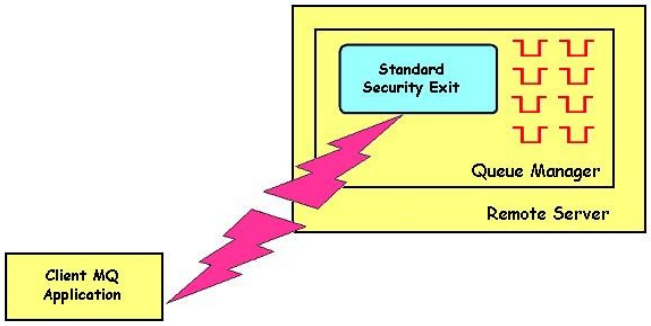
MQSSX for z/OS Queue Manager To Queue Manager Configuration Manual



Capitalware Inc.
Unit 11, 1673 Richmond Street, PMB524
London, Ontario N6G2N3
Canada
sales@capitalware.com
https://www.capitalware.com

Last Updated: July 2020.

Table of Contents

1 Introduction

1.1 Overview

MQ Standard Security Exit for z/OS (z/MQSSX) is a solution that allows a company to control and restrict who is accessing a IBM MQ resource. The security exit will operate with IBM MQ v5.3.1, v6.0, v7.0, v7.1, v8.0, v9.0, v9.1 and v9.2 for z/OS environments. It works with Server Connection, Receiver, Requester and Cluster-Receiver channels of IBM MQ queue manager.

The MQ Standard Security Exit for z/OS solution is comprised of a server-side security exit.

The server-side security exit has the ability to allow or restrict the incoming UserID. The server-side security exit uses a regular expression parser to parse the incoming client UserID against a predefined regular expression pattern.

The server-side security exit supports the concept of 'Proxy IDs'. After a user has been successfully validated against the native OS or file based validation data and the 'Proxy Mode' flag is set, then the security exit will look up the user's UserID in the Proxy file for their Proxy ID. The Proxy ID will be used for all MQ interactions.

The server-side security exit has the ability to allow or restrict users from connecting with a blank UserID value. This is controlled by the server-side security exit's property keyword 'AllowBlankUserID'.

The server-side security exit has the ability to block users from logging in with the 'CHIN' or the CHIN's Started-task UserIds. This is controlled by the server-side security exit's property keyword 'Allowmqm'.

The server-side security exit has the capability to allow or limit the incoming channel connections according to the name of the associated Server Connection channel (SVRCONN). Each Server Connection channel can be allocated a maximum number of connections and the server-side security exit will ensure that this maximum is not exceeded.

Client connections to a queue manager are limited by either channel name or the 'DefaultMCC' property keyword in the initialization file. In today's use of J2EE applications, it is a possibility that one J2EE application could overwhelm the queue manager with client connections, thus preventing any connections being made from other applications.

The server-side security exit has the ability to allow or restrict the incoming IP address, hostname and/or SSL DN. The server-side security exit uses a regular expression parser to parse the incoming client IP address and/or SSL DN against a predefined regular expression pattern.

The server-side security exit has the ability to allow or restrict the incoming UserID against a group. A list of groups can be queried for the incoming UserID. The groups are stored a group file.

2 Queue Manager To Queue Manager Overview

This section provides an overview of how z/MQSSX can verify the IP Address and/or UserId of the connection request from one queue manager to any queue manager.

As mentioned in Chapter 1, z/MQSSX is comprised of a server-side security exit.

2.1 Sender and Receiver Channel Pair

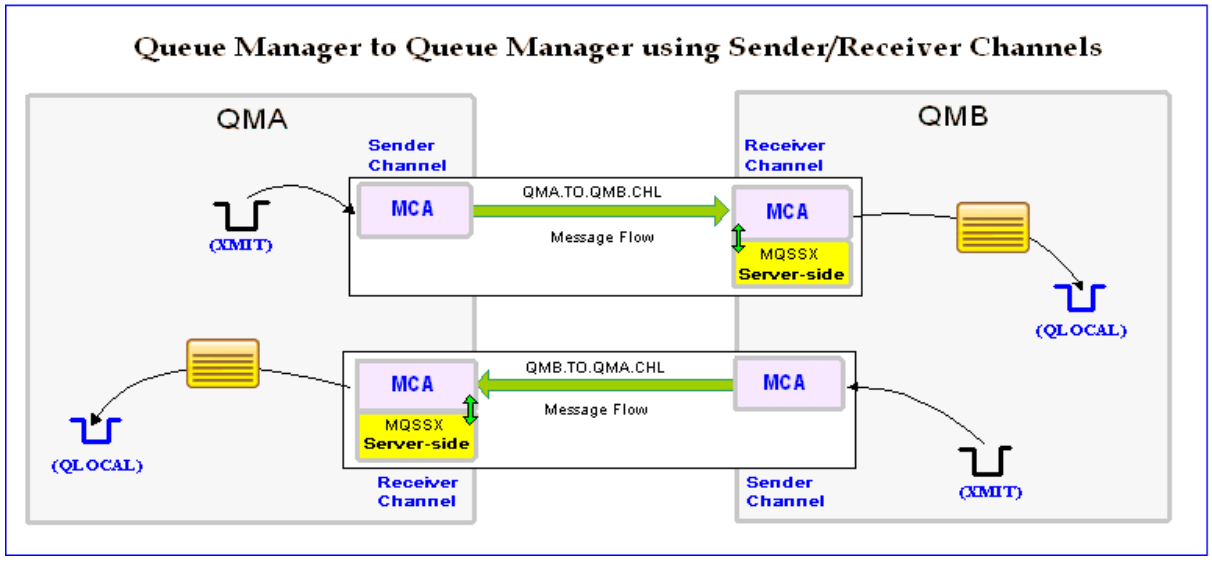
As noted below (in yellow) in the diagram, the z/MQSSX server-side security exit works with the Receiver (RCVR) channel.

