Tribon M1 / M2 Project Security Setup

1 Preface

One TRIBON project is a complex environment which consists of different kind of information. There are data banks, default files, project configuration file, symbols, applications' input and output files, etc. Each of these items has to be accessed and supported in the right way. For example, the data banks have to be accessed only trough the applications that are especially designed for this purpose. Opening any of the data banks' files as a text file for example may corrupt the data bank and destroy the information inside, hence to destroy the model information.

Considering the TRIBON working environment in the real live, we have to admit that one TRIBON project will be accessed by a number of people, specialists in their area - pipe, hull, outfitting, etc., but with different computer skills. In order to build one trouble less working environment, we must protect the sensitive project information from the human's mistakes and at the same time to provide flexible and unrestricted way of working for every project participant.

The purpose of this document is to give to the reader a basic understanding for TRIBON project environment, the usage of the different project's items and some examples of how these items could be organized and protected using the standard Windows security facilities.

2 Basic concept

In the real practice one TRIBON project is accessed in client-server working environment. In other words , the project and all its components are located on the server while the designers' workstations (client PCs) are running the applications locally and access the model information located on the server. This way all project participants use the latest model information and the latest project settings. All sensitive information is located in one place (on the server) and it is easy to back up or restore it when required.

2.1 The server

Generally when we say "server", we have in mind a powerful computer running Windows Server operating system. On this machine we could set up a number of software servers to handle the client-server networking environment. Such servers could be DNS, DHCP, Telnet, FTP etc. On the same machine we could create and configure different computers, groups and users accounts with the corresponding level of privileges and file access permissions. Usually we setup this machine as a domain controller. These settings are network wide and even if the user login from different client's workstation he will have always one and the same privileges.

TRIBON Server

Normally we call "TRIBON server" the machine where the TRIBON projects are located. This could be the same domain controller, a second domain controller or even just a normal computer running Windows Workstation software but with higher performance. However for a workgroup of 3 to 7 designers one workstation dedicated for TRIBON server could be more than enough, but for bigger design offices Windows Server operating system is recommendable.

What we call "TRIBON Server" is actually a set of software servers (windows services) and project relevant data banks and ASCII files. Depending on the purpose of this software we can define the following items:

- TRIBON License Server
- TRIBON Data Base Server
- TRIBON Surface Server
- TRIBON Project Server

The common practice is to have all of them configured and working on one and the same machine and usually this is a Windows Server platform. In some rare cases the surface server could be located on a different PC or even there could be more than one surface servers running in the network. At this moment I would like to point out only the difference between Data Base Server and Project Server. For many users both servers sounds as one and the same functionality, but it is quite different actually. The Data Base server is supposed to provide access to the data banks where the model objects are stored, while the Project server's usage is to keep the project's definitions and to provide this information to the client's PCs, serving d065...sdb files in fact.

TRIBON Client

Usually this is the designer's PC which is running Windows Workstation software. TRIBON software must be installed on this machine as well. It is user's choice whether a full installation to be done or only the required packages for this particular working place to be installed.

Generally the client's PC access the information located on the server in two ways:

- TRIBON data banks are accessed using TRIBON data base server and its sub servers based on PowerRPC Portmapper service
- For all other files the standard Windows file sharing is used

3 Hardware considerations

When it comes to the hardware specification, for all users there are three main concerns:

- cost of the hardware
- reliability
- performance

Usually all these factors depends each of the other. The trick is to find the best compromise between the cost and the performance of the system. And when we say performance, we should notice that the overall system performance actually depends on several components:

Server - its performance and reliability will affect all clients' workstations. The following items must be considered when select the server's hardware:

- Hard disks - to be as quick as possible and on SCSI interface. 10,000 rpm/s and RAID system should be considered.
- Operating Memory - 1024 MB of RAM or more
- CPU speed - 2GHz Pentium IV or higher. If you do not plan to run TRIBON SURFACE server on this machine, the CPU speed is not of crucial importance
- Video card - It will not affect the client's performance in any way. However for the need of the locally running applications a good graphical card should be considered
- UPS - strongly recommendable item dedicated for this particular server only but not to provide a power supply to the whole workgroup

Networking - another important component. Even if you have the most powerful server in the world, if your network is weak you can't achieve good performance and reliability. Please take under consideration network switches or switching hubs on 100MBS interface. If possible arrange 1GBS interface for the server. Very often you could increase the performance of one existing network simply by splitting it on a several VLAN.

Client's workstation - normally its performance will have direct impact only on the processes (applications) which are running locally. The hard disk speed would affect the applications startup but not the whole design process. The most important items to be considered for the client are:

- CPU speed - for Windows 2000 and TRIBON M1v4 Pentium III on 1GHz could be suitable. If you are going to migrate to Windows XP and TRIBON M2 - better consider Pentium IV at 1.5 GHz or higher
- Operating Memory - minimum 512 MB
- Video Card - this is one of the most important factors especially if you use TRIBON shading facility often. Consider one of the newest RADEON or NVIDIA models with minimum 64 MB memory.

4 Project permissions set up

In this chapter we will go step by step through the main procedures involved in the process of TRIBON Project set up. We will do this from the system administrator's point of view, concerning the project structure, files and directories placement and permissions, domain users and groups' accounts. Some of the projects environment variables might be used as examples only. However, the exact setup of all possible projects' parameters (environment variables) is not a subject of this document.

4.1 Client - Server environment

What we call client - server environment?

To have it, we need at least two computers connected each to other via local network or Internet. For any particular task we could define one of these computers to act as a server and the other one to be the client. In one large network group we might have as many possibilities as the number of the machines in the network is. When it comes to TRIBON software - we have no limitation. Actually any PC with TRIBON installation is ready to act as a server. Then we should consider its hardware resources, the version of the operating system and how that particular PC is used. Obviously the normal designer's workstation is not the best choice to use it for a server as it completely depends from the user who is working there. Of course it might be used for small workgroups, but for network with more than 5 PCs it is preferable to have one machine dedicated for server.

In this document we will consider the following client - server environment.

Server:

Windows 2000 server operating system used for: Primary Domain controller, DHCP, DNS file and print server.

Windows 2000 server operating system used for: Secondary domain controller and TRIBON Server (TB Project server, TB DataBase Server, TB Surface Server).

TRIBON M1v4 complete installation has been made on this machine. However, in order to use it as a TRIBON server it is not necessary to install all TRIBON applications, but it is recommendable. When you have them all it is much easier to test the projects' setup and to perform different maintenance tasks when required comparing to the case when only the minimum set of services is installed. The host name of this machine will be " tbserver " so we could easy refer to it when necessary.

Clients:

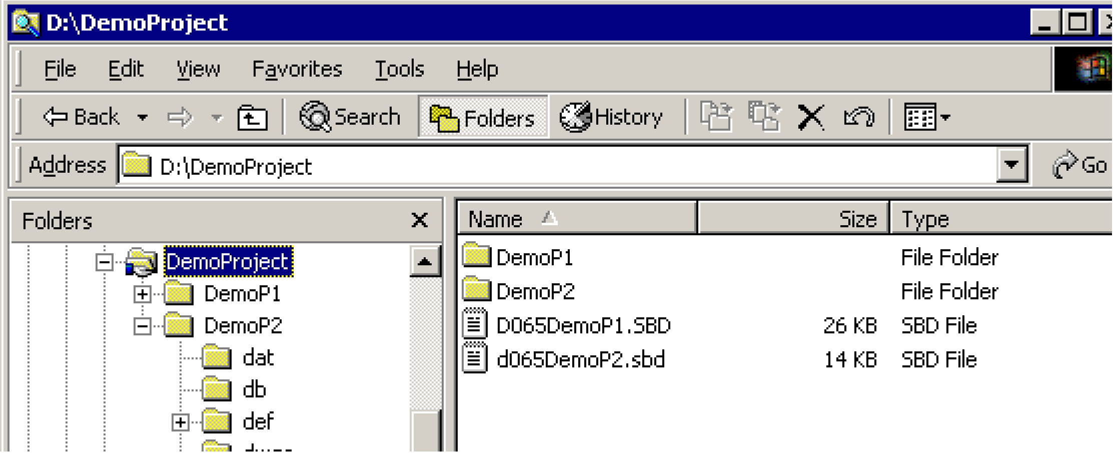
Any PC with Windows 2000 Professional (Workstation) or Windows XP Professional (Workstation) and TRIBON software installation

