left menu 'Startup'



Site Options -

Host Info

Site Name: Equens Test Connection

Host name: ftp.server.com

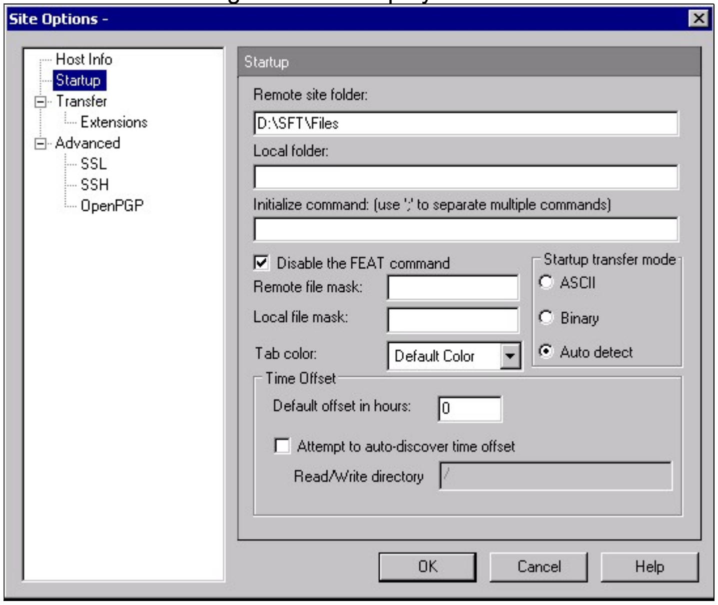
UserID: sftusername

Password: |||||||||| ☑ Save password

Account: ☐ Save account

Comment:

- The following screen is displayed
- Type the folder where the local files are stored
- Tick the 'Disable FEAT command'
- Click in the left menu 'Advanced', option 'SSL'
- The following screen is displayed.



Site Options -

Startup

Remote site folder: D:\SFT\Files

Local folder:

Initialize command: (use ';' to separate multiple commands)

☑ Disable the FEAT command

Remote file mask:

Local file mask:

Tab color: Default Color

Startup transfer mode

○ ASCII

○ Binary

● Auto detect

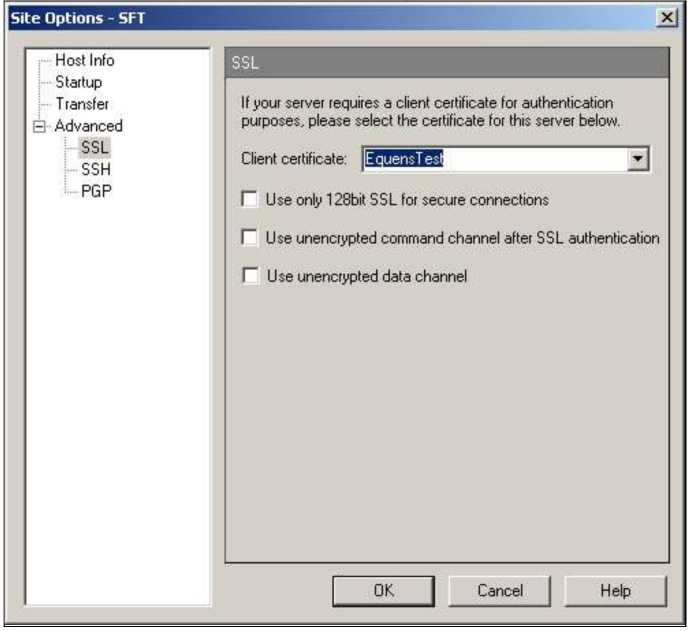
Time Offset

Default offset in hours: 0

☐ Attempt to auto-discover time offset

Read/Write directory /

- Select in 'Client certificate' the appropriate certificate for this connection (Possibly you have imported both the production- and the test certificate)
- Click 'OK'
- The connection is now set up



Site Options - SFT

SSL

If your server requires a client certificate for authentication purposes, please select the certificate for this server below.

