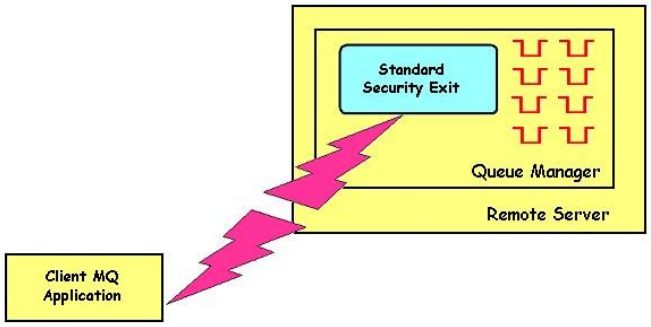
MQ Standard Security Exit for z/OS Overview



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 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 are stored a group file.

1.2 Executive Summary

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

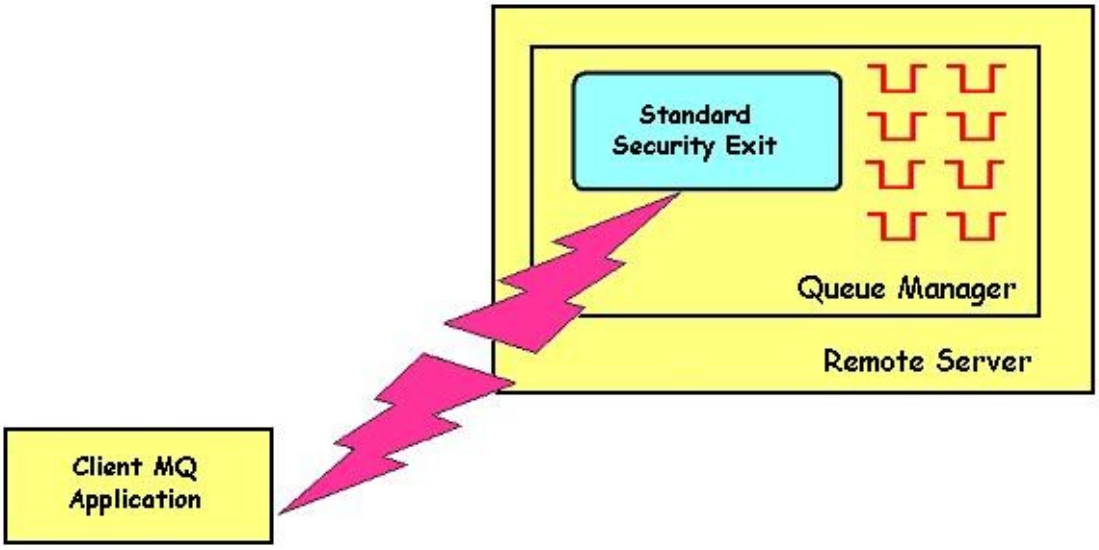
The server-side security exit is available as:

- z/OS load-module

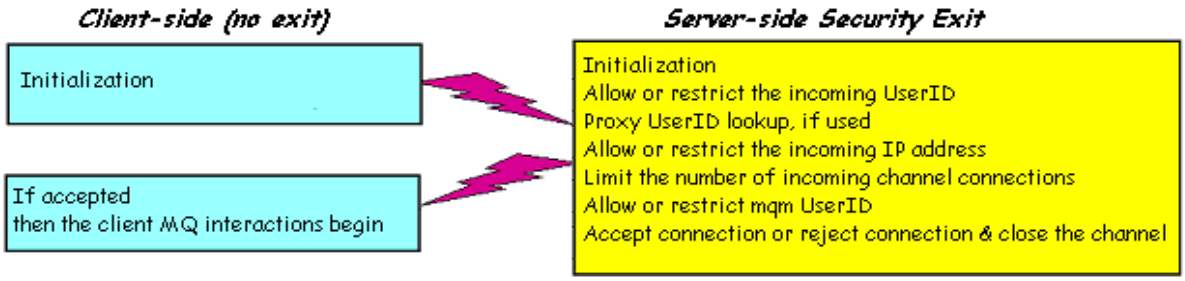
The major features of MQ Standard Security Exit for z/OS are as follows:

- 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 the 'CHIN' or the CHIN's Started-task 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 logging capability for all connecting client applications regardless if they were successful or not.
- Provides logging capability via Write To Operator (WTO) facility.

1.3 Context Diagram (Logical View)



1.4 Security Message Flow (Logical View)



1.5 Prerequisites

This section details the minimum supported software levels. These prerequisites apply to the server-side installations of MQ Standard Security Exit for z/OS.

1.5.1 Operating System

MQ Standard Security Exit for z/OS can be installed on any of the following supported servers:

1.5.1.1 IBM z/OS

- IBM z/OS v1.4 or higher

1.5.2 IBM MQ

- IBM MQ for z/OS v5.3.1, v6.0, v7.0, v7.1, v8.0, v9.0, v9.1 and v9.2