



How to setup WebSphere MQ for z/VSE V3.0 and WebSphere MQ for Windows V7.0 with secured connections using SSL/TLS

Last formatted on: Monday, February 27, 2017

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:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows XP, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

Contents

1	Introduction	5
2	Check for latest information	5
3	Installing the prerequisite programs	5
3.1	MQ installation on VSE	5
3.2	Maintaining security profiles	6
3.3	MQ installation on Windows	7
4	Configuring MQ.....	12
4.1	MQ configuration on VSE	13
4.1.1	Defining the queue manager.....	13
4.1.2	Defining the local queue.....	14
4.1.3	Defining the transmission queue	15
4.1.4	Defining the remote queue	16
4.1.5	Defining the sender channel	17
4.1.6	Defining the receiver channel.....	17
4.1.7	Defining batch communications.....	18
4.1.8	Defining Log settings	18
4.1.9	Starting MQ on VSE.....	19
4.2	MQ configuration on Windows	19
4.2.1	Defining the local queue.....	19
4.2.2	Defining the transmit queue	22
4.2.3	Defining the remote queue	23
4.2.4	Defining the sender channel	26
4.2.5	Defining the receiver channel.....	28
4.3	Testing the setup.....	30
4.3.1	Sending a test message to VSE	30
4.3.2	Sending a test message to Windows.....	32
5	Configuring for SSL/TLS	33
5.1	Creating the keys and certificates	34
5.1.1	Uploading the certificate items to VSE.....	38
5.1.2	Specifying the correct certificate label for MQ	39
5.1.3	Creating an MQ key database.....	41
5.1.4	Storing the certificate items in the MQ key database	42
5.2	SSL/TLS configuration on VSE	45
5.2.1	Configuring the queue manager for SSL/TLS	45
5.2.2	Checking for available SSL/TLS cipher suites	46
5.2.3	Configuring the channels for SSL/TLS.....	47
5.3	SSL/TLS configuration on Windows	47
5.3.1	Configuring the queue manager for SSL/TLS	47
5.3.2	Configuring the channels for SSL/TLS.....	48
6	Implementing SSL/TLS client authentication	49
6.1	Configuring for client authentication on VSE.....	49
6.2	Configuring for client authentication on Windows	49
7	Using SSL/TLS peer attributes	50
7.1	Example 1: specifying matching peer attributes	51
7.2	Example 2: specifying peer attributes which do not match	52
8	Configuring a remote queue manager	52
8.1	What you can do remotely	52
8.2	Preparing the VSE side for PCF	53
8.3	Defining additional queues	53
8.4	Defining the MQ Explorer reply model queue	54
8.5	Defining a server-connection channel	54
8.6	Defining a remote queue manager	55
8.7	Exchanging test messages	58
8.8	Defining SSL/TLS.....	60
8.8.1	Defining SSL/TLS for the Windows side	60

8.8.2	Defining SSL/TLS for the VSE side	61
9	Troubleshooting	63
9.1	Ciphers 2F and 35 do not work	63
9.2	Message sequence number error	63
9.3	RC =2092 when sending a test message to Windows	63
9.4	Open of file MQFADMIN failed	64
9.5	No space available for PUT request	64
10	More information	66

Changes

Nov, 12, 2008 – initial version.

Feb 2009 – updates for WMQ for z/VSE 3.0

March 2009 – info about remote configuration using the MQ Explorer

January 2016 – added section 2 on page 5

February 2017 – added section 9.1 on page 63

1 Introduction

This paper describes the setup of a secure connection between MQSeries for VSE and WebSphere MQ 7.0 on a Windows XP.

The following software has been used in the test setup.

- z/VSE 4.2.0 GA version
- MQSeries for VSE V2.1.2 and V3.0.0
- TCP/IP for VSE/ESA 1.5F as part of z/VSE 4.2 GA version
- VSE Connector Server as part of z/VSE 4.2 (job STARTVCS)
- Java 1.6.0 from Sun Microsystems
- MQSeries for Windows V7.0
- MQSeries for Windows Explorer V7.0 (part of MQSeries for Windows V7.0)

In fact two VSE test systems have been setup, one with MQSeries for VSE 2.1.2 and the other one with WebSphere MQ for z/VSE V3.0. In the following, the shown panels were taken from WMQ V3.0 but there is absolutely no difference in the setup compared to MQ for VSE V2.1.2.

Note: WebSphere MQ for z/VSE V3.0 is out of service since Sept 30, 2015.

2 Check for latest information

The information contained in this White Paper is also available in IBM Redbook *Security on IBM z/VSE*, SG24-7691. The book is available online at:

<http://www.redbooks.ibm.com/abstracts/sg247691.html?Open>

Check the publication dates to see which information is newer. The latest technical information in this White Paper is from February 2017.

3 Installing the prerequisite programs

Note that MQ Security cannot be activated when using the Basic Security Manager (BSM), because BSM does not support all needed CICS resource classes. For Security we would need an ESM, like CA TopSecret.

3.1 MQ installation on VSE

A detailed description of the installation of MQSeries on VSE is beyond the scope of this document. I was using Redbook “Using MQSeries for VSE, SG24-5647” and followed the steps as described in chapter 1 “Installation”. I used the following resources:

- PRD2 .MQSERIES: contains all members restored from tape
- MQ .USER .CATALOG with name MQMCAT on volume SYSWK2

After creating all necessary resources and doing all the definitions, transaction MQSU must be invoked in order to initialize the MQSeries configuration file. Before being able to invoke any MQ transaction, we have to define a generic security profile to the Basic Security Manager (BSM).

The next section shows how all MQ transactions, starting with the two letters MQ, are defined to the BSM via a generic security profile. Further transactions, like the TST2 transaction used to send some test messages, must be defined in the same way.

3.2 Maintaining security profiles

Enter dialog “Maintain Transaction Profiles” (fastpath 2.8.1.1) and add a new security profile.

```

IESADMBSLE                MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:      TCICSTRN                ACTIVE
START...                  (CASE SENSITIVE)
OPTIONS:  1 = ADD          2 = CHANGE          5 = DELETE          6 = ACCESS LIST

   OPT      PROFILE NAME                DESCRIPTION                UNIVERSAL AUDIT
   1        ftp                    IBM SUPPLIED                ACCESS VALUE
   -        iccf                    IBM SUPPLIED                22
   -        lpr                      IBM SUPPLIED                12

PF1=HELP                3=END
PF7=BACKWARD          8=FORWARD          9=PRINT
    
```

Define a generic profile MQ* as shown below.

```

IESADMBSAE                MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:      TCICSTRN

Add Profile:

PREFIX.....              _____          CICS region

RESOURCE NAME.....  MQ
                        Maximum length is 4 characters.

GENERIC.....  1
                        (1=yes, 2=no)

UNIVERSAL ACCESS...  _
                        (_=None, 2=Read, 3=Update, 4=Alter)

AUDIT-LEVEL 1 .....  1
ACCESS-LEVEL 1 .....  2
                        (_=None, 1=Failure, 2=Success, 3=All)
                        (2=Read, 3=Update, 4=Alter, _=default)

AUDIT-LEVEL 2 .....
ACCESS-LEVEL 2 .....
DESCRIPTION.....  IBM SUPPLIED
                        Optional remark
PF1=HELP                3=END                5=UPDATE
    
```

Define an access list for the generic profile.

```

IESADMBSLE                MAINTAIN SECURITY PROFILES
BSM RESOURCE CLASS:      TCICSTRN                ACTIVE
START... M                (CASE SENSITIVE)
OPTIONS:  1 = ADD          2 = CHANGE          5 = DELETE          6 = ACCESS LIST

   OPT      PROFILE NAME                DESCRIPTION                UNIVERSAL AUDIT
   6        *MQ                    IBM SUPPLIED                ACCESS VALUE
   -        NEWC                    IBM SUPPLIED                12
   -        OLPD                    IBM SUPPLIED                12

PF1=HELP                3=END
PF7=BACKWARD          8=FORWARD          9=PRINT
    
```

Press **Enter**.

```

IESADMBSLA                MAINTAIN ACCESS LIST
BSM   CLASS: TCICSTRN     PROFILE: MQ
START....                NUMBER OF ENTRIES ON LIST: 00000
OPTIONS:  1 = ADD         2 = CHANGE         5 = DELETE

      OPT   NAME   ACC

      1

PF1=HELP                 3=END
PF7=BACKWARD            8=FORWARD

```

Enter option **1** (Add) and press **Enter**. Now add the profile to GROUP01 with access 2.

```

IESADMBSAA                MAINTAIN ACCESS LIST
BSM   CLASS: TCICSTRN     PROFILE: MQ

Add Userid or Groupid:

      NAME..... GROUP01           Userid or Groupid

      ACCESS..... 2                (_=None,
                                   2=Read, 3=Update, 4=Alter)

PF1=HELP                 3=END                 5=UPDATE

```

Press **PF5** (Update). You must then rebuild the security tables via dialog 2.8.3

Now the MQSU transaction can be invoked. An output similar to the below should be displayed.

```
MQSU: MQSeries install completed, 6457 input records read.
```

3.3 MQ installation on Windows

A 90-days trial version of WebSphere MQ V7.0 has been downloaded from

<https://www14.software.ibm.com/webapp/dswdown/dswdown.wss/web/searchDescription>

The install file WMQv700Trial-x86_nt.zip comprises about 569 MB.

Launching the setup.exe shows an install dialog that allows checking for some prerequisites:

- Windows XP + SP2
- WebSphere Eclipse Platform V3.3

On the Network Configuration tab I selected NO.

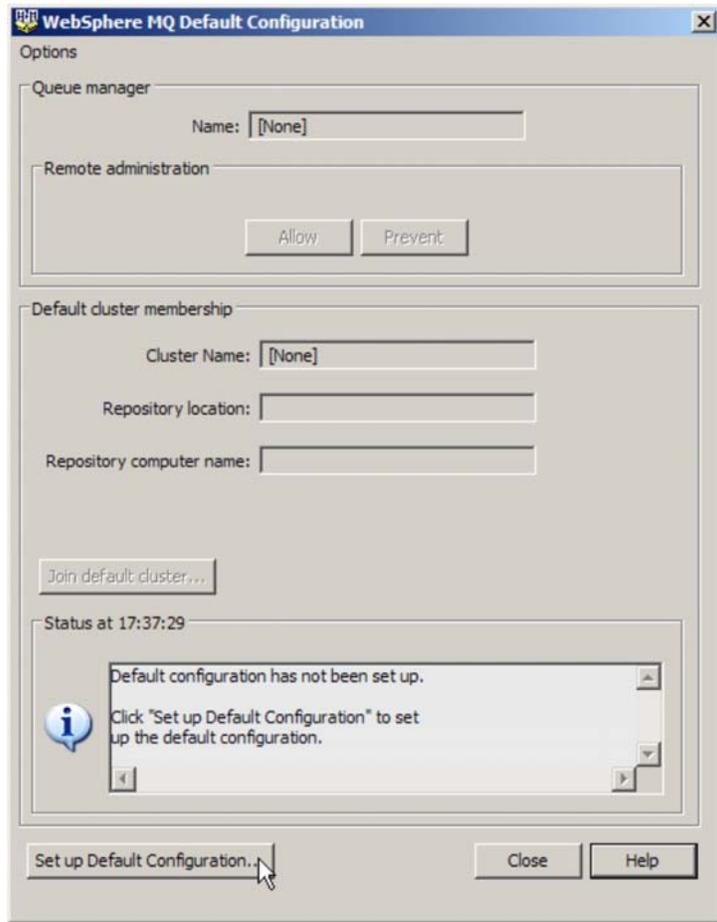
Note: If WebSphere Eclipse Platform is not installed on your PC, you can install it from the downloaded WebSphere MQ package. “WebSphere Eclipse” must not be mixed up with the standard “Eclipse” IDE as downloaded from www.eclipse.org.

Enter directory Prereqs/IES and launch the setup.exe. This is also described on following web page:

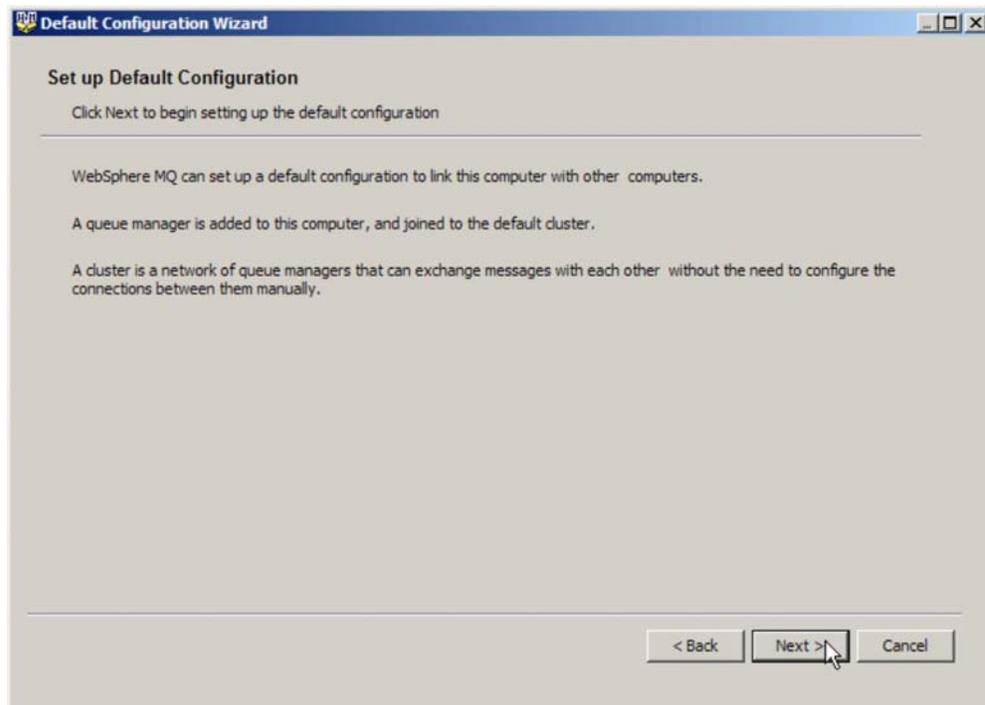
<http://www.ibm.com/support/docview.wss?uid=swg21206995>

After installing WebSphere Eclipse, WebSphere MQ 7.0 can now be installed. After copying files, WebSphere MQ does some network configuration.

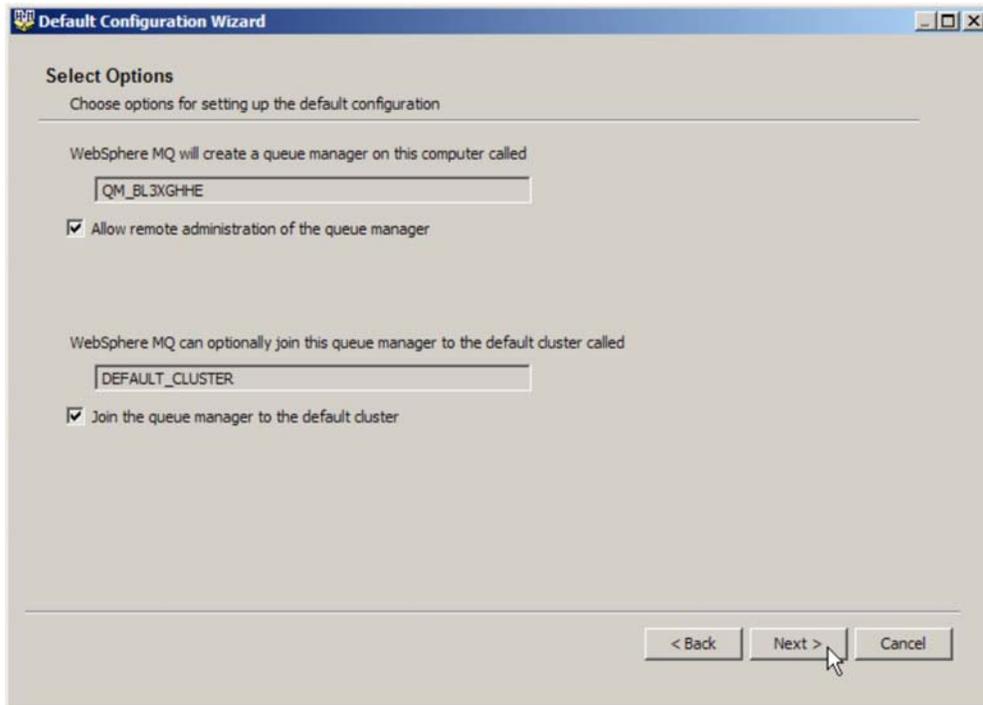
I again answered NO to the question if there are any domain controllers running Windows 2000



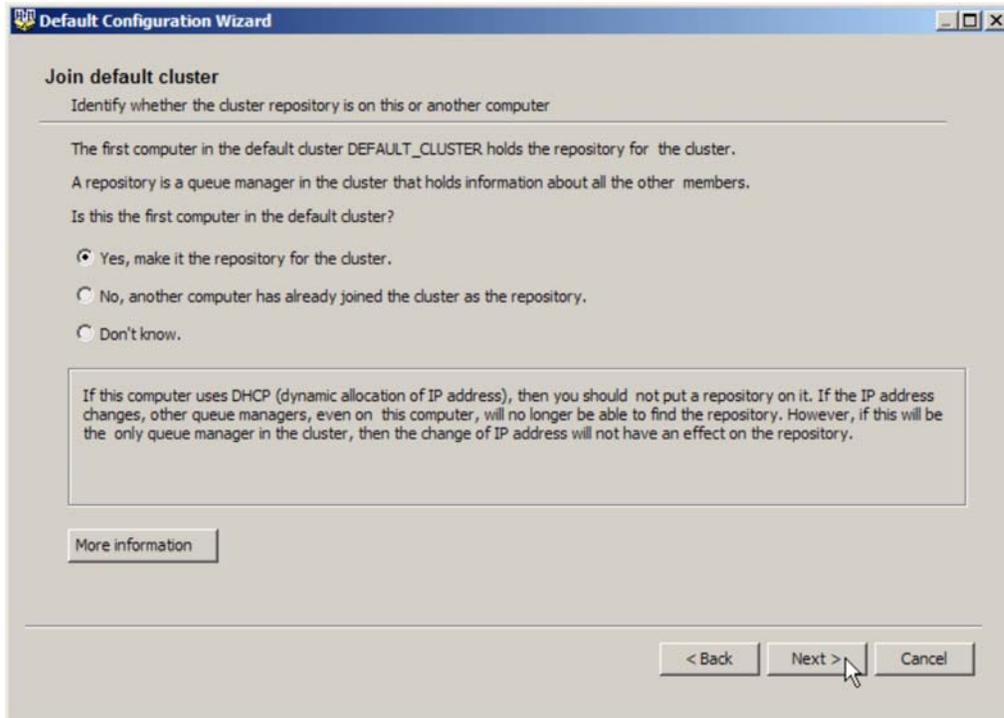
Click button **Setup Default Configuration**.



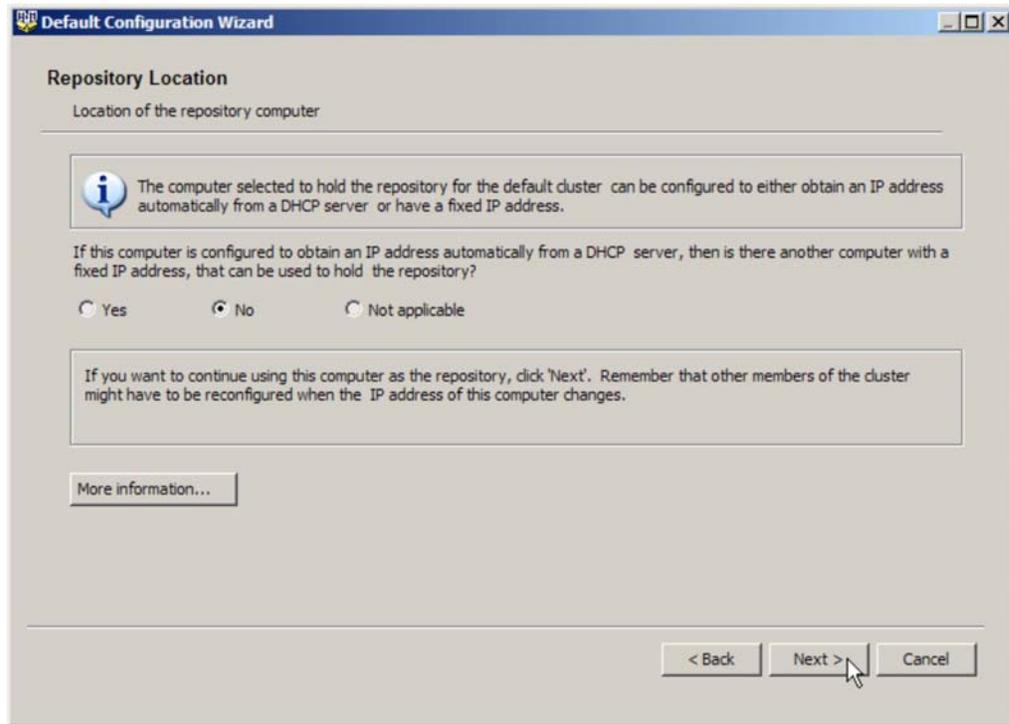
Press **Next**.



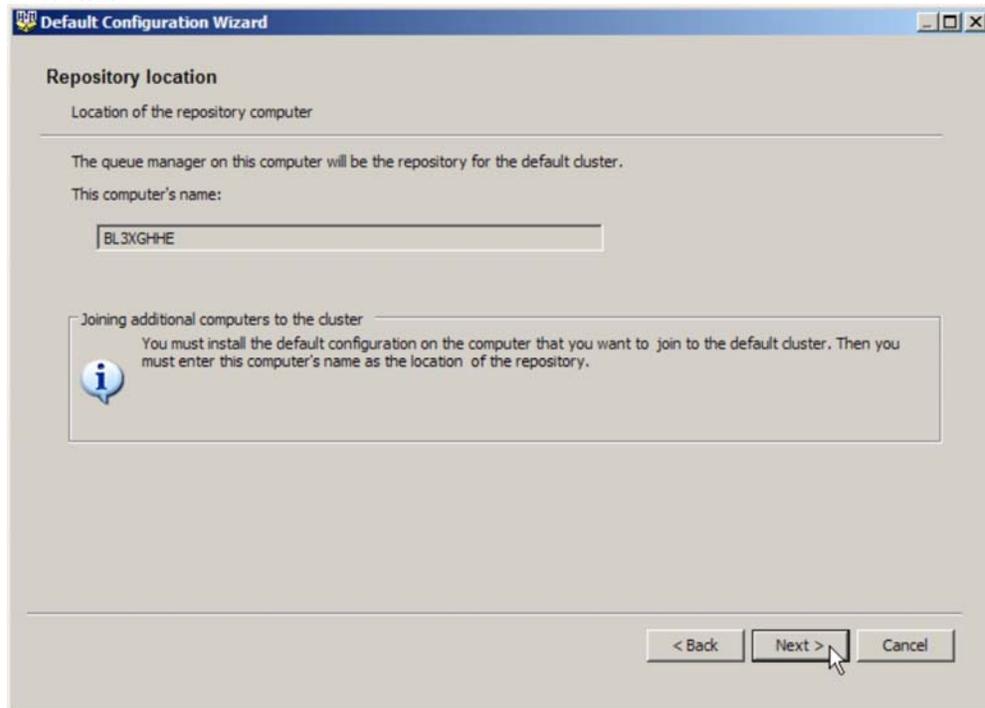
Press **Next**.