Client certificate: EquensTest

☐ Use only 128bit SSL for secure connections

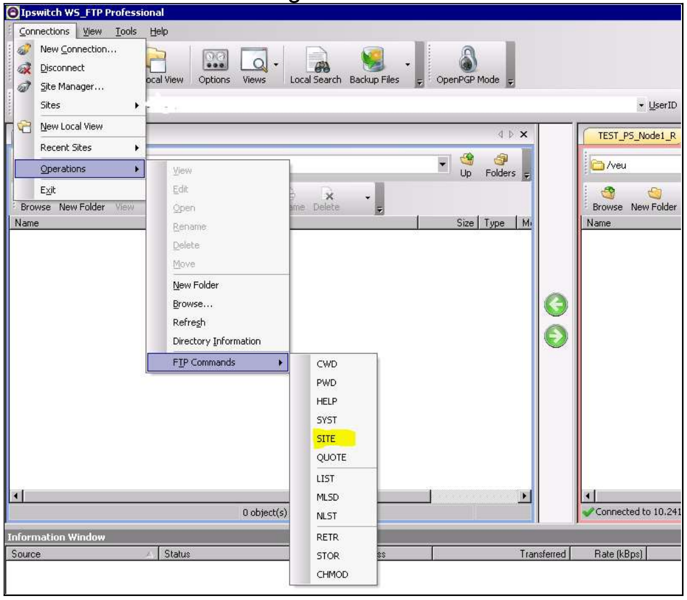
☐ Use unencrypted command channel after SSL authentication

☐ Use unencrypted data channel

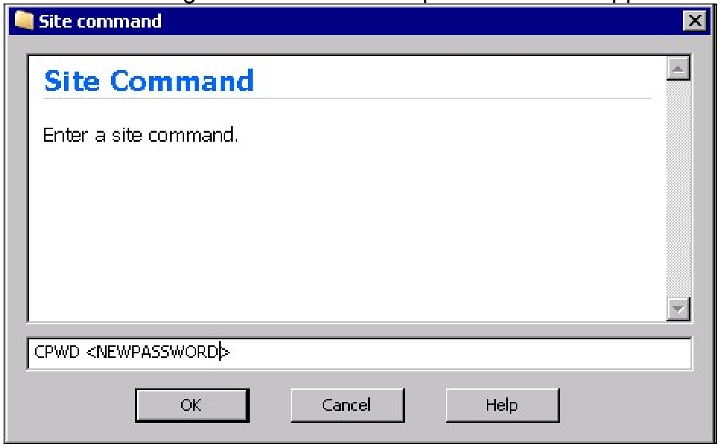
1.3 Changing the password

Please note:
Before changing the password a successful connection must be made.

- Choose in the menu the option 'File', 'Operations', 'FTP Commands', 'SITE', as shown in the figure below



- The screen 'Site command' appears
- Type the characters 'CPWD', a space and a new password, as shown in the figure below
- Click 'OK'
- In the log 'SITE CPWD <new password>' will appear



Site Command

Enter a site command.

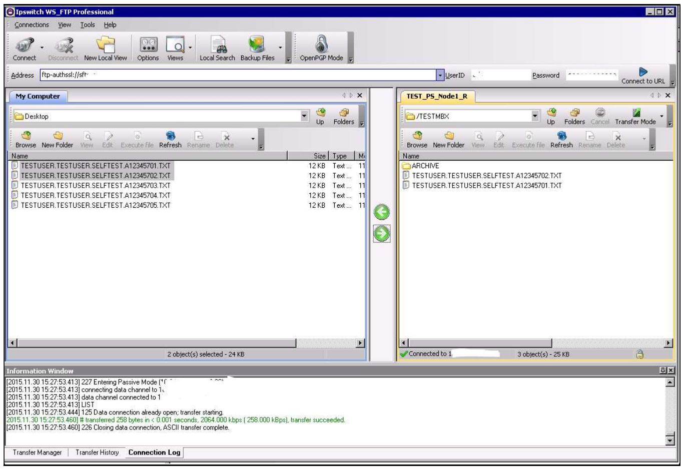
CPWD <NEWPASSWORD>

The message:
'200 CPWD successful' appears in the Connection Log if the password change is successful. Adjust the password in the connection configuration if you saved the password in WS_FTP.

