What's new in MQ Message Encryption

Roger Lacroix
roger.lacroix@capitalware.com
https://www.capitalware.com

Background and Problem Statement

- Does your company want its message data in a viewable format?
- Does your company require that sensitive data be stored and/or transmitted in a secure format that complies with PCI and/or GDPR security requirements?
- MQ Message Encryption provides protection of data in a queue and/or topic (data at rest).

What's new in MQ Message Encryption v4

- Added Topic section so that MQME will protect topics.
- Added UseExcludeTopics and ExcludeTopics keywords to explicitly exclude topics from being protected.
- Added EncPassPhrase keyword to support the use of encrypted PassPhrase. Added 'enc_pp' program that will create an encrypted PassPhrase.
- Changed when the authorization is perform. Now it is done during the MQOPEN rather than MQGet and/or MQPUT/1.

What's new in MQ Message Encryption v4

- Support for MQ clients performing Pub/Sub
- Support for AMQP clients performing Pub/Sub
- Support for MQTT clients performing Pub/Sub

Data Protection for Queues & Topics

MQ Message Encryption (MQME) vs IBM MQ AMS (Advanced Message Security)

- IBM MQ AMS included with the MQ Advanced license. (Previously, required a separate license purchase)
- MQME is $299.00 (cheaper in volume) per queue manager plus 15% yearly maintenance and support fee

Data Protection for Queues & Topics (2)

Major Features of MQME:

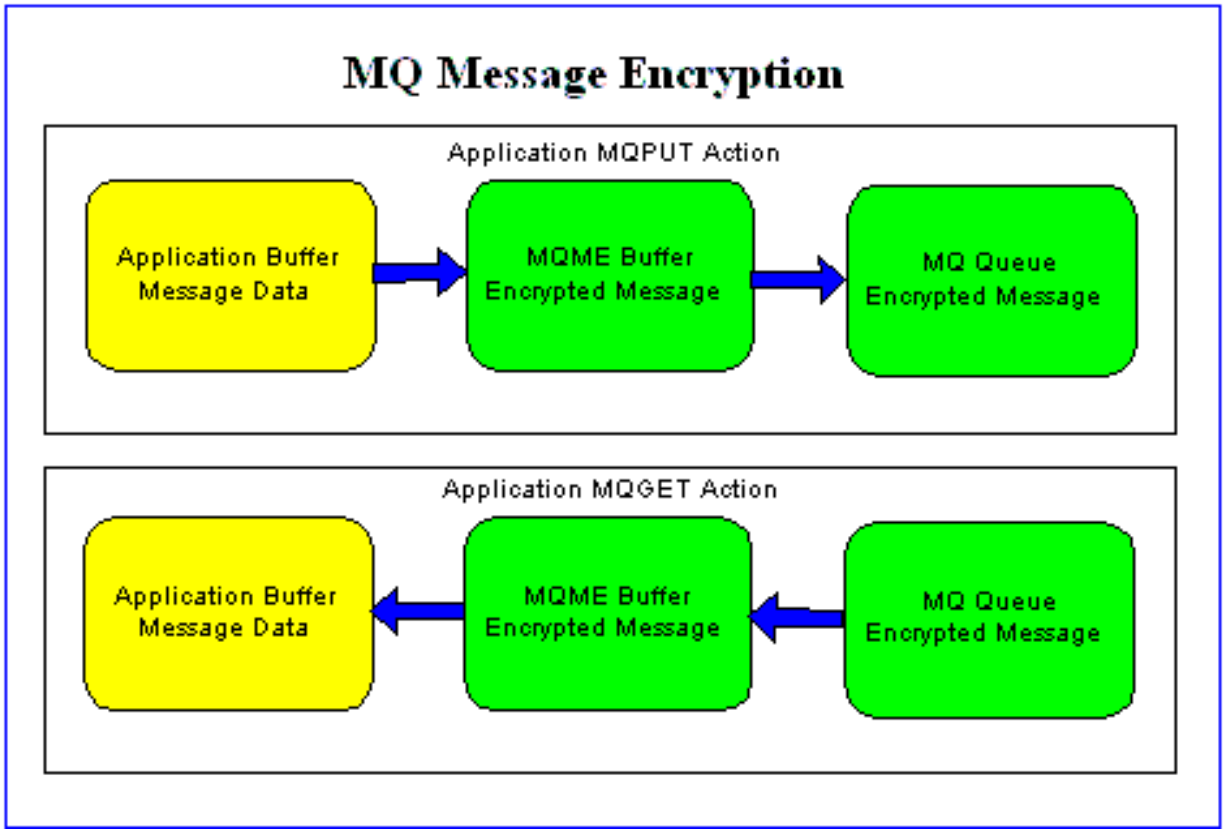
- Easy to set up and configure (unlike SSL/TLS)
- No application changes required
- All message data written to a selected queue will be encrypted
- Secure encryption methodology using AES with 128, 192 or 256-bit keys
- Uses the SHA-2 to create a cryptographic hash function (digital signature)

