PSQL 8.5 Security Release and Elliott NTFS Setting

PSQL 8.5 Security Release

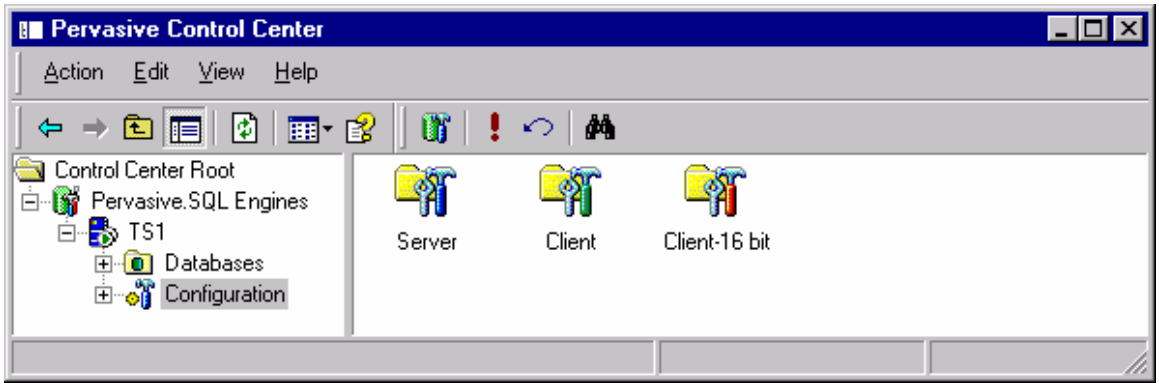
PSQL 8.5 introduces the ability for users to use the Btrieve database without the need for granting OS level file access rights.

In the past, in order for users to use the Elliott database, you had to assign O/S level file access rights for Elliott and its subdirectories. This is a potential problem since users, intentionally or unintentionally, may use Windows Explorer and damage the Elliott directory and data files.

PSQL 8.5 resolves this problem for Elliott users. However, there are certain O/S level settings that need to be performed to make this functional. This document only applies to Microsoft Windows NT, 2000 or 2003 Servers only. For other O/S environments like Netware, users should be able to find a corresponding solution by reading this document. For users who purchased PSQL 8.x from Netcellent, PSQL 8.5 is a free upgrade by simply making a request to Netcellent.

Enabling PSQL 8.5 Security Feature

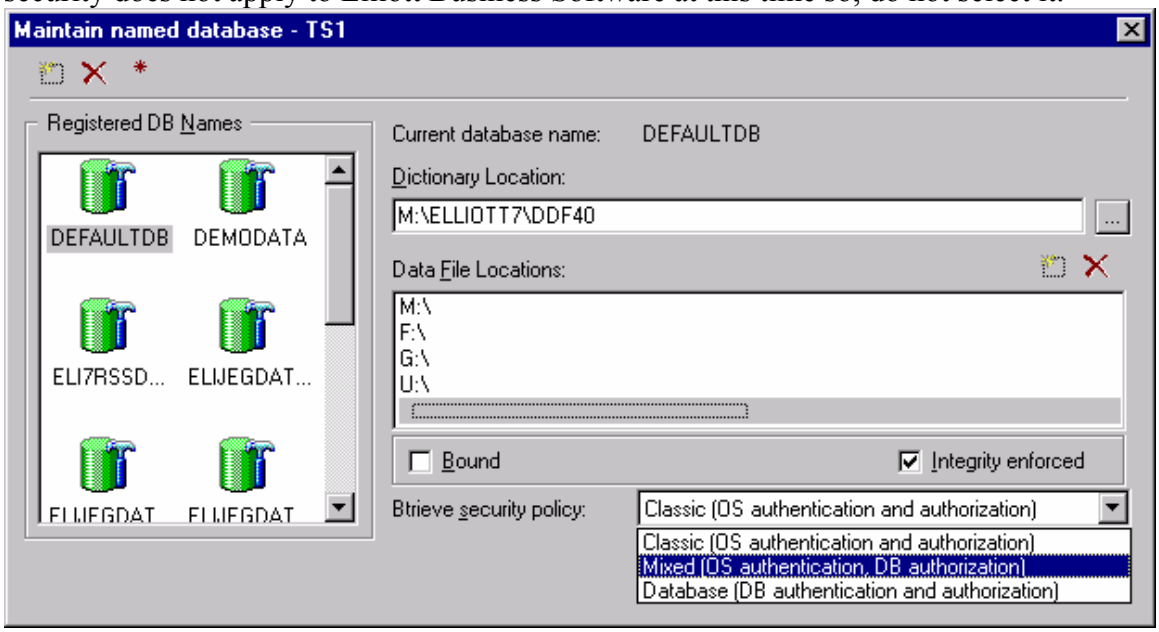
To enable the PSQL 8.5 Security Feature, bring up the Pervasive Control Center. Expand the Pervasive.SQL Engines node and the server node and right click on the "Configuration" node. Click on "Maintain Named Database."



In the Maintain Named Database window, highlight the DEFAULTDB database name. Enter the directory where Elliott DDF files reside in the "Dictionary Location" field.