There is a Message Channel Agent (MCA) at each end of the channel. The MCA is a component that handles the sending and receiving of messages between queue managers. Before the MCA can send and receive messages, the z/MQSSX server-side security exit must verify the incoming UserId and/or IP Address as detailed below:

- The MCA that is running the Receiver channel will call z/MQSSX server-side security exit to verify the incoming UserId and/or IP Address.

After verification has been successful, the channel will go to a 'Running' state and the messages will flow along the channel.

The following diagram highlights security exits in an MQ environment:



2.2 Server and Requester Channel Pair

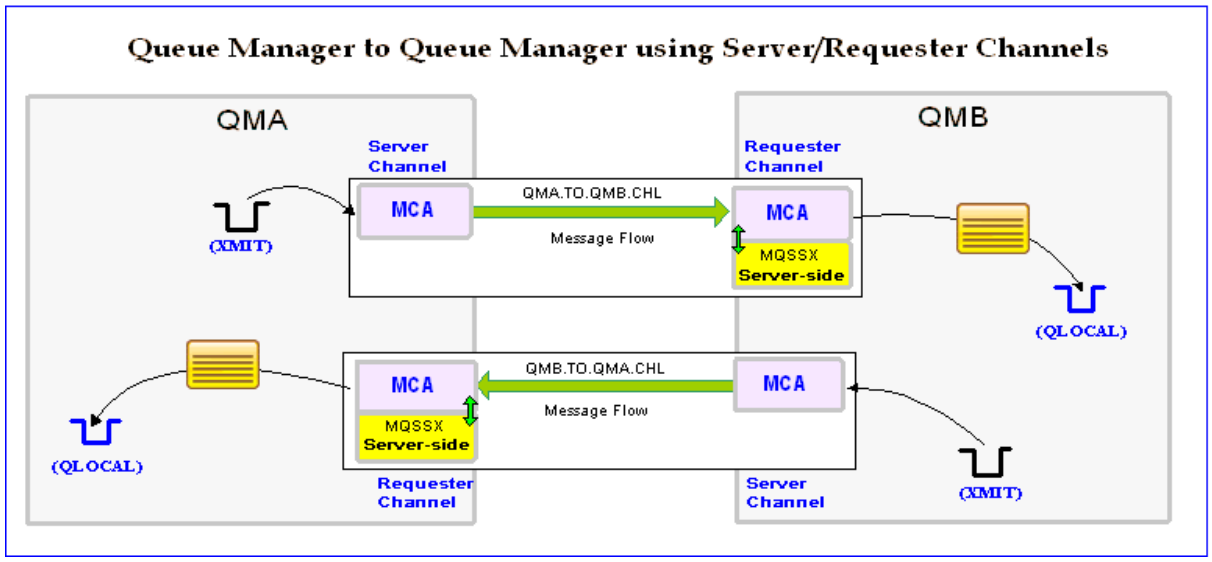
As noted below (in yellow) in the diagram, the z/MQSSX server-side security exit works with the Requester (RQSTR) channel.

There is a Message Channel Agent (MCA) at each end of the channel. The MCA is a component that handles the sending and receiving of messages between queue managers. Before the MCA can send and receive messages, the z/MQSSX server-side security exit must verify the incoming UserId and/or IP Address as detailed below:

- The MCA that is running the Requester channel will call z/MQSSX server-side security exit to verify the incoming UserId and/or IP Address.

After verification has been successful, the channel will go to a 'Running' state and the messages will flow along the channel.

The following diagram highlights security exits in an MQ environment:



3 Configuring a Receiver Channel

This section describes the necessary entries to enable the server-side security exit on a Receiver Channel. The server-side security exit and its data will be applied to 2 fields of the Receiver Channel. The MQ Administrator will need to update these 2 fields of the Receiver Channel.

For more information on server-side IniFile parameters, please review *Appendix A* of the ***MQSSX for z/OS Server-side Installation and Operation*** manual.

