



SFT User Manual C:D

Secure File Transfer with Connect:Direct

Document date:	15 November 2016
Classification:	Open
Version:	4.0

Copyright © equensWorldline SE and/or its subsidiaries. All rights reserved.

equensWorldline is an expert leader in e-payment services and a registered trademark of Worldline. Confidential information owned by equensWorldline, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from equensWorldline. After approval, any copy or reproduction will include the following: acknowledgement of the source, reference and date of the publication, and all notices set out on this page.

Contents

1	Introduction	5
1.1	Maintenance of this document.....	5
1.2	Target groups	5
1.3	Test versus Production environment	5
1.4	Structure of this manual.....	5
2	Connect:Direct network variants and infrastructure	6
2.1	Two network variants	6
2.2	Connect:Direct via internet.....	6
2.3	Connect:Direct via E-Line	6
3	Security	7
3.1	Encrypted file transmission via TLS.....	7
3.2	Authentication by means of certificates	8
3.3	Client certificate	8
4	File naming convention and routing mechanism	9
4.1	Connect:Direct file name convention.....	9
4.2	Receipt of different file types	10
4.3	Multiple destination id's (optional)	10
4.4	Customized Naming Convention	10
5	Fall-back and backup facilities	11
6	Configuration of your network	12
6.1	Configuration of your firewall.....	12
6.2	Configuration of the Connect:Direct node in your environment.....	12
6.3	Certificates	12
7	Testing your connection	13
7.1	Difference between the three test types	13
7.2	Connection test.....	14
7.3	File transfer test.....	14
8	File sending	16
8.1	Automatic file sending.....	16
8.2	Binary file sending.....	16
9	File delivery.....	17
10	Using compressed files	18
10.1	Sending and receiving compressed files	18

10.2	Receiving compressed files	19
11	Support processes: questions and changes	20
11.1	Connect:Direct availability	20
11.2	Contact information department Customer Services.....	20
11.3	Information on the equensWorldline website.....	20
11.4	Changing connection specifications	21
11.5	Changing connection type	21
11.6	Terminating the connection	21
11.7	Changing and terminating processing agreements.....	21

1 Introduction

This manual provides information regarding equensWorldline Secure File Transfer services, in particular the Connect:Direct connection type.

1.1 Maintenance of this document

This document is managed and maintained by equensWorldline 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 Customer Services of equensWorldline (for contact details, see chapter 11, 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 programmers who are involved in the implementation and use of the Connect:Direct connection.

1.3 Test versus Production environment

equensWorldline 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 Connect:Direct
- How to make a connection
- Recurring procedures

The first section describes how equensWorldline has configured the connection with Connect:Direct 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 the backup and fall-back is set up.

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

- The technical aspects of the connection (organisation of your network)
- Testing your connection.

The third section explains in detail the activities that recur. This section comprises chapters 9 to 11, which contain the following information:

- How to send files
- How files are delivered
- How to handle compressed files
- How to submit questions and/or changes

2 Connect:Direct network variants and infrastructure

2.1 Two network variants

Two network variants can be used for Connect:Direct

- Connect:Direct via internet
- Connect:Direct via a private E-Line.

With a connection via the internet there is no guaranteed availability and bandwidth by equensWorldline, 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 Connect:Direct via internet

This network variant is the preferred choice of both equensWorldline 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 equensWorldline strongly recommends using firewalls.

2.3 Connect:Direct via E-Line

For banks and large corporations, equensWorldline 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 equensWorldline.

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 department Customer Services 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.

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
- Use of a Secure Point of Entry (SPOE)

Confidentiality

Confidentiality regarding public and internal connections will be guaranteed through the use of Connect:Direct with Secure+ (TLS plus encryption).

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:

- Check (netmap) on both IP-address and node name
- Check on Common Name in the client certificate
- Contract conclusion checks (processing contracts)

3.1 Encrypted file transmission via TLS

Connect:Direct with Secure+ provides security by authentication and encryption to exchange files that contain confidential information. In use, Connect:Direct with Secure+ will be very similar to standard Connect:Direct, but one important difference is the fact that all confidential information will be encrypted via TLS and a strong cipher suite as AES. The nodes will automatically carry this out for you.