Enter all drive letters that may contain Btrieve or PSQL data in "Data File Location." It is very important that you use the lowest common denominator for Data File Location. This will insure that all applications that use Btrieve data will have access to their database if you intend to turn on the PSQL 8.5 security feature. Otherwise, the application that uses Btrieve data that is not covered by the "Data File Locations" will receive a Btrieve error 94.

In the Btrieve security policy box, choose “Mixed” to turn on the PSQL 8.5 security feature. “Classic” means the traditional OS file level security. This disables the PSQL 8.5 security feature and returns PSQL back to PSQL 2000 security mode. “Database” security does not apply to Elliott Business Software at this time so, do not select it.



Click OK to save the setting. The security feature will not take effect until you stop and start the services of both PSQL 8.5 relational and transactional engine. Alternatively, you can reboot the server.

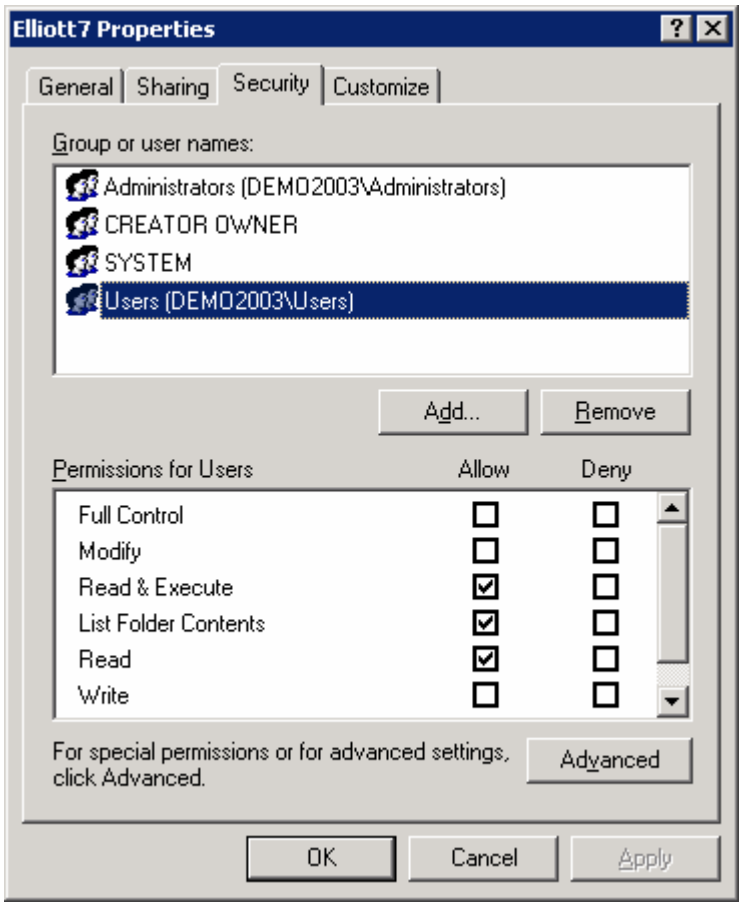
After this change, your Elliott system should continue to function. If you receive an error 94, then check the drive letter you entered in the “Data File Location” box of the “Maintain named database” window through the PCC configuration. Make sure the drive letter and path you entered cover the Elliott application’s data.

Assigning Rights to the Elliott & Sub Directory

In order for users to run the Elliott application, the user must be able to read Elliott data in both the Elliott root and Programs subdirectory. The read permission for all other subdirectories is also necessary, except in DATA and other corresponding DATA subdirectories. IMAGES, FIMAGES, SPEC, CONTRACT and SOUND are related to the Elliott link function and the system administrator needs to decide whether to let users update these directories or not. The LOG directory is related to logging API and File I-O functions. The MACRO directory is related to the Elliott MACRO function. System Administrators may use their own discretion to decide whether to grant update privileges to these directories or not.

System Administrators must assign the following NTFS rights to Elliott and Elliott subdirectories in order for Elliott to function:

- **Read & Execute**
- **List Folder Contents**
- **Read**



This is typically done through assigning rights to the "Users", "Domain Users" or "Everyone" group. Since these rights are most likely assigned by the O/S by default already, you probably won't need to do anything. To verify if these securities had been

assigned, bring up Windows explorer and right click on ELLIOTT7 folder and choose "Properties". Then choose the "Security" tab. If the right is granted for all users, then nothing needs to be done. If not, please add the group and security that will cover all users that use the Elliott application. By default, the rights you assigned at ELLIOTT7 directory level will be inherited by the subdirectories and files.