3.1 z/OS

On z/OS, SCYEXIT and SCYDATA will contain the following values assuming a default install:

- SCYEXIT
  MQSSX
- SCYDATA
  MQSSXIN

The following is an example of an MQSC command for creating a Receiver Channel with the server-side security exit and its data:

```
DEFINE CHANNEL ('QMA.TO.QMB.CHL') CHLTYPE(RCVR) +
       TRPTYPE(TCP) +
       SCYEXIT('MQSSX') +
       SCYDATA('MQSSXIN') +
       REPLACE
```

4 Configuring a Requester Channel

This section describes the necessary entries to enable the server-side security exit on a Requester Channel. The server-side security exit and its data will be applied to 2 fields of the Requester Channel. The MQ Administrator will need to update these 2 fields of the Requester Channel.

For more information on server-side IniFile parameters, please review *Appendix A* of the ***MQSSX for z/OS Server-side Installation and Operation*** manual.

4.1 z/OS

On z/OS, SCYEXIT and SCYDATA will contain the following values assuming a default install:

- SCYEXIT
  MQSSX
- SCYDATA
  MQSSXIN

The following is an example of an MQSC command for creating a Receiver Channel with the server-side security exit and its data:

```
DEFINE CHANNEL ('QMA.TO.QMB.CHL') CHLTYPE(RQSTR) +
       TRPTYPE(TCP) +
       SCYEXIT('MQSSX') +
       SCYDATA('MQSSXIN') +
       REPLACE
```

5 Appendix A – License Agreement

This is a legal agreement between you (either an individual or an entity) and Capitalware Inc. By opening the sealed software packages (if appropriate) and/or by using the SOFTWARE, you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, promptly return the disk package and accompanying items for a full refund.
SOFTWARE LICENSE

1. GRANT OF LICENSE. This License Agreement (License) permits you to use one copy of the software product identified above, which may include user documentation provided in on-line or electronic form (SOFTWARE). The SOFTWARE is licensed as a single product, to an individual user, or group of users for Muliple User Licenses and Site Licenses. This Agreement requires that each user of the SOFTWARE be Licensed, either individually, or as part of a group. A Multi-User License provides for a specified number of users to use this SOFTWARE at any time. This does not provide for concurrent user Licensing. Each user of this SOFTWARE must be covered either individually, or as part of a group Multi-User License. The SOFTWARE is in use on a computer when it is loaded into the temporary memory (i.e. RAM) or installed into the permanent memory (e.g. hard disk) of that computer. This software may be installed on a network provided that appropriate restrictions are in place limiting the use to registered users only.

2. COPYRIGHT. The SOFTWARE is owned by Capitalware Inc. and is protected by United States Of America and Canada copyright laws and international treaty provisions. You may not copy the printed materials accompanying the SOFTWARE (if any), nor print copies of any user documentation provided in on-line or electronic form. You must not redistribute the registration codes provided, either on paper, electronically, or as stored in the files MQSSX IniFile or any other form.

3. OTHER RESTRICTIONS. The registration notification provided, showing your authorization code and this License is your proof of license to exercise the rights granted herein and must be retained by you. You may not rent or lease the SOFTWARE, but you may transfer your rights under this License on a permanent basis, provided you transfer this License, the SOFTWARE and all accompanying printed materials, retain no copies, and the recipient agrees to the terms of this License. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except to the extent the foregoing restriction is expressly prohibited by applicable law.

LIMITED WARRANTY

LIMITED WARRANTY. Capitalware Inc. warrants that the SOFTWARE will perform substantially in accordance with the accompanying printed material (if any) and on-line documentation for a period of 365 days from the date of receipt.

CUSTOMER REMEDIES. Capitalware Inc. entire liability and your exclusive remedy shall be, at Capitalware Inc. option, either (a) return of the price paid or (b) repair or replacement of the SOFTWARE that does not meet this Limited Warranty and that is returned to Capitalware Inc. with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be

warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, Capitalware Inc. disclaims all other warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to the SOFTWARE and any accompanying written materials.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable law, in no event shall Capitalware Inc. be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use or inability to use the SOFTWARE, even if Capitalware Inc. has been advised of the possibility of such damages.

6 Appendix B – Notices

Trademarks:

AIX, IBM, MQSeries, OS/2 Warp, OS/400, iSeries, MVS, OS/390, WebSphere, IBM MQ and z/OS are trademarks of International Business Machines Corporation.

HP-UX is a trademark of Hewlett-Packard Company.

Intel is a registered trademark of Intel Corporation.

Java, J2SE, J2EE, Sun and Solaris are trademarks of Sun Microsystems Inc.

Linux is a trademark of Linus Torvalds.

Mac OS X is a trademark of Apple Computer Inc.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation.

UNIX is a registered trademark of the Open Group.

WebLogic is a trademark of BEA Systems Inc.