How to setup Secure FTP with VSE

VSE as server and as client

Last formatted on: Thursday, August 06, 2009

Joerg Schmidbauer
jschmidb@de.ibm.com

Dept. 3229
VSE Development
IBM Lab Böblingen
Schönaicherstr. 220

D-71032 Böblingen
Germany

Disclaimer

This publication is intended to help VSE system programmers setting up infrastructure for their operating environment. The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk. Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment. Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of other companies:

Contents

Changes

Aug 17, 2007 – more details on PORTRANGE parameter on page 28.
Sep 21, 2007 - added disclaimer and some more details about DATAPORT and PORTRANGE on pages 25 and 26
Nov 05, 2007 – added note about interactive FTP client on page 27.
Nov 28, 2008 – added info about how to create the server key and certificate with OpenSSL (see page 20)
Dec 2008 – added info about problem of z/VM FTP client with FTPD UNIX-mode (see notes on page 12)
Jan 2009 – added info about TCP/IP fix ZP15F264 on page 4.
Aug 2009 – corrected link to Filezilla server

1 Introduction

This paper describes the setup of secure FTP in various scenarios with VSE acting as server or as client. This involves the creation of RSA key pairs and digital certificates on the different server sides. For simplification, we do not purchase certificates from official Certificate Authorities (CAs), but create our own set of so called self signed certificates. Self-signed certificates are not signed by an official CA and therefore work only in a closed test environment.

The following software has been used in the test setup.

- z/VSE 4.1.0 GA version
- TCP/IP for VSE/ESA 1.5E as part of z/VSE 4.1 GA version
- VSE Connector Server as part of z/VSE 4.1.0 (job STARTVCS)
- Java 1.4.2 from Sun Microsystems
- Keyman/VSE, update from 03/2007
- FileZilla server version 0.9.23 beta
- FileZilla client version 2.2.30
- Symantec Client Firewall Version 8.7.4.97
- OpenSSL Light 0.98

Note: when using TCP/IP for VSE/ESA **1.5F**, the following fixes are necessary for secure FTP:

- 204, 206, 244, 247, 251, 252, 253
- 264 if you are using FileZilla client and **TLS 1.0** for connecting to VSE.

2 VSE as Server

Setting up Secure FTP with VSE as the server is pretty much the same as setting up SSL for use with the VSE Connector Server or CICS Web Support. This is described in detail in the z/VSE e-business Connectors User's Guide that you can download from

http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#conn

In the following sections we describe how secure FTP is set up using VSE as the server side.

2.1 Generate the server key and certificates

The easiest way to generate all necessary keys and certificates for the VSE server side is by using the Keyman/VSE utility which is provided by IBM without warranty for free download from

http://www.ibm.com/servers/eserver/zseries/zvse/downloads/

Keyman/VSE is a Java application, which is typically installed on a Personal Computer. It has the following prerequisites.

- Java 1.4 or higher on the workstation side
- TCP/IP for VSE/ESA 1.5E on the VSE side

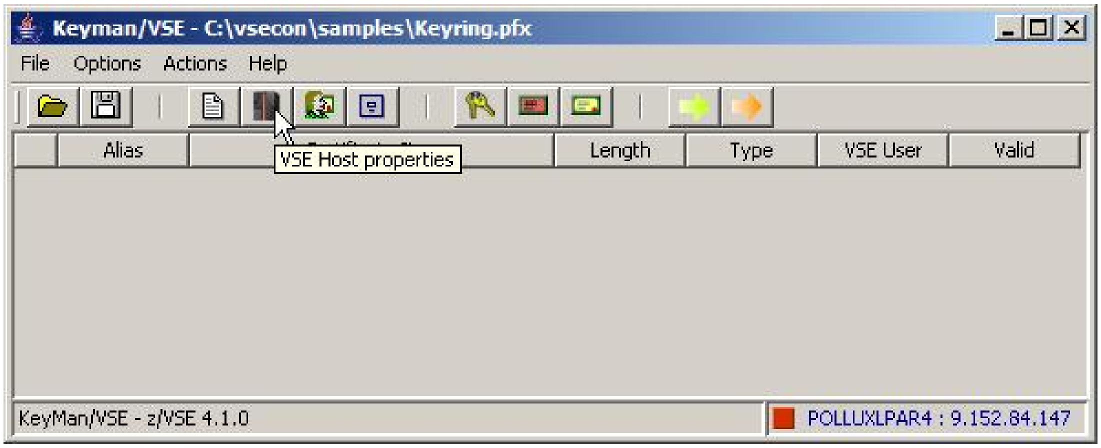
- VSE Connector Server up and running in non-SSL mode on the VSE side

Although Keyman/VSE provides many functions for manually creating keys and certificates, sign certificate requests, and so on, the easiest way for creating the necessary files on VSE is using the Wizard dialog for creating a self-signed keyring. For details about Keyman/VSE functions refer to the HTML-based help of the Keyman tool.

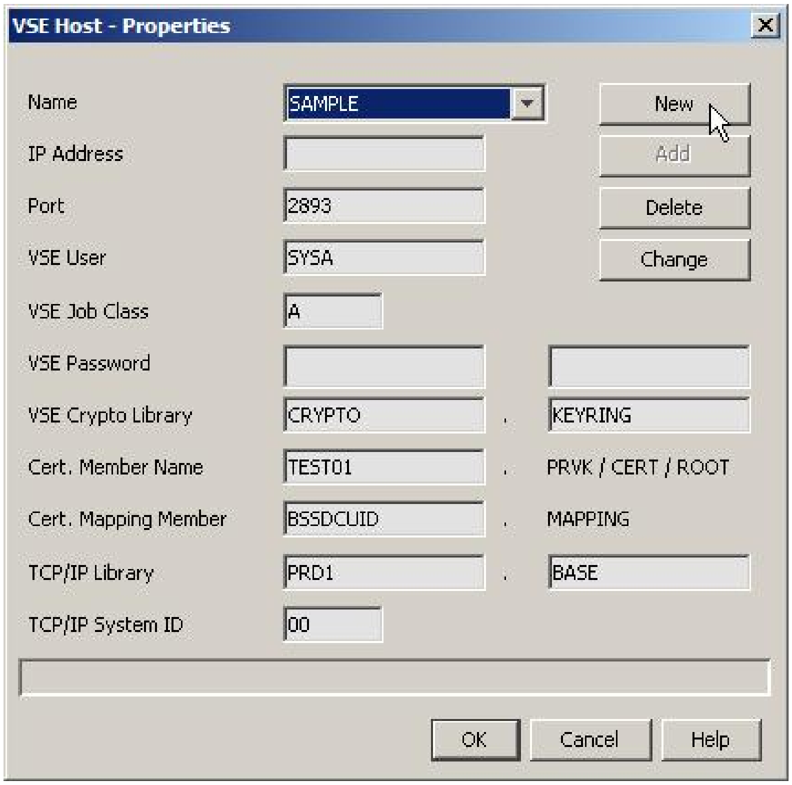
Our first step is to start Keyman/VSE and entering the properties of your VSE system. This information is needed later for sending created keys and certificates to VSE.

2.1.1 Define the properties of your VSE system

On the main window click on the **VSE host properties** toolbar button.



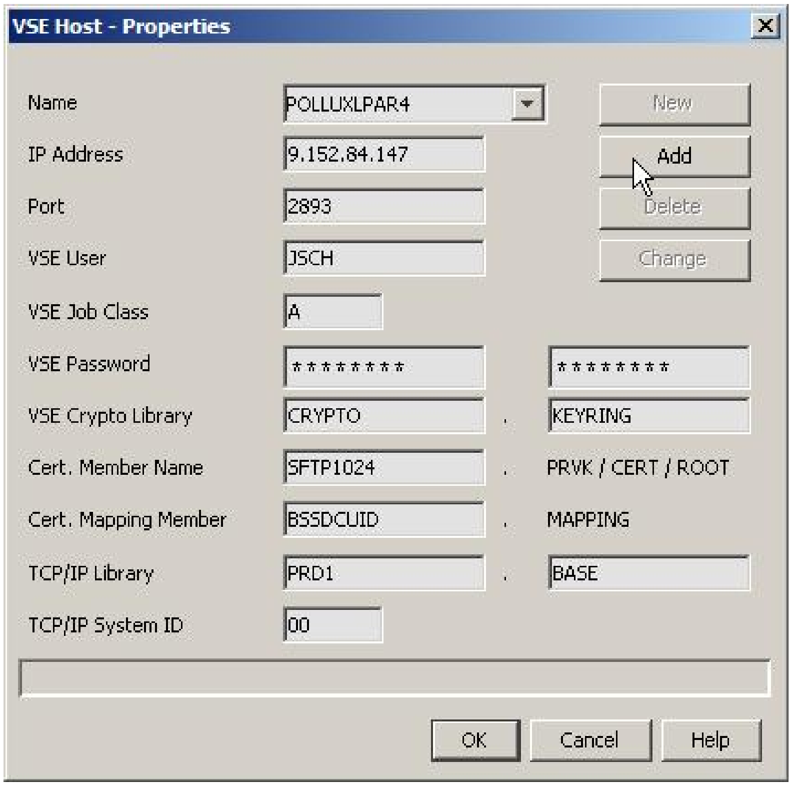
On the **VSE Host – Properties** dialog box enter the required information for your VSE system. Press the **New** button to create a new VSE host definition.



VSE Host - Properties

Name: SAMPLE
IP Address:
Port: 2893
VSE User: SYSA
VSE Job Class: A
VSE Password:
VSE Crypto Library: CRYPTO . KEYRING
Cert. Member Name: TEST01 . PRVK / CERT / ROOT
Cert. Mapping Member: BSSDCUID . MAPPING
TCP/IP Library: PRD1 . BASE
TCP/IP System ID: 00

Then enter a unique name for your VSE system, its IP address, the port number of the VSE Connector Server, a VSE user ID together with its password and so on.



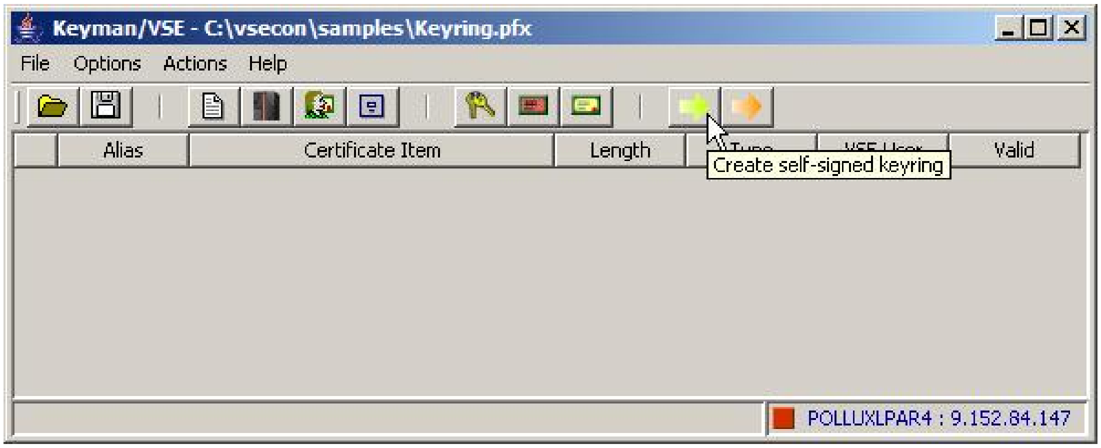
VSE Host - Properties

Name: POLLUXLPAR4
IP Address: 9.152.84.147
Port: 2893
VSE User: JSCH
VSE Job Class: A
VSE Password: ******** ********
VSE Crypto Library: CRYPTO . KEYRING
Cert. Member Name: SFTP1024 . PRVK / CERT / ROOT
Cert. Mapping Member: BSSDCUID . MAPPING
TCP/IP Library: PRD1 . BASE
TCP/IP System ID: 00

Then press the **Add** button to add the new definition. We are now ready to create the VSE server key and the necessary certificates.

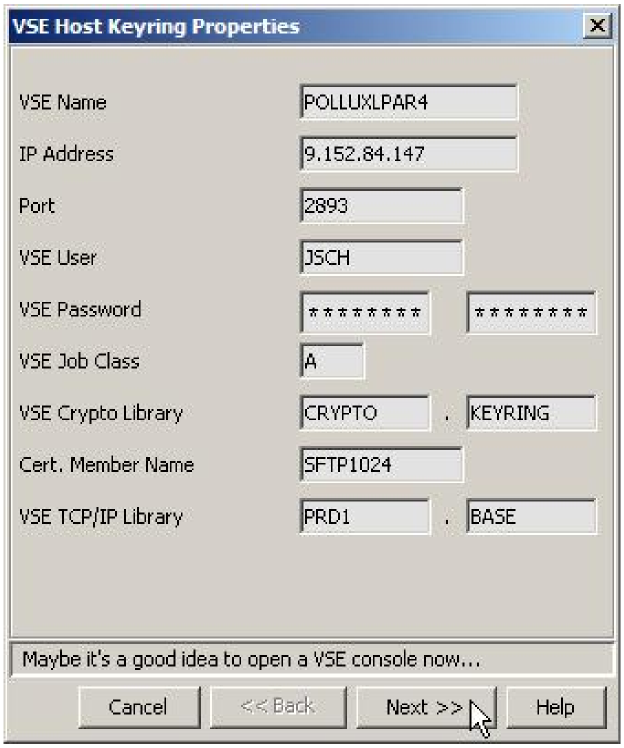
2.1.2 Create the VSE key and certificates

Click on **the Create self-signed keyring** toolbar button.


