

MQSeries Explorer Security

Author: Neil Kolban, IBM ATS

E-Mail: kolban@us.ibm.com

Change history:

11/6/2000	First Release
11/7/2000	Updates on scydata length
1/18/2002	Doc Updates

MQSeries Explorer Security

This document describes a solution for MQSeries Explorer Security exposures as well as providing a background on some of the problems that are resolved.

MQSeries Explorer Exposures

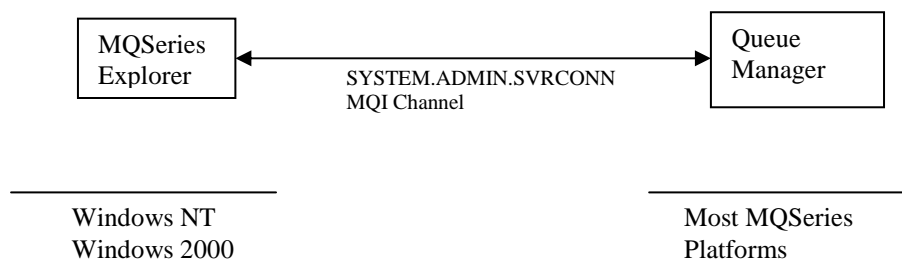
With the arrival of MQSeries V5.1 for Windows NT, a new and valuable addition was made to the MQSeries family of products. Included in this release was a component called the "MQSeries Explorer". This component provided a graphical user interface environment to perform administration of both local and remote MQSeries queue managers.

Queue managers can be remotely administered by creating a SRVCONN channel definition called "SYSTEM.ADMIN.SVRCONN". In addition the MQSeries Command Server and Channel Listener demons must be started.

With these settings in place, a user on an NT system can invoke the MQSeries Explorer and connect to the remote queue manager and perform remote administration.

The MQSeries Explorer connects to the remote queue manager as an MQSeries Client. When the client connects, it implicitly passes the userid of the Windows NT logged in user that is running the MQSeries Explorer. The remote queue manager will then execute administration commands with the MQSeries authorization of that user. The user propagated should have sufficient MQSeries authority to perform the requested administration commands.

The following diagram illustrates the MQSeries Explorer connection ...



Unfortunately, the scenario described opens a serious vulnerability in MQSeries security. When the Queue Manager receives the MQSeries Explorer connection request, it does not validate that the requests arriving actually came from the legitimate end user. For example, if a user called "MQADMIN" were authorized on the Queue Manager system, anyone who knew how to create a local NT user id could create one called MQADMIN on their local system and be granted full authority to administer the remote queue manager.

MQSeries Explorer Security exits

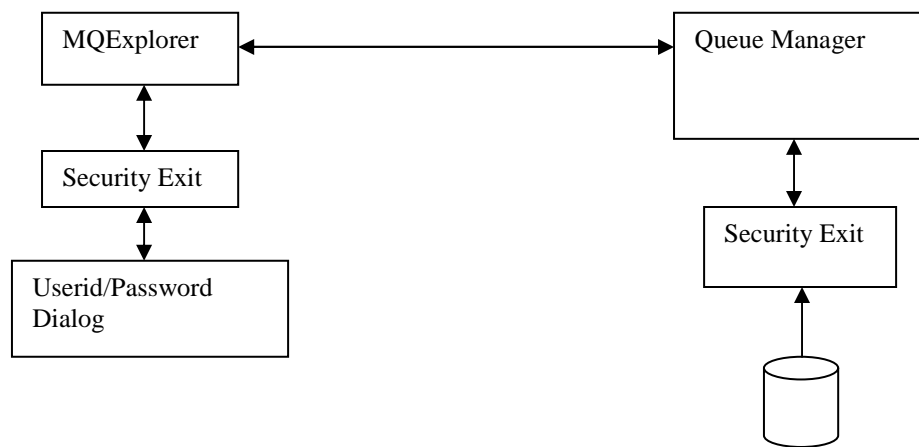
Fortunately, MQSeries has inherent architecture to resolve just these kind of issues. When an MQSeries channel is formed between two systems, a pair of Security Exits can be designed and implemented which exchange arbitrary security information and, based on that information, can either allow or disallow incoming connection requests.

A pair of security exits have been designed and implemented to enhance the function of MQSeries Explorer.

