PMOD Audit Trail Network License (PATL)

USER MANUAL
Version 4.4

PMOD is a software
FOR RESEARCH USE ONLY (RUO)
and must not be used for diagnosis or treatment of patients.

(C) 1996-2022, Printed on December 2, 2022

This page is intentionally left blank.

1. PMOD Audit Trail Network License 5
1.1 Purpose 5
1.2 System Organization 5
1.3 User Authentication 6
1.4 Data Protection 6
1.5 Audit Trail 6
2. Installation 8
2.1 System Setup 8
2.1.1 User Administration System 8
2.1.2 ATL Server System 8
2.1.3 ATL Client Systems 8
2.2 PMOD ATL Server Installation and Configuration 8
2.2.1 PMOD Software Installation 9
2.2.2 Overview Tables 9
2.2.3 Starting PMOD for System Configuration 9
2.2.4 System Configuration 11
2.2.4.1 Audit Trail Configuration 11
2.2.4.1.1 Audit Trail Database Creation 12
2.2.4.1.2 Transaction Server for Audit Trail and Licensing 13
2.2.4.2 Study Database Configuration 13
2.2.4.2.1 Study Database Creation 13
2.2.4.2.2 Transaction Servers for Study Databases 14
2.2.4.2.3 Database Cleanup 15
2.2.4.3 User Configuration 16
2.2.4.3.1 User Creation 16
2.2.4.4 DICOM Server Configuration 17
2.2.4.4.1 DICOM Client Configuration 18
2.2.4.4.2 DICOM Server Definition 18
2.2.4.4.3 Advanced DICOM Server Options 20
2.2.4.4.4 Client Script Generation 21
2.2.4.5 Administrator Password Change 22
2.2.5 Starting of the Servers 22
2.2.6 Database Access Rights 22
2.2.7 Audit Trail Configuration 25
2.3 Client Installation 25
3. Maintenance Operations 27
3.1 Stopping/Starting of the Servers 27
3.2 Audit Trail Inspection 27
3.3 Annual Maintenance 30
3.4 Licenses Control 30

4. Data Processing 32

4.1 Starting the PMOD Client 32

4.2 Data Processing 33

4.3 DICOM Data Import 33

4.4 Data Migration 34

5. Appendix 38

6. PMOD Disclaimer 39

7. PMOD Copyright Notice 40

Index 41

1 PMOD Audit Trail Network License

1.1 Purpose

The PMOD ATL version provides an enterprise solution for the application of PMOD in controlled environments with the following features:

- Client-server architecture to separate user administration and data storage from data processing.
- Central data storage in server databases to prevent access from outside of PMOD.
- Central user and data administration from within a privileged account.
- Central user authentication by using the enterprise-wide user administration.
- Access list control for databases to restrict access to authorized users.
- Data access exclusively through client-server communication.
- Central audit trail logging which is transparent to the user.

Note that within the ATL version some of the normal PMOD functionality gets blocked for unprivileged users.

1.2 System Organization

The PMOD ATL version requires a dedicated client-server setup.

Server

At the heart of the setup is a computer system which acts as a protected server ("server"). It

- runs the PMOD license server,
- authenticates the users,
- maintains the user properties,
- hosts the databases containing the data,
- writes the audit trail information into a database.

To prevent unauthorized access and ensure data security, the server should be located in a protected server room ("data center"), and only allow the administrator login.

Clients

The actual data analysis is performed on client machines which have a PMOD software installed. Note that no local PMOD configuration is required.

A user starts PMOD on a client with a script which includes the server address information. Hereby, a sign-on procedure is performed which checks the authorization of the user. If he is known to the PMOD server he can log in and his dedicated configuration is retrieved from the server before he can start working. Thereafter, he can load images from the databases for which he has been authorized. He can process the images and save the results, but he cannot delete objects from the database unless he is authorized. He may add text comments to database objects for clarification purposes. All information logging the user's work is immediately sent to the server and recorded in the audit trail. The user is allowed to change the applications setting in his profiles, which is updated centrally.

The administrator can open the PMOD configuration while working on a client, using the central administration password. Thereafter, he can adjust the system configuration as well as the user configurations and save the changes to the server.

Client-Server Communication

The client-server communication employs PMOD's proprietary transaction server communication protocol using configurable IP ports. The communication can optionally be encrypted and/or compressed. Encryption is recommended for communication across public infrastructure. As it slows communication down, is may not be necessary for communication within an institution. Compression on the other hand can speed up data transmission across slow network connections.

1.3 User Authentication

Authentication ensures that only authorized persons can access data, and that data transformations can unequivocally be attributed to an individual. PMOD distinguishes between a privileged administrator ("PMOD administrator") who installs the software and configures the environment, and the data analysts ("PMOD users") who perform the actual data analysis.

Administrator

The administrator must authorize himself each time he accesses the PMOD configuration. An initial password is provided upon shipment of the program. It can be changed by the administrator and is stored in an encrypted form in the */properties/global.start* file.

After entering the PMOD configuration, the administrator can define PMOD users. For each user he specifies a name, an initial password, his working environment, and adds the user to the access list of the database(s) he is entitled to use. Each PMOD user can also (optionally) be mapped to a user of the underlying operating system ("OS user").

PMOD Users

When a PMOD client is started, PMOD first compares the name of the user logged into the operating system with the list of configured PMOD users. If a PMOD user is found with a matching OS user, login proceeds automatically without requesting a password. In this case authentication is based on the assumption of a correct sign-on to the operating system. Such a configuration is recommended in homogeneous environments like *Active Directory*.

Otherwise, the user has to select his PMOD user name from the list of all configured PMOD users, and log in with his password. The password is initially set by the administrator, but can be changed by the user. The password, is encrypted and saved in */properties/global.start.*

1.4 Data Protection

PMOD provides mechanisms for data protection, which must be combined with the recommended administrative measures as described above 5. If these requirements are fulfilled, data can only be accessed by authorized PMOD users using PMOD's transaction server communication. Regular PMOD users can only read and add data, while delete operations require dedicated privileges.

1.5 Audit Trail

The purpose of the audit trail is to ensure that all data transformations are exactly documented. In PMOD, the audit trail can be recorded in files or in a database. With file-based recording, the system maintains a separate audit trail text file for each PMOD user, which resides on the server machine so as to prevent unauthorized access. Additionally, there is an audit trail text file for system actions. With database recording of the audit trails, all information resides in a single database which supports flexible filtering and data export. We strongly recommend using a database for the audit trail. File based audit trails should only be used in small test environments.

References:

FDA Publication: Part 11, Electronic Records; Electronic Signatures — Scope and Application. Aug. 2003. http://www.cfsan.fda.gov/~dms/guidance.html.

2 Installation

The PMOD ATL version installation includes the following tasks:

- Preparation of a secured server system and a central user authentication environment.
- Installation of the PMOD software on the server.
- Configuration of the server installation: creation of databases, starting of the database server processes, addition of users and definition of their access rights to the databases.
- Setup of the client part of the PMOD software on all clients, or to a common share which is accessible to all clients. Note that the clients require no local configuration.

The installation steps should be performed in the exact order as described below.

2.1 System Setup

2.1.1 User Administration System

It is strongly recommended to employ the operating system to ensure authentication for the PMOD ATL users.

In a Windows environment, the Active Directory (AD) can be employed for central user administration. It supports many features for a strict user authentication policy, for instance:

- Request for a password change after first login.
- Request for a password change after 90 days.
- Locking out of a user after 5 failed login attempts.

To employ the AD for a secure PMOD ATL installation, the following setup is proposed:

- All machines running PMOD should belong to the AD.
- There should be a global group "PMOD Group" for the PMOD users.
- The PMOD Group should only contain PMOD users.
- The AD password requirements should reflect the company security policy.
- All PMOD users should be configured as "OS users".

2.1.2 ATL Server System

The PMOD ATL server handles the licenses, the databases and the audit trails. Therefore, the PMOD server installation should reside on a secured server which is not directly accessible by the clients or users. In this way, access to the data is only possible through the PMOD transaction server facility.

2.1.3 ATL Client Systems

A single instance of the PMOD software should be installed on a network share with read/execute permission for the PMOD Group from all clients. In this way, all users can start PMOD using one single PMOD installation. Note that no configuration of this PMOD installation is required, since all configurations are maintained by the server installation.

2.2 PMOD ATL Server Installation and Configuration

Please follow the steps described below in the proposed order to set up the system.

2.2.1 PMOD Software Installation

Perform a standard PMOD installation on the server machine (separate operating system dependent installation document) and copy the license file *pstarter.lcs* into the *Pmod4.4/system/lcs* sub-directory.

2.2.2 Overview Tables

In the following steps, a server and user structure will be configured which can become quite complex. It is recommended to set up a table to keep an overview of the definitions as you proceed.