In addition to "Users", you need to make sure the following three security groups are added for ELLIOTT7 directory. Depending on your operation system, these three security groups may be added already:

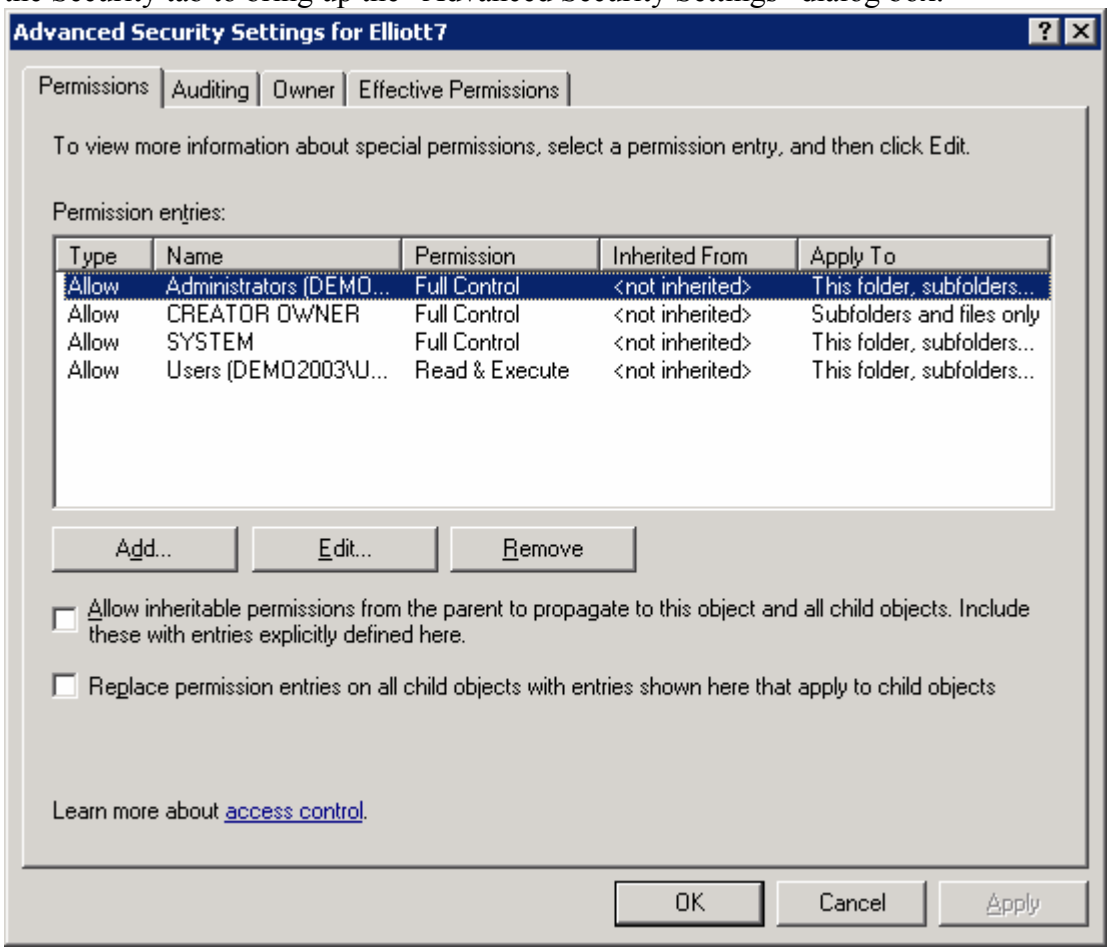
- **SYSTEM**: PSQL 8.5 engine on the server by default is running under system account. It is necessary that PSQL 8.5 engine has sufficient right to access the files in ELLIOTT7 directory. If you do not see SYSTEM, then add it and give full control to SYSTEM.
- **Administrators (Local Security Group)**: It is also possible PSQL 8.5 engine on the server is running as the local Administrators. If you do not see Local Administrators, then add it and give full control to Local Administrators.
- **CREATOR OWNER**: If you do not see CREATOR OWNER, then add it and give full control to CREATOR OWNER. With CREATOR OWNER added, then when a file is created, the owner shall have the full access right to that file. This is necessary to support Elliott Spooled Reports where the user who creates the spooled reports should be able to view/print the reports, as well as delete the spooled reports.

Assigning Special Rights to the Elliott Root Directory

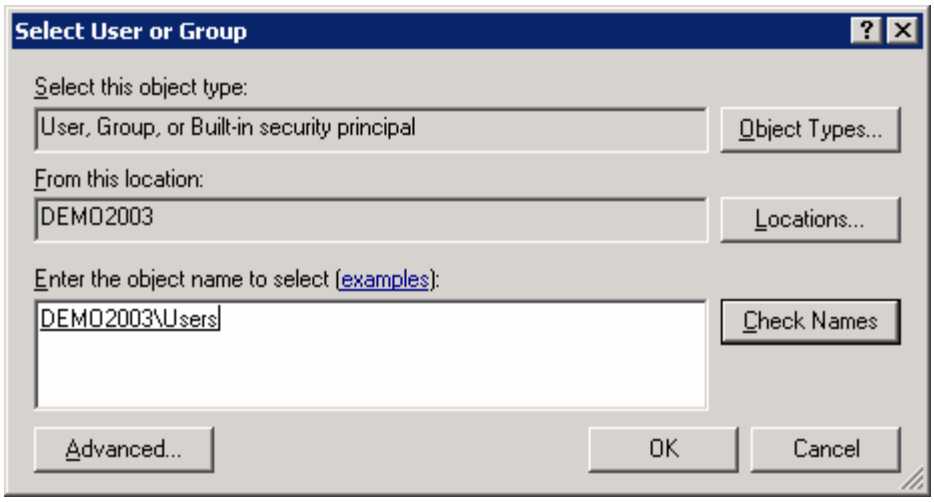
In addition to "Read & Execute", "List Folder Contents" and "Read" privilege, you need assign additional rights to the Elliott root directory, ***but not inherited by the subdirectories***. This includes:

- Create File and Write Data

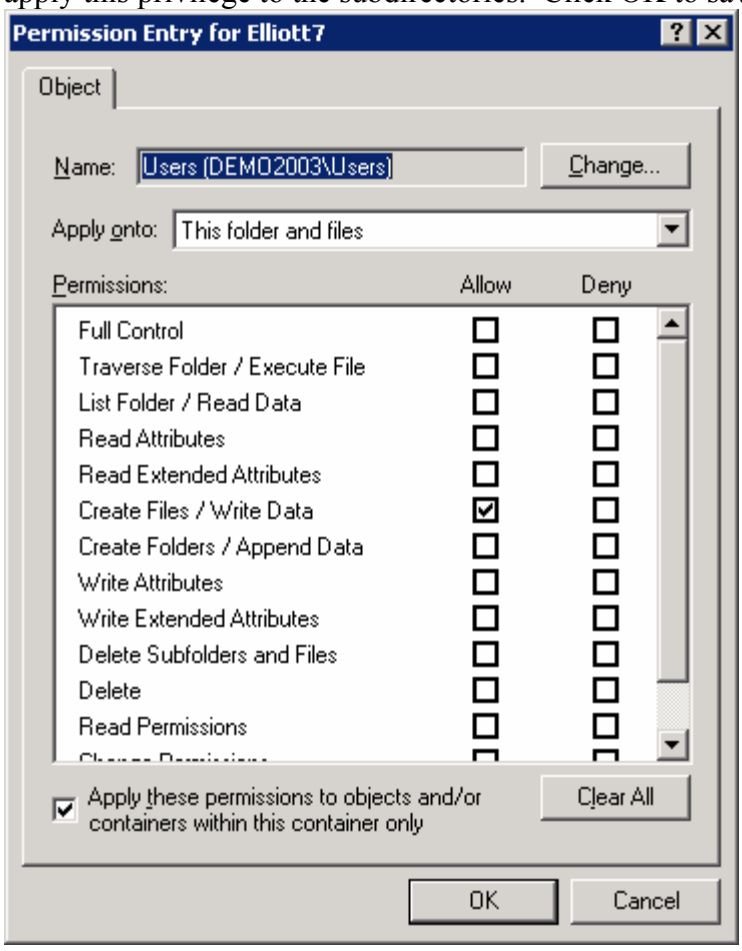
This is necessary for Elliott to create the USER#999.DAT file as a user count control mechanism. Failure to create the USER#999.DAT file will result in Elliott giving the error message indicating it has run out of user licenses. Click the "Advanced" button in the Security tab to bring up the "Advanced Security Settings" dialog box.



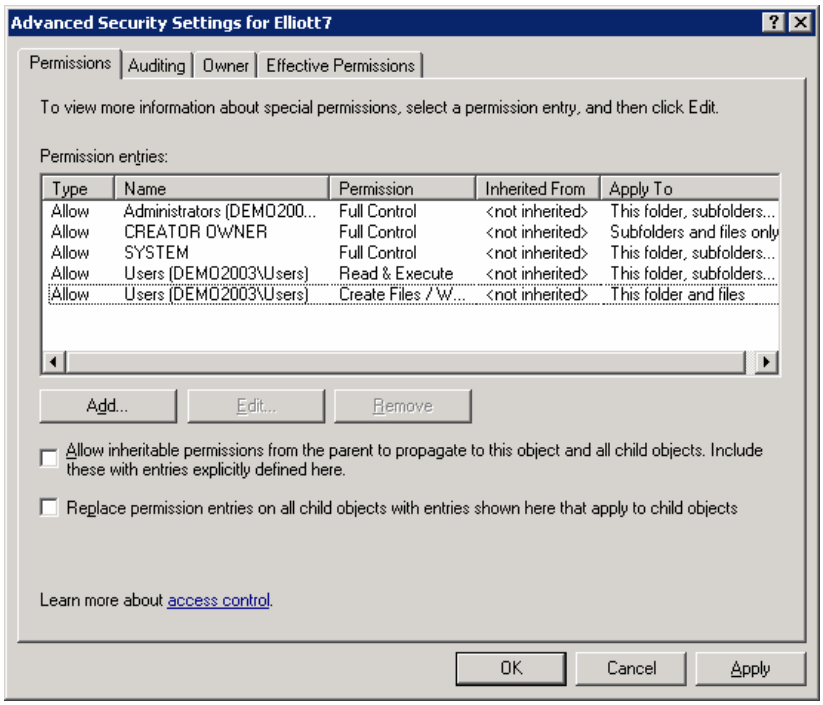
Click "Add" for additional rights for the "Users" group. Notice we do not use "Edit" for the existing "Users" entry because we do not wish the rights we added here to be inherited by the subdirectories. Add the "Users" group then click "OK".



In the Permission Entry dialog, check the "Create Files/Write Data" privilege. Make sure the "Apply onto" box uses "**This folder and files**" and check "**Apply these permissions to objects and/or containers within this container only**" because we do not want to apply this privilege to the subdirectories. Click OK to save.