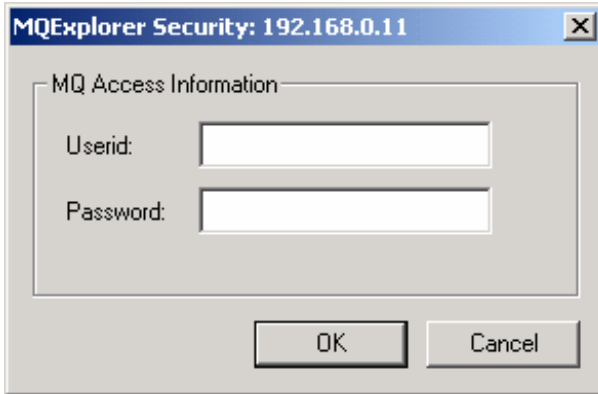
The exits consist of two DLLs or shared libraries. One is a Windows DLL that must be installed (copied) onto the machine on which MQSeries Explorer is installed. The other is either a DLL or Unix shared library which must be copied to the machine that is to be administered.

When MQSeries Explorer is configured with the security exit and a connection request is sent to a remote machine, a dialog will appear prompting for a userid and password pair. When supplied, this authentication information is sent to the partner exit at the queue manager. The exit will then search a file for a matching userid/password combination and, only if present, will the connection be formed with the authority of that userid.

The logic of the solution is shown in the following diagram:



The dialog displayed prompting for the userid/password is as follows:



It contains the name of the connection to the remote queue manager as part of the dialog title (unfortunately, the name of the target queue manager is not supplied by MQSeries to the security exit for MQSeries clients).

The data file located at the target queue manager contains userid/password pairs. This file is flat ASCII format with each userid/password pair on a single line and white space separating the userid from the password. The following illustrates a sample configuration file:

```
MQAdmin      adminpw123
Payroll      xyZZy
Support      WonderLand
```

When a userid is supplied by the MQSeries Explorer, it is searched for in the file. If the password associated with the user matches the password supplied, the MQExplorer client session is authorized as the associated user and has all the MQSeries privileges of that user. Note that the user's password for MQSeries Explorer authentication is the one contained in the password file and not necessarily any password associated with the user for operating system authentication.

Installing the package

The package consists of two DLLs, one to be located at the queue manager and one to be located at the workstations running MQSeries Explorer.

Installing and configuring at the Queue Manager

On the machine where the queue manager to be administered resides, the SecExitRcvr.dll file must be installed. This file can be copied into the default exits directory of MQSeries ... for example:

Windows NT	C:\Program Files\MQSeries\exits
Linux	???

Next, the password file must be created and some userid/password pairs added. The path and name of the file must be 32 characters or less as this is the maximum amount of data that may be passed to an exit as a parameter. The format of the file should be as illustrated previously. For example:

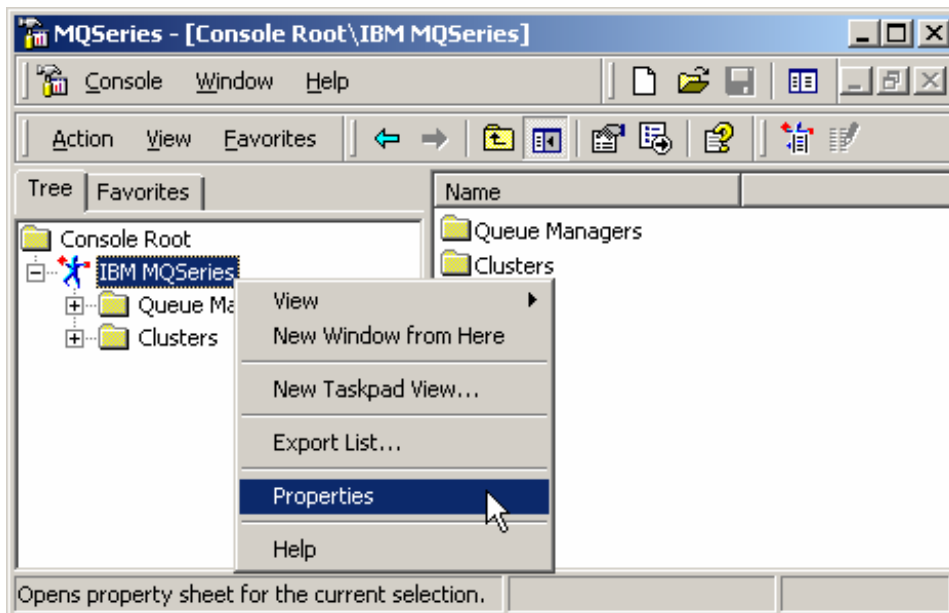
```
MQAdmin      adminpw123
Payroll     xyZZy
Support     WonderLand
```