Data Protection for Queues & Topics (3)

Major Features of MQME (cont'd):

- Support for MQ clustering
- Group authority checking against the local OS groups or a group file
- Standard MQ feature, GET-with-Convert, is supported
- Provides high-level logging capability for encryption / decryption processing
- Yearly cost per queue manager: $45 vs $400

Data Protection for Queues & Topics (4)



Data Protection for Queues & Topics (5)

	MQME	MQ AMS
End-to-End Encryption	Yes	Yes
Supported Encryption	AES128, AES192, AES256	RC2, DES, 3DES, AES128, AES256
Digital Signature	SHA-2	MD5, SHA-1, SHA-2
Requires the purchase of an SSL certificate for each end point (~$400 USD)	**NO**	Yes
PCI compliant for separation of digital signature and message data in the message payload	Yes	No
Show encrypted message data to unauthorized users	**NO**	Yes

Data Protection for Queues & Topics (6)

	MQME	MQ AMS
Support Publish/Subscribe	Yes	**NO**
Support for Cluster Queues	Yes	Yes
MQGet with Convert for C/COBOL applications	Yes	Yes
MQGet with Convert for C++ applications	Yes	Yes
MQGet with Convert for Java applications	Yes	Yes
MQGet with Convert for .NET (C#) applications	Yes	Yes
Distribution lists	Yes	**NO**
IBM MQ classes for .Net in a managed mode	Yes	**NO**

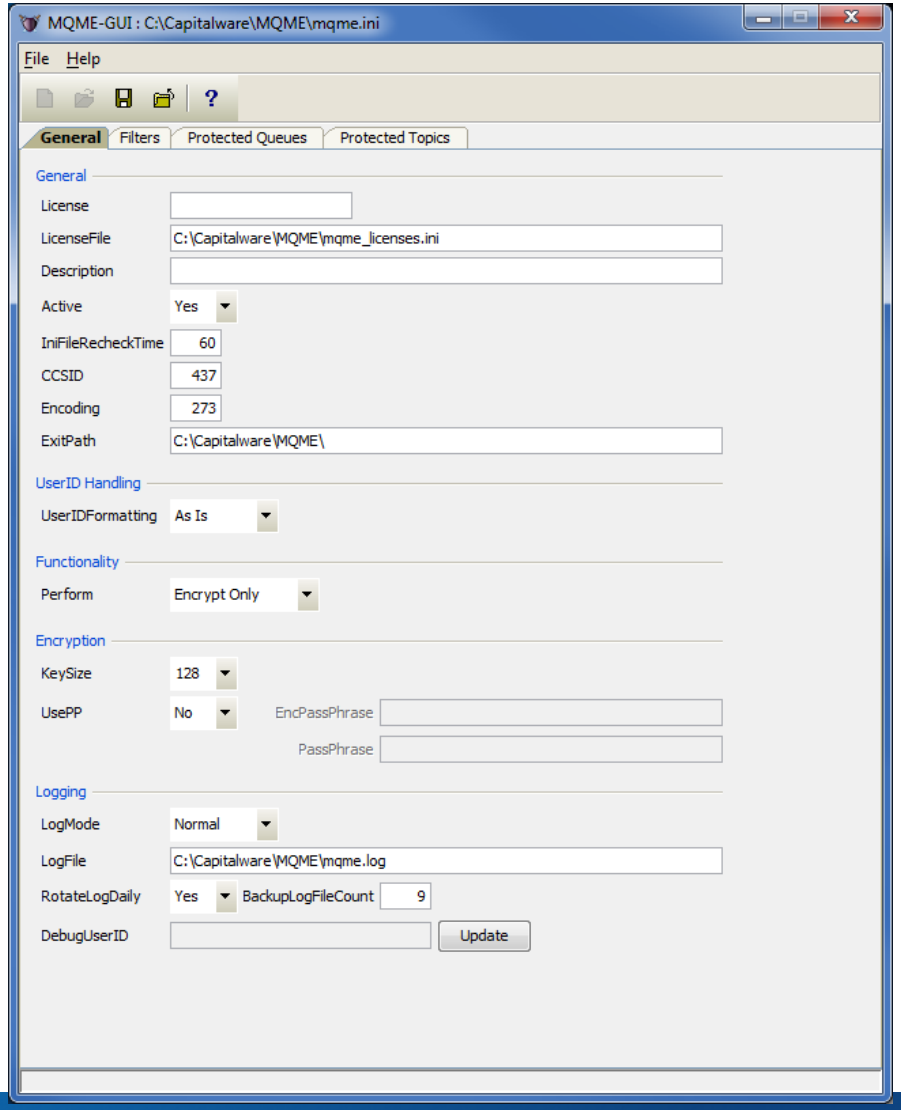
Data Protection for Queues & Topics (7)