4.2 Project Server (projects' definition) access

4.2.1 Server side

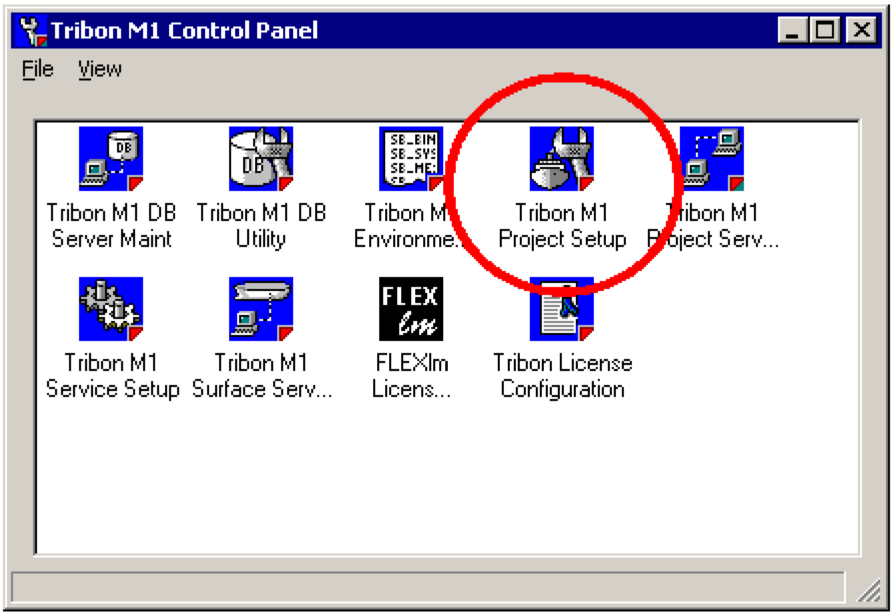
Let we start building our project environment.

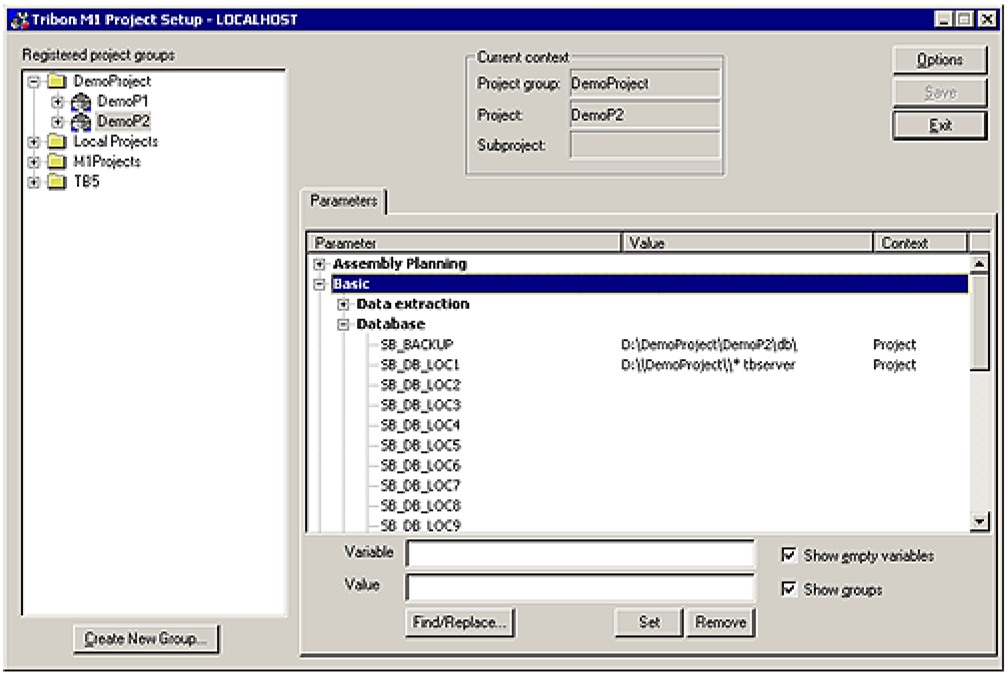
First of all we need a separate directory dedicated to hold all TRIBON Project's information. For this reason we create a directory called "DemoProject" located on disk "D". As a general rule we use disk "C" for the operating system and software installation only. Disk "D" we usually dedicate for data storage.



Name	Size	Type
DemoP1		File Folder
DemoP2		File Folder
D065DemoP1.SBD	26 KB	SBD File
d065DemoP2.sbd	14 KB	SBD File

There are two project directories DemoP1 and DemoP2 and two project definition files D065DemoP1.sbd and d065DemoP2.sbd. In this chapter we will focus on d065...sbd files. They consists of the main projects environment variables that define the location of the project's data banks and directories. In order to make these definitions known to TRIBON we must set up the project server first. For this reason we use "TRIBON M1 Project Setup" program from "TRIBON M1 Control Panel"





Tribon M1 Project Setup - LOCALHOST

Registered project groups

- DemoProject
  - DemoP1
  - DemoP2
- Local Projects
- M1Projects
- TB5

Current context

Project group: DemoProject

Project: DemoP2

Subproject:

Parameters

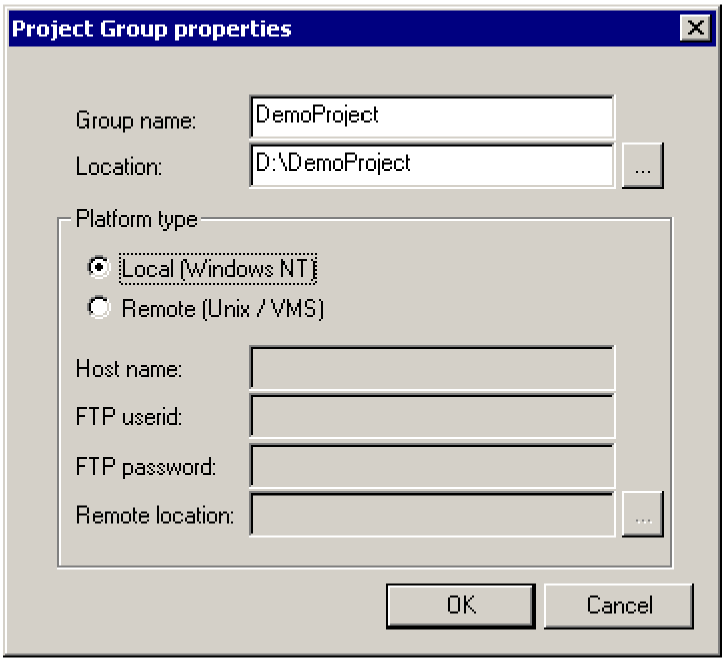
Parameter	Value	Context
Assembly Planning		
Basic		
Data extraction		
Database		
SB_BACKUP	D:\DemoProject\DemoP2\db\	Project
SB_DB_LOC1	D:\\DemoProject* tbserver	Project
SB_DB_LOC2		
SB_DB_LOC3		
SB_DB_LOC4		
SB_DB_LOC5		
SB_DB_LOC6		
SB_DB_LOC7		
SB_DB_LOC8		
SB_DB_LOC9		

Variable

Value

☑ Show empty variables

☑ Show groups



Project Group properties

Group name: DemoProject

Location: D:\DemoProject

Platform type

● Local (Windows NT)

○ Remote (Unix / VMS)

Host name:

FTP userid:

FTP password:

Remote location:

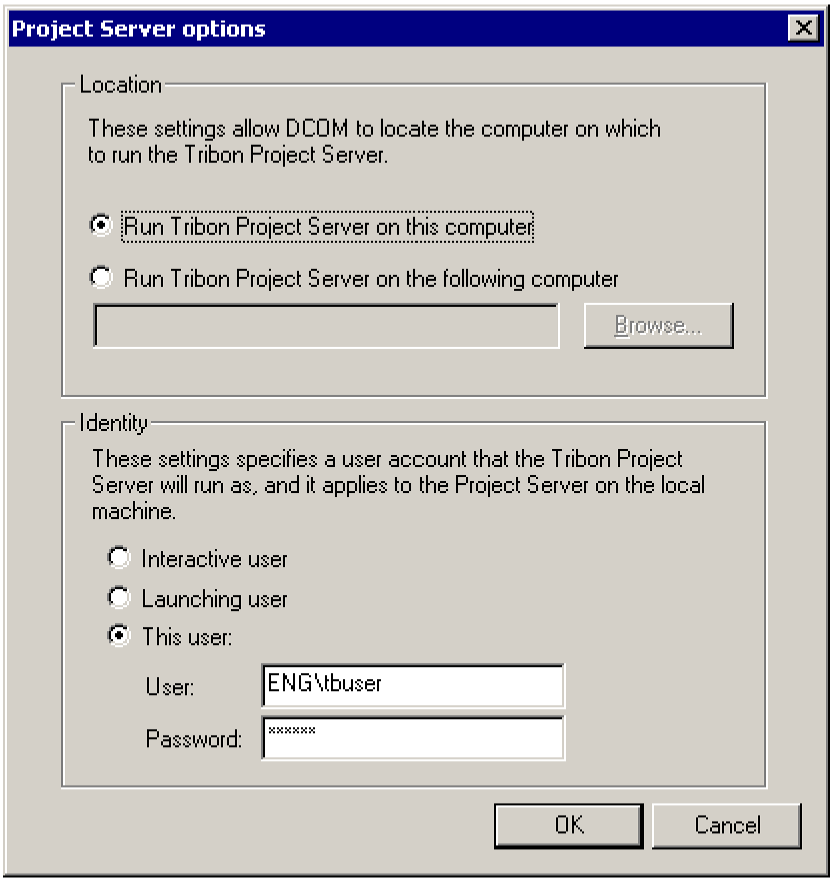
Click on "Create New Group" button and key in the group name and the location in the group's properties dialog box.

We always select Local (Windows NT) for the platform type when it is a Windows based project. The "Remote" option is used for projects located on UNIX or VMS platform, but it is not a subject of this document.

Note that "Location" must point to the directory where the project definition files are located.

This way we can create a number of different project groups to be hosted by this server and each group may consist of a number of projects. In this case two projects DemoP1 and DemoP2 will be made immediately available as their project definition files (d065...sbd) already exists in the directory pointed by the field "Location". We can add more projects to this project group by simply creating a new project definition file right in the location directory (D:\DemoProject). Please note that it is not obligatory the project's structure (data banks and files) to be located under the same directory. This is just one of the variations that we could have.

Now when we have a project group created, we must setup the project server options. Click on the "Options" button and consider the following dialog.



Project Server options

Location

These settings allow DCOM to locate the computer on which to run the Tribon Project Server.

● Run Tribon Project Server on this computer

○ Run Tribon Project Server on the following computer

Identity

These settings specifies a user account that the Tribon Project Server will run as, and it applies to the Project Server on the local machine.

○ Interactive user

○ Launching user

● This user:

User: ENG\tbuser

Password: ******

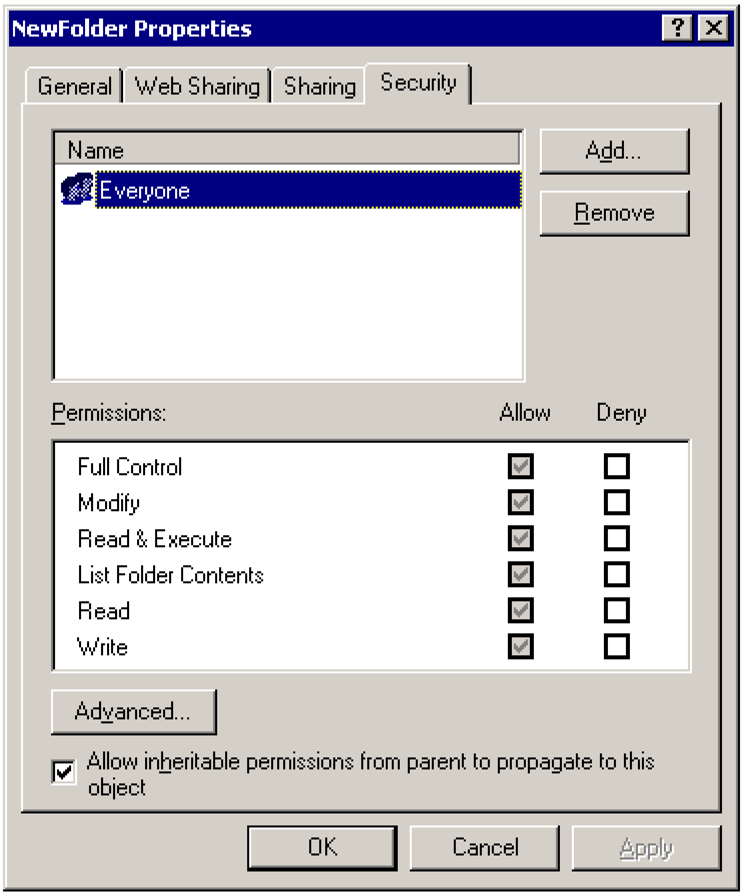
Here we have two important items. The first one is that in the "Location" the option "Run Tribon Project Server on this computer" must be selected. The second one is that we must assign a dedicated user, which account will be used by the project server. For this reason in Identity "This user:" must be selected and then in the "User:" field we specify the users account in the following syntax: DOMAIN\USER_NAME. The user's password is required as well.

Please note that this must be a valid user's account. It must be previously created in the domain controller and must belong to the domain administrators group. This account we dedicate only for the project server purposes and will not be used for ordinary work or by company's employee. When ready, press "OK" button to return to the main application window.

From this application we can modify the project definition files. When a project name is selected, the project's variables will be listed in the "Parameters" window. Click on any variable and change its value in the "Value" field. Then click "Set". When ready with all changes, the project definition can be stored using "Save" button. Please note that this function will overwrite the project definition file (d065...sbd) and the variables might be listed not in the same order as they were in the original file. If you want to keep the original file formatting, you should edit it in an external text editor and use project setup application only for reference.

4.2.2 File Permissions

At last we are in position where we can start setting up the access permissions of the project data. We could do this task even earlier, but for the sake of the documentation structure I have selected this point, where to involve the files' permissions and the users' privileges. From this point further we will have to create Windows domain users groups and users, and to set up file and directory access permissions.



Name
Everyone

Permissions:

	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

In Windows 2000 Server if you create a new directory right in the core directory of the disk (for example D:\NewFolder), the operating system gives full file access permissions to everyone by default. Where "Everyone" is a special users' group build in Windows. These permissions are inherited from the parent directory - " D:\ " in our case. Obviously we do not want everyone to access our data and to have full control on it; otherwise we would not spend time on writing / reading this document. Hence, we have to create our own groups and users and manipulate their privileges as needed.

Let we consider the following users' groups created in the domain:

- TBOUTFIT - all users that will work with TRIBON outfitting applications should belong to this group
- TBHULL - for all users that will run TRIBON Hull applications
- TBMANAGE - the members of this group should be the persons responsible for the project set up and maintenance on TRIBON application level

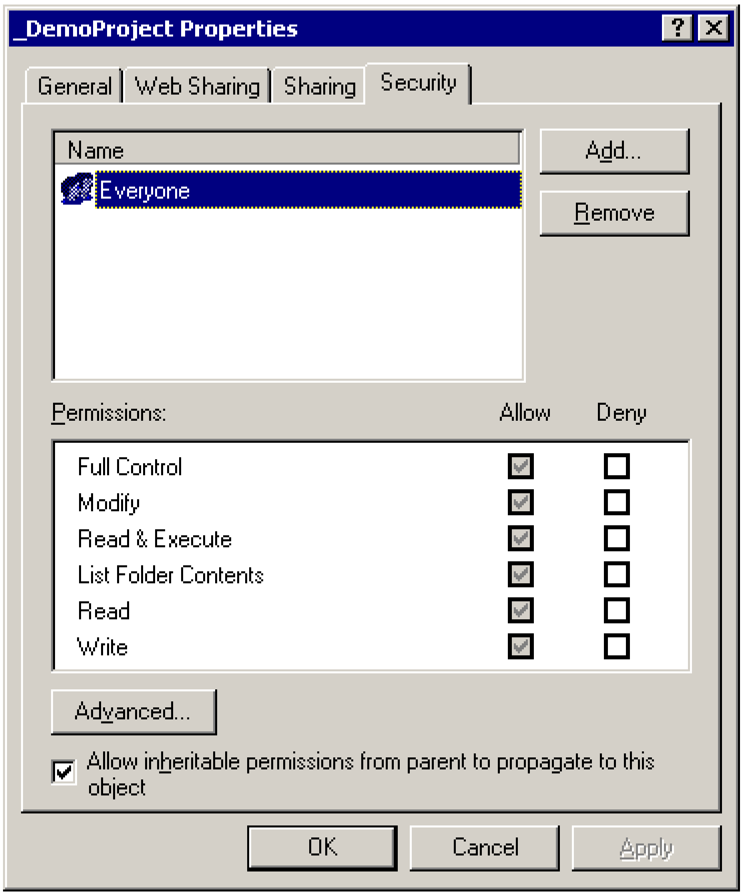
Please note that the groups' names are not obligatory and you could prefer to create them using different names. Also you may have one and the same user to belong to more than one user's group.