Keyman/VSE - C:\vsecon\samples\Keyring.pfx
File
Options
Actions
Help
Alias
Certificate Item
Length
Type
VSE User
Valid
Create self-signed keyring

POLLUXLPAR4 : 9.152.84.147

Fill in the required information on the next dialog box

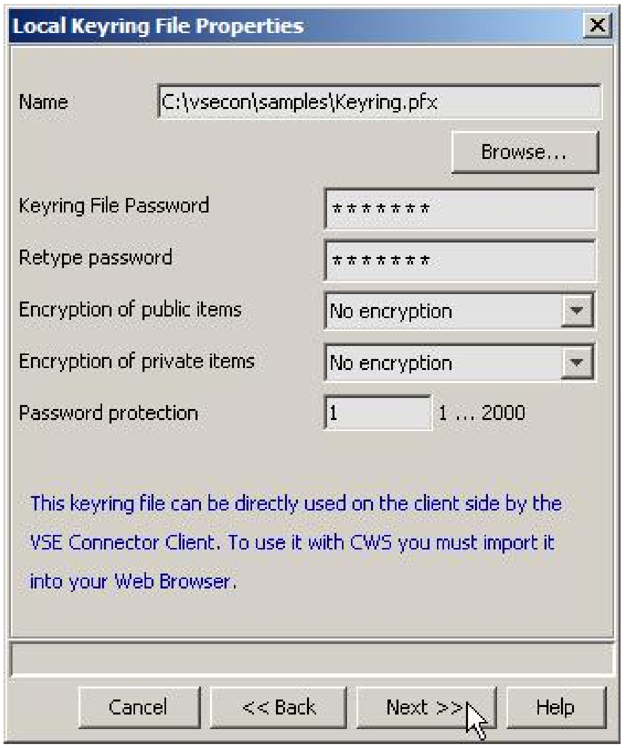


VSE Name	POLLUXLPAR4	
IP Address	9.152.84.147	
Port	2893	
VSE User	JSCH	
VSE Password	********	********
VSE Job Class	A	
VSE Crypto Library	CRYPTO .	KEYRING
Cert. Member Name	SFTP1024	
VSE TCP/IP Library	PRD1 .	BASE

Maybe it's a good idea to open a VSE console now...

Press **Next**.

On the next dialog specify a password which is used for protecting the local keyring file. You should leave the settings for the encryption of public and private items on **No encryption**. Otherwise there might be problems when reading the file afterwards.



Local Keyring File Properties

Name: C:\vsecon\samples\Keyring.pfx

Keyring File Password: *******

Retype password: *******

Encryption of public items: No encryption

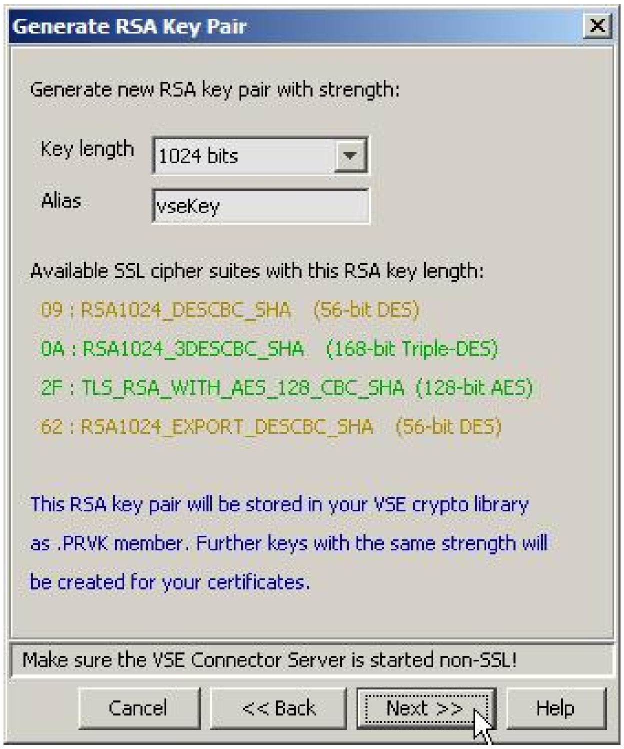
Encryption of private items: No encryption

Password protection: 1 (1 … 2000)

This keyring file can be directly used on the client side by the VSE Connector Client. To use it with CWS you must import it into your Web Browser.

Press **Next**.

On the next dialog box specify the key length of your server key and a unique alias string to identify the key. The box shows you a list of available cipher suites with the selected RSA key length. This association has been removed with TCP/IP fix ZP15E250; refer to the notes below Table 1 on page 14.



Generate RSA Key Pair

Generate new RSA key pair with strength:

Key length: 1024 bits

Alias: vseKey

Available SSL cipher suites with this RSA key length:

09 : RSA1024_DESCBC_SHA (56-bit DES)

0A : RSA1024_3DESCBC_SHA (168-bit Triple-DES)

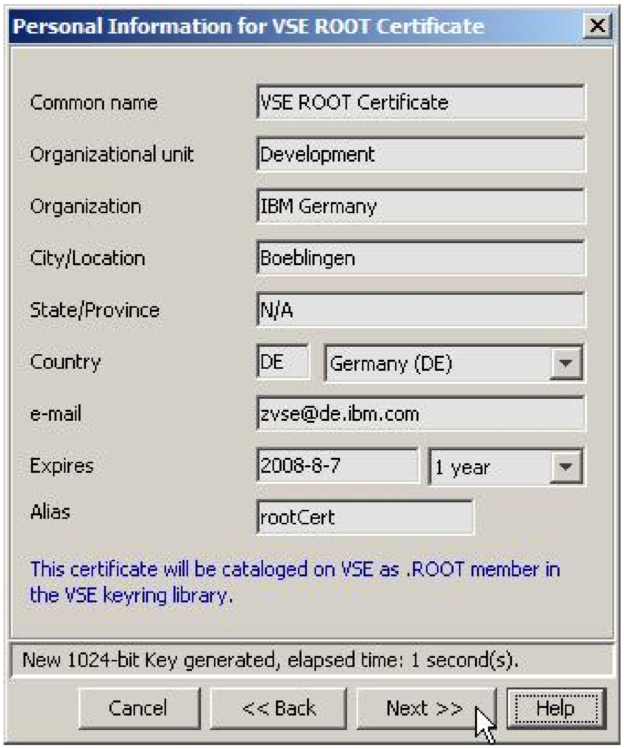
2F : TLS_RSA_WITH_AES_128_CBC_SHA (128-bit AES)

62 : RSA1024_EXPORT_DESCBC_SHA (56-bit DES)

This RSA key pair will be stored in your VSE crypto library as .PRVK member. Further keys with the same strength will be created for your certificates.

Make sure the VSE Connector Server is started non-SSL!

Press **Next**. On the following dialog box specify the personal information for the VSE ROOT certificate.



Personal Information for VSE ROOT Certificate

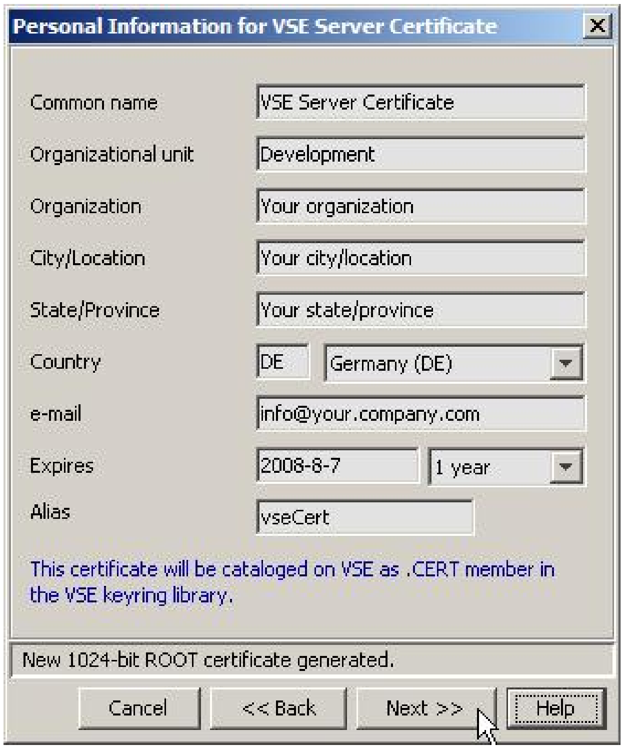
Common name	VSE ROOT Certificate
Organizational unit	Development
Organization	IBM Germany
City/Location	Boeblingen
State/Province	N/A
Country	DE Germany (DE)
e-mail	zvse@de.ibm.com
Expires	2008-8-7 1 year
Alias	rootCert

This certificate will be cataloged on VSE as .ROOT member in the VSE keyring library.

New 1024-bit Key generated, elapsed time: 1 second(s).

Press **Next**.

On the following dialog box specify the personal information for the VSE server certificate.



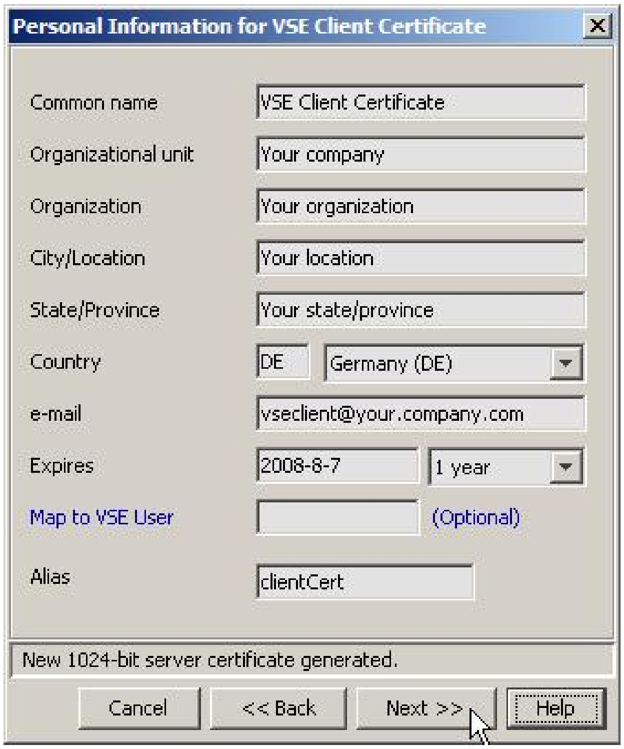
Personal Information for VSE Server Certificate

Common name	VSE Server Certificate
Organizational unit	Development
Organization	Your organization
City/Location	Your city/location
State/Province	Your state/province
Country	DE Germany (DE)
e-mail	info@your.company.com
Expires	2008-8-7 1 year
Alias	vseCert

This certificate will be cataloged on VSE as .CERT member in the VSE keyring library.

New 1024-bit ROOT certificate generated.

Press **Next**. A client certificate is only needed for Client Authentication.

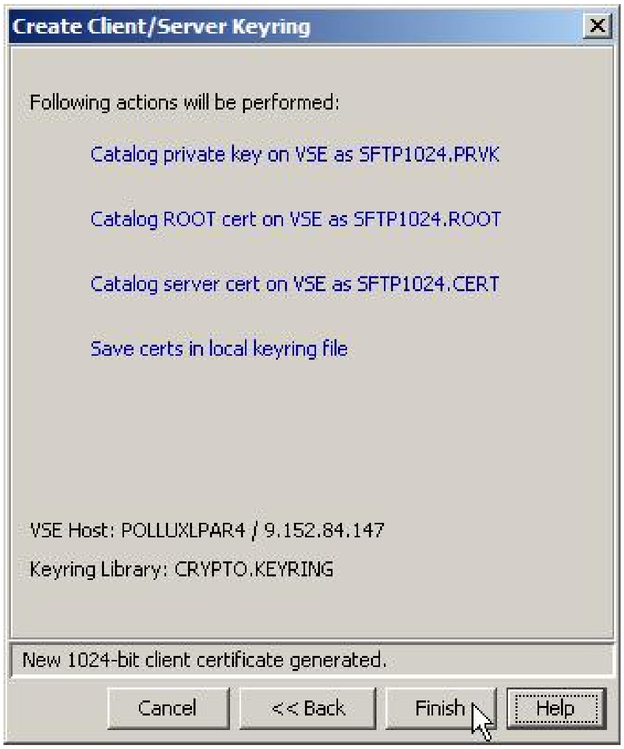


Personal Information for VSE Client Certificate

Common name	VSE Client Certificate
Organizational unit	Your company
Organization	Your organization
City/Location	Your location
State/Province	Your state/province
Country	DE Germany (DE)
e-mail	vseclient@your.company.com
Expires	2008-8-7 1 year
Map to VSE User	(Optional)
Alias	clientCert

New 1024-bit server certificate generated.

Press **Next**.



Create Client/Server Keyring

Following actions will be performed:

Catalog private key on VSE as SFTP1024.PRVK

Catalog ROOT cert on VSE as SFTP1024.ROOT

Catalog server cert on VSE as SFTP1024.CERT

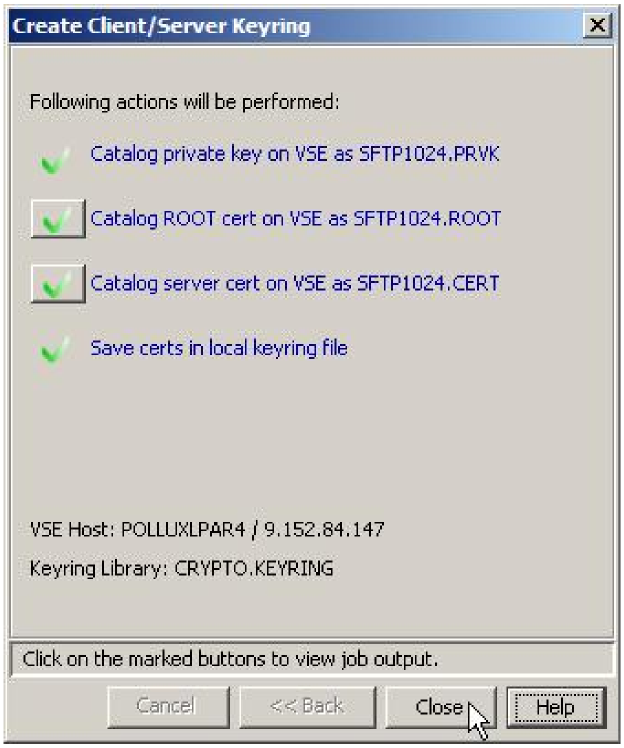
Save certs in local keyring file

VSE Host: POLLUXLPAR4 / 9.152.84.147

Keyring Library: CRYPTO.KEYRING

New 1024-bit client certificate generated.