The tables below represent the structure which is established in the example configuration of this documentation:

Transaction Servers

	Audit Trail Log & License Server	Import Database	Study Database 1	Study Database 2
DB Name	**Audit**	**Import**	**Study1**	**Study2**
Port	**5201**	**5202**	**5203**	**5204**
IP Address	**127.0.0.1**	**127.0.0.1**	**127.0.0.1**	**127.0.0.1**
Encryption	No	No	No	No
Users (d = delete)		**ATL_Manager** (d)	**ATL_Manager** (d) **ATL1**	**ATL_Manager** (d) **ATL1** **ATL2**

DICOM Server

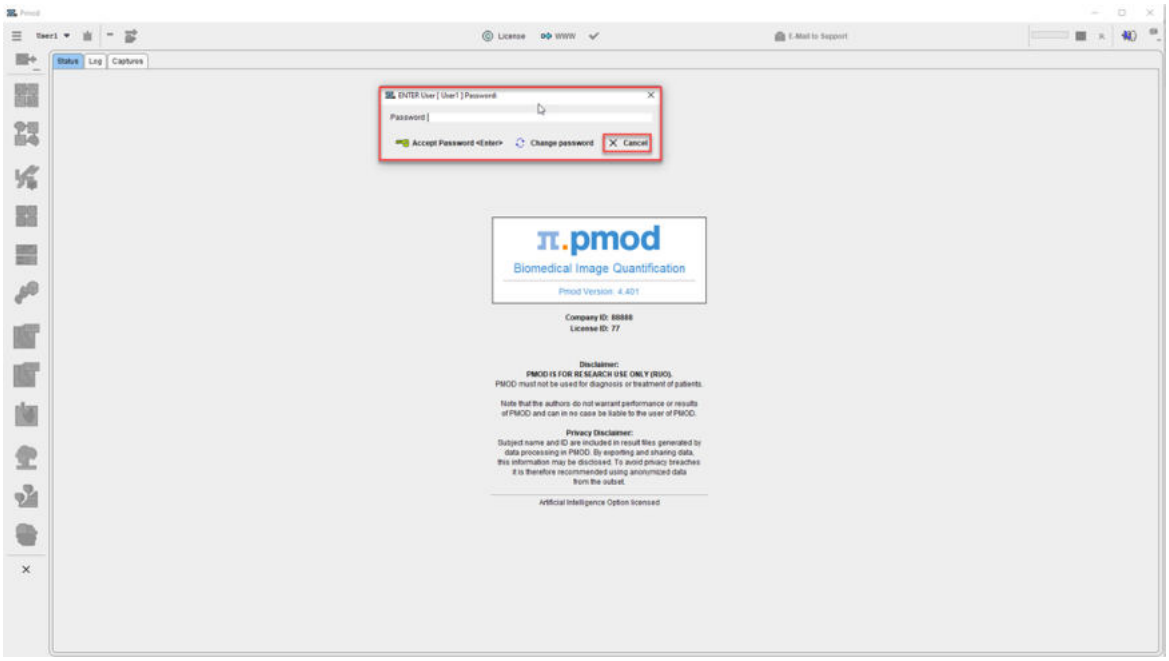
Definition	Value
Application Entity Title	**Pmod**
Port	**5030**
IP Address	**127.0.0.1**
Encryption	**No**
User on **USERS** tab *)	**ATL_Manager**
Import Database	**Import**

*) a user is required to define the saving behavior of the DICOM server.

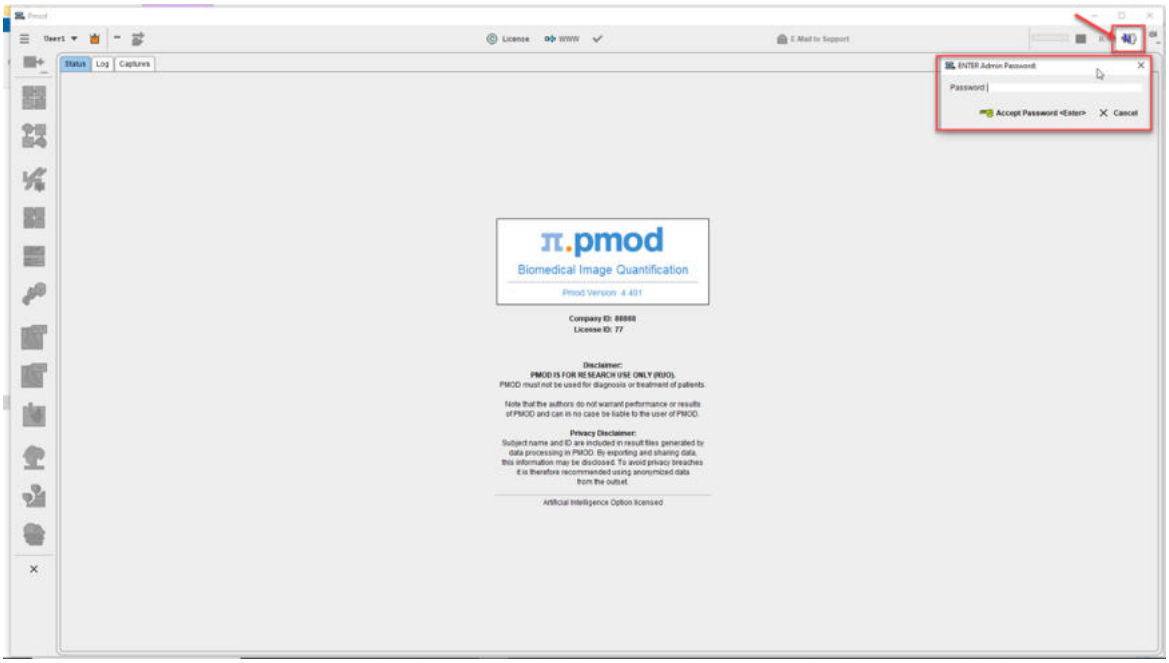
Empty overview tables are available in the Appendix 38 and can be used during the installation of PMOD ATL software.

2.2.3 Starting PMOD for System Configuration

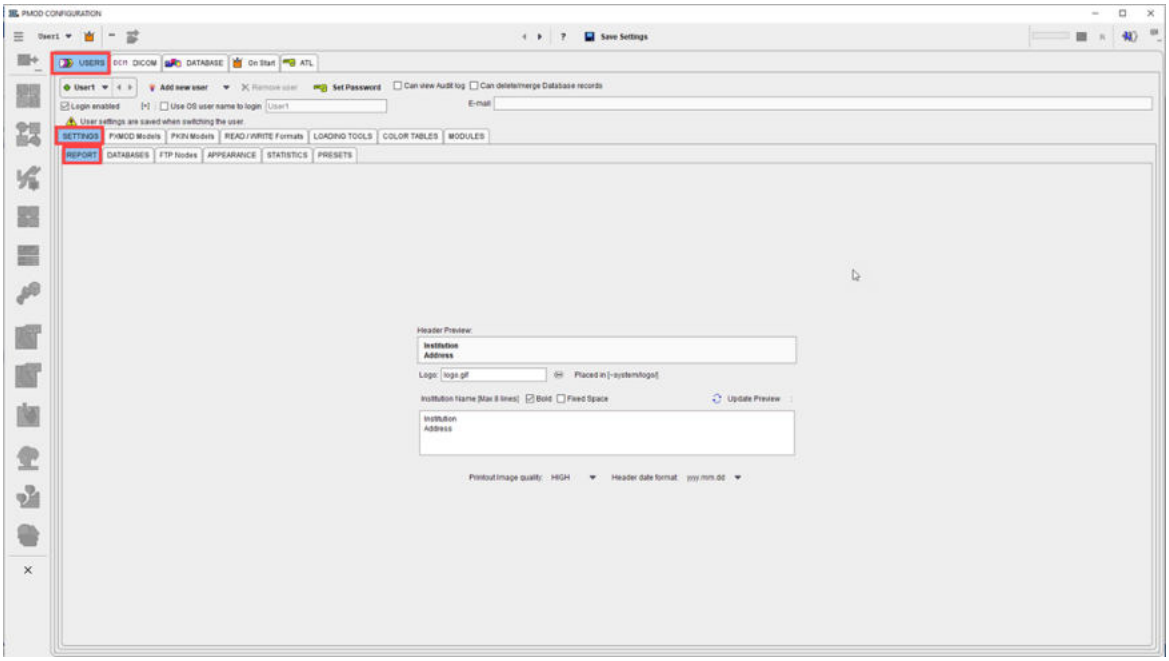
After the installation, start PMOD using the RunPmod script in the *Pmod4.4/Start* directory. As per default there is a single PMOD user "user 1" configured, automatic sign-on proceeds and prompts for a password. Please **Cancel** this window **ENTER User [user 1] Password:**



and enter the configuration by the **Configuration** icon in upper right corner as illustrated below:

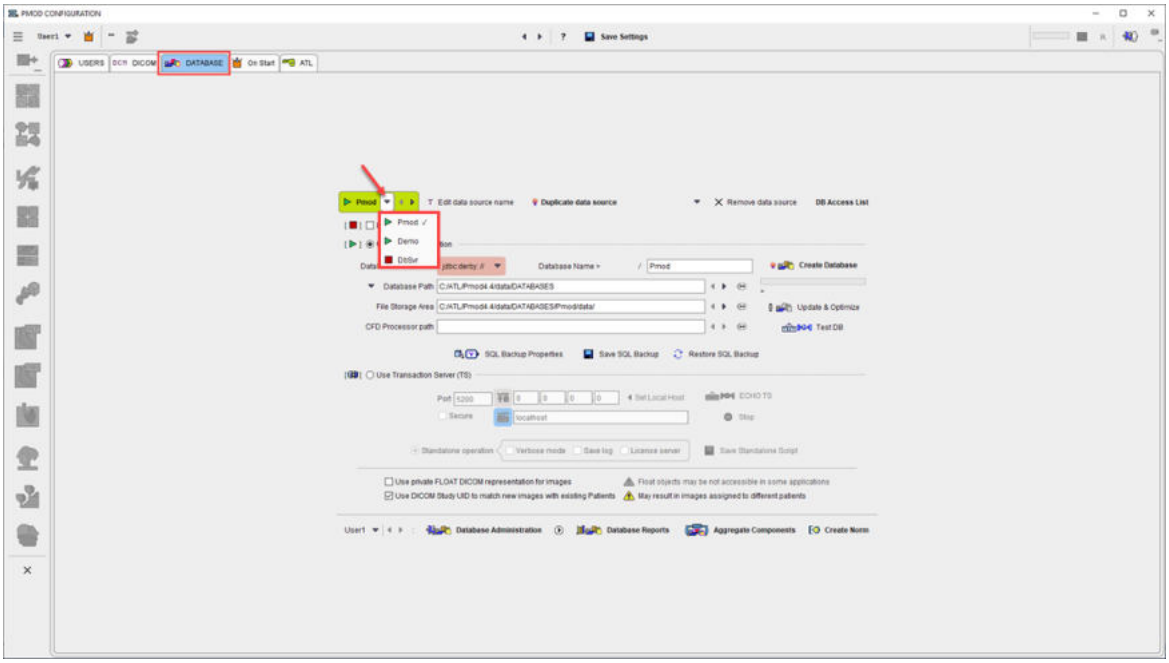


The system prompts for the initial administrator password which can be found in the delivery notes. After entering the correct password, the configuration window appears.