At this point we need some users as well. Let we consider:

- tbuser - this account will be used for the project server identity and for troubleshooting as well. It must be a member of "Administrators" group.
- hull_user - example account to be used to run TRIBON Hull applications. Make it a member of "Domain Users" and "TBHULL" groups.

Now we can set up the files and directories permissions for the project. We will do this on a few steps. The first step is to set up the permissions on the highest project group level - directory D:\DemoProject

Open one Windows File explorer and right click on the directory D:\DemoProject - select "Properties" from the mouse context menu and in the "DemoProject Properties" window press "Security" tab. Most probably, you will see the following picture:

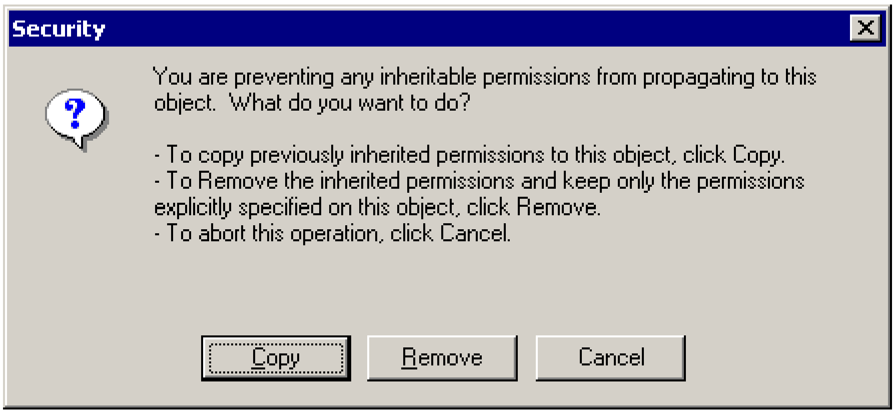


Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

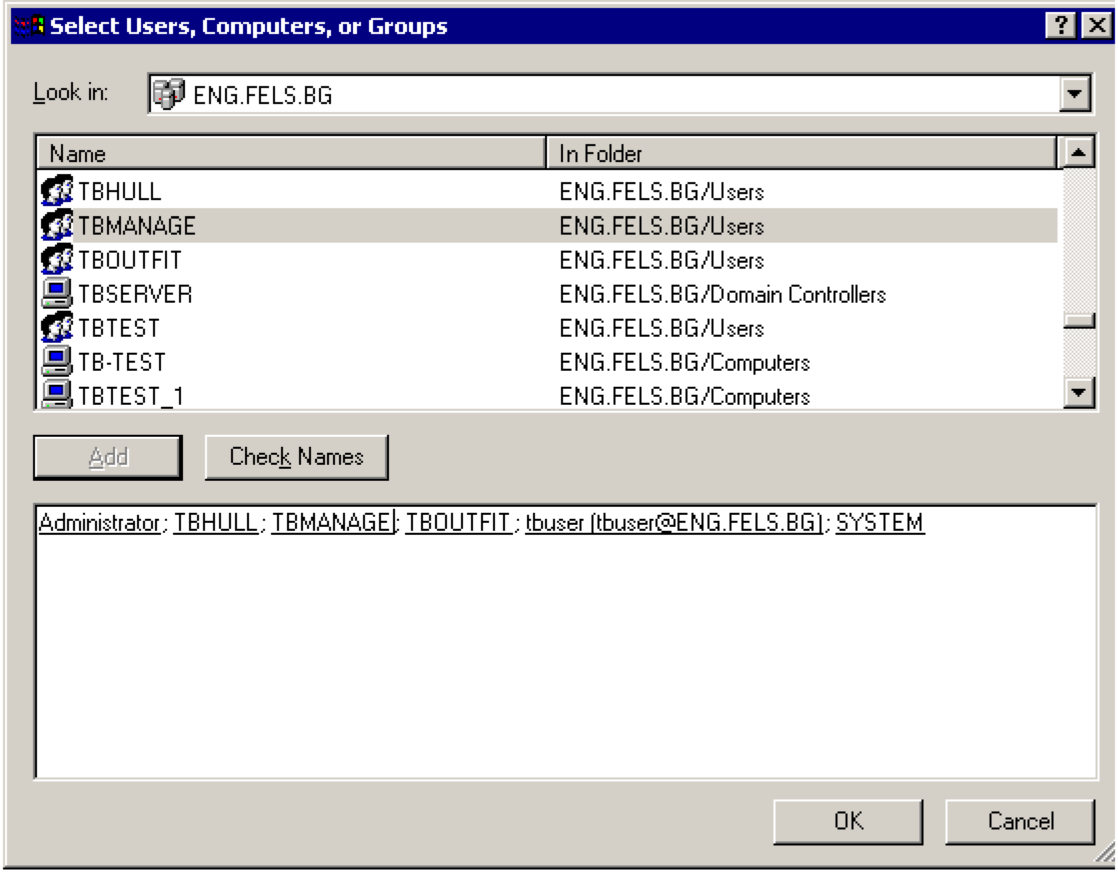
The first think to do here is to unselect the check box at the bottom of the window. This way we remove the link for permission inheritance from the parent object. When you do that a security warning dialog box will be shown and the system will ask you what to do with the existing permission setup. Select "Copy" as we will use the same option on the next stages as well and then click on "Everyone" and press "Remove" button. This way nobody have access to the selected directory and we can start making a list of our users and groups to who we want to grand access privileges.



You are preventing any inheritable permissions from propagating to this object. What do you want to do?

- To copy previously inherited permissions to this object, click Copy.
- To Remove the inherited permissions and keep only the permissions explicitly specified on this object, click Remove.
- To abort this operation, click Cancel.

Now click "Add" and the following dialog will be shown.



Look in: ENG.FELS.BG

Name	In Folder
TBHULL	ENG.FELS.BG/Users
TBMANAGE	ENG.FELS.BG/Users
TBOUTFIT	ENG.FELS.BG/Users
TBSERVER	ENG.FELS.BG/Domain Controllers
TBTEST	ENG.FELS.BG/Users
TB-TEST	ENG.FELS.BG/Computers
TBTEST_1	ENG.FELS.BG/Computers

Administrator ; TBHULL ; TBMANAGE ; TBOUTFIT ; tbuser (tbuser@ENG.FELS.BG) ; SYSTEM

From the list in the top window select the corresponding user or group and press "Add" in order to collect all required members. The following objects must be selected:

- Administrator - user
- tbuser - user
- TBHULL - group
- TBMANAGE - group
- TBOUTFIT - group
- SYSTEM - group (build in the operating system)