Press **Finish**.



Create Client/Server Keyring

Following actions will be performed:

✓ Catalog private key on VSE as SFTP1024.PRVK

✓ Catalog ROOT cert on VSE as SFTP1024.ROOT

✓ Catalog server cert on VSE as SFTP1024.CERT

✓ Save certs in local keyring file

VSE Host: POLLUXLPAR4 / 9.152.84.147

Keyring Library: CRYPTO.KEYRING

Click on the marked buttons to view job output.

Press **Close**.

Now you have three VSE library members cataloged into CRYPTO.KEYRING. The PRVK member contains the RSA key pair, the ROOT member contains the self-signed VSE ROOT certificate, and the CERT member contains the VSE server certificate.

```
LD SFTP*.*

DIRECTORY DISPLAY    SUBLIBRARY=CRYPTO.KEYRING      DATE: 2007-08-07
                                                 TIME: 11:43
--------------------------------------------------------------------
 M E M B E R      CREATION   LAST     BYTES    LIBR CONT SVA  A- R-
NAME     TYPE     DATE       UPDATE   RECORDS  BLKS STOR ELIG MODE
--------------------------------------------------------------------
SFTP1024 CERT     07-08-07   -  -      724 B       1 YES   -    -   -
SFTP1024 PRVK     07-08-07   -  -     2048 B       3 YES   -    -   -
SFTP1024 ROOT     07-08-07   -  -      686 B       1 YES   -    -   -
L113I RETURN CODE OF LISTDIR IS  0
L001A ENTER COMMAND OR END
```

You can also close the Keyman/VSE tool now. As we don't need the server key on the client side, the key was not saved to the local file.

2.2 Setup and start the VSE FTP server

In general there are two types of FTP servers in VSE:

- External FTP daemons, which run in a separate VSE partition
- Internal FTP daemons, which run as a subtask in the TCP/IP partition

The following JCL starts an external SSL-enabled FTP server on VSE.

```
* $$ JOB JNM=FTPSERV,CLASS=8,DISP=D
* $$ LST CLASS=A
// JOB FTPSERV
// OPTION LOG,NOSYSDMP
// OPTION SYSPARM='00'
/* LIBDEF *,SEARCH=(PRD1.BASE)
// EXEC FTPBATCH,SIZE=FTPBATCH,PARM='UNIX=YES,FTPDPORT=990,SSL=SERVER'
SET DIAGNOSE ON
SET SSL PRIVATE CRYPTO.KEYRING.SFTP1024 NOCLAUTH
/*
/&
* $$ EOJ
```

When running the FTP server, some console messages are issued.

```
F8 0008 // JOB FTPSERV
        DATE 08/07/2007, CLOCK 12/03/38
F8 0118 FTP302I Connected to TCP/IP Sysid 00 in F7 from F8
...
F8 0118 FTP900I FTP Daemon: FTPBSRVR listening on 9.152.84.147,990
F8 0118 FTP304I FTPX1000 subtask is running 005044E0
F8 0118 FTP314I Command connection SSL secured, data connection:PRIVATE
F8 0118 FTP306I Commands from SYSIPT COMPLETED
```

You may check the listening port here again. In our example the server listens on port 990.

Here is the TCP/IP command for starting an internal FTP server with the same properties.

```
DEFINE FTPD,ID=FTPDSSL,PORT=990,COUNT=1,TIMEOUT=9000,UNIX=YES, -
   DRIVER=FTPDAEMN,SSL=YES,SSLKEY=CRYPTO.KEYRING.SFTP1024, -
   SSLVER=SSLV3,SSLCIPHER=ALL,SSLDATACONN=PRIVATE
```

Notes:

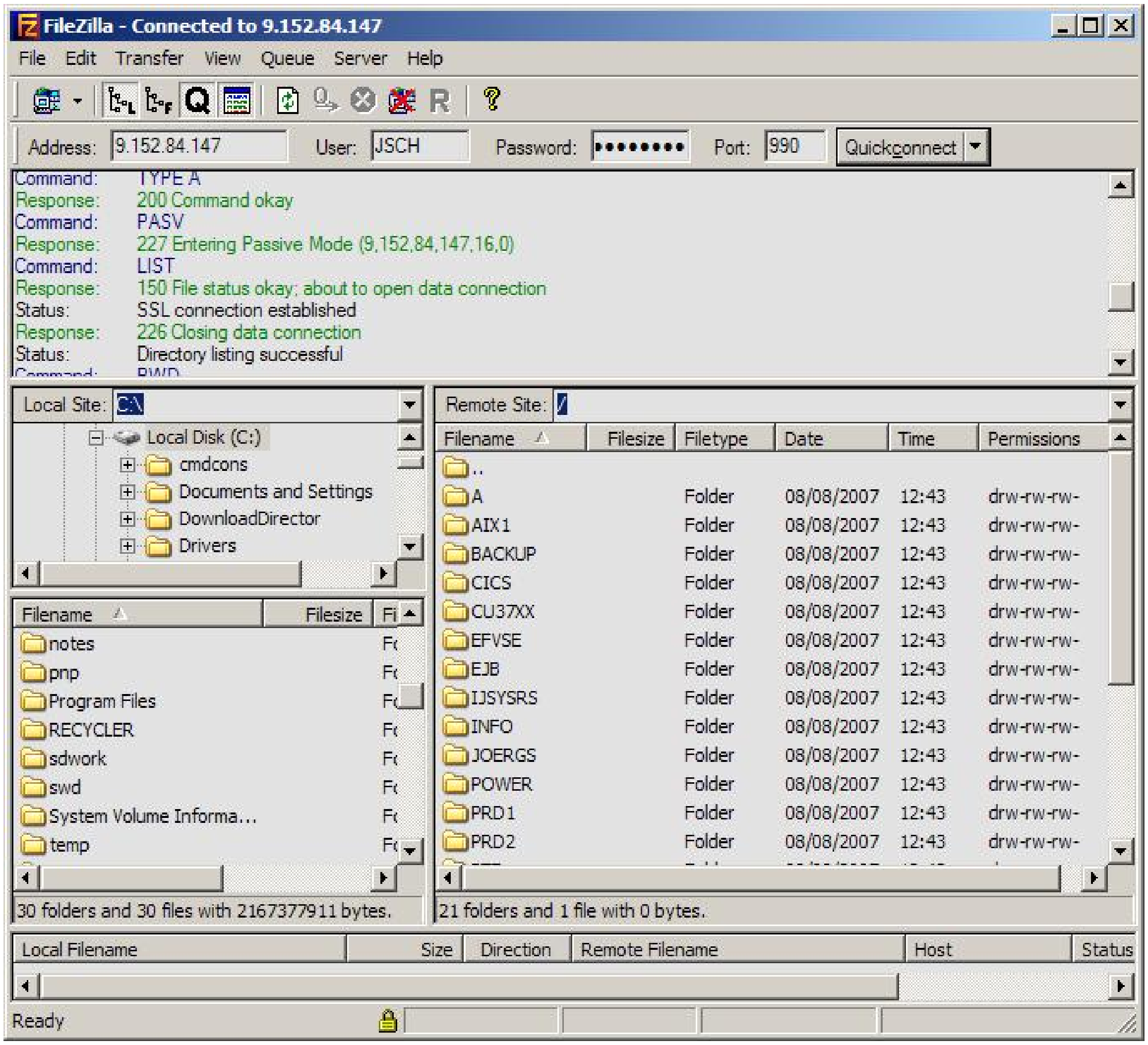
- It is important that you define the FTP daemon with **UNIX=YES** to make the VSE file system accessible for the Filezilla FTP client. Without UNIX mode, the VSE file system will appear as just one single <Directory> entry which cannot be accessed by the FTP client.

- On the other hand, the z/VM FTP client has a problem when the FTPD is defined with UNIX-mode. All transferred data records are truncated to 80 characters. So when you are also using z/VM to access VSE via FTP, you should define a second FTPD on VSE with UNIX=NO. Messages similar to the following appear on the VSE console when the problem occurs.

  ```
  FTP928E Record 1 larger then max(80) for ptf/file UNIX=YES
  IPN549E IPCCDROP error: Invalid ownership 01
  ```

2.3 Connect to VSE using an FTP client

In our example we use the FileZilla FTP client. After connecting to the VSE FTP server, the VSE directory listing is retrieved.


FileZilla - Connected to 9.152.84.147
File Edit Transfer View Queue Server Help
Quickconnect

Address: 9.152.84.147 User: JSCH Password: •••••••• Port: 990

```
Command:   TYPE A
Response:  200 Command okay
Command:   PASV
Response:  227 Entering Passive Mode (9,152,84,147,16,0)
Command:   LIST
Response:  150 File status okay; about to open data connection
Status:    SSL connection established
Response:  226 Closing data connection
Status:    Directory listing successful
```

Local Site: C:\

- Local Disk (C:)
  - cmdcons
  - Documents and Settings
  - DownloadDirector
  - Drivers

Filename	Filesize	Fi
notes		F(
pnp		F(
Program Files		F(
RECYCLER		F(
sdwork		F(
swd		F(
System Volume Informa...		F(
temp		F(

30 folders and 30 files with 2167377911 bytes.

Remote Site: /

Filename	Filesize	Filetype	Date	Time	Permissions
..					
A		Folder	08/08/2007	12:43	drw-rw-rw-
AIX1		Folder	08/08/2007	12:43	drw-rw-rw-
BACKUP		Folder	08/08/2007	12:43	drw-rw-rw-
CICS		Folder	08/08/2007	12:43	drw-rw-rw-
CU37XX		Folder	08/08/2007	12:43	drw-rw-rw-
EFVSE		Folder	08/08/2007	12:43	drw-rw-rw-
EJB		Folder	08/08/2007	12:43	drw-rw-rw-
IJSYSRS		Folder	08/08/2007	12:43	drw-rw-rw-
INFO		Folder	08/08/2007	12:43	drw-rw-rw-
JOERGS		Folder	08/08/2007	12:43	drw-rw-rw-
POWER		Folder	08/08/2007	12:43	drw-rw-rw-
PRD1		Folder	08/08/2007	12:43	drw-rw-rw-
PRD2		Folder	08/08/2007	12:43	drw-rw-rw-

21 folders and 1 file with 0 bytes.

Local Filename	Size	Direction	Remote Filename	Host	Status

Ready

On the VSE side, the FTP daemon tells you, which ciphers are used in the current connection.

```
F7 0098 0005: FTP900I FTP Daemon: FTPDSSL listening on 9.152.84.147,990
F7 0098 0034: FTP922I Control connection using SSL TLSV1 Cipher=0035
        (01670000)
F7 0098 0034: FTP909I JSCH in session with 9.152.216.58,1694
F7 0098 0034: FTP910I Data connection open 9.152.216.58,1695 (4101)
F7 0098 0034: FTP922I Data connection using SSL TLSV1 Cipher=0035 (0166F000)
```

Cipher 0035 means that transferred data is encrypted using AES-256. Here is the complete list of supported cipher suites and their meaning.