2.2.4 System Configuration

Select the DATABASE tab. From the initial PMOD installation there will be configured an empty database **PMOD,** an example data sources **Demo** and a database server **DbSvr**. To see the list select the down arrow as indicated in the illustration below.



It is recommended to remove the **Demo** and the **DbSvr** data source. To this end select the **Demo** data source and then activate **Remove data source**. Repeat the procedure for the **DbSvr** data source. Now you are ready to proceed with the configuration.

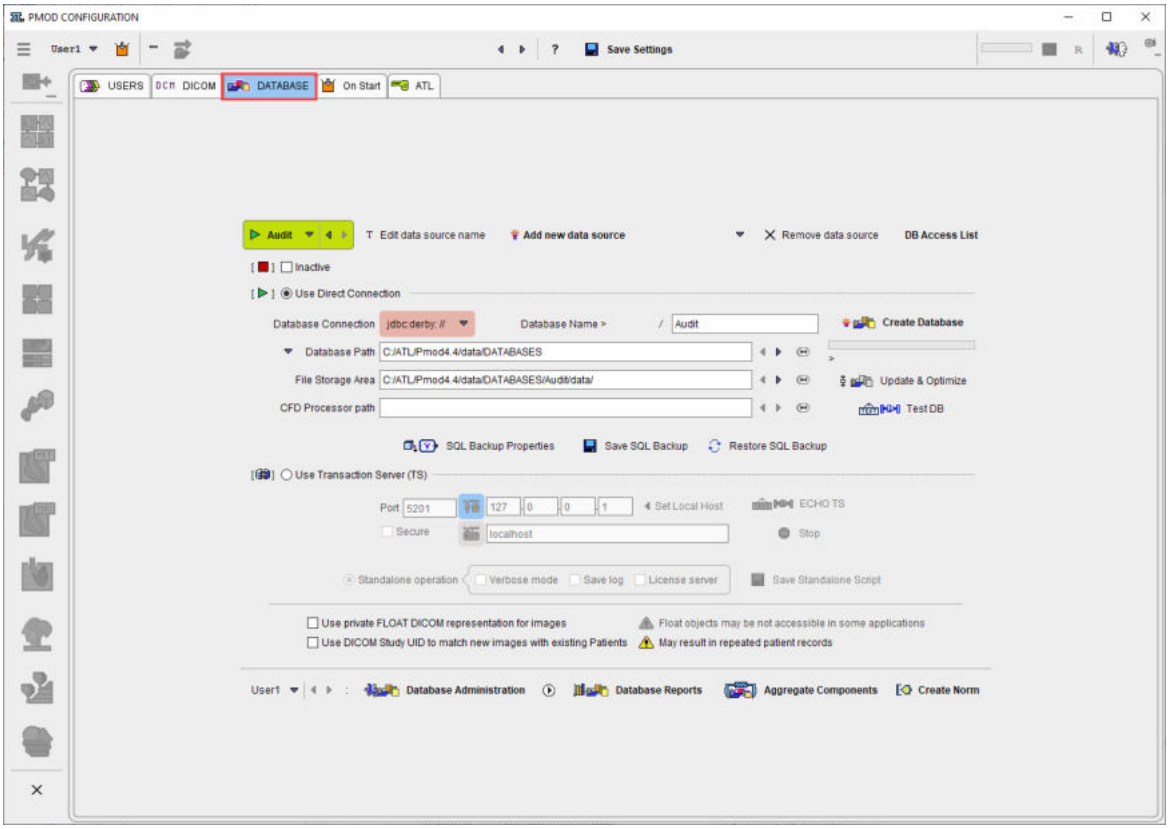
2.2.4.1 Audit Trail Configuration

The log entries which constitute the audit trail can be saved as files or in a dedicated database. However, the use of an audit trail database is strongly recommended because it offers highly flexible

filtering mechanisms for generating audit trail reports. Some users create a new audit trail database for each calendar year as a means to limit the database size.

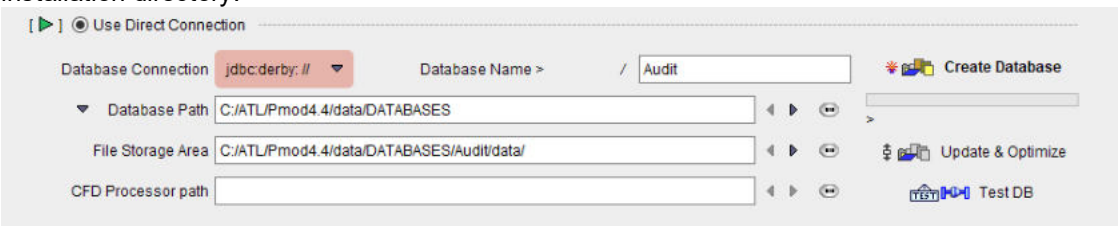
2.2.4.1.1 Audit Trail Database Creation

Select the DATABASE tab.



Perform the following steps for creating the audit trail database.

1. Activate **Add new data source** to create the data source for the audit log. In the message window enter the name of the audit trail database, in the example **Audit**. A new empty database definition is shown as illustrated below. Per default it assumes a **JDBC connection**, an embedded Java database using the driver **jdbc:derby**, and a location of the data in the installation directory.



Please refer to the PMOD Base Functionality Guide for the details about databases.

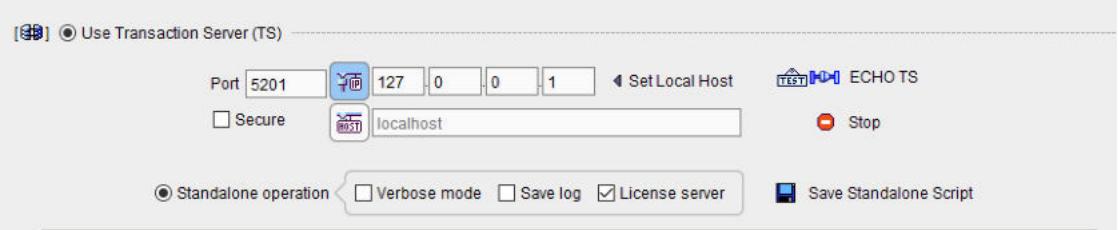
2. After the proper database configuration has been entered, activate **Create Database** to initiate the actual creation of the audit trail database. The successful creation is confirmed in a message window.

2.2.4.1.2 Transaction Server for Audit Trail and Licensing

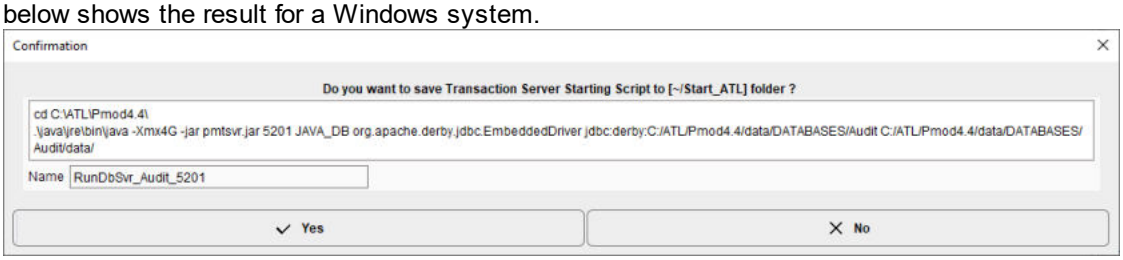
The audit trail database should be managed by a transaction server process which also acts as a license server. It should not be used to save actual data.

Perform the following steps to define the transaction server and create a script for starting the server as a process.

1. Switch the radio button from **Use Direct Connection** to **Use Transaction Server**.



2. Configure the properties of the transaction server. The **Secure** box is for enabling secure communication. This mode should be used if the communication is not confined within the institution. Otherwise it will slow down the communication speed unnecessarily.
3. An important property is the IP **Port** for the communication. It must be a unique number not used by any other transaction server or other process. The default port is **5201**.
4. Another important property is the **IP address**. It must contain the address of the host in which the servers are running, so typically the system on which the configuration is performed. For this system the IP address can be obtained by activating the **Set Local Host** button. Note that entering "localhost" in the **HOST** area will NOT work!
5. Check the box **License Server** so that the transaction server also manages the licenses. Activate the **Save Standalone Script** button. A dialog window appears which shows the contents of the created script. The script is dependent on the operating system. The example below shows the result for a Windows system.



6. Select **Yes** to save the starting script with the specified **Name** in the subdirectory *Start_ATL* of the PMOD installation directory.

Note: Do NOT switch the radio button back to Use JDBC Connection. The transaction server should run at all times so command window should remain open.

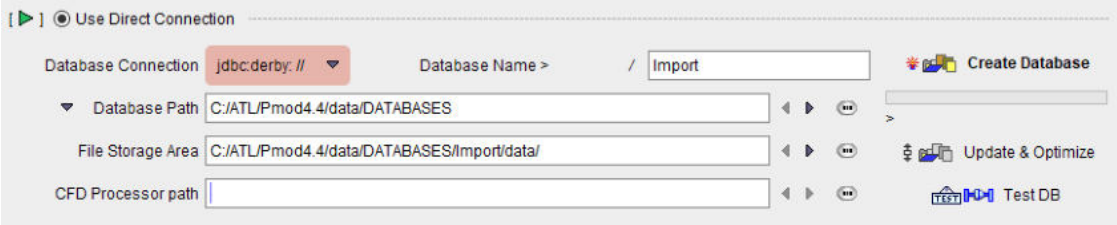
2.2.4.2 Study Database Configuration

The PMOD server can host several study databases which can be used in parallel. Initially, a database is created by the administrator in an interactive PMOD session of the server installation. From then on, all accesses to the database are serviced by a transaction server process which needs to be started from a dedicated script.

2.2.4.2.1 Study Database Creation

In **Users Configuration** window go to **DATABASE** tab and perform the following steps for creating the databases which are used for saving the study data. They are the same steps as for the audit trail database.

1. Activate **Add new data source**. In the message window enter the name of the database, in the example **Import** as this database will be used for data import. A new empty database definition is shown as illustrated below. Per default it assumes a **JDBC connection**, an embedded Java database using the driver **jdbc:derby**, and a location of the database information relative to the installation directory.



