Using Microsoft Access Securely

White Paper – Produced by LinkedIn Professional Microsoft Access Developers' Network (PMADN) Group

Date: Tuesday, January 12, 2016

Acknowledgements and Key Contributors

This White Paper is a collaborative writing project by members of the LinkedIn Professional Microsoft Access Developers' Network (PMADN). The PMADN group is a business and information exchange networking group for the benefit of the Microsoft Access Professional Developers community including VBA, VSTO/.Net technical discussions as well as general consulting & business analysis and other relevant topics. Our members include several MVPs & MS insiders.

A list of key contributors, to this paper, follows:

PMADN Contributor	Professional Credentials	Contributor Role
Michelle Meyer	Owner - 1st Contact Databases	Lead Writer – Project Manager
Mark Burns	Sr. MS-Access / SQL Server Developer at TD Bank for Global Technical Talent	Owner of PMADN LinkedIn Group
Patrick Headley	President and Application/Database Developer at Linx Consulting, Inc.	Technical Contributor & Reviewer
David Harris	Director at CropCheck Ltd	Technical Contributor & Reviewer
David Nealey	Sr. Lead Capture Manager	Technical Contributor & Reviewer
Frank Rotolo	Business Consultant and Developer	Technical Contributor & Reviewer
Bonnie Hicks	Lead HR Database Analyst - The Home Depot	Technical Contributor & Reviewer
Jack Leach	Business Software Solutions Expert, owner of Dymeng Services	Technical Contributor & Reviewer

Table of Contents

Preface

With each passing year, the costs of data management software continue to rise. In addition, organizations always have local data which doesn't fit into the proprietary software packages. Microsoft Access is a very cost effective and timely solution to local data management needs. However, there are many fears and misunderstandings about MS Access and its capabilities. One of the largest false beliefs is that MS Access is not safe to use for sensitive data. This paper details best practices for using Microsoft Access securely, in your organization.

Local Data Niche

In order to fully explore the security of MS Access, it is highly important to understand where it belongs in the data management toolbox. Specifically MS Access is designed to be used for local data management. Local data can be defined as follows:

1. Information that does not "fit" into an organizations' enterprise software.
2. Information that is shared by a core group of users, this can include, but is not limited to information:
   a. Shared by users in one department
   b. Shared, by workgroups, across multiple departments.
   c. Which intersects multiple software packages, but needs to be managed independently – to minimize double-entry in separate software systems

By its' very nature information is dynamic, it evolves over time. Local data is organic, it arises when co-workers are solving problems and come up with new ways to identify, track and manage the information around those problems. Local data reflects the creativity of an organization's employees. Very often local data is quite critical. Much of the time, it is local data which distinguishes an organization, or department within an organization, from its' competitors.

Security Starts by Using the Correct Tool for the Job

Within the Microsoft suite of products, MS Excel is designed for data analysis and very basic data management. The next product in Microsoft's data management suite is MS Access. Two signs that information has evolved to the point of needing relational data management follow:

Network folders full of spreadsheets for every reporting period, or complimentary data type

Frequent copy/pasting of one spreadsheet application to a new reporting period, or new set of data is a major sign that Excel is being misused. This dynamic can actually lead to some pretty serious errors. An example of the dangers can be found in this Forbes Article detailing the impact of Excel spreadsheet copy/pasting practices on the financial crash of 2007. http://www.forbes.com/sites/timworstall/2013/02/13/microsofts-excel-might-be-the-most-dangerous-software-on-the-planet/

Spreadsheets trying to manage complex one-to-many relationships

Often spreadsheets have multiple columns handling the same type of data, but categorized differently in each column. Or, spreadsheet applications consist of multiple interlinking spreadsheet files, all dependent on each other. Both these instances may mean it's time to do an analysis and decide if the data is complex enough to move to a relational database level.