Hex Code	Cipher Suite	Handshaking (*)	Encryption	Min. TCP/IP
01	SSL_RSA_WITH_NULL_MD5	512	None	1.5D
02	SSL_RSA_WITH_NULL_SHA	512	None	1.5D
08	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	512	40 bits	1.5D
09	SSL_RSA_WITH_DES_CBC_SHA	1024	56 bits	1.5D
0A	SSL_RSA_WITH_3DES_EDE_CBC_SHA	1024	168 bits	1.5D
2F	TLS_RSA_WITH_AES_128_CBC_SHA	1024 / 2048	128 bits	1.5E
35	TLS_RSA_WITH_AES_256_CBC_SHA	1024 / 2048	256 bits	1.5E
62	RSA1024_EXPORT_DESCBC_SHA	1024	56 bits	1.5D

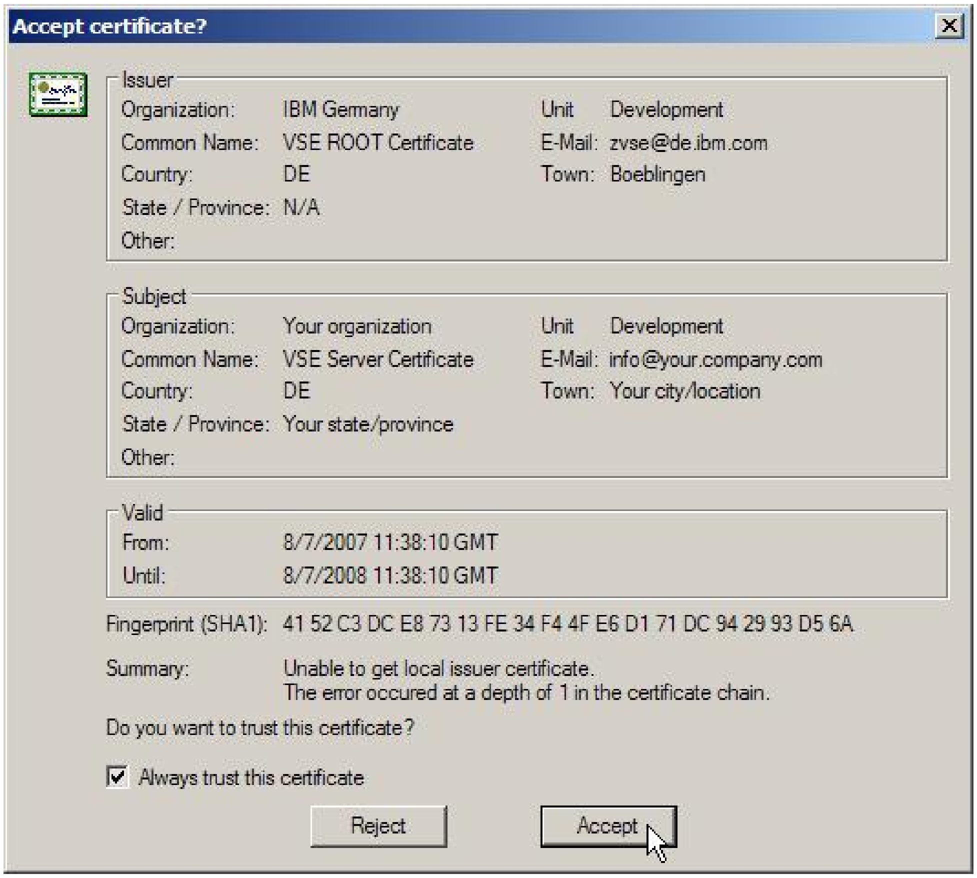
Table 1: available cipher suites on VSE

Notes:

- When using 2048-bit keys you need a Crypto Express2 or PCI-X Cryptographic Coprocessor card.
- AES support was introduced with TCP/IP fix ZP15E214.
- AES-128 is available as hardware function on IBM System z9 and z10 processors and is much faster than the software implementations provided by TCP/IP. It is used transparently by TCP/IP when available.
- (*) TCP/IP fix ZP15E250 removes the restriction of allowing some cipher suites only with a specific RSA key length. If you look at the RFC2240 for TLS you will notice that it does not have a RSA key size associated with the specific cipher suites. Any cipher suite can now be used with any of the RSA key sizes.

2.4 Transfer the certificate to the client side

The FileZilla client allows importing the server certificate into its certificate store while opening a secure FTP session, so it is not necessary to transfer the certificate in advance. Simply accept the server certificate permanently when the following message box appears on the client side.


Accept certificate?

Issuer
Organization: IBM Germany Unit Development
Common Name: VSE ROOT Certificate E-Mail: zvse@de.ibm.com
Country: DE Town: Boeblingen
State / Province: N/A
Other:

Subject
Organization: Your organization Unit Development
Common Name: VSE Server Certificate E-Mail: info@your.company.com
Country: DE Town: Your city/location
State / Province: Your state/province
Other:

Valid
From: 8/7/2007 11:38:10 GMT
Until: 8/7/2008 11:38:10 GMT

Fingerprint (SHA1): 41 52 C3 DC E8 73 13 FE 34 F4 4F E6 D1 71 DC 94 29 93 D5 6A

Summary: Unable to get local issuer certificate.
The error occured at a depth of 1 in the certificate chain.

Do you want to trust this certificate?

☑ Always trust this certificate

For permanently adding this certificate to the server, mark the checkbox **Always trust this certificate** and click on **Accept**. When you do not mark the checkbox, you will get this message box whenever connecting to VSE again.

3 VSE as Client

Setting up Secure FTP with VSE as the client side, involves some configuration effort on a FTP server outside of VSE unless both sides are VSE systems.

In the following sections we use the popular Open Source FTP server FileZilla as one example of a non-VSE FTP server.

3.1 Sample Setup with FileZilla Server

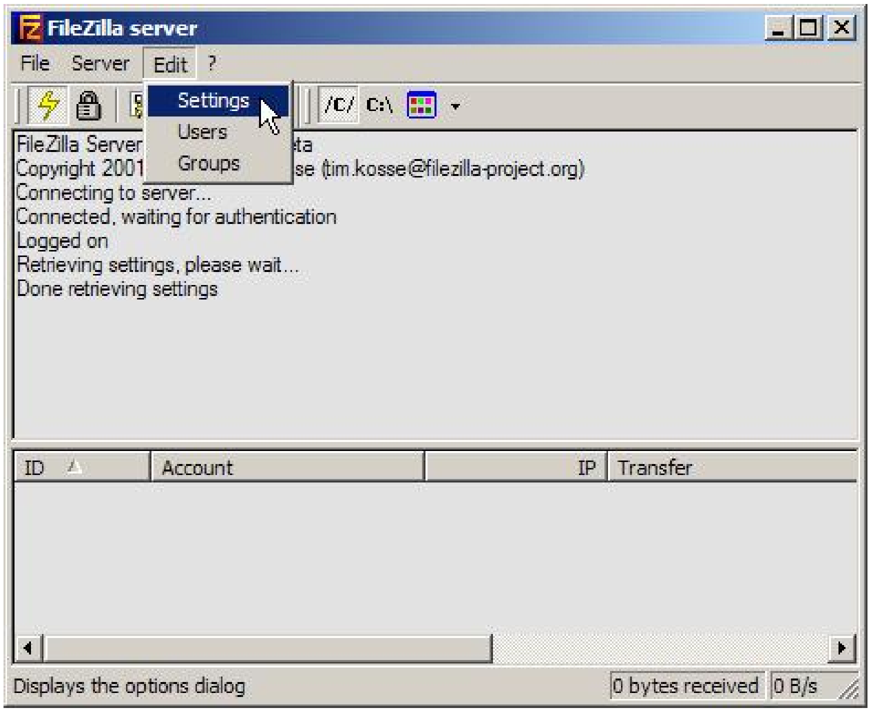
You can download the FileZilla Server from

http://filezilla-project.org/

Note: on Windows the FileZilla server is installed as a Windows service and started automatically when Windows is started. You might want to not always start the server for security reasons. To configure server startup for manual startup, open the Windows Control panel, click on Administrative Tools, click on Services, and change the startup option for the FileZilla server to manual startup.

3.1.1 Generate the server key and certificate

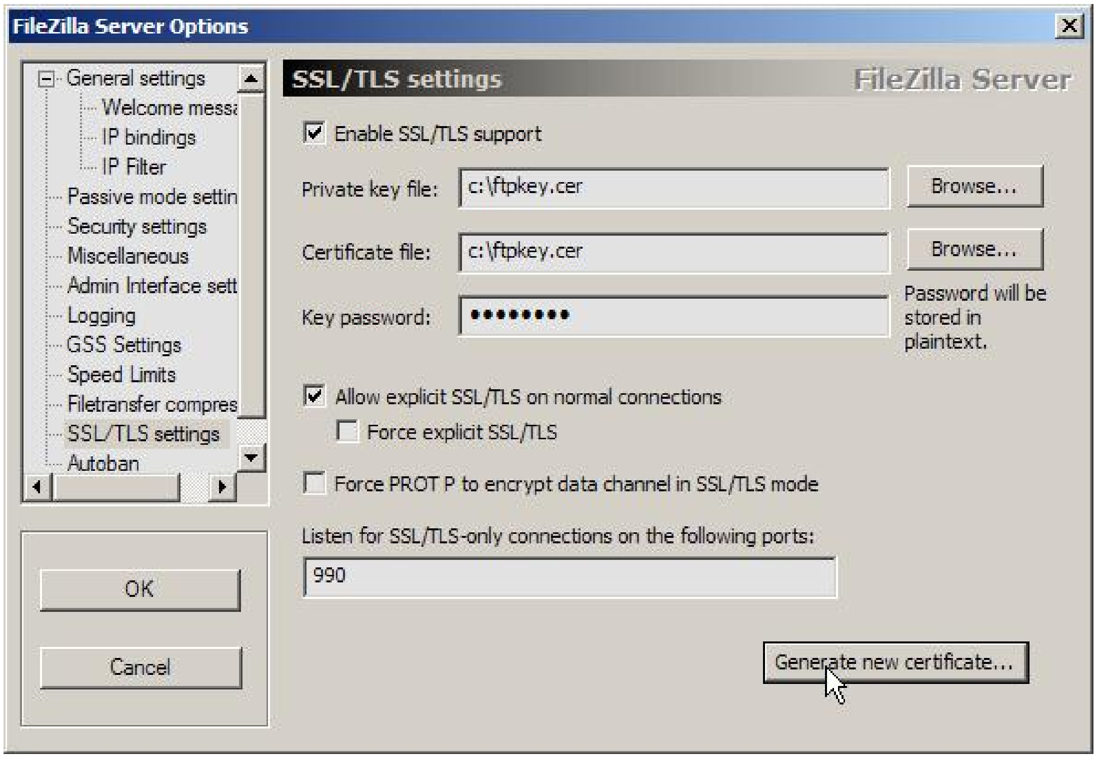
This functionality is provided by the FileZilla server. Start the server and open the FileZilla server interface. Then open the **Settings** dialog.



```
FileZilla Server                ta
Copyright 2001                  se (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving settings, please wait...
Done retrieving settings
```

Displays the options dialog | 0 bytes received | 0 B/s

On the FileZilla Server Options box select **SSL/TLS Settings** and specify the filename(s) for the server key and the certificate file. Both items can be stored into the same file. You have also to specify a password for the key file. This password would be needed later when importing the key file into a Web Browser for further use e.g. in a SSL setup.



SSL/TLS settings

☑ Enable SSL/TLS support

Private key file: c:\ftpkey.cer

Certificate file: c:\ftpkey.cer

Key password: ●●●●●●●●● Password will be stored in plaintext.

☑ Allow explicit SSL/TLS on normal connections

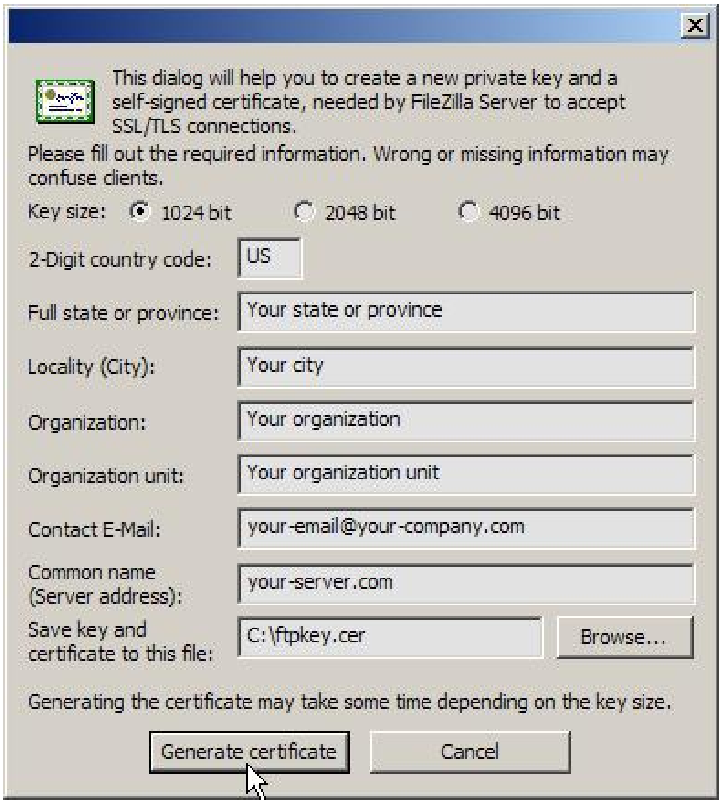
☐ Force explicit SSL/TLS

☐ Force PROT P to encrypt data channel in SSL/TLS mode

Listen for SSL/TLS-only connections on the following ports: 990

Then press the **Generate new certificate** button.

On the next dialog box fill in the required text fields and press the **Generate certificate** button.



This dialog will help you to create a new private key and a self-signed certificate, needed by FileZilla Server to accept SSL/TLS connections.

Please fill out the required information. Wrong or missing information may confuse clients.

Key size: ● 1024 bit ○ 2048 bit ○ 4096 bit

2-Digit country code: US

Full state or province: Your state or province

Locality (City): Your city

Organization: Your organization

Organization unit: Your organization unit

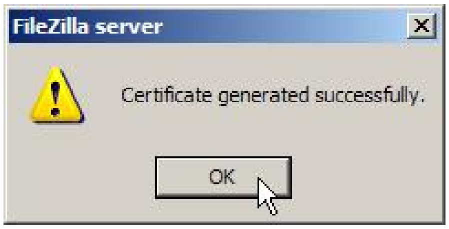
Contact E-Mail: your-email@your-company.com

Common name (Server address): your-server.com

Save key and certificate to this file: C:\ftpkey.cer

Generating the certificate may take some time depending on the key size.