	MQME	MQ AMS
Message Service client for .Net (XMS) applications	Yes	**No**
Message Service client for C/C++ (XMS) applications	Yes	**No**
Protection of SYSTEM.* queues	Yes	Yes
Require application code changes	No	No
Supported Platform: Unix (AIX, HP-UX & Solaris)	Yes	Yes
Supported Platform: Linux (x86, x86-64, Power & System z)	Yes	Yes
Supported Platform: Windows	Yes	Yes
Supported Platform: IBM i (OS/400)	Yes	Yes

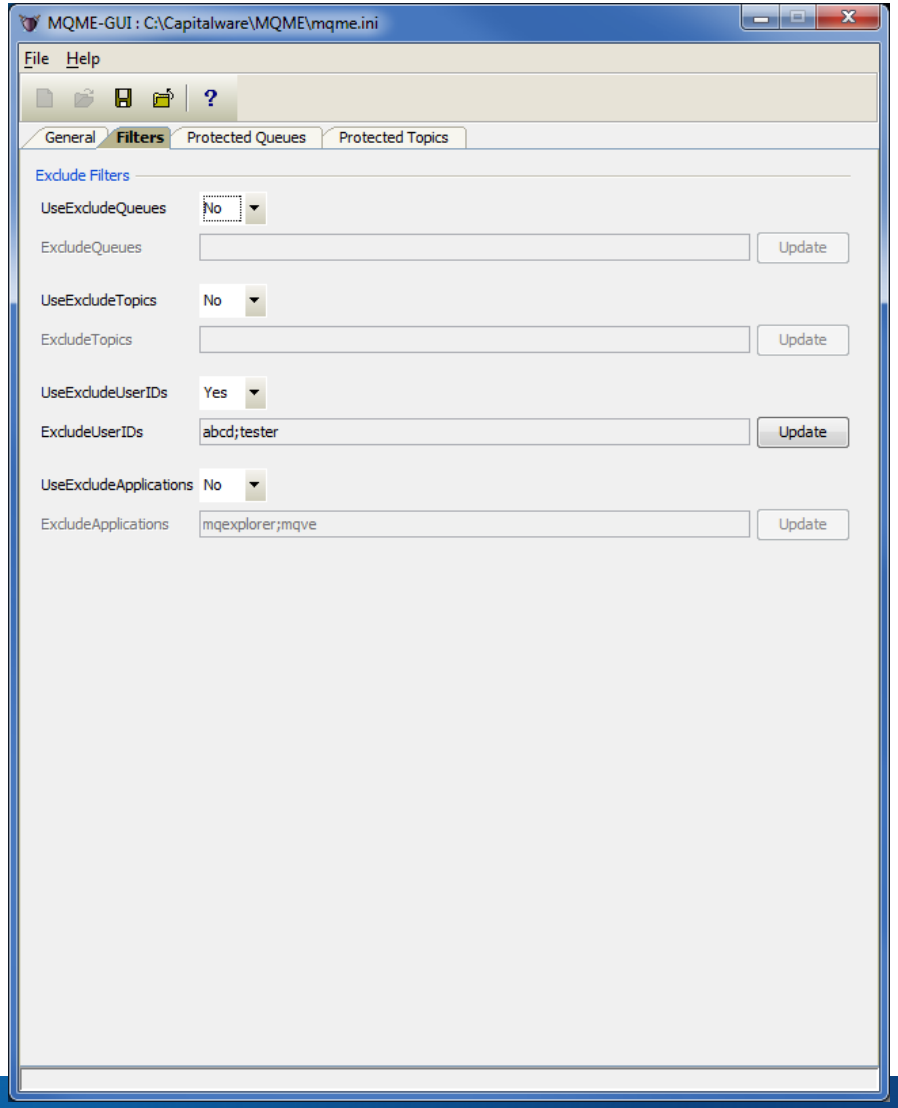
MQME IniFile

```
[default]
License=
LicenseFile=C:\Capitalware\MQME\mqme_licenses.ini
LogMode=N
LogFile=C:\Capitalware\MQME\mqme.log
RotateLogDaily=Y
Active=Y
IniFileRecheckTime=60
ExitPath=C:\Capitalware\MQME\
UserIDFormatting=A
Perform=E
KeySize=128
UseExcludeQueues=N
UseExcludeTopics=N
UseExcludeUserIDs=Y
ExcludeUserIDs=abcd;tester
UseExcludeApplications=N
ExcludeApplications=mqexplorer;mqve
#
[Q:TEST.*]
ApplicationsForGet = ag1
ApplicationsForPut = ap1
GroupFileForGet = C:\Capitalware\MQME\groupsForGet.ini
GroupFileForPut = C:\Capitalware\MQME\groupsForPut.ini
GroupsForGet = grp1;grp2
GroupsForPut = GrpA;GrpB
KeySize = 256
UseApplicationsForGet = Y
UseApplicationsForPut = Y
UseGroupFileForGet = Y
UseGroupFileForPut = Y
UseGroupsForGet = Y
UseGroupsForPut = Y
UserIDsForGet = roger
UserIDsForPut = Test1;Test2
#
[Q:ABC.*]
KeySize = 256
UserIDsForGet = appl01;appl02;appl03
#
[T:TEST/ABC]
UserIDsForGet = fred;barney;wilma
```

