Deploying DINO_G *updated 11/12/20*

1. Introduction

DINO is a split Microsoft Access database with user-level security. DINO has a front-end database containing the forms, queries and the programming and a back-end database containing the data. There is also a separate security file (work group file) 'shortcuts', that are used to open the front-end and back-end databases and a help file.

The principle is that the back-end database is placed on a central server in a location that is accessible to all database users and that each user has a local copy of the front-end saved locally (e.g. C: drive). Each copy of the front-end database is linked to the same back-end database. The security file is best located in the same folder as the back-end database.

Files needed to set up the unsecured and secured front-end/back-end versions:

- DINO_Gambia.chm - compiled help file
- DINO_G_Shared_fe.mdb - unsecured front-end database
- DINO_G_Shared_Sec_fe.mdb - secured front-end database
- DINO_G_Shared_be.mdb - unsecured back-end database
- DINO_G_Shared_Sec_be.mdb - secured back-end database
- DINO_G_Shared_Security.mdw - security (workgroup) file
- Open DINO_G_Shared_Sec - BE - shortcut to open the back-end database
- Open DINO_G_Shared_Sec - FE - shortcut to open the front-end database

Login Details

- See word document file "SecurityFileDetails.docx"

Additional Background Information

There is a simple version of DINO in addition to the split front-end/back-end version. Either can be secured using the security model.

- Simple (DINO_G_Shared.accdb). Just one object holding all forms, queries and the data.
    - Best for single small studies where perhaps just one or two concurrent users is likely.
    - Easy to set up and use.
    - Cannot limit permissions - everyone with a copy can do what they like with it including changing the design of the database. A database password can be set to help prevent users without the password from accessing it.
    - Can be put on a server, but there would be a slight (unnoticeable in practice) decrease in performance and multiple concurrent users increase slightly the risk of database corruption. If not held on a server the user will need to manage backups.
    - Updating the database means the developer has access to any data stored.
- Front-end/Back-end (DINO_G_Shared_fe/be, DINO_G_Shared_Sec_fe/be). Two databases; one holding the forms and queries, another just holding the data.
    - Best where DINO likely to be used for multiple studies, perhaps as a corporate (or group) resource and/or multiple concurrent users expected.
    - Cannot limit permissions - everyone with a copy can do what they like with it including changing the design of the database. A database password can be set to help prevent users without the password from accessing it.

    - Best network performance and resilience against corruption and easily backed up as part of corporate strategy.
    - Easier to update the database by simply providing a new front-end and distributing to users.
    - Usually no need for the developer to have access to the data.
- Pros and cons of using the front-end/back-end security model.
    - Much more complicated to set up. Experience has shown that even with detailed instructions the prospect seems daunting to end users.
    - Each individual user can have different levels of permissions for each object. For example user A, might be able to update foods and run analysis programs but not update coding, user B might only have read permissions to the foods table, not be able to run any (or just some) analysis programs and be able to code diet records.
    - The user name is captured on login which can be used to record who did what (e.g. each coding record is noted with the coder's login name, which could be used to monitor performance).
    - Managing the security (e.g. setting up new users, assigning them to groups etc.) can be an on-going task though not too onerous if you know what you are doing. Not all Access developers are comfortable managing security.
    - The security model is not supported by the latest Access database format (.accdb files). The latest version of Access does however run the old database format (.mdb files).

2. Saving front-end/back-end databases to new location

- Decide upon a suitable network location for the back-end database (e.g. \\YourServer\Studies\DietTools\DINO). It is possible to deploy DINO on a single PC. The disadvantages are that only one person can access the database and that security (i.e. backups etc.) might not be done as well as on a central network server).
- Copy DINO_G_Shared_be.mdb to the back-end folder.

  If setting up the secured database, copy DINO_G_Shared_**Sec**_be.mdb, DINO_G_Shared_Security.mdw and Open DINO_G_Shared_Sec - BE to the back-end folder.

- Decide upon a suitable location for the front-end database. We recommend this is on a local PC (e.g. C:\Work\DINO)
- Copy DINO_G_Shared_fe.mdb and DINO_Gambia.chm to the front-end folder.

  If setting up the secured database, copy DINO_G_Shared_**Sec**_fe.mdb, DINO_Gambia.chm and Open DINO_G_Shared_Sec - FE to the front-end folder.

