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.

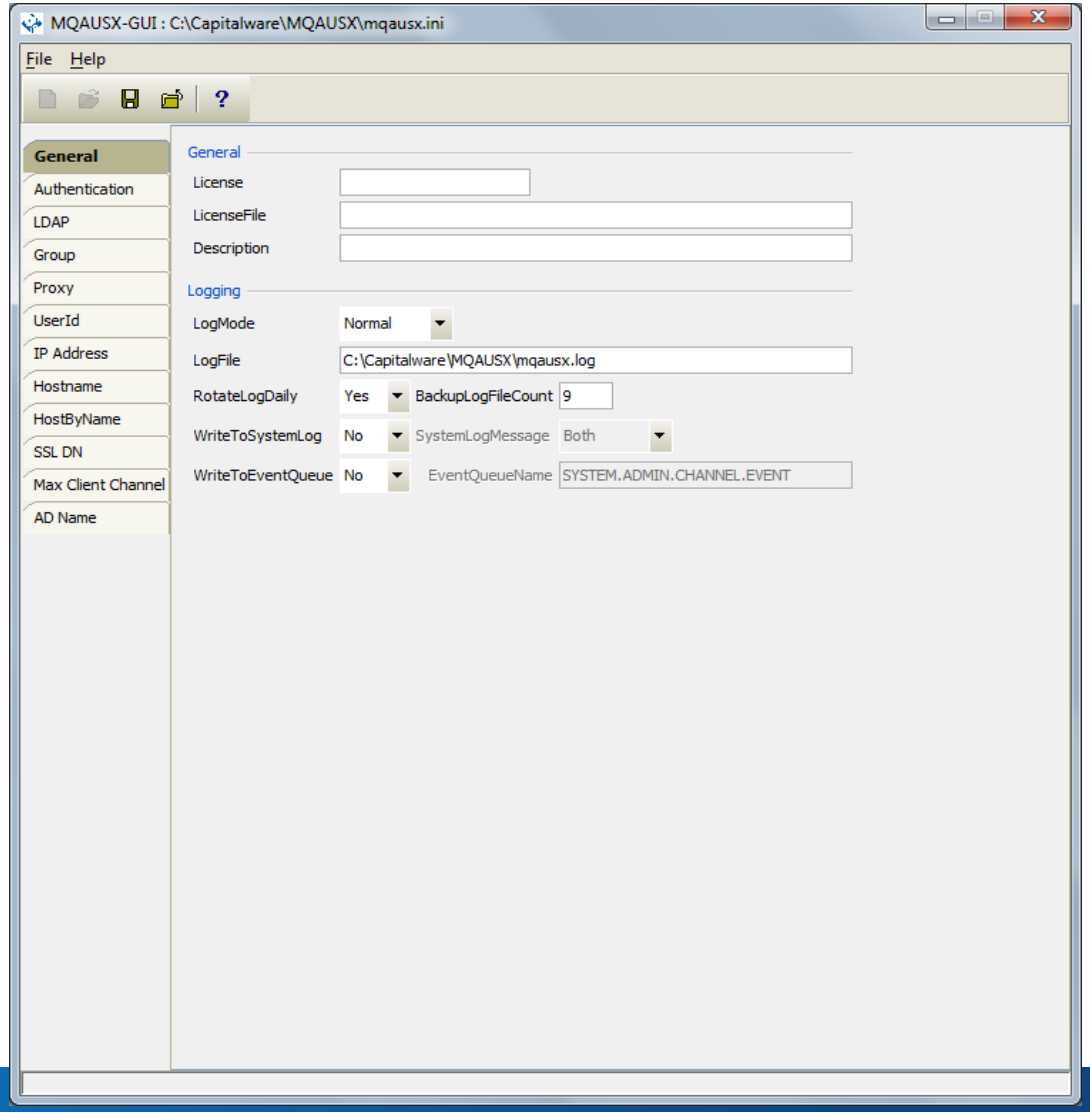
z/MQAUSX Secondary Features

- 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.