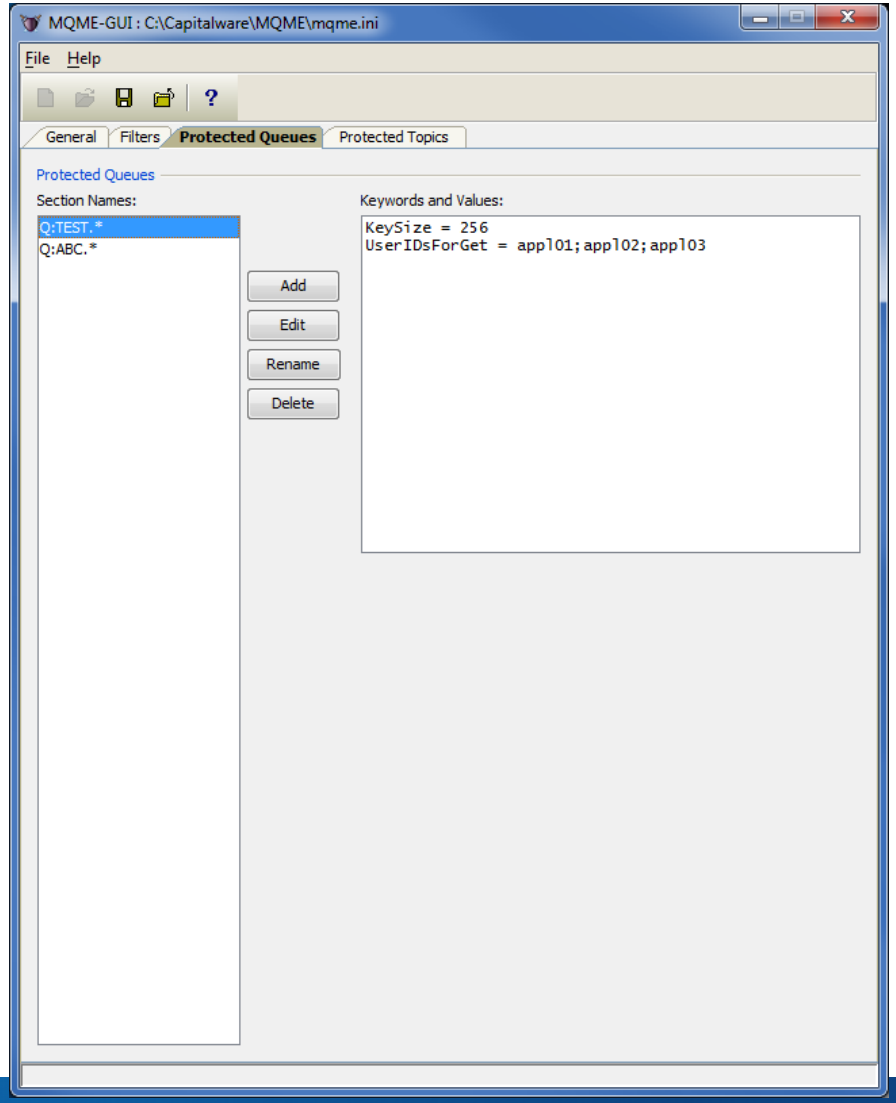
MQME-GUI


MQME-GUI : C:\Capitalware\MQME\mqme.ini
File Help
General Filters Protected Queues Protected Topics
General
License
LicenseFile C:\Capitalware\MQME\mqme_licenses.ini
Description
Active Yes
IniFileRecheckTime 60
CCSID 437
Encoding 273
ExitPath C:\Capitalware\MQME\