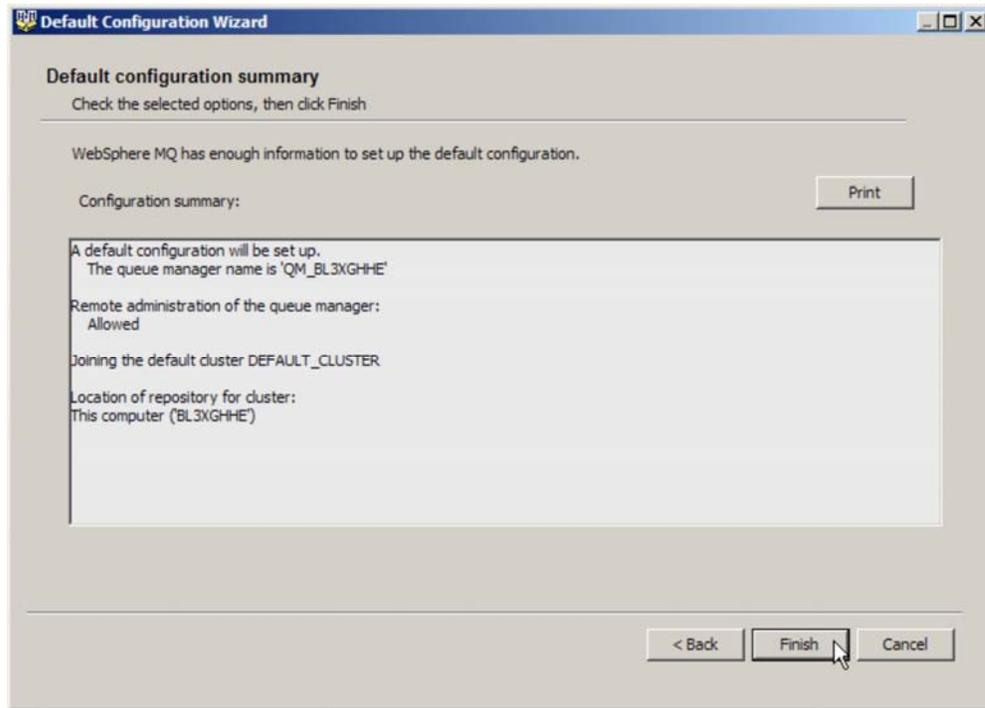
Press **Next**.



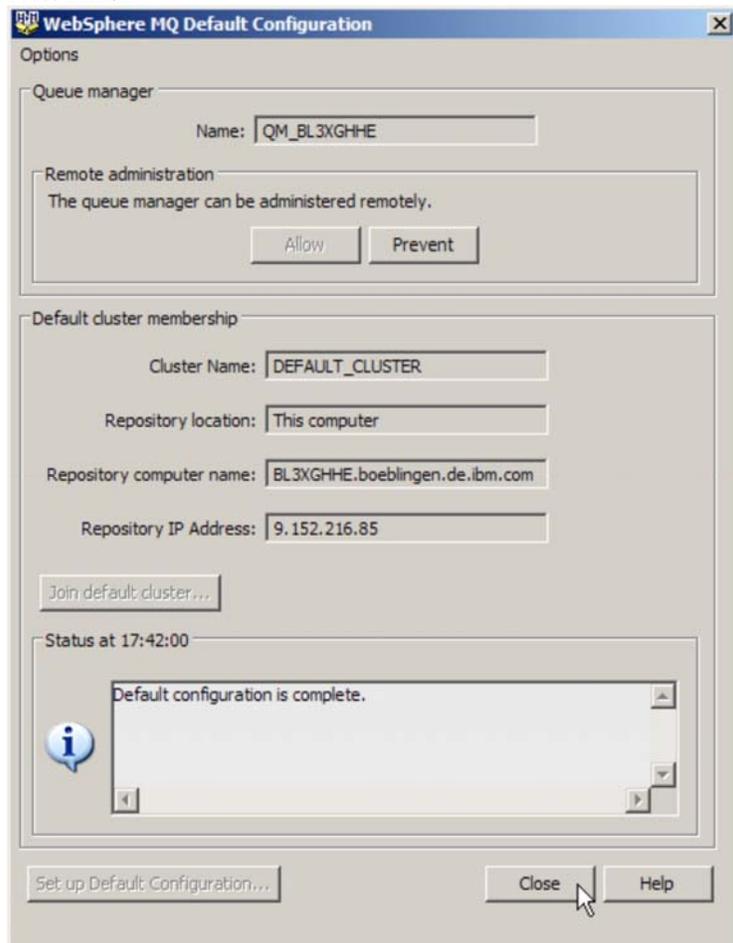
Press Next.



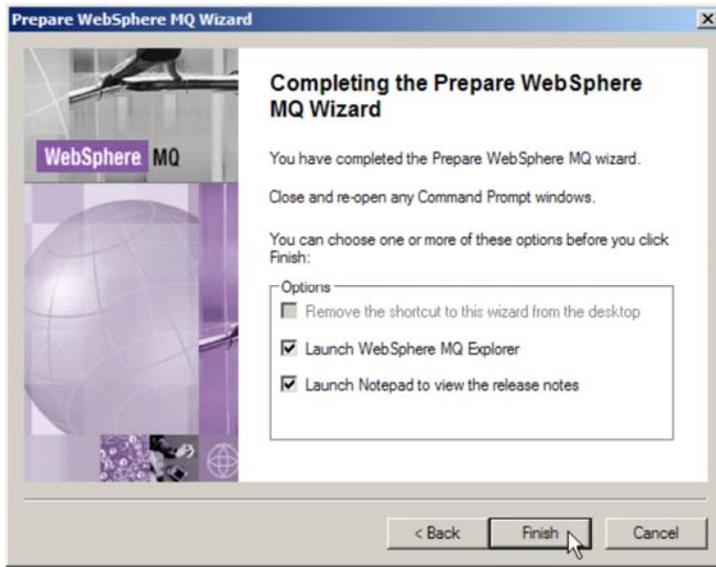
Press Next.



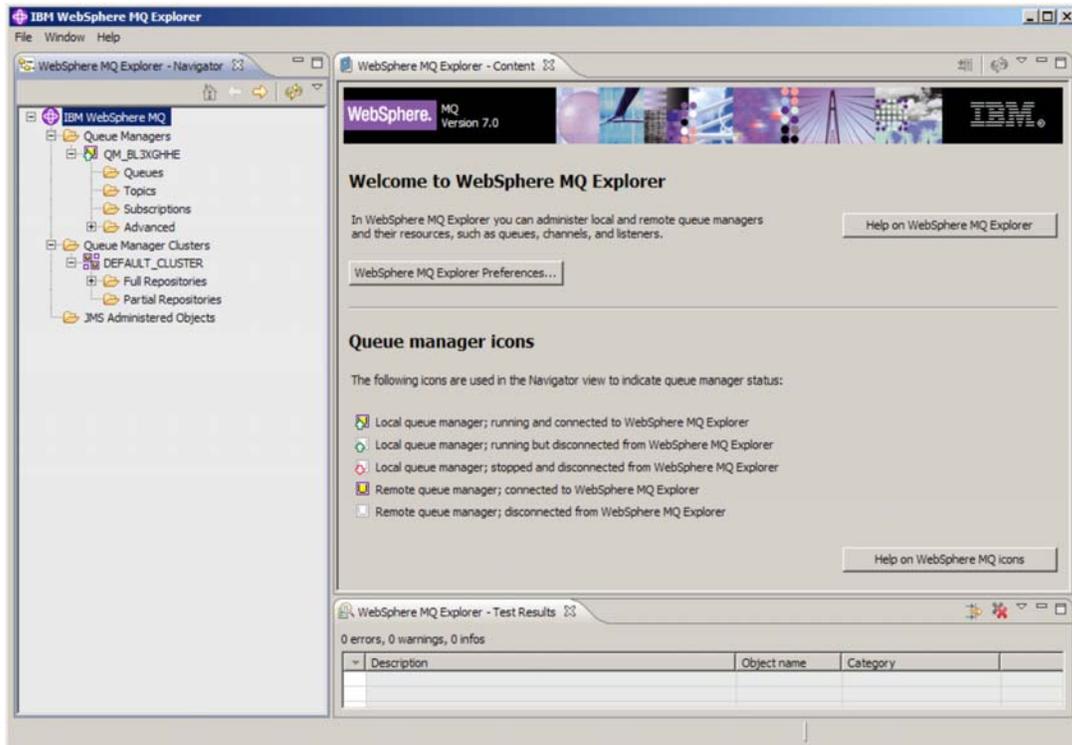
Press **Finish**.



Now the default configuration is complete. Press **Close**.



Press **Finish** to launch the WebSphere MQ Explorer.



4 Configuring MQ

This chapter describes how to configure MQ on both sides.

4.1 MQ configuration on VSE

As described in Redbook “Using MQSeries for VSE” in section 1.4 “Initial configuration”, we have to

- Define the VSE queue manager
- Define the system queues
- Define the sender and receiver channels

There is a good picture in Redbook “WebSphere V5 for Linux on zSeries Connectivity Handbook - SG24-7042”, Chapter 8, section 8.4, showing the relations of the various queues and channels.

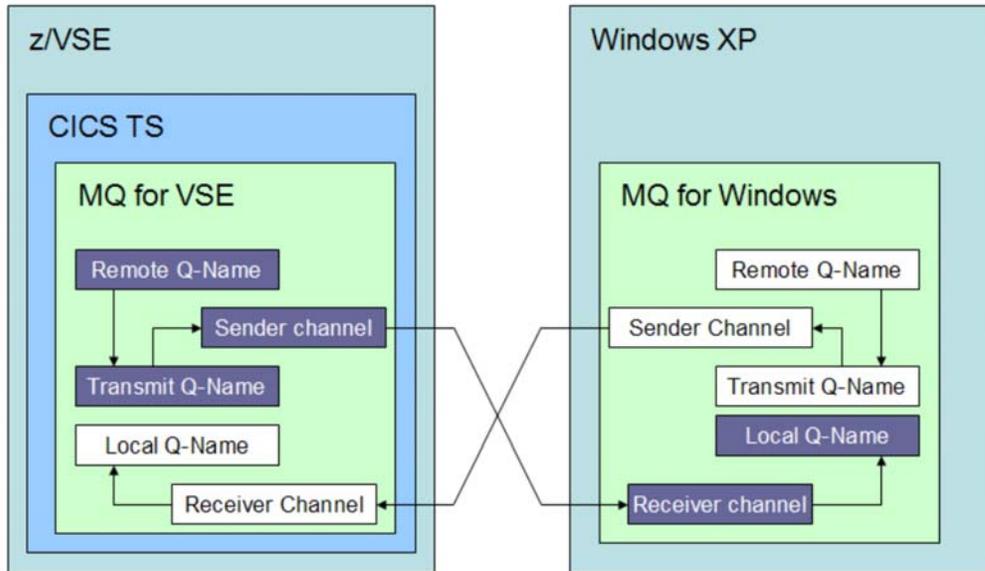


Figure 1: MQ queues and channels

We will use the following names for the various queues and channels:

	VSE	Windows
Queue Manager	QMGR.VSE	QM_BL3XGHHE
Local Q-Name	VSE42	WINXP
Remote Q-Name	WINXP	VSE42
Transmit Q-Name	XMT.WINXP	XMT.VSE42
Sender channel	VSE.TO.WIN	WIN.TO.VSE
Receiver channel	WIN.TO.VSE	VSE.TO.WIN

Table 1: MQ queue and channel names

First we have to establish the MQSeries environment in CICS via the MQSE transaction. At this point you should have made the necessary security definitions as described in MQ installation on VSE on page 5.

4.1.1 Defining the queue manager

After running MQSE, you can now invoke the MQ Master terminal transaction MQMT to define the VSE queue manager. Select option **1** (Configuration) and again option **1** (Global System Definition).

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:17:41              Global System Definition              CIC1
MQWMSYS              Queue Manager Information              A000
Queue Manager . . . . . : QMGR.VSE
Description Line 1. . . . . :
Description Line 2. . . . . :
                Queue System Values
Maximum Connection Handles.: 00000100      System Wait Interval : 00000030
Maximum Concurrent Queues .: 00000100      Max. Recovery Tasks  : 0000
Allow TDQ Write on Errors  : Y      CSMT      Local Code Page . . : 01047
Allow Internal Dump . . . . : Y      Subsystem id . . . . : MQV1
                Queue Maximum Values
Maximum Q Depth . . . . . : 00100000      Maximum Global Locks.: 00001000
Maximum Message Size. . . . : 00002048      Maximum Local Locks .: 00001000
Maximum Single Q Access . . : 00000100
                Global QUEUE /File Names
Configuration File. : MQFCNFG
LOG Queue Name. . . : SYSTEM.LOG
Dead Letter Name. . : SYSTEM.DEAD.LETTER.QUEUE
Monitor Queue Name. : SYSTEM.MONITOR

Requested record displayed.
PF2=Return PF3=Quit PF4/Enter=Read      PF9=Com PF10=Log PF11=Evt PF12=Ext

```

At this point we just define the Queue Manager name and keep all other defaults.

Press **PF6** to permanently update your queue manager definition.

4.1.2 Defining the local queue

Define the local queue via MQMT, option 1.2.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:19:05              Queue Main Options              CIC1
MQWMQQUE              SYSTEM IS ACTIVE              A000

                Default Q Manager. : QMGR.VSE

Object Type. . . . . :      L = Local Queue
                        M = Model Queue
                        R = Remote Queue
                        AQ = Alias Queue
                        AM = Alias Queue Manager
                        AR = Alias Reply Queue

Object Name. . . . . : VSE42

PF2=Return PF3=Quit PF4/Enter=Read PF5=Add PF6=Update
                        PF9=List PF12=Delete

```

Press **PF5** (Add) to continue.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:18:44              Queue Definition Record              CIC1
MQWMQQUE        QM - QMGR.VSE                              A000

                Local Queue Definition

Object Name. . . . . : VSE42
Description line 1 . . . . :
Description line 2 . . . . :

Put Enabled . . . . . : Y   Y=Yes, N=No
Get Enabled . . . . . : Y   Y=Yes, N=No

Default Inbound status . . : A   A=Active,I=Inactive
      Outbound status. . : A   A=Active,I=Inactive

Dual Update Queue. . . . . :

Automatic Reorganize (Y/N) : N   Start Time: 0000 Interval: 0000
VSAM Catalog . . . . . :

PF2=Return  PF3=Quit  PF4/Enter=Read  PF5=Add  PF6=Update
                                PF9=List  PF10=Queue  PF12=Delete
    
```

Press **PF5** to get to the queue extended definition panel.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:20:55              Queue Extended Definition              CIC1
MQWMQQUE        A000

Object Name: VSE42

General          Maximums          Events
Type . . . : Local      Max. Q depth . . : 00100000  Service int. event: N
File name . : MQFI001  Max. msg length: 00002048  Service interval . : 00000000
Usage . . . : N         Max. Q users . . : 00000100  Max. depth event . : N
Shareable . : Y         Max. gbl locks : 00001000  High depth event . : N
Dist.Lists . : Y        Max. lcl locks : 00001000  High depth limit . : 000
                                           Low depth event . . : N
                                           Low depth limit . . : 000

Triggering
Enabled . . : N         Transaction id.:
Type . . . . :          Program id . . :
Max. starts: 0001      Terminal id . . :
Restart . . : N        Channel name . . :
User data . . :
:

PF2=Return  PF3=Quit  PF4/Enter=Read  PF5=Add  PF6=Update
          PF9=List  PF10=Queue
    
```

During the MQ installation several VSAM files have been created that can be used for the various queues. Enter the name of a VSAM file to be used for this queue (e.g. MQFI001) and press **PF5** again to finish.

4.1.3 Defining the transmission queue

Use MQMT, path 1.2 to add another local queue with name XMT.WINXP. Press **PF5** to get to the below panel.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
09:52:02              Queue Definition Record              CIC1
MQWMQUE        QM - QMGR.VSE                              A000

                Local Queue Definition

Object Name. . . . . : XMT.WINXP
Description line 1 . . . . . :
Description line 2 . . . . . :

Put Enabled . . . . . : Y   Y=Yes, N=No
Get Enabled . . . . . : Y   Y=Yes, N=No

Default Inbound status . . . : A   A=Active,I=Inactive
      Outbound status. . . : A   A=Active,I=Inactive

Dual Update Queue. . . . . :

Automatic Reorganize (Y/N) : N   Start Time: 0000 Interval: 0000
VSAM Catalog . . . . . :

PF2=Return  PF3=Quit  PF4/Enter=Read  PF5=Add  PF6=Update
                        PF9=List  PF10=Queue  PF12=Delete
    
```

Press **PF10** (Queue) to get to the queue extended definition panel.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
09:49:51              Queue Extended Definition              CIC1
MQWMQUE        A000

Object Name: XMT.WINXP

General          Maximums          Events
Type . . . : Local      Max. Q depth . . : 00100000  Service int. event: N
File name  : MQF0001    Max. msg length: 00002048  Service interval  : 00000000
Usage . . . : T         Max. Q users . . : 00000100  Max. depth event  : N
Shareable  : Y         Max. gbl locks  : 00001000  High depth event  : N
Dist.Lists : Y         Max. lcl locks  : 00001000  High depth limit  : 000
                                           Low depth event . : N
                                           Low depth limit . : 000

Triggering
Enabled . . : Y         Transaction id.:
Type . . . : E         Program id . . : MQPSEND
Max. starts: 0001     Terminal id . . :
Restart . . : N       Channel name . : VSE.TO.WIN
User data :
:
PF2=Return  PF3=Quit  PF4/Enter=Read  PF5=Add  PF6=Update
                        PF9=List  PF10=Queue
    
```

Change the USAGE parameter to T (transmission). Press **PF5** to finally add the new queue.

4.1.4 Defining the remote queue

Now let's define the remote queue for processing outgoing messages to Windows. Use MQMT path 1.2 to define a remote queue with name WINXP. Press **PF5** to get to the below panel.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:22:41              Queue Definition Record              CIC1
MQWMQUE        QM - QMGR.VSE                              A000

                Remote Queue Definition

Object Name. . . . . : WINXP
Description line 1 . . . . :
Description line 2 . . . . :

Put Enabled . . . . . : Y   Y=Yes, N=No
Get Enabled . . . . . : Y   Y=Yes, N=No

Remote Queue Name. . . . . : WINXP
Remote Queue Manager Name. : QM_BL3XGHHE
Transmission Queue Name. . : XMT.WINXP

PF2=Return  PF3=Quit  PF4/Enter=Read  PF5=Add  PF6=Update
                PF9=List  PF12=Delete
    
```

Enter the system specific parameters for Remote Queue Name, Remote Queue Manager Name, and Transmission Queue name.

Press **PF5** to add the remote queue.

4.1.5 Defining the sender channel

Channels are defined via MQMT, options **1** (Configuration) and **3** (Channel Definitions).

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:24:03              Channel Record                      CIC1
MQWMCHN          A000

Channel : VSE.TO.WIN
Desc. . : SENDER CHANNEL TO WINXP
Protocol: T (L/T)  Type : S (S=Snd/R=Rcv/V=Srv/Q=Req/C=svrConn)  Enabled : Y

Sender/Server
Remote TCP/IP port . . . . : 01414      Short/Long retry count . . : 00000000
Get retry number . . . . . : 00000000  Short retry interval . . . : 00000000
Get retry delay (secs) . . . : 00000000  Long retry interval . . . : 00000000
Convert msgs (Y/N) . . . . . : N        Batch interval . . . . . : 00000000
Transmission queue name. . . : XMT.WINXP
TP name. . . . . :

Sender/Receiver/Server/Requester
Connection : 9.152.222.125
Max Messages per Batch . . . : 000001   Message Sequence Wrap . . . : 000999999
Max Message Size . . . . . : 0002048   Dead letter store (Y/N) . . : N
Max Transmission Size . . . . : 032766   Split Msg (Y/N) . . . . . : N
Max TCP/IP Wait . . . . . : 000000

F2=Return  PF3=Quit  PF4=Read  PF5=Add  PF6=Upd  PF9=List  PF10=SSL  PF11=Ext  PF12=Del
    
```

Parameter “Connection” specifies the IP address of the Windows PC. It should have a static IP address. When using DHCP, make sure you always have the same IP address. Parameter **Message sequence wrap** must match with the corresponding definition on Windows, refer to section Defining the receiver channel on page 28.

4.1.6 Defining the receiver channel

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:24:42              Channel Record                          CIC1
MQWMCHN              A000
Channel   : WIN.TO.VSE
Desc.    : RECEIVER CHANNEL FROM WINXP TO VSE
Protocol: T (L/T)   Type : R (S=Snd/R=Rcv/V=Srv/Q=Req/C=svrConn) Enabled : Y

Sender/Server
Remote TCP/IP port . . . . : 01414      Short/Long retry count . . : 00000000
Get retry number . . . . : 00000002    Short retry interval . . . : 00000000
Get retry delay (secs) . . : 00000010  Long retry interval . . . : 00000000
Convert msgs(Y/N) . . . . : N          Batch interval . . . . . : 00000000
Transmission queue name. . :
TP name. . . . .

Sender/Receiver/Server/Requester
Connection :
Max Messages per Batch . . . : 000050    Message Sequence Wrap . . . : 000999999
Max Message Size . . . . . : 0002048    Dead letter store(Y/N) . . : N
Max Transmission Size . . . : 032766     Split Msg(Y/N) . . . . . : N
Max TCP/IP Wait . . . . . : 000000

PF2=Return PF3=Quit PF4=Read PF5=Add PF6=Upd PF9=List PF10=SSL PF11=Ext PF12=Del
    
```

Press **PF5** to add the new definition. Parameter **Message sequence wrap** must match with the related value in the sender channel on Windows, refer to section Defining the sender channel on page 26.

4.1.7 Defining batch communications

Batch communications are necessary when you want to access MQ from batch.

Start MQMT and enter options **1** (Configuration) and **1** (Global System Definition). Then press **PF9** (PF9=Comms).

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:25:32              Global System Definition                CIC1
MQWMSYS              Communications Settings                  A000

TCP/IP settings                      Batch Interface settings
TCP/IP listener port : 01414          Batch Int. identifier: MQBISERV
Licensed clients . . . : 00000        Batch Int. auto-start: Y
Adopt MCA . . . . . : N
Adopt MCA Check . . . : N             Channel Auto-Definition
                                        Auto-definition . . . : Y
                                        Auto-definition exit :

SSL parameters
Key-ring sublibrary : CRYPTO.KEYRING
Key-ring member . . : MQ02

PCF parameters
System command queue : SYSTEM.ADMIN.COMMAND.QUEUE
System reply queue . : SYSTEM.ADMIN.REPLY.QUEUE
Cmd Server auto-start: N
Cmd Server convert . : N
Cmd Server DLQ store : N

PF2=Queue Manager details PF3=Quit PF4/Enter=Read PF6=Update
    
```

Specify **Y** for batch auto-start, adopt MCA, and adopt MCA check. Then press **PF6** to update the definition.

4.1.8 Defining Log settings

Sometimes it is convenient to have all MQ messages on the operator console. To define the Log settings, start MQMT, path 1.1 and press **PF10**. Column "C" specifies whether MQ messages are written to the console also.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:26:03      Global System Definition                      CICI1
MQWMSYS       Log and Trace Settings                        A000

      Log Settings      Q C      Trace Settings

Informational . . . . : Y Y      MQI calls . . . . . : N
Warning . . . . . : Y Y      Communication . . . . : N
Error . . . . . : Y Y      Reorganization . . . . : N
Critical . . . . . : Y Y      Data conversion . . . . : N
      System . . . . . : N

      - and/or -

Communication . . . . : Y Y
Reorganization . . . . : Y Y
System . . . . . : Y Y

PF2=Queue Manager details  PF3=Quit  PF4/Enter=Read  PF6=Update

```

4.1.9 Starting MQ on VSE

Now MQ can be started on VSE via MQMT, option **2** (Operations) and **4** (Initialization / Shutdown of System). You should get the following messages on the console.

