

HOW TO CREATE NEW ECN USERS

The ECN application has a **built in user administration system** that manages each user's rights to edit records and their role as member of a group with special privileges.

The **User Administration form** is accessible only against the password allocated for a generic user id **Admin**. The Admin default password is **adminpsw** and this password should be replaced after getting familiar with the application.

IMPORTANT: do not remove this user id Admin from application.

Usually the User Administration task is performed by so called **ECN Administrators**.

The application is delivered with two default user ids for this role, **ecnadmin1** and **ecnadmin2** (passwords: **admin1psw**, **admin2psw**).

IMPORTANT: ecnadmin1 and ecnadmin2 should be replaced later with real user ids in both ECN's built-in security system (User Administration form) and MSAccess security system (ECN dedicated MDW file ECN2K.mdw).

Starting with version 6.06 of ECN application both regular users and administrators are created in workgroup security file via ECN User Administration form.

A user id checked as ECN administrator will be added (or deleted if unchecked) to **Admins Group** in **ECN2K.mdw** workgroup security file.

Regular users are created as part of **Users Group** in the same workgroup file.

The user rights against objects in this application are set per group and not individually.

The MDW file delivered has set the tables and queries **Ownership** to Admins Group and therefore users registered in the Admins Group can create new ECN users.

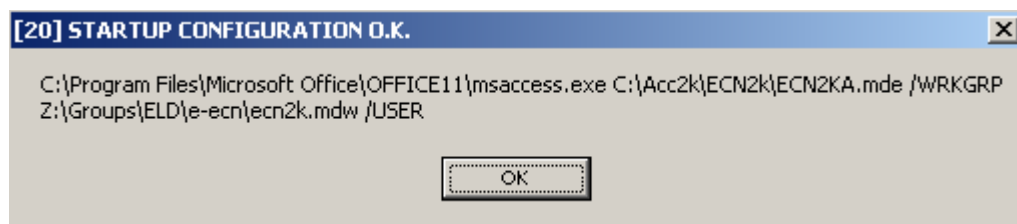
The default MDW file delivered with the application contains sample users to cover each required type.

HOW TO SOLVE A WORKGROUP SECURITY FILE ISSUE

The **ECN shortcut** on your desktop is pointing to an executable file that will attempt to identify the existent environment in order to create the proper shortcut. Among other things this executable verifies the existence of **ecn2k.mdw**, which is the workgroup security file for the application. When you create users from your Admin installation you have to make sure that you're working on the **ecn2k.mdw** file located on the shared network drive which in your case is **Z:\Groups\ELD\e-ecn**.

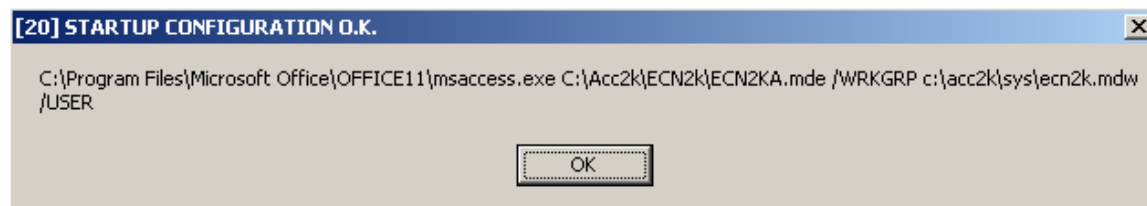
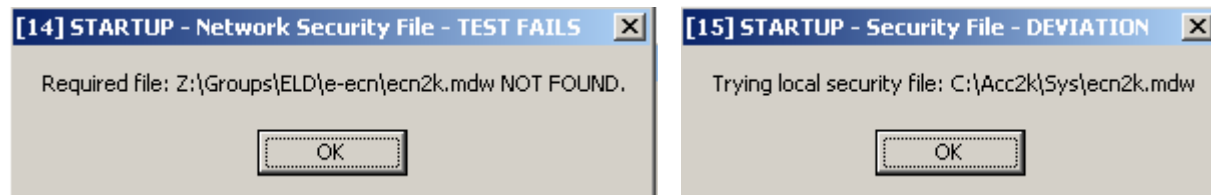
If you don't see users created from your admin workstation when running ECN from another user's workstation it means that you are not looking at the same **ecn2k.mdw** workgroup security file.