UserID Handling
UserIDFormatting As Is
Functionality
Perform Encrypt Only
Encryption
KeySize 128
UsePP No
EncPassPhrase
PassPhrase
Logging
LogMode Normal
LogFile C:\Capitalware\MQME\mqme.log
RotateLogDaily Yes
BackupLogFileCount 9
DebugUserID
Update

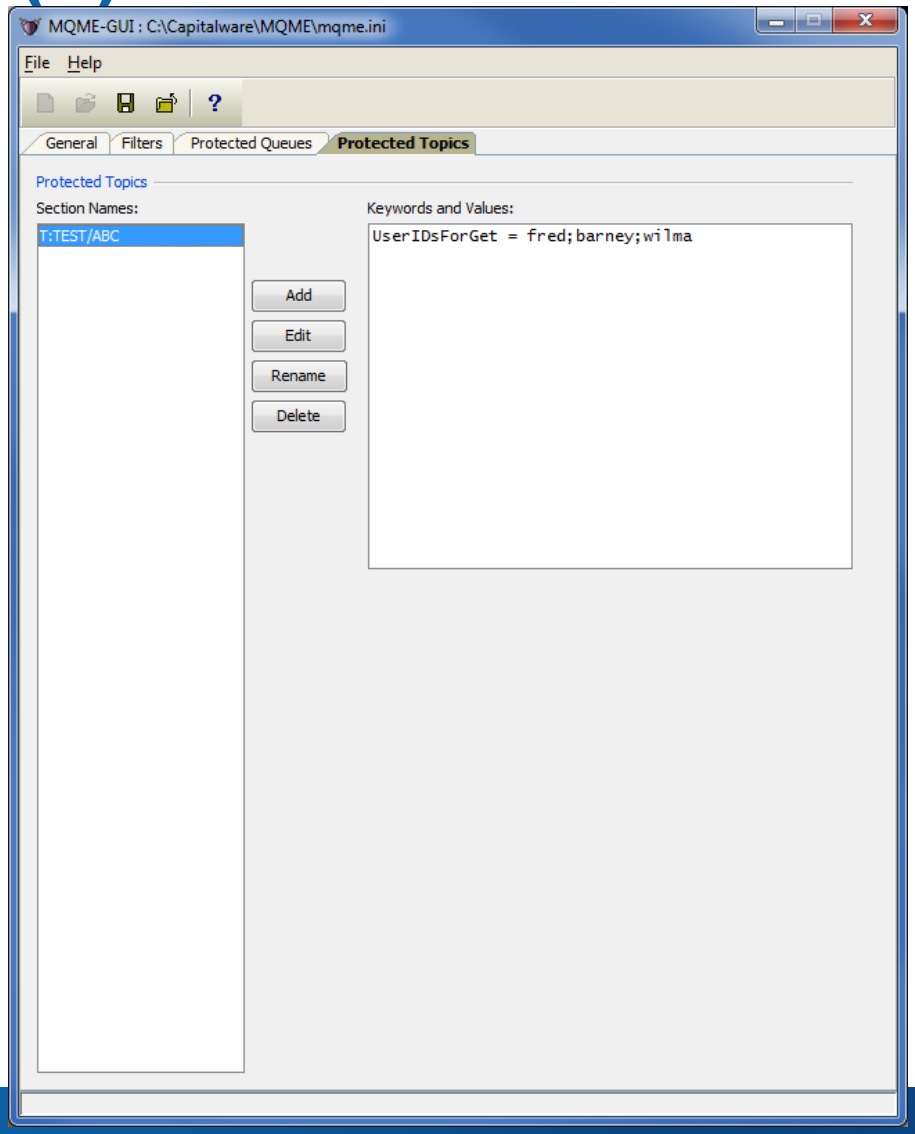
MQME-GUI (2)