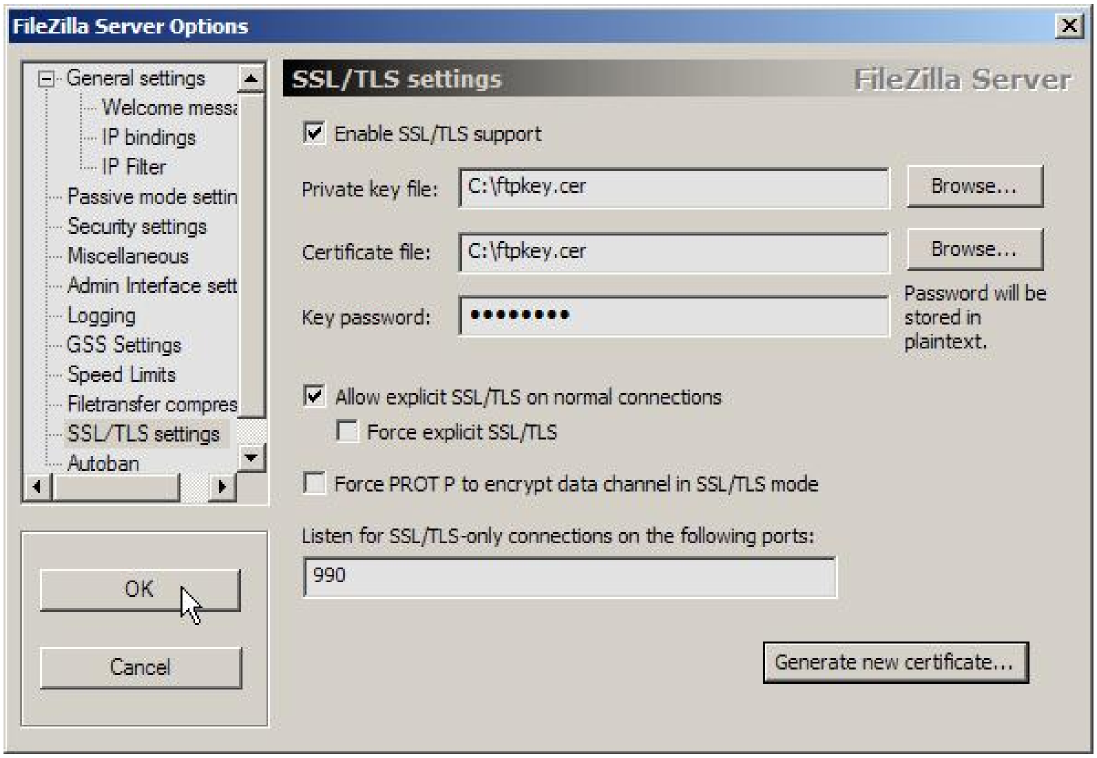
Note: the created certificate has a validity period of **one year**. FileZilla does not allow specifying any other validity period. Refer to section 3.1.2 on page 20 for how to use OpenSSL to create a certificate with a different validity period.



FileZilla server

Certificate generated successfully.

Press **OK**.



FileZilla Server Options

SSL/TLS settings

☑ Enable SSL/TLS support

Private key file: C:\ftpkey.cer

Certificate file: C:\ftpkey.cer

Key password: ••••••••• Password will be stored in plaintext.

☑ Allow explicit SSL/TLS on normal connections

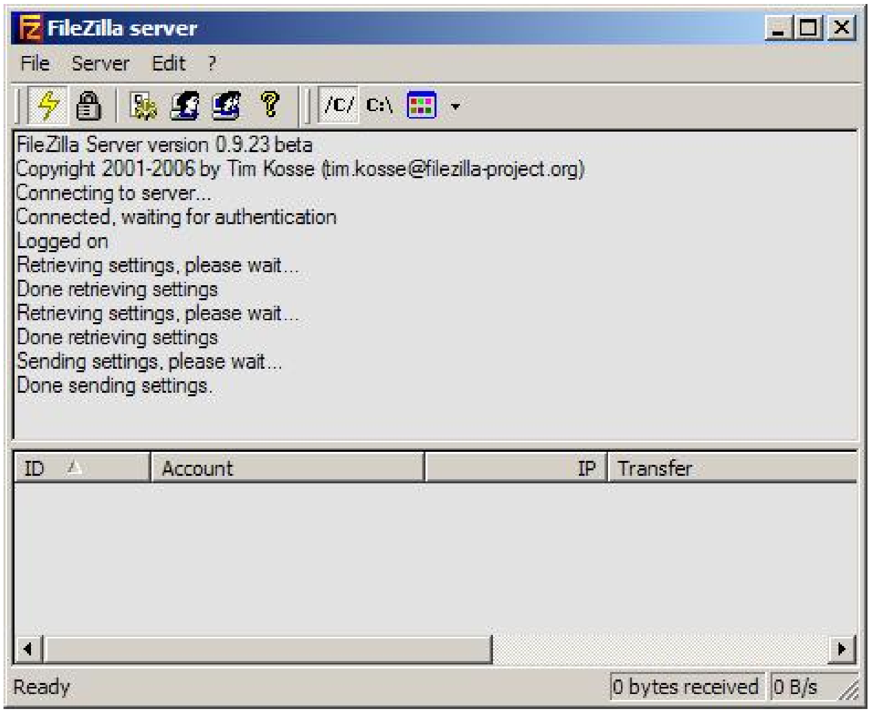
□ Force explicit SSL/TLS

□ Force PROT P to encrypt data channel in SSL/TLS mode

Listen for SSL/TLS-only connections on the following ports:

990

Now press **OK** on the FileZilla Server options box. The server stores the settings for further use.



```
FileZilla Server version 0.9.23 beta
Copyright 2001-2006 by Tim Kosse (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving settings, please wait...
Done retrieving settings
Retrieving settings, please wait...
Done retrieving settings
Sending settings, please wait...
Done sending settings.
```

The private key and the certificate are now stored in local file c:\ftpkey.cer. FileZilla stores the data in base64 text form. When you look at the file contents with a text editor, it will look like:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDmYs6yuU/5Fq5vCHkIvwKMmpJuQEWMUpOF7BJoY8Dt1Lfp+fER
4SLLrnFrxL6NBG735namX1Ed7Du3/9LIEIAlE6u0z0bGuie6699zenZwBUqAcaZL
RzgMSyYEiTUUy4Pa9mvuKRAGGPP/8WjOEkzx5ieiUAGSTSXpXtKzNEyWiwIDAQAB
AoGAD/aWteGLPgopSf4/TLDXf2CSdtszNnbeS/BAkkUfMBuGJssvvfpoi85pg3sd
...
gcJ5Phq811pcxmrpzAcCQQCyGWtJTw1ceENAyJpGJKSzB7FOEjZL5NO5vgwkFulC
F651IQFfYCo3XRZXJSypF42RUCiMsJjipUQFpL0cKGEo
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDADCCAmmgAwIBAgIBADANBgkqhkiG9w0BAQUFADCBxTEYMBYGA1UEAxMPeW91
ci1zZXJ2ZXIuY29tMQswCQYDVQQGEwJVUzEfMB0GA1UECBMWWW91ciBzdGF0ZSBv
ciBwcm92aW5jZTESMBAGA1UEBxMJWW91ciBjaXR5MRowGAYDVQQKExFZb3VyIG9y
...
EeEiy65xa8S+jQRu9+Z2pl9RHew7t//SyBCAJROrtM9Gxronuuvfc3p2cAVKgHGm
S0c4DEsmBIk1FMuD2vZr7ikQBhjz//FozhJM8eYnolABkk0l6V7SszRMlosCAwEA
ATANBgkqhkiG9w0BAQUFAAOBgQCH1VcZJKVwCTHJCz0W7RHgrPgadMQTxNe6IKE/
Jce0fmA7aq0ruukSnG7NxAe2p3fWuKe+C8Vq2vE0hnG99AH4XIVr33Ri1pOUnyQj
cKVdXO/XCC9ta4N24QZW1lGD6Nxp/sgoLsPbWbhKS4/CHNZKcmJjrTJSSAn2aBJv
ds10ig==
-----END CERTIFICATE-----
```

Our next step is now to read the FTP server certificate from the local file and send it to VSE. The following section shows how to use OpenSSL to create a certificate with another validity periof than one year. You can skip this section if you created the certificate with FileZilla as described above.

3.1.2 Using OpenSSL to create the server key and certificate

This section describes how to create the server key and certificate using OpenSSL in order to specify a different validity period than one year. At the time of writing this document this is the only way I know of doing so. FileZilla does not accept PFX or JKS files as the key or certificate file. Only base64-encoded (PEM) files can be used and OpenSSL seems to be the only available application that creates the right format.

To install OpenSSL on Windows XP I downloaded two files from

- http://www.slproweb.com/products/Win32OpenSSL.html

The links to the two files on above web page are:

- Win32 OpenSSL v0.9.8i Light
- Visual C++ 2008 Redistributables (you need these runtime components for OpenSSL)

First download and install the Visual C++ Redistributables, then install OpenSSL Light.

To create the key and certificate files, open a command prompt and browse to the OpenSSL install and bin directory.

Then enter following command string:

```
openssl req -new -x509 -keyout ftpkey.pem -out ftpcert.pem -days 3650
```

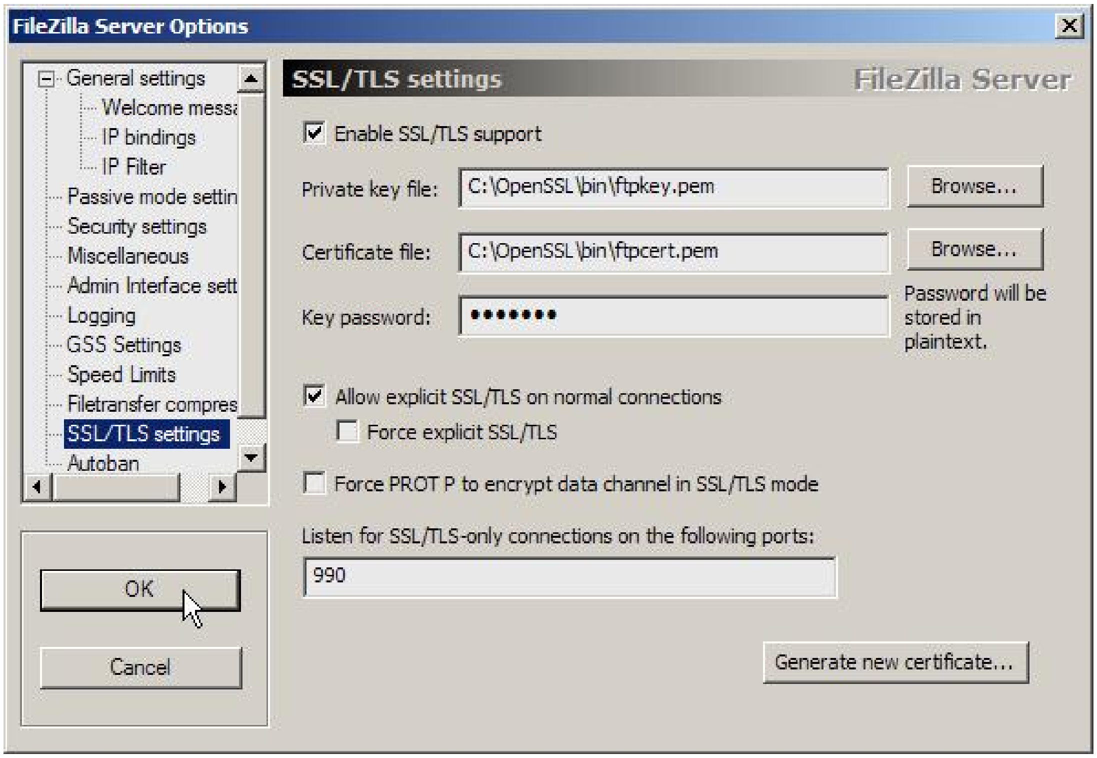
In this example, the certificate will be valid for 10 years (3650 days).

You will be prompted to specify your personal information:

```
C:\OpenSSL\bin>openssl req -new -x509 -keyout ftpkey.pem -out ftpcert.pem -days
3650
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.......................................................++++++
..........................++++++
writing new private key to 'ftpkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:BW
Locality Name (eg, city) []:Boeblingen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IBM Germany
Organizational Unit Name (eg, section) []:Development
Common Name (eg, YOUR name) []:9.152.222.125
Email Address []:zvse@de.ibm.com

C:\OpenSSL\bin>
```

Now open the FileZilla settings dialog and enter the file names for the key and certificate files.



SSL/TLS settings

☑ Enable SSL/TLS support

Private key file: C:\OpenSSL\bin\ftpkey.pem

Certificate file: C:\OpenSSL\bin\ftpcert.pem

Key password: •••••••

Password will be stored in plaintext.

☑ Allow explicit SSL/TLS on normal connections

□ Force explicit SSL/TLS

□ Force PROT P to encrypt data channel in SSL/TLS mode

Listen for SSL/TLS-only connections on the following ports:

990

Press **OK**.

Now continue with the next section to upload the certificate to VSE.

3.1.3 Send the server certificate to VSE

There are two ways of sending a certificate to VSE. You can simply copy the text form of the certificate into a VSE/POWER job or you can use the Keyman/VSE tool to upload the certificate to VSE.

3.1.3.1 Create a VSE/POWER job

Paste the text form of the certificate into a job like shown in this example and specify the member name of the VSE library member which shall contain the certificate on your VSE system.