Please refer to the PMOD Base Functionality Guide for the details about databases.

2. The **File Storage Area** path defines where the actual data are saved. It is recommended to point this path to a fast, protected share which can not be reached by any user directly, and which is covered by a regular backup strategy.

3. After the proper database configuration has been done, activate **Create Database** to create the empty tables of database **Import**. The successful creation is confirmed.

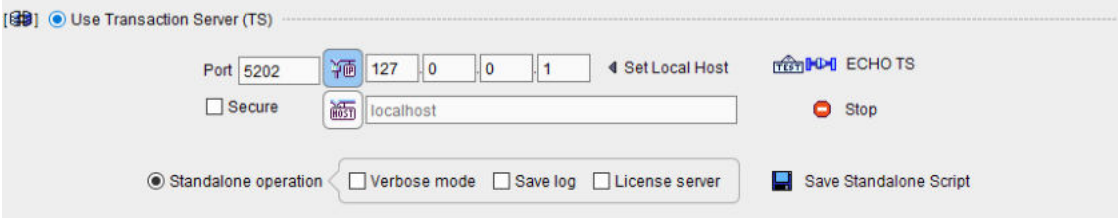
In our example the steps 1 to 3 are repeated for creating the **Import** database as well as the two study databases **Study1** and **Study2**.

2.2.4.2.2 Transaction Servers for Study Databases

Each of the study databases must be managed by a transaction server process. Please perform the following steps to define the transaction server and create a starting script for each database (in the example: **Import**, **Study1**, **Study2**).

1. Select the **Import** database in the data sources list.

2. Switch the radio button from **Use JDBC connection** to **Use Transaction Server**.



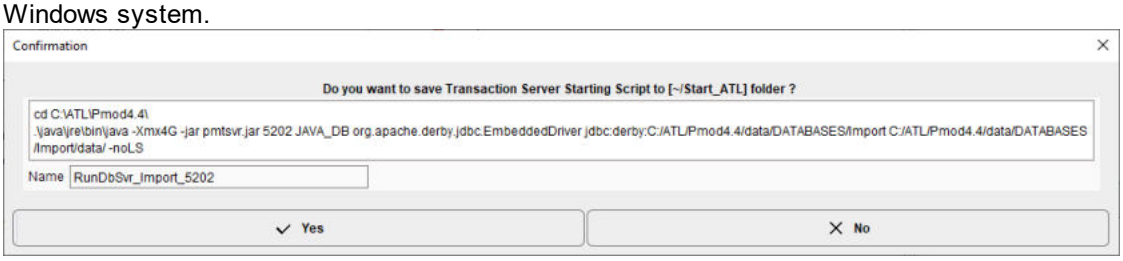
3. Configure the properties of the transaction server. The **Secure** box is for enabling secure communication. This mode should be used, if the communication is not confined within the institution. Otherwise it will slow down the communication speed unnecessarily.

4. An important property is the IP **Port** for the communication. It must be a unique number not used by any other transaction server or other process. As the default port of **5201** is already used by the transaction server for the audit trail, use the next free port **5202** for the **Import** server.

5. Another important property is the **IP address**. It contain the address of the server system which can be obtained by activating the **Set Local Host** button. Note that entering "localhost" in the **HOST** area will NOT work!

6. Activate **Save Standalone Script**. A dialog window appears which shows the contents of the created script. The script is dependent on the operating system. The example below is for a

Windows system.



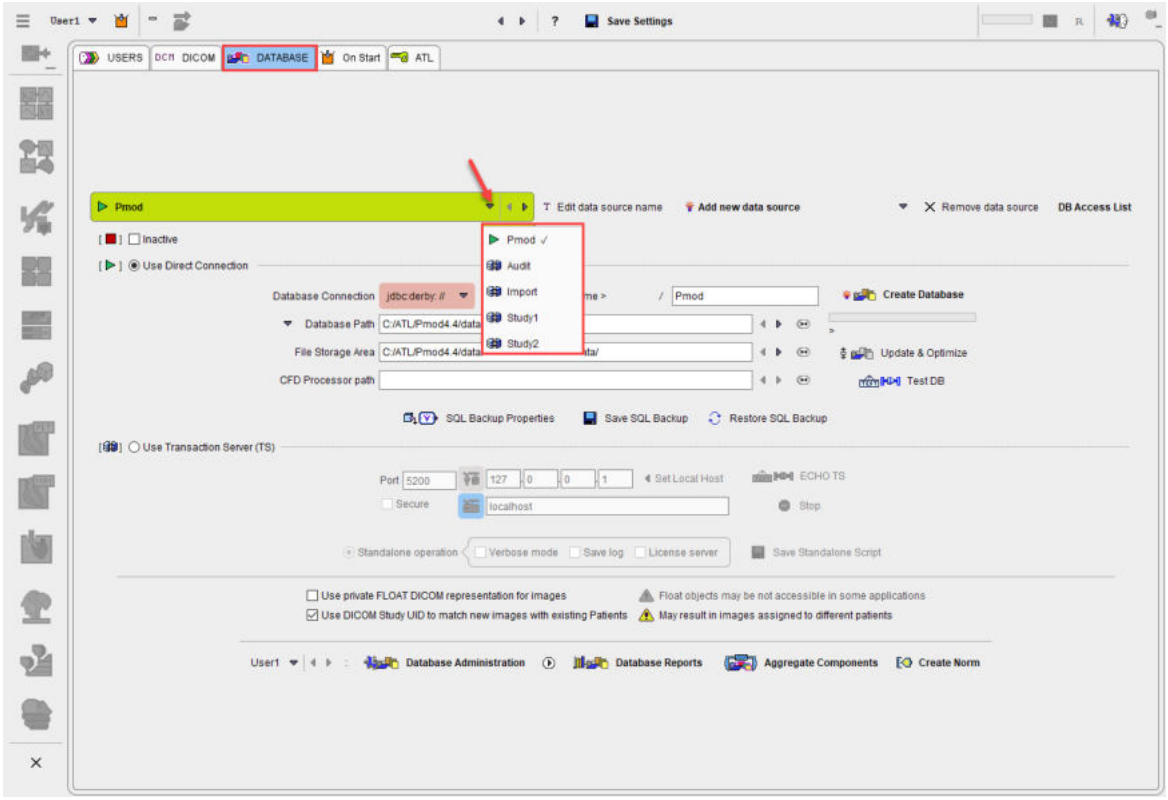
7. Select **Yes** to save the starting script with the specified **Name** in the subdirectory *Start_ATL* of the PMOD installation directory.

Repeat steps 1 to 7 for the **Study1** and the **Study2** databases using port **5203** for **Study1** and port **5204** for **Study2**.

Note: Do *NOT* switch the radio button back to Use JDBC Connection.

2.2.4.2.3 Database Cleanup

From the initial PMOD installation there will be an example data sources configured, **Pmod**. To see the list of data sources select the arrow indicated in the illustration below.

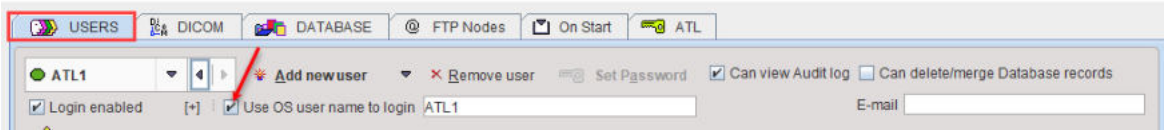


It is recommended to clean up and remove the example data sources. To this end select the **Pmod** data source and then activate **Remove data source**. At the end only the relevant data sources should be listed, each with a symbol to indicate that the database is served by a transaction server.

2.2.4.3 User Configuration

PMOD distinguishes between a privileged PMOD administrator who installs the software and configures the environment, and the PMOD users who perform the actual data analysis. The administrator has no user account. He can only open the configuration tool for administrative purposes, but not start any processing tool.

The PMOD users configuration can be performed on the **USERS** tab.

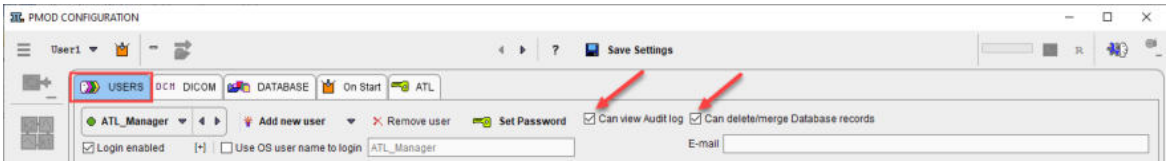


The e-mail specification is mandatory for the Project Tracker. It allows sending information about the assigned tasks to the specified user. The Project tracker documentation is under preparation..

2.2.4.3.1 User Creation

User with Data Manager Role

It is recommended to set up one or two PMOD users (with or without OS login) who have rights to all the databases, including deleting permission. In our example we create a local user called **ATL_Manager**.



Please perform as follows:

1. Select the **Add new user** button to create a new user entry.
2. Edit the name under which the user will be known to PMOD, **ATL_Manager**.
3. Leave the **Use OS user name to login** unchecked.
4. Define the initial password of the user with the **Set Password** button. The password is encrypted and saved in */properties/global.start*

PMOD Users without OS login

The recommended way for setting up PMOD users is to define users which are authenticated by a password maintained within PMOD. In this case the user definition is done as follows:

1. Select the **Add new user** button to create a new user entry.
2. Edit the name under which the user will be known to PMOD, eg to **ATL2**.
3. Leave the **Use OS user name to login** unchecked. This user will have to be authenticated by a password in PMOD.
4. Set the initial password of the user with the **Set Password** button. As with the administrator password, it is encrypted and saved in */properties/global.start*

PMOD Users with OS Login

As an alternative it is possible setting up PMOD users identification based on the the operating system user name login. In this case the user definition is done as follows:

1. For the first user it is recommended to keep the default **user 1** entry. For the other users please activate the **Add new user** button to create a new user entry.