```

MQI0030I - WMQ for z/VSE system starting
MQI0035I - WMQ for z/VSE licensed support for      0000 clients
MQI0040I - WMQ for z/VSE system started
MQI0200I - MQI000000I Queue manager started
MQI0200I - MQI006041I TCP/IP listener started
MQI0100I - WMQ Batch Interface (MQBISERV) started

```

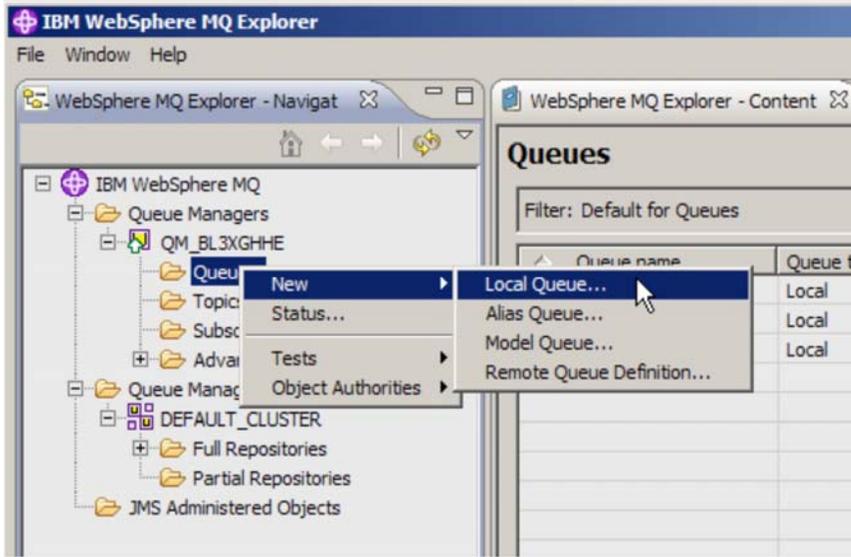
You should now check the CICS job output for any security violations, caused by transactions not defined to BSM.

4.2 MQ configuration on Windows

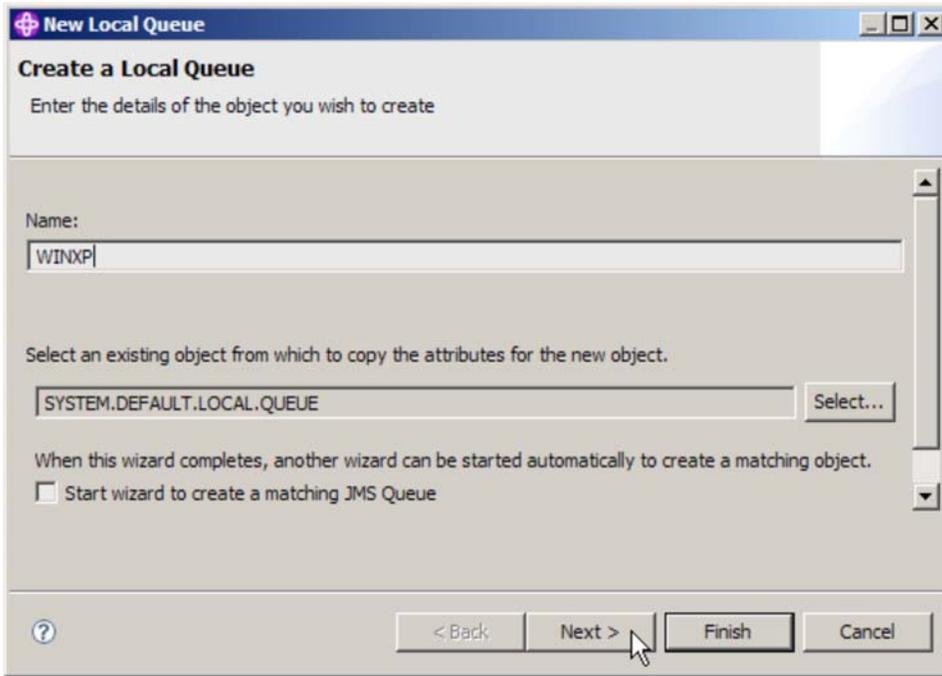
Basic network configuration was already done during the WebSphere MQ installation. Now start the MQ Explorer to continue with the VSE specific definitions.

4.2.1 Defining the local queue

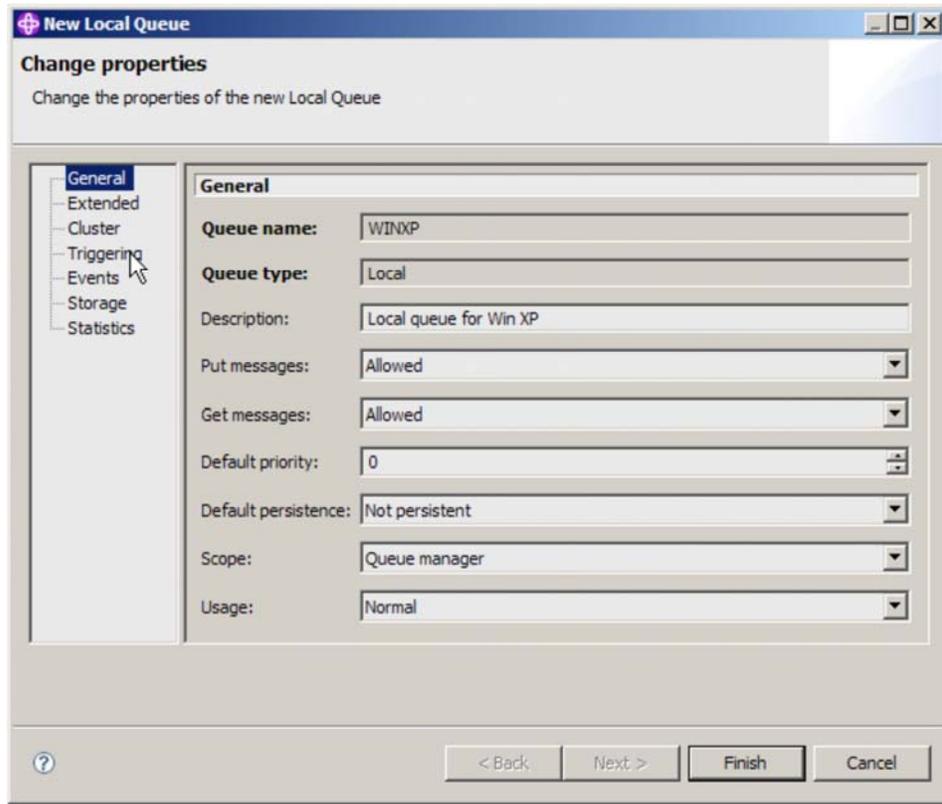
Select **Queues - New - Local Queue**.



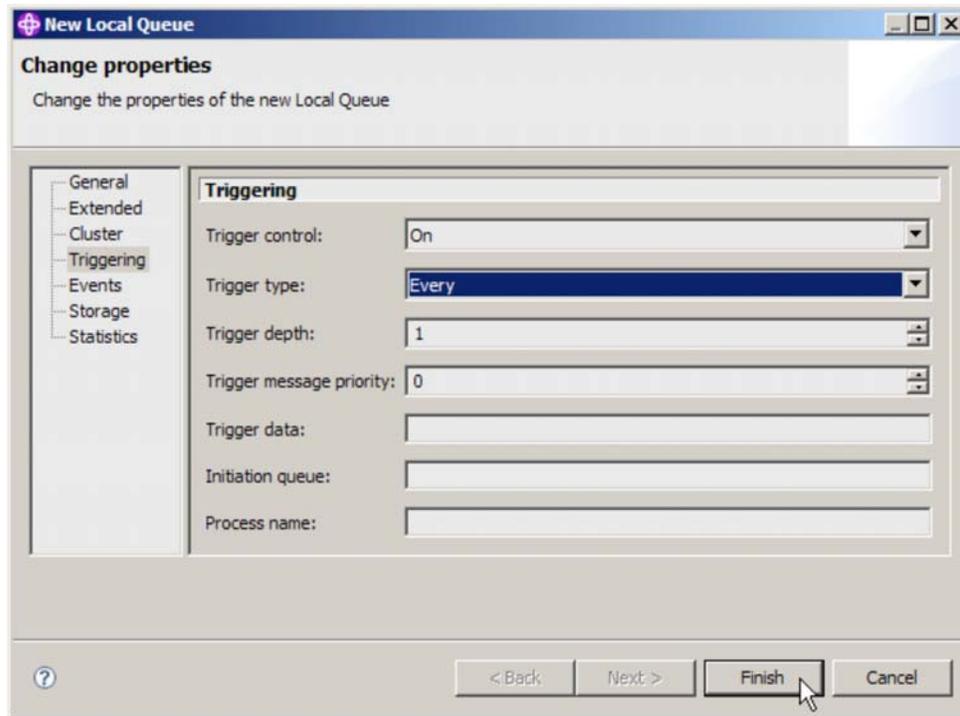
Enter the local queue name **WINXP**.



Press **Next**.



Select **Triggering**.

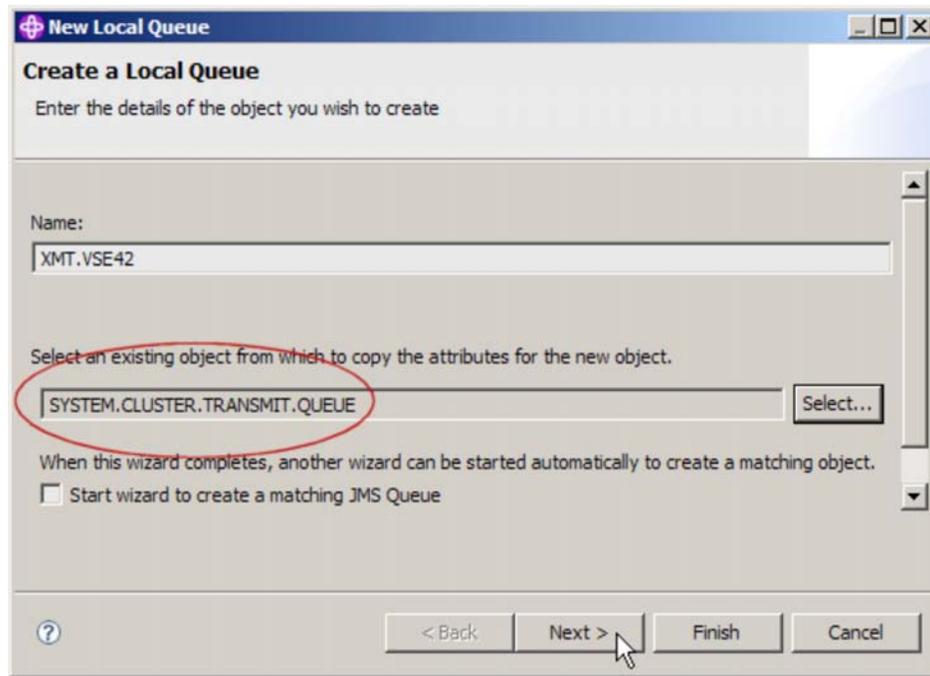


Select Trigger control **On** and Trigger type **Every**.

Press **Finish**.

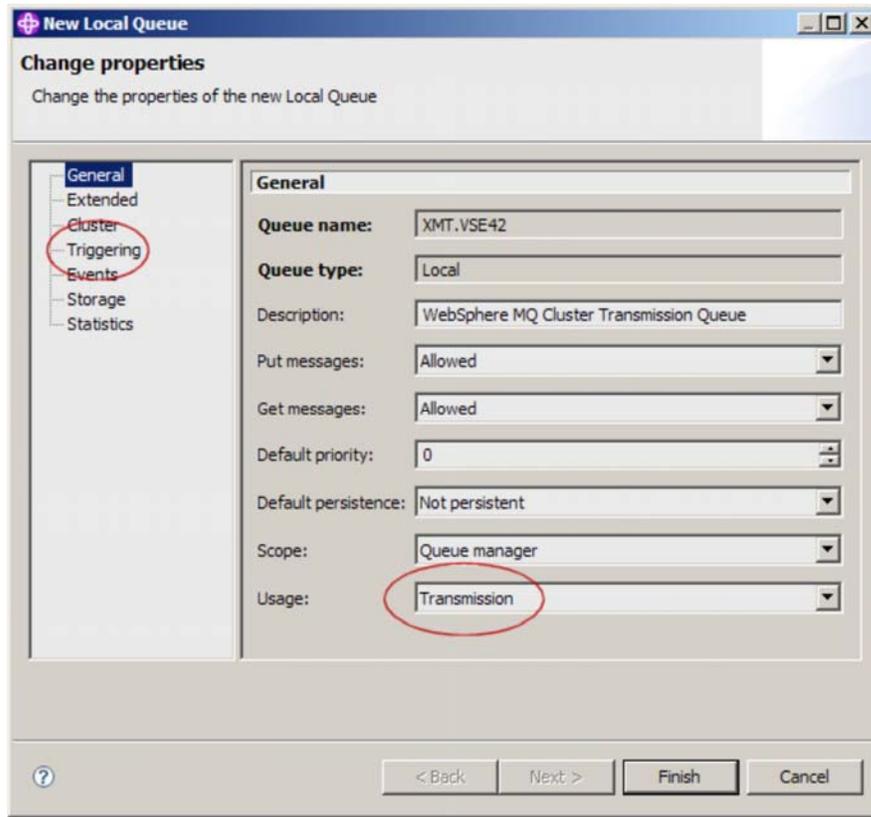
4.2.2 Defining the transmit queue

Select **Queues – New – Local queue**.

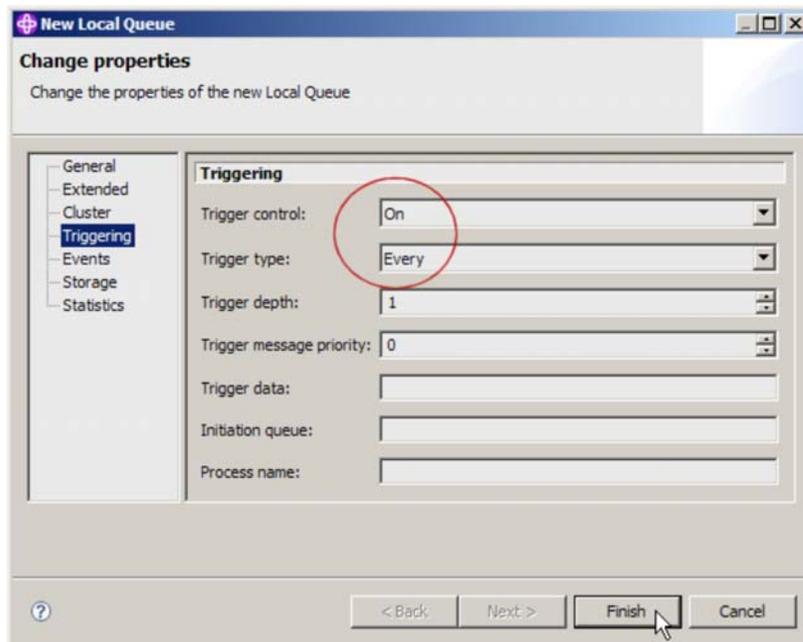


Press the **Select** button and select `SYSTEM.CLUSTER.TRANSMIT.QUEUE` as the model for the queue. Then enter the name of the transmit queue: **XMT.VSE42**

Press **Next**.



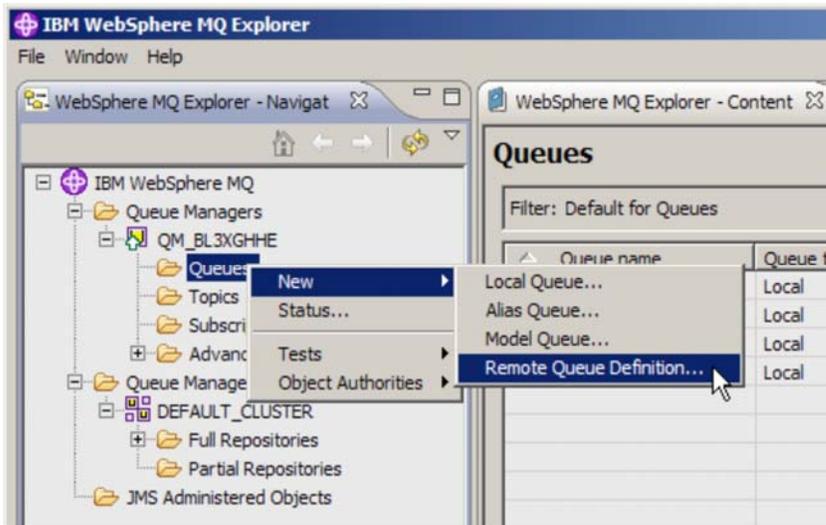
Usage should display **Transmission**. Then select the **Triggering** tab.



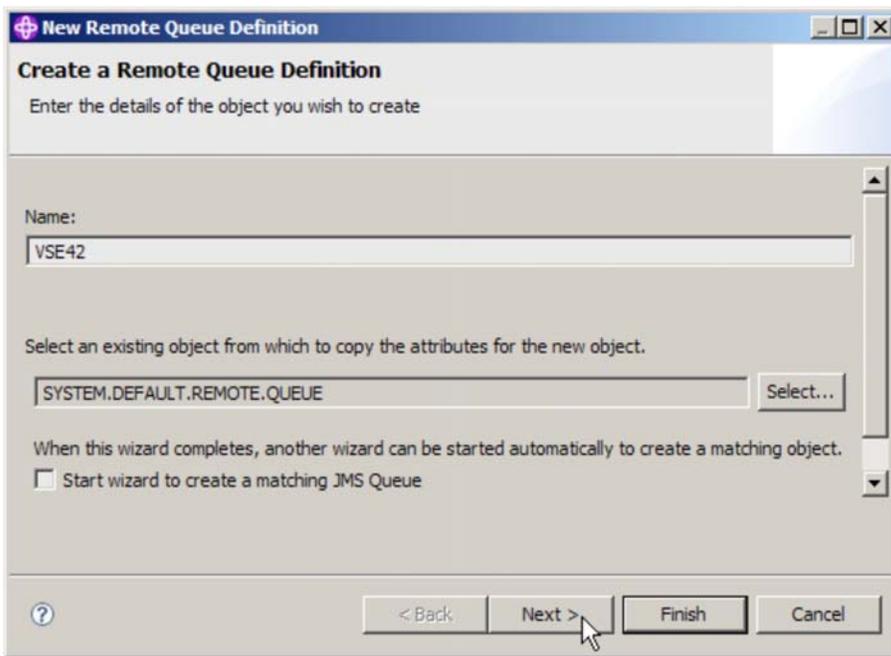
On tab Triggering specify Trigger control **On** and Trigger type **Every**. Press **Finish**.

4.2.3 Defining the remote queue

Select **Queues - New - Remote Queue Definition**.

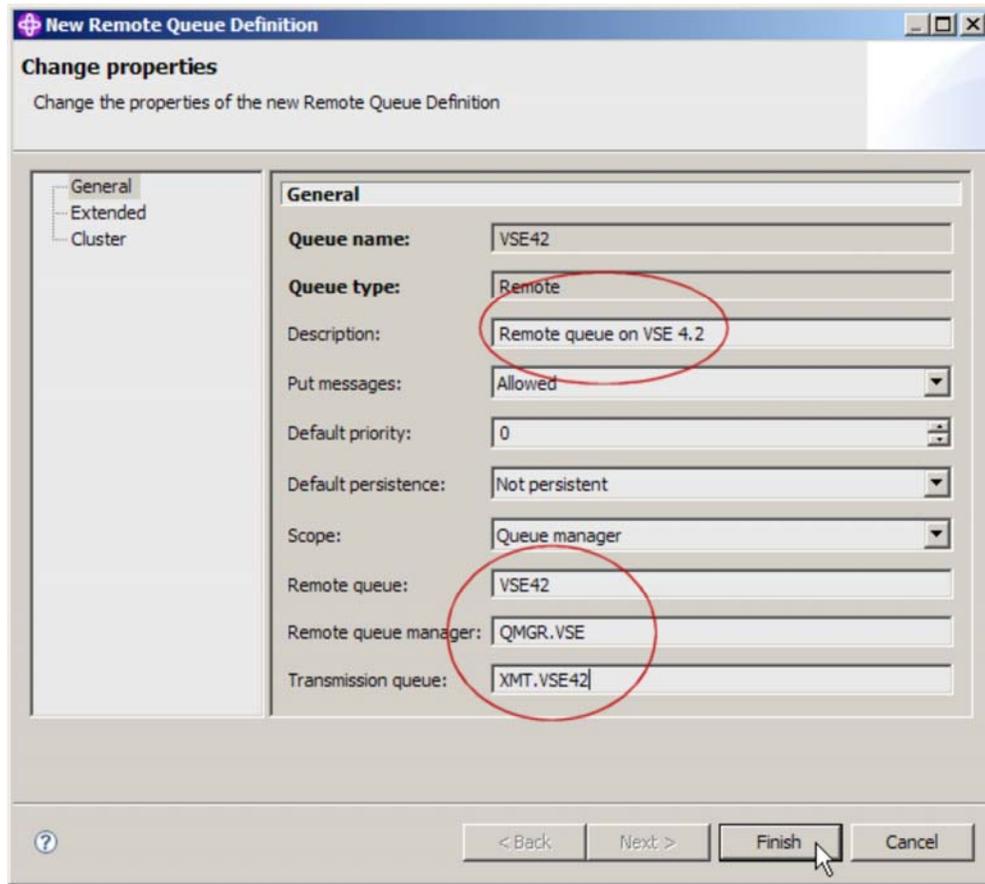


Enter the name of the remote queue: VSE42.



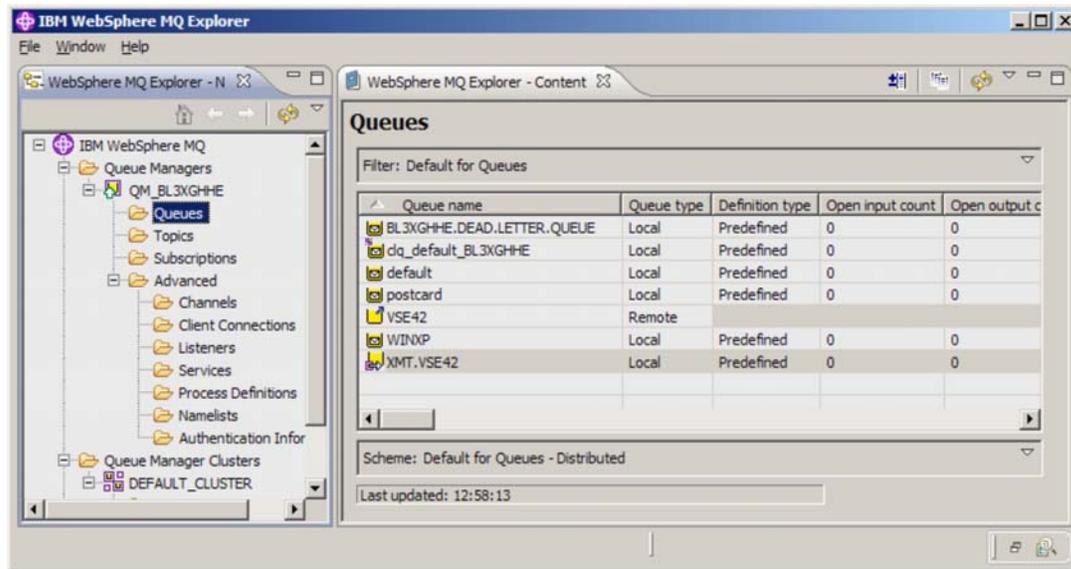
Press **Next**.

On the next box specify the remote queue name (VSE42), the remote queue manager (QMGR.VSE), and the transmission queue name (XMT.VSE42).



Press **Finish**.

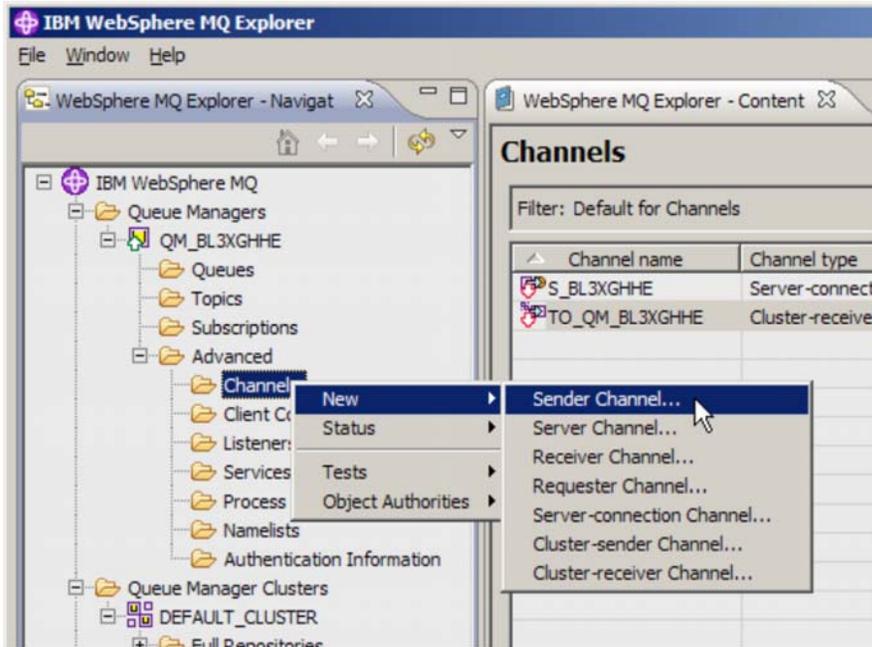
We now have following queues:



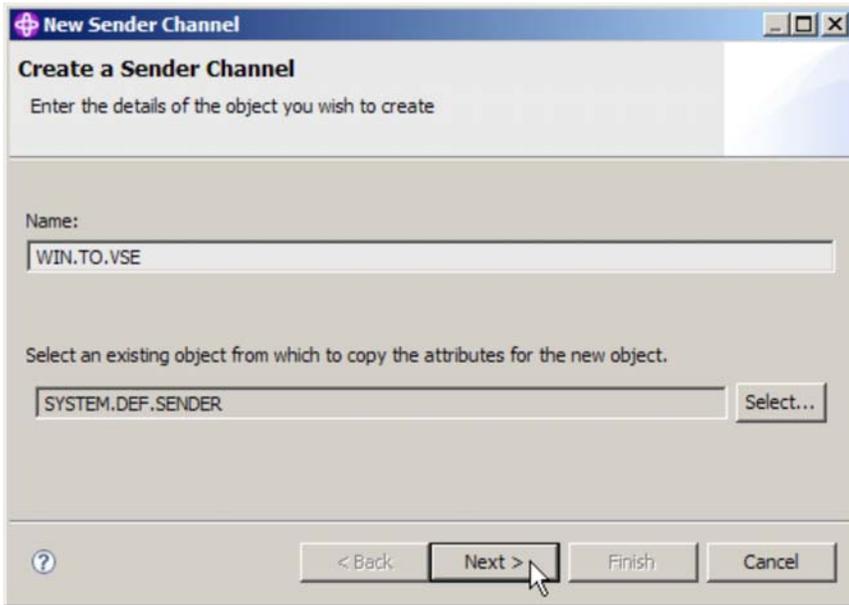
Now let's define the sender and receiver channel.

4.2.4 Defining the sender channel

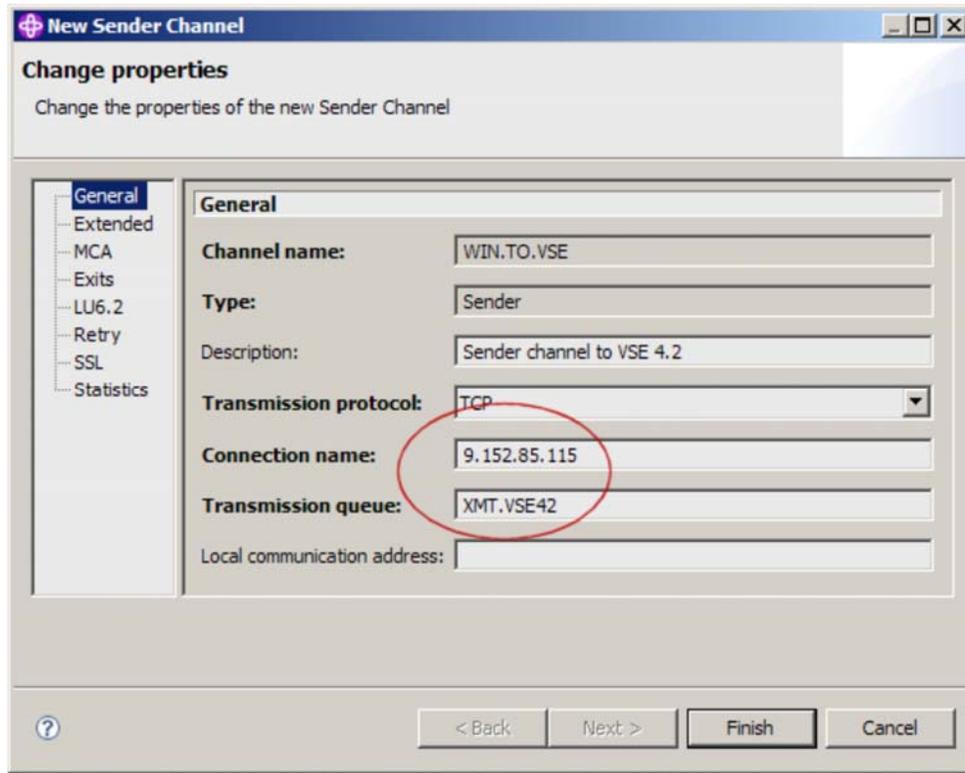
Select **Channels – New – Sender Channel**



Enter the name of the sender channel: WIN.TO.VSE.

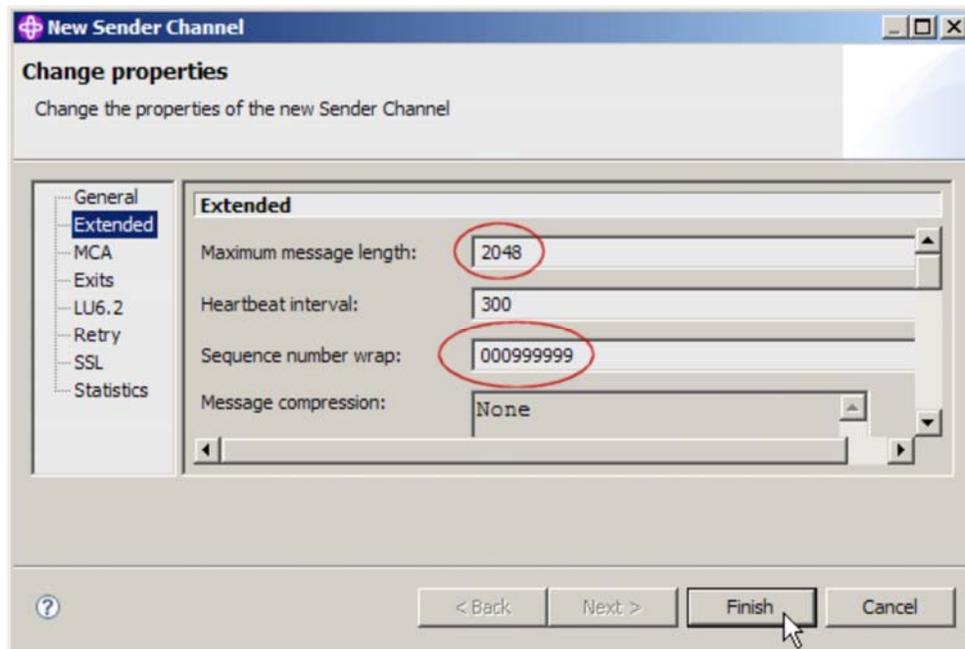


Press **Next**.



Specify the IP address of your VSE system and the related transmission queue name.

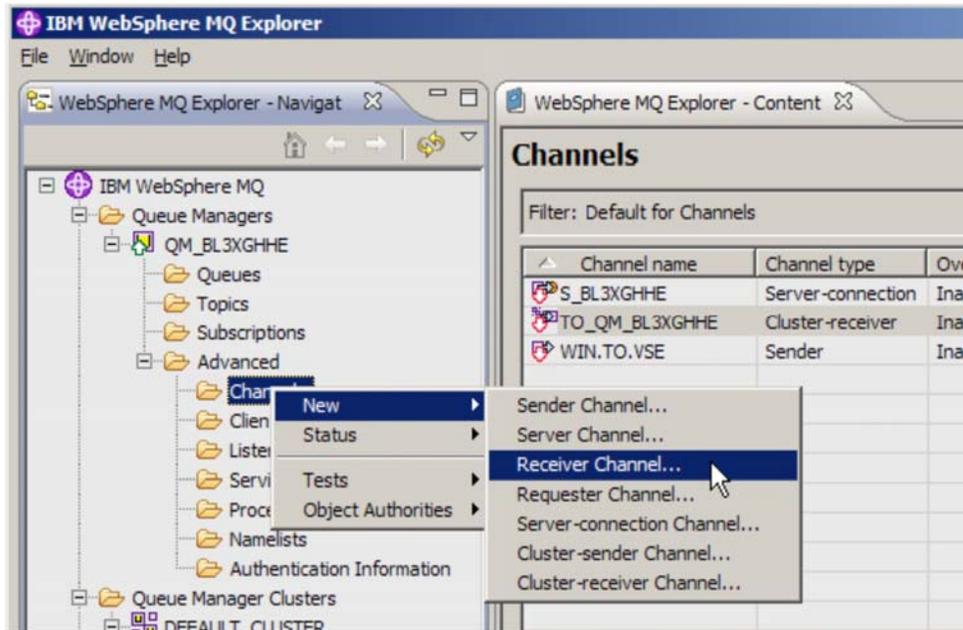
Now select the **Extended** tab.



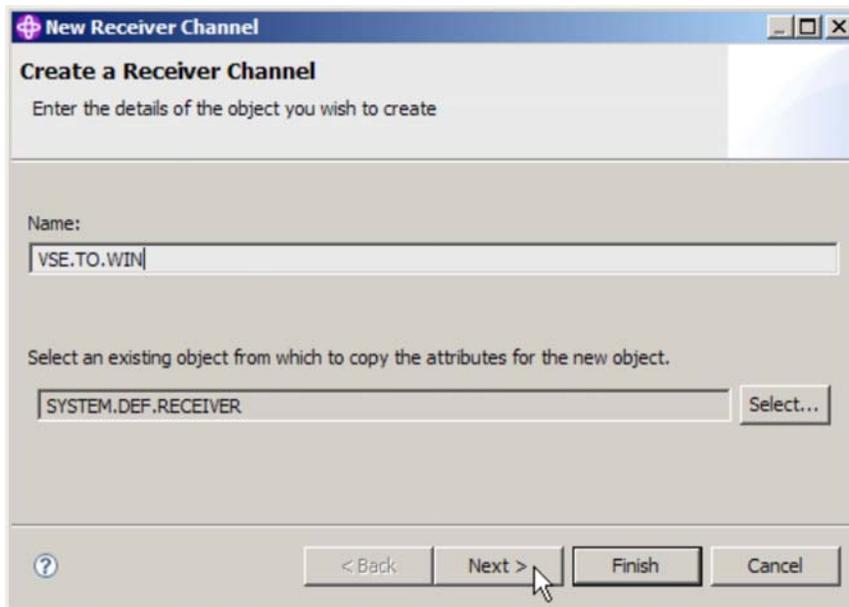
The values for **Maximum message length** and **Sequence number wrap** must match the values of the corresponding receiver channel on the VSE side. Refer to section Defining the receiver channel on page 17.

4.2.5 Defining the receiver channel

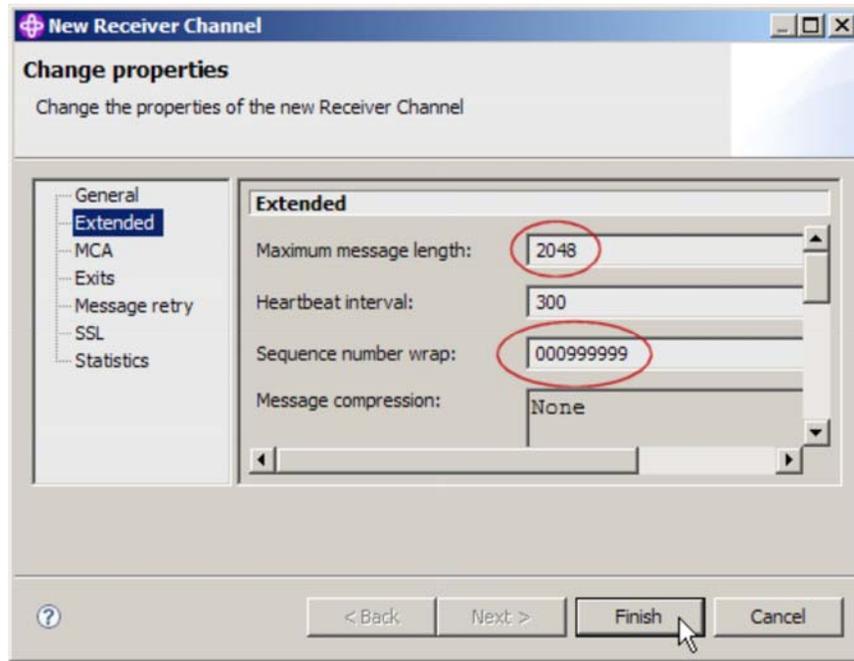
Select **Channels – New – Receiver Channel**.



Enter the name of the receiver channel: VSE.TO.WIN.

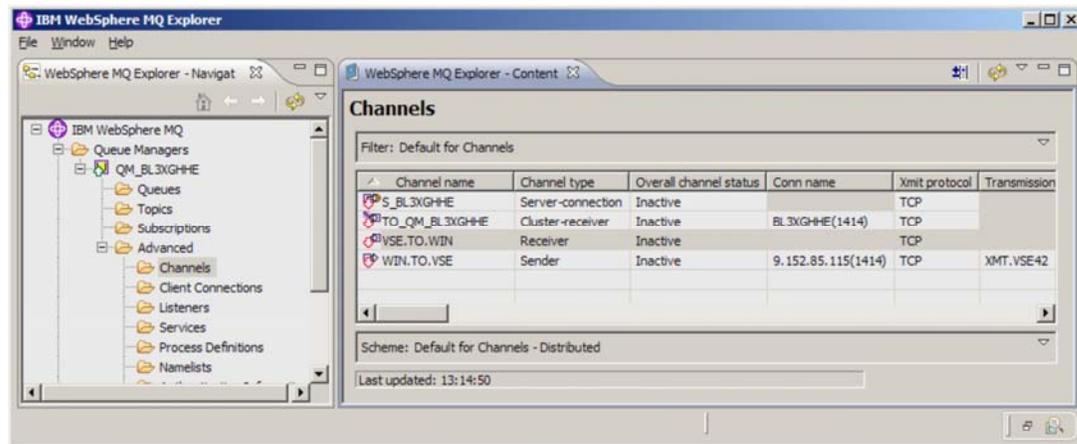


Press **Next** and select **Extended**.

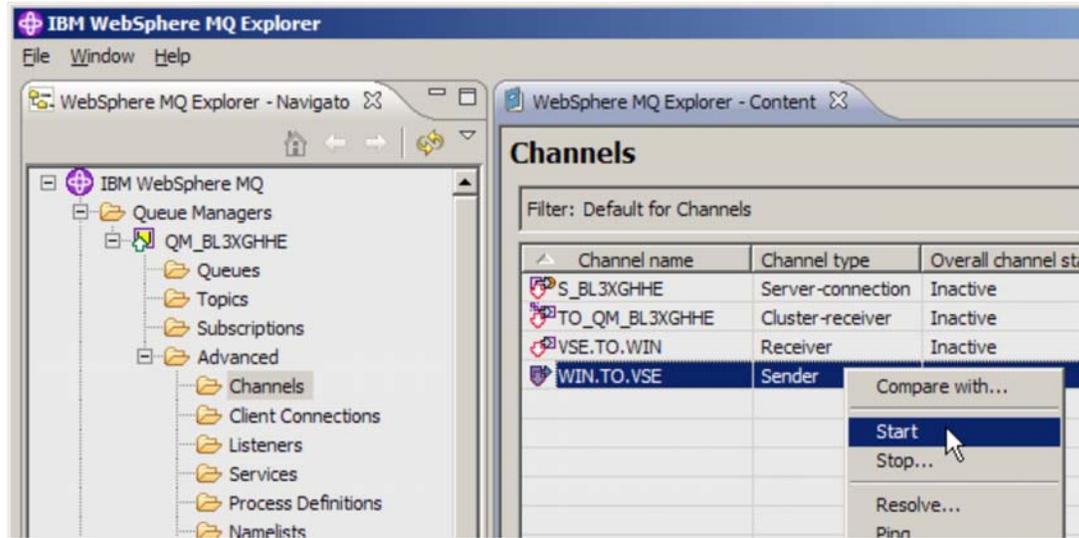


The values for **Maximum message length** and **Sequence number wrap** must match the values of the corresponding sender channel on the VSE side. Refer to section Defining the sender channel on page 17.

We now have the following channels:



Note that the sender channel must be started before any message can be sent.



The new **Overall channel status** should now be **Running**.

4.3 Testing the setup

Now let's test our setup by sending some test messages from Windows to VSE and vice versa.

4.3.1 Sending a test message to VSE

First start MQMT on VSE and enter **3** (Monitoring) and **1** (Monitor queue). Then select the local queue VSE42. Currently there are no messages on the queue, i.e. QDEPTH is zero.