```
$$ JOB JNM=CIALROOT,CLASS=0,DISP=D
$$ LST CLASS=A
// JOB CIALROOT
// OPTION SYSPARM='00'            SysId of main TCP/IP partition
// EXEC CIALROOT,SIZE=CIALROOT,PARM='CRYPTO.KEYRING.MYCERT'
-----BEGIN CERTIFICATE-----
MIIDADCCAmmgAwIBAgIBADANBgkqhkiG9w0BAQUFADCBxTEYMBYGA1UEAxMPeW91
ci1zZXJ2ZXIuY29tMQswCQYDVQQGEwJVUzEfMB0GA1UECBMWWW91ciBzdGF0ZSBv
ciBwcm92aW5jZTESMBAGA1UEBxMJWW91ciBjaXR5MRowGAYDVQQKExFZb3VyIG9y
Z2FuaXphdGlvbjEfMB0GA1UECxMWWW91ciBvcmdhbml6YXRpb24gdW5pdDEqMCgG
...
S0c4DEsmBIk1FMuD2vZr7ikQBhjz//FozhJM8eYnolABkk0l6V7SszRMlosCAwEA
ATANBgkqhkiG9w0BAQUFAAOBgQCH1VcZJKVwCTHJCz0W7RHgrPgadMQTxNe6IKE/
Jce0fmA7aq0ruukSnG7NxAe2p3fWuKe+C8Vq2vE0hnG99AH4XIVr33Ri1pOUnyQj
cKVdXO/XCC9ta4N24QZW1lGD6Nxp/sgoLsPbWbhKS4/CHNZKcmJjrTJSSAn2aBJv
```

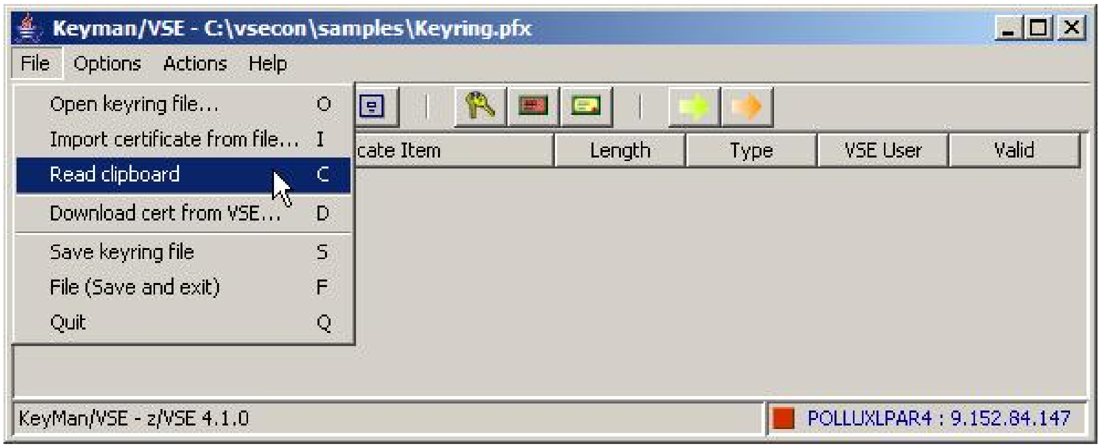
```
ds10ig==
-----END CERTIFICATE-----
/*
/&
$$ EOJ
```

Submitting this job to VSE will catalog a new VSE library member MYCERT.ROOT in sublibrary CRYPTO.KEYRING.

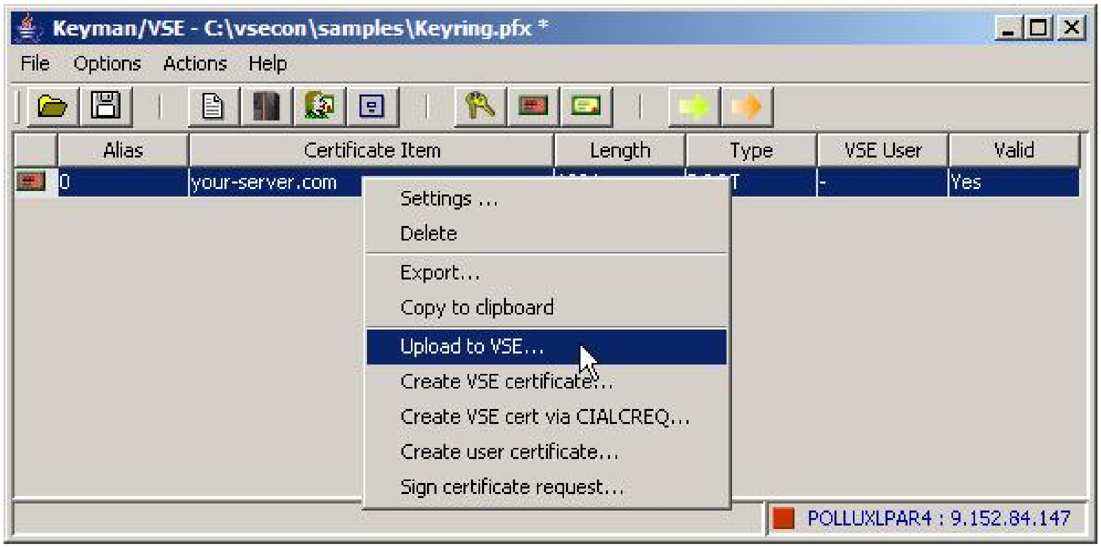
3.1.3.2 Use the Keyman/VSE tool

Simply copy the certificate text including the delimiter lines BEGIN CERTIFICATE and END CERTIFICATE into the clipboard and read the clipboard contents in Keyman/VSE.

Note: as an alternative, you can read the file created by FileZilla or OpenSSL directly using **the Import certificate from file** menu choice with Keyman/VSE, **build date August 2007 or later**.


Keyman/VSE - C:\vsecon\samples\Keyring.pfx
File Options Actions Help
Open keyring file... O
Import certificate from file... I
Read clipboard C
Download cert from VSE... D
Save keyring file S
File (Save and exit) F
Quit Q
cate Item
Length
Type
VSE User
Valid
KeyMan/VSE - z/VSE 4.1.0
POLLUXLPAR4 : 9.152.84.147

The certificate is now available for upload in in Keyman/VSE.

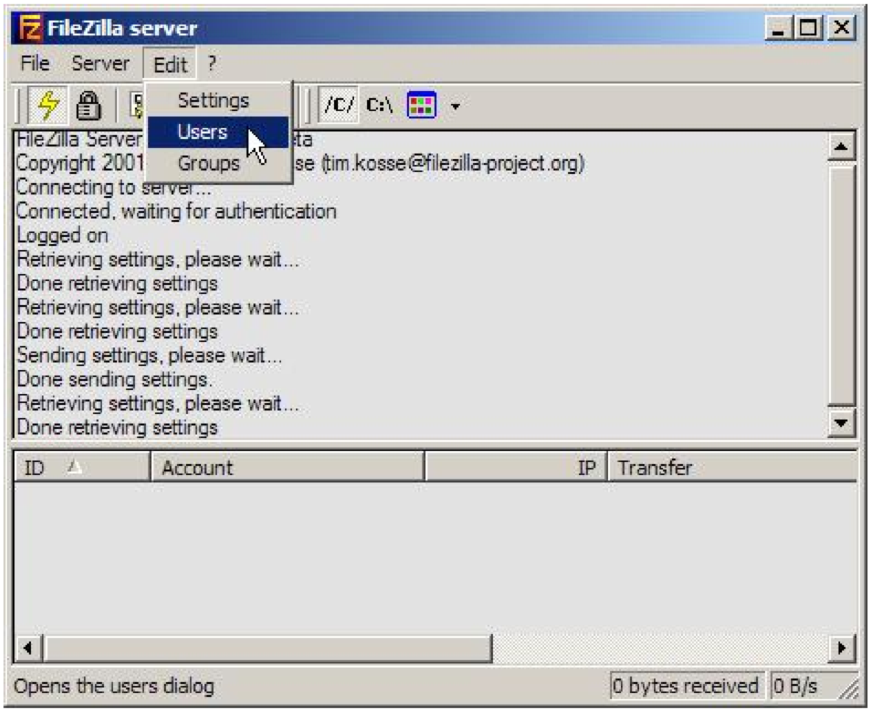

Keyman/VSE - C:\vsecon\samples\Keyring.pfx *
File Options Actions Help
Alias
Certificate Item
Length
Type
VSE User
Valid
0
your-server.com
-
Yes
Settings ...
Delete
Export...
Copy to clipboard
Upload to VSE...
Create VSE certificate...
Create VSE cert via CIALCREQ...
Create user certificate...
Sign certificate request...
POLLUXLPAR4 : 9.152.84.147

Before doing the upload make sure that the right VSE system is shown in the lower right corner of the main window (here POLLUXLPAR4) and that the VSE Connector Server is running on VSE.

Refer to section 5.1 on page 31 if you have problems uploading the certificate.

3.1.4 Define an FTP user in FileZilla

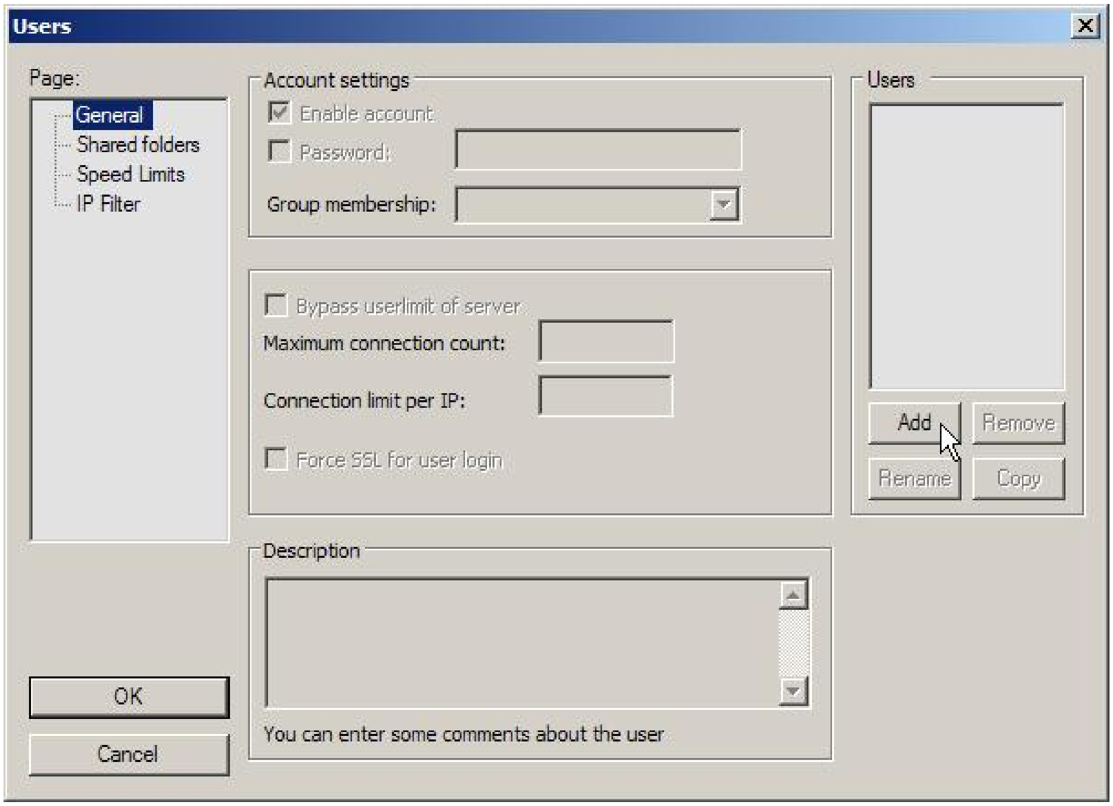
To setup an FTP user in the FileZilla server follow these steps.



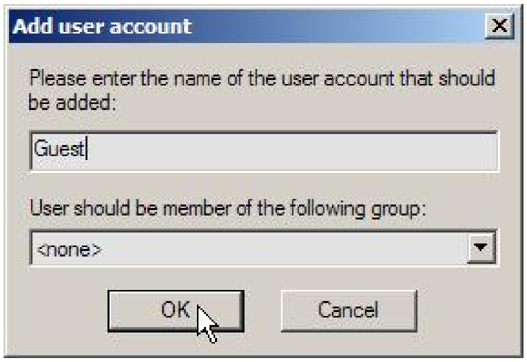
```
FileZilla Server              ta
Copyright 2001                se (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving settings, please wait...