Your Advanced Security Settings dialog should now look like the following:

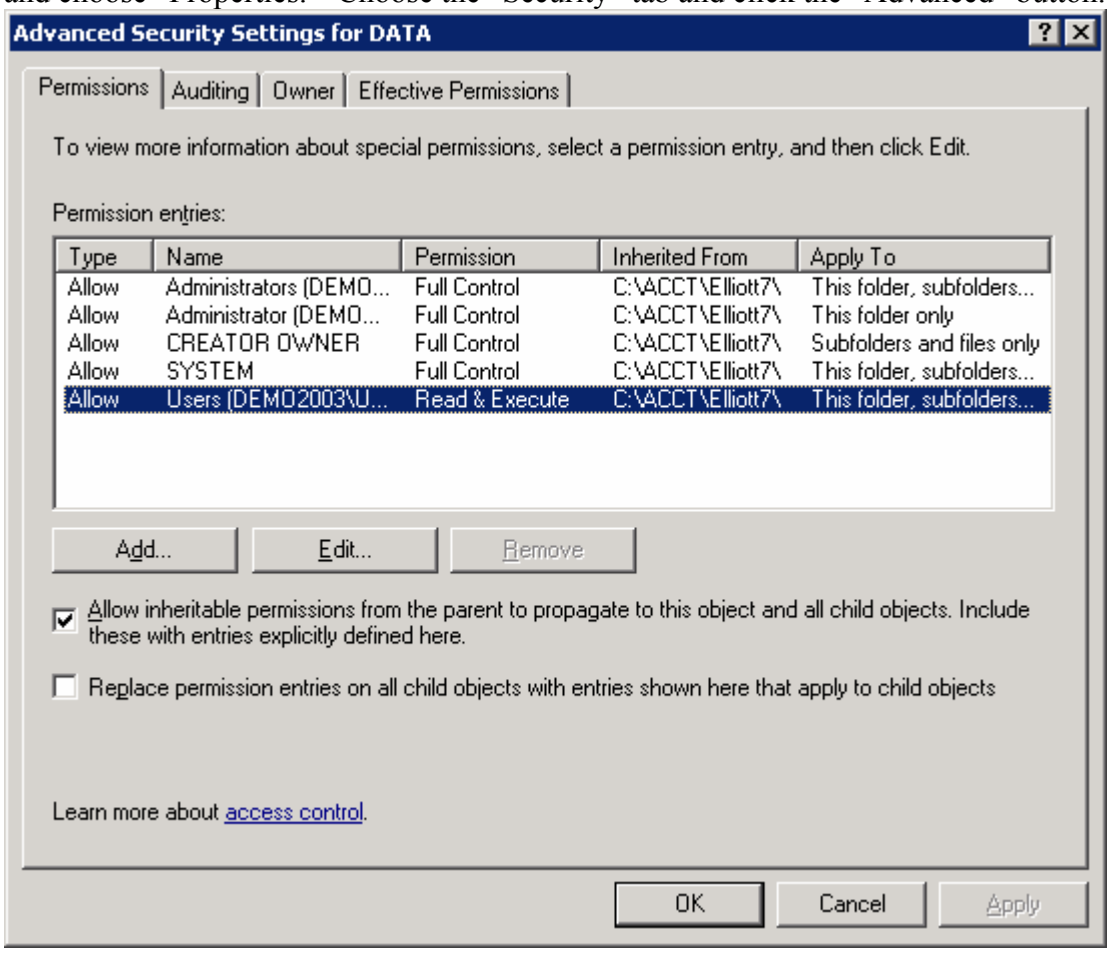

Advanced Security Settings for Elliott7
Permissions
Auditing
Owner
Effective Permissions
To view more information about special permissions, select a permission entry, and then click Edit.
Permission entries:
Type
Name
Permission
Inherited From
Apply To
Allow
Administrators (DEMO200...
Full Control
<not inherited>
This folder, subfolders...
Allow
CREATOR OWNER
Full Control
<not inherited>
Subfolders and files only
Allow
SYSTEM
Full Control
<not inherited>
This folder, subfolders...
Allow
Users (DEMO2003\Users)
Read & Execute
<not inherited>
This folder, subfolders...
Allow
Users (DEMO2003\Users)
Create Files / W...
<not inherited>
This folder and files
Add...
Edit...
Remove
Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.
Replace permission entries on all child objects with entries shown here that apply to child objects
Learn more about access control.
OK
Cancel
Apply

Assigning Rights to the Elliott Data Directory

Elliott data directories require special configuration. On one hand, we should not allow the "Read" privilege in the parent directory to propagate to this directory for security reasons. On the other hand, we need to allow users to create spooled reports in this directory. On top of these issues, there are certain DAT files that are not controlled by the Pervasive PSQL 8.5 engine that we need to allow users to access. The requirements outlined here apply to all DATA directories including TUTORIAL. The TUTORIAL directory is a good testing environment to ensure your security settings are defined correctly.

Remove Read Inheritance And Allow Spooling Reports to Data Dir.

