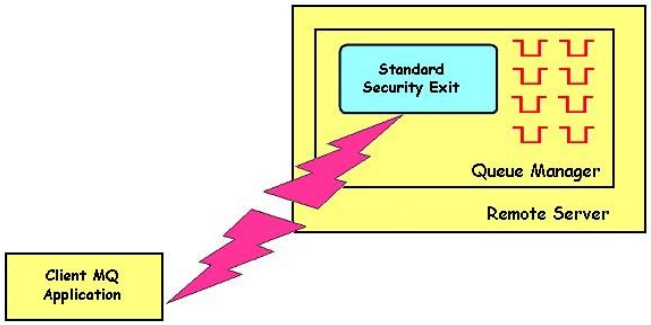
MQ Standard Security Exit Overview



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

Last Updated: January 2021.
© Copyright Capitalware Inc. 2005, 2021.

Table of Contents

1 INTRODUCTION.....1

1.1 Overview.....1
1.2 Executive Summary.....2
1.3 Context Diagram (Logical View).....3
1.4 Security Message Flow (Logical View).....3
1.5 Prerequisites.....4
1.5.1 Operating System.....4
1.5.2 IBM MQ.....5
1.5.3 Windows 64-bit.....5

1 Introduction

1.1 Overview

MQ Standard Security Exit (MQSSX) is a new solution that allows a company to control and restrict who is accessing a IBM MQ resource. The security exit will operate with IBM MQ v7.1, v7.5, v8.0, v9.0, v9.1 and v9.2 in Windows, Unix, IBM i and Linux environments. It works with Server Connection, Receiver, Requester and Cluster-Receiver channels of IBM MQ queue manager.

The MQ Standard Security Exit 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 'mqm' or 'MUSR_MQADMIN' or 'QMQM' 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 MQAdmin can enable Excessive Client Connections alerting system that counts the number of connections over a period of time (i.e. Day / Hour / Minute) and writes a message to the log when the count exceeds a particular value. If the keyword WriteToEventQueue is set to ‘Y’ then an event message is also written to an event queue. ECC feature is designed to catch applications that are poorly written, for example, applications that continuously connect and disconnect from the queue manager for every message sent or received.

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 can be in the local OS or a group file.

On AIX, HP-UX, Linux, Solaris and Windows, MQSSX can be configured and used with a non-default installation of MQ in a multi-install MQ environment.

Note: Raspberry Pi is a Linux ARM 32-bit OS (Operating System). Hence, simply follow the Linux 32-bit instructions for installing and using the solution on a Raspberry Pi.

1.2 Executive Summary

The MQ Standard Security Exit solution contains a server-side security exit.

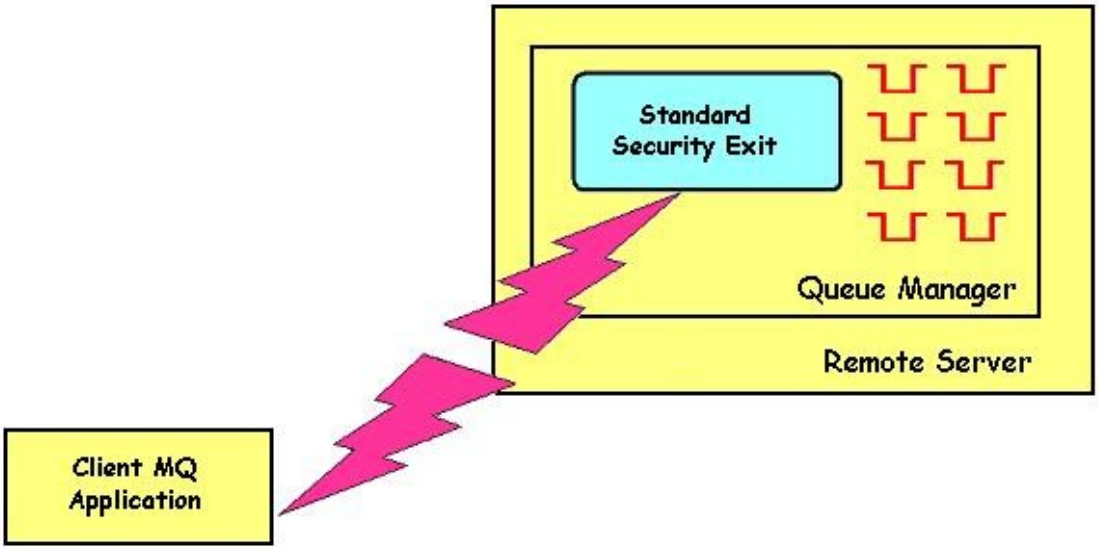
The server-side security exit is available in 3 forms:

- Windows DLL
- Shared library for AIX, HP-UX, Linux, and Solaris.
- IBM i exit module

