CU2 Global Pty Ltd

The Global Data Conversion Experts

ConvertU2 Technologies

The Data and Software Conversion Experts

Microsoft Access Workgroup Security Management in a 2SQL Conversion Project.

February 2014

Table of Contents

INTRODUCTION 3

MICROSOFT ACCESS WORKGROUP SECURITY MANAGEMENT 4

DATABASE SECURITY. 4

OBJECT LEVEL SECURITY 5

Introduction

Microsoft Access Workgroup Security is obsolete as of Access 2010. However, if earlier versions of Microsoft Access databases have Workgroup Security, and are opened with Access 2010, problems can occur. These problems depend on the features of Workgroup Security that were used when creating the original Access database.

Experience shows that Microsoft Workgroup Security is only used in a very small proportion of Access databases, in less than 1%. This usage frequency may have well figured in Microsoft's decision to drop the facility.

However for those databases which do use it, Workgroup Security can be applied at the ***Database*** level or at the ***Object*** level (Tables, Queries, Forms, Reports, Macros, Modules). Again, experience shows that around ***99%*** of Workgroup Security implementations are at the ***Database*** level and only around ***1%*** are at the ***Object*** level.

2SQL utilizes Access 2010 and SQL Server 2008 R2 as core operational components. Therefore should you wish to convert and migrate an Access database containing Access Workgroup Security then this database needs to be reviewed ***prior*** to being processed by 2SQL.

This document assumes that the reader has a basic knowledge of Access Workgroup Security in discussing the various types and management strategies for handling this issue.

A comprehensive overview of Access Workgroup Security is discussed in the following link:

http://support.microsoft.com/kb/305542

____

Microsoft Access Workgroup Security management

There are two types of Workgroup Security in Microsoft Access:

- Database Security – utilized in approximately 99 % of Workgroup Security implementations.
- Object Level Security – only utilized in around 1 % of Workgroup Security implementations.

Database Security.

Database Security at the ***user level*** is when a ***user name*** and ***password*** is used to open the database. This is not to be confused with Access Database passwords, which operate at the database level requiring ***any*** user to enter the database password, that can still be implemented and is not part of Workgroup Security.

When new databases are created with this kind of Workgroup Security, the '**Owner**' property of the Access database is set to that of the user name that is logged in using Workgroup Security. If this user name is **NOT** admin, the database will not be able to be converted to Access 2007/2010 format.

There are two solutions to this:

1. Open the database in the version of Microsoft Access that the database was created in prior to Access 2007/2010 and then, using WorkGroup Security, change the owner back to Admin. However this is not always possible due to lost passwords or workgroup files.
2. Create a brand new database in Access 2010, and import all the objects from the original database, into the new one. This is a very reliable method to overcome Workgroup Security at the database level.

Security at the ***Database*** Level has a SQL Server Equivalent. It is called SQL Server Authentication and 2SQL is able to use either Access or SQL Server Authentication when performing the database conversion.

If SQL Server Authentication is not used during the conversion it can be implemented very easily after the conversion, taking only minutes to apply.

Object Level Security

Object Level Security relates to security and permissions on Tables, Queries, Forms, Reports, Modules and Macros. This level of Security is much more complex to remediate.

Each object that has Workgroup Security must have **all** permission restrictions removed and the owner of each object must also be changed back to Admin.

For the ***Table*** and ***Query*** objects there is a SQL Server equivalent. It is called SQL Server Permissions and any SQL Server DB Administrator should have competency in setting it up.

For the other objects, ***Forms, Reports, Macros and Modules*** there is no equivalent in SQL Server as these objects **do not go across to SQL Server**. They stay in the Access front-end.

Remembering that Access 2010 does not implement Workgroup Security, then Forms, Reports, Macros and Modules can't have this type of security associated with them as a result of Microsoft's withdrawal of support.

If security for these objects is still required after conversion then a site specific security module would be required to be written for the database. This is done in the VBA code area of Access**.**

____