2. Edit the name under which the user will be known to PMOD, eg to **ATL1**. This name will be used in the Audit Log.
3. To make this a PMOD user who is identified through his OS login, check the **Use OS user name to login**.
4. Enter into the text field to the right the exact name as used by the operating system, in the example **ATL_User1**. Note that the PMOD user name and the OS name are completely independent, but it is recommended to maintain a reasonable agreement between them. As a hint, the OS name of the user who started PMOD is shown in the terminal window.

User with Extended Permission

Per default, PMOD users have very restricted rights. However, deleting may be required sometimes in a controlled manner. Therefore it is possible to assign to dedicated users extended permissions, but still not with full administrator permissions. The following options are available:

- **Can delete/merge Database records**: With this box checked, the user can delete/merge from the databases to which he is entitled.
- **Can view Audit log:** With this box checked, the user can inspect the current audit log from the PMOD ToolBox. Users which have access to the Audit log can access also the Project Tracker (PT) on the Pmod Toolbox.

2.2.4.4 DICOM Server Configuration

Currently, there are four methods to import DICOM image data into a study database.

1. The PMOD user loads images from disk or CD files and saves them to a study database. This has the advantage, that the user will be listed as data creator in the database. However, be aware that the images in the database will not be the original image data, but objects created by PMOD.
2. The original images are sent to a PMOD DICOM server, which saves the images to a dedicated database. This has the advantage, that the original image data are saved without any modification. However, the DICOM server will be listed as the data creator, so there is no identification possible who introduced the data.
3. Images are dropped into a dedicated directory which is regularly scanned and the data imported into a database. This is a variant of the DICOM server solution and has the same advantages and disadvantages.
4. The data are brought into a database by replication from another database. In this case the user who initiates the replication will be listed as the data creator.

Data Import Recommendation

The following organization is recommended:

1. The dedicated **Import** database is used as an intermediate data pool from which the data are further distributed to the actual study databases.
2. A PMOD DICOM server process is established which is able to receive image data per DICOM network protocol and saves all received images as original data to the **Import** database.

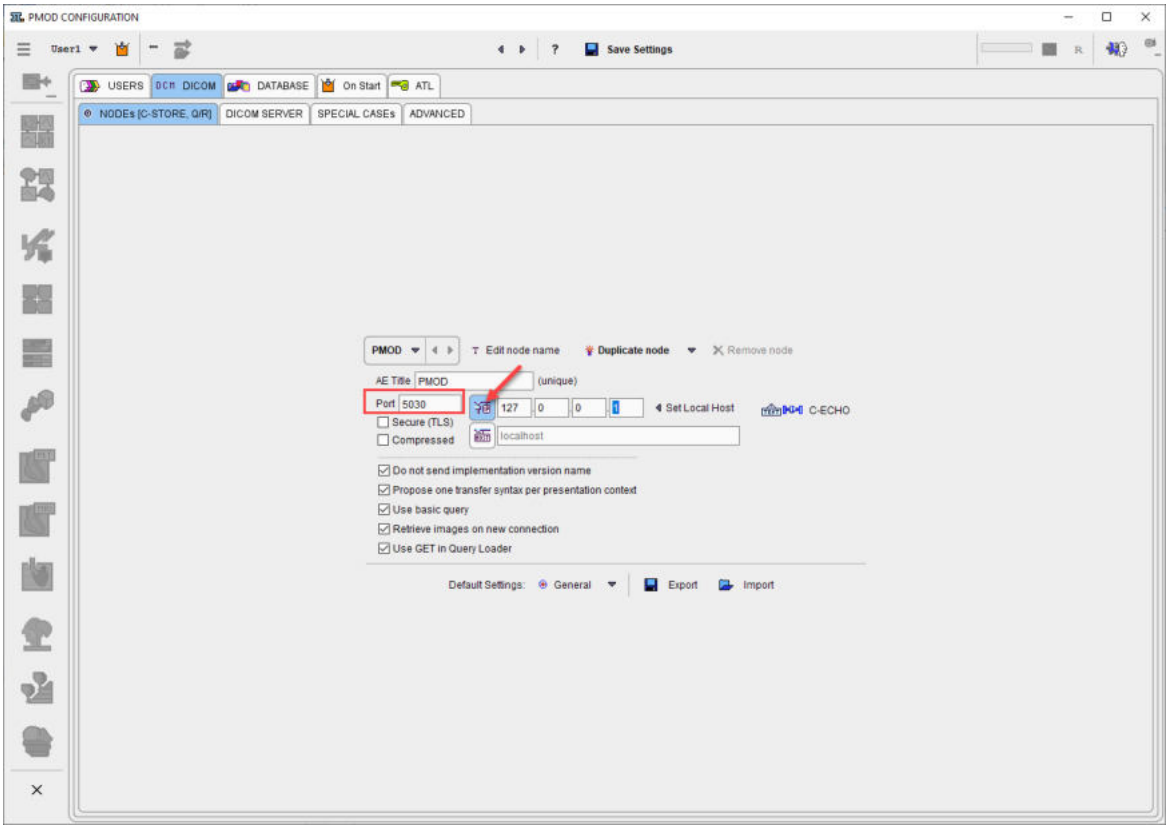
3. The dedicated PMOD user **ATL_Manager** is given access rights to the **Import** database and all study databases. This user is in charge of moving the received image data to the appropriate study databases, ending up with the original images.

The sections below describe the configuration of the DICOM Client and of the DICOM server to implement this organization.

2.2.4.4.1 DICOM Client Configuration

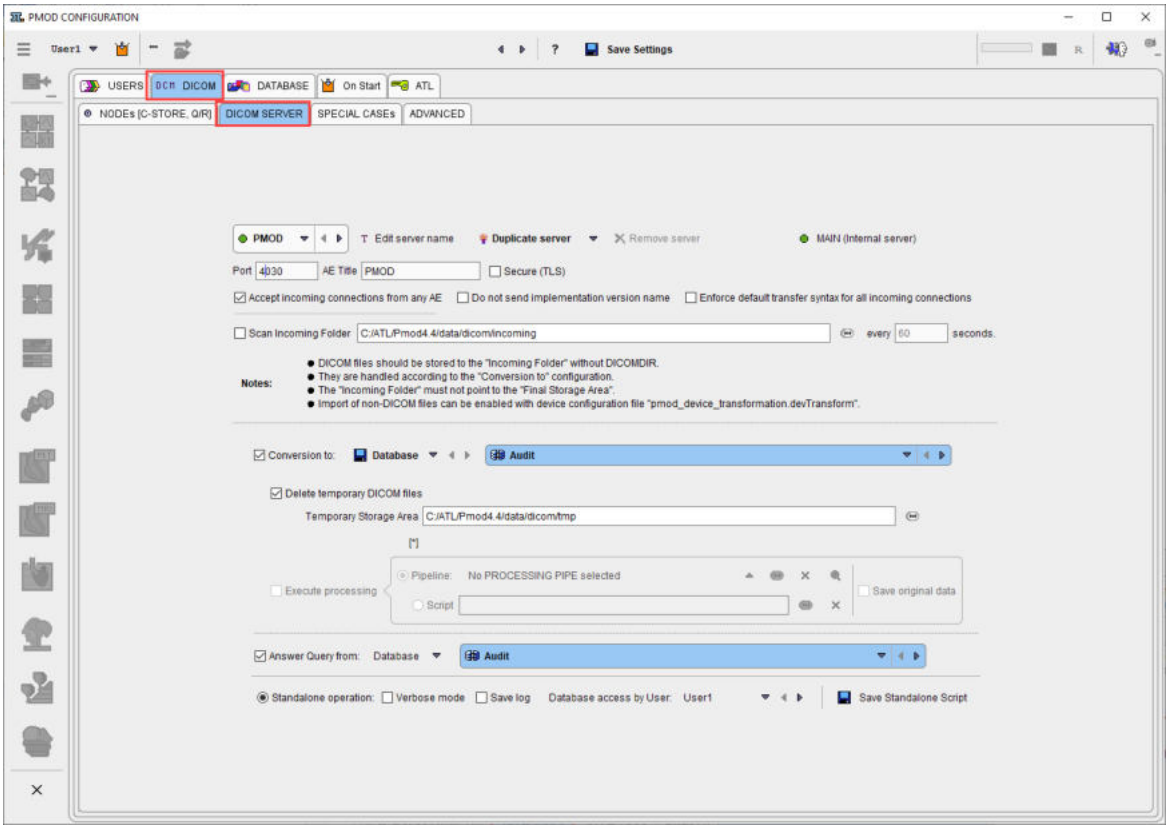
To import data into the ATL system, DICOM clients need to be configured which can send the original study data to the PMOD DICOM Server. In such a client, the PMOD DICOM Server has to be appropriately configured.

The configuration should also be done in the ATL Server configuration as illustrated below. In the **NODEs** panel of the **DICOM** panel, enter the **AE Title**, the **Port** number, and the server **IP** address exactly as in the DICOM Server configuration 18. This configuration will allow the easy import of DICOM data by all PMOD clients as discussed below.



2.2.4.4.2 DICOM Server Definition

To configure the DICOM server please select the **DICOM** panel of the configuration window and select the **DICOM SERVER** tab.



The DICOM server of a particular system is defined by two entities, the:

- **Port** number on which the server is listening,
- **Application Entity Title** (AET) which has been given to the server.

Note:

On Linux systems there exist reserved ports which require special permission to allocate. If such a port is defined as the PMOD DICOM server port, the server cannot be started from a user account and issues a message *Permission denied*. Starting as root will normally succeed, but this has the disadvantage that the saved files will all belong to the root. To prevent this situation a higher port number (typically >4000) should be used on Linux, rather than the default DICOM port 104.