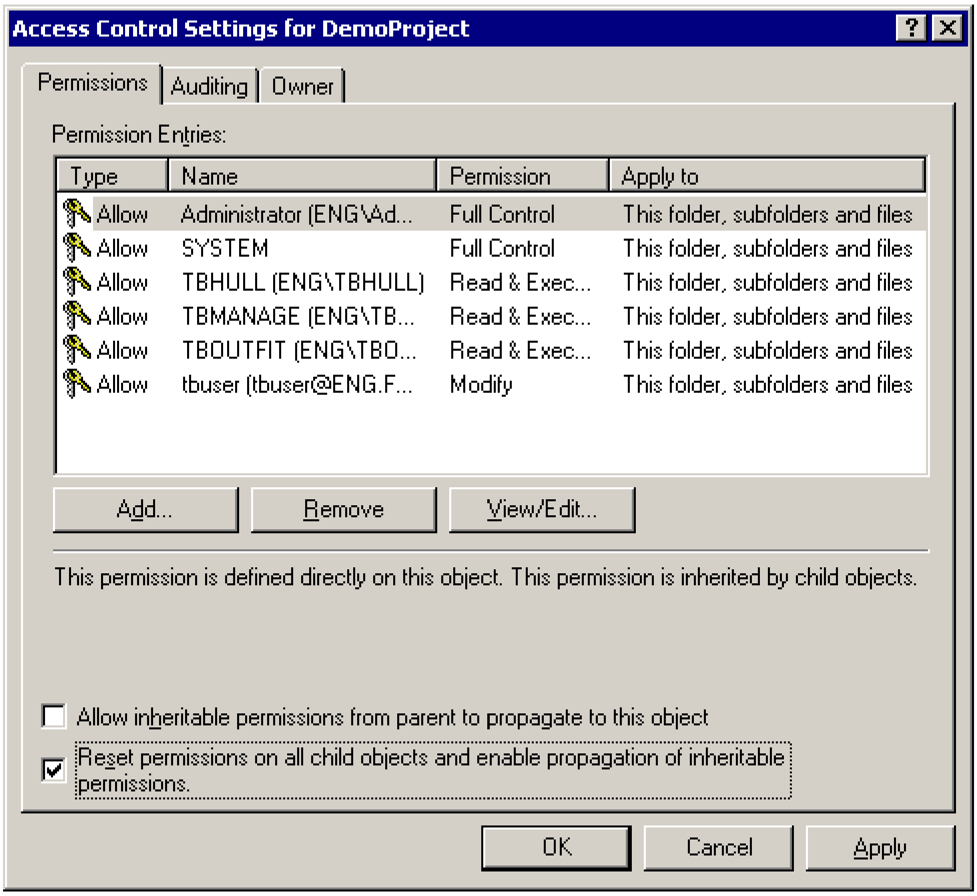
When ready press OK to continue. All selected objects will be listed in the security tab and to every one of them the following permissions will be granted:

- Read & Execute
- List Folder Contents
- Read

Now we have to modify some of the permissions as follow:

- For Administrator - add "Full Control" - just select the corresponding check box
- For SYSTEM - add "Full Control"
- For tbuser - add "Modify". "Write" will be selected automatically.

When ready, press "Advanced". A new dialog will be presented. The only think to do here is to select "Reset permissions on all child objects" check box and click "Apply". A message box with request to confirm this operation will be shown. Click "Yes" to confirm.



Access Control Settings for DemoProject

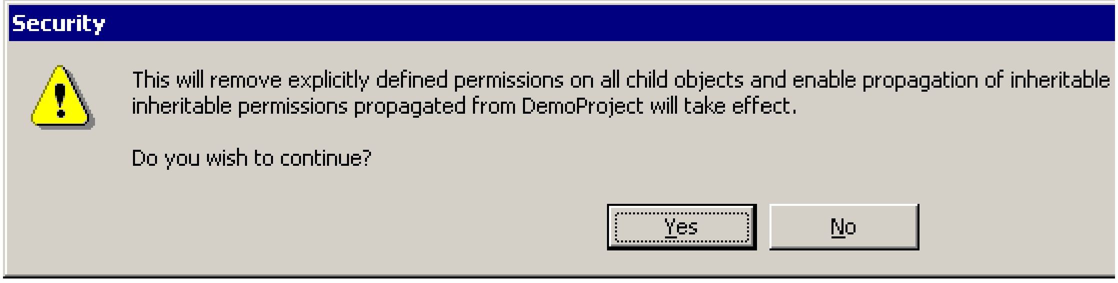
Permission Entries:

Type	Name	Permission	Apply to
Allow	Administrator (ENG\Ad...	Full Control	This folder, subfolders and files
Allow	SYSTEM	Full Control	This folder, subfolders and files
Allow	TBHULL (ENG\TBHULL)	Read & Exec...	This folder, subfolders and files
Allow	TBMANAGE (ENG\TB...	Read & Exec...	This folder, subfolders and files
Allow	TBOUTFIT (ENG\TBO...	Read & Exec...	This folder, subfolders and files
Allow	tbuser (tbuser@ENG.F...	Modify	This folder, subfolders and files

This permission is defined directly on this object. This permission is inherited by child objects.

□ Allow inheritable permissions from parent to propagate to this object

☑ Reset permissions on all child objects and enable propagation of inheritable permissions.



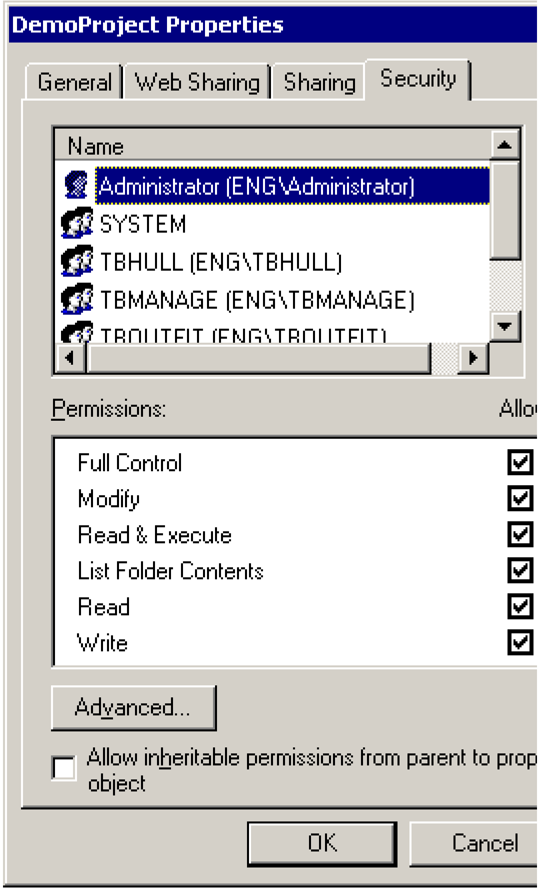
Security

This will remove explicitly defined permissions on all child objects and enable propagation of inheritable inheritable permissions propagated from DemoProject will take effect.

Do you wish to continue?

Doing this, all files and sub folders located under D:\DemoProject will take the same settings for file access permissions. This is our base for further security development.

Example of how Administrator's and tbuser's settings should looks like.



DemoProject Properties

General | Web Sharing | Sharing | Security

Name

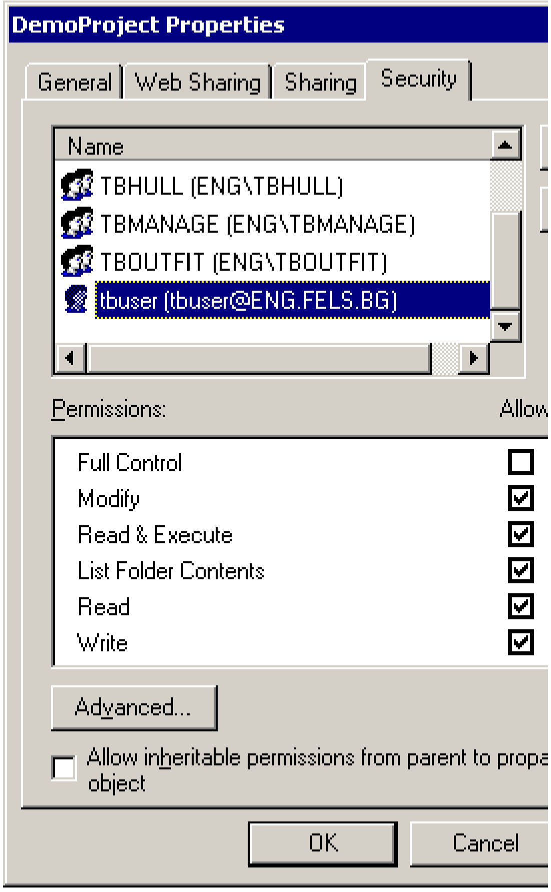
- Administrator (ENG\Administrator)
- SYSTEM
- TBHULL (ENG\TBHULL)
- TBMANAGE (ENG\TBMANAGE)
- TBOUTFIT (ENG\TBOUTFIT)

Permissions:	Allo
Full Control	☑
Modify	☑
Read & Execute	☑
List Folder Contents	☑
Read	☑
Write	☑

Advanced...