```

12/16/2008          IBM WebSphere MQ for z/VSE Version 3.0.0          DBDCCICS
11:30:38           Monitor Queues                                    CIC1
MQWMMOQ                                                    A000

                    QUEUING SYSTEM IS ACTIVE
                    DETAIL QUEUE INFORMATION

VSE42
INBOUND:  STATUS B  ENABLED Y  OPEN Q          1

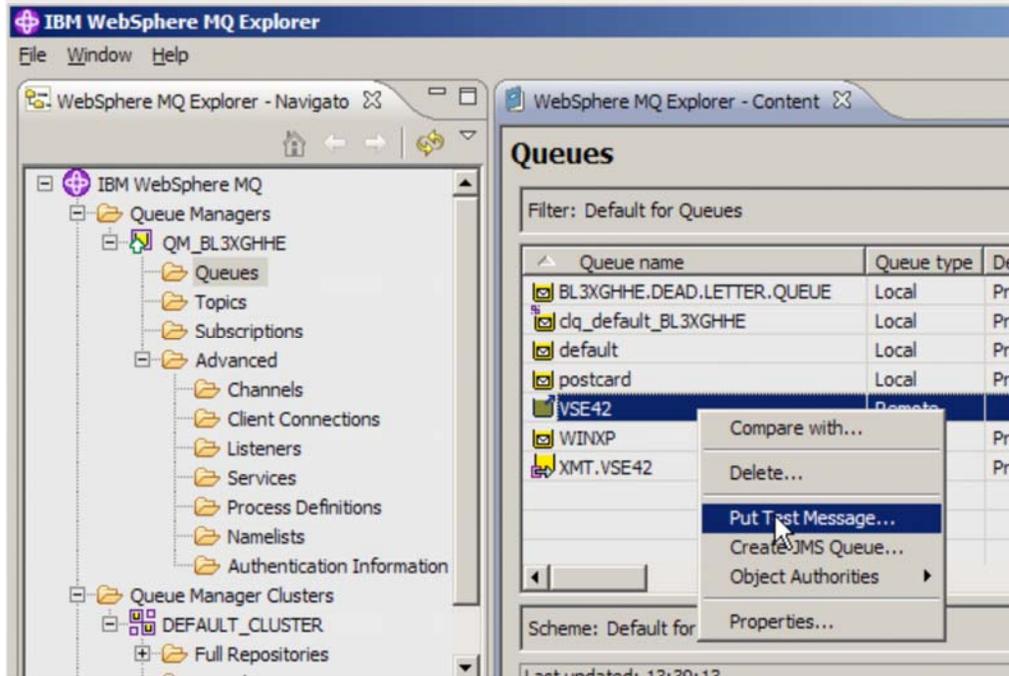
OUTBOUND:  STATUS I  ENABLED Y  OPEN Q          0

BOTH:     FIQ       0    LIQ       0  GETS       0  QDEPTH     0

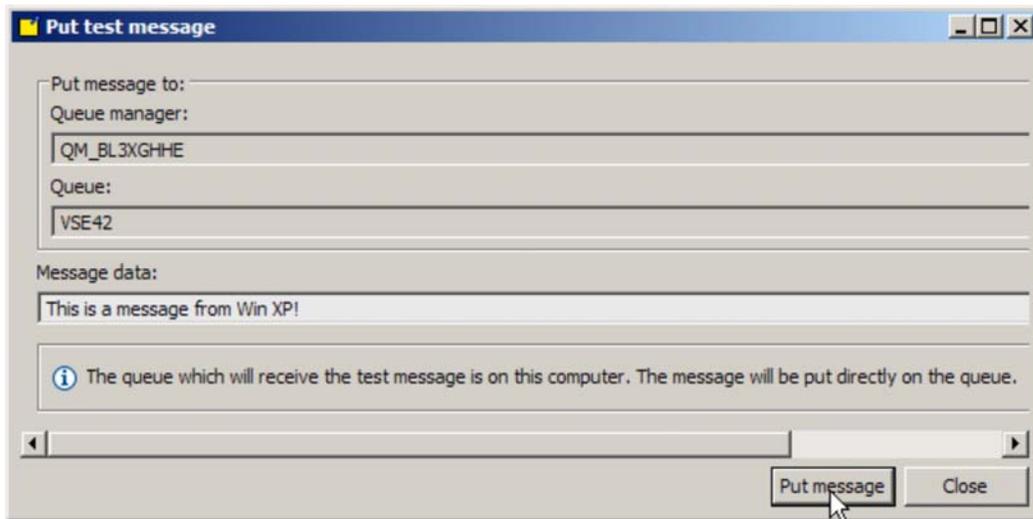
Enter=Refresh  PF2=Return  PF3=Exit  PF10=List
    
```

On Windows start the sender channel, if not already started.

Then right-click the remote queue VSE42 and select **Put Test Message**.



In the following box enter some message text.



Press **Put message**.

On the VSE side you should see the message by pressing **Enter** to refresh the panel.

```

12/16/2008          IBM WebSphere MQ for z/VSE Version 3.0.0          DBDCCICS
11:30:38           Monitor Queues                                   CIC1
MQWMMOQ                                                    A000
                                QUEUING SYSTEM IS ACTIVE
                                DETAIL QUEUE INFORMATION
VSE42
INBOUND:  STATUS B  ENABLED Y   OPEN Q           1
OUTBOUND: STATUS I  ENABLED Y   OPEN Q           0

BOTH:     FIQ           0   LIQ           1   GETS           0   QDEPTH           1

Enter=Refresh  PF2=Return  PF3=Exit  PF10=List
    
```

The QDEPTH value has increased by one. You may now browse the queue to see the message.

Press PF2 twice to return to the main MQMT panel and select **4** (Browse Queue Records). Enter the queue name to browse (VSE42).

```

12/16/2008          IBM WebSphere MQ for z/VSE Version 3.0.0          DBDCCICS
11:32:20           Browse Queue Records                           CIC1
MQWDISP                                                    A000
                                SYSTEM IS ACTIVE
Object Name: VSE42
QSN Number : 00000001      LR-          0, LW-          1, DD-MQFI001
Queue Data Record
Record Status : Written.      PUT date/time : 20081215131509
Message Size : 00000011      GET date/time :                               ASCII
Offset .....!.....!.....!.....!.....!.....!.....!.....!.....!.....!
00000 This is a message from WinXP!