Done retrieving settings
Retrieving settings, please wait...
Done retrieving settings
Sending settings, please wait...
Done sending settings.
Retrieving settings, please wait...
Done retrieving settings
```

Opens the users dialog | 0 bytes received | 0 B/s

In the **Edit** menu, click on **Users**. On the **Users** dialog box click on the **Add** button and enter the name of your FTP user ID.



Enter the name of the FTP user.



Please enter the name of the user account that should be added:

Guest

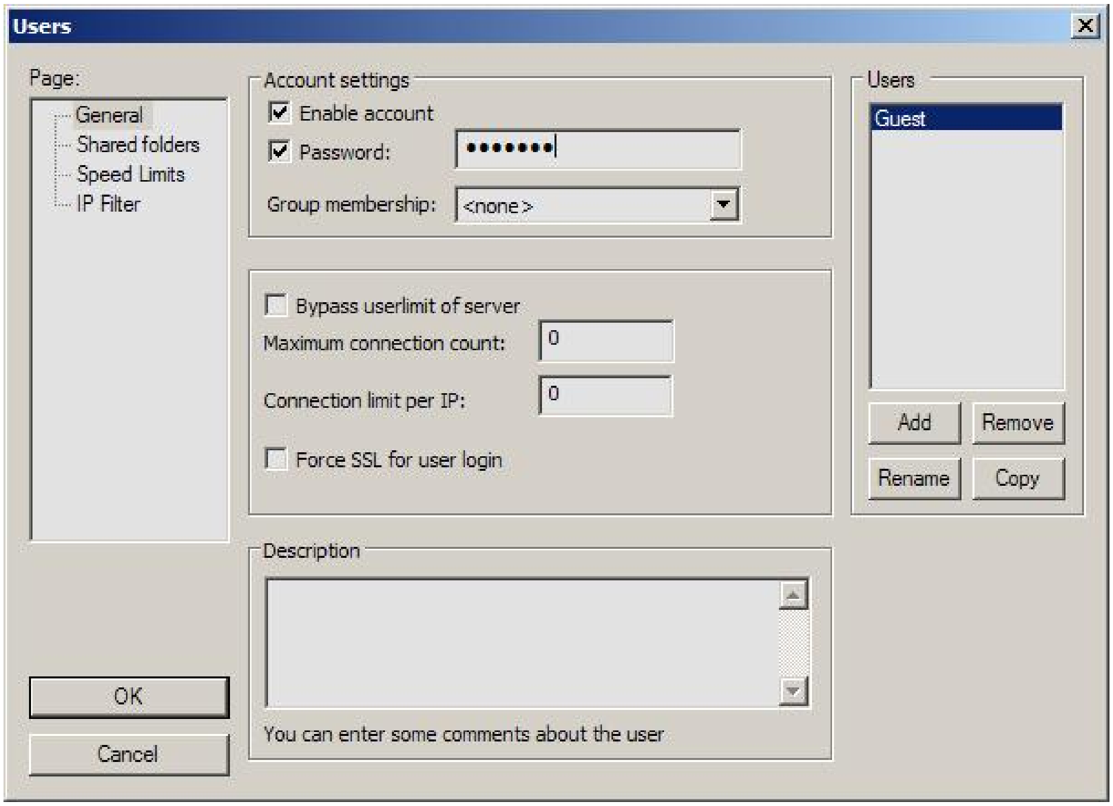
User should be member of the following group:

<none>

Now you have to specify a password for this user.

Notes:

- Passwords are case sensitive. When you specify the password in uppercase letters on the VSE side, you must also use uppercase letters here.
- User IDs are **not** case sensitive, i.e. you may use mixed case letters when defining the user in FileZilla, but use uppercase letters on the VSE side.



Users

Account settings

☑ Enable account

☑ Password: •••••••

Group membership: <none>

□ Bypass userlimit of server

Maximum connection count: 0

Connection limit per IP: 0

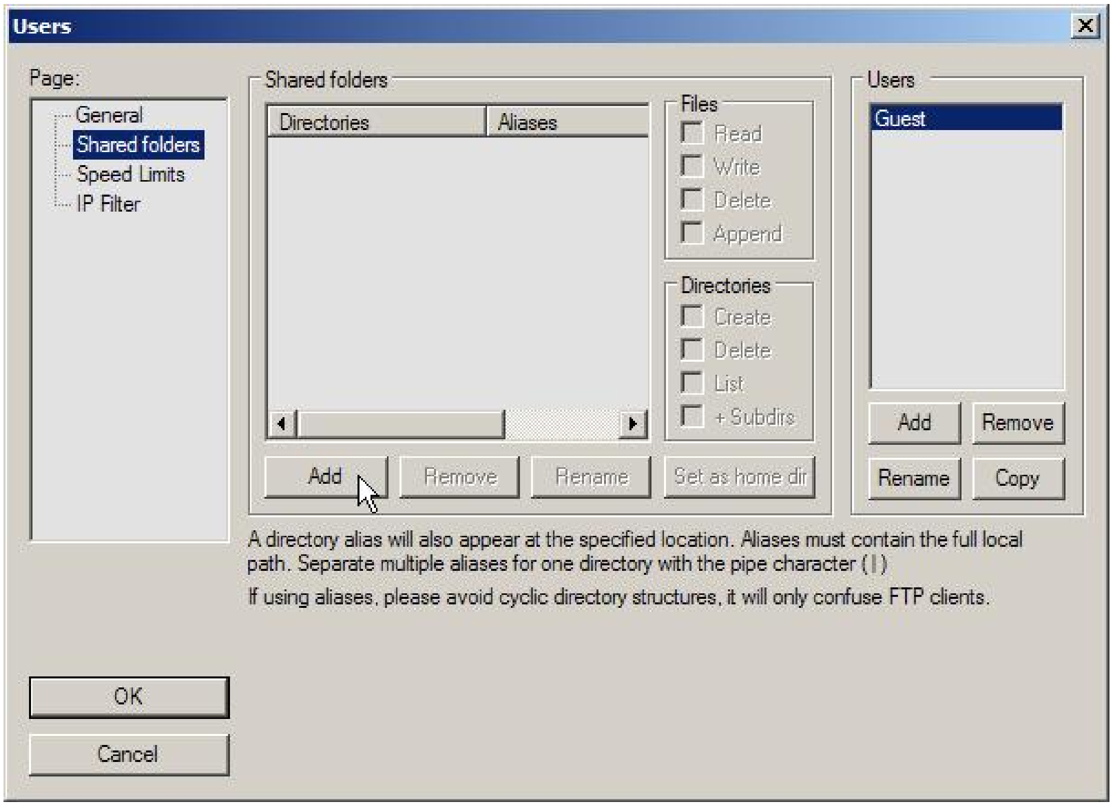
□ Force SSL for user login

Description

You can enter some comments about the user

Users: Guest

In addition to that, you have to specify a home directory for this user. Otherwise connections are not possible.



Users

Shared folders

Directories	Aliases

Files

□ Read

□ Write

□ Delete

□ Append

Directories

□ Create

□ Delete

□ List

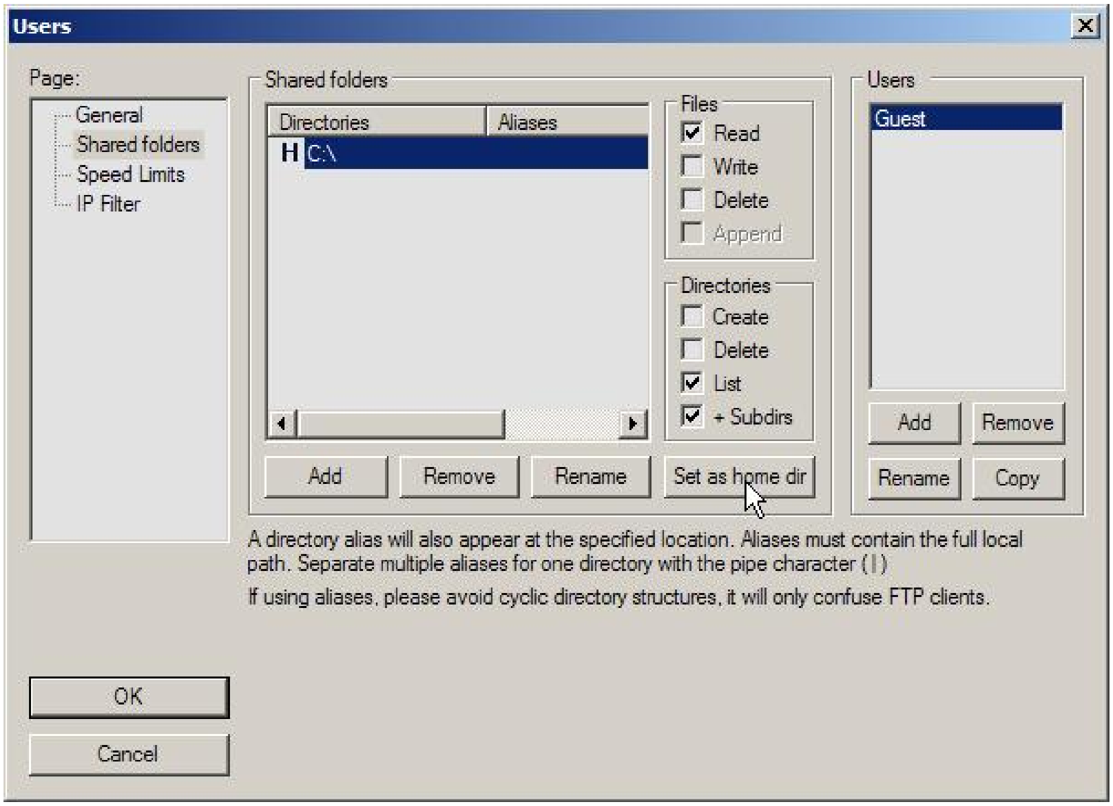
□ + Subdirs

Users: Guest

A directory alias will also appear at the specified location. Aliases must contain the full local path. Separate multiple aliases for one directory with the pipe character (|)

If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.

On this dialog box press the **Add** button.



H C:\

Files

☑ Read
□ Write
□ Delete
□ Append

Directories

□ Create
□ Delete
☑ List
☑ + Subdirs

Guest

A directory alias will also appear at the specified location. Aliases must contain the full local path. Separate multiple aliases for one directory with the pipe character (|)

If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.

Then press the **Set as home dir** button. You might want to customize the security settings in the **Files** and **Directories** group boxes also.

Now press **OK** to leave the **Users** dialog box. We are now ready to connect to the server from a VSE system.

3.2 Connect to the server using the VSE FTP client

You can now connect to the FTP server using the VSE FTP client. The IP address shown in the job belongs to the Windows workstation where the FileZilla server runs.