□ Allow inheritable permissions from parent to prop object

OK | Cancel



DemoProject Properties

General | Web Sharing | Sharing | Security

Name

- TBHULL (ENG\TBHULL)
- TBMANAGE (ENG\TBMANAGE)
- TBOUTFIT (ENG\TBOUTFIT)
- tbuser (tbuser@ENG.FELS.BG)

Permissions:	Allow
Full Control	□
Modify	☑
Read & Execute	☑
List Folder Contents	☑
Read	☑
Write	☑

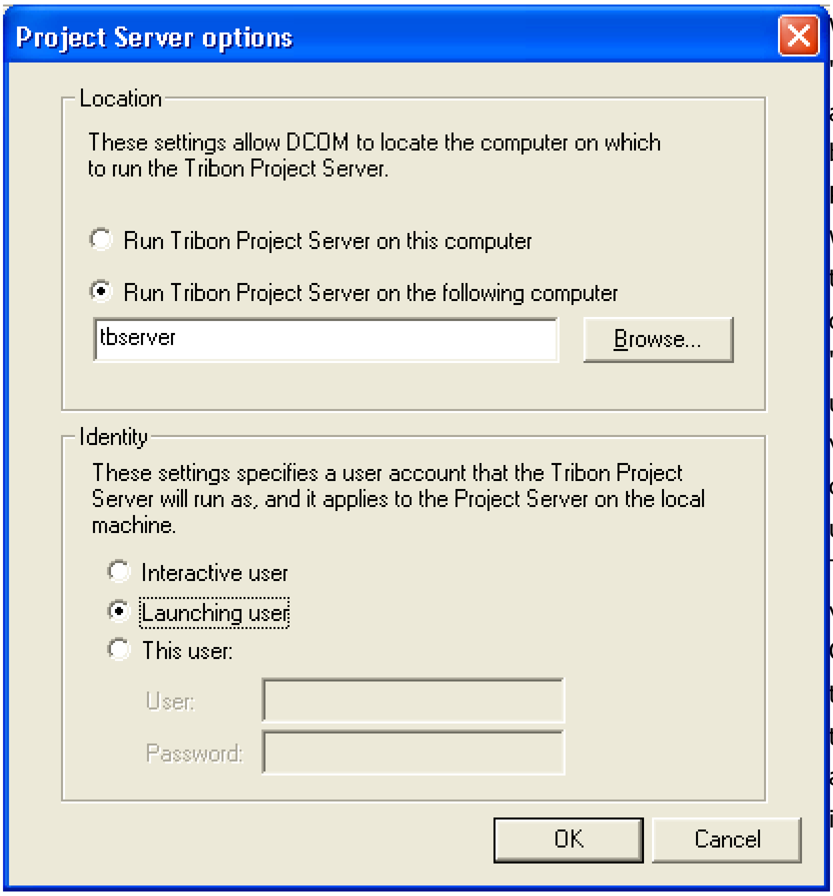
Advanced...

□ Allow inheritable permissions from parent to propa object

OK | Cancel

Client side

Once the project server is ready, we can set up the client workstation to use it. For this reason at the user's PC simply run "Tribon Project selection" program and click the "Options" button. On this window we must select "Run Tribon Project Server on the following computer" and to specify the host name of the machine where the project server is running. In this case it is "tbserver". The Identity option is not important at the client side, so we can leave it as is by default - "Launching user".



Location

These settings allow DCOM to locate the computer on which to run the Tribon Project Server.

○ Run Tribon Project Server on this computer

● Run Tribon Project Server on the following computer

tbserver

Identity

These settings specifies a user account that the Tribon Project Server will run as, and it applies to the Project Server on the local machine.

○ Interactive user

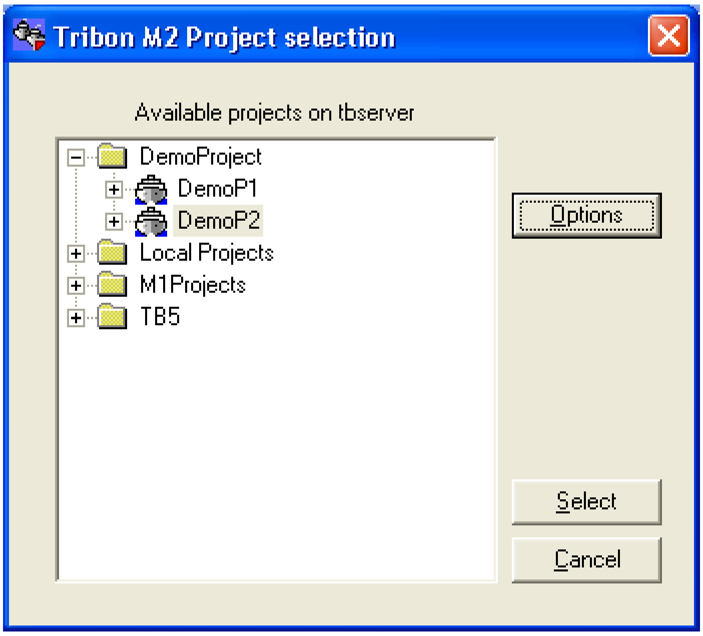
● Launching user

○ This user:

User:

Password:

When ready, press "OK" and a list of all available projects will be shown in the Project selection window. Select one of them to make it current and press "Select". This will set up the project's variables on the client's PC and will update the local Tribon environment variables located at C:\Tribon\M1\Config\tbenvtable.sbd. In this example we assume that Tribon is installed on disk "C".



Available projects on tbserver

- DemoProject
  - DemoP1
  - DemoP2
- Local Projects
- M1Projects
- TB5

4.3 Data Base access

4.3.1 Tribon data base background

One native TRIBON data bank consists of 4 different files:

- D:\DemoProject\DemoP2\db\ppidb.dat
- D:\DemoProject\DemoP2\db\ppidb.idx
- D:\DemoProject\DemoP2\db\ppidb.eob
- D:\DemoProject\DemoP2\db\ppidb.lck

In this example:

- ppidb is the data bank name
- D:\DemoProject\DemoP2\db is the path to the data bank
- ppidb.dat and ppidb.idx are data bank's index files
- ppidb.eob is the data file
- ppidb.lck is a lock file

The Tribon applications do not use these physical file names to access the data banks. Instead, Tribon environment variables for data bank access are used. These variables are predefined in the system and must be setup in the project definition file - d065...sbd. For example the drawings data bank definition may looks like:

SB_PDB D:\DemoProject\DemoP2\db\ppidb

Please note that we do not put any file extension in the definition above.

Defining the data banks' environment variables in this way is quite enough for getting access to them if they are located on the hard disk of the local PC, but when we want to have access to the data banks located on a remote machine, some additional variables will be necessary. These environment variables are SB_DB_LOC1 - SB_DB_LOC9. We can use up to 9 variables in order to set up the remote data base access.

In our case all data banks are located on the server, which host name is "tbserver" and physically reside on disk "D" under D:\DemoProject\DemoP2\db\ directory. So, we can use only one variable.

SB_DB_LOC1 D:\\DemoProjects\\* tbserver

This way we say that our data banks are located on machine with name "tbserver" and reside on its local disk "D" somewhere under directory "DemoProject".

4.3.2 Tribon data base server

The client-server access to a data bank located on a remote machine is based on ONC RPC (Open Network Computing Remote Procedure Calls). In order to provide access to data bank located on the server we must have the following Windows services running on the server machine:

- PowerRPC Portmapper

- TRIBON M1 DB Service

TRIBON M1 DB Service is what we call "superserver". Its executable file is - ea312.exe. This superserver listens to calls from client applications and when the first request to access a data bank arrive, the superserver run another program - ea310.exe which we call "subserver". One the server machine we may have only one superserver process, but more than one subserver processes. For every application accessing the data banks, we must have one subserver process dedicated to transfer the data between the application and the data banks. When the application is terminated the corresponding subserver process should be automatically stopped. In other words, if you have 10 Tribon applications accessing data bases located somewhere on the server, then you should have one ea312 process and ten ea310 processes running on the server. If you do not have any Tribon application running - you should have only one ea312 process running on the server.