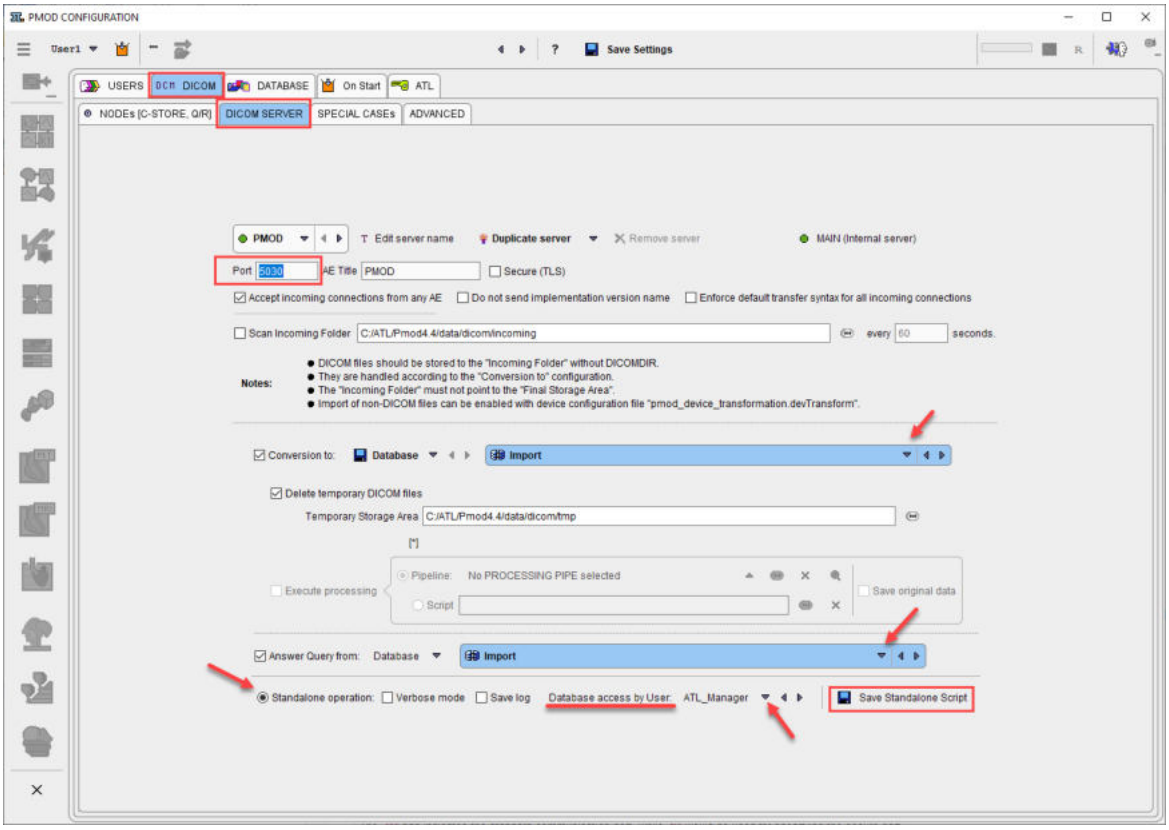
Please note that in PMOD ATL example we are using port number 5030 not default 4030.

Besides the basic server information there is an additional check relevant for the DICOM server operation: **Accept incoming connections from any AE**. If it is checked, any association request will be accepted, so images will be received from any system, otherwise only from known systems. Note that as long as the sending node is not configured, it will not be able to retrieve images from the PMOD DICOM server.

DICOM Server Saving Definition

There is still one configuration missing for the DICOM server, namely what he has to do with the received data. This can be done as follows in the same panel as above. Make sure that for Database access by user **ATL_Manager** user is selected from the list. Then select on the **DICOM** tab the **DICOM SERVER** panel as illustrated below.

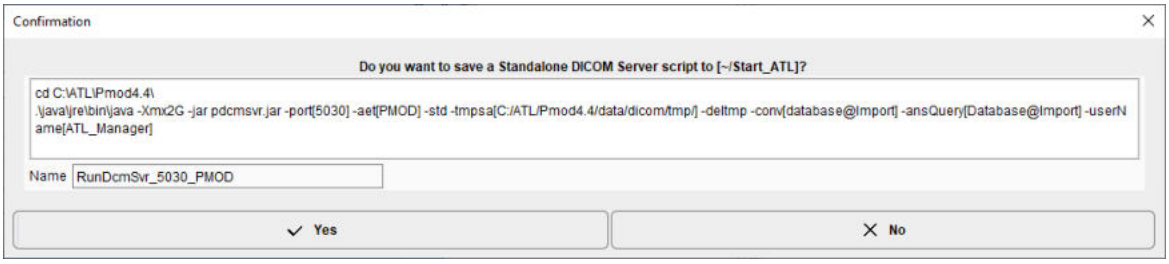
Make sure that the **Conversion to** box is checked, the format is set to **Database**, and the **Import** database is selected. With this configuration the original DICOM data will be added to the **Import** database.



The **Answer Query from** box can be deactivated to disallow remote querying. In the example above querying will be allowed to the **Import** database.

Script for DICOM Server

The **Save Standalone Script** button serves for generating a starting script for the DICOM server with the defined configuration and definition. It shows a dialog window where all the above settings and definitions are summarized. The script content is shown, and can be saved in the *Start_ATL* folder within the *Pmod4.1* directory by the **Yes** button under a given **Name**.



The **-std** flag indicates the standard communication port, while **-tls** would be used for specifying the secure port.

2.2.4.4.3 Advanced DICOM Server Options

Support for Secure DICOM

Standard DICOM communication is not secure, and therefore is not recommended over public networks. To overcome this problem, a DICOM supplement has been finalized which allows implementing secure connections. PMOD supports one of the proposed variants called BASIC TLS SECURE TRANSPORT CONNECTION PROFILE. Of the three optional features (entity authentication, encryption, integrity check) encryption is implemented in the current release. As a

consequence, the data transferred can only be interpreted by the target DICOM server with which the communication has been established.

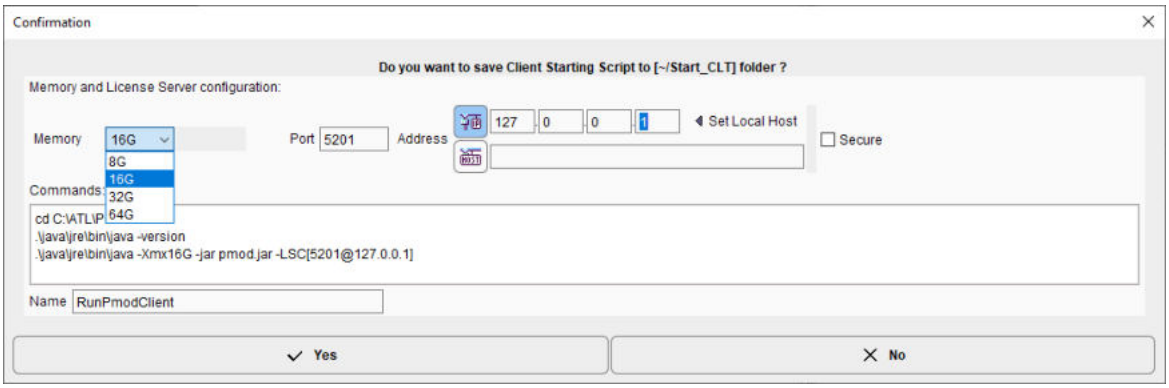
The PMOD server may be configured to accept secure and insecure connections at the same time on two different ports. One port is designated for standard TCP/IP connection and the other for secure TLS connections. To enable secure DICOM, enable the **Secure (TLS)** checkbox, define a port number, and the AET.

DICOM Import from Directory

Normally the DICOM server is receiving data over the network from DICOM clients. However, it is also possible to have the DICOM server scan a directory and treat found DICOM series in the same way as if they had arrived by the network. This functionality can be configured by the **Scan Incoming Folder** box. If it is checked, the directory to be scanned can be entered as well as a scanning interval **every ... seconds**. This import feature can be used to add DICOM images to a PMOD database. Note that after processing the images by the DICOM server they are removed from the incoming folder.

2.2.4.4.4 Client Script Generation

The clients will use a script to start PMOD wherein the license server must pe properly specified. The client script can be generated with the **Save Client Starting Script** button on the **ATL** tab. It opens a dialog window as illustrated below.



The transaction server **Port** and **Address** should already correspond to the ones configured for the Audit trail license server. In addition, the amount of RAM to be used by the client is available for configuration under the **Memory** selection. Note that the allocated memory cannot be bigger than the physical RAM available on the client system.

It is however recommended to make sure the correct properties of the license server are configured:

1. **Address:** It must contain the address of the server system, which can be obtained by activating the **Set Local Host** button. Note that entering "localhost" in the **HOST** area will NOT work!
2. **Port:** It must contain the port number of the transaction server which was configured as the license server 13, in the example **5201**.
3. Transfer syntax: The **Secure** box must be configured exactly as for the license server.
4. Memory configuration: must be lower than the physical RAM available on the client system.
5. Select **Yes** to save the starting script with the specified **Name** in the subdirectory *Start_CLT* of the PMOD installation directory.

A confirmation message is shown which reminds the user that some information in the script may be edited once the client system is configured.

2.2.4.5 Administrator Password Change

The administrator password should be changed. This can be done on the **ATL** tab using the **Change Pmod's Admin Password** button. Upon exit the new password is stored in an encrypted form in the */properties/global.start* file.

If there is a need to reset the administrator password to the initial one, please remove the line starting with ADMIN_PSWD in *global.start*.

2.2.5 Starting of the Servers

At this point of the configuration the transaction servers and the DICOM server can be started. Please close the PMOD **Users configuration** window with **Ok**, and stop PMOD by selecting **Quit** from the ToolBox.

Start the transaction servers using the scripts which can be found in the *Pmod4.3/Start_ATL* sub-directory. This can be done by double-clicking the script files, or by opening a command window per server and entering the complete name of the script.

1. **RunDbSvr_Audit_5201**: Starts the transaction server for the **Audit** database and license server functionality.
2. **RunDbSvr_Import_5202:** Starts the transaction server for the **Import** database to which the DICOM server will save.
3. **RunDbSvr_Study1_5203, RunDbSvr_Study2_5204**, etc: Start the transaction servers for the databases configured for studies 1 and 2.
   Similarly, start the transaction server for all other study databases.

Note: Per default the output of the transaction servers is shown in the respective terminal windows. To redirect the output to a file please add the -o argument to the end of the command in the starting script.

Then start the DICOM server double-clicking the script **RunDcmSvr_5030_PMOD** which was saved in the *Start_ATL* directory.