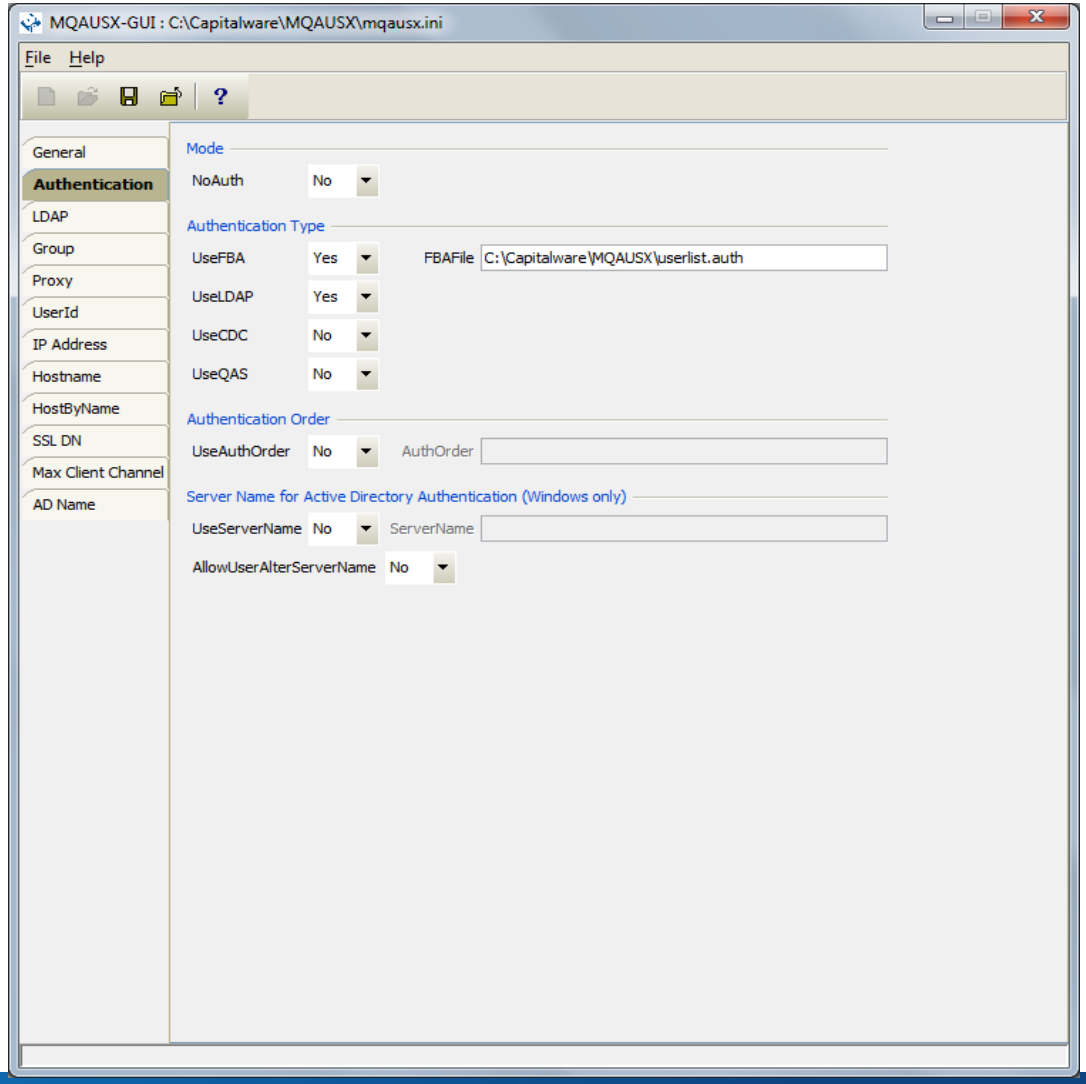
MQAUSX & z/MQAUSX Keywords

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

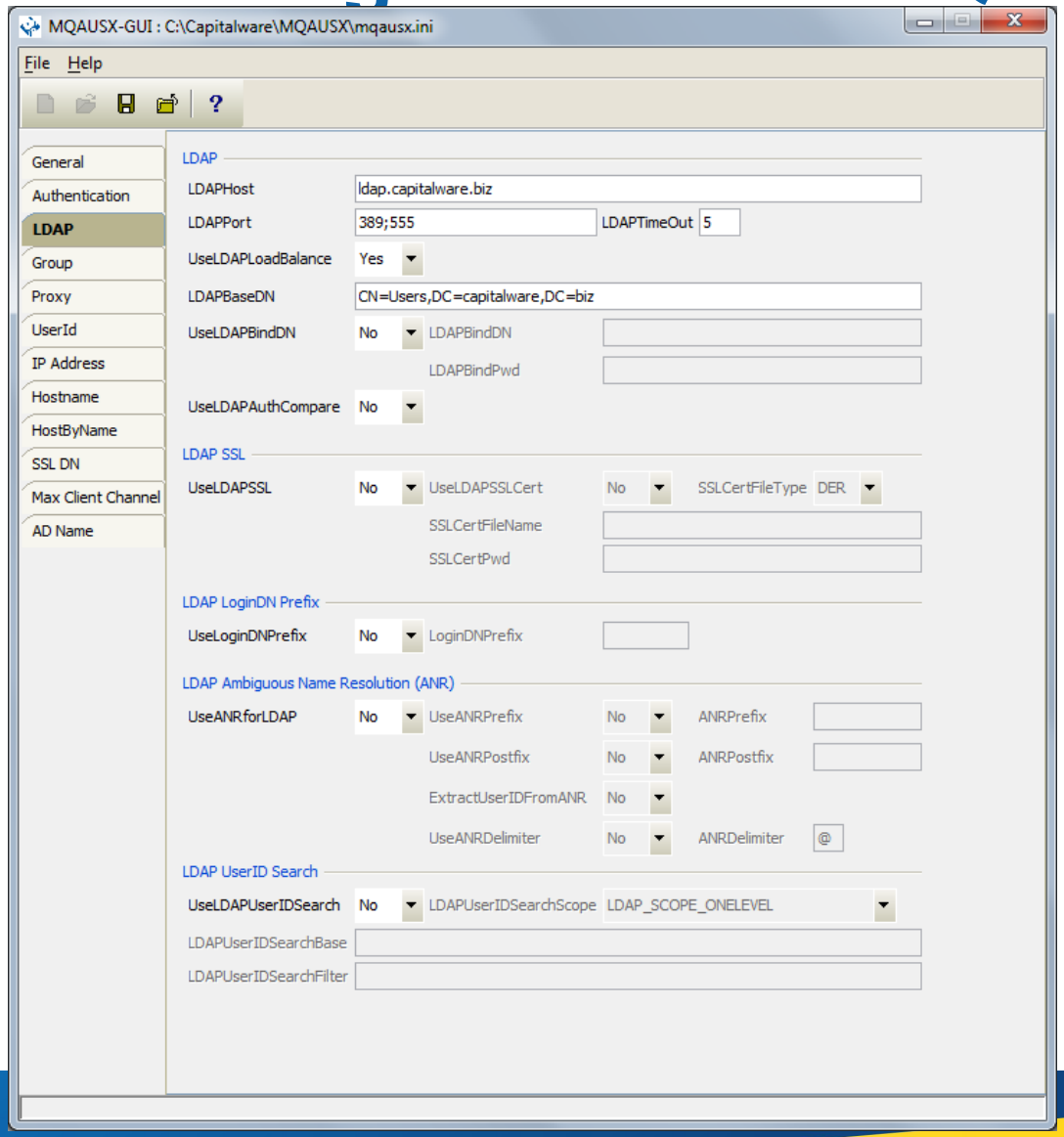
MQAUSX Configuration via MQAUSX-GUI



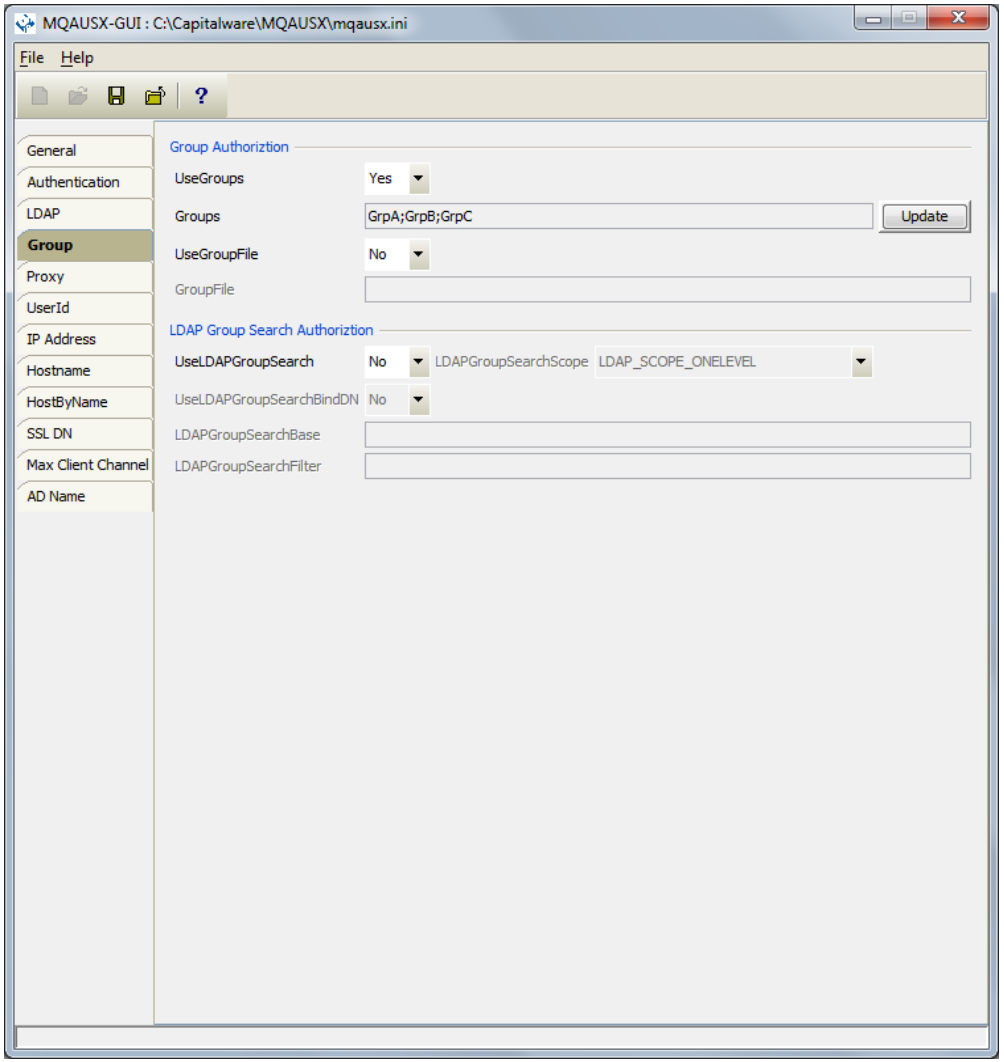
MQAUSX Configuration via MQAUSX-GUI