Enter=Process  PF2=Return  PF3=Quit   PF4=Next   PF5=Prior
                PF7=Up     PF8=Down  PF9=Hex    PF10=Hdr   PF11=MD
    
```

4.3.2 Sending a test message to Windows

You can use the TST2 transaction to send a number of test messages to VSE (the TST2 transaction must be defined to BSM, refer to section 3.2 on page 6). On a clear CICS screen enter:

```
TST2 PUT 10 WINXP
```

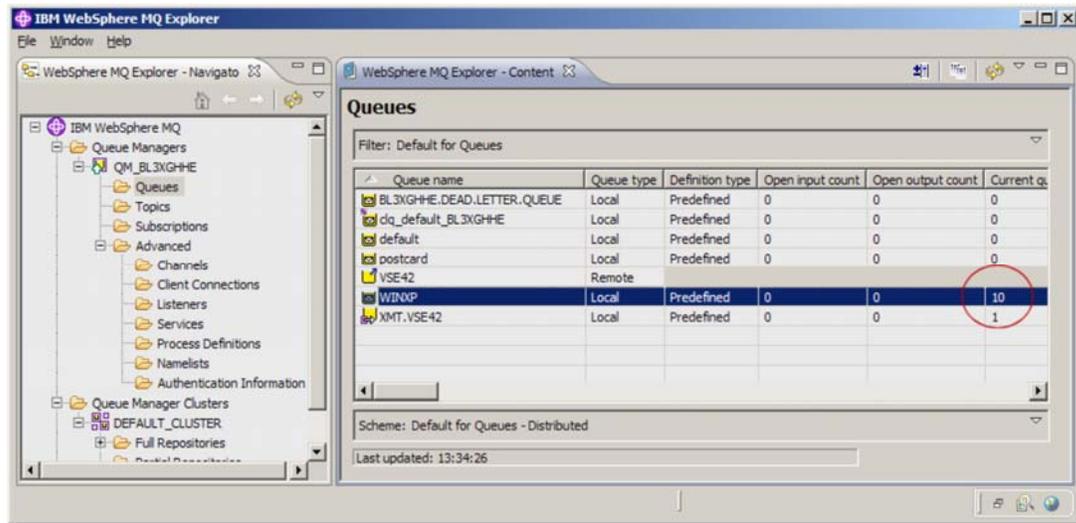
The output should be similar to:

```

FULL CYCLE HAS BEEN PERFORMED SUCCESSFULLY
QUEUE USED -      WINXP

NUMBER OF MESSAGES PROCESSED -      10
TOTAL SECONDS ..... -      00:00:00
    
```

On the Windows side, you should see the 10 messages in the local queue WINXP.



5 Configuring for SSL/TLS

SSL/TLS in general has two flavors:

- SSL/TLS server authentication and
- SSL/TLS client authentication.

Which type to use is configured at the server side (receiver channel). With MQSeries both sides can be server or client at the same time when messages shall be exchanged. Whenever sending an MQ message, the sender is the client, whenever receiving an MQ message the receiver is the server. This must be considered when implementing SSL with MQSeries.

In the following setup, first a set of keyring members (PRVK, ROOT, and CERT) is created with Keyman/VSE and uploaded to VSE. Then the two certificates are stored in a MQ key database file on Windows XP.

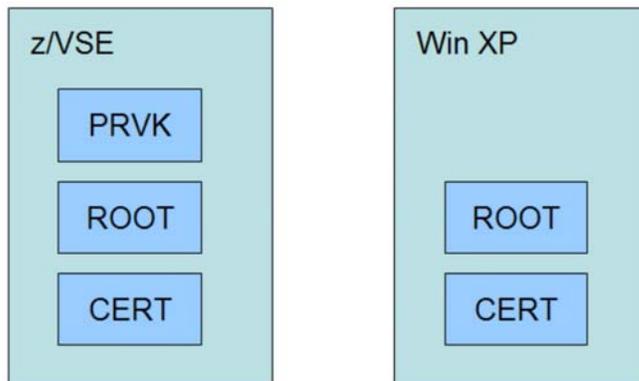


Figure 2: Keyring setup on VSE and Windows

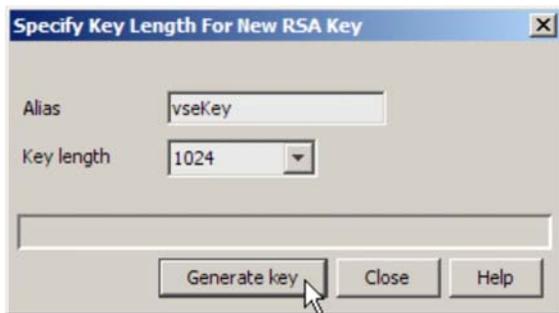
With this setup both sides can be SSL server or SSL client. When VSE is the server (receiver), the certificate contained in the CERT member is sent to the client (sender). When Windows is the server, the user certificate in the key database is sent to VSE.

5.1 Creating the keys and certificates

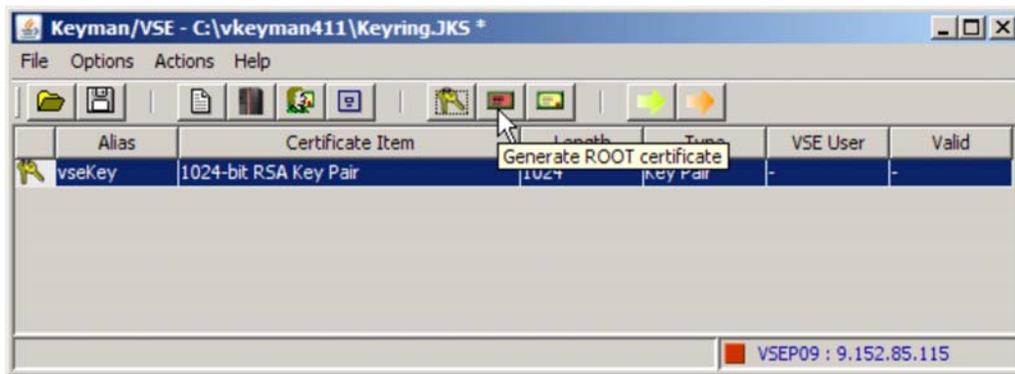
Start the Keyman/VSE tool and create a new RSA key pair.



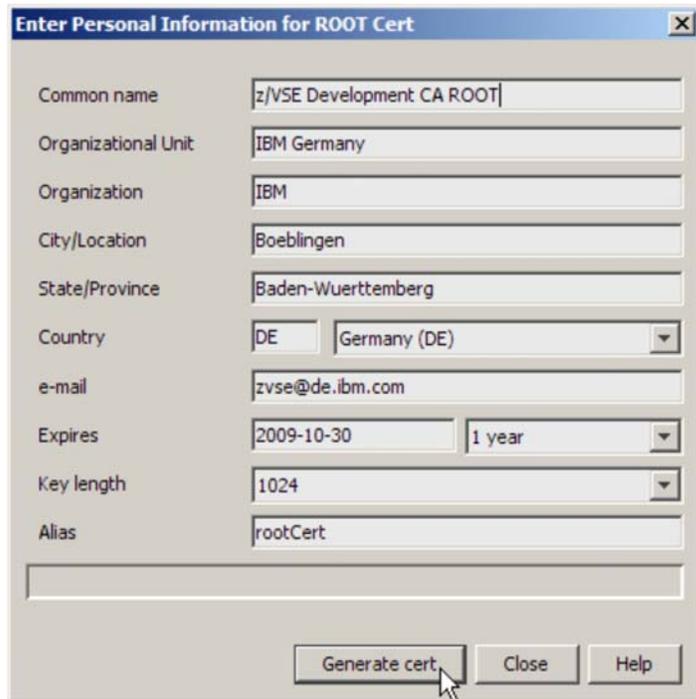
Specify the key length of the RSA key pair. Note that you would need a PCIXCC or Crypto Express2 card for processing 2048 bit keys on VSE.



Now create a new self-signed root certificate.

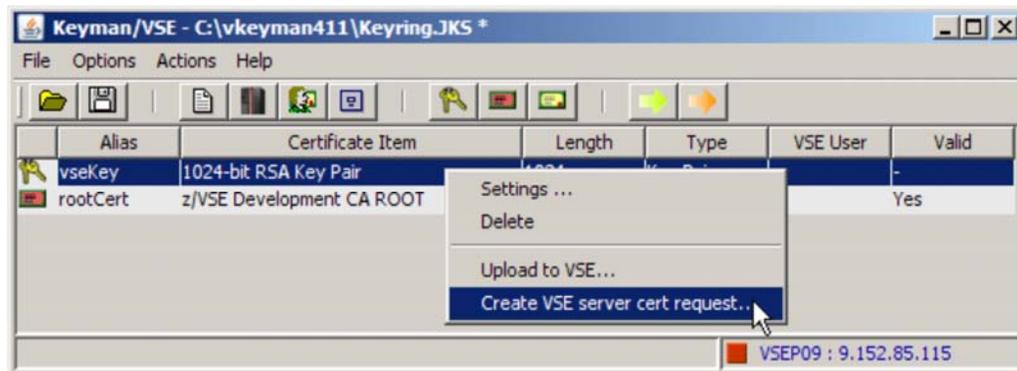


Specify some personal information to identify this ROOT certificate.



Press **Generate cert** to create the certificate.

The next step is now to create a certificate request for the server certificate. This request will later be signed by the already created ROOT certificate, which creates the VSE server certificate. Now right-click the RSA key and select **Create VSE server cert request**.



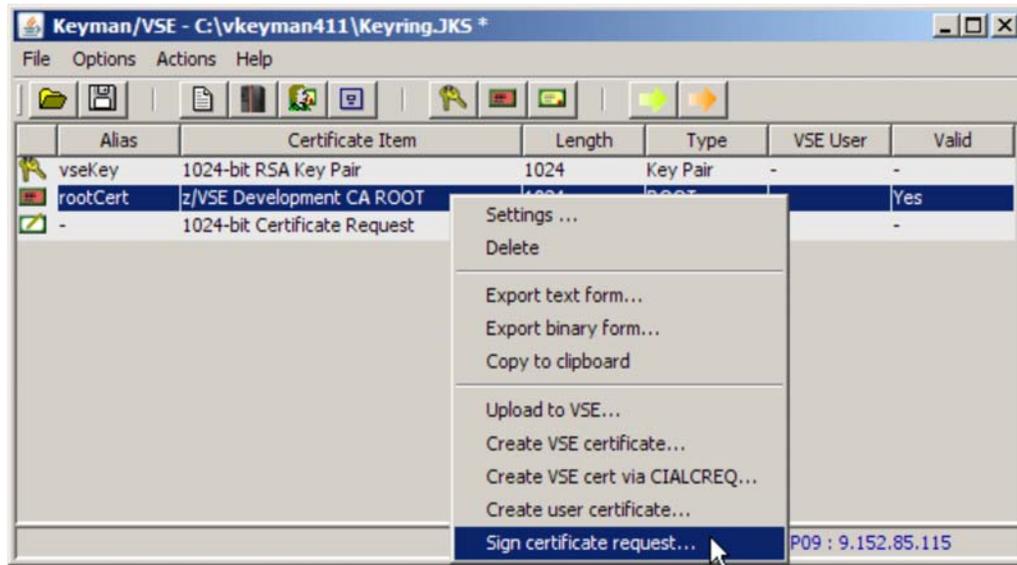
As said above, the server certificate is created by signing the certificate request with your root certificate. In the following box enter some personal information to identify the VSE server certificate.



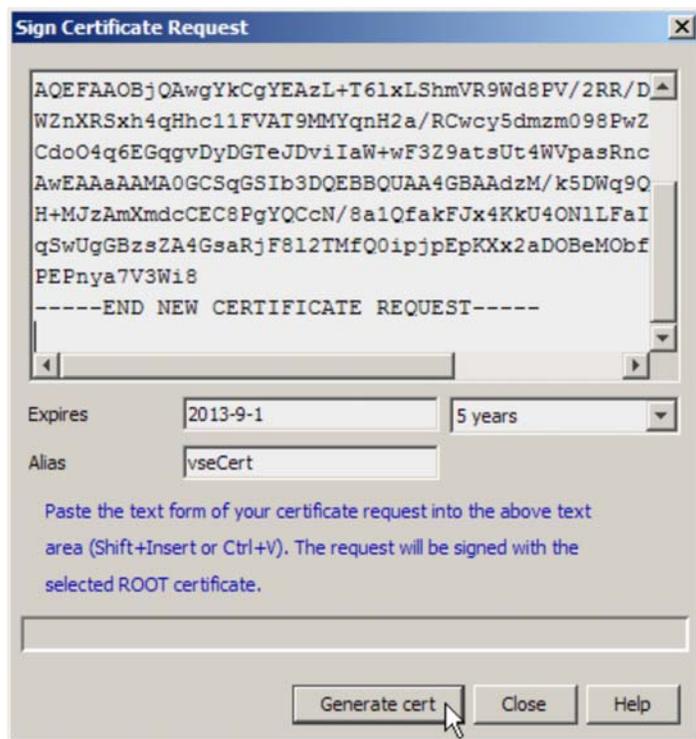
Press **Generate** to create the certificate request.



The next step is to copy the certificate request to the clipboard. Right-click the certificate request and select **Copy to clipboard**.



Now right-click the ROOT certificate and select **Sign certificate request**. Then paste the clipboard content into the text area of the next box as shown below.



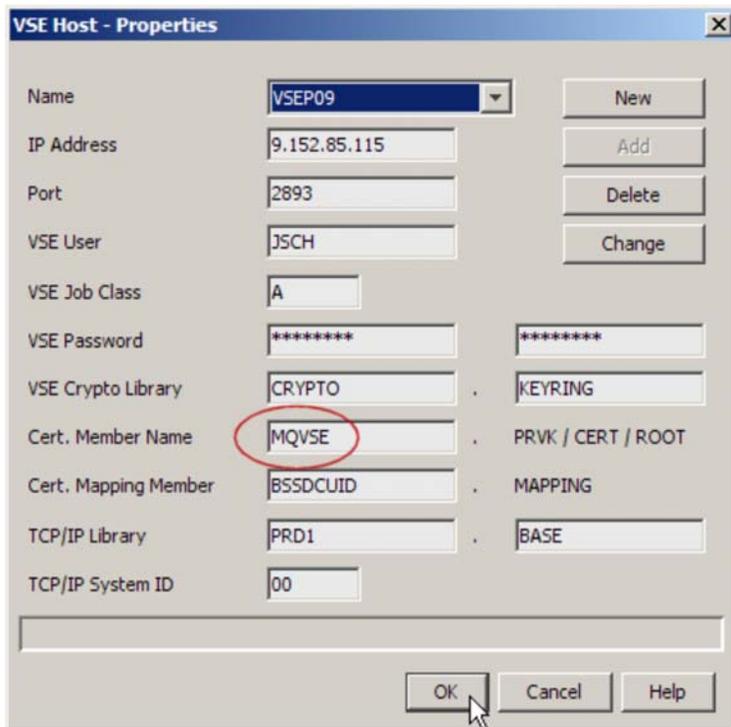
Press **Generate cert** to create the VSE server certificate. The certificate request can be deleted now.



You should now have these three items in Keyman/VSE. The next step is uploading these three items to VSE.

5.1.1 Uploading the certificate items to VSE

In the Keyman/VSE main window open the VSE Host properties window and enter a name for the VSE library members that are uploaded. This is the name of the VSE keyring.



Press OK to return to the Keyman/VSE main window.

Now upload all three items to VSE by right-clicking an item and selecting **Upload to VSE**.



Repeat this step for all three items in the list. Finally, there are three library members cataloged in the VSE keyring library. Don't close the Keyman/VSE tool for now.

```

DIRECTORY DISPLAY      SUBLIBRARY=CRYPTO.KEYRING      DATE: 2008-11-05
                                TIME: 11:38
-----
 M E M B E R      CREATION   LAST      BYTES   LIBR  CONT  SVA  A-  R-
 NAME            DATE       UPDATE   RECORDS  BLKS  STOR  ELIG  MODE
-----
MQVSE           08-11-05   - -      707 B   1     YES  -   -   -
MQVSE           08-11-05   - -     2048 B   3     YES  -   -   -
MQVSE           08-11-05   - -      710 B   1     YES  -   -   -
L113I RETURN CODE OF LISTDIR IS 0
    