Microsoft accommodates data evolution by offering a relational database tool designed specifically for local data management. MS Access surpasses other relational databases in the following ways:

1. MS Access is the most cost effective RAD (Rapid Application Development) tool on the market. Because of its' native development tools, MS Access programs faster and cheaper than .Net and other competitors. Bottom line thinking applies here. Used properly MS Access can save your organization a lot of money in both development time, and budget dollars.
2. MS Access is the most flexible relational database tool on the market. Again internal programming tools allow for faster and cheaper application revisions.
3. One of the most common local data management needs is to integrate unique internal data with information stored in other software packages. MS Access integrates very easily with other database platforms, making it a fantastic tool for a data integration project.
4. MS Access can be used quite successfully in a multi-user environment.
5. MS Access is built by Microsoft, and works seamlessly with other MS Office products. Whether it is Excel, Outlook or Word, MS Access can share data without investing exorbitant amounts of time in programming.

Microsoft Access Security Best Practices (Basics)

Microsoft Access is designed to be used on your network and stored in your network folder structure. But, unlike many other files stored on your network, Microsoft has built-in basic security capabilities, as well. If data is highly sensitive, then organizations can add to the basic security measures by building split database applications. The benefits of split applications will be discussed later. This section focuses on the basic security measures you can used with any .accdb Access application.

1. Store your MS Access Database in secure folders, limited to qualified users. Using integrated windows login authentication, to limit which users have access to files all over your network, is currently the industry paradigm. This approach applies to all your MS Access files, as well.
2. Distribute runtime versions to your end users and install full versions of Access only on Application developer or administrator machines. This can help contain costs, as well.
    a. Runtime versions limit the proliferation of "data islands" where IT has no knowledge of, or control over, sensitive data
        i. (As a side note, data islands can occur with Excel and other products, but IT does not have the option of running Excel runtime – for example – on user machines.)
    b. Runtime versions also provide a layer of protection to source code, the navigation pane, tables and design mode of forms and reports.
3. Encrypt your database by using a database password
4. Use the Trust Center Settings. Specifically, trust center settings allow an Access application administrator to limit the file path an Access application can be used from. Actually, all Microsoft Office products have the ability to set trusted locations.

Microsoft Access Security with Split Databases

There are many reasons to use a split database model in your organization. In short, when you split an Access database, you're moving all Access tables and data to a more robust Server side database. Then you link the Server tables back to the MS Access frontend file.

Organizations use the split database model all the time. An Access application can evolve. In the beginning data storage may reside in native Access tables. But, over time, the application can evolve and grow in size, complexity and number of users. At that point, it is often wise to move Access data to a more robust and secure backend server database. The most common server database, used as a backend to Access applications, is Microsoft's SQL Server database. This Microsoft Knowledge Base article on upsizing Access Data is well worth your read. From the article:

> **Benefits of upsizing a database to SQL Server**
>
> ... Improved security using a trusted connection, SQL Server can integrate with Windows system security to provide a single integrated access to the network and the database, employing the best of both security systems. This makes it much easier to administer complex security schemes.

Specifically, server level databases make it possible to use Active Directory Integrated Windows Logins and Security Groups to control access to database tables. By incorporating the stronger server level security, it is possible to protect your Access applications in ways you can't when the data resides in native tables. Active Directory security can be used to:

1. Determine which user is logged into the database
2. Create roles to designate permissions for logged in users. Permissions can restrict user privileges, at table level.
3. In addition – by using Active Directory - ODBC Data Connectors are more secure, because saved login strings with user names and passwords, go away. With Active Directory controls at SQL level, all Access requires is the use of Windows NT authentication – SQL will do the rest.

Beyond using Active Directory Security, there are other ways that server databases can control access to data. SQL Views can be used to limit which datasets a user sees. For instance users may only need to view customer records for their district. In a situation, such as this, it is possible to write a query at SQL level, which limits the record-set to a specified district. These queries are called SQL Views. Once the SQL View is written and stored it can be linked back to an Access frontend file. This is a subtle way to limit which records a user can view, but it is effective. Where Active Directory settings can control user privileges (at table level), SQL views can filter the data a user is allowed to view &/or edit down to a specific subset of records (such as all customers in one district).