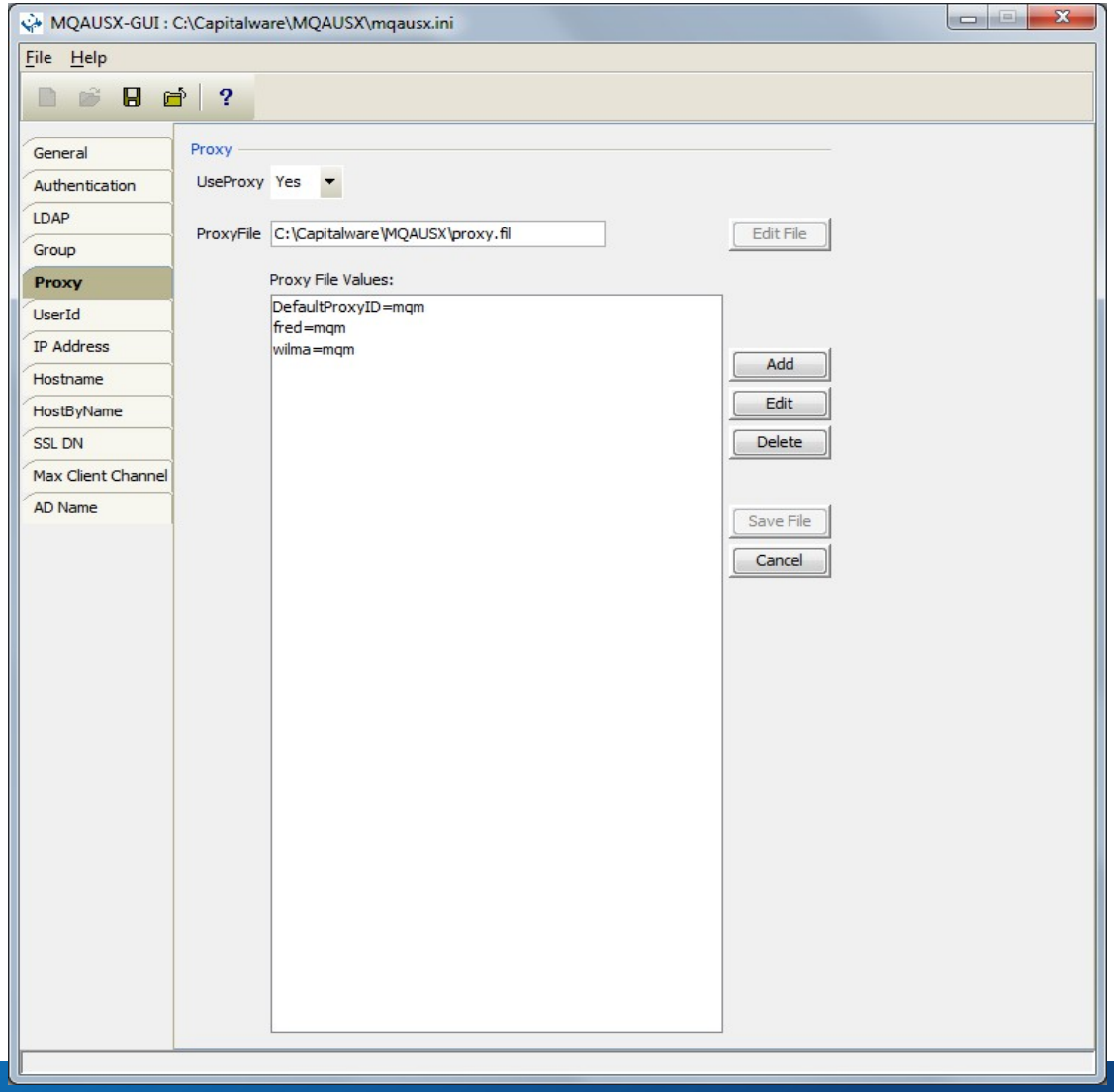
MQAUSX Configuration via MQAUSX-GUI



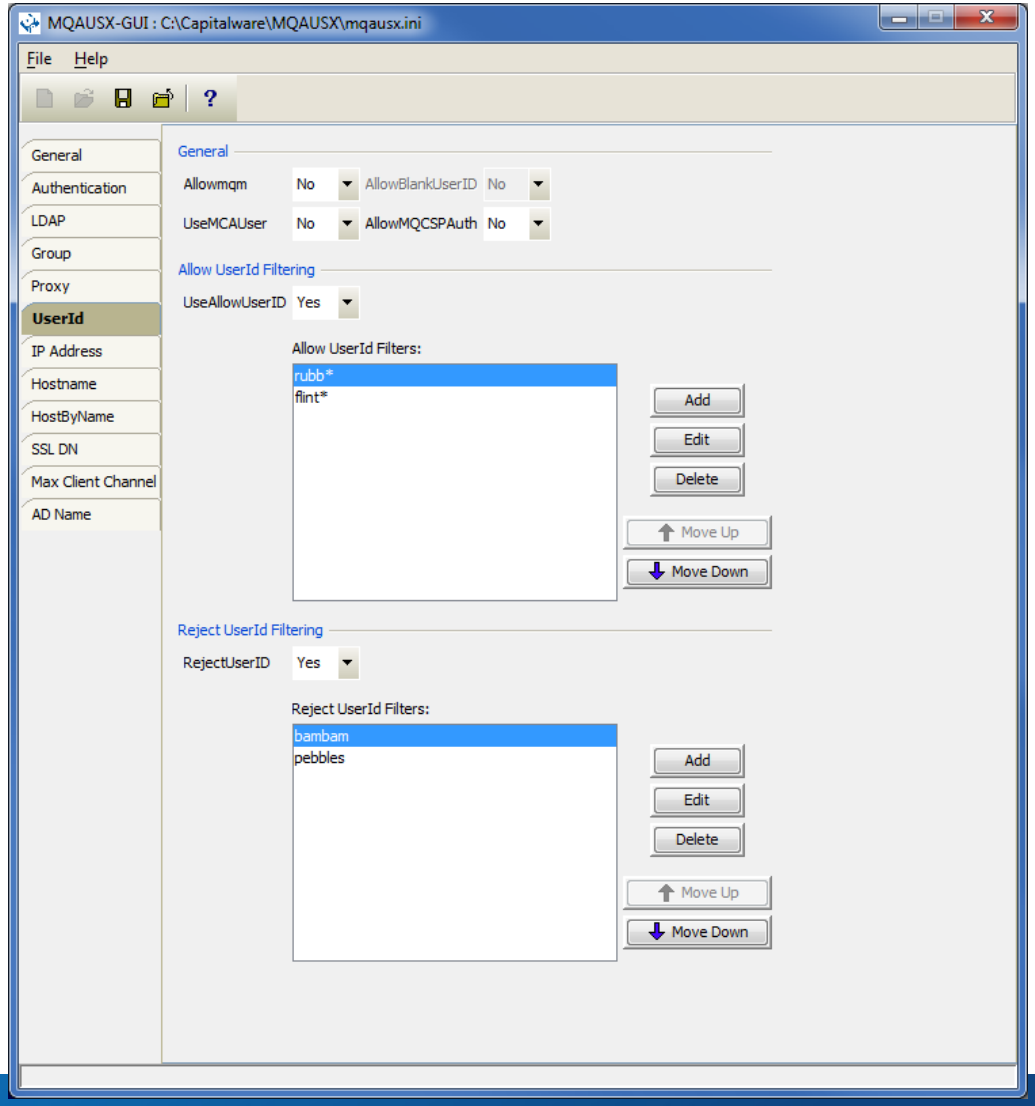
MQAUSX Configuration via MQAUSX-GUI



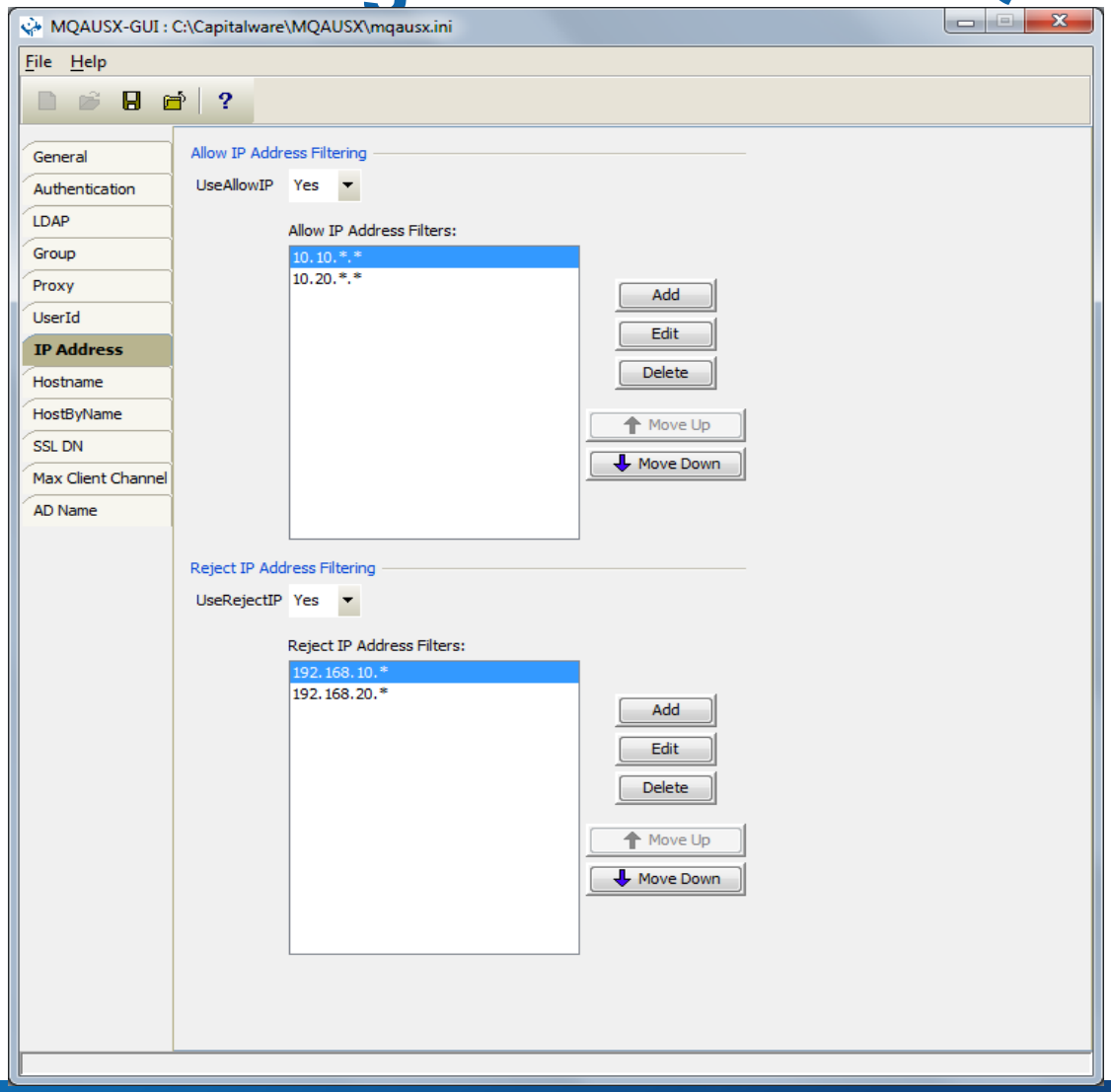
MQAUSX Configuration via MQAUSX-GUI



