

Deploying DINO v1.1 *updated 07/06/2021*

1. Introduction

Written in Microsoft Access, DINO (Diet In Nutrients Out) is an all-in-one food composition and dietary intake system. It was developed by the Human Nutrition Research Unit of the Medical Research Council, for in-house and other third-party studies in 2004. It was subsequently modified to utilise the National Diet and Nutrition Survey (NDNS) nutrient databank and to record intake for the first 11 years of the NDNS rolling programme. The database is supplied at the point in time at which it ceased to be used for the recording of dietary intake by the NDNS team. The help file had not been updated for some time.

The database can be viewed and/or modified by anyone using Microsoft Access. It would depend on the user's level of knowledge of MS Access what changes could safely be made to DINO. An experienced developer could change anything and everything. All models are provided to open showing the DINO menu for using the database. To open DINO for design purposes you must hold down the 'Shift' key on your keyboard when opening the database. Help for Microsoft Access is well supported on the Internet. Google can be your friend!

DINO is provided in three different models each of which have benefits and drawbacks. Here is a summary of the models provided in the download:

- **Simple. Just one database holding all forms, queries and the data.**
 - For use as a tool for single small studies where perhaps just one or two concurrent users is likely.
 - Very 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.
 - Multiple concurrent users slightly increase the risk of database corruption. If not held on a server the user will need to manage backups.
- **Front-end/Back-end. 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.
 - Quite easy to set up.
 - 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 limit access.
 - Best network performance and resilience against corruption and easily backed up as part of corporate strategy.

- **Front-end/Back-end using user level security. As per the Front-end/Back-end model with an added security file.**
 - 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 be able to code diet records, have only read permissions to the foods table, and not be able to run any (or just some) analysis programs.
 - 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).
 - More complicated to set up.
 - 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 user-level security.

2. Deployment Instructions

Decide which model you are going to use. Deploying the databases can be undertaken by competent Windows users by following the steps below. No special IT permissions are required.

2.1 Simple Model:

Choose a location for your database. It could be a local C: drive folder or a location on the network depending on your needs and requirements. It should be treated as any other file for security and backups et cetera. Double-click to open. Put the help file (DINO_S.chm) in a folder called C:\Work\DINO to allow the help file to open when press F1.

2.2 Front-end/Back-end Model:

Ideally the back-end database is placed on a central server in a location that is accessible to all database users (e.g. \\YourServer\Studies\DietTools\DINO) and that each user has a local copy of the front-end and help file saved locally (recommend C:\Work\DINO to allow the help file (DINO_S.chm) to open when press F1). Each copy of the front-end database is linked to the same back-end database. Double-click the front-end database to open.

The front-end database will then need to be linked to the back-end database. Follow the instructions in the step [2.3.3 'Point' the front-end database to the back-end database](#) to complete the set-up process.

2.3 Front-end/Back-end using user level security

Ideally 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 and help file 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. Shortcuts can be saved, once modified, to any suitable location.

Files needed:

- DINO_S.chm – compiled help file
- DINO_S.mdb – front-end database
- DINO_S_be.mdb – back-end database
- DINO_S_Secured.mdw – security (workgroup) file
- Open DINO S BE – shortcut to open the back-end database
- Open DINO S – shortcut to open the front-end database

Login Details

- User Name: Administrator
- Password: \$haredAdmin

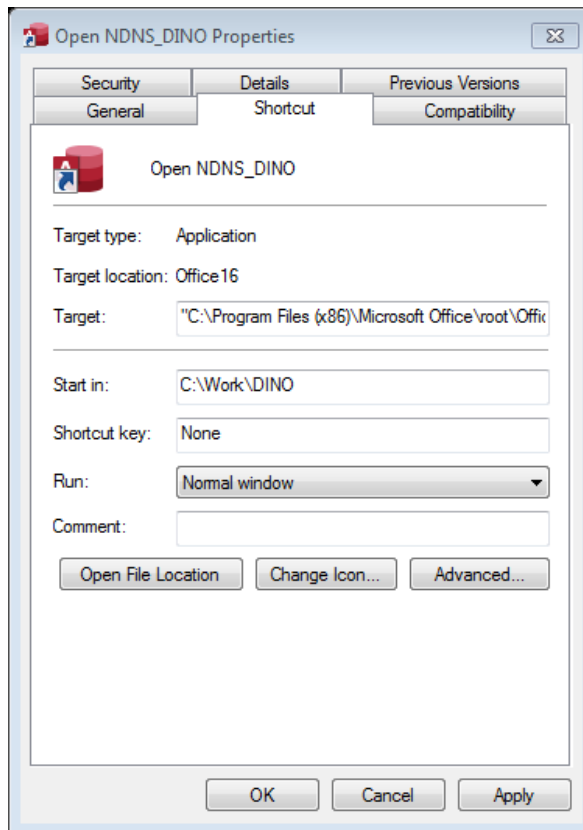
2.3.1 Copying Files

- Decide upon a suitable location for the back-end database. Ideally the back-end database is placed on a central server in a location that is accessible to all database users (e.g. \\YourServer\Studies\DietTools\DINO) and that each user has a local copy of the front-end saved locally (e.g. C:\Work\DINO). 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. 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_S_be.mdb, DINO_S_Secured.mdw and Open DINO S BE to the back-end folder.
- Decide upon a suitable location for the front-end database. Ideally this is on a local PC (e.g. C:\Work\DINO)
- Copy DINO_S.mdb and Open DINO S to the front-end folder.
- Copy DINO_S.chm in C:\Work\DINO (to allow the help file to open when press F1).