```

5.1.2 Specifying the correct certificate label for MQ

After uploading the keyring members to VSE, the two certificates must be stored in a local keyring file. This file will later be imported into the MQ key database.

Before storing the two certificates in the local keyring file, you have to change the certificate label of the VSE certificate. WebSphere MQ requires the following naming convention:

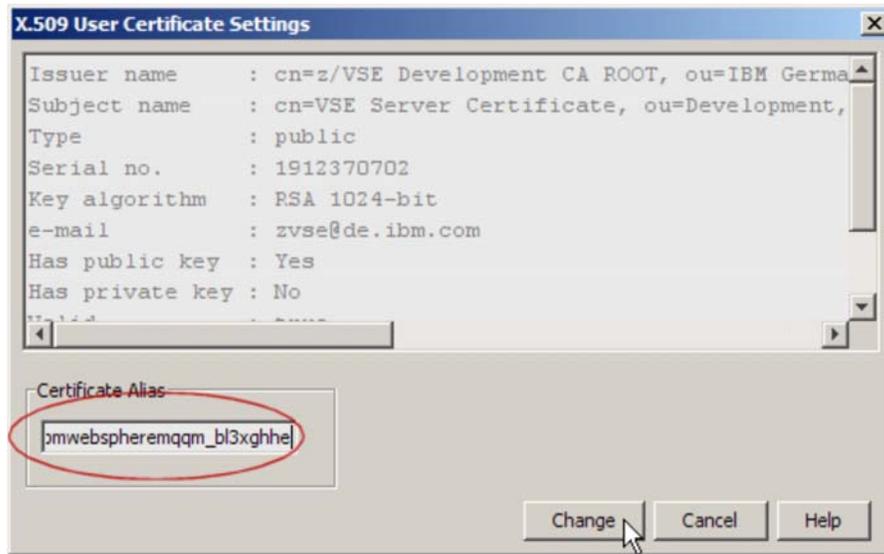
- `ibmwebsphermq` in lowercase letters, concatenated with the MQ queue manager name, also in lowercase letters.

In our example the label is therefore: `ibmwebsphermqmqm_b13xghe`

In the Keyman/VSE tool open the settings box of the VSE certificate.



Change the label to the applicable string in your installation.

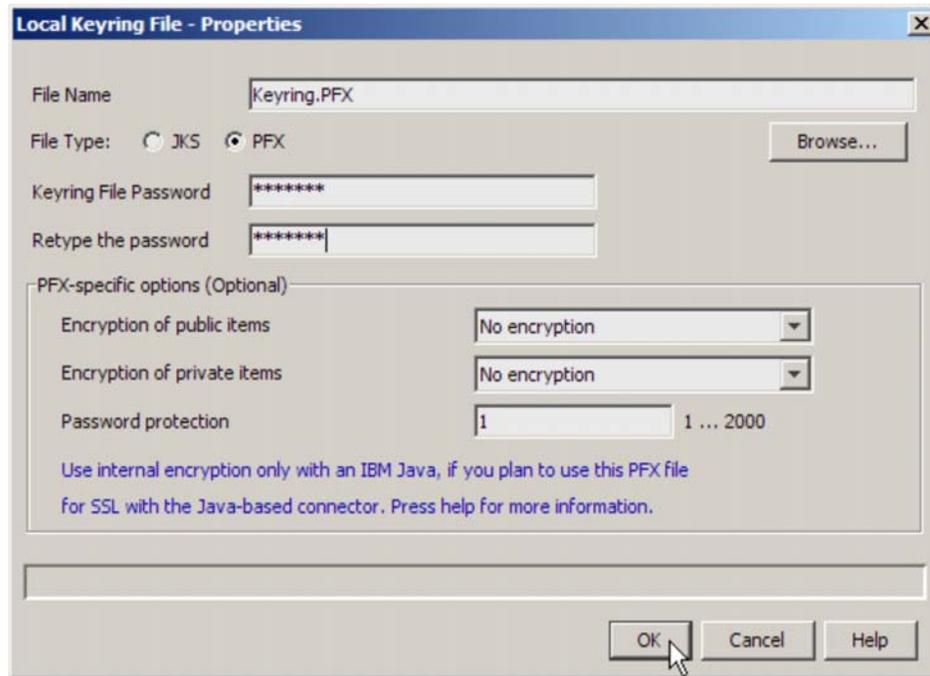


Press **Change**.

You can now delete the RSA key and save the keyring file.



On the next box select PFX and enter a keyring file password.



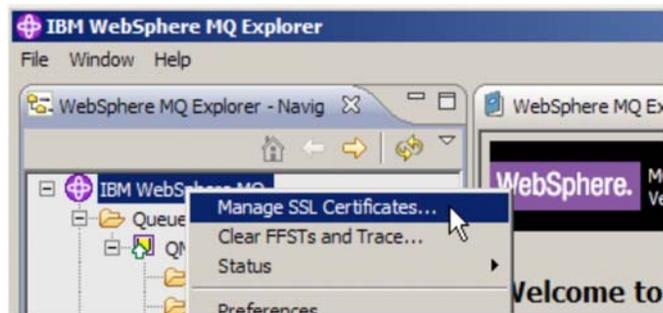
Press **OK**.

In the next sections this keyring file will be imported into the MQ key database.

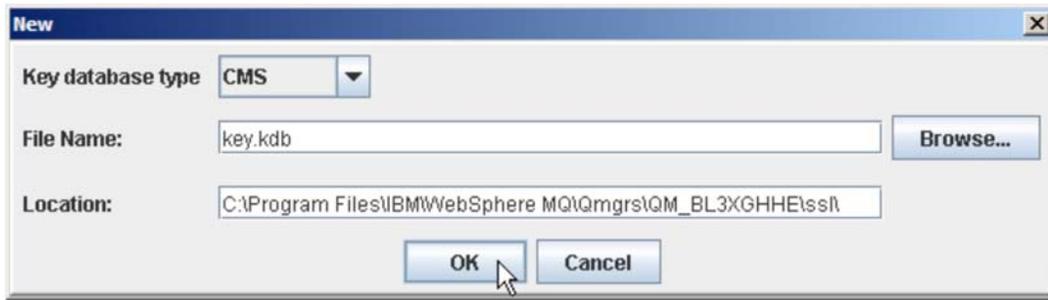
Note: it is vital to import the complete PFX file into the key database to not lose the private key of the self-signed root certificate.

5.1.3 Creating an MQ key database

In the MQ Explorer, select **IBM WebSphere MQ – Manage SSL Certificates**. The IBM Key Management GUI opens.



In the IBM Key Management GUI, select **Key Database File – New**. On the next box enter the file name and location of the database and click **OK**.



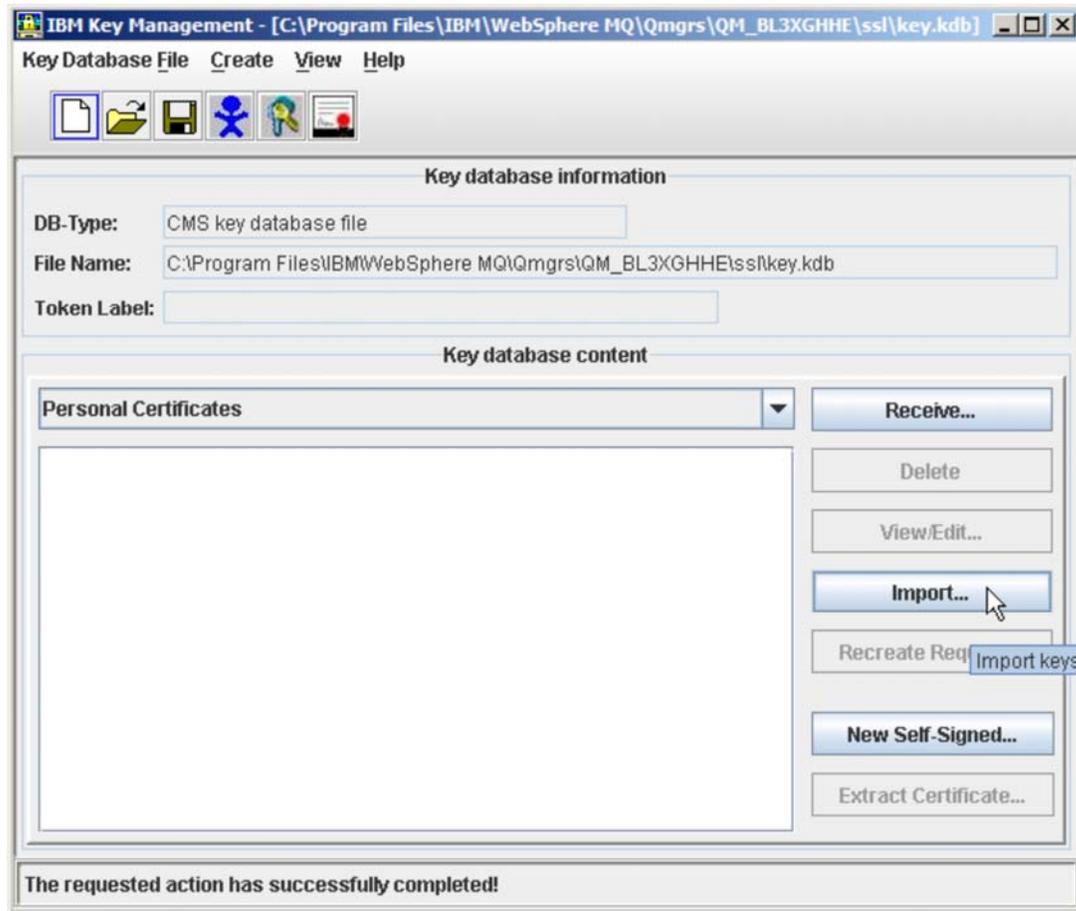
Select **Key Database File – Change Password** to specify the key database password.



Note: it is vital to create a password stash file. When opening an SSL session, MQ needs to access the key database and therefore needs the password. The stash file contains an encrypted copy of the password and is accessed by MQ at runtime. It is located in the same directory as the key repository, with the same filename, but with an .sth extension.

5.1.4 Storing the certificate items in the MQ key database

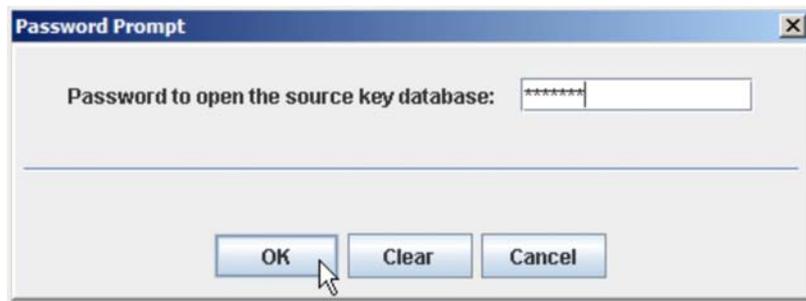
In the IBM Key Management GUI select **Personal Certificates** from the listbox and press the **Import** button.



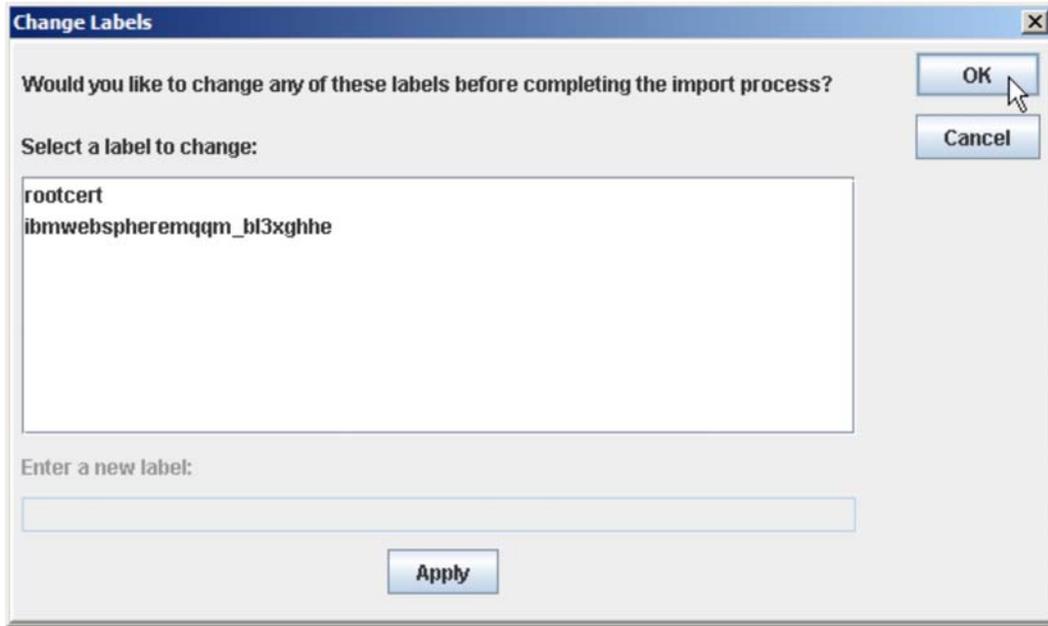
On the Import Key dialogbox, select PKCS12 and browse to the previously saved keyring file.



Press **OK**. On the next box enter your keyring file password.

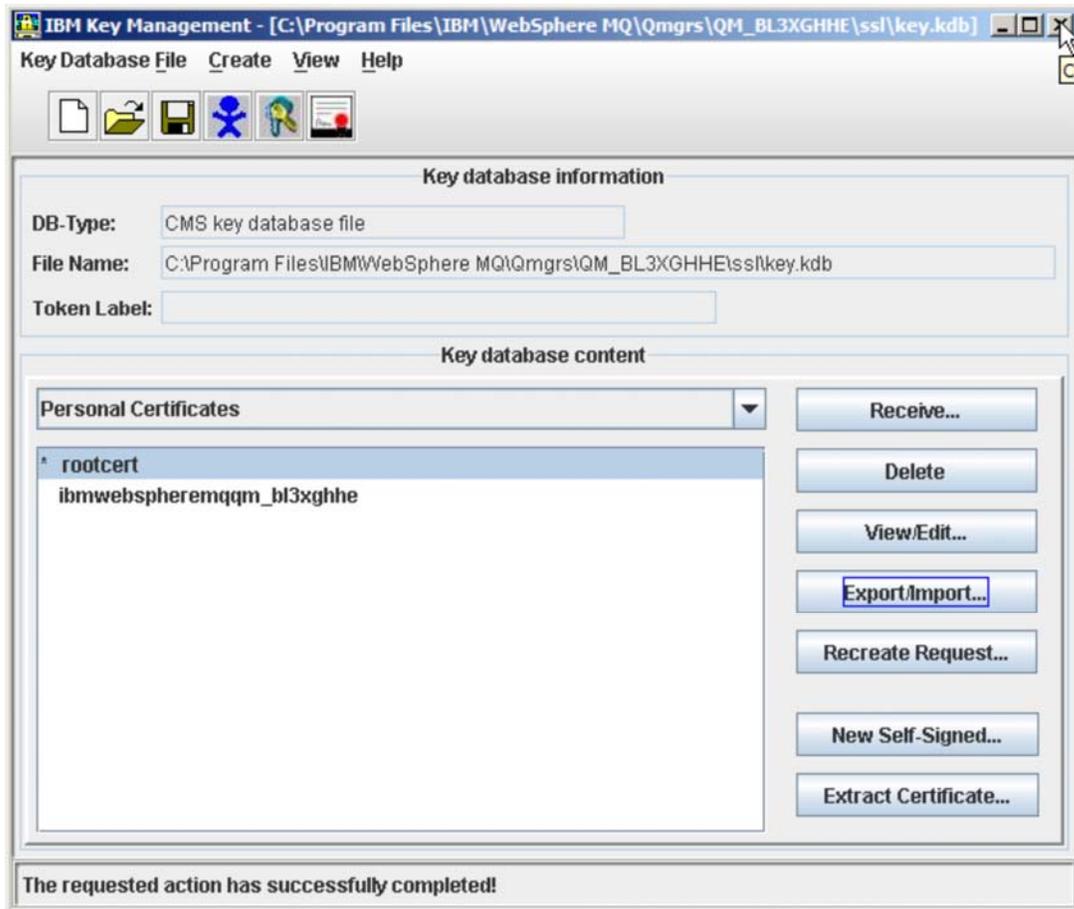


On the next box you should see the two certificates previously created with Keyman/VSE. The VSE certificate should display the required label `ibmwebspheremq` concatenated with your queue manager name.



Press **OK**.

The two certificates are now imported into the MQ key database.



You can now close the IBM Key Management GUI.

5.2 *SSL/TLS configuration on VSE*

You have to configure SSL in the queue manager definition and in the MQ channels. MQ queues are not affected by SSL.

5.2.1 *Configuring the queue manager for SSL/TLS*

Enter the VSE keyring library and the name of the keyring members.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:33:40       Global System Definition                    CIC1
MQWMSYS        Communications Settings                      A000

TCP/IP settings                                Batch Interface settings
TCP/IP listener port : 01414                    Batch Int. identifier: MQBISERV
Licensed clients . . : 00000                    Batch Int. auto-start: Y
Adopt MCA . . . . . : N                        Channel Auto-Definition
Adopt MCA Check . . : N                        Auto-definition . . : Y
                                                Auto-definition exit :

SSL parameters
Key-ring sublibrary : CRYPTO.KEYRING
Key-ring member . . : MQVSE

PCF parameters
System command queue : SYSTEM.ADMIN.COMMAND.QUEUE
System reply queue . : SYSTEM.ADMIN.REPLY.QUEUE
Cmd Server auto-start: N
Cmd Server convert . : N
Cmd Server DLQ store : N

PF2=Queue Manager details  PF3=Quit  PF4/Enter=Read  PF6=Update
    
```

5.2.2 Checking for available SSL/TLS cipher suites

Table 2 shows the list of currently supported SSL cipher suites on VSE.

Hex Code	VSE Cipher Suite Name	Encryption strength
01	SSL_RSA_WITH_NULL_MD5	None
02	SSL_RSA_WITH_NULL_SHA	None
08	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	40 bits
09	SSL_RSA_WITH_DES_CBC_SHA	56 bits
0A	SSL_RSA_WITH_3DES_EDE_CBC_SHA	112 bits
2F	TLS_RSA_WITH_AES_128_CBC_SHA	128 bits
35	TLS_RSA_WITH_AES_256_CBC_SHA	256 bits

Table 2: Supported SSL cipher suites on VSE

Notes:

- When using 2048-bit or 4096-bit RSA keys you need a Crypto Express card.

To make sure SSL is licensed on your VSE system, issue a Q PROD,ALL to the TCP/IP partition to see your current TCP/IP license keys.

```

100 q prod,all
F7 0097 IPN253I << TCP/IP Product Keys >>
F7 0097 IPN885I CPU ID: 0572AF (057216)
F7 0097 IPN886I Stack..... (IBM)
F7 0097 IPN886I Base..... included in Stack
F7 0097 IPN886I Telnet..... included in Stack
F7 0097 IPN886I FTP..... included in Stack
F7 0097 IPN886I LPR..... included in Stack
F7 0097 IPN886I HTTP..... included in Stack
F7 0097 IPN886I CAF..... Not licensed
F7 0097 IPN886I NFS..... Not licensed
F7 0097 IPN886I SSL..... included in Stack <-- SSL must be included.
F7 0097 IPN886I GPS..... Not licensed
F7 0097 IPN886I SecureFTP... included in Stack
F7 0097 IPN886I SeeVSE..... Not licensed
F7 0097 IPN886I HFS..... Not licensed
F7 0097 IPN886I eMail..... Not licensed
F7 0097 IPN886I AES..... Not licensed
    
```

Note: At the time of writing this document, the output of the Q PROD,ALL command is misleading, because AES is included in the SSL component, but displayed separately as not licensed. If SSL is licensed, also AES is available.

In this test setup the following combinations of cipher suites on VSE and Windows worked.

VSE cipher suite hex code	WebSphere MQ 7.0 cipher suite name	Encryption strength
01	NULL_MD5	None
02	NULL_SHA	None
09	DES_SHA_EXPORT	56 bits
0A	TRIPLE_DES_SHA_US	112 bits

Table 3: valid combinations of cipher suites on VSE and Windows

Note: The two AES cipher suites did not work for some unknown reason. An update to this document will describe how to use AES when this problem is solved.

I could not find any matching cipher suite in the WebSphere MQ Explorer for the VSE cipher specs 08 and 62. Also note that the names of the cipher suites in WebSphere MQ are different from the names used on VSE. Table 3 shows the combinations that must be used in the WebSphere MQ 7.0 Explorer.

5.2.3 Configuring the channels for SSL/TLS

To define the SSL parameters for the sender channel press **PF10** at the “Maintain Channel Record” screen (MQMT option 1.3).

```

11/04/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
15:13:04      Channel SSL Parameters                        CIC1
MQWMCHN                                             A000

Channel Name: VSE.TO.WIN      Type: S

SSL Cipher Specification. : 0A      (2 character code)
SSL Client Authentication : 0      (Required or Optional)

SSL Peer Attributes:
>
>
>
>
>
>

SSL channel parameters displayed.
F2=Return PF3=Quit PF4=Read F6=Update

```

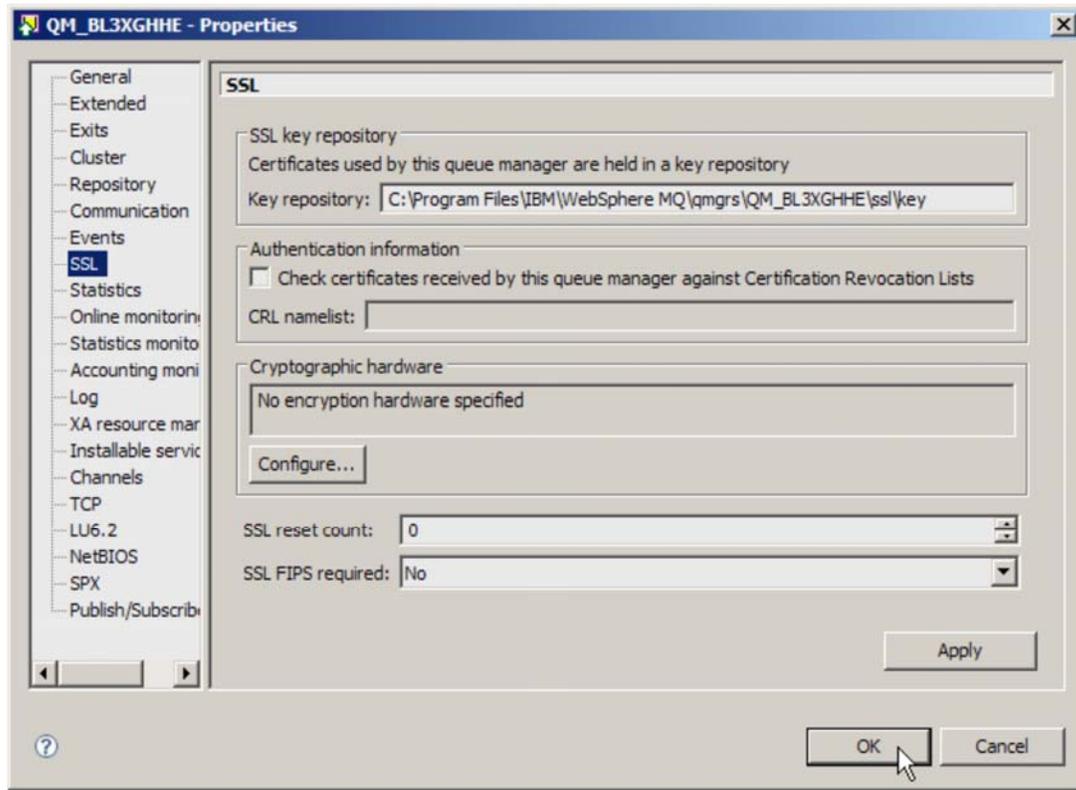
The definition for the receiver channel is identical. Now you should restart MQ on VSE.

5.3 SSL/TLS configuration on Windows

At this point we assume that you already have setup the MQ key database as described in section 5.1.3 on page 41.

5.3.1 Configuring the queue manager for SSL/TLS

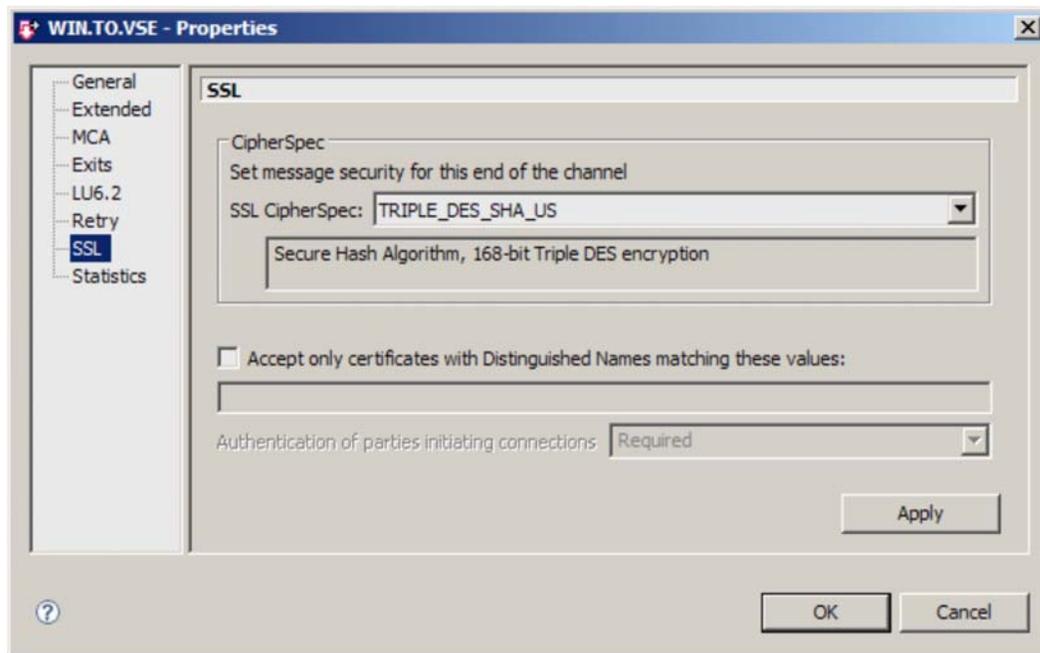
Select your Windows queue manager and display its properties. Select tab **SSL**.



Enter the full path to the key database, including the name of the key database file without the ending .kdb.

5.3.2 Configuring the channels for SSL/TLS

Display the properties of the sender channel and select tab **SSL**.



Select a cipher suite that is also supported by VSE and press **OK**. Refer to Table 3 on page 47 for a list of valid combinations of cipher suites. Then restart the channel.

The definition for the receiver channel is identical.

6 Implementing SSL/TLS client authentication

SSL client authentication is always configured for the receiver channel, which is the SSL server.

6.1 Configuring for client authentication on VSE

When VSE is the receiver (server), SSL client authentication is defined for the receiver channel by changing parameter “SSL Client Authentication” to R (Required). On Windows, the sender channel can be left unchanged.

SSL client authentication means that the client authenticates itself by sending a client certificate to the SSL server. In this case, the client certificate is given by the user certificate with label `ibmwebspheremqmqm_b13xghhe` in the key database. No additional setup is necessary.

6.2 Configuring for client authentication on Windows

When Windows is the receiver (server), SSL client authentication is defined for the receiver channel by selecting “Required” from the drop-down listbox “Authentication of parties initiating connections”. On VSE, the sender channel can be left unchanged.

In this case, the client certificate is given by the CERT member in the VSE keyring library. No additional setup is necessary.

7 Using SSL/TLS peer attributes

When creating a certificate, you have to specify some personal information, which becomes part of the certificate as the “subject name”. When signing the certificate, the name of the signer becomes part of the certificate as the “issuer name”. These “names” are called “Distinguished Names” and are strings consisting of a series of keyword/value pairs.

Supported keywords are:

CN	Common name
C	Country
ST	State or province
L	Locality
O	Organization
OU	Organization Unit
SERIAL	Serial number

The SSL peer attributes field in the channel definition is a 256-character case-sensitive field that can be used to ensure a remote partner’s certificate contains identifiable attributes. This requires that the remote partner provided a certificate during SSL initial negotiation. If the remote partner fails to provide a certificate, then any check against the SSL Peer Attributes field will fail, and the channel will be terminated. The SSL Peer Attributes field expects a value (if any) in the form:

key=value, key=value, etc.

where key is one of the supported keywords (see above). For more information about specifying peer attributes, including the use of wildcards and white space characters, refer to the “MQSeries for VSE System Management Guide, GC34-5364”.

You can display the subject name of your certificates either via Keyman/VSE or using the IBM Key Management tool.

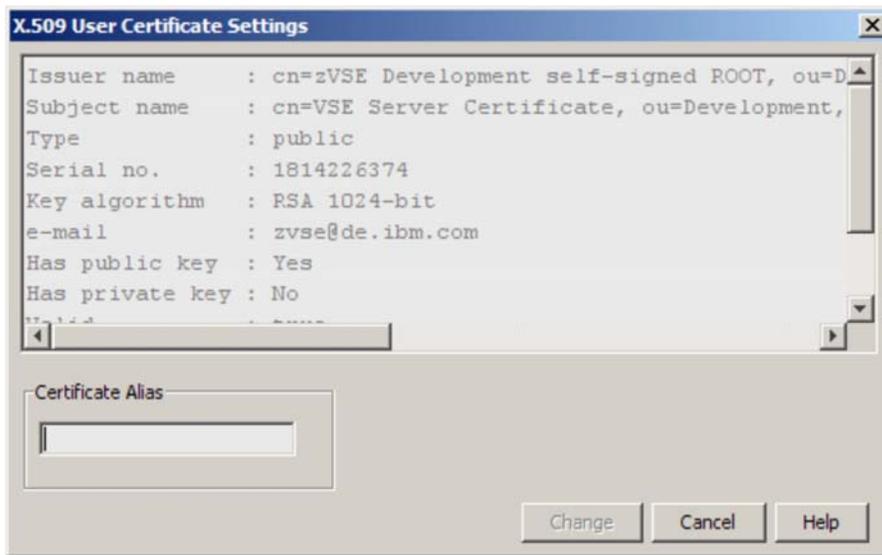
In Keyman/VSE just double-click a certificate to display its properties. You can directly view the certificates on VSE by clicking on the Show keyring library toolbar button.



In the next window, double-click a certificate to view its properties.



The next box shows the certificate properties.



The subject name string shows the attributes that can be specified on the VSE side as peer attributes. The next sections show how to specify peer attributes on the VSE side.