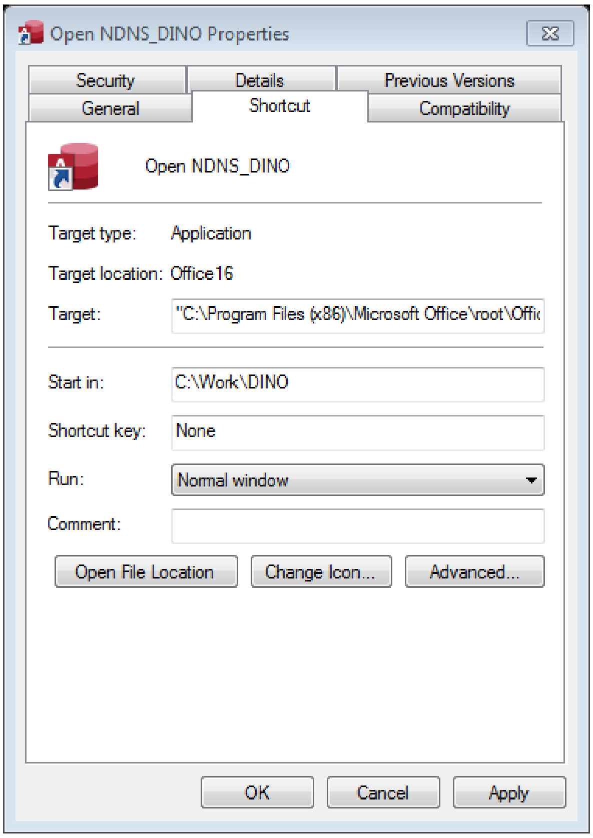
3. Modify the shortcuts for the secured front-end/back-end version

Skip this step if setting up the unsecured FE/BE version.

Please note that paths that include spaces must be enclosed within quotes (e.g. "C:\Program Files (x86)\Microsoft Office\root\Office16\MSACCESS.EXE", but quotes are not needed where there are no spaces (e.g. C:\Work\DINO).

- Establish the full path to your MSAccess.exe program (something like C:\Program Files (x86)\Microsoft Office\ Office16 but will vary by version and setup options)

- Right-click ‘Open DINO_G_Shared_Sec - FE’ in your front-end folder and select ‘Properties’. Select the ‘Shortcut’ tab.



Open NDNS_DINO Properties

Open NDNS_DINO

Target type: Application

Target location: Office16

Target: "C:\Program Files (x86)\Microsoft Office\root\Offic

Start in: C:\Work\DINO

Shortcut key: None

Run: Normal window

Comment:

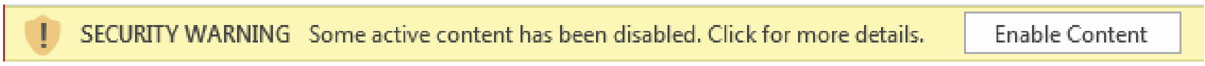
- The ‘Target;’ parameter is made up of three parts; location of the program to run (MSACCESS.EXE), the database to open, and the location of the security file. Something like this: "C:\Program Files (x86)\Microsoft Office\root\Office16\MSACCESS.EXE" "C:\Work\DINO\DINO_G_Shared_Sec_fe.mdb" /wrkgrp "\\YourServer\Studies\DietTools\DINO\DINO_G_Shared_Security.mdw”.
    - Blue part: Replace the path to MSACCESS.exe with the path and file name of your executable copy of Access (MSACCESS.EXE).
    - Red part: Replace the path to the front-end database with the path you have chosen for your front-end database (DINO_G_Shared_Sec_fe.mdb).
    - Green part: Replace the path to the security file with the path you have chosen for your security file, which is probably the same as your back-end database. This could be a mapped drive (e.g. S:\DietTools\DINO)
    - /wrkgrp is required (it ‘tells’ the system which security file to use)
- The ‘Start in:’ parameter should be set to the same folder as your front-end database.
- Click OK.
- Right-click ‘Open DINO_G_Shared_Sec - BE, which should be in the back-end folder, and select ‘Properties’. Select the ‘Shortcut’ tab.
- Follow the above instructions except that the red part of the target parameter should point to the back-end database and the start in parameter should be the folder containing the back-end database.

4. ‘Point’ the front-end database to the back-end database.

- Unsecured version: Hold shift and open the file DINO_G_Shared.mdb.

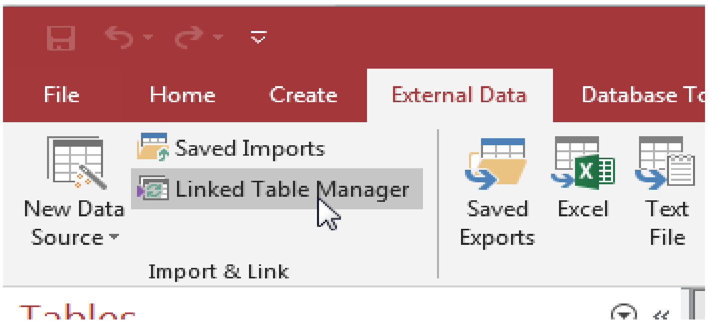
  Secured version: Open the front-end database using the shortcut. Enter your user name and password and then hold down the shift key at the point you press enter or click OK.