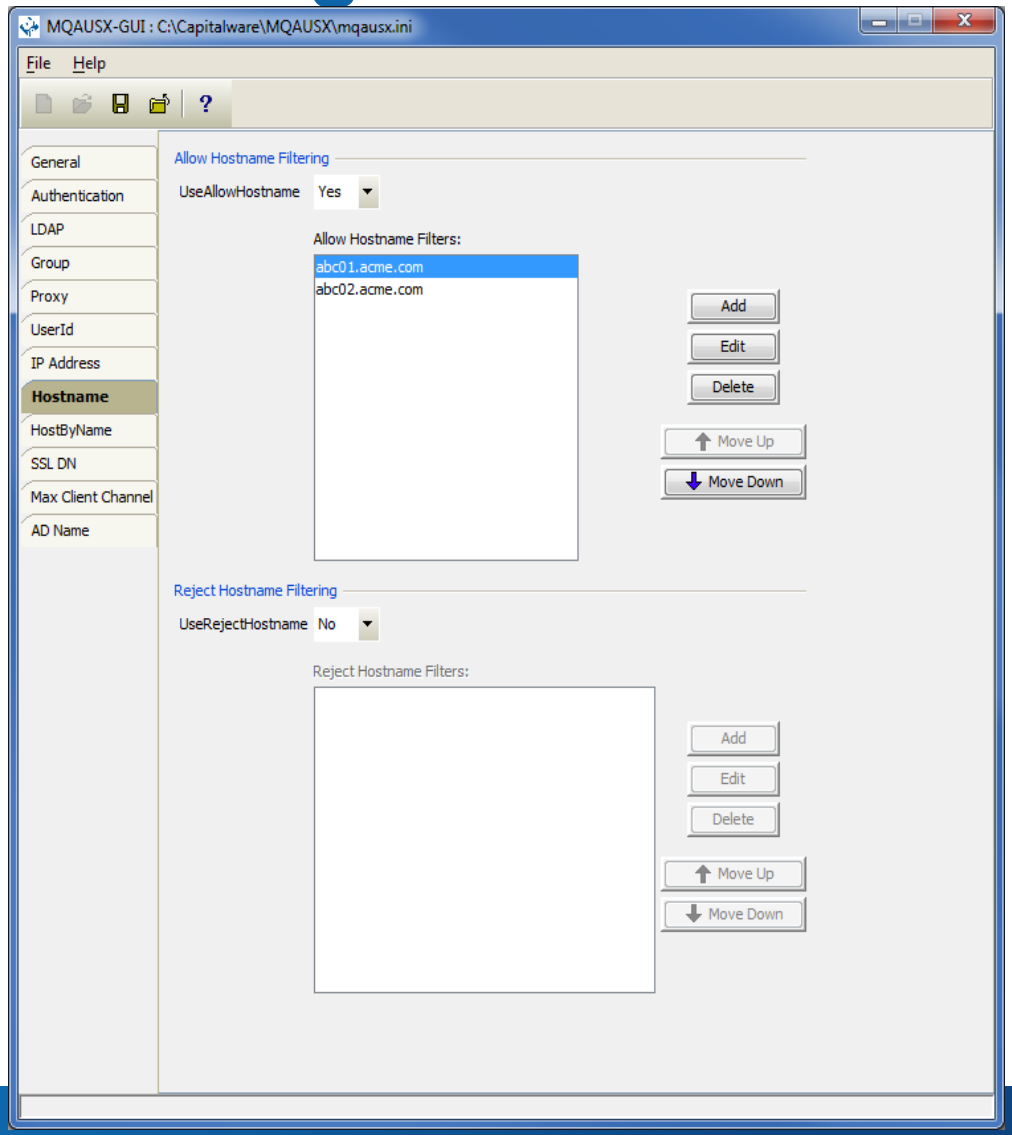
MQAUSX Configuration via MQAUSX-GUI



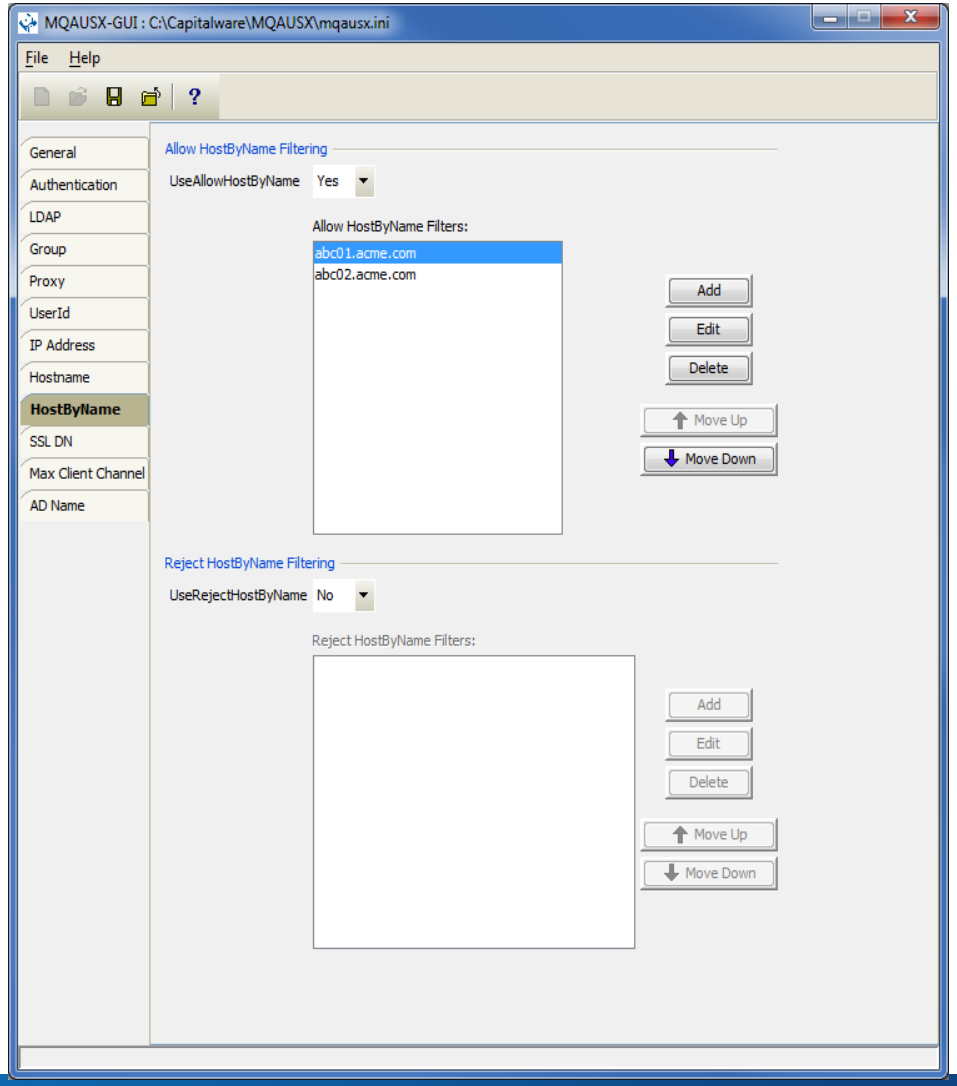
MQAUSX Configuration via MQAUSX-GUI



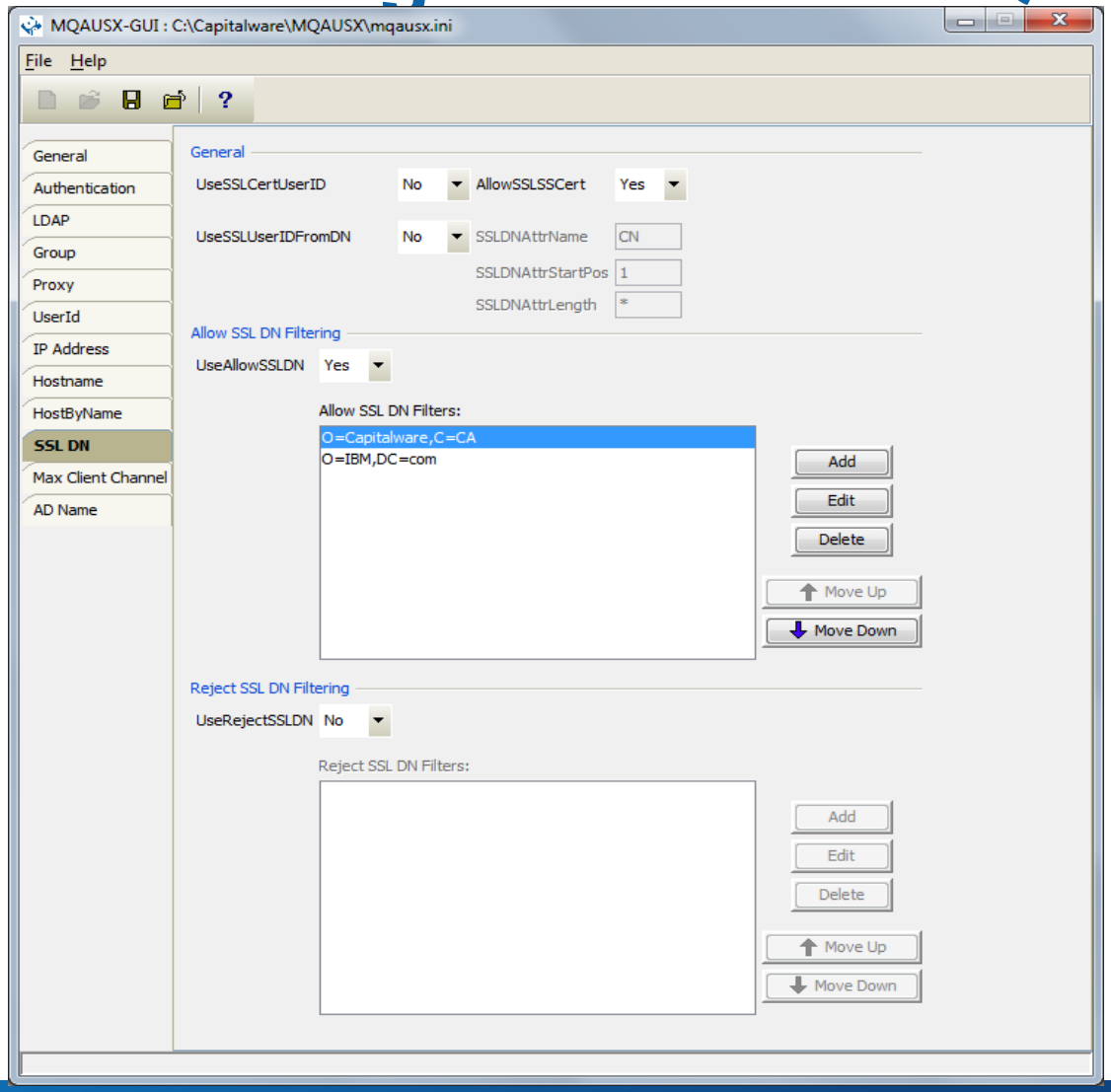
MQAUSX Configuration via MQAUSX-GUI



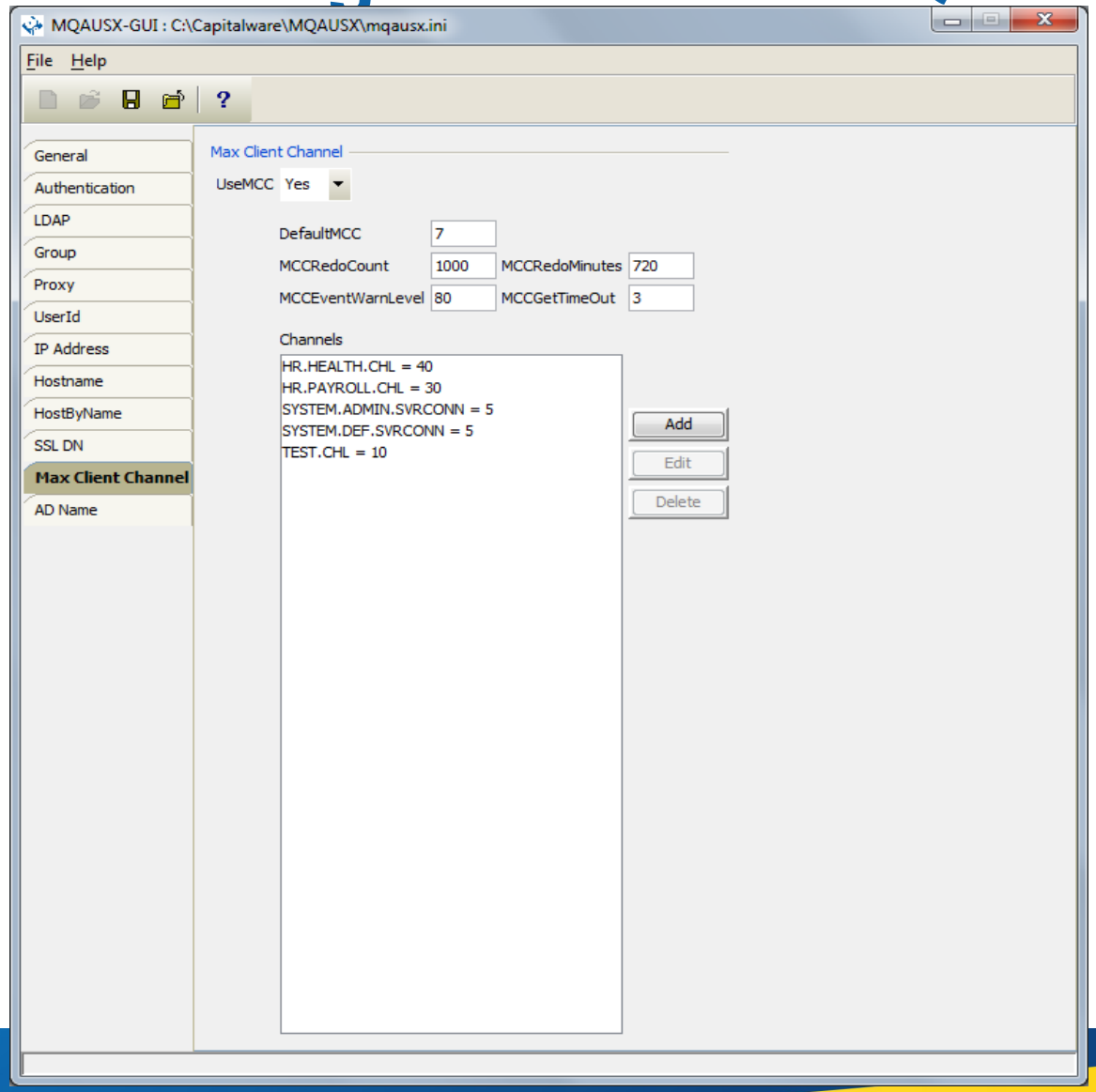