```
* $$ JOB JNM=FTPBATCH,CLASS=4,DISP=D
// JOB FTPBATCH
// OPTION SYSPARM='00'
// LIBDEF PHASE,SEARCH=PRD1.BASE
// EXEC FTPBATCH,SIZE=FTPBATCH,PARM='SSL=CLIENT'
SET SSL PRIVATE CRYPTO.KEYRING.MYCERT NOCLAUTH ALL
LOPEN
LUSER JSCH
LPASS MYPASSW
LAUTH SSL
OPEN 9.152.216.58   990
AUTH SSL
PROT P
USER GUEST
PASS GUESTPW
DIR
```

```
CLOSE
LCLOSE
QUIT
/*
/&
* $$ EOJ
```

Make sure, that the certificate name matches the name you specified when uploading the certificate to VSE. In this example we used the member name MYCERT.

In the job, LUSER and LPASS specify a VSE user together with its password. These parameters are necessary on order to enable the FTP client to access the VSE file system. USER and PASS specify the remote FTP user and its password as defined on the server side in section Define an FTP user in FileZilla on page 23. Remember that the remote password (PASS) is case sensitive.

Note: the interactive FTP client (CICS FTP transaction) is **not** SSL enabled.

4 Considerations on Firewalls

It is typical for company Intranets that network access is controlled by Firewalls. This implies that very often all port numbers are blocked except some very few ports which are open for use by selected Intranet applications.

When using the Keyman/VSE tool to upload a generated private key to VSE in a Firewall controlled network, port 6045 must be open, because this port is used by default by the CIALSRVR program, which receives the key material on VSE.

Regarding FTP, it is unfortunately not sufficient to for example open port 21 for unsecured FTP connections and port 990 for secure FTP connections, because the FTP protocol is based on the use of a control connection (port 21 or 990 respectively) and one or more data connections, which are opened dynamically during an FTP session when transferring data like files or even directory lists. It depends on the FTP server and client implementations, which port numbers are selected in a particular case.

To overcome this problem, most FTP servers provide the possibility to either use active or passive FTP mode.

4.1 Passive versus active FTP mode

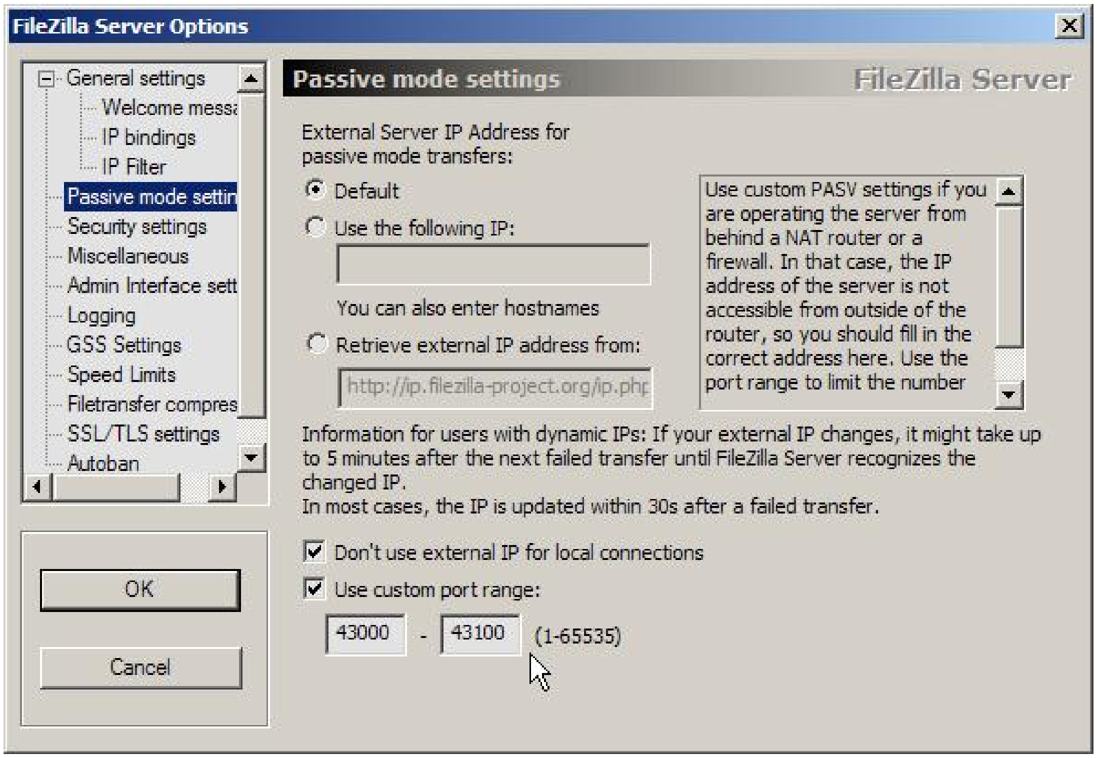
In short, active FTP mode means that the FTP client tells the FTP server which data port to use for the transfer of a given file. When the server now connects to this port, from the client’s Firewall perspective it is an incoming connection from a remote system. Passive mode is initiated by the FTP client and tells the server to specify the data port. This implies that the server must be configured to have some port numbers open for use to connect to passive FTP clients.

You can find a very good discussion of active versus passive FTP mode on

http://slacksite.com/other/ftp.html

4.2 Restricting the port range on the server side

The FileZilla server allows restricting the range of used data ports. In the **FileZilla Server Options** box select **Passive Mode Settings** and specify the range of open ports in your company Intranet.



Passive mode settings

External Server IP Address for passive mode transfers:

● Default

○ Use the following IP:

You can also enter hostnames

○ Retrieve external IP address from: http://ip.filezilla-project.org/ip.php

Use custom PASV settings if you are operating the server from behind a NAT router or a firewall. In that case, the IP address of the server is not accessible from outside of the router, so you should fill in the correct address here. Use the port range to limit the number

Information for users with dynamic IPs: If your external IP changes, it might take up to 5 minutes after the next failed transfer until FileZilla Server recognizes the changed IP.
In most cases, the IP is updated within 30s after a failed transfer.

☑ Don't use external IP for local connections

☑ Use custom port range:

43000 - 43100 (1-65535)

TCP/IP for VSE/ESA 1.5E provides a new command PORTRANGE to deal with Firewall issues. The command is described in the TCP/IP Operator Commands book that is available online at

http://www.e-vse.com/download.htm

The command can be entered at the operator console or specified in your IPINIT member and applies to all FTP servers and clients running on this VSE system.

Syntax: `PORTRange ,HIgh=num ,LOw=num`

Usage example:

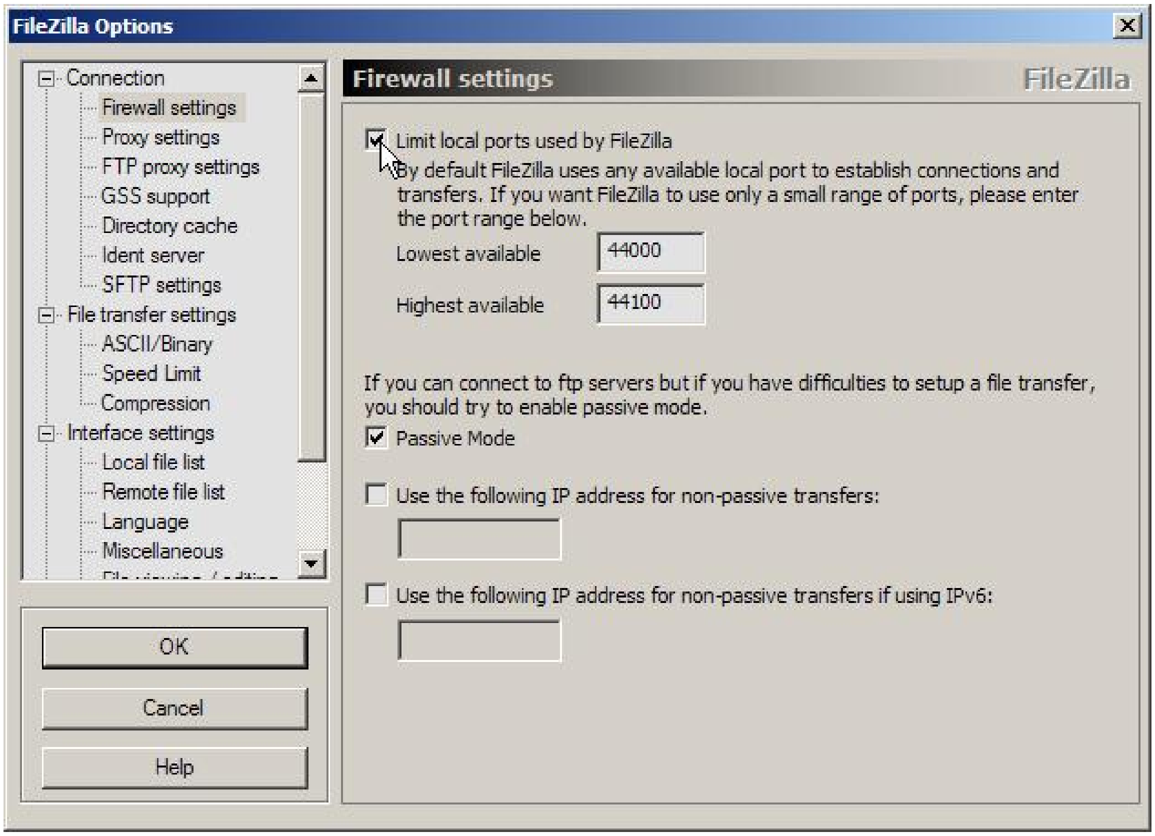
```
F7-0104 IPN300I Enter TCP/IP Command
104 PORTRANGE, LOW=4096, HIGH=65535
F7 0098 IPN127E Port range changed to 4096 65535
```

The 4096 and 65535 are the defaults if not specified. Any range with at least a 4096 difference can be used. This applies to all free port requests.

Note: as PORTRANGE is a TCP/IP command and not an FTPBATCH or FTPD parameter, the values defined here apply to the entire stack, i.e. to all FTP servers and clients.

4.3 Restricting the port range on the client side

The FileZilla client allows restricting the port range in a similar way as the server.



Firewall settings

☑ Limit local ports used by FileZilla

By default FileZilla uses any available local port to establish connections and transfers. If you want FileZilla to use only a small range of ports, please enter the port range below.

Lowest available: 44000

Highest available: 44100

If you can connect to ftp servers but if you have difficulties to setup a file transfer, you should try to enable passive mode.

☑ Passive Mode

☐ Use the following IP address for non-passive transfers:

☐ Use the following IP address for non-passive transfers if using IPv6:

If VSE acts as the client, the PORTRANGE parameter applies in the same way as for the server.

4.4 Considerations on the DATAPORT parameter

The VSE FTPBATCH application has another optional parameter to specify a data port. This parameter was also undocumented in August 2007.

```
EXEC FTPBATCH,PARM='xxx,DATAPORT=43000'
```

Our tests showed that this data port is only used for transferring files, but is e.g. not used when issuing a DIR command to the remote platform. The DIR list is transferred via another randomly selected port and with each following DIR command, the port number is increased. This means that the Firewall administrator is forced to open additional ports to get it to work.

Note: Connectivity Systems, Inc. recommends to **not** using this parameter except for exceptional conditions. It forces the FTPBATCH job to use one single specific data port, and this could cause some other problems. For example, when many incoming connections have to be handled by one DATAPORT, the port gets opened and closed in very short time intervals. This may block further connections.

For more information about VSE FTPBATCH parameters, refer to

http://www.e-vse.com/download.htm

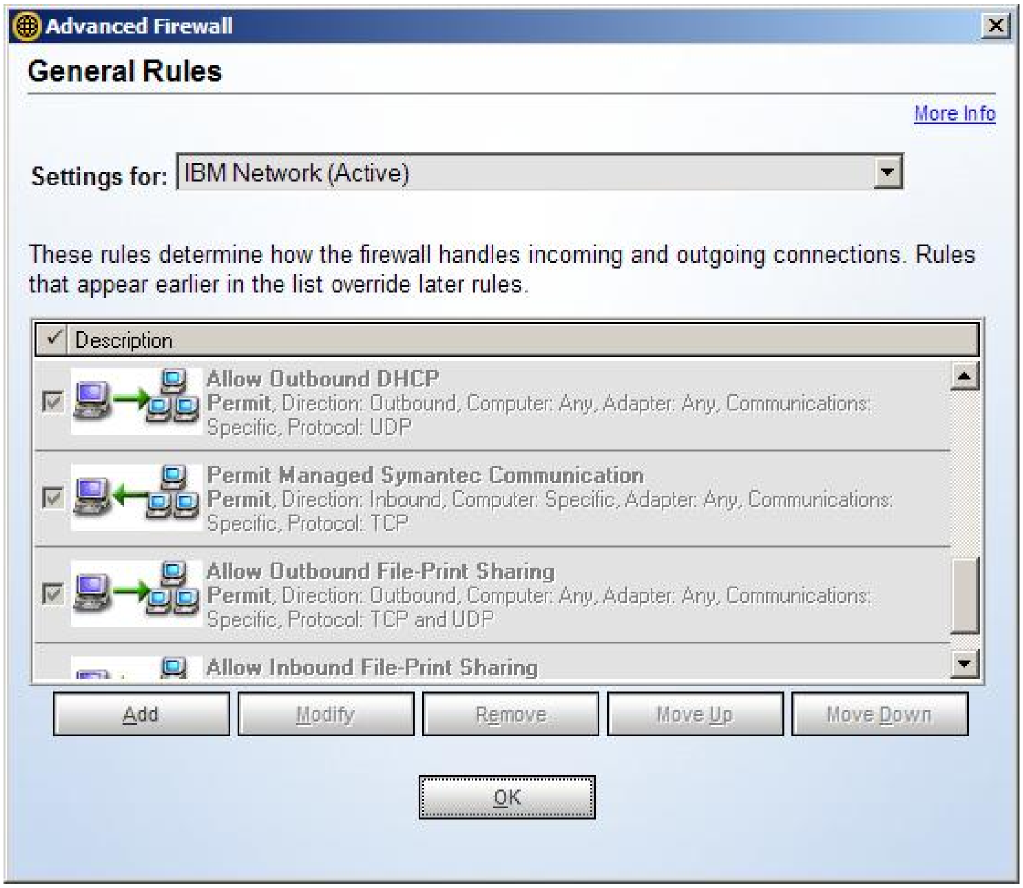
and click on

- User Guide (beta), and
- Optional Features (GPS, NFS, SSL, CAF, SecureFTP, and See-TCP/IP for VSE).

4.5 Firewall configuration

One important Firewall setting is the permission or blocking of the different IP protocols: TCP, UDP, and ICMP. At least the TCP protocol must be permitted in order to get FTP to work.

Here is an example of how the Symantec Client Firewall handles these definitions. Depending on the used Firewall product, the user interface may be different.



General Rules

Settings for: IBM Network (Active)

These rules determine how the firewall handles incoming and outgoing connections. Rules that appear earlier in the list override later rules.

✓	Description
☑	**Allow Outbound DHCP** **Permit**, Direction: Outbound, Computer: Any, Adapter: Any, Communications: Specific, Protocol: UDP
☑	**Permit Managed Symantec Communication** **Permit**, Direction: Inbound, Computer: Specific, Adapter: Any, Communications: Specific, Protocol: TCP
☑	**Allow Outbound File-Print Sharing** **Permit**, Direction: Outbound, Computer: Any, Adapter: Any, Communications: Specific, Protocol: TCP and UDP
	Allow Inbound File-Print Sharing

5 Troubleshooting

This section describes some known problems.

5.1 Cannot submit a VSE/POWER job with Keyman/VSE

Symptom:

When uploading the server certificate to VSE via Keyman/VSE, the CIALROOT job never appears in the VSE reader queue. But it is e.g. possible to display the contents of the VSE keyring library. The connection indicator at the right lower corner of the Keyman/VSE main window is green, showing that the IP connection to the VSE Connector Server is established.

Possible reason:

You are using an External Security Manager (ESM), like CA TopSecret or BIM Alert and the ESM is not correctly configured so that your VSE user can submit VSE/POWER jobs via the VSE Connector Server.

When using CA TopSecret, use following command to give your VSE user full authorization.

```
TSS ADD(user-ID) IESINIT(IESEADM) IESTYPE(USERTYPE1,NEW,SELECT)
IESFL1(BAT,PSL,COD,VSAM) IESFL2(BQA,ESC,COU,CMD,OLPD,XRM)
```

Currently I do not have any information of how to configure BIM Alert. You may disable security in the VSE Connector Server to overcome this problem. Modify job skeleton SKVCSCFG in ICCF library 59 like shown below. Then catalog the config member using job skeleton SKVCSCAT and restart the connector server.

```
; *****************************************************************
; SECURITY CONFIGURATION
; - SECURITY: FULL     - LOGON, RESOURCE AND USER TYPE CHECKING
;             RESOURCE - LOGON AND RESOURCE, BUT NO USER TYPE
;                        CHECKING.
;             LOGON    - LOGON, BUT NO RESOURCE AND USER TYPE
;                        CHECKING
;             NO       - NO LOGON, RESOURCE AND USER TYPE CHECKING
; *****************************************************************
  SECURITY = NO
```

5.2 SSL handshaking fails

Symptom:

SSL handshaking fails when connecting from FTPBATCH on VSE to FileZilla server. FileZilla shows these error messages in the FileZilla server interface window:

```
150 Opening data channel for file transfer.
Data connection SSL warning: SSL3 alert write: fatal: handshake failure
Data connection SSL warning: SSL_accept: error in SSLv3 read client hello C
```

Possible reason:

You are using TCP/IP for VSE/ESA 1.5F and some fixes are missing. Check for following 15F zaps: 244, 247, 251, 252, and 253.

6 More information

You can find more information on these web pages.

VSE Homepage
http://www.ibm.com/servers/eserver/zseries/zvse/

Keyman/VSE tool and VSE Connector Client
http://www.ibm.com/servers/eserver/zseries/zvse/downloads/

FileZilla server and client
http://filezilla-project.org/

TCP/IP Optional Features (GPS, NFS, SSL, CAF, SecureFTP, and See-TCP/IP for VSE)
http://www.csi-international.com/download.htm

z/VSE V4R2 Administration, SC33-8304
http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#vse

Discussion of FTP active and passive mode
http://slacksite.com/other/ftp.html

OpenSSL website
http://www.openssl.org/

Win32 OpenSSL installation files
http://www.slproweb.com/products/Win32OpenSSL.html