Important Note: After the initial server configuration and starting of the transaction and dicom servers the *RunPmodClient.bat* script should be used both for normal work and administrative tasks. Please remember that before using the server script *RunPmod.bat* in the *Start* directory all clients should be switched off (single user environment). All transaction and dicom servers should be restarted after any administrative changes on server.

2.2.6 Database Access Rights

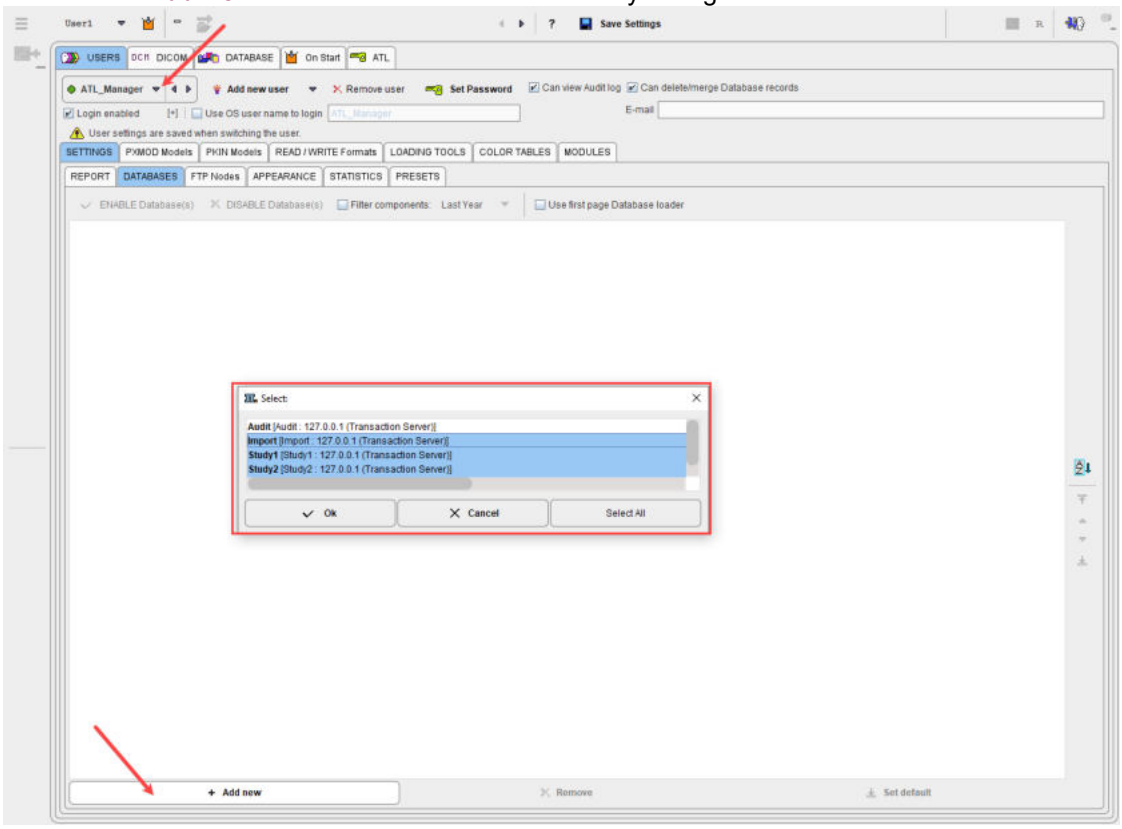
To define database access for the users, please start the PMOD using the *RunPmodClient.bat* in the *Pmod4.1/Start_CTL* sub-directory, and enter the **Config** menu with the administrator password.

Enabling Database Access for a User

The administrator has to explicitly configure all databases to which a PMOD user has access. This is done on the **USERS** panel:

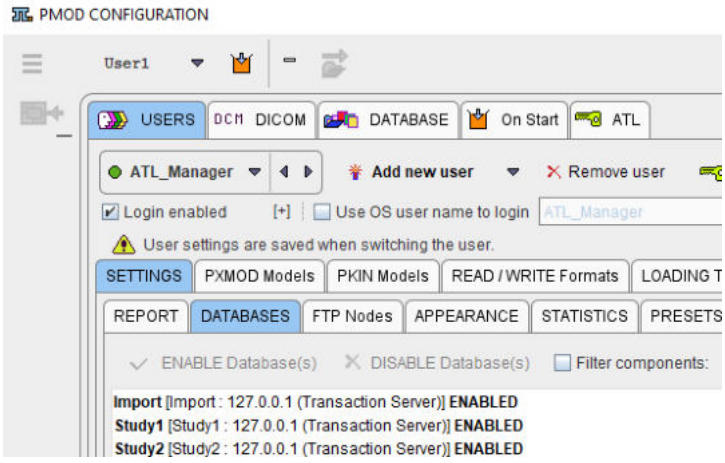
1. Select the user, in our example the **ATL_Manager**.
2. Select the **DATABASES** tab in the **SETTINGS** panel.

3. Activate the **Add new** button to see the list of currently configured databases:



Select the relevant study databases and close with **Ok**.

4. As a result, the databases to which the user has access are shown in the list with the **ENABLED** mark.

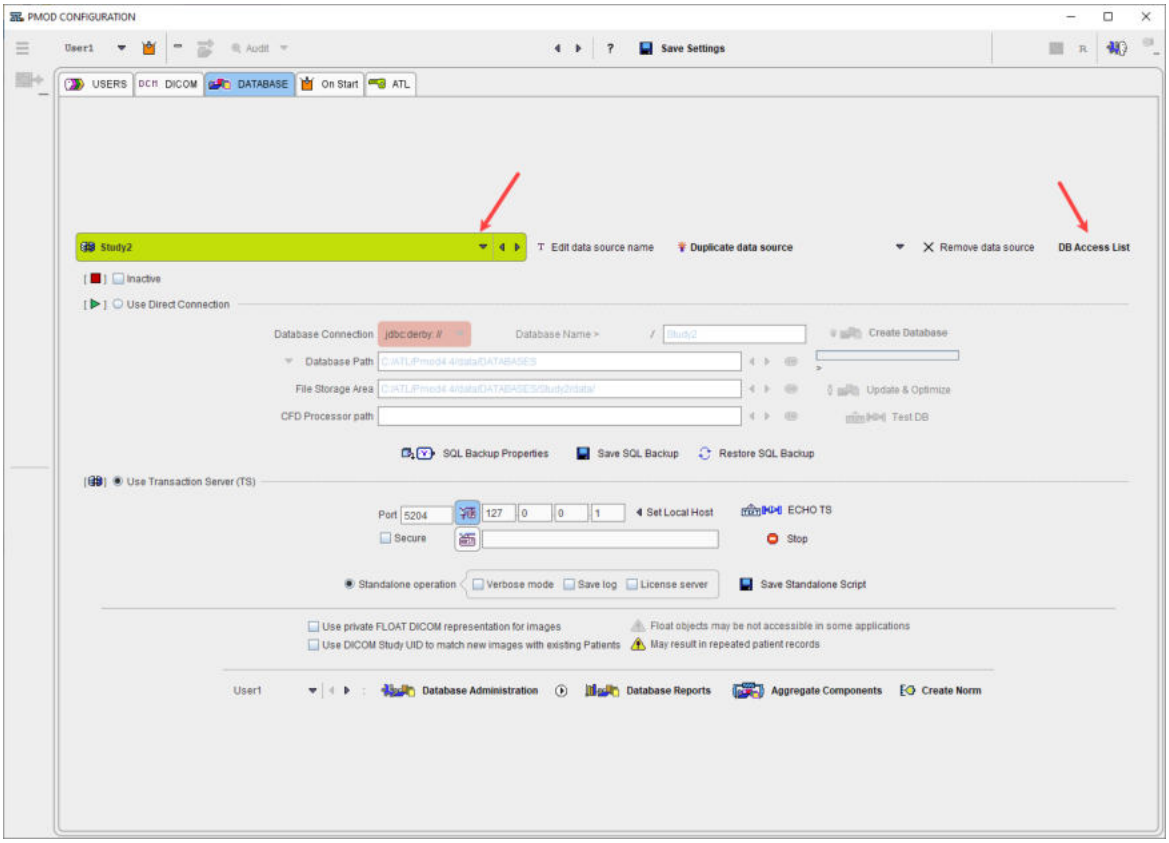


For the user **ATL1** enable the **Study1** and **Study2** databases, and for **ATL2** only **Study2**.

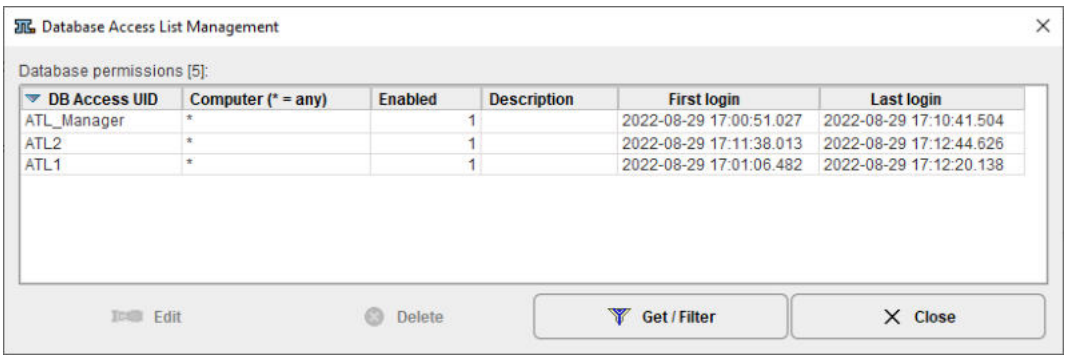
Database Access List

For each database, a user access list is maintained. This list is synchronized with the configuration described above, but provides some more detail.