7.1 Example 1: specifying matching peer attributes

In a first test let's specify some peer attributes that match with the partner's client certificate. On VSE display the properties of the receiver channel and add following peer attributes. You have to stop the channel before you can specify any peer attributes.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:35:17              Channel SSL Parameters                  CIC1
MQWMCHN                                               A000

Channel Name: WIN.TO.VSE                Type: R

SSL Cipher Specification. : 0A          (2 character code)
SSL Client Authentication : R          (Required or Optional)

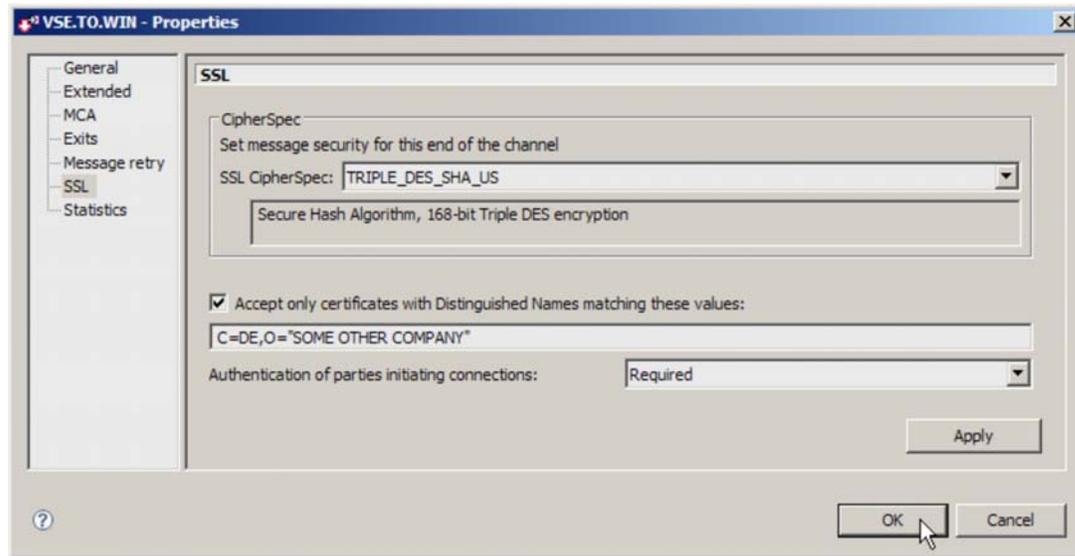
SSL Peer Attributes:
> C=DE,O=IBM                            <
>                                         <
>                                         <
>                                         <

Channel record updated OK.
F2=Return PF3=Quit PF4=Read F6=Update
    
```

With this setup, the SSL connection can be established.

7.2 Example 2: specifying peer attributes which do not match

Now let's enter some peer attributes on Windows which do not match with the certificate sent from VSE. Display the properties of the receiver channel and change the SSL peer properties as shown in the following picture.



In this case the connection cannot be established. The SYSTEM.LOG shows:

```
Receiver responded with error
CHANNEL ID:    VSE.TO.WIN
SSL Peer Name mismatch
NEGOTIATIONS FAILED TO COMPLETE.
```

8 Configuring a remote queue manager

Configuring a VSE queue manager remotely is a new feature with WMQ for z/VSE V3.0. The process is described in the WebSphere MQ for z/VSE V3.0 System Management Guide, chapter 4.

Additional software requirements are:

- WebSphere MQ Explorer V6.0.2.6, or later
- WebSphere MQ Explorer V7.0.0.1, or later

Updates to the WebSphere MQ Explorer are available at

<http://www.ibm.com/software/integration/wmq/support/>

8.1 What you can do remotely

Using the remote configuration functionality of the MQ Explorer, you can

- Display and change queue manager attributes

- Display VSE queues, channels, and namelists
- Display and change the queue, channel and namelist properties
- Put test messages on both sides, Windows and VSE
- Configure the channels for SSL

You cannot

- Start the WebSphere MQ environment on VSE. This must be done with MQMT on VSE.

The following sections describe the additional steps needed to enable remote configuration.

8.2 Preparing the VSE side for PCF

Remote administration of WebSphere MQ for z/VSE is done using Programmable Command Format (PCF) messages. Therefore, you have to define and start a PCF command server.

```

12/16/2008      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
12:10:45      Global System Definition                      CIC1
MQWMSYS      Communications Settings                        A000

TCP/IP settings      Batch Interface settings
TCP/IP listener port : 01414      Batch Int. identifier: MQBISERV
Licensed clients . . : 00000      Batch Int. auto-start: Y
Adopt MCA . . . . . : N
Adopt MCA Check . . : N          Channel Auto-Definition
                                   Auto-definition . . : N
                                   Auto-definition exit :

SSL parameters
Key-ring sublibrary : CRYPTO.KEYRING
Key-ring member . . : MQVSE

PCF parameters
System command queue : SYSTEM.ADMIN.COMMAND.QUEUE
System reply queue . : SYSTEM.ADMIN.REPLY.QUEUE
Cmd Server auto-start: Y
Cmd Server convert . : Y
Cmd Server DLQ store : N

Record updated OK.
PF2=Queue Manager details  PF3=Quit  PF4/Enter=Read  PF6=Update

```

Specify Y for Cmd Server auto-start and Cmd server convert. Channel auto-definition or an auto-definition exit is not required for MQ Explorer. By default MQ Explorer uses the SYSTEM.ADMIN.SVRCONN channel which is a default definition, so auto-definition is not required. However, using auto-definition would pose a security risk and an exit should be used in this case.

When restarting WebSphere MQ on VSE, the following line should appear in the SYSTEM.LOG or on the console if optional logging to console is enabled.

```
MQI0200I - MQI007000I PCF command server started
```

Now you have to define some additional queues. You can use the MQJINSG.Z sample MQSC job to create these queues, but you must define the system command and reply queues (explained above) before you can run the job.

8.3 Defining additional queues

Following default queues must be defined on the VSE side before you can use the MQ Explorer to remotely administer your z/VSE queue manager. The default names for these queues and their default CICS filenames are:

```
SYSTEM.DEFAULT.ALIAS.QUEUE      n/a
```

```

SYSTEM.DEFAULT.LOCAL.QUEUE      MQFDEFS
SYSTEM.DEFAULT.MODEL.QUEUE     MQFDEFS
SYSTEM.DEFAULT.REMOTE.QUEUE    n/a
SYSTEM.MQEXPLORER.REPLY.MODEL  MQFADMN

```

Refer to section Open of file MQFADMN failed on page 64 for how to define the MQFADMN file.

8.4 Defining the MQ Explorer reply model queue

The SYSTEM.MQEXPLORER.REPLY.MODEL queue should be defined as a temporary queue so that the queue is deleted when the queue is closed. Defining it as a dynamic queue would lead to the VSAM file defined for the model queue filling up. In the test setup the reply model queue has been first defined as dynamic, which caused the problem described in section 9.5 on page 64.

The size of the VSAM file that holds the MQ Explorer reply queue has to be large enough to hold all the reply messages for the duration of the MQ Explorer session. A temporary dynamic queue is not deleted until the queue handle is closed i.e. when MQ Explorer disconnects from the z/VSE system. In WebSphere MQ for z/VSE, messages stay in the VSAM file marked as "Deleted" after they are gotten from the queue. The message records are physically deleted only when the queue is deleted or reorganized.

To change the queue definition, either use the queue maintenance transaction MQMQ or MQMT (options 1.2) and edit the SYSTEM.MQEXPLORER.REPLY.MODEL queue. The Def. type sets the model's definition type to T or P.

```

02/26/2009      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
08:35:48              Queue Extended Definition              CIC1
MQWMQUE                                               A000

Object Name: SYSTEM.MQEXPLORER.REPLY.MODEL

General                Maximums                Events
Type . . . : Model    Max. Q depth . . : 00100000  Service int. event: N
File name  : MQFADMN  Max. msg length: 00002048  Service interval  : 00000000
Usage . . . : N       Max. Q users . . : 00000100  Max. depth event  : N
Shareable  : Y       Max. gbl locks  : 00001000  High depth event  : N
Def. type  : T       Max. lcl locks  : 00001000  High depth limit  : 000
                                           Low depth event . : N
                                           Low depth limit . : 000

Triggering
Enabled . . : N       Transaction id. :
Type . . . :          Program id . . :
Max. starts: 0001    Terminal id . . :
Restart . . : N      Channel name . . :
User data  :
:

Requested record displayed.
PF2=Return  PF3=Quit  PF4/Enter=Read  PF5=Add  PF6=Update
             PF9=List  PF10=Queue

```

The picture in section 8.7 on page 58 still shows the wrong definition.

8.5 Defining a server-connection channel

In our setup we defined a server-connection channel, by default named SYSTEM.ADMIN.SVRCONN. However, the MQ Explorer can be configured to use any channel name which should map to an SVRCONN channel on VSE, or you can use channel auto-definition.

```

02/20/2009      IBM WebSphere MQ for z/VSE Version 3.0.0      DBDCCICS
11:57:56              Channel Record          DISPLAY      CIC1
MQWMCHN              A000
Channel : SYSTEM.ADMIN.SVRCONN
Desc. . . : MQ Explorer server-connection channel
Protocol: T (L/T)   Type : C (S=Snd/R=Rcv/V=Srv/Q=Req/C=svrConn)  Enabled : Y

Sender/Server
Remote TCP/IP port . . . . . : 00000      Short/Long retry count . . : 000000000
Get retry number . . . . . : 000000000    Short retry interval . . . : 000000000
Get retry delay (secs) . . . : 000000000    Long retry interval . . . : 000000000
Convert msgs(Y/N) . . . . . : N           Batch interval . . . . . : 000000000
Transmission queue name. . . :
TP name. . . :

Sender/Receiver/Server/Requester
Connection :
Max Messages per Batch . . . : 000001      Message Sequence Wrap . . . : 999999999
Max Message Size . . . . . : 0018000      Dead letter store(Y/N) . . : N
Max Transmission Size . . . : 065535      Split Msg(Y/N) . . . . . : N
Max TCP/IP Wait . . . . . : 000000

Channel record displayed.
F2=Return PF3=Quit PF4=Read PF5=Add PF6=Upd PF9=List PF10=SSL PF11=Ext PF12=Del

```

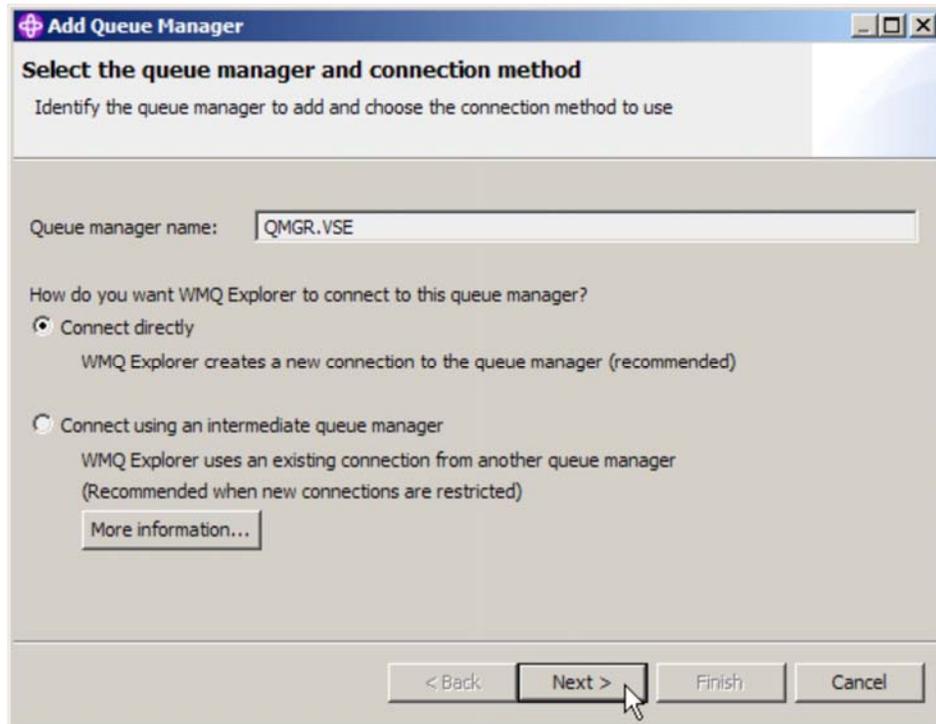
The VSE side is now ready. We can now add the VSE queue manager as remote queue manager in MQ Explorer.

8.6 Defining a remote queue manager

Before you can define a remote queue manager using the MQ Explorer, MQ must be started on VSE. To define a remote queue manager, select **Queue Managers – Add remote Queue Manager**.

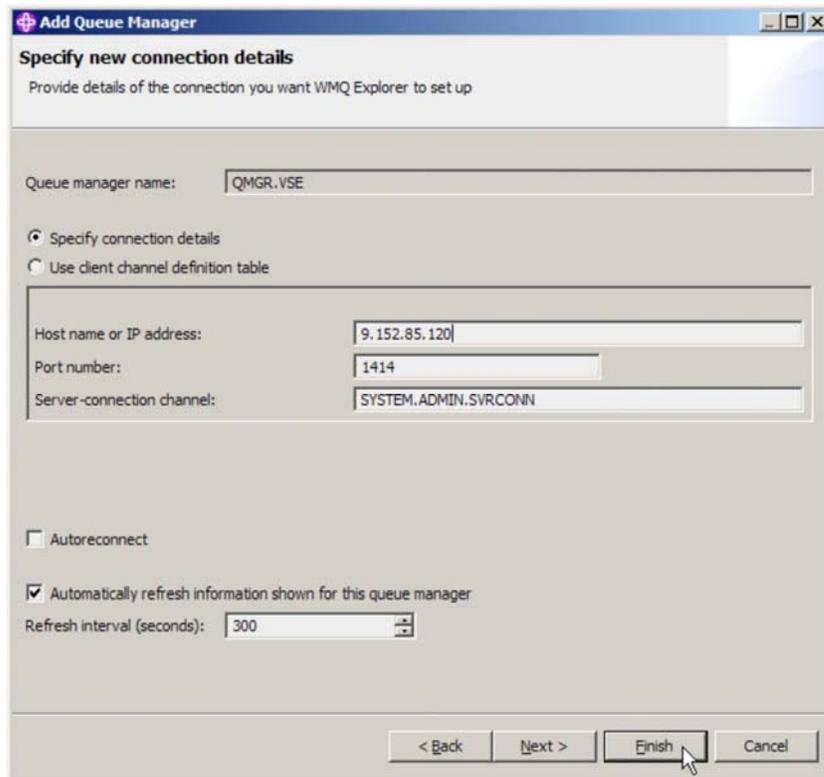


In the next box enter the name of the VSE queue manager.



Press **Next**.

In the following box enter the IP address or host name of your VSE system.

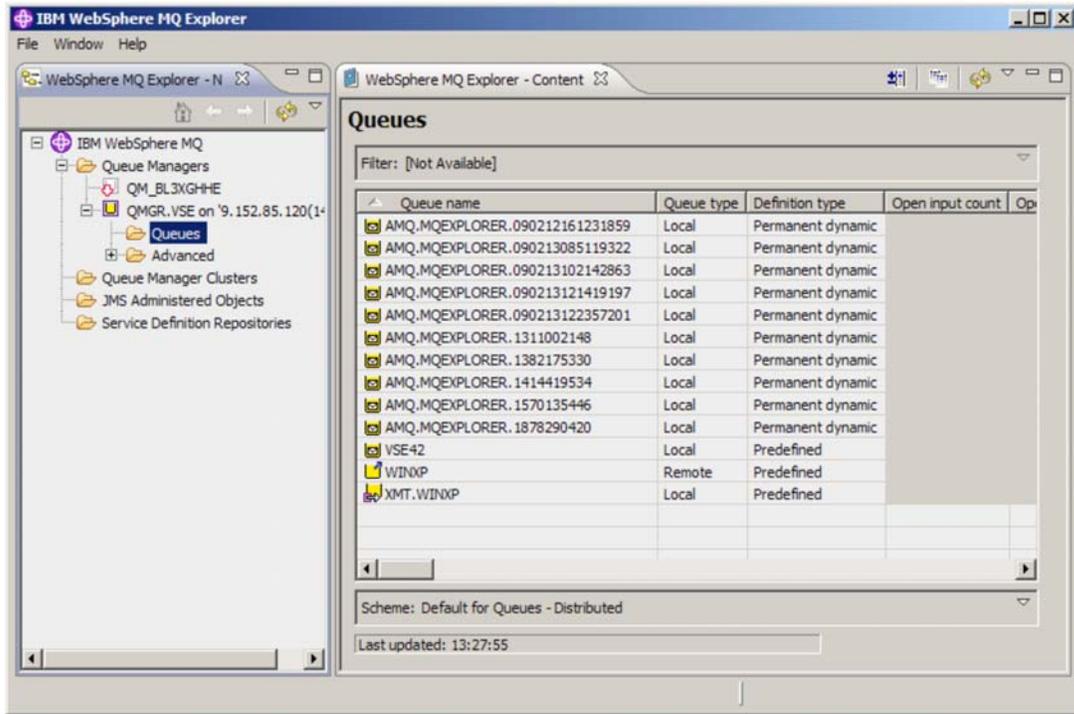


Press **Finish**.

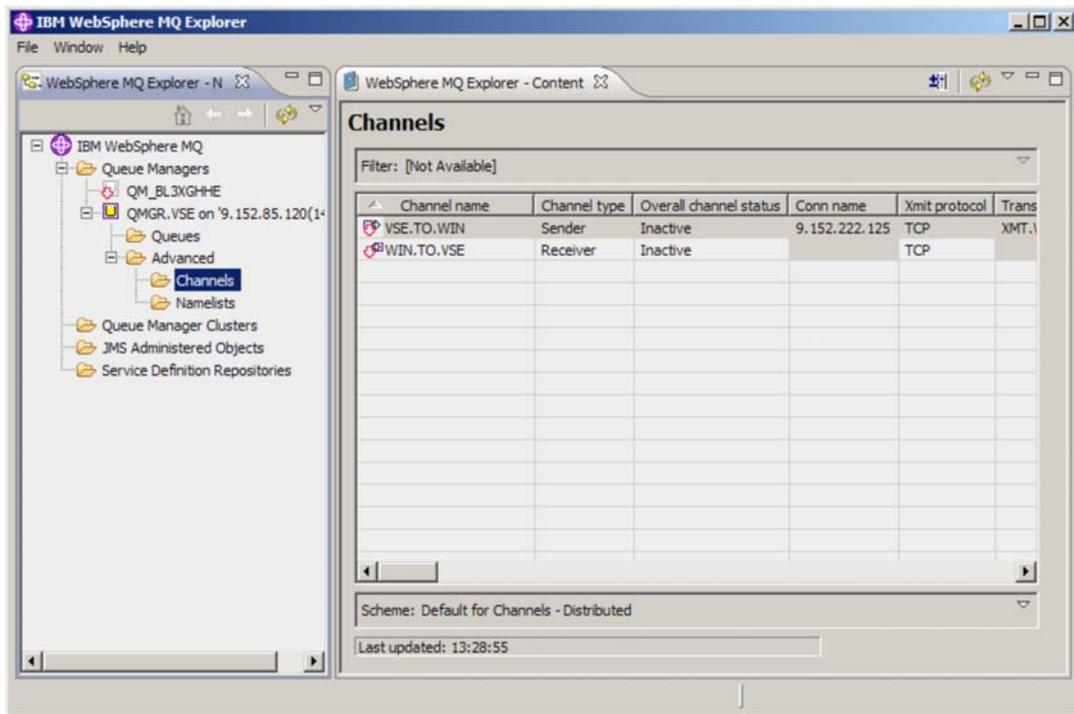
The MQ Explorer should now display the VSE queue manager with its queues and channels.

Below picture shows the VSE queues.

Note: the picture still shows the MQ Explorer reply model queue defined as permanent/dynamic, which caused some problems. Refer to section Defining the MQ Explorer reply model queue on page 54.



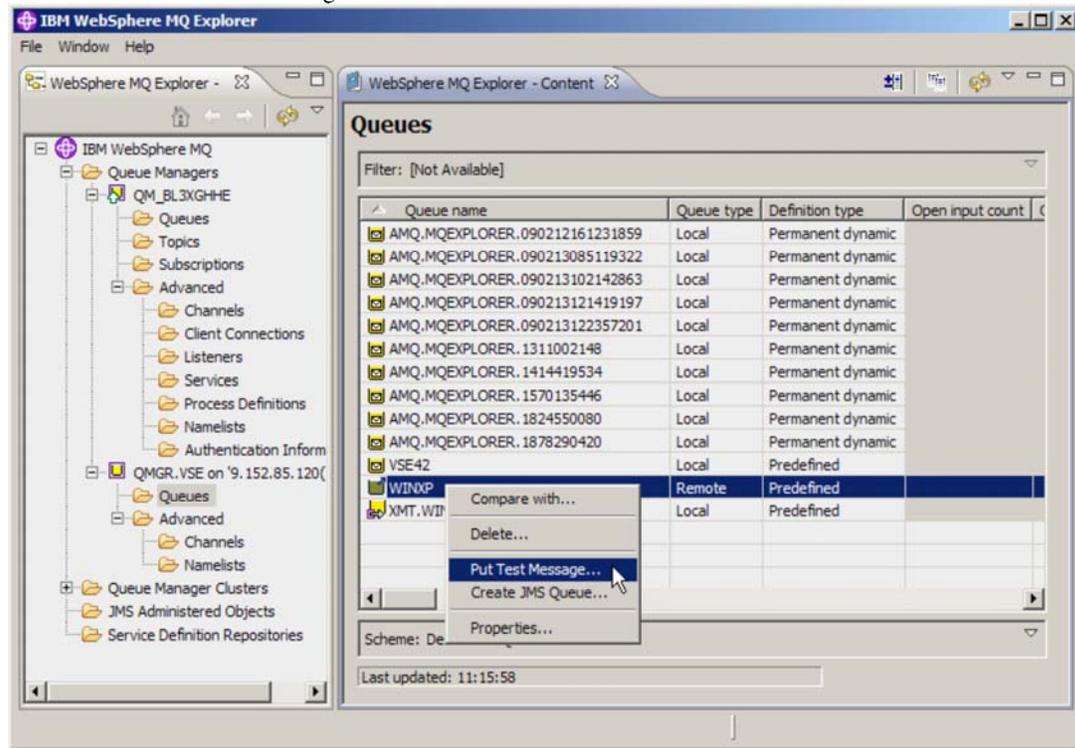
Below picture shows the VSE channels.



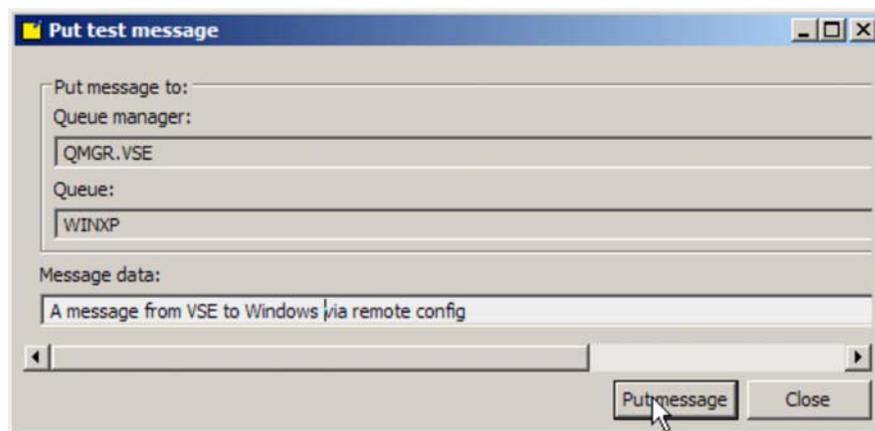
When MQ on VSE is stopped, the remote queue manager gets automatically disconnected. After restarting MQ on VSE, you can reconnect the remote queue manager. No other actions are possible until the queue manager is connected.

8.7 Exchanging test messages

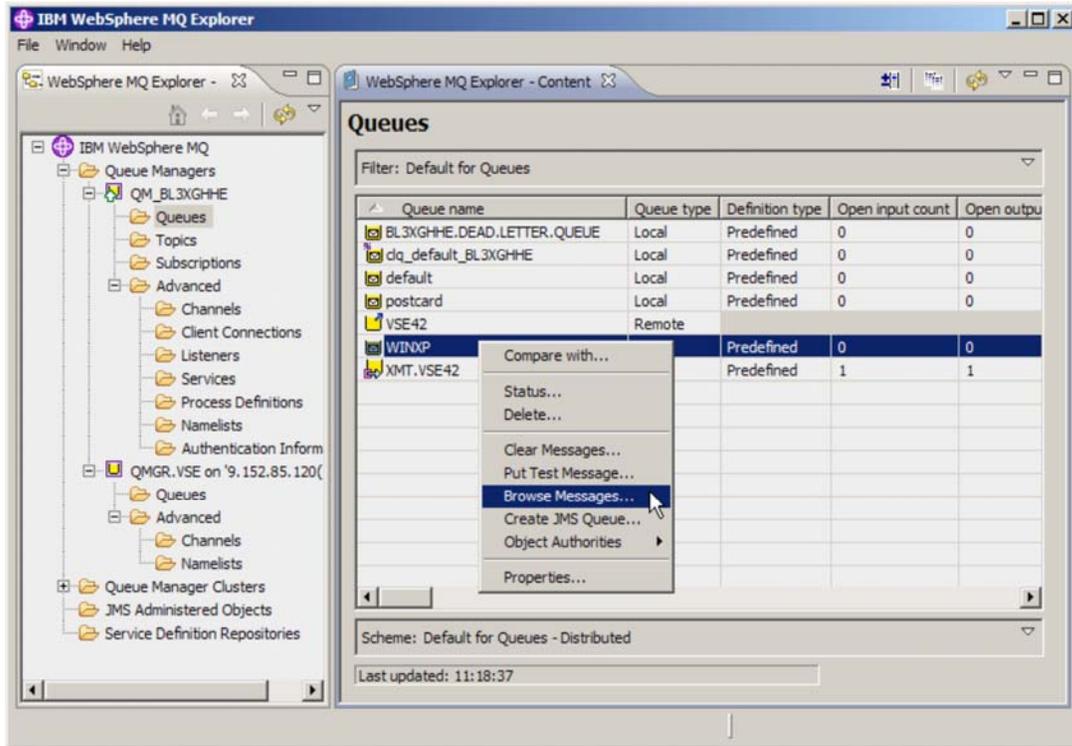
You can now exchange test messages between VSE and Windows via the MQ Explorer. The following example shows how to send a test message from VSE to Windows.



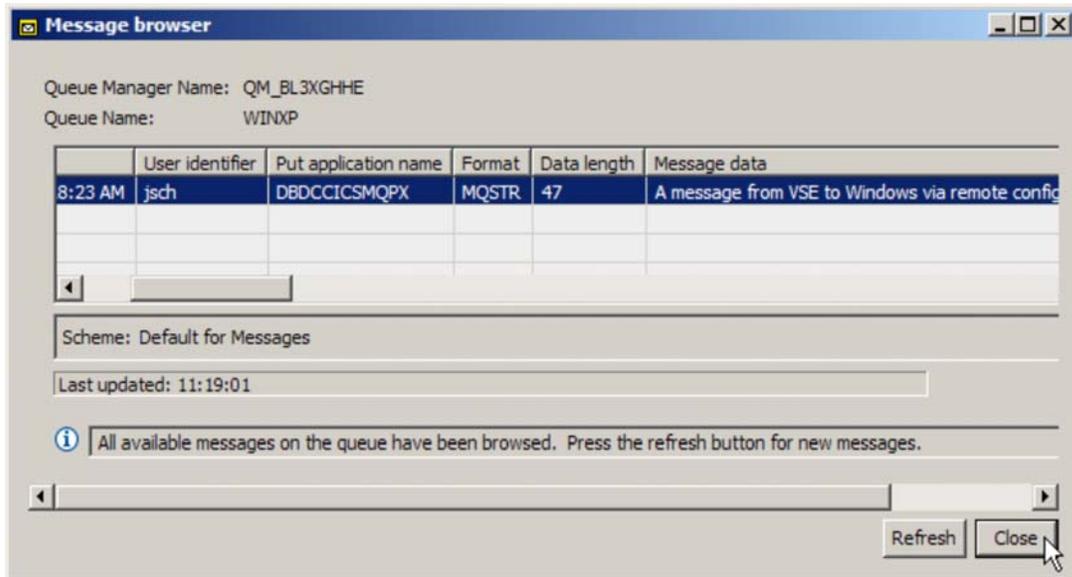
Enter some message text in the next box.



Press **Put message** to send the message from VSE to Windows via remote configuration in the MQ Explorer.



The next box shows that the message arrived in the WINXP queue on Windows.



Press **Close** to leave the box.

8.8 Defining SSL/TLS

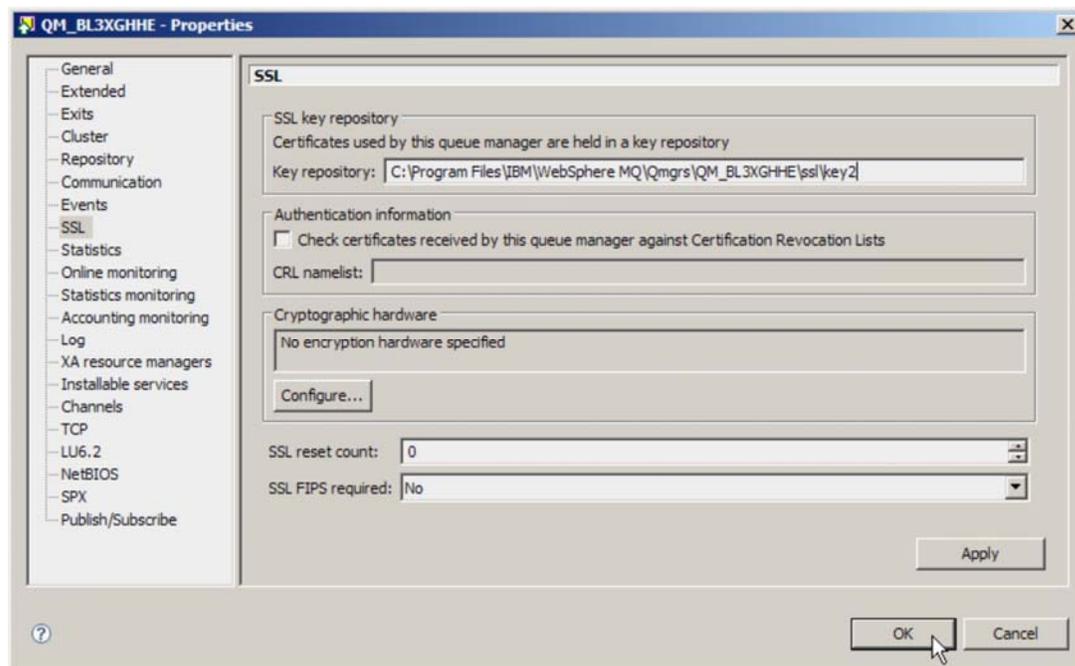
In previous chapters we discussed the problem of finding the right SSL cipher suites, so that the defined hex code on VSE matches with the defined cipher suite on Windows. Refer to Table 3 on page 47.

With the remote configuration via the MQ Explorer, this is now easy, because you now just define the same cipher suite name on both sides and the MQ Explorer translates the cipher suite name into the hex code used on the VSE side.

8.8.1 Defining SSL/TLS for the Windows side

First let's check again that the Windows queue manager has the right definitions.

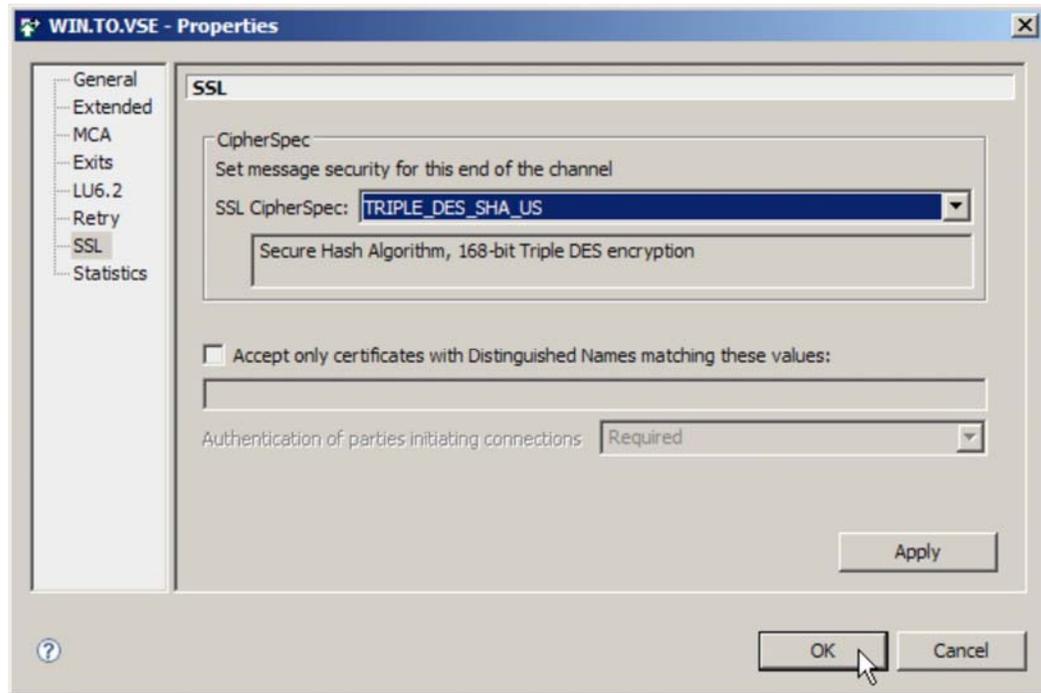
Display the Windows queue manager properties and select the SSL tab.



Verify that the displayed information is correct and press **OK**.

Now let's define SSL for the sender channel. Before doing so, the sender channel must be stopped. The new SSL properties will become active when restarting the channel.

Then display the sender channel properties window and select the SSL tab. Select one of the SSL cipher suites that can be used together with VSE, refer to Table 3 on page 47.

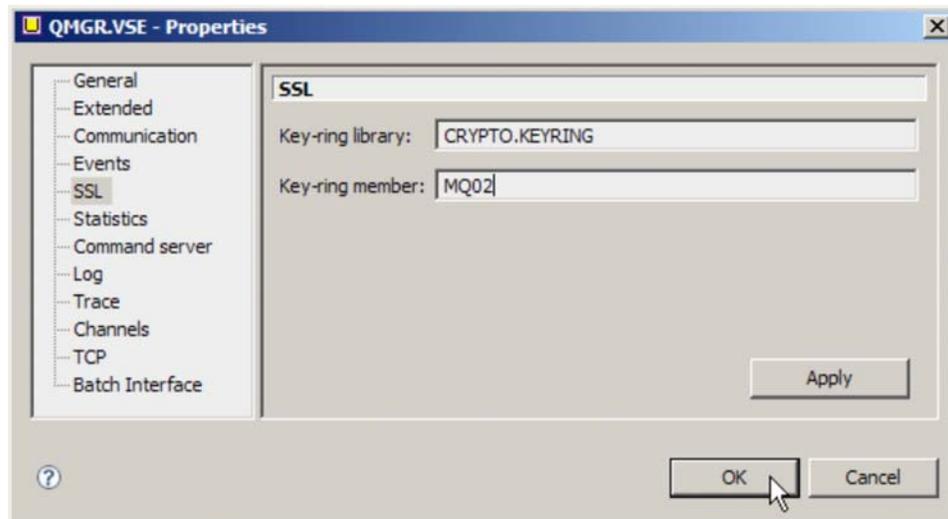


Press **OK**.

Don't restart the sender channel at this point, because we first have to define SSL for the VSE receiver channel.

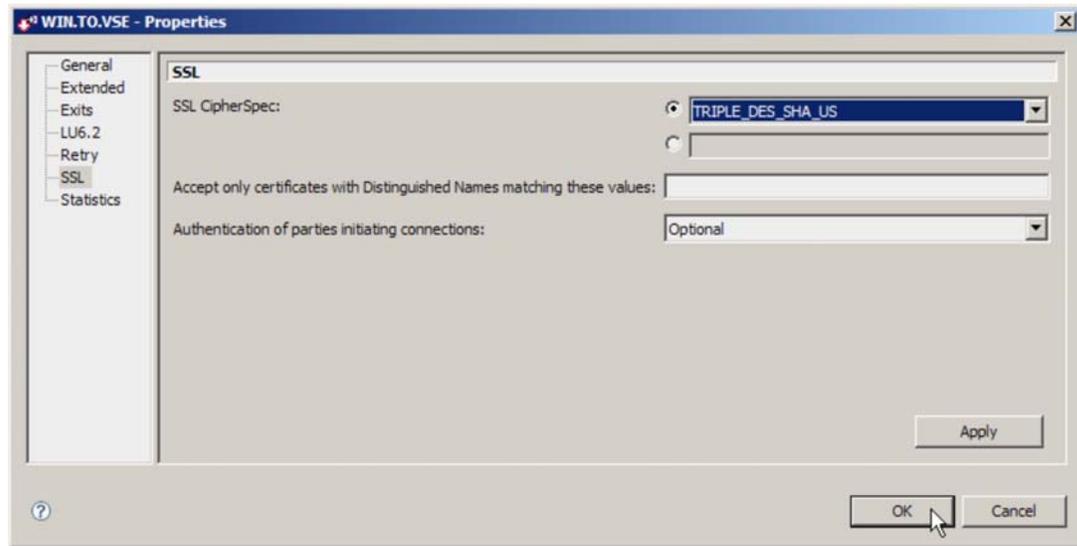
8.8.2 Defining SSL/TLS for the VSE side

Check that the VSE queue manager has the right definitions. Display the VSE queue manager properties and select the SSL tab. Without remote configuration this step would have to be done on VSE using the MQMT transaction.



Press **OK**.

Now let's define the SSL cipher suite for the VSE receiver channel. Display the receiver channel properties window and select the SSL tab.



Press **OK**.

Note: the AES-based cipher suites that do not work together with VSE (refer to Table 3 on page 47) are not displayed in the drop-down list box for selecting the SSL CipherSpec.

Just for completeness, let's now check on the VSE side, how the MQ Explorer made the definitions remotely on the VSE side.

Start the MQMT transaction and display the properties of the receiver channel.