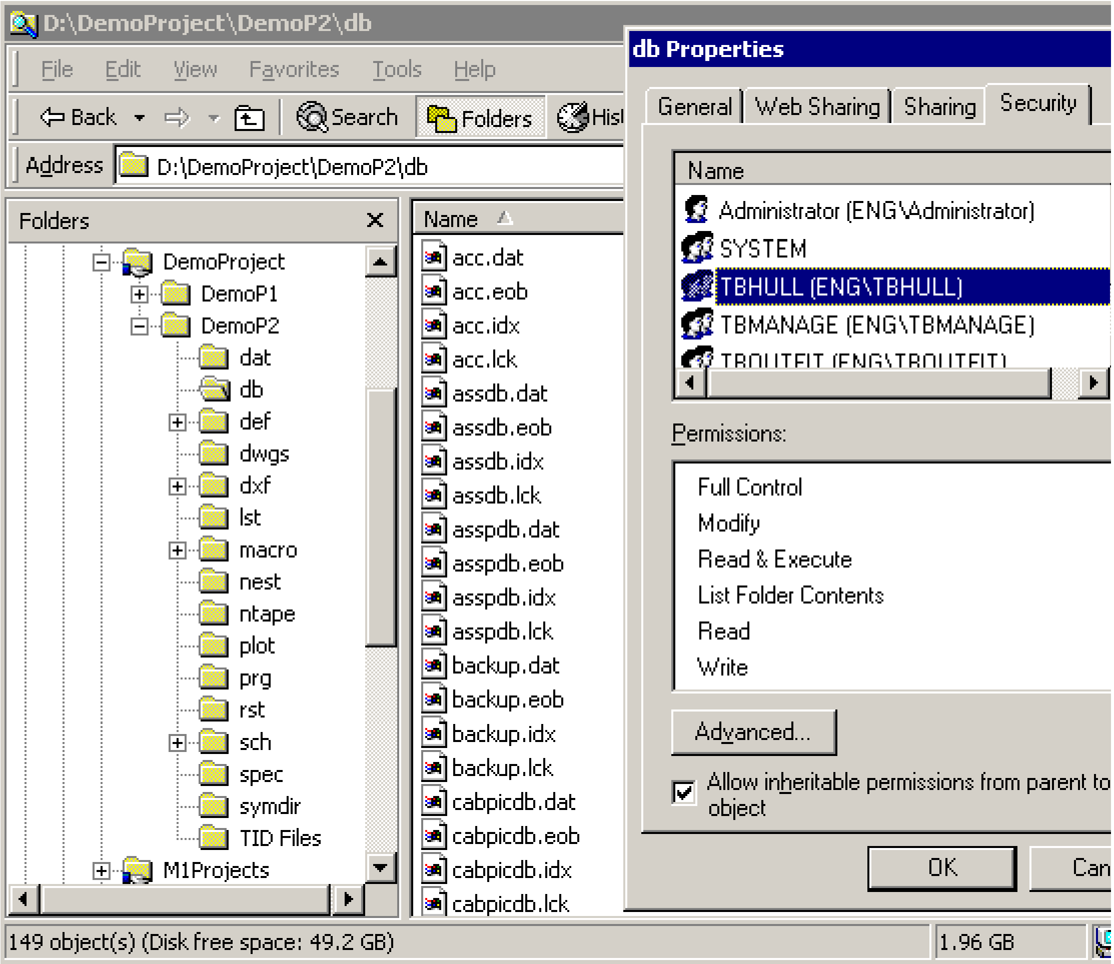
4.3.3 Tribon data base security

One of the common problems with the data bank is that some of the users may open one of the data base files using application that is not designed for this purpose or even delete some of the files. For example if we edit D:\DemoProject\DemoP2\db\ppidb.dat in application like Windows Notepad the data base could be completely destroyed. So, many system administrators are looking for a suitable way to protect the data base integrity from the users' mistakes or lack of experience. Fortunately, there is an easy way to achieve quite satisfactory level of protection from this kind of "mistakes". Of course it will not protect the data base if the ordinary Tribon applications are used and some of the objects inside are modified or deleted, but our task now is not to protect the data base from Tribon actually.

Obviously, if we want to prevent the data base files access from the users, we must give them no permission to write or modify these files. And we have done this already! If you check the Security properties for D:\DemoProject\DemoP2\db folder or for any of the data base files located there, you will see that the groups TBHULL, TBMANAGE and TBOUTFIT can only read these files, but can not modify them. Hence, any user who belongs to one of these groups and have no other special privileges granted could not modify the data banks outside Tribon. The user "tbuser" have "Mofify" and "Write" privileges granted, so he could copy, rename and even delete these files. But we have negotiated already that this username will not be used for design purposes, but only for maintenance when required. So this is not a problem. The Administrator and the SYSTEM group are granted with "Full Control". Hope that the administrator is not going to destroy the data base.

The important item here is SYSTEM. This account is used by Windows and this is the account we actually need to grant full control over the data banks if we want to access them using Tribon. All data transfer between the data banks and Tribon applications is done by the applications' subservers based on the PowerRPC Portmapper service. That is why the normal user no needs to have direct access to the data base files.

This image illustrate the security permissions settings fro TBHULL group over the data base directory. Actually these permissions has been set in one of the previous steps, when we have instructed Windows to reset the permissions of all child objects under D:\DemoProject folder.



4.4 Project's files access

In this chapter we will consider some of the other project's directories security settings. Let we take a look at D:\DemoProject\DemoP2\lst folder first. This folder is dedicated for the applications' output and log files. Hence, all users must be able to create and modify files here. In order to arrange such access level we use Windows File Explorer again. Right click on the folder D:\DemoProject\DemoP2\lst and from the context menu select "Properties". Click on the security tab and use the same technique as in 4.2.2 starting from the point where we unselect the check box "Allow inheritable permissions from the parent ". Then select each of the users' groups - TBHULL, TBMANAGE and TBOUTFIT and tick the "Modify" check box. Finally, use "Advanced" to "Reset permissions of all child objects". The permission setting for LST directory is ready.

It is the same requirement for D:\DemoProject\DemoP2\plot and D:\DemoProject\DemoP2\dat folders - all Tribon users should have "Modify" privileges there, so you could consider selecting all three directories in the previous step and setup the security properties in at once.

Hull related folders:

- D:\DemoProject\DemoP2\nest
- D:\DemoProject\DemoP2\ntape
- D:\DemoProject\DemoP2\sch

Using the same technique give "Modify" privileges only to TBHULL group.

Pipe related folders:

- D:\DemoProject\DemoP2\prg
- D:\DemoProject\DemoP2\rst
- D:\DemoProject\DemoP2\spec

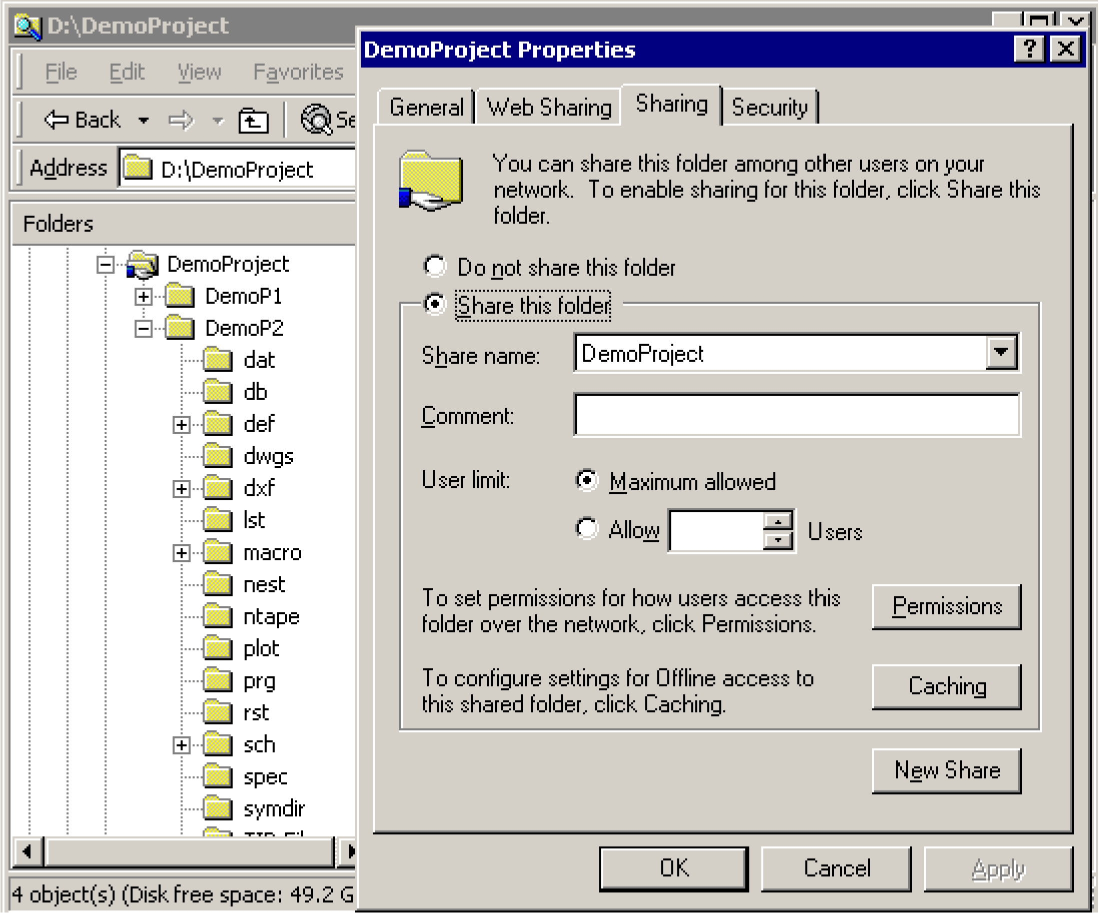
Using the same technique give "Modify" privileges only to TBOUTFIT group.