MQME-GUI : C:\Capitalware\MQME\mqme.ini
File Help
General Filters Protected Queues Protected Topics
Exclude Filters
UseExcludeQueues No
ExcludeQueues Update
UseExcludeTopics No
ExcludeTopics Update
UseExcludeUserIDs Yes
ExcludeUserIDs abcd;tester Update
UseExcludeApplications No
ExcludeApplications mqexplorer;mqve Update

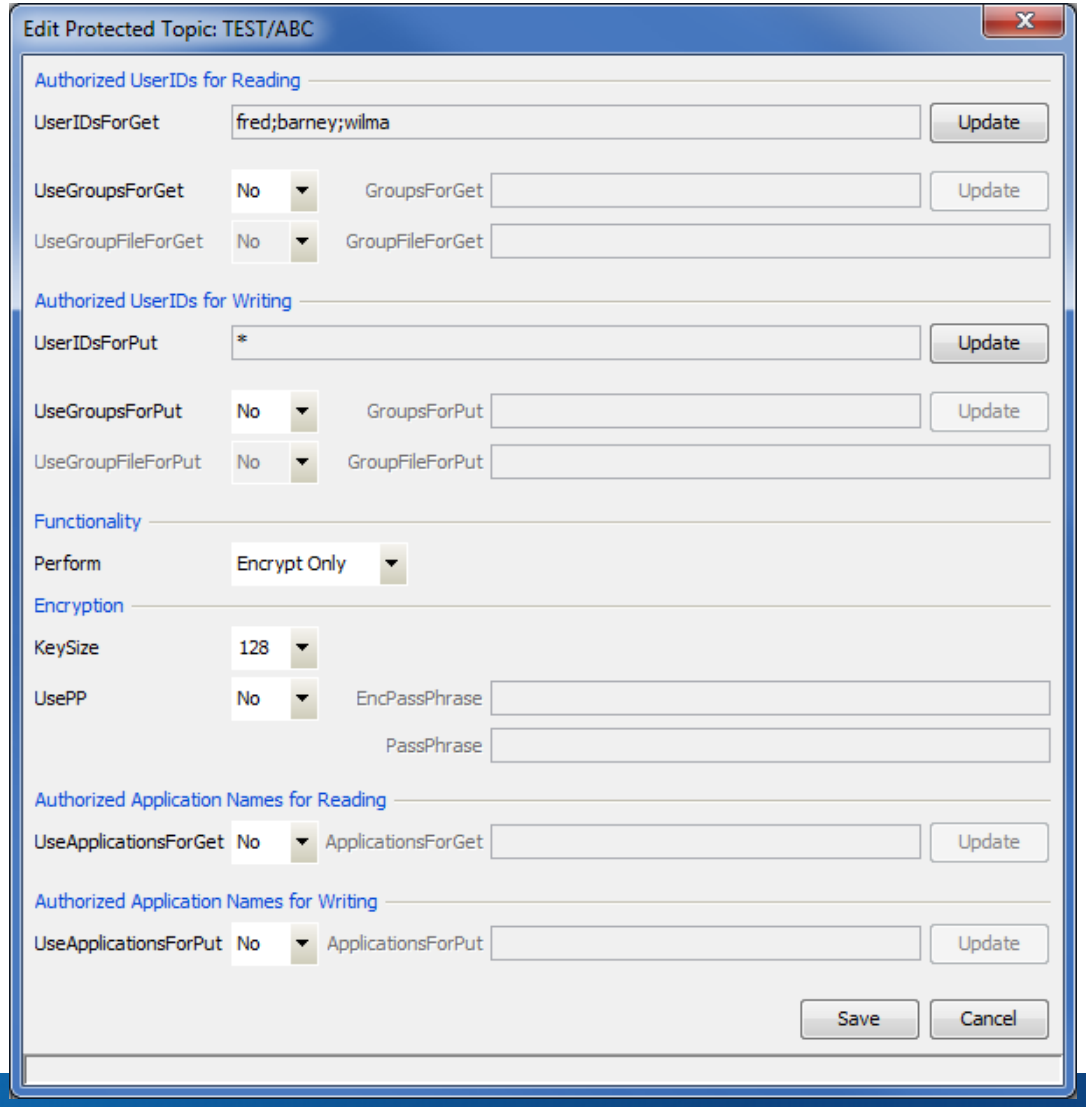
MQME-GUI (3)