By default the following strong cipher suites are acceptable by equensWorldline unless agreed otherwise:

- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA256
- RSA_WITH_AES_256_CBC_SHA256

3.2 Authentication by means of certificates

An important aspect of the Connect:Direct infrastructure is the use of digital certificates. The Connect:Direct nodes are equipped with certificates for the purpose of authentication. This authentication is based on the nodes only accepting one another's certificates when they have been signed by the correct (equensWorldline) Certificate Authority.

A Public Key Infrastructure (PKI) service will be used to issue certificates. equensWorldline 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.

equensWorldline will have full control over issuing of certificates and will determine which certificate applications will be accepted or rejected via a RA function. equensWorldline 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 equensWorldline Certificate Policy, downloadable from our website: www.equensWorldline.com (Support - Manuals).

In case your security policy does not allow the usage of the equensWorldline PKI certificates, please contact the department Customer Services of equensWorldline.

3.3 Client certificate

The client certificate of the customer will be checked by equensWorldline using client authentication. The Common Name in the client certificate is checked against the Common Name registered at the equensWorldline PKI (as given by customer during the certificate request procedure).

You will find more information on how to obtain an equensWorldline certificate in a separate document: "Obtain a certificate for Secure File Transfer".

4 File naming convention and routing mechanism

When you wish to exchange files with equensWorldline via Connect:Direct, the file names must comply with a specific naming convention.

Files sent in will be routed to the appropriate equensWorldline processing system on the basis of the file name. equensWorldline will not be able to route sent files if their name does not comply with 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 Connect:Direct file name convention

The following standard will apply within Connect:Direct with regard to the structure of file names:

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

The separate fields are defined as follows:

Explanation of file name components

Field	Format	Length	Description
<prefix>	lowercase	8	Must be /mailbox/ This part will be stripped from the filename after it is received.
<SENDER>	UPPERCASE, alpha-numeric	1-8	The ID (router address) of the submitting party. This will be assigned by equensWorldline 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 equensWorldline
<TYPE>	UPPERCASE, alpha-numeric	1-8	The ID of the file type being exchanged. The file type determines the type of processing by equensWorldline. The file types to be used will be assigned by equensWorldline.
<REFERENCE>	UPPERCASE, alpha-numeric	1-8	A unique alpha-numeric file reference ID assigned by the submitting party. The field must start with a letter and 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
- The maximum field length is eight characters

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

/mailbox/R0001234.SFT.PACS008.C1234567.XML

4.2 Receipt of different file types

A customer will be able to receive numerous file types via Connect:Direct. 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>.

4.3 Multiple destination id's (optional)

equensWorldline 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 Customer Services of equensWorldline for more information.

4.4 Customized Naming Convention

However we prefer the standard naming convention, on request we can deviate from the standard and agree on a custom specific naming convention. Please contact the department Customer Services of equensWorldline for additional information if you are unable to comply to the standard naming convention.

5 Fall-back and backup facilities

equensWorldline 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 Connect:Direct connection with the primary location.

In the event of a network failure in the primary location, the system will automatically use the network infrastructure in the secondary location. With the exception of a brief hiccup, the client 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 Connect:Direct traffic for the different network variants is routed to the secondary location. During these procedures it will not be possible to connect to equensWorldline. 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 Connect:Direct at network level. Once the connection has been made it will be possible to work with Connect:Direct at transportation level.

Two network variants can be used for Connect:Direct:

- Connect:Direct via internet
- Connect:Direct via E-Line

The specifications for these network variants are described in chapter 2 'equensWorldline Connect:Direct Network variants and infrastructure'.

6.1 Configuration of your firewall

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

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

6.2 Configuration of the Connect:Direct node in your environment

Node name/IP address

For configuring your Connect:Direct node you will need to add the IP-address and the node name of the equensWorldline Connect:Direct node in your configuration.