1.4 Sending and receiving files

Below you see the main screen of WS_FTP with:

- Top left the local files
- Top right your mailbox with the files at Worldline
- Below the information window with the tabs:
  - Transfer Manager
  - Transfer History
  - Connection Log



Address: ftp-authssl://sft

UserID

Password

Desktop

Name	Size	Type	M
TESTUSER.TESTUSER.SELFTEST.A12345701.TXT	12 KB	Text ...	11
TESTUSER.TESTUSER.SELFTEST.A12345702.TXT	12 KB	Text ...	11
TESTUSER.TESTUSER.SELFTEST.A12345703.TXT	12 KB	Text ...	11
TESTUSER.TESTUSER.SELFTEST.A12345704.TXT	12 KB	Text ...	11
TESTUSER.TESTUSER.SELFTEST.A12345705.TXT	12 KB	Text ...	11

2 object(s) selected - 24 KB

/TESTMBX

Name
ARCHIVE
TESTUSER.TESTUSER.SELFTEST.A12345702.TXT
TESTUSER.TESTUSER.SELFTEST.A12345701.TXT

Connected to 1

3 object(s) - 25 KB

```
[2015.11.30 15:27:53.413] 227 Entering Passive Mode (1
[2015.11.30 15:27:53.413] connecting data channel to 1
[2015.11.30 15:27:53.413] data channel connected to 1
[2015.11.30 15:27:53.413] LIST
[2015.11.30 15:27:53.444] 125 Data connection already open; transfer starting.
2015.11.30 15:27:53.460] # transferred 258 bytes in < 0.001 seconds, 2064.000 kbps ( 258.000 kBps), transfer succeeded.
[2015.11.30 15:27:53.460] 226 Closing data connection, ASCII transfer complete.
```

For the different ways of sending and receiving files, please consult the WS_FTP documentation. One way is to click the file and then click the green 'upload' or 'download' arrows.

1.5 Summary error situations

Please check if your (error) message appears in the list with known error situations given below.

Error categories

The majority of the errors are in the following categories:

Connection problem or DNS problem

If the connection runs through the internet, the access to internet can easily be checked with the internet browser or with command line tools.

TCP/IP ports not open for outgoing connections

Please check the settings of the firewall

Configuration errors FTP-client

Please check the settings of the FTP-client

Known error situations

A number of known error situations are recognizable by the messages in the WS_FTP logs:

Connection problem or DNS problem

Finding Host ftp.server.com…

After this no message: *220 FTP Server ready for new user*

TCP/IP ports not accessible

Connecting to ‚IP-address>:<port>…
After this no message: *220 FTP Server ready for new user*
Port for Command connection not accessible

Port failed 451 Requested action aborted: session in inconsistent state
Port for Data connection not accessible. This message appears because the client tries to switch to Active FTP mode and that is not accepted by our server.

Server problems

SSL Connect error 2 (after 66 seconds)
Server Timeout – No server (CA) certificate received. Most probably your firewall blocks the TLS connection

Configuration errors client

503 Bad sequence of commands
No TLS given with server type. The server expects the AUTH TLS command before the USER command to start up the needed TLS-connection. TLS is indicated, but no client certificate given.

SSL Connect error 2 (after 1 second)
A wrong client certificate is given (i.e. TEST instead of PRODUCTION) or your firewall blocks the TLS connection.

SSL Connect error 1
425 Can't open data connection
No Passive given in the configuration. The client starts in Active mode and sends the PORT command. The server reports that the data connection from the server cannot be setup. The client tries automatically the Passive mode and the data connection will be finally setup.

530 Login incorrect
The TLS session is OK, but an incorrect user/password is used.
Characteristics of WS_FTP
200 PORT command successful
425 Can't open data connection
WS_FTP switches from Passive to Active mode. This is unwanted behaviour that cannot be prevented with the configuration options. The client also switches back to Passive mode.