```

02/19/2009          IBM WebSphere MQ for z/VSE Version 3.0.0          DBDCCICS
11:43:58           Channel SSL Parameters                            CIC1
MQWMCHN                                                    A000

Channel Name: WIN.TO.VSE          Type: R

SSL Cipher Specification. : 0A      (2 character code)
SSL Client Authentication :         (Required or Optional)

SSL Peer Attributes:
>                                     <
>                                     <
>                                     <
>                                     <

SSL channel parameters displayed.
F2=Return PF3=Quit PF4=Read F6=Update
    
```

MQ Explorer has correctly used the hex code of the cipher suite TRIPLE_DES_SHA_US.

You can now put a test message from Windows to VSE via SSL.

9 Troubleshooting

This chapter describes some problems encountered during the test setup.

9.1 Ciphers 2F and 35 do not work

As described in section 5.2.2 on page 46, the two AES cipher suites did not work for some unknown reason. This problem is currently unsolved and will probably ever be. Use cipher suite 0A instead although the use of Triple-DES makes you vulnerable by the SWEET32 issue. Refer to our security bulletin on <http://www.ibm.com/systems/z/os/zvse/support/preventive.html#security>

9.2 Message sequence number error

Symptom:

When starting the sender channel on Windows, or when trying to put a message to VSE, following messages appear on the VSE console.

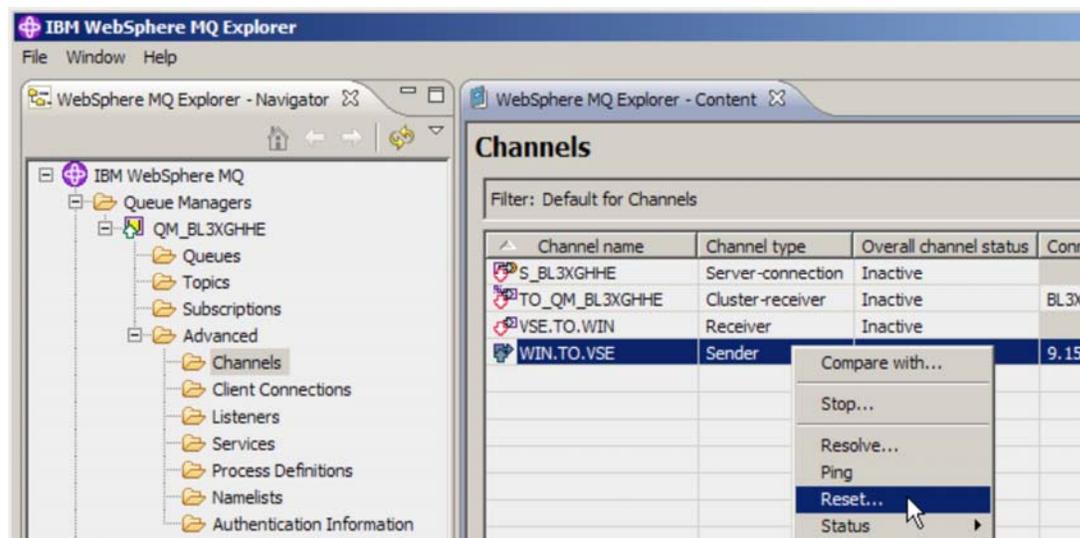
```
MQI0200I - MQI501028W Channel re-synchronization error
MQI0200I - MQI000003E Channel Message Sequence Number error
```

Reason:

There is a mismatch of the message sequence numbers on both ends. In our test setup this is most likely caused by the fact that we already exchanged messages between Windows and the first VSE system running MQ 2.1.2. To resolve the problem you have to reset the message sequence number on the sending end.

The problem showed up a second time after upgrading the MQ Explorer to V7.0.0.1. This time the receiver channel had to be reset.

On Windows just right-click the sender channel and perform a Reset.



9.3 RC =2092 when sending a test message to Windows

Symptom:

When sending a test message to Windows via TST2, an rc = 2092 is issued. TST2 displays following message.

```
MQ  ERROR:  LEVEL =INIT      , FUNC  =OPEN      , CC    =0002, RC    =2092****
```

Reason:

The USAGE parameter of the transmission queue is invalid. This error often happens, because the default USAGE when defining a local queue is set to N (normal). For the transmission queue you have to change the value to T (transmission). See section Defining the transmission queue on page 15.

9.4 Open of file MQFADMN failed

Symptom:

Following messages appear on the VSE console when trying to define the VSE queue manager as remote queue manager in MQ Explorer.

```
F2 0110 4228I FILE MQFADMN      OPEN  ERROR X'DC'(220) CAT=MQMCAT
      (OPNRP-20) THE BUFFERS IN BLDVRP TOO SMALL OR CI SIZE TOO LARGE
F2 0109 DFHFC0964 DBDCCICS Open of file MQFADMN failed. VSAM codes - 8502,
      0008,00DC
```

Reason:

The MQFADMN file is defined by job skeleton MQJQUEUE.Z with a max record size of 16000, which leads to a too large CI size of 16384. Delete the file and define it again with following values.

```
* $$ JOB JNM=MQJADMN,DISP=D,CLASS=A
* $$ LST DISP=H,CLASS=Q,PRI=3
// JOB MQJADMN DEFINE ADMN FILE
// EXEC IDCAMS,SIZE=AUTO
      DELETE (WMQZVSE.MQFADMN) CL NOERASE PURGE -
          CATALOG (MQ.USER.CATALOG)
      SET MAXCC = 0
DEF
  CLUSTER (NAME (WMQZVSE.MQFADMN) -
    FILE (MQFADMN) -
    VOL (SYSWK2) -
    RECORDS (1000 400) -
    RECORDSIZE (200 8000) -
    INDEXED -
    KEYS (56 0 ) -
    SHR (2)) -
  DATA (NAME (WMQZVSE.MQFADMN.DATA) CISZ(4096)) -
  INDEX (NAME (WMQZVSE.MQFADMN.INDEX) CISZ(512)) -
  CATALOG (MQ.USER.CATALOG)
/*
/&
* $$ EOJ
```

The same problem showed up for file MQFDEFS. Redefining the file as shown above solved the problem.

9.5 No space available for PUT request

Symptom:

Following messages repeatedly appear on the VSE console.

```
MQI0200I - MQI102091E No space available for PUT request
```

MQI0200I - MQI007022W PCF command processor could not send response message

Reason:

In our setup we first defined the MQFADMN file with RECORDS (300 200) which caused this problem. Obviously, the number of records should be increased. Redefining the file with RECORDS (1000 400) solved the problem.

The error occurs when an inbound queue is full. There are two ways to check which queue is full:

Use transaction MQQM and page through the display looking for FULL inbound status. This will also display the VSAM file that needs to be DELETE/DEFINE.

```

02/20/2009          IBM WebSphere MQ for z/VSE Version 3.0.0          DBDCCICS
08:41:22           Monitor Queues                                  CIC1
MQWMMOQ                                                    A000

                      QUEUING SYSTEM IS ACTIVE

S QUEUE              FILE      T INBOUND  OUTBOUND          LRDepth
XMT.WINXP            MQFO001 Y IDLE    IDLE              32             0
AMQ.MQEXPLORER.29884872 MQFADMN N FULL   ACTIVE           0              2
    
```

A second way is to browse the SYSTEM.LOG queue. Press PF1 to display last messages and then PF5 to display previous messages until you get the MQI102091E msg. You can then either use MQMQ to display the queue details to obtain the VSAM file. If the SYSTEM.LOG queue is full then messages are sent to CICS log so the MQI102091E messages may be there.

```

02/20/2009          IBM WebSphere MQ for z/VSE Version 3.0.0          DBDCCICS
08:44:45           Browse Queue Records                          CIC1
MQWDISP            SYSTEM IS ACTIVE                              A000

Object Name: SYSTEM.LOG
QSN Number : 00000172      LR-          0, LW-          173, DD-MQFLOG
Queue Data Record
Record Status : Written.    PUT date/time : 20090220084421
Message Size : 00000711    GET date/time :

MQI102091E PRG:MQPQUE1 TRN:MQCX TRM:... TSK:00500 02/20/2009 08:44:21
No space available for PUT request
QUEUE ID : AMQ.MQEXPLORER.29884872

2100-PUT-SET-QSN - QFULL status
9999-NOSPACE
EIBFN: 1206 EIBRCODE: 000000000000 EXEC LINE: 000000
EIBRESP: 00000000 EIBRESP2: 00000000 EIBRSRCE: ABCODE:

Information displayed.
5655-U97 Copyright IBM Corp. 2008. All rights reserved.
Enter=Process PF2=Return PF3=Quit PF4=Next PF5=Prior
PF11=MD PF12=Explain
    
```

10 More information

MQSeries for VSE System Management Guide, GC34-5364

<http://www.ibm.com/support/docview.wss?rs=171&uid=swg21230557>

WebSphere MQ for z/VSE V3.0 System Management Guide, GC34-6981

<http://www.ibm.com/software/integration/wmq/library/library3x.html>

Using MQSeries for VSE, SG24-5647, Redbook

<http://www.redbooks.ibm.com/abstracts/sg245647.html?Open>

Service summary for MQSeries for VSE 2.1.2

http://www.ibm.com/support/docview.wss?rs=171&context=SSFKSJ&context=SSWHKB&dc=DB500&q1=MQSeries+for+VSE&q2=MQSeries+for+VSE+2.1.0&uid=swg21230557&loc=en_US&cs=utf-8&lang=en

Download WebSphere MQ for Windows V7.0 (90-days trial version)

<https://www14.software.ibm.com/webapp/dswdown/dswdown.wss/web/searchDescription>

WebSphere MQ Security - SC34-6588

<http://www.elink.ibm.com/publications/servlet/pbi.wss?CTY=US&FNC=SRX&PBL=SC34658802>

WebSphere MQ library

<http://www.ibm.com/software/integration/wmq/library/library6x.html>

WebSphere MQ Version 6 and Web Services. SG24-7115, Redbook

<http://www.redbooks.ibm.com/abstracts/sg247115.html?Open>

WebSphere V5 for Linux on zSeries Connectivity Handbook - SG24-7042, Redbook

<http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg247042.html?Open>

Download Keyman/VSE from the VSE Internet homepage

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

z/VSE V4R2 Administration, SC33-8304

<http://www.ibm.com/servers/eserver/zseries/zvse/documentation/#vse>