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

Secure+

When using Connect:Direct you will exchange files that may contain confidential information via Connect:Direct with Secure+. In use, Connect:Direct with Secure+ will be very similar to standard Connect:Direct, but one important difference is the fact that all confidential information will be encrypted via TLS and a strong cipher suite such as AES. The nodes will automatically carry this out for you.

By default the following strong cipher suites are acceptable by equensWorldline unless agreed otherwise:

- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA256
- RSA_WITH_AES_256_CBC_SHA256

6.3 Certificates

You need to install the CA certificate for the equensWorldline PKI and your certificate into the Connect:Direct configuration. The Common Name for your certificate is checked against the Common Name registered at equensWorldline Connect:Direct host.

Note: when Key Usage extensions attributes are used, Connect:Direct demands both serverAuth and clientAuth attributes.

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 equensWorldline 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 Customer Services of equensWorldline and the relevant business unit.

7.1 Difference between the three test types

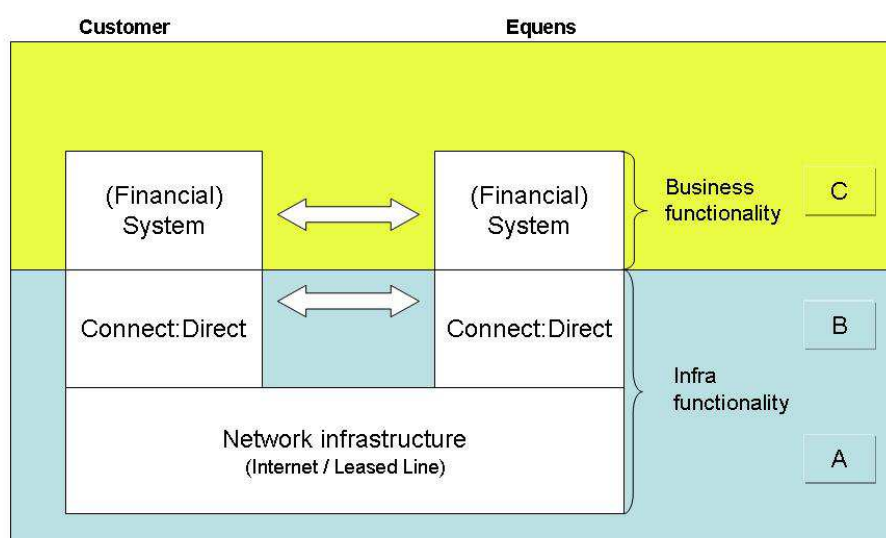
Tests can be carried out at three levels:

- 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 Connect:Direct 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 equensWorldline databases
- You must have installed a Connect:Direct node
- You must have installed both the client and CA root certificates

7.2 Connection test

Connection test features and conditions

Features of the Connect:Direct connection test	
Feature	Description
Subject	This involves aspects such as: <ul style="list-style-type: none"> Setting up a connection with Connect:Direct and Secure+
Objective	Checking whether the Connect:Direct specifications have been properly implemented at the customers' side.
Conditions	You do not need to contact equensWorldline in order to carry out this test.
Importance	Recommended
Environment	Production or test/acceptance environment

Connection test execution

You can use your Connect:Direct in the production or test/acceptance environment to test whether a connection can be established. Please refer to the documentation of your Connect:Direct node for setting up a connection.

7.3 File transfer test

File transfer test features and conditions

Connect:Direct file transfer test features	
Feature	Description
Subject	Routing to and from yourself.
Objective	Checking whether file transfers between equensWorldline and the customer via Connect:Direct are successful.
Conditions	You do not need to contact equensWorldline 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.

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 Connect:Direct:

/mailbox/R0001234.R0001234.SELFTEST.TEST1234.TXT

Please refer to section 4.2 'Connect:Direct file name convention' for the file name structure.

- Set up a connection to the Connect:Direct node of equensWorldline
- Send the file to yourself
See section 9, 'File sending'
The file will be fully processed at equensWorldline. This means the file will be routed to the <DESTINATION>, in this case yourself. The file will be pushed to your Connect:Direct node.
- Check if the file is delivered at your Connect:Direct node.