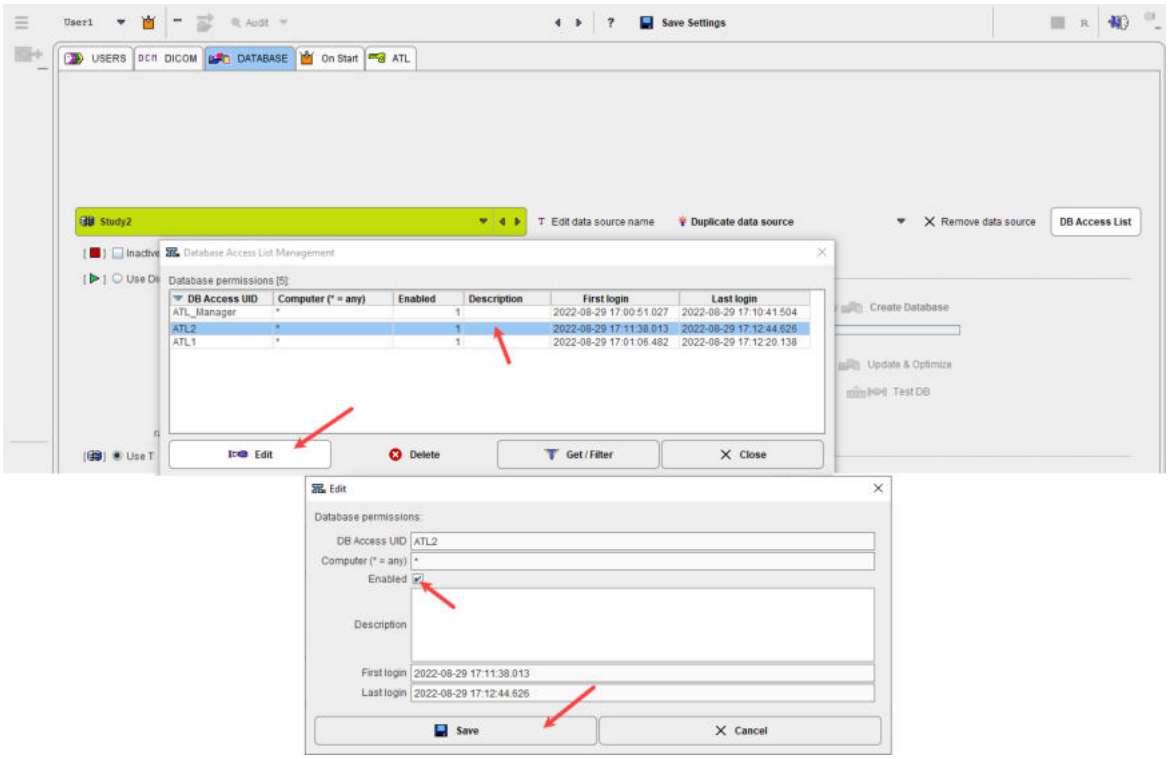
To see and edit the database access lists select the top **DATABASE** tab of the configuration then the **DB Access List** button near the data source creation/removal. It shows a dialog window as illustrated below.



The **DB Access UID** contains the name of the PMOD user. The **Computer** column shows the systems from which the user can access the database. If the "*" is shown, user access from all client systems are allowed. It can be restricted by replacing * by a computer host name. A value of **0** in the **Enabled** column indicates that the user has no database access, whereas **1** indicates enabled access. The **Description** is a convenience field which can be edited by the administrator for commenting purposes. **First login** and **Last login** give some information about the activity of the user.

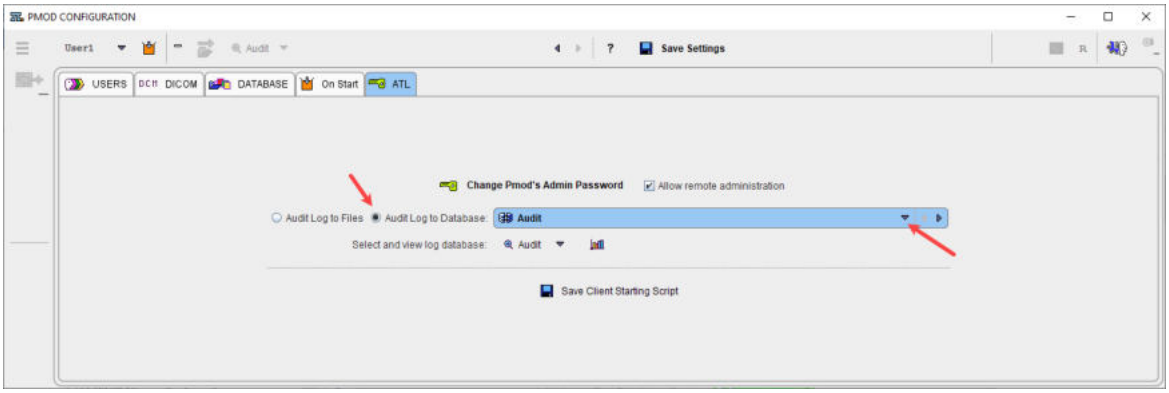


The **Edit** button serves for editing the selected access list entry as illustrated below. For instance, by removing the **Enabled** check, the user **ATL2** can be blocked from the selected database.



2.2.7 Audit Trail Configuration

The last step for the audit log configuration is the assignment, where the audit log output is saved. Select the **ATL** tab of the **Users** configuration window opened.



To use the database for the audit log select **Audit Log to Database**, and chose the prepared **Audit** entry from the list of currently available databases. As an alternative, with the **Audit Log to Files** configuration, the log information will be saved in to user-specific text files.

At this point only PMOD (not the transaction servers and DICOM server) should be restarted after closing the **Users configuration** window with **Ok** and quitting the ToolBox.

2.3 Client Installation

The clients will run PMOD locally. In contrast to a standard PMOD installation, they will not use the local properties, but retrieve the dedicated properties of the user at login.

If all the clients are homogeneous, i.e. using the same operating system, it is recommended setup a single PMOD client installation on a share which can be reached by all clients and is mounted in the same manner so that they can use the same starting script.

If all the clients are not homogeneous, they require an individual setup because of the differing Java environment.

Homogeneous Client Environment

Please proceed with the client configuration as described below. For the explanation it is assumed that the installation is performed on the common share *P:\ATL-Client*.

In a first step install PMOD with a suitable Java environment.

1. On a PMOD Client system, start a PMOD installation from CD.
2. Point the installation directory to **P:\ATL-Client**.
3. Enable only the item **PMOD Software**, and disable all other items.
4. Complete the installation without importing properties.
5. Remove all scripts in the *Pmod4.4\Start* directory

Note: Do NOT copy the license file to the client installation.

In a second step tailor the client starting script.

1. Copy the client starter script *RunPmodClient.bat* from the *Start_CLT* directory on the server to the *P:/ATL-Client/Pmod4.4/Start* directory.
2. Then edit *P:/ATL-Client/Pmod4.4/Start /RunPmodClient.bat.* The part which has to be edited is the path of the installation as it will be seen from the client systems. Also, the maximal allocated memory may be increased from 16000MB for example to 20GB (-Xmx20000M or -Xmx20G) for a system with 24GB pf physical RAM available.

```
cd P:\ATL-Client\Pmod4.4\
.\java\jre\bin\java -version
.\java\jre\bin\java -Xmx20000M -jar pmod.jar -LSC[5201@127.0.0.1]
```

Now the client script can be tested. After a certain time, the PMOD toolbox should appear.

Heterogeneous Client Environment

If the client systems have differing operating systems, a common installation is not possible. In this case a local installation per client should be performed and configured as described above. The only difference is that the common share path *P:\ATL-Client* is replaced by a local directory.

3 Maintenance Operations

3.1 Stopping/Starting of the Servers

Server Stopping

To ensure proper shutdown each server should be stopped with Ctrl+C signal (closing terminal can break onging operations). For instance, the DICOM server will continue until the last image of a data transfer has been received.

If for maintenance reasons the servers have to be stopped the following order is recommended:

1. Stopping the DICOM server and waiting for its termination, so that received images can yet be announced to the database.
2. Stopping the study database transaction servers using Ctrl+C.
3. Stopping the audit trail and license server.

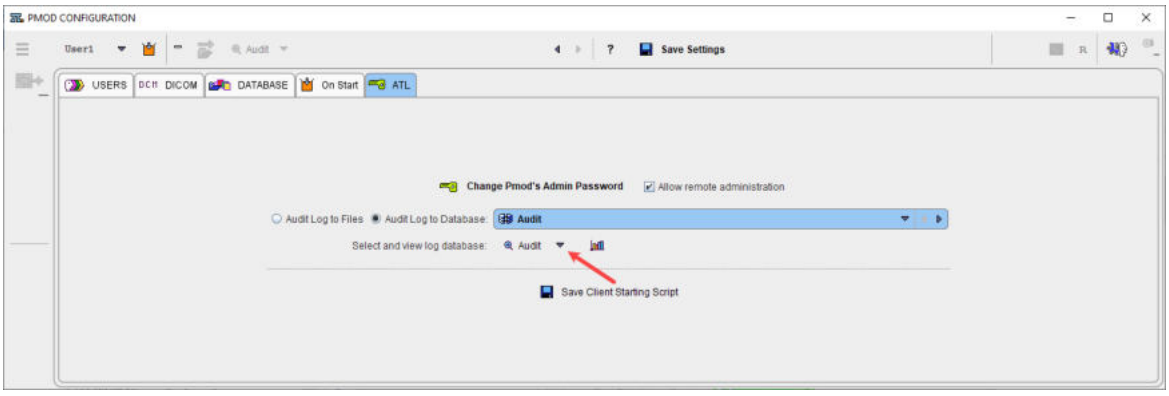
Server Starting

After maintenance it is recommended to start the servers with the scripts in the *Start_ATL* folder in the following order:

1. Start the audit trail and license server.
2. Start the study database transaction servers.
3. Start the DICOM server.

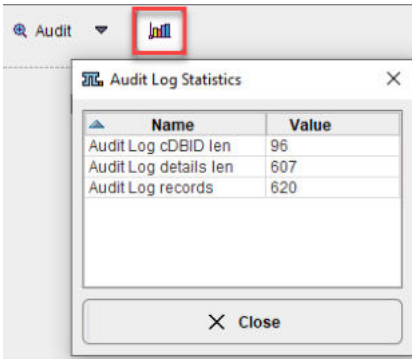
3.2 Audit Trail Inspection

The audit trail can either be inspected from the ToolBox, or from the **ATL** tab of the **Config** Window.