MQAUSX Configuration via MQAUSX-GUI



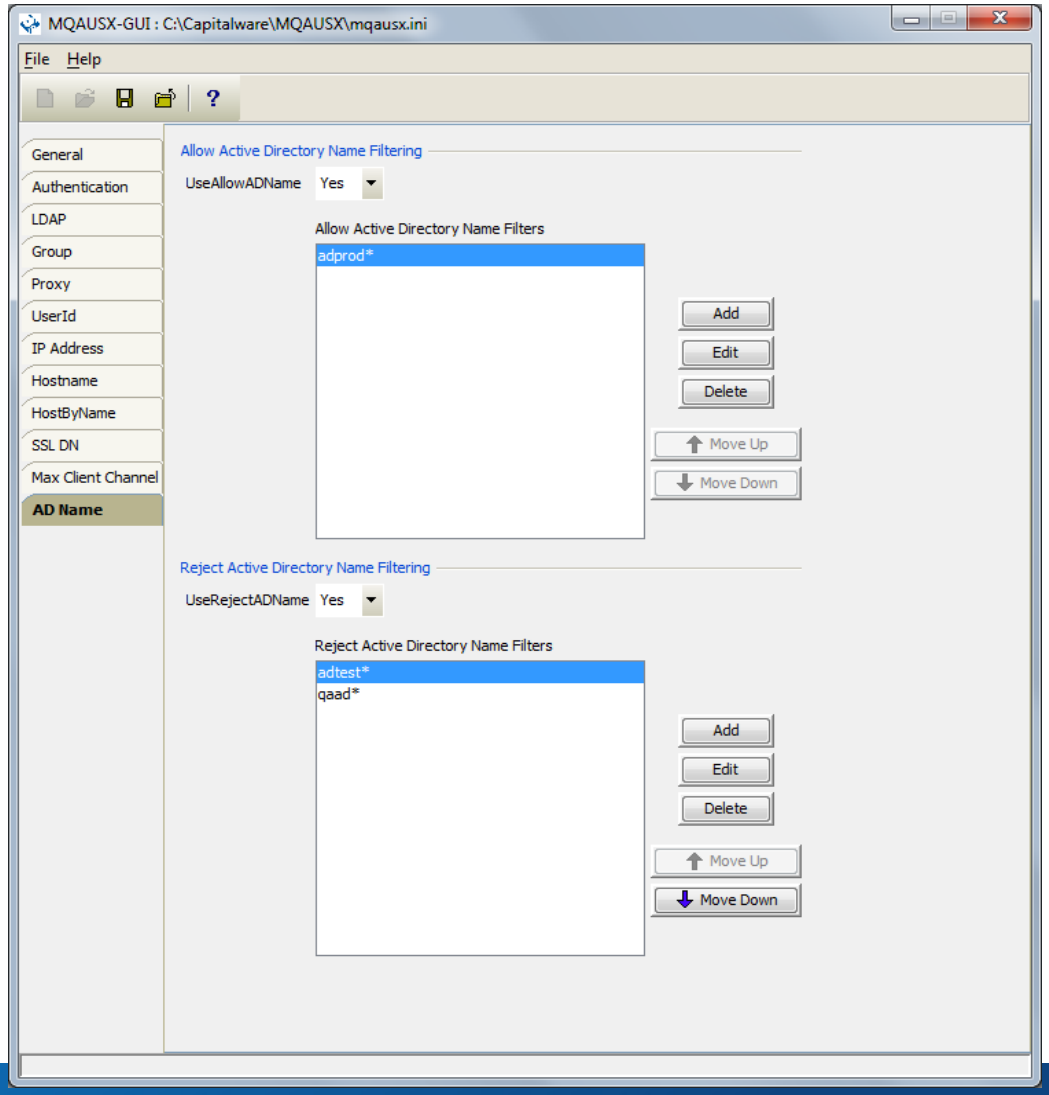
MQAUSX Configuration via MQAUSX-GUI



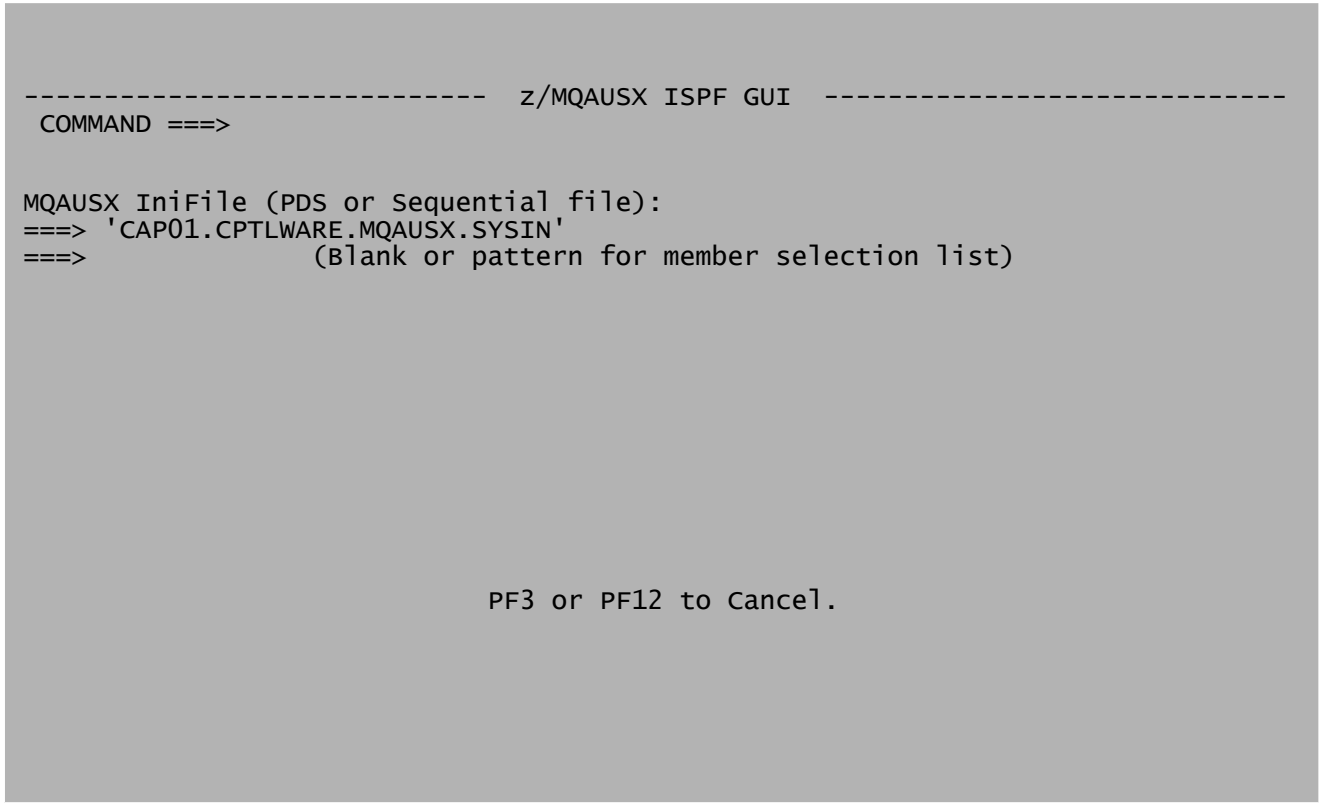
MQAUSX Configuration via MQAUSX-GUI



MQAUSX Configuration via MQAUSX-GUI



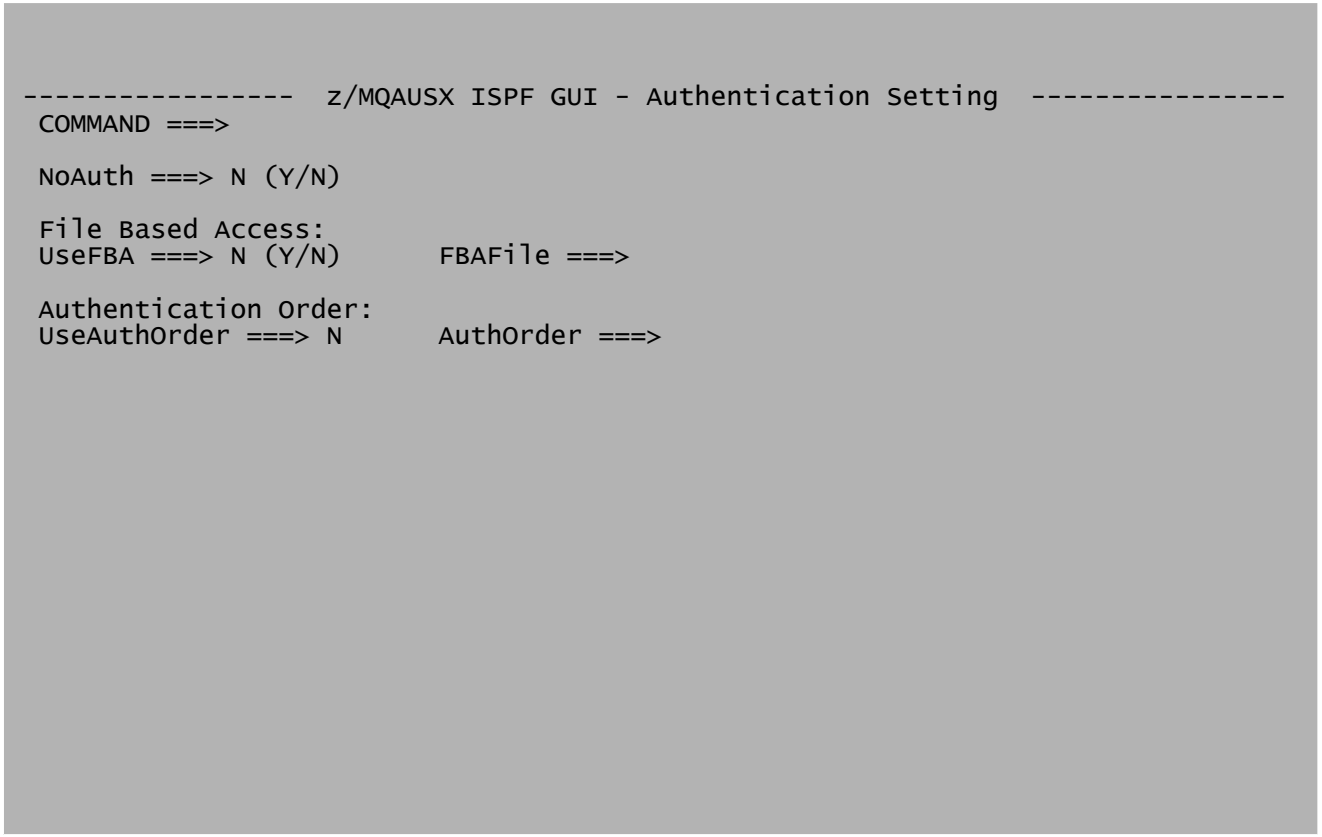