A special consideration is required for D:\DemoProject\DemoP2\def folder. Normally it is dedicated for the applications default files. The user's account "tbuser" already have read/write access to its contents. However, if you need to allow more users to modify the default files there, you might consider to give "Modify" privileges to TBMANGE group and to make those users members of this group as well.

You might have some additional folders in your project structure. Considering the usage of the information there and the purpose of the folders you might give or restrict the user's access in the same manner as described above.

4.5 Making the project available for the clients' workstations

Now when the project's security permissions are set up we should consider the possibility to access this project from the client's PC. We have nothing more to do about the data banks as the superserver and the subserver will take care about this task. But for all other files and folders Tribon use the standard Windows network file share facility. So, we have to share the project group folder in order to make it available for the clients. From Windows File Explorer, right click on D:\DemoProject folder and select "Sharing".



D:\DemoProject

DemoProject Properties

General | Web Sharing | Sharing | Security

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: DemoProject

Comment:

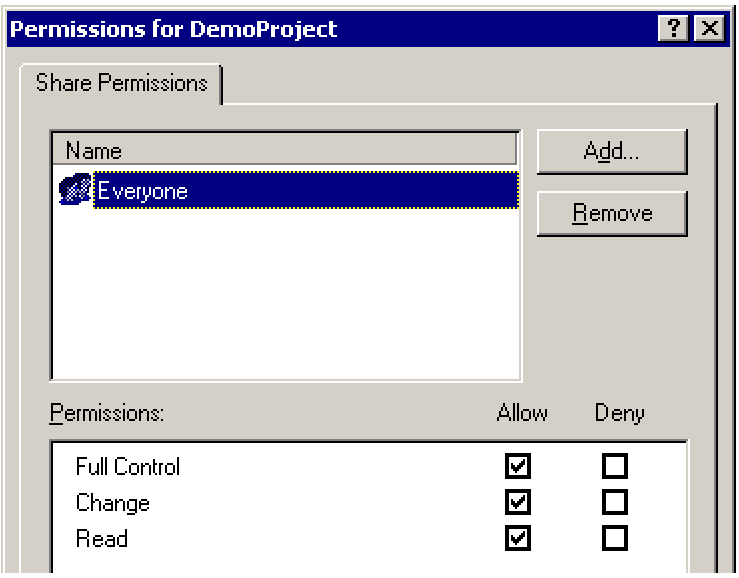
User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

4 object(s) (Disk free space: 49.2 G



Permissions for DemoProject

Share Permissions

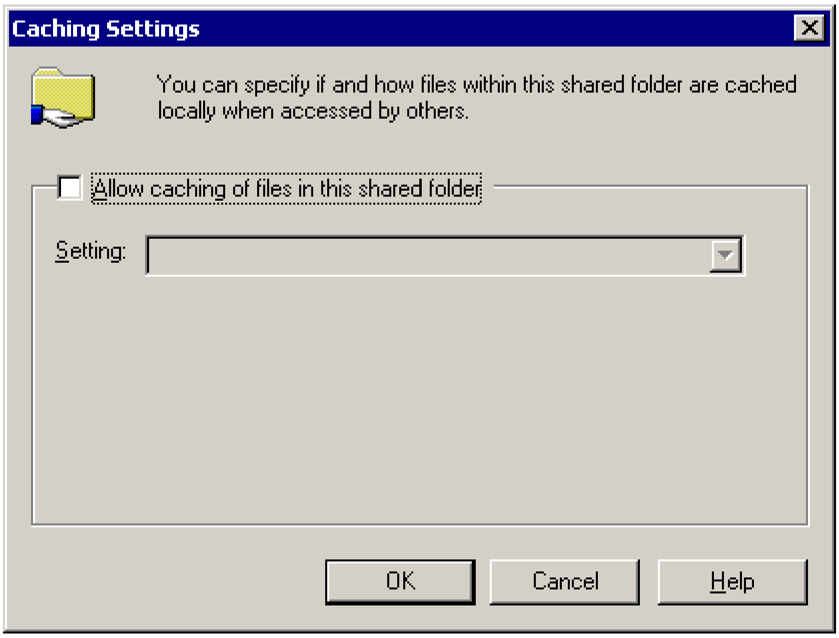
Name
Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Click "Share this folder" radio button and key in the share name. On this example the share name is the same as the folder name.

If you check the Permissions properties, you will see that "Everyone" has a full control on this shared resource. This is not a problem for our security considerations, as we have already set the file access permissions for the project's folders and the operating system will not allow unauthorized access to these resources despite of the full control granted to everyone for the shared folder. So we leave this setting as it is.

Now, click the "Caching" button. It is important here to deactivate "Allow caching of files in this shared folder" option. Unselect the check box and press "OK".



Caching Settings

You can specify if and how files within this shared folder are cached locally when accessed by others.

□ Allow caching of files in this shared folder

Setting:

When ready, press "OK" on the sharing dialog in order to close the properties window.

At this point the client's workstations have access to both data banks and ordinary project files. For accessing the network shared resources we could use "Map Network Drive" Windows facility at the client's PC, but actually I prefer another way. In the project definition file, when we define the project environment variables and their values, we can use network path syntax like this \\computer_name\share_name\File_or_folder...

For example:

- SBD_DEF1 \\Tbserver\DemoProject\DemoP2\def\sbd_def1.def
- SBGD_DEF \\Tbserver\DemoProject\DemoP2\def\
- SBGD_PRINT \\Tbserver\DemoProject\DemoP2\lst\

This way we avoid the need to "Map" the network drive to each client.

Now we can select this project at the client's PC to make it current and hopefully to run any TRIBON application. At the same time our data banks and valuable files like the project definition file, application default files and hull schemes are relatively protected.

4.6 Some additional considerations

In order to gain a maximal benefit from the project security settings described in this document, you have to consider some additional requirements.

The first one is - every user in your organization who may have to work with Tribon must have his own login user name and password. And he must use it.

The second requirement is - every user to belong to the proper security group (TBHULL, TBMANAGE, TBOUTFIT). This way, when you put the user in one or more of these groups, you grand or restrict his access to the network resources as he automatically is granted with the same security privileges as the corresponding group is.

A special consideration is required for the project definition file. In chapter 4.2.2 we have granted with privileges to edit the project definition file only the following accounts: SYSTEM, Administrator and tbuser. And if you try to use different login name and open the project definition file over the network, you will be able to read it but not save the file. However, if you run "Project Setup" program from Tribon control panel using any users account, you will be able to change the project settings and to update this file (d065...sbd). You will be able to do that, because despite of the login name you use at the client's PC, Tribon Project setup utility will use the tbuser's accounts as we have already setup it in chapter 4.2.1. So, if you want your project definition file to be really protected, consider changing its security properties for the tbuser's account in order to grand him with Read only permission. Then you might arrange a separate user's account to be used to edit this file. Pay attention to the fact that if you do this, then you will not be able to use Project Setup program to change the projects environment variables. Instead you have to do that in Notepad.