The linked Microsoft article focuses on upsizing to SQL server. But, Microsoft Access can be used as a frontend to the following databases, as well. These databases are commonly used in large organizations and they are all capable of utilizing Windows Active Directory Security, and serving as a backend to MS Access applications:

1. SQL Server
   a. Evolving Microsoft Access Applications to Microsoft SQL Server
   b. How to Link a Microsoft Access Database to a Microsoft SQL Server Database?
   c. Connecting to SQL Server Using Windows Authentication
2. SQL Azure
   a. Connecting on-premises Active Directory to Azure AD
   b. Access 2010 and SQL Azure
   c. Microsoft Access and Cloud Computing with SQL Azure Databases
3. Oracle
   a. Using Oracle Database with Microsoft Active Directory
   b. Authenticating Database Users with Windows
   c. Creating an Oracle connection to a Microsoft Access Application
4. Informix
   a. Single Sign On with Informix Dynamic Server Using Windows AD

Using Active Directory security groups to control who can read &/or write to specific tables, at a database level, adds a server level of Windows Authentication. A second level of windows authentication controls who has rights to the folders Access files are stored in. Server level windows authentication adds a layer of protection many other files don't receive. This is a very important consideration. Weigh, for instance, all the work involved in "going paperless". Organizations spend millions of dollars scanning sensitive documents into computer systems. These .pdf documents are stored in folder structures protected with windows authentication. But, they do not have the added layer of protection at a server level. If windows authentication is enough to protect sensitive .pdf "paperless" files, it is enough to protect sensitive data in an Access application, especially when that application is also protected at a server level.

After taking the facts into consideration, common myths and misunderstandings about the security shortcomings of MS Access fall away. Not only is MS Access safe to use, for sensitive, local data, it is also the best choice for your organization's local data.

1. Firstly, Microsoft Access is a top notch RAD tool. Rapid Application Development matters.
   a. It saves your organization time and money. The application and end-users are (both) up and running faster.
   b. In addition, RAD, means revisions and maintenance is faster and more efficient. Again, this saves you time and money.
2. MS Access is a Microsoft product and integrates seamlessly with other Office Suite products.
3. Used in conjunction with SQL Server, MS Access has the following advantages:
   a. It can be used in robust applications with high end-user counts.
   b. It can be used for sensitive data
   c. It can be used in hybrid applications. SQL gives your organization the ability to combine on-site Access applications with web side applications.
4. MS Access is a fantastic tool for data integration. It can link and integrate data from the following types of data sources:
   a. Excel
   b. ODBC data sources (SQL Server, Oracle, MySQL, etc..)
   c. XML files
   d. SharePoint Lists
   e. dBase Files
   f. Outlook Folders
5. MS Access includes native report writing capabilities. This also matters. Many RAD tools allow you to rapidly construct data entry forms, but don't give you the capacity to build affiliated reports and queries, MS Access does.

Security is impacted by which data management tool you use. The longer it takes to develop a solution, the more likely it is that end-users will improvise and find their own solutions. This dynamic can (and often does) lead to data being managed in ways that are vulnerable to mischief. If the application can't be easily revised, end users will also end up trying to "go it alone" and once again the solutions, they design, may be more vulnerable to mischief than professionally designed solutions.

Another security consideration, and reason to use MS Access, is hybrid applications. Web based applications are all the rage these days. But, organizations are increasingly using a hybrid approach to their data management. Decision makers are picking and choosing which data sets need web side access, and keeping the rest of it on premise. This is another layer of protection, and MS Access fits squarely into the hybrid model because it integrates so easily with so many server side databases. Not only that, the speed of application development in MS Access means your organization can reserve the high costs of scripting for only those capabilities needed on web side. Not only can MS Access be used securely, in your organization, because of all the points listed above – it should be your organization's "go to tool" for local data management.