Finally, the SYSTEM.ADMIN.SVRCONN channel definition must be altered to point to the new security exit. The following runmqsc command will achieve this task:

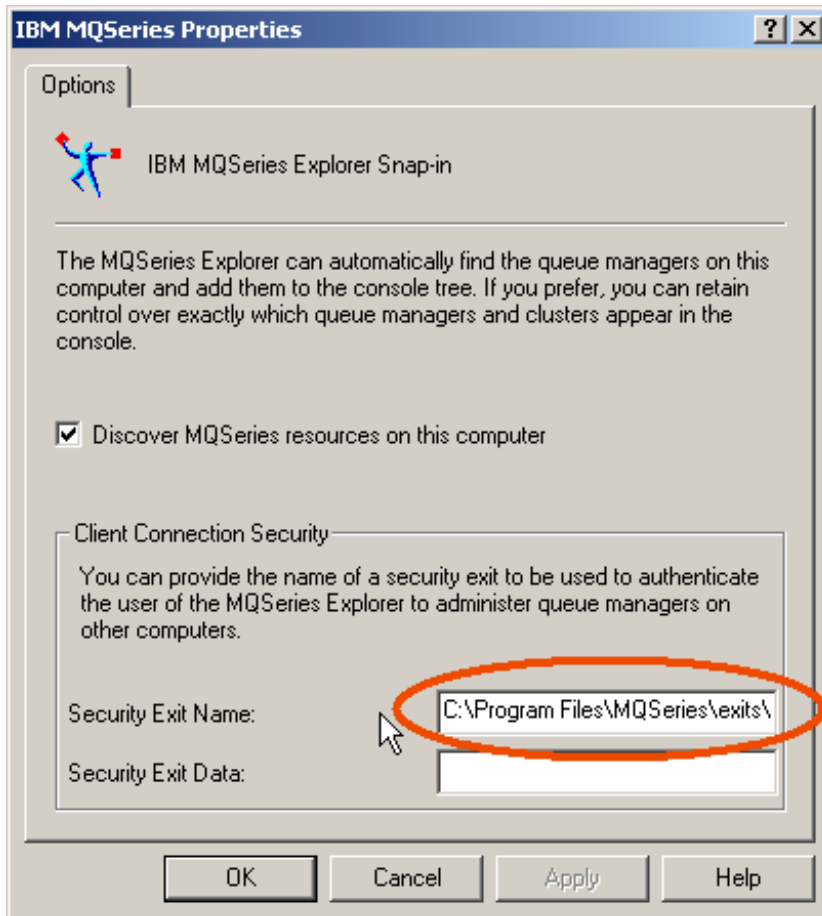
```
alter channel(SYSTEM.ADMIN.SVRCONN) +
  secyexit('C:\Program Files\MQSeries\exits\SecExitRcvr(SecExitRcvr)') +
  secydata('C:\mq\password.txt')
```

Installing and configuring on the Workstation

On the machines which will execute the MQSeries Explorer, the ExpSecExit.dll file must be installed. This can also be installed in the default exit directory. To configure MQSeries Explorer to utilize the exit, start MQSeries Explorer as normal and right-click "IBM MQSeries" and select "Properties" from the context menu which appears:



The following dialog will appear:



Within the dialog, an area is provided to supply a named security exit (highlighted). This can be set to the name of the MQSeries Explorer exit ... for example:

```
C:\Program Files\MQSeries\exits\ExpSecExit(SecExitSdr)
```

Note the entry-point name within the exit is called SecExitSdr.

The MQSeries Explorer side exit does not need to be passed any parameters so the Security Exit Data field may be left empty.

Once entered, save the MQSeries Explorer console from the "Console" and then "Save" menus. Now when a new connection is formed to a **remote** queue manager, the MQSeries Explorer will display the dialog prompting for a userid and password. Be sure and test with a remote connection to a queue manager as a local connection (server binding) does not connect through any security exits.

Further notes

This package was developed to provide a working sample of MQSeries security for the MQSeries Explorer interface. Currently the package is **only** available as compiled code

on Windows NT/2000. Source may be released in the future. If additional queue manager binaries are required for further platforms, please contact me and we can attempt to arrange for those to be built/tested.