To verify what workgroup security file will be used to open the ECN application when running from a particular workstation you can run the **C:\ACC2K\ECN\ecn_ZETEC_test_startup.exe** test file.



At the end of the test the **shortcut** used to open the application in that workstation will be shown in a message box and ideally is to see as workgroup security **Z:\Groups\ELD\e-ecn\ecn2k.mdw**.

If this is not the case and you see **C:\Acc2k\Sys\ecn2k.mdw**, then you should replace **ecn2k.mdw** on user's local folder with the one on the shared **Z:\Groups\ELD\e-ecn** folder.



Having the same security file on the local as the one on the shared network drive is a temporary fix to allow user's access to the application.

IMPORTANT: installing the Admin setup package might delete **Z:\Groups\ELD\e-ecn\ecn2k.mdw**. Always make a copy of the workgroup security file before running the admin setup; otherwise there is a chance to have wiped out all the work done on user accounts.

IMPORTANT: if the **windows/network user name** in a workstation does not have allocated **full rights** in **Z:\Groups\ELD\e-ecn** shared folder and is the first user that opens the ECN application he won't be able to create the **ldb file**, which indicates that the workgroup security file is opened.

Select from ECN toolbar **Info/Access Info** to open the form below.

Access properties and LDB Viewer

Logged in as	user1	Logged on Users	ROTINSOFT1 -- tuser	References	Name	Broken	Repair	Major:	4
OLE/DDE Timeout	120 seconds				VBA	No		Minor:	0
DDE Requests are	not ignored				Access	No		Built In	<input checked="" type="checkbox"/>
Record Locking is	No Locks				DAO	No		VBA	<input type="checkbox"/>
Open Mode	Shared				ADODB	No		Is Broken	<input type="checkbox"/>
Jet Engine Version	0.3.0.51	Name:	VBA	GUID:	{000204EF-0000-0000-C000-000000000046}				
Access	Retail	Full Path:	C:\Program Files\Common Files\Microsoft Shared\VBA\VBA6\WBE6.DLL						
Access Version	11.0	Access Directory	C:\Program Files\Microsoft Office\OFFICE11\						
Access Lic Key		Access INI File	msacc30.ini						
Access Workgroup	Z:\Groups\ELD\e-ecn\ecn2k.mdw	App revision date	20040711						
Default Directory	Z:\Groups\ELD\e-ecn\	O.S.	Win2003						
Open File Path	C:\Acc2k\ECN2k\ECN2KA.mde	System Directory	C:\WINDOWS\system32						
Windows Directory	C:\WINDOWS	DBEngine properties:							
		App Visible property = True							
		Version: 3.6							
		LoginTimeout: 20							
Database:	Z:\Groups\ELD\e-ecn\ECN2kdat.mdb	Retrieve Info							
<input type="checkbox"/> Use Jet 4.0's UserRoster									
Display Option:									
<input checked="" type="radio"/> All users logged in since file was created					<input type="radio"/> Users that left the database in a suspect state				
<input type="radio"/> Users who are currently logged in					<input type="radio"/> Count of Users				
Number Of Users:	0	Can't create LDB filename.							
<p>If Can't create LDB file name it means that the user logged on the workstation running the ECN application does not have Full Rights in Z:\Groups\ELD\e-ecn\ folder and most likely that it has Read Only. Ask the Network administrator to allow Full Rights for this user.</p>									
Name : Admin									
Account Info: T									
The logon script executed.									
This is a default account type that represents a typical user.									

Important is to see as Access Workgroup **Z:\Groups\ELD\e-ecn\ecn2k.mdw** and nothing instead of **can't create LDB file name**. If possible allocate as ECN user id the Windows user id.

Having full rights allocated for all ECN users in **Z:\Groups\ELD\e-ecn** folder won't endanger the back-end files. The critical files are protected against accidental deletion via replication manager, which keeps them opened all the time in background. One other approach, if not using the replication manager, is to run from admin workstation a utility that opens in read-only mode the back-end files. All users will be able to read & write the files but it will be impossible to delete them. This utility file is a free add-on and I will make-it available with next revision of admin setup package.