MQME-GUI : C:\Capitalware\MQME\mqme.ini
File Help
General Filters Protected Queues Protected Topics
Protected Queues
Section Names:
Q:TEST.*
Q:ABC.*
Add
Edit
Rename
Delete
Keywords and Values:
KeySize = 256
UserIDsForGet = appl01;appl02;appl03

MQME-GUI (4)


MQME-GUI : C:\Capitalware\MQME\mqme.ini
File Help
General Filters Protected Queues Protected Topics
Protected Topics
Section Names:
T:TEST/ABC
Keywords and Values:
UserIDsForGet = fred;barney;wilma
Add
Edit
Rename
Delete

MQME-GUI (4)

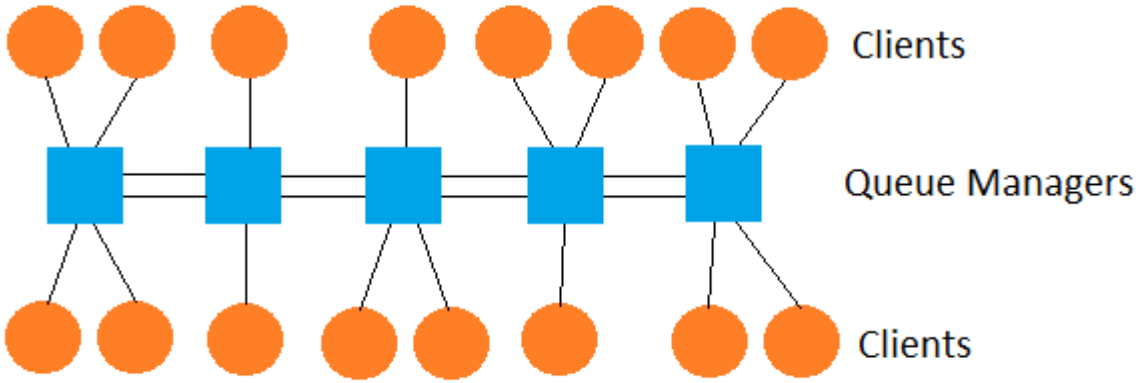

Edit Protected Topic: TEST/ABC
Authorized UserIDs for Reading
UserIDsForGet
fred;barney;wilma
Update
UseGroupsForGet
No
GroupsForGet
Update
UseGroupFileForGet
No
GroupFileForGet
Authorized UserIDs for Writing
UserIDsForPut
*
Update
UseGroupsForPut
No
GroupsForPut
Update
UseGroupFileForPut
No
GroupFileForPut
Functionality
Perform
Encrypt Only
Encryption
KeySize
128
UsePP
No
EncPassPhrase
PassPhrase
Authorized Application Names for Reading
UseApplicationsForGet
No
ApplicationsForGet
Update
Authorized Application Names for Writing
UseApplicationsForPut
No
ApplicationsForPut
Update
Save
Cancel