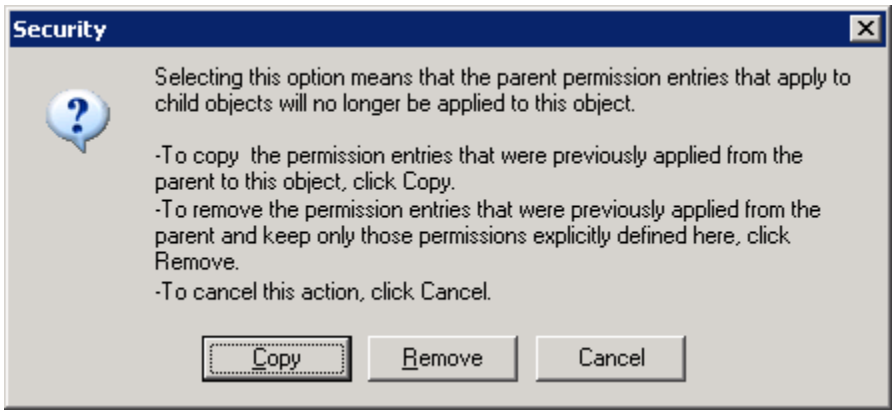
Use Windows Explorer to right click the DATA directory under the ELLIOTT7 directory and choose "Properties." Choose the "Security" tab and click the "Advanced" button.



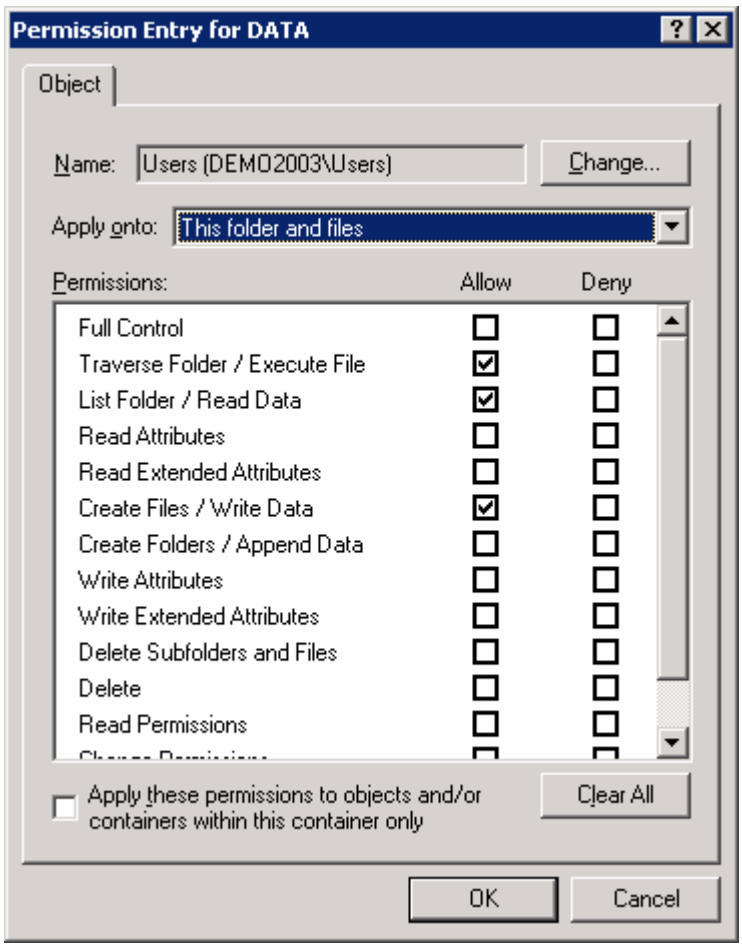
Uncheck the box labeled "Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here." This is necessary in order to remove the users' inheritable rights from the parent directory for "Read" privileges.

On the following message box, if you choose "Remove", then it will remove certain system and administrator level rights that we wish to preserve along with the Users group

rights we wish to get rid off. If you do so, then you'll need to manually add the System and Administrator rights back. It is suggested you choose "Copy" to preserve the rights.



After you uncheck the rights for inheritance from the parent, now you can modify the users' rights to the DATA directory. Highlight the Users group and click "Edit" in the "Advanced Security" Dialog box. The following dialog should appear:



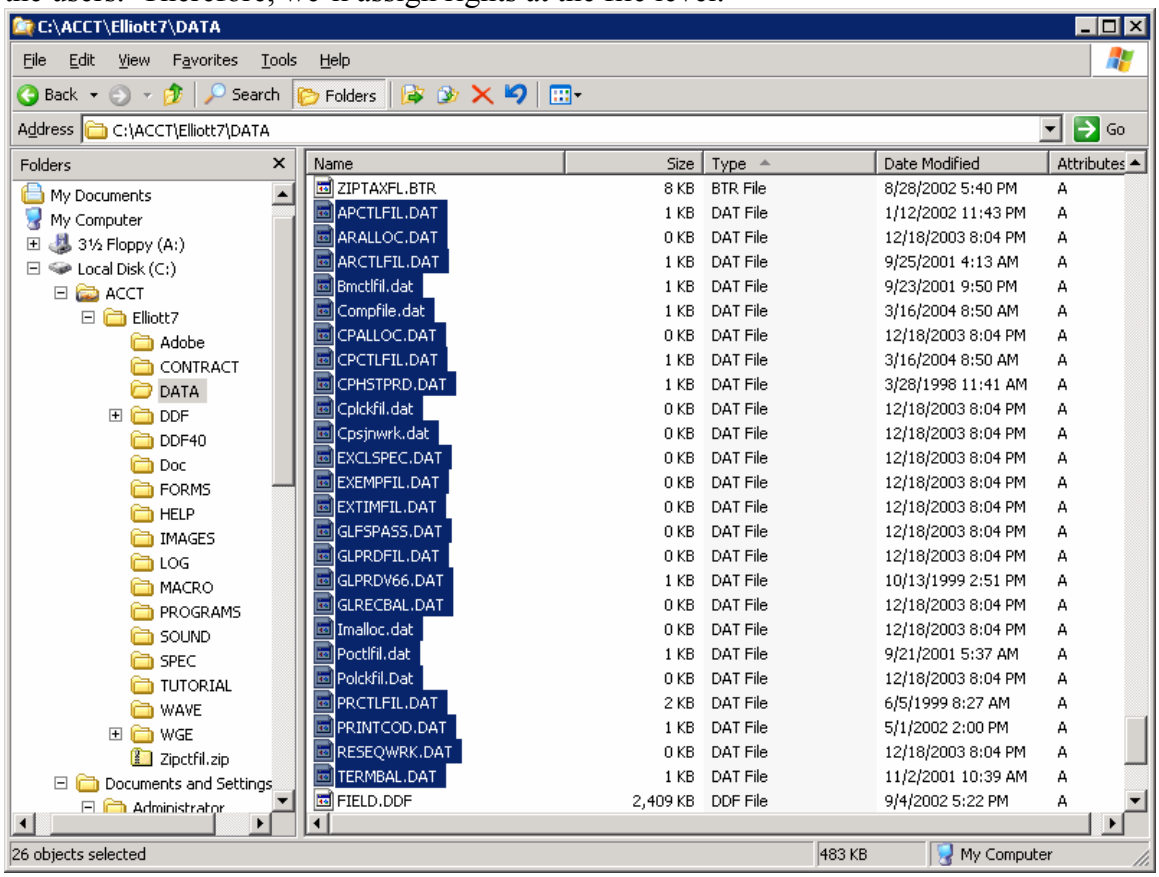
Make sure the Users group has the following rights:

- **Traverse Folder / Execute File**
- **List Folder / Read Data**
- **Create Files / Write Data**

The "Create Files / Write Data" is necessary for users to create spooled reports. We do not need to give "Read" privilege to spooled reports because by default, the users who create the report is the owner and will have full access to that report. The "Traverse Folder/Execute File" & "List Folder / Read Data" is necessary to make Spooled Report Manager to display reports properly.

Give Rights to Read & Update DAT Files in Data Directories

There are certain files in the Elliott data directory that are not Btrieve format. These are typically the setup control files for the module or company file. Unfortunately, you will need to assign rights to these files in order for users to run Elliott correctly. We do not want to assign rights at the directory level because that will give too many privileges to the users. Therefore, we'll assign rights at the file level.



Use Windows Explorer, highlight DATA directory on the right side pane. The left side should display all files under DATA directory. Click on the "Type" column heading so the files will be sorted by their extension. We need to highlight the following files:

- DAT files: These are the control and company setup files
- BMP files: These are the image files for Laser Form printing
- DDF files: These are the Pervasive Database definition files.

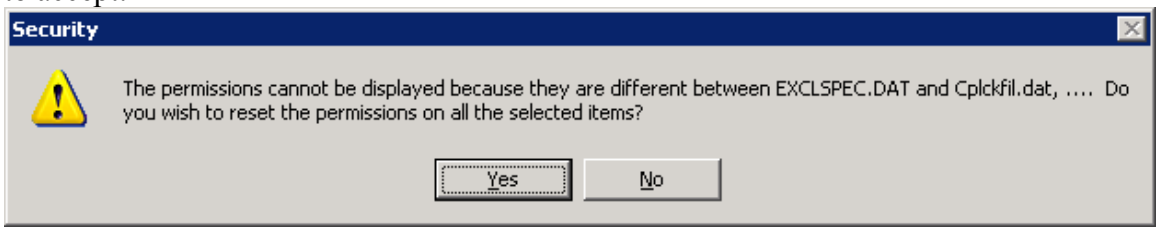
For DAT Files, you need to grant the Users group all the rights except “Full Control” and “Delete”. For BMP files, you need to grant “Read/Execute”, “List Folder Contents” & “Read” privileges. For simplicity, you can grant BMP files the same access right as DAT files.

For DDF files, it depends on whether you have the following scenarios:

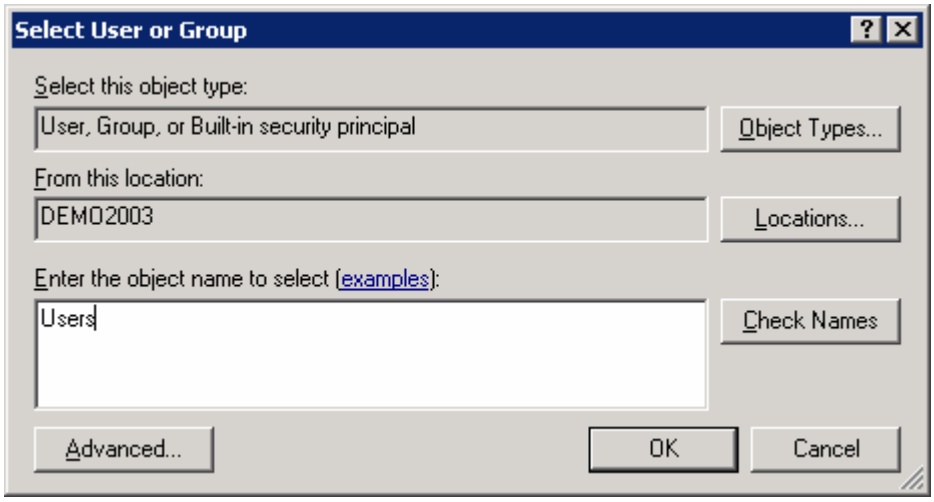
- Use Starship
- Use Crystal Report to Access Elliott Data through Database File Method
- Use Other Tools to Access Elliott Data through Database File Method

If you only access Elliott data from third party tools through ODBC, then you do not need to grant right to DDF files for users. If you do, you should grant the following rights to users: “Read/Execute”, “List Folder Contents” & “Read” privileges. Please be aware of third party tools may place certain dictionary files in the DATA directory where user will need to have access to those files at the O/S level in order to function. If that is the case, then assign users O/S right for those files as well. For example, with Crystal Report, if you choose to create dictionary files (*.DC*) and save the dictionary files in the DATA directory, then you will need to give users access to those files at O/S level if users need to run Crystal Report base on those dictionary files.

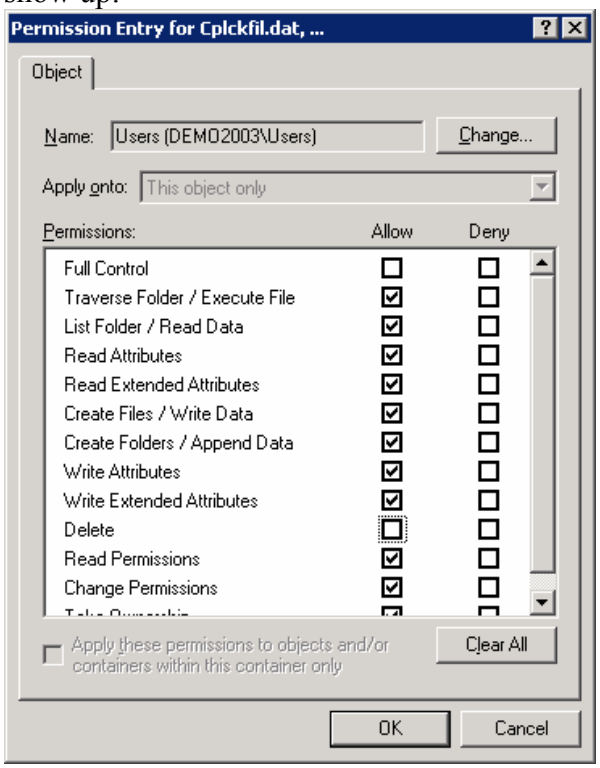
Once you highlight all the necessary files in the DATA directory, right click and choose “Properties”. Choose the Security tab. If you receive the following message, click “Yes” to accept:



Click the “Advanced” button in the Dialog box and choose “Add” in the “Advanced Security Settings” dialog box. (Note: It is not the Edit button. You can’t edit the inheritance privilege for the Users group).



Select “Users” group and click the “OK” button. The Permission Dialog Box should show up:



For DAT files, uncheck the “Full Control” and “Delete” permission boxes. Click OK to save. For BMP and DDF and other files in the DATA directory, please read previous explanations for setting up the security rights.

Testing of your NTSF Setting

The Elliott application is complicated and you should test your NTFS security settings. The following are some suggestions:

1. It is suggested you start to implement security settings from the TUTORIAL directory and fully test it before you implement the DATA directory.
2. Make sure you always grant rights for Administrators with full access. When an issue in Elliott comes up, test against the Administrator's account to see if it works. If it does, then most likely it is a security setting problem. By default, Administrator should have full access to Elliott and subdirectories as long as you do not remove it.
3. Make sure you implement Security settings for a DATA directory after Elliott is fully up and running and all necessary files are created. Otherwise, the file level access rights you granted may not work properly since those files may not exist yet.
4. Login as a non-Administrator and test the following functions:
    a. Spool a report to disk
    b. View and Print spooled reports
    c. Delete a spooled report
    d. Edit Company File or perform Module level setup.
    e. Print a Laser Form.

Special Consideration for Credit Card Processing

If you are processing credit cards or need a directory under the Elliott directory to store temporary files, be sure that you allow the following security settings for the directory:

- **Create Files / Write Data**
- **Delete Subfolders and Files**

Special Consideration for Sales Order Import & Export

Make sure the users who will perform Sales order Import & Export is granted with full access right to the directory where Sales Orders Import & Export ASCII file will reside.

Conclusion

In order to take advantage of the PSQL 8.5 security improvements, the security setup of the Elliott directory is complicated. There may be other directories and users that require special security settings that are not covered in this document. It is suggested you talk to your Elliott reseller and your network consultant to perform proper configuration. Extensive testing is suggested before implementing it live.