2.3.2 Modify the shortcuts

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 S' in your front-end folder and select 'Properties'. Select the 'Shortcut' tab.

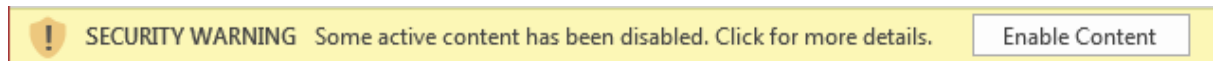


- The 'Target;' parameter is made up of three parts; location of the program to run (MSACCESS.EXE), the database to open, and the location of the security file. Something like this: "C:\Program Files (x86)\Microsoft Office\root\Office16\MSACCESS.EXE" "C:\Work\DINO\DINO_S.mdb" /wrkgrp "\\YourServer\Studies\DietTools\DINO\DINO_S_Secured.mdw".
- 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_S.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 S 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.

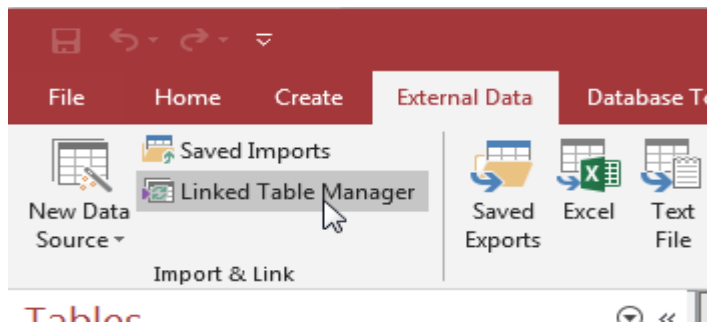
2.3.3 'Point' the front-end database to the back-end database.

- 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

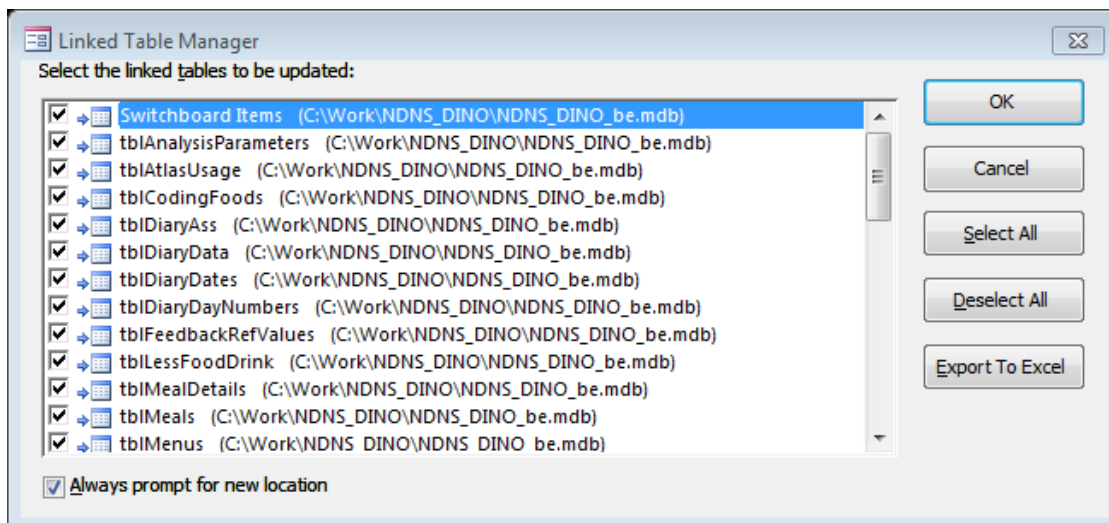
commands to be displayed instead of the normal DINO menu. The first time you open the database you may receive a security warning:



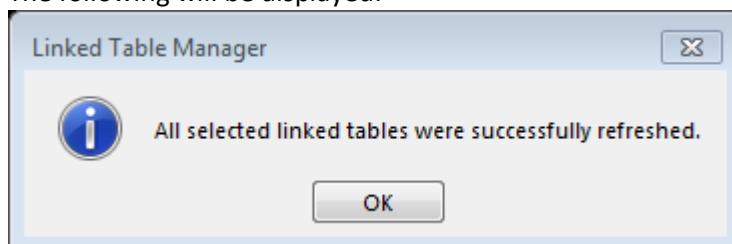
- Click Enable Content. (Still hold shift when you pass this stage if you want to modify the database).
- Select Linked Table Manager from the 'External Data' tab



- The Linked Table Manager will open.
- Check Always prompt for new location, click 'Select All' as shown below



- Click OK
- 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:



- Click OK.

- Confirm databases linked by closing the front-end database and opening it using the shortcut without shift. The DINO menu should be displayed.

2.3.4 Set Up security

- You have one administrator login (Login name: Administrator Password: \$shared_Admin).
- 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_S.mdb), the shortcut (Open DINO S) and the help file (DINO_S.chm).
- Provide all users with User names and, if defined (Recommended), passwords. Passwords can be set or changed via the DINO menu system.