MQ Security Grid

- A “quick drop and go” way to have protected queues and protected messages across multiple queue managers:
  - Remote queues
  - Cluster queues
  - Even works with messages that originate from a client connection
  - And of course, local and alias queues

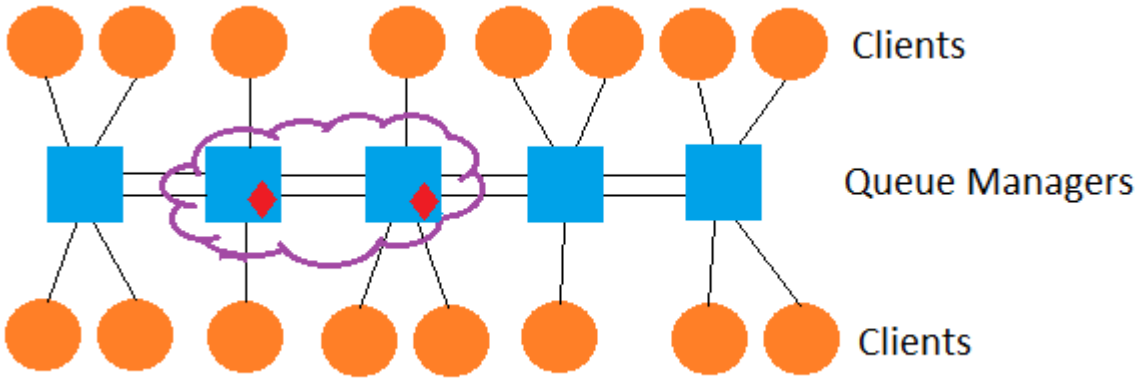
MQ Security Grid (2)

A standard MQ environment:



MQ Security Grid (3)

MQME deployed to 2 queue managers:

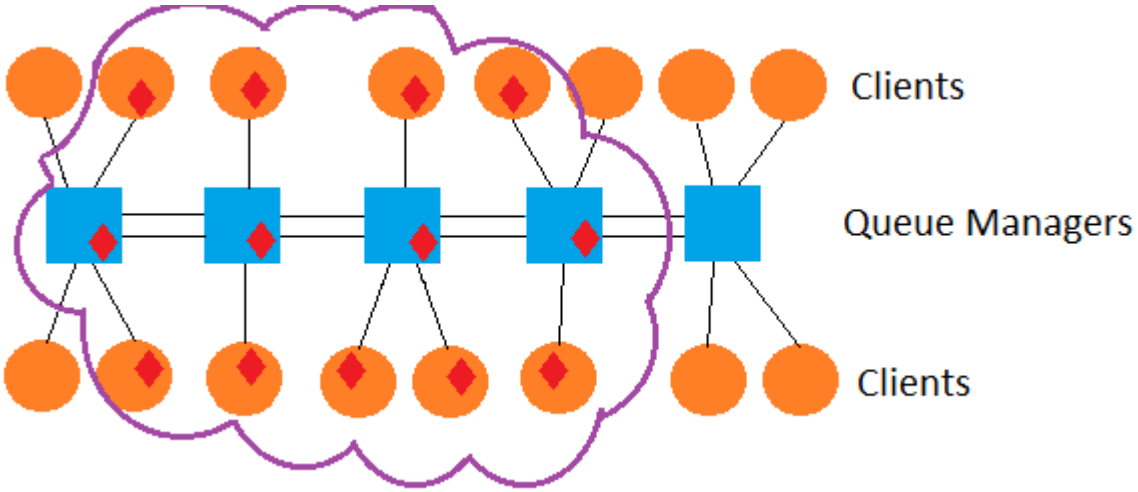


MQ Security Grid (5)

- Messages that “hop” between queue managers “can” stay encrypted if the user wishes.
- Will require MQME on the “final” queue manager for decryption but not on the intermediary queue managers.
- Does not require SSL/TLS for channel encryption!
- Does not require MQCE for channel encryption!

MQ Security Grid (4)

MQME deployed to 4 queue managers & 9 clients:



Questions & Answers