Configuration via MQAUSX-ISPF-GUI



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.
```

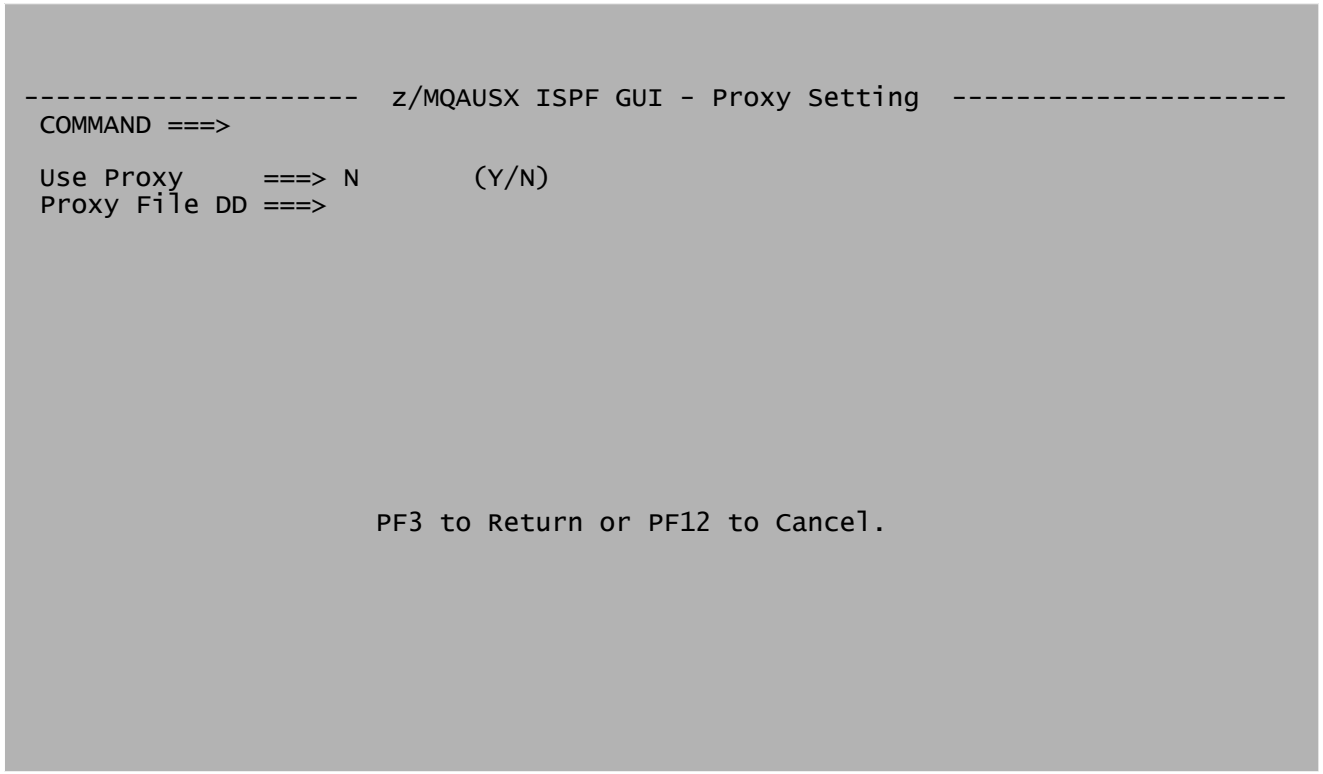
Configuration via MQAUSX-ISPF-GUI



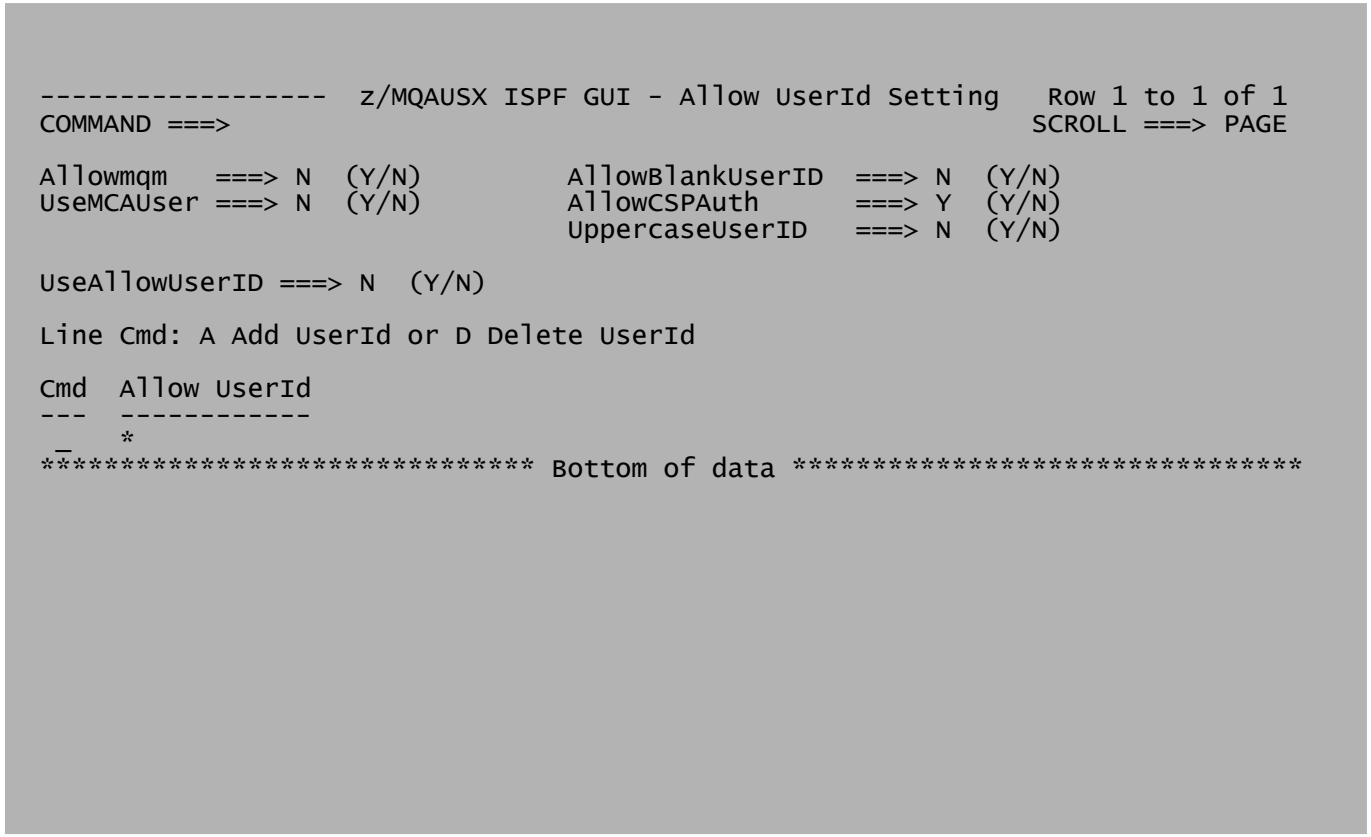
Configuration via MQAUSX-ISPF-GUI