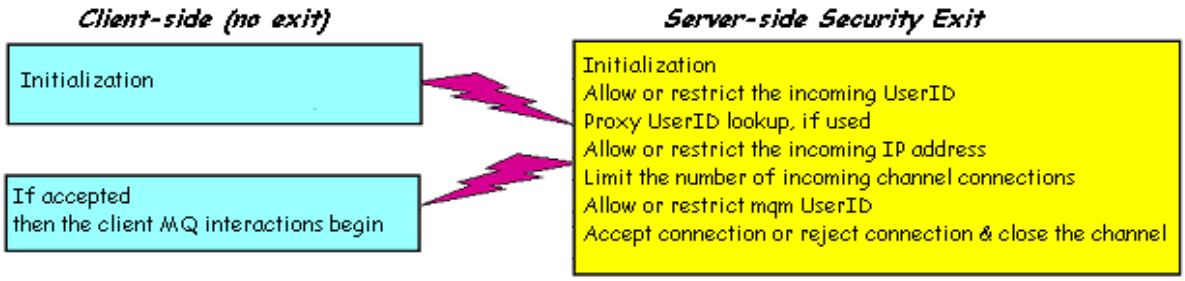
The major features of MQ Standard Security Exit are as follows:

- Allows or restricts the incoming UserID against a regular expression pattern
- Allows or restricts the incoming UserID against a Group
- Provides support for Proxy UserIDs
- Allows or restricts the incoming IP address against a regular expression pattern
- Allows or restricts the incoming hostname against a regular expression pattern
- Allows or restricts the incoming SSL DN against a regular expression pattern
- Limit the number of incoming channel connections on a SVRCONN channel.
- Allows or restricts the use of 'mqm', 'MUSER_MQADMIN' or 'QMQM' UserIDs
- Ability to set the maximum number of allowable connections per a given channel (MCC)
- Ability to monitor for excessive client connections (ECC) and then generate an alert
- Provides monitoring tool tie-in by using custom MQ event messages
- Provides logging capability for all connecting client applications regardless if they were successful or not.

1.3 Context Diagram (Logical View)



1.4 Security Message Flow (Logical View)



1.5 Prerequisites

This section provides the minimum supported software levels. These prerequisites apply to server-side installations of MQ Standard Security Exit.

1.5.1 Operating System

MQ Standard Security Exit can be installed on any of the following supported servers:

1.5.1.1 IBM AIX

- IBM AIX 6L version 6.1 or higher

1.5.1.2 HP-UX IA64

- HP-UX v11.23 or higher

1.5.1.3 IBM i (OS/400)

- IBM i V6R1 or higher

1.5.1.4 Linux x86

- Red Hat Enterprise Linux v5, v6, v7, v8
- SUSE Linux Enterprise Server v11, v12, v15

1.5.1.5 Linux x86_64 (64-bit)

- Red Hat Enterprise Linux v5, v6, v7, v8
- SUSE Linux Enterprise Server v11, v12, v15

1.5.1.6 Linux on POWER

- Red Hat Enterprise Linux v5, v6, v7, v8
- SUSE Linux Enterprise Server v11, v12, v15

1.5.1.7 Linux on zSeries (64-bit)

- Red Hat Enterprise Linux v5, v6, v7, v8
- SUSE Linux Enterprise Server v11, v12, v15

1.5.1.8 Raspberry Pi (Linux ARM 32-bit)

- Raspberry Pi OS v9 or higher

1.5.1.9 Sun Solaris

- Solaris SPARC v10 or higher
- Solaris x86_64 v10 or higher

1.5.1.10 Windows

- Windows 2008, 2012 or 2016 Server (32-bit & 64-bit)
- Windows 7, 8, 8.1 & 10 (32-bit & 64-bit)

1.5.2 IBM MQ

- IBM MQ v7.1, v7.5, v8.0, v9.0, v9.1 and v9.2 (both 32-bit and 64-bit)

Operating System	MQ v7.1, v7.5, v8.0, v9.0, v9.1 and v9.2
AIX v6.1 or higher	64-bit
HP-UX IA64 v11.23 or higher	64-bit
IBM i (OS/400)	64-bit
Linux x86	32-bit
Linux x86_64	64-bit
Linux on POWER	64-bit
Linux on zSeries	64-bit
Raspberry Pi ARM	32-bit
Solaris SPARC v10 & v11	64-bit
Solaris x86_64 v10 & v11	64-bit
Windows 2008, 2012, 2016, 7, 8, 8.1 & 10	32-bit & 64-bit

1.5.3 Windows 64-bit

The following is the software prerequisite for Windows 64-bit:

- Microsoft Visual C++ 2010 Redistributable Package (x64)
  https://www.microsoft.com/en-ca/download/details.aspx?id=14632