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

8 File sending

You can send files to equensWorldline using commands in your Connect:Direct node. When sending files you will need to initiate the transfer.

You can also send compressed (zipped) data files. Please refer to chapter 11 'Using compressed files' for additional information.

Please note:

The maximum file size for Connect:Direct is 2 GB (uncompressed).

8.1 Automatic file sending

Most Connect:Direct nodes have the possibility to send files automatically. The node can be configured so that it will check a directory on the local system for waiting files. If this is the case, the files will be sent to equensWorldline without any further action being required from the user. If the files are sent successfully the node can remove the files.

You can use a 'File agent' for this, but you are responsible for further automation, equensWorldline does not provide support for this.

8.2 Binary file sending

Some file types, such as files with the extension .ZIP, .DAT, .PDF or .BIN must be sent in binary mode.

For more information on sending files binary with Connect:Direct, please consult the Connect:Direct documentation of Sterling Commerce.

If you send a binary file as a non-binary file, it may arrive corrupted at the destination.

9 File delivery

Files addressed to you are 'pushed' to you by Connect:Direct, you do not need to take the initiative to retrieve the files. The output files will be put on your Connect:Direct node, if the files need to be placed in a specific directory on your node, please indicate this on the Service Request Form when requesting the Connect:Direct connection.

Previously pushed files can be resend for a limited period of time. Please contact the department Customer Services of equensWorldline if you want to receive a file that already has been supplied.

10 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 send and receive compressed files, please see section 9.3, "Binary file sending".

10.1 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 equensWorldline before it is routed to the <DESTINATION> and can be zipped again by equensWorldline, 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.

10.2 Receiving compressed files

Conditions

If you wish to receive compressed output from equensWorldline, 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 equensWorldline 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 file name convention.

For example: the archive MFC.R0001234.VERWINFA.A1234567.ZIP would contain the file MFC.R0001234.VERWINFA.A1234567.TXT

11 Support processes: questions and changes

11.1 Connect:Direct availability

Secure File Transfer will be available 24/7.

Maintenance will be scheduled between Saturday 7:00a.m. and Sunday 4:00p.m.

11.2 Contact information department Customer Services

Support for File Transfer products will be provided by the department Customer Services of equensWorldline.

The support will encompass the following:

- Answering questions by telephone
- Dealing with incidents
- Monitoring the file exchange and any underlying network connections

Please note:

The support that Customer Services will provide is intended for situations involving a standard connection to Connect:Direct.

In other instances, Customer Services will not provide any support for matters relating to the client's domain.

Customer Services is available from Monday to Friday, with the exception of bank holidays.

- Opening hours: 8:00 am – 6:00 pm
- Telephone: 0900-0660 (for customers in The Netherlands, local rate)
- Telephone: +31 (0)88 38 56860 (for customers outside The Netherlands)
- E-mail: supportdesk-ew@equensworldline.com

Please note:

Please submit any questions by telephone, not by e-mail (unless otherwise instructed).

11.3 Information on the equensWorldline website

On www.equensWorldline.com you will find the following information regarding Secure File Transfer and the various connection types:

- Brochures
- Manuals
- Forms

11.4 Changing connection specifications

You can use the 'Service Request Form Connect:Direct' for:

Register and deregister

- The 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 connect via the internet or via a Leased Line
- Whether you want to receive compressed files

At which e-mail address you would like to receive error messages

E-mail messages that inform you of a file that could not be processed, for example, because 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.equensWorldline.com (Support - Forms)

This Service Request Form only concerns the *transport* of files/data. For the *processing* of the data files you are sending/receiving, you will need to make agreements with the appropriate (processing) department of equensWorldline.

11.5 Changing connection type

If you wish to deliver data using a connection type other than Connect:Direct, please contact the department Customer Services.

11.6 Terminating the connection

The Connect:Direct agreement must be terminated by means of a written request. Please use the Service Request Form to request a termination of the Connect:Direct agreement.

When terminating the connection you must ensure that all streams you use with Connect:Direct are migrated in a timely fashion. This means that the relevant processing agreements must be amended.

11.7 Changing and terminating processing agreements

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