Mandatory Access Control

Introduction

Mandatory access control (MAC) is a security strategy that applies to multiple user environments. It enforces the strictest level of control among other popular security strategies. Intended for government and military use to protect highly classified information, enterprise businesses are increasingly implementing MAC to protect sensitive personal information (SPI) and to meet other stringent security requirements.

A key differentiator for MAC is that it restricts individual resource owners from granting or denying access to their resources. Instead, security is administered by a central authority, such as a system administrator. Users or owners cannot change the access of other users or objects. MAC is sometimes referred to as non-discretionary access control. By contrast, discretionary access control (DAC) allows each user to control access to their own objects.

System administrators can optionally enable Web Query for MAC. When doing so, the sign on password for the QWQADMIN profile will be removed. QWQADMIN will continue to own Web Query objects and run the server jobs, but users will no longer be able to sign in as QWQADMIN. Removing the password and sign-on capability restricts the owner privileges of QWQADMIN, hence enabling MAC compliance. (Though the password is removed, status of the QWQADMIN profile must still be *ENABLED.)

Web Query uses the IBM Toolbox for Java as its default Java Database Connectivity (JDBC) driver. When MAC is enabled, Web Query instead uses the IBM Developer Kit for Java, commonly known as the native JDBC driver. Though the JDBC driver is transparent to Web Query end users, the native JDBC driver is better suited to Web Query when the QWQADMIN password is removed.

Web Query administrative tasks can be performed without a QWQADMIN sign-on. Administrators can use their own ID to manage Web Query, rather than share the QWQADMIN profile. This supports basic security principals that each user should be uniquely identified in a system and that each operation should be accountable to only one user.

Among the administrative tasks, Security Center and console functions can be performed by Web Query administrators. To access the full server console, expand Reporting Servers on the Web Query portal, right click EDASERVE, and select Reporting Server Console. The server console can alternatively be accessed directly on port 12333, but not all console functions are available to a Web Query administrator with this approach, so it is recommended to access the console from the portal tree.

Web Query administrators themselves can be managed by system administrators without a QWQADMIN sign-on and without logging in to Security Center. A system administrator can add or remove a Web Query administrator using the Register Web Query User (REGWQUSR) and Remove Web Query User (RMVWQUSR) commands. The commands require security administrator, *SECADM, authority.

By default, MAC is disabled for Web Query. A password must be set for the QWQADMIN profile or Web Query will fail to start. To enable Web Query for MAC, see the prerequisites and instructions in the following sections.

Prerequisites for MAC Enablement

Before enabling Web Query for MAC, a system administrator can easily determine if all prerequisites are met by running this command:

```
CALL QWEBQRY/MACPREREQ
```

Web Query enforces the following prerequisites when enabling MAC.

1. Web Query 2.2.1 group PTF level 6 or later must be installed.
2. The following PTF for IBM Toolbox for Java (JTOpen 9.4) must be applied, per your 5770SS1 operating system level:
   V7R1M0 SI65613
   V7R2M0 SI65619
   V7R3M0 SI65622
3. The system value QMLTTHDACN that determines multithreaded job action must have a setting of 1 or 2. For more information on the system value, refer to https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_73/rzakz/rzakzqmltthdacn.htm.
4. Jobs that run Web Query programs or CL commands must have a job CCSID other than 65535. (The native JDBC driver does not allow a job CCSID of 65535.)
5. The Java extensions directory, /qibm/userdata/java400/ext, should not contain a version of jt400.jar. It can cause conflicts with the native JDBC driver used for MAC enablement. It is best practice to put .jar files in the class path of the application that requires them, rather than in the global extension directory that is common to all Java applications.

Enabling MAC

Web Query must be installed, and must be started at least one time, before it can be enabled for MAC. The first startup performs tasks that complete the installation process.

Following are the one-time steps to enable Web Query for MAC.

1. End Web Query using the End Web Query (ENDWEBQRY) or Work Web Query (WRKWEBQRY) command.
2. Run the command: `CALL QWEBQRY/QWQMACCONF PARM('1')`. The system administrator will need *ALLOBJ authority to run the command.
3. Start Web Query using the Start Web Query (STRWEBQRY) or WRKWEBQRY command.

The QWQMACCONF program will remove the password from QWQADMIN profile and perform necessary configuration changes that allow it to be removed.

Migration Considerations

The Web Query product, 5733-WQX, can be migrated from one system to another using the Migrate Web Query (MIGWEBQRY) command. It's a very convenient command, for example, when moving a test environment to the production partition, or when moving to new hardware. During a migration, the MAC status of Web Query on the target system is overwritten by that of the source system.

Any migrations using MIGWEBQRY from Web Query version 1, 5733-QU2, to the current version 5733-WQX must be done before MAC is enabled on the target system.