  This will enable you to modify set up or design of the front-end database as it allows the database navigation window and full commands to be displayed instead of the normal DINO menu. The first time you open the database you may receive a security warning:

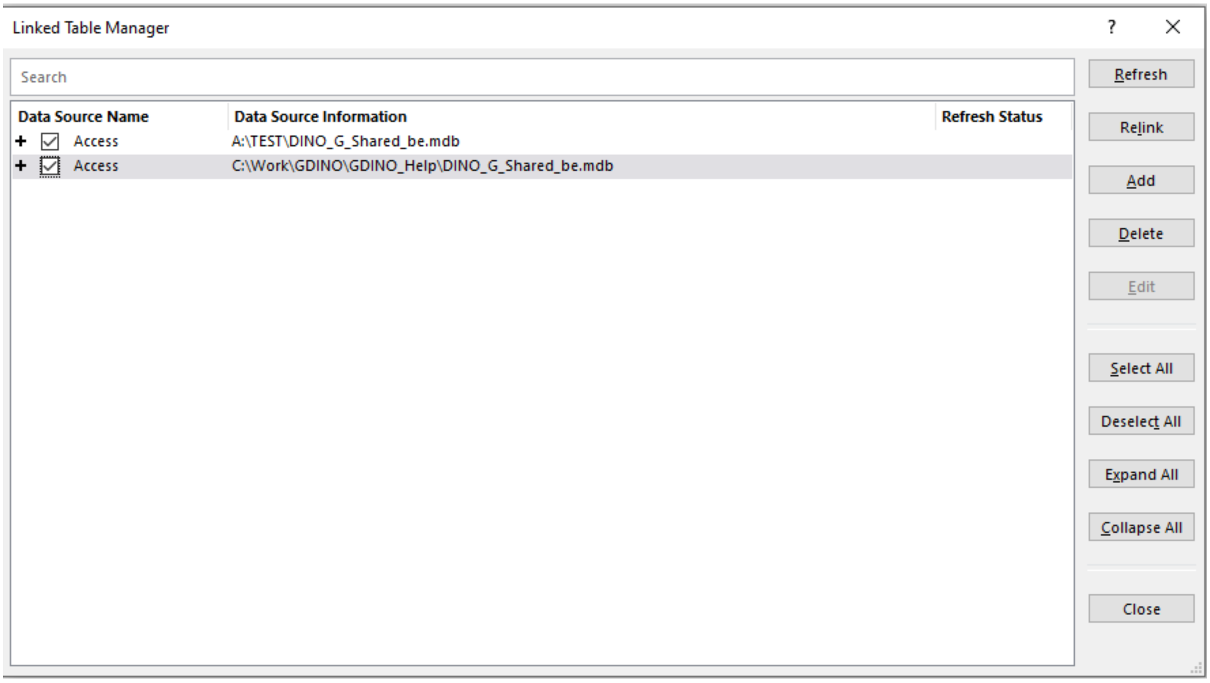


SECURITY WARNING Some active content has been disabled. Click for more details.

- Click Enable Content. Still hold shift when you pass this stage.
- Select Linked Table Manager from the ‘External Data’ tab



- The Linked Table Manager will open.
- Check the box under Data Source Name and click “Relink”.

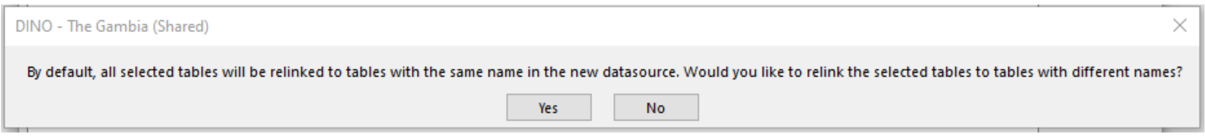


Linked Table Manager

Search

Data Source Name	Data Source Information	Refresh Status
+ ☑ Access	A:\TEST\DINO_G_Shared_be.mdb	
+ ☑ Access	C:\Work\GDINO\GDINO_Help\DINO_G_Shared_be.mdb	

- A box will appear asking you to select location to save the tables. Navigate to the back-end database and open it.
- The following will be displayed:



By default, all selected tables will be relinked to tables with the same name in the new datasource. Would you like to relink the selected tables to tables with different names?

- Click No (do not rename the tables).
- An alert saying the database “could not find the object ‘tblQuestions’” might appear. Click OK.
- Confirm databases linked by closing the front-end database and opening it using the shortcut without shift. You will be asked to log in (see SecurityFileDetails.docx), then the DINO menu should be displayed.

5. Set Up security

- See the file SecurityFileDetails.docx for complete log-in information.
- You have one administrator login. Use this login to create as many new users as you require and assign them to the appropriate security groups. There are five main groups of users:

  - Analysts - Gives permissions to run analysis reports and extracts
  - Coders - Gives permissions to code diet intake
  - SuperCoders - Gives additional coding permissions, such as able to set up studies etc. Must still be a member of the Coders group.
  - Foods - Gives permissions to administer foods
  - Subjects - Gives permissions to establish subjects

- Unless you particularly need to limit what your users can do, suggest you add them to all of the above groups.
- Here is a link to a website that can tell you everything you need to know about MS Access User-Level security http://www.databasedev.co.uk/permissions.html
- Provide all users with a **copy of the front-end database folder** (e.g. C:\Work\DINO) containing the front-end database (DINO_G_Shared_fe.mdb), the shortcut (Open DINO_G_Shared_Sec - FE) and the help file (DINO_Gambia.chm).
- Provide all users with User names and, if defined (Recommended), passwords. Passwords can be set or changed via the DINO menu system.