```
----------------------  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.
```

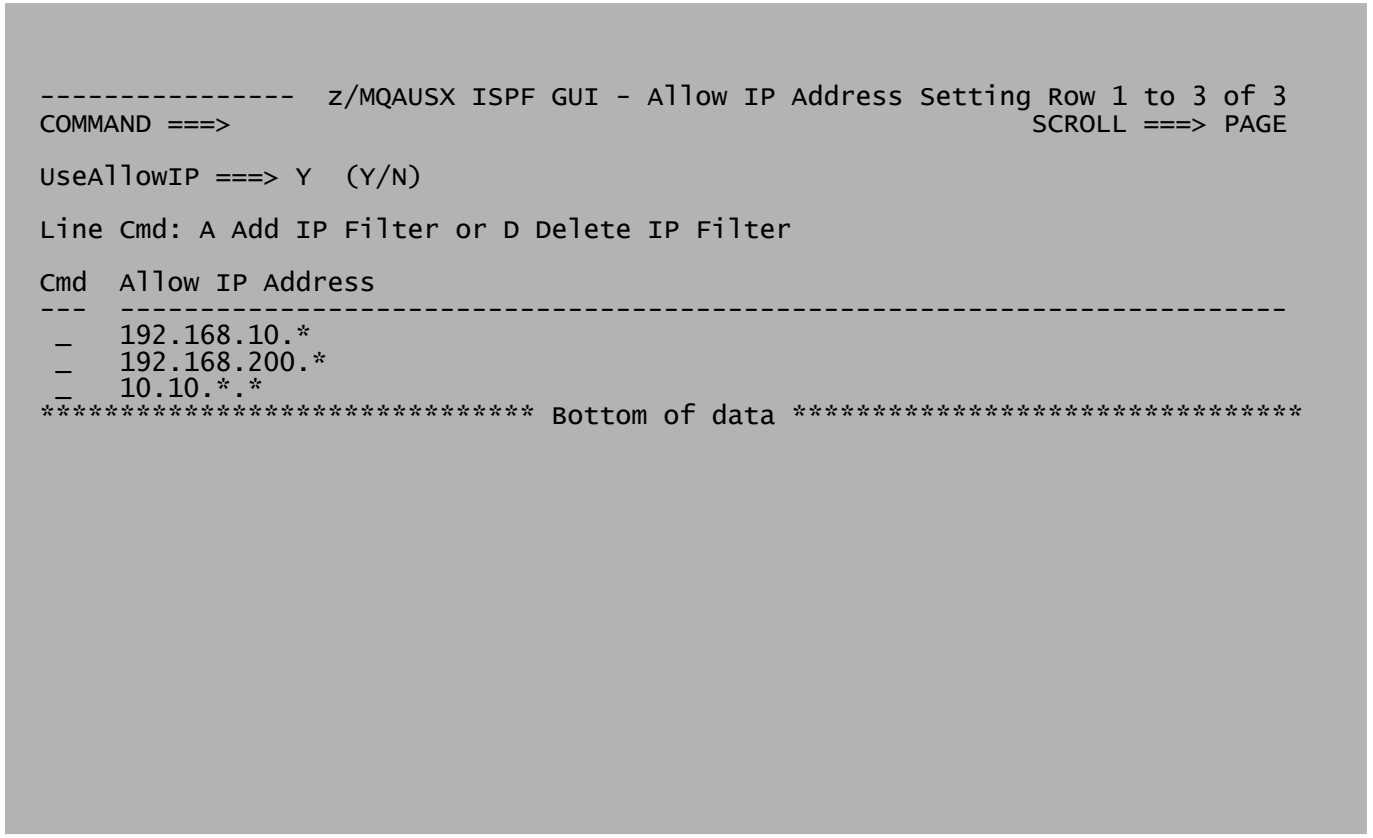
Configuration via MQAUSX-ISPF-GUI



Configuration via MQAUSX-ISPF-GUI



Configuration via MQAUSX-ISPF-GUI



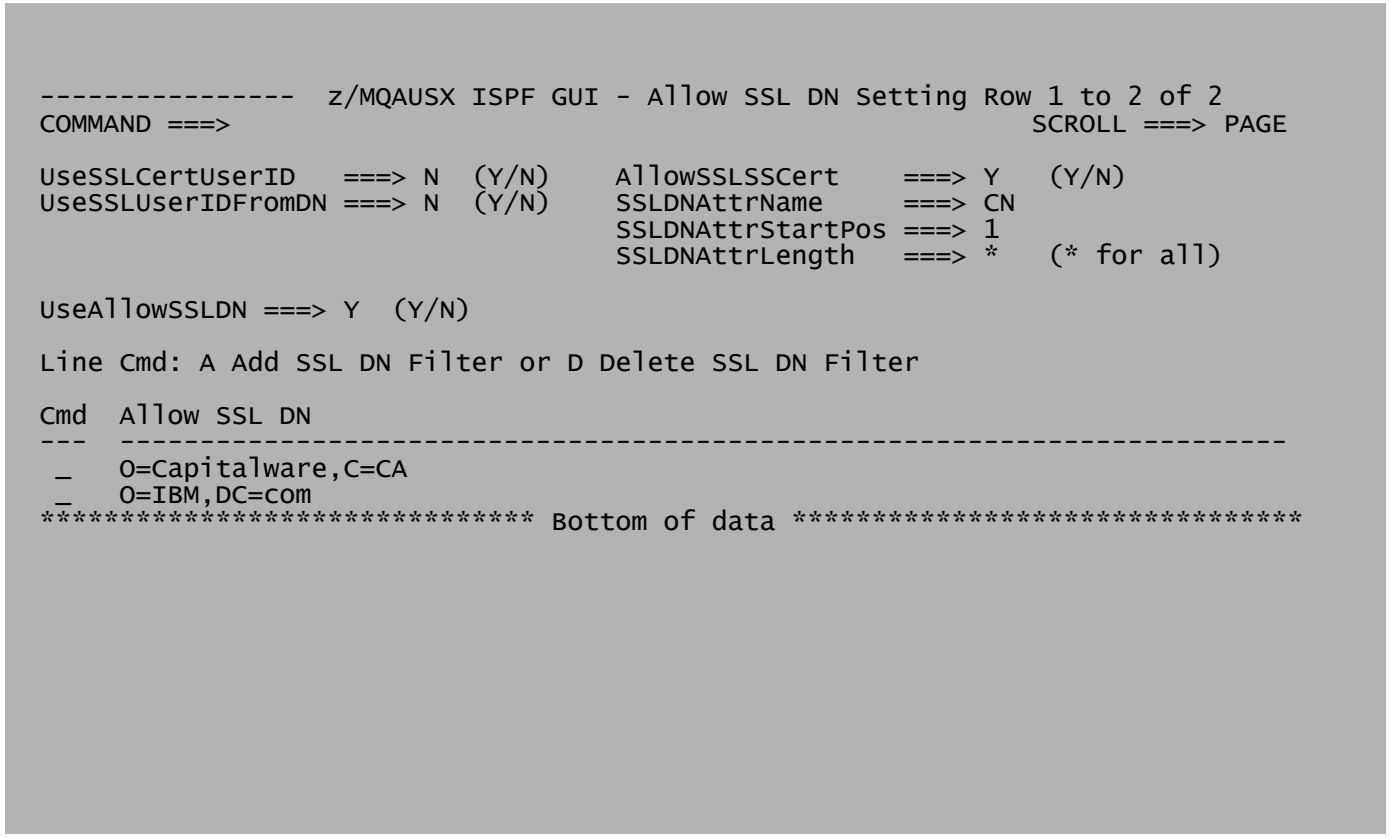
Configuration via MQAUSX-ISPF-GUI

```
----------------  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 ********************************
```

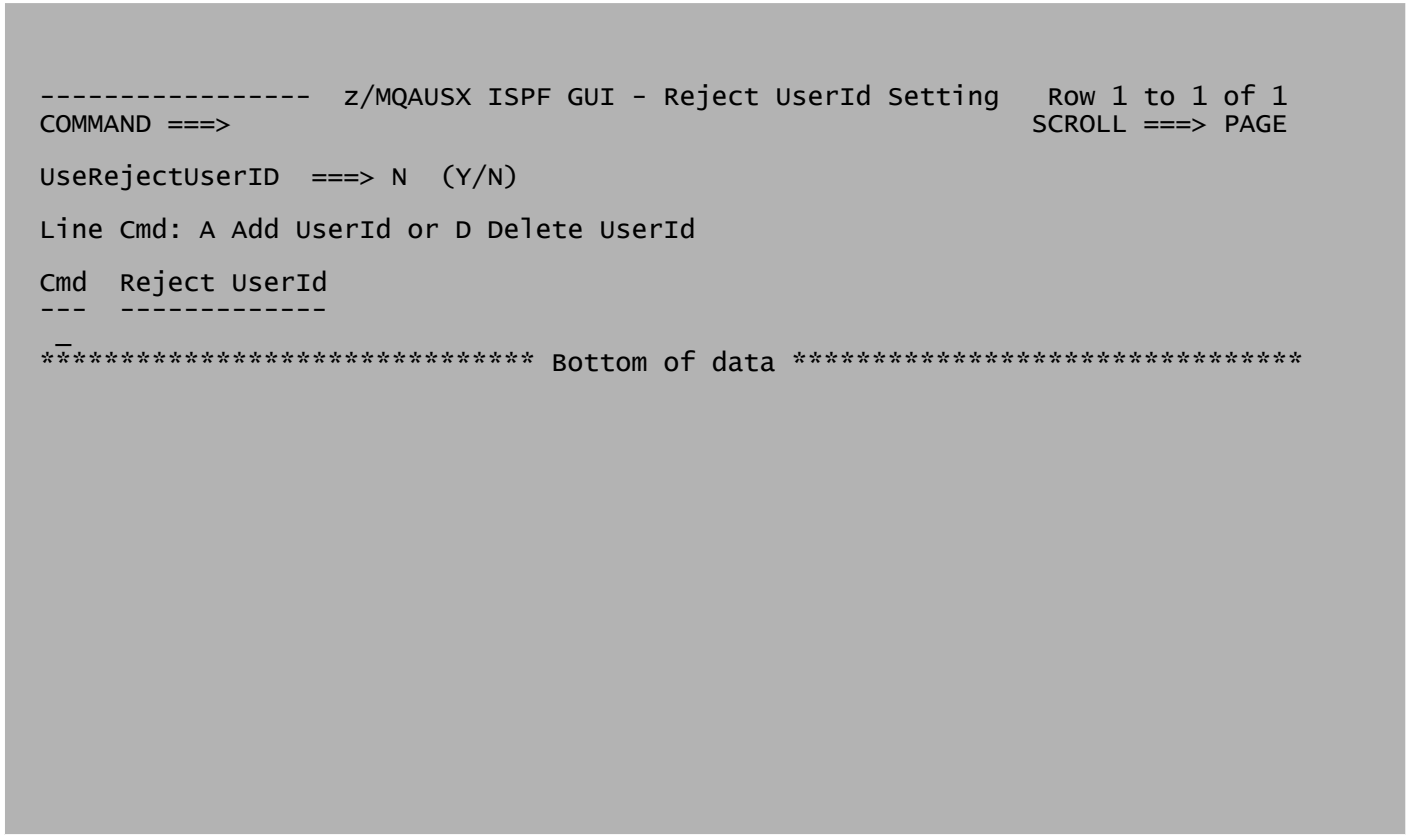
Configuration via MQAUSX-ISPF-GUI

```
----------------  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 ********************************
```

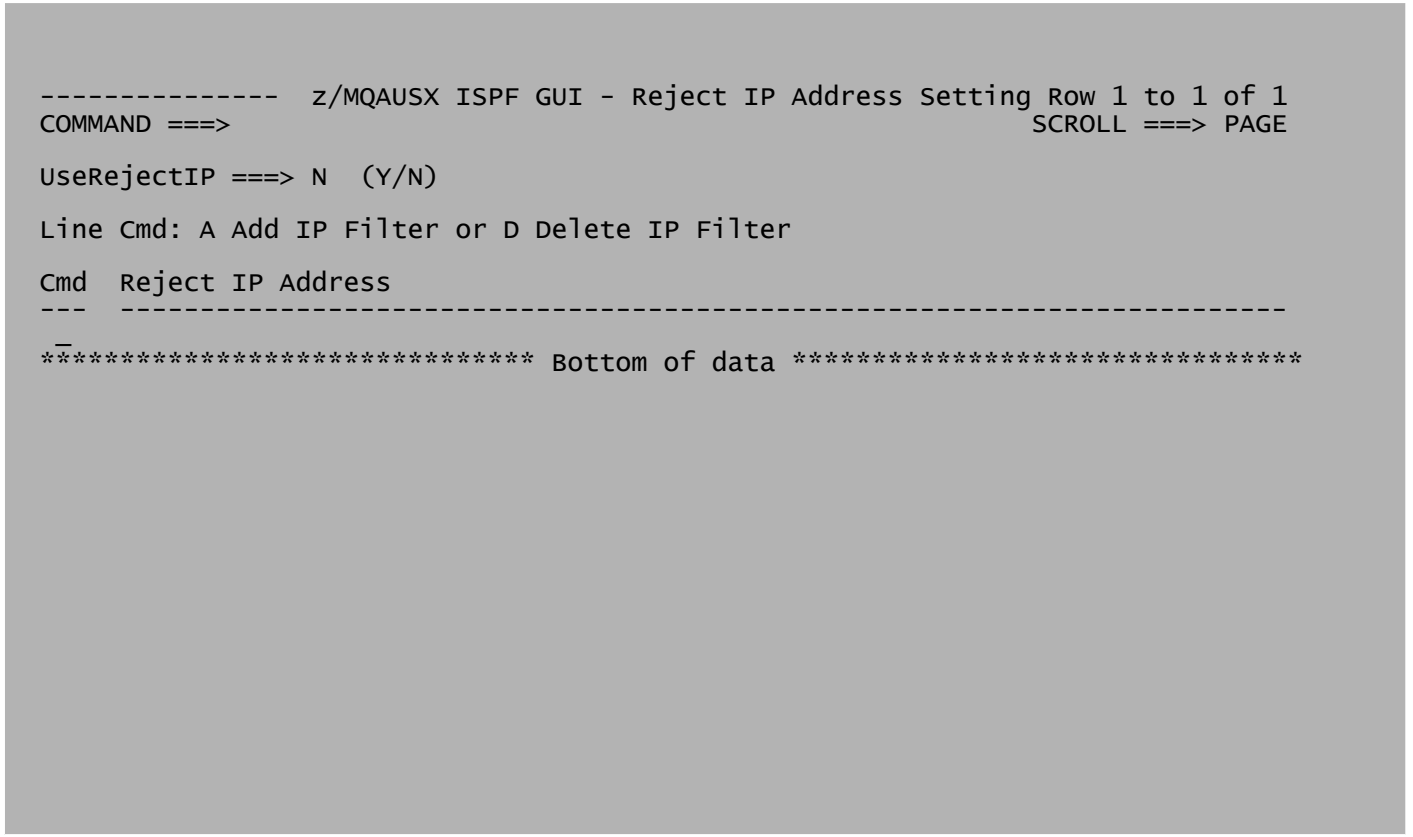
Configuration via MQAUSX-ISPF-GUI



Configuration via MQAUSX-ISPF-GUI



Configuration via MQAUSX-ISPF-GUI



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
MCCEventWarnLevel  ===> 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