

MQ Security with Capitalware's MQAUSX & z/MQAUSX

Roger Lacroix
roger.lacroix@capitalware.biz
<http://www.capitalware.biz>

MQAUSX & z/MQAUSX Overview

- MQ Authenticate User Security Exit (MQAUSX) & MQ Authenticate User Security Exit for z/OS (z/MQAUSX) are solutions that allows a company to fully authenticate a user who is accessing a WebSphere MQ resource.
- MQAUSX authenticates the user's UserId and Password against the server's native OS system, LDAP server, Microsoft's Active Directory, Quest Authentication Services, Centrify's DirectControl or an encrypted MQAUSX FBA file.
- z/MQAUSX authenticates the user's UserId and Password against the z/OS server's native OS system. or an encrypted MQAUSX FBA file.

MQAUSX & z/MQAUSX Overview

- The **same** client-side security exit first checks if the server-side exit is defined for the particular channel. The client-side exit will receive a security token to be used in the encryption process of the user's password. It will prompt the user for his / her UserId and Password, encrypt the data and send it to the server-side security exit.

MQAUSX & z/MQAUSX are 3 products in 1

- If the client application is configured with the client-side security exit then the user credentials are encrypted and sent to the remote queue manager. ***This is the best level of security.***
- If the client application is not configured with the client-side security exit then the user credentials are sent in plain text to the remote queue manager. This feature is available for Java/JMS, Java and C# DotNet client applications. For native applications (i.e. C/C++), then the application must use and populate the MQCSP structure with the UserID and Password.
 - Using MQAUSX with No Client-side Security Exit - Part 1 (coding examples)
http://www.capitalware.biz/rl_blog/?p=638
 - Using MQAUSX with No Client-side Security Exit - Part 2 (configuring tools like MQ Explorer, SupportPac MO71, MQ Visual Edit, etc..)
http://www.capitalware.biz/rl_blog/?p=659
- If the MQAdmin sets the MQAUSX IniFile parameter NoAuth to Y then it functions just like MQ Standard Security Exit (MQSSX or z/MQSSX). MQSSX does not authenticate. It filters the incoming connection based on UserID, IP address, hostname and/or SSL DN.

MQAUSX Secondary Features

- 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 SSL DN against a regular expression pattern
- Allows or restricts the incoming UserID against a regular expression pattern
- Allows or restricts the incoming AD server name against a regular expression pattern (Windows only)
- 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 turn off server-side authentication
- Provides monitoring tool tie-in by using custom MQ event messages
- Provides logging capability for all connecting client applications regardless if they are successful or not.

z/MQAUSX Secondary Features

- 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
- Limit the number of incoming channel connections on a SVRCONN channel.
- Allows or restricts the use of 'CHIN' or the CHIN's Started-task UserIDs
- Ability to turn off server-side authentication
- Allows or restricts the incoming UserID against a regular expression pattern when authentication is off
- Provides logging capability for all connecting client applications regardless if they were successful or not.
- Provides logging capability via Write To Operator (WTO) facility.

MQAUSX & z/MQAUSX Keywords

- MQAUSX has 103 keywords and values that can be used.
- z/MQAUSX has 62 keywords and values that can be used.

MQAUSX Configuration via MQAUSX-GUI

The screenshot displays the MQAUSX-GUI configuration window. The title bar indicates the file path: C:\Capitalware\MQAUSX\mqausx.ini. The window has a menu bar with 'File' and 'Help'. Below the menu bar is a toolbar with icons for file operations and help. A left-hand sidebar contains a list of configuration categories: General, Authentication, LDAP, Group, Proxy, UserId, IP Address, Hostname, HostByName, SSL DN, Max Client Channel, and AD Name. The 'General' category is selected and highlighted. The main area of the window is divided into two sections: 'General' and 'Logging'. The 'General' section includes fields for License, LicenseFile, and Description. The 'Logging' section includes a LogMode dropdown set to 'Normal', a LogFile text box containing 'C:\Capitalware\MQAUSX\mqausx.log', a RotateLogDaily dropdown set to 'Yes' with a BackupLogFileCount of 9, a WriteToSystemLog dropdown set to 'No' with a SystemLogMessage dropdown set to 'Both', and a WriteToEventQueue dropdown set to 'No' with an EventQueueName text box containing 'SYSTEM.ADMIN.CHANNEL.EVENT'.

MQAUSX-GUI : C:\Capitalware\MQAUSX\mqausx.ini

File Help

General

Authentication

LDAP

Group

Proxy

UserId

IP Address

Hostname

HostByName

SSL DN

Max Client Channel

AD Name

General

License

LicenseFile

Description

Logging

LogMode Normal

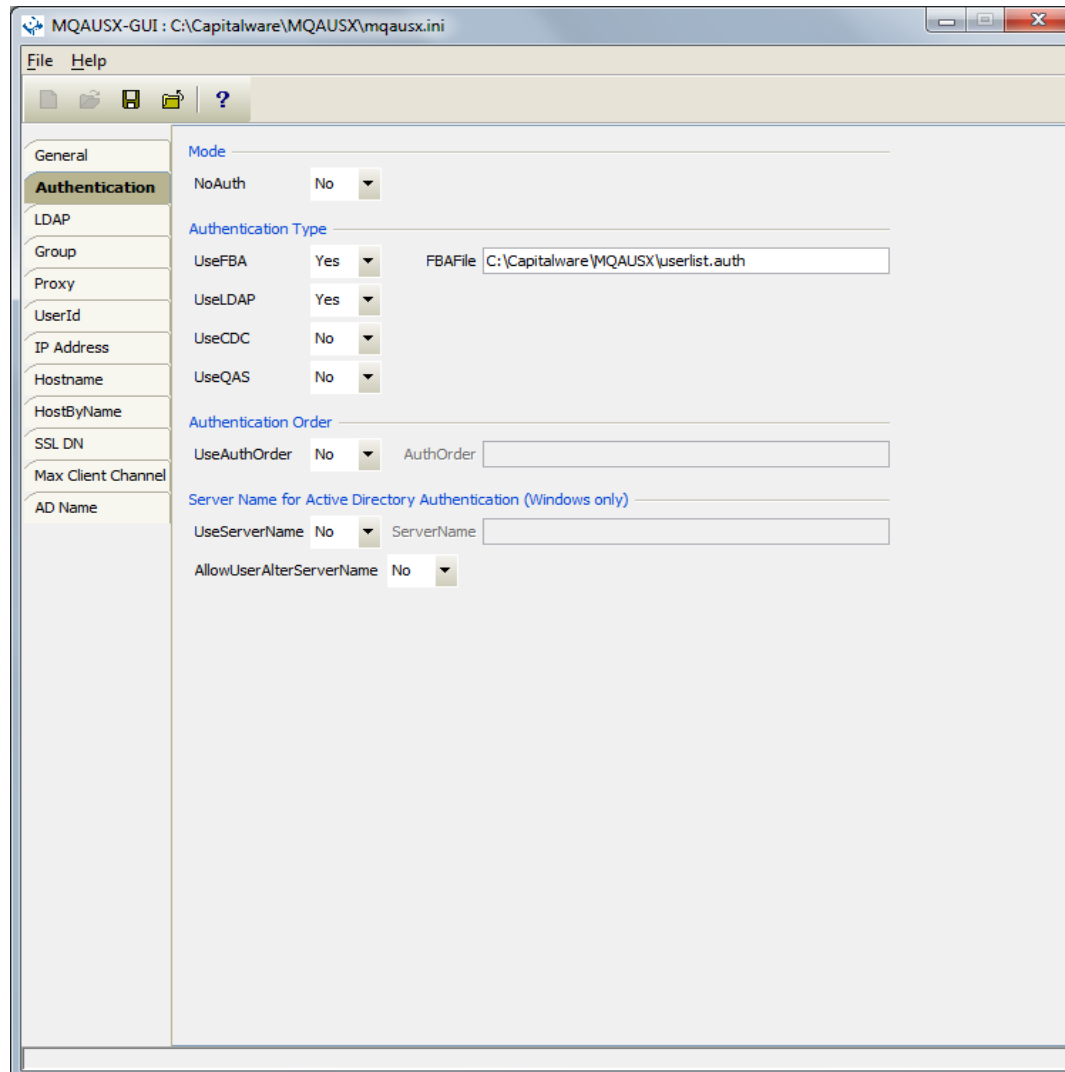
LogFile C:\Capitalware\MQAUSX\mqausx.log

RotateLogDaily Yes BackupLogFileCount 9

WriteToSystemLog No SystemLogMessage Both

WriteToEventQueue No EventQueueName SYSTEM.ADMIN.CHANNEL.EVENT

MQAUSX Configuration via MQAUSX-GUI



MQAUSX Configuration via MQAUSX-GUI

The screenshot displays the MQAUSX-GUI configuration window, titled "MQAUSX-GUI : C:\Capitalware\MQAUSX\mqausx.ini". The window features a menu bar with "File" and "Help", and a toolbar with icons for file operations and help. A left-hand sidebar contains a list of configuration categories: General, Authentication, LDAP (selected), Group, Proxy, User Id, IP Address, Hostname, HostByName, SSL DN, Max Client Channel, and AD Name. The main content area is divided into several sections for LDAP configuration:

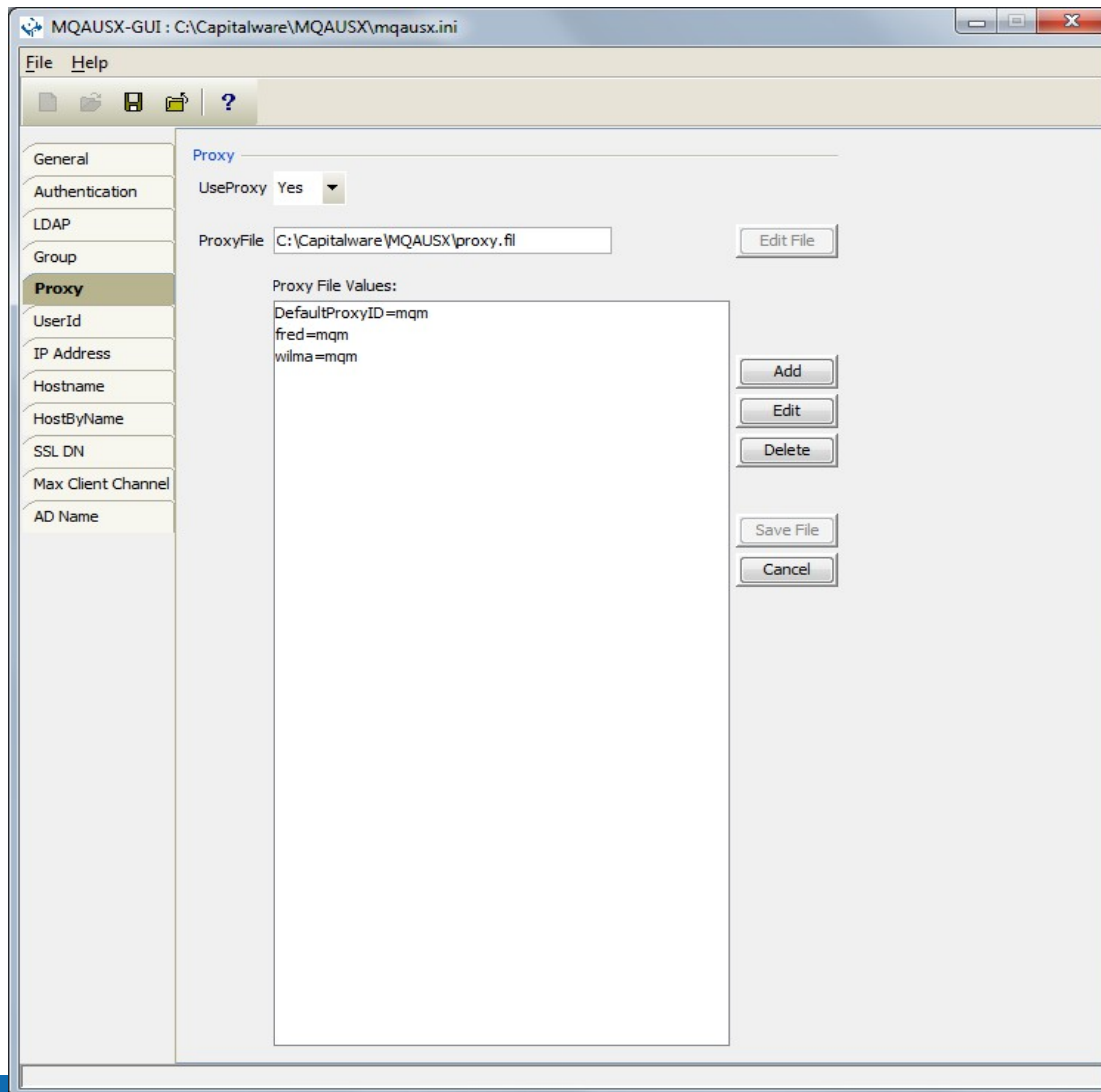
- LDAP Section:**
 - LDAPHost: ldap.capitalware.biz
 - LDAPPort: 389;555
 - LDAPTimeOut: 5
 - UseLDAPLoadBalance: Yes (dropdown)
 - LDAPBaseDN: CN=Users,DC=capitalware,DC=biz
 - UseLDAPBindDN: No (dropdown)
 - LDAPBindDN: (empty text field)
 - LDAPBindPwd: (empty text field)
 - UseLDAPAuthCompare: No (dropdown)
- LDAP SSL Section:**
 - UseLDAPSSL: No (dropdown)
 - UseLDAPSSLCert: No (dropdown)
 - SSLCertFileType: DER (dropdown)
 - SSLCertFileName: (empty text field)
 - SSLCertPwd: (empty text field)
- LDAP LoginDN Prefix Section:**
 - UseLoginDNPrefix: No (dropdown)
 - LoginDNPrefix: (empty text field)
- LDAP Ambiguous Name Resolution (ANR) Section:**
 - UseANRforLDAP: No (dropdown)
 - UseANRPrefix: No (dropdown)
 - ANRPrefix: (empty text field)
 - UseANRPostfix: No (dropdown)
 - ANRPostfix: (empty text field)
 - ExtractUserIDFromANR: No (dropdown)
 - UseANRDelimiter: No (dropdown)
 - ANRDelimiter: @ (text field)
- LDAP UserID Search Section:**
 - UseLDAPUserIDSearch: No (dropdown)
 - LDAPUserIDSearchScope: LDAP_SCOPE_ONELEVEL (dropdown)
 - LDAPUserIDSearchBase: (empty text field)
 - LDAPUserIDSearchFilter: (empty text field)

MQAUSX Configuration via MQAUSX-GUI

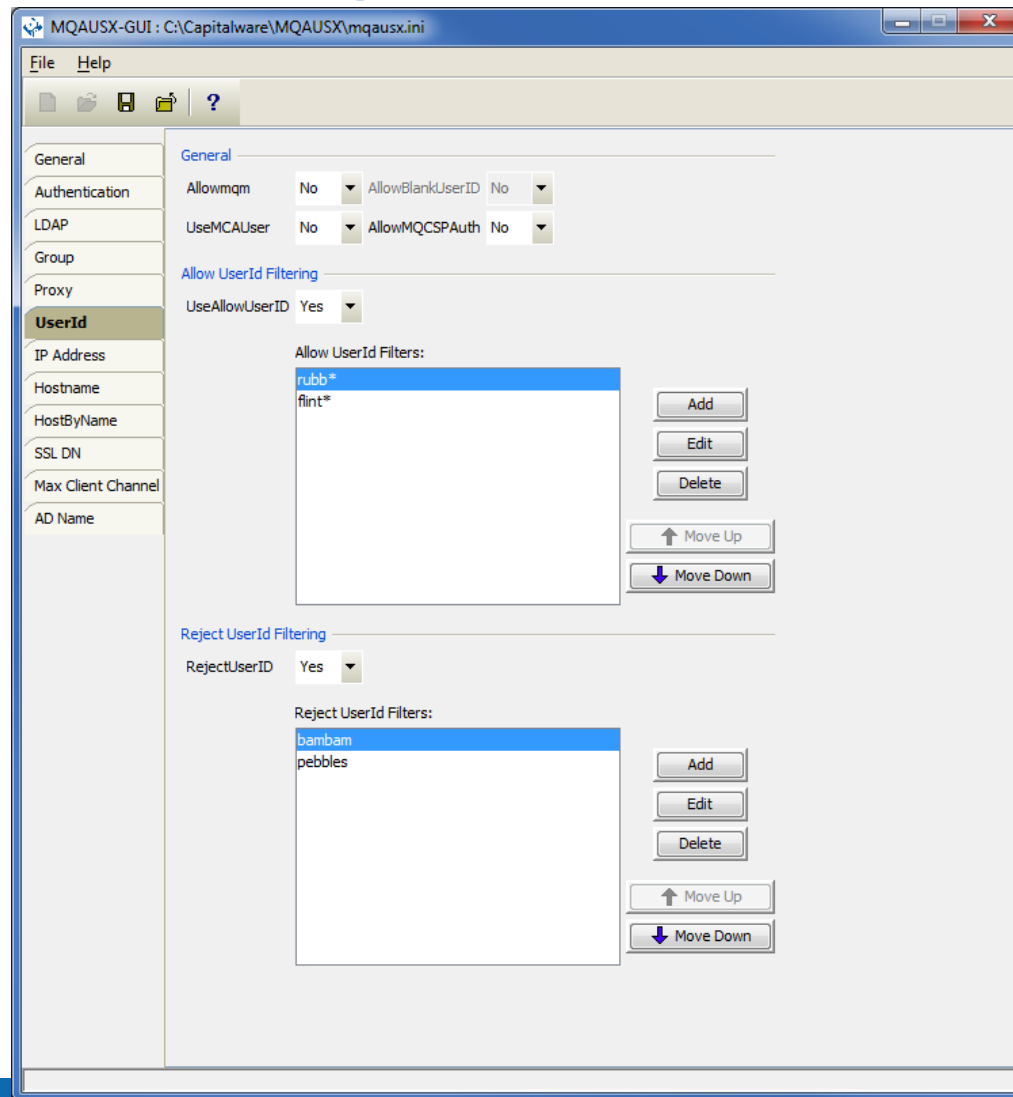
The screenshot displays the MQAUSX-GUI configuration window. The title bar reads "MQAUSX-GUI : C:\Capitalware\MQAUSX\mqausx.ini". The interface includes a menu bar with "File" and "Help", and a toolbar with icons for file operations and help. A left-hand sidebar lists configuration categories: General, Authentication, LDAP, Group (selected), Proxy, UserId, IP Address, Hostname, HostByName, SSL DN, Max Client Channel, and AD Name. The main panel is titled "Group Authorization" and contains the following settings:

- UseGroups:** Yes (dropdown)
- Groups:** GrpA;GrpB;GrpC (text field) with an **Update** button
- UseGroupFile:** No (dropdown)
- GroupFile:** (empty text field)
- LDAP Group Search Authorization:**
 - UseLDAPGroupSearch:** No (dropdown)
 - LDAPGroupSearchScope:** LDAP_SCOPE_ONELEVEL (dropdown)
 - UseLDAPGroupSearchBindDN:** No (dropdown)
 - LDAPGroupSearchBase:** (empty text field)
 - LDAPGroupSearchFilter:** (empty text field)

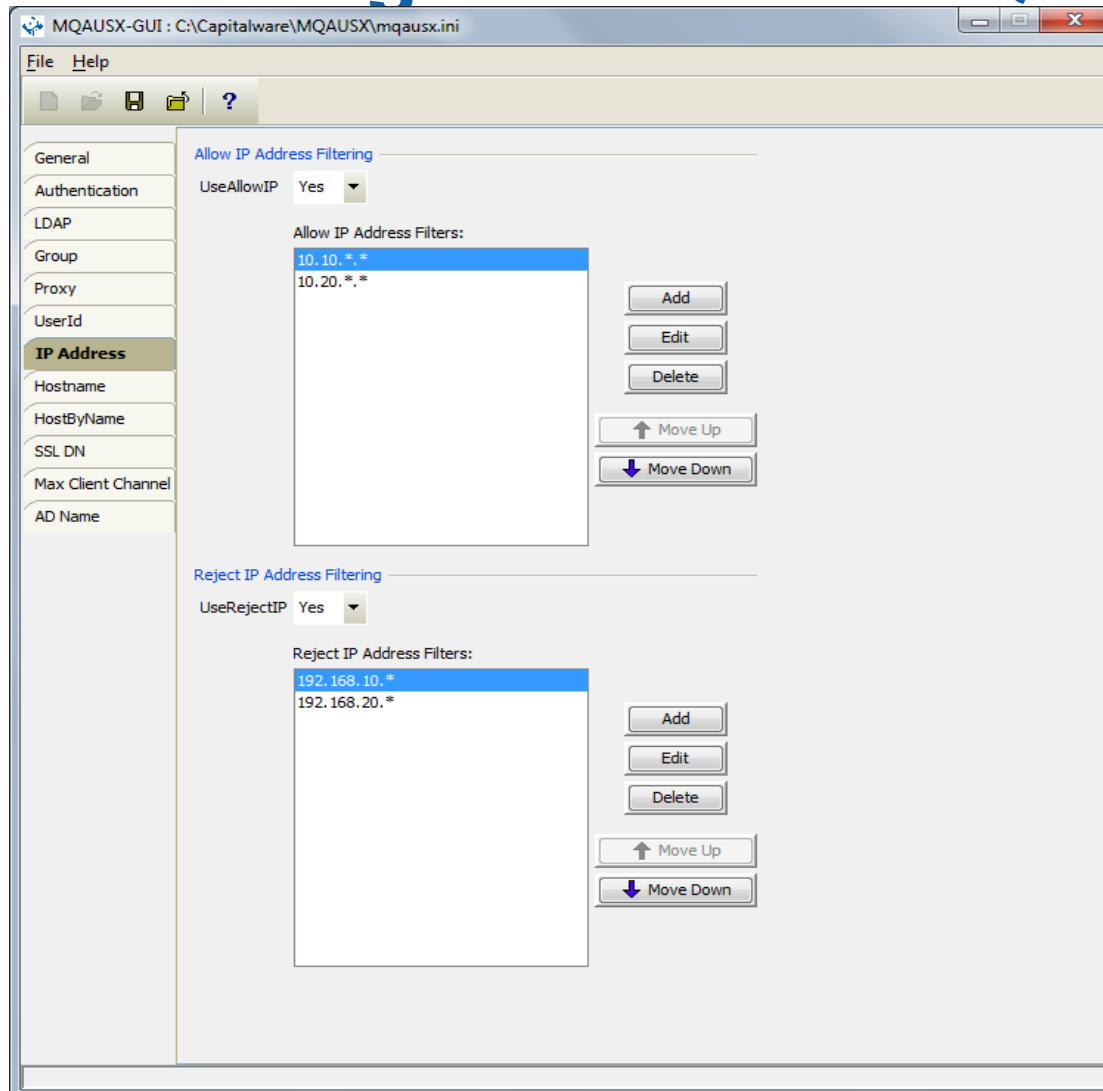
MQAUSX Configuration via MQAUSX-GUI



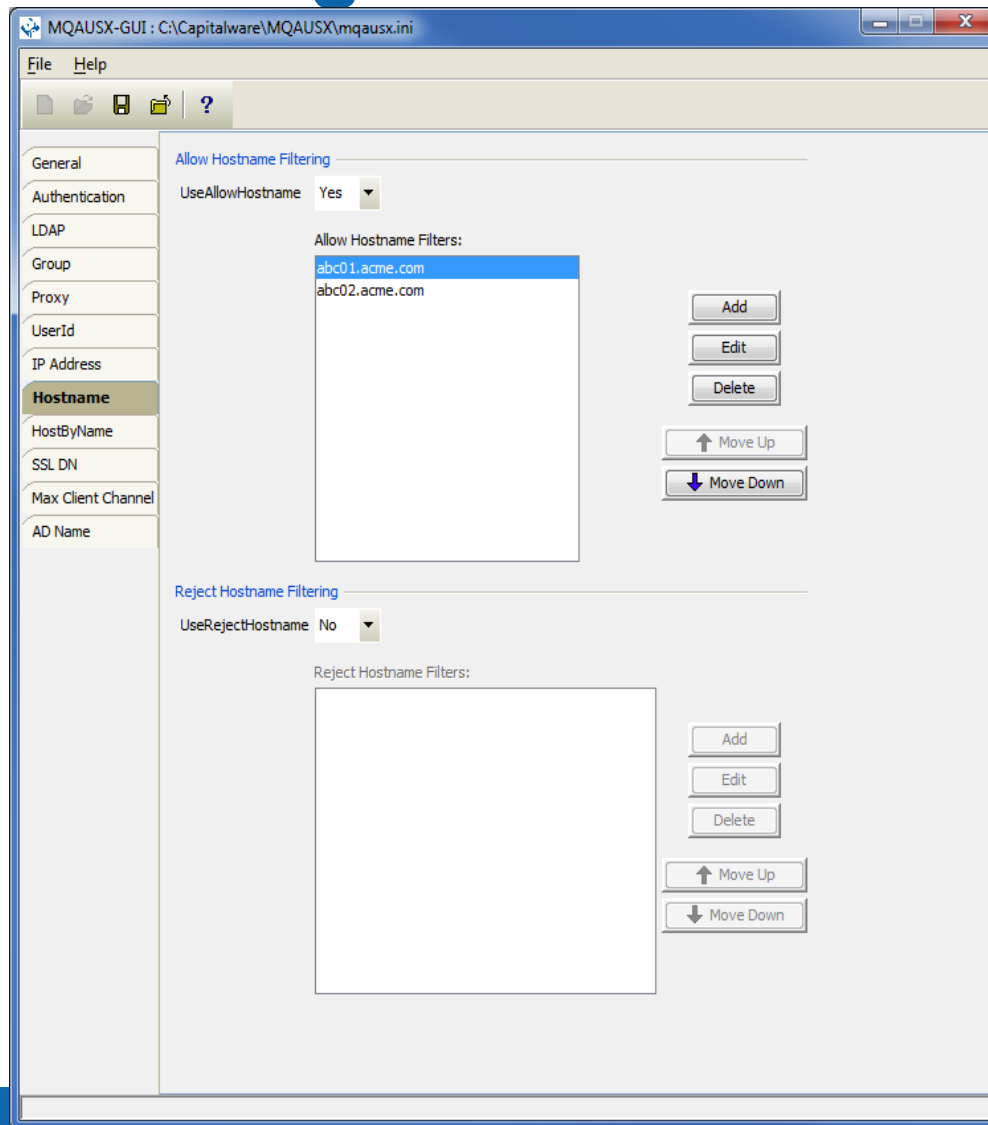
MQAUSX Configuration via MQAUSX-GUI



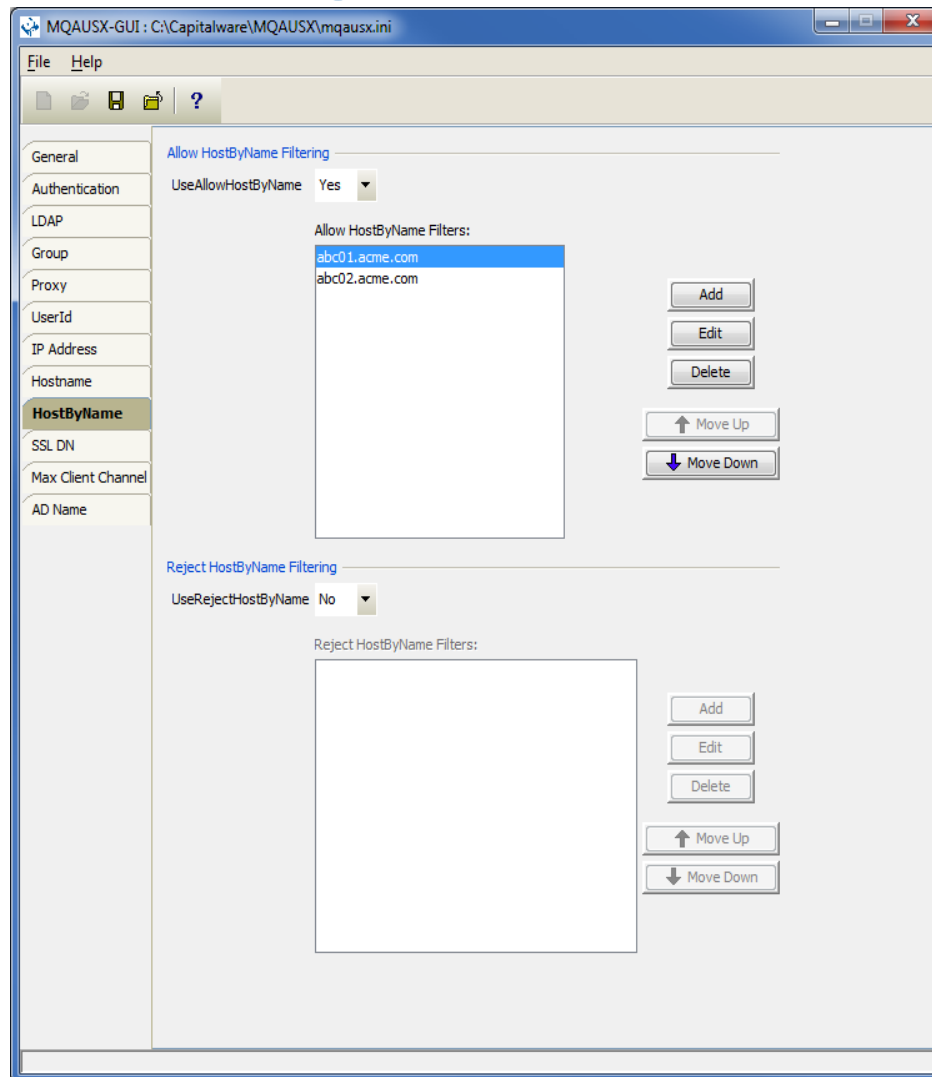
MQAUSX Configuration via MQAUSX-GUI



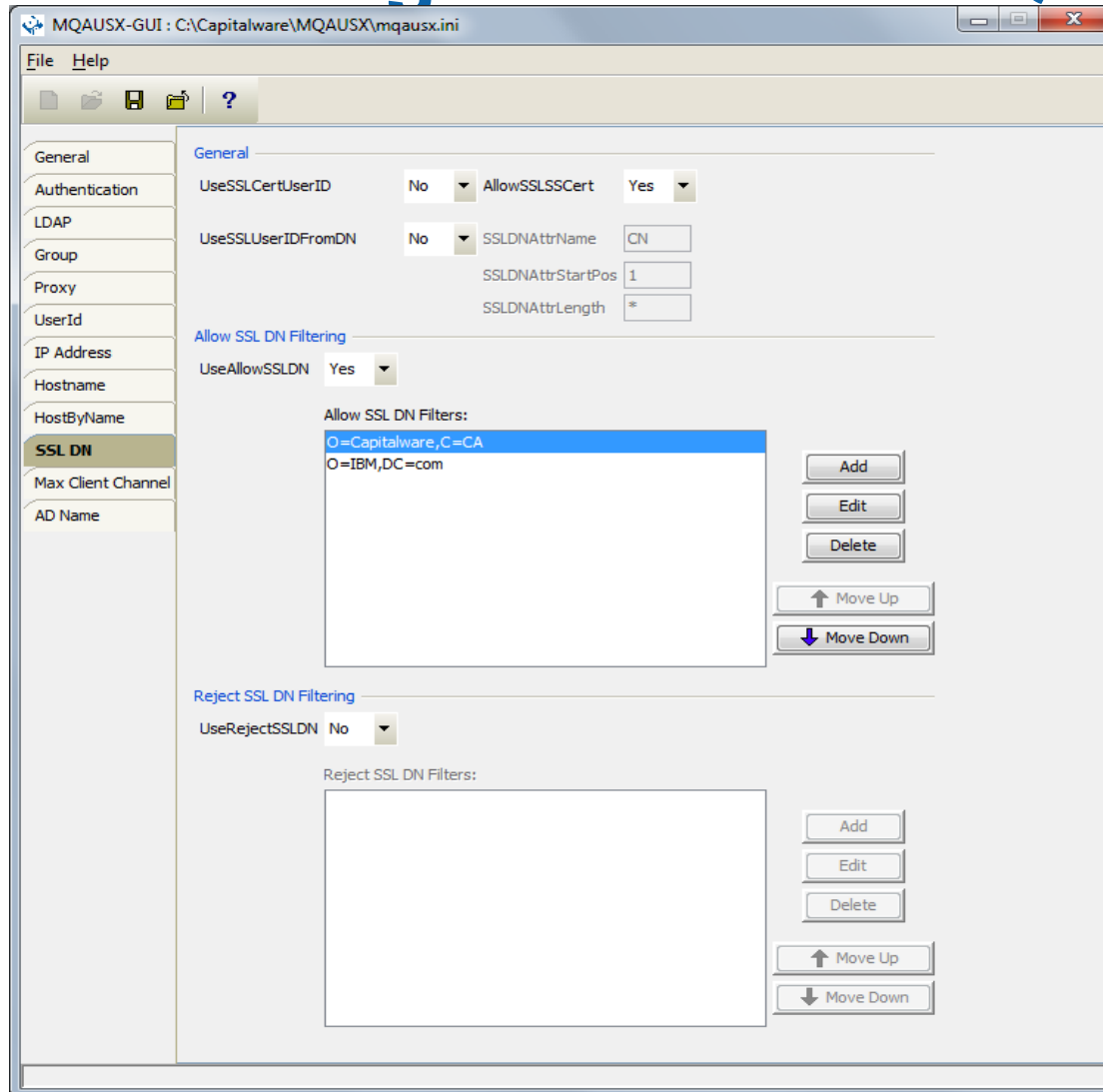
MQAUSX Configuration via MQAUSX-GUI



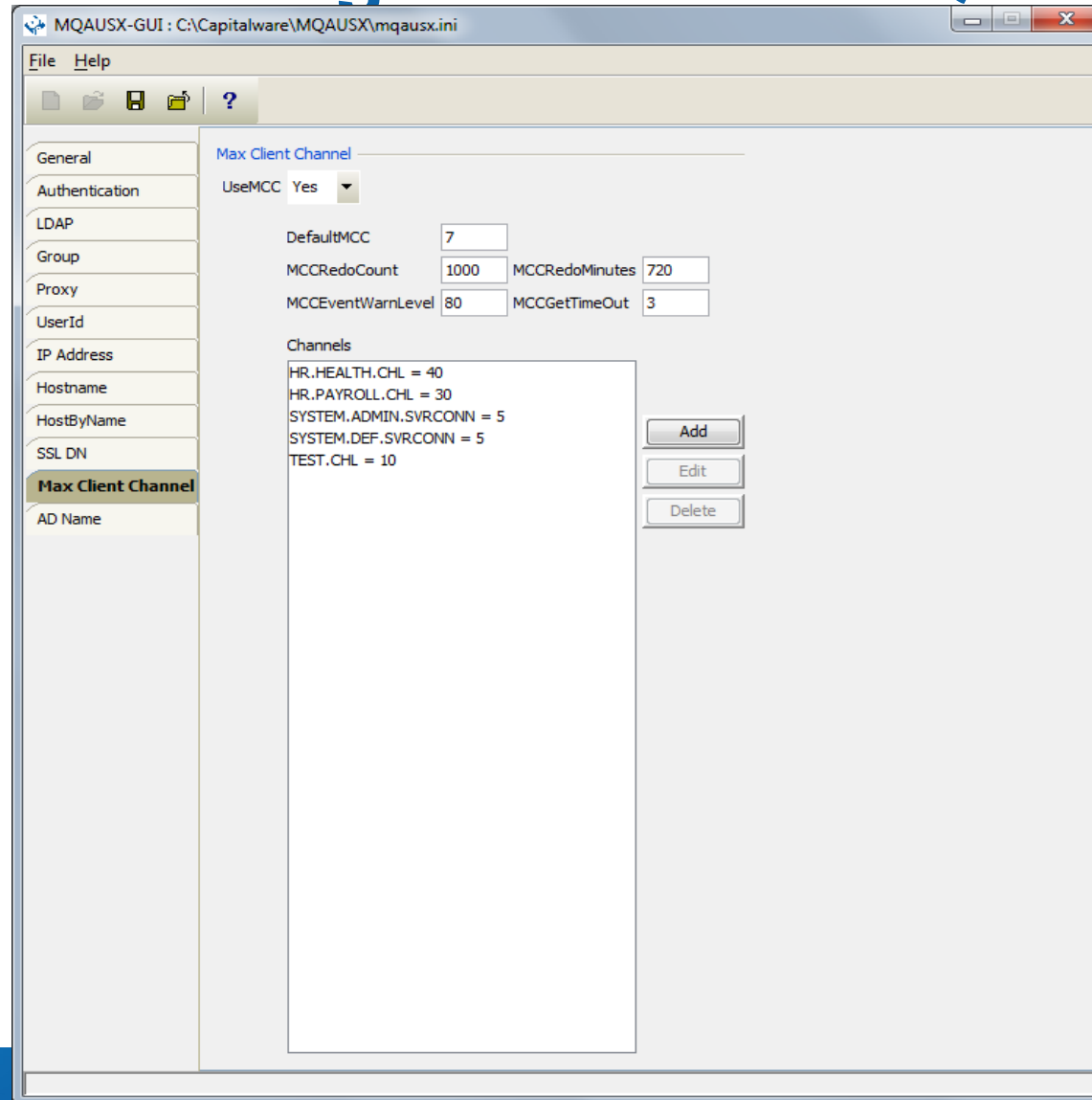
MQAUSX Configuration via MQAUSX-GUI



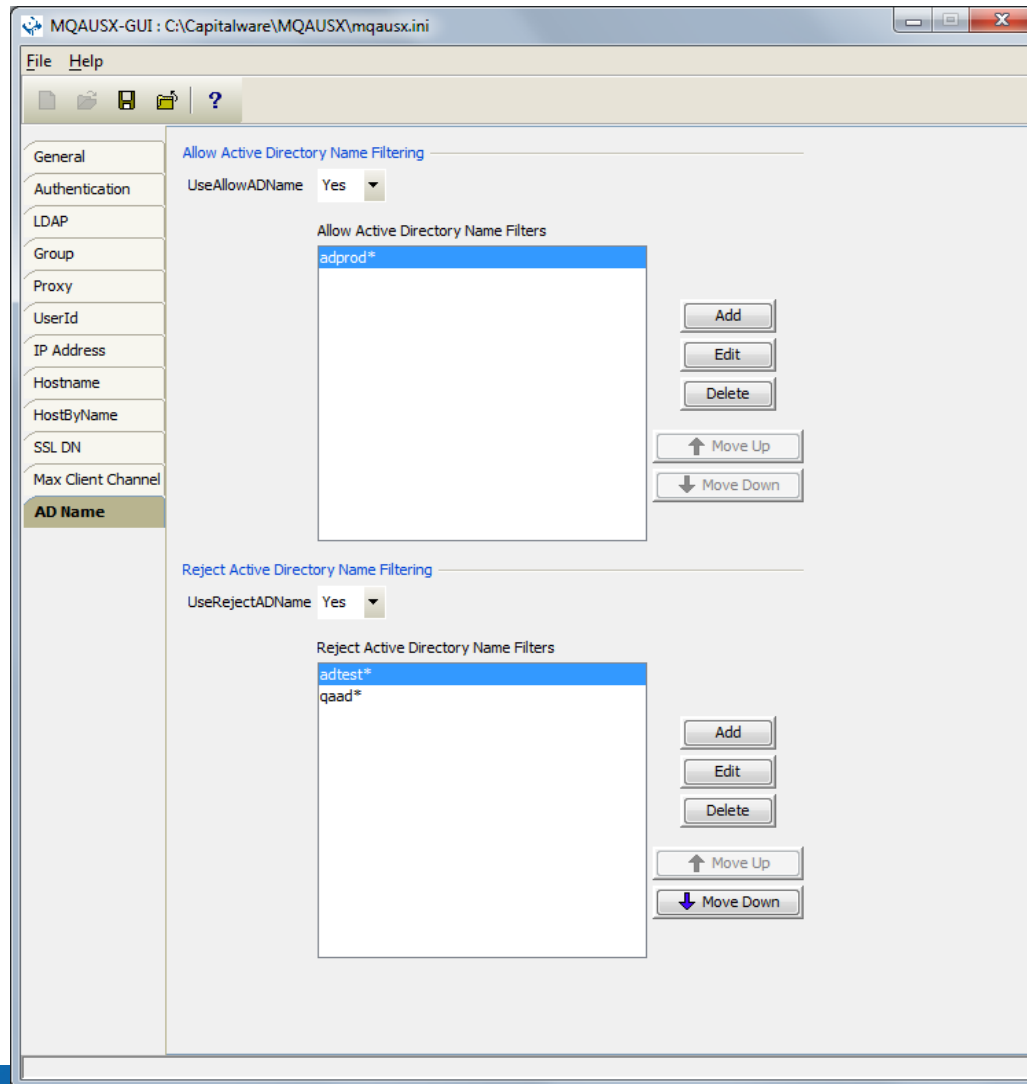
MQAUSX Configuration via MQAUSX-GUI



MQAUSX Configuration via MQAUSX-GUI



MQAUSX Configuration via MQAUSX-GUI



Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI -----  
COMMAND ==>  
  
MQAUSX IniFile (PDS or Sequential file):  
==> 'CAP01.CPTLWARE.MQAUSX.SYSIN'  
==> (Blank or pattern for member selection list)  
  
PF3 or PF12 to Cancel.
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - General Setting -----  
COMMAND ==>  
  
License Key ==>  
LicenseFile ==>  
Description ==>  
  
Log Mode          ==> N          (Q/N/V/D)  
Log File DD       ==> SYSPRINT  
WriteToSystemLog  ==> N          (Y/N)  
SystemLogMessage ==> B          (B/A/R)  
WriteToEventQueue ==> N          (Y/N)  
EventQueueName    ==> SYSTEM.ADMIN.CHANNEL.EVENT  
  
Sequence Number  ==> N          (Y/N)  
  
PF3 to Return or PF12 to Cancel.
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Authentication Setting -----  
COMMAND ==>  
  
NoAuth ==> N (Y/N)  
  
File Based Access:  
UseFBA ==> N (Y/N)      FBAFile ==>  
  
Authentication Order:  
UseAuthOrder ==> N      AuthOrder ==>
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Group Setting -----  
COMMAND ==>  
Use Groups    ==> Y          (Y/N)  
Groups       ==> GrpA,GrpB,GrpC  
Group File DD ==> 'CAP01.CPTLWARE.MQAUSX.SYSIN(GRPIN)'  
  
PF3 to Return or PF12 to Cancel.
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Proxy Setting -----  
COMMAND ==>  
Use Proxy      ==> N      (Y/N)  
Proxy File DD ==>  
  
PF3 to Return or PF12 to Cancel.
```


Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Allow UserId Setting      Row 1 to 1 of 1
COMMAND ==>                                           SCROLL ==> PAGE

Allowmqm      ==> N  (Y/N)          AllowBlankUserID ==> N  (Y/N)
UseMCAUser    ==> N  (Y/N)          AllowCSPAuth      ==> Y  (Y/N)
                                           UppercaseUserID ==> N  (Y/N)

UseAllowUserID ==> N  (Y/N)

Line Cmd: A Add UserId or D Delete UserId

Cmd  Allow UserId
---  -----
_    *
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Allow IP Address Setting Row 1 to 3 of 3
COMMAND ==> SCROLL ==> PAGE

UseAllowIP ==> Y (Y/N)

Line Cmd: A Add IP Filter or D Delete IP Filter

Cmd Allow IP Address
-----
- 192.168.10.*
- 192.168.200.*
- 10.10.*.*
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Allow Hostname Setting Row 1 to 2 of 2
COMMAND ==>                                     SCROLL ==> PAGE

UseAllowHostname ==> Y (Y/N)

Line Cmd: A Add Hostname Filter or D Delete Hostname Filter

Cmd  Allow Hostname
-----
_   abc01.acme.com
_   abc02.acme.com
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Allow HostByName Setting Row 1 to 2 of 2
COMMAND ==> SCROLL ==> PAGE

UseAllowHostByName ==> Y (Y/N)

Line Cmd: A Add HostByName Filter or D Delete HostByName Filter

Cmd Allow HostByName
-----
_ abc01.acme.com
_ abc02.acme.com
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Allow SSL DN Setting Row 1 to 2 of 2
COMMAND ==> SCROLL ==> PAGE

UseSSLCertUserID ==> N (Y/N) AllowSSLSSCert ==> Y (Y/N)
UseSSLUserIDFromDN ==> N (Y/N) SSLDNAttrName ==> CN
SSLDNAttrStartPos ==> 1
SSLDNAttrLength ==> * (* for all)

UseAllowSSLDN ==> Y (Y/N)

Line Cmd: A Add SSL DN Filter or D Delete SSL DN Filter

Cmd Allow SSL DN
-----
_ O=Capitalware,C=CA
_ O=IBM,DC=com
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Reject UserId Setting      Row 1 to 1 of 1
COMMAND ==>                                           SCROLL ==> PAGE
UseRejectUserID ==> N (Y/N)
Line Cmd: A Add UserId or D Delete UserId
Cmd  Reject UserId
---  -----
-
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Reject IP Address Setting Row 1 to 1 of 1
COMMAND ==>                                     SCROLL ==> PAGE

UseRejectIP ==> N (Y/N)

Line Cmd: A Add IP Filter or D Delete IP Filter

Cmd  Reject IP Address
-----
-
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Reject Hostname Setting Row 1 to 1 of 1
COMMAND ==>                                     SCROLL ==> PAGE
UseRejectHostname ==> N (Y/N)
Line Cmd: A Add Hostname Filter or D Delete Hostname Filter
Cmd  Reject Hostname
-----
-
***** Bottom of data *****
```


Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Reject HostByName Setting Row 1 to 1 of 1
COMMAND ==>                                     SCROLL ==> PAGE

UseRejectHostByName ==> N (Y/N)

Line Cmd: A Add HostByName Filter or D Delete HostByName Filter

Cmd  Reject HostByName
-----
-
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Reject SSL DN Setting Row 1 to 1 of 1
COMMAND ==>                                SCROLL ==> PAGE
UseRejectSSLDN ==> N (Y/N)
Line Cmd: A Add SSL DN Filter or D Delete SSL DN Filter
Cmd  Reject SSL DN
-----
-
***** Bottom of data *****
```

Configuration via MQAUSX-ISPF-GUI

```
----- z/MQAUSX ISPF GUI - Max Client Channel Settin Row 1 to 3 of 3
COMMAND ==> SCROLL ==> PAGE

UseMCC          ==> Y      (Y/N)      DefaultMCC      ==> 7
MCCRedoCount    ==> 5000                MCCRedoMinutes  ==> 720
MCCEventWarnLev ==> 80                  MCCGetTimeOut   ==> 3

ModelQueueName  ==> SYSTEM.COMMAND.REPLY.MODEL
CommandQueueName ==> SYSTEM.COMMAND.INPUT
TempDynPrefix   ==> SYSTEM.MQAUSX.*

Line Cmds: A Add Channel or D Delete Channel

Cmd  Channel Name          Max Channel Limit
----  -
_    ABC.CHL                30
_    SYSTEM.DEF.SVRCONN     10
_    SYSTEM.ADMIN.SVRCONN   5
***** Bottom of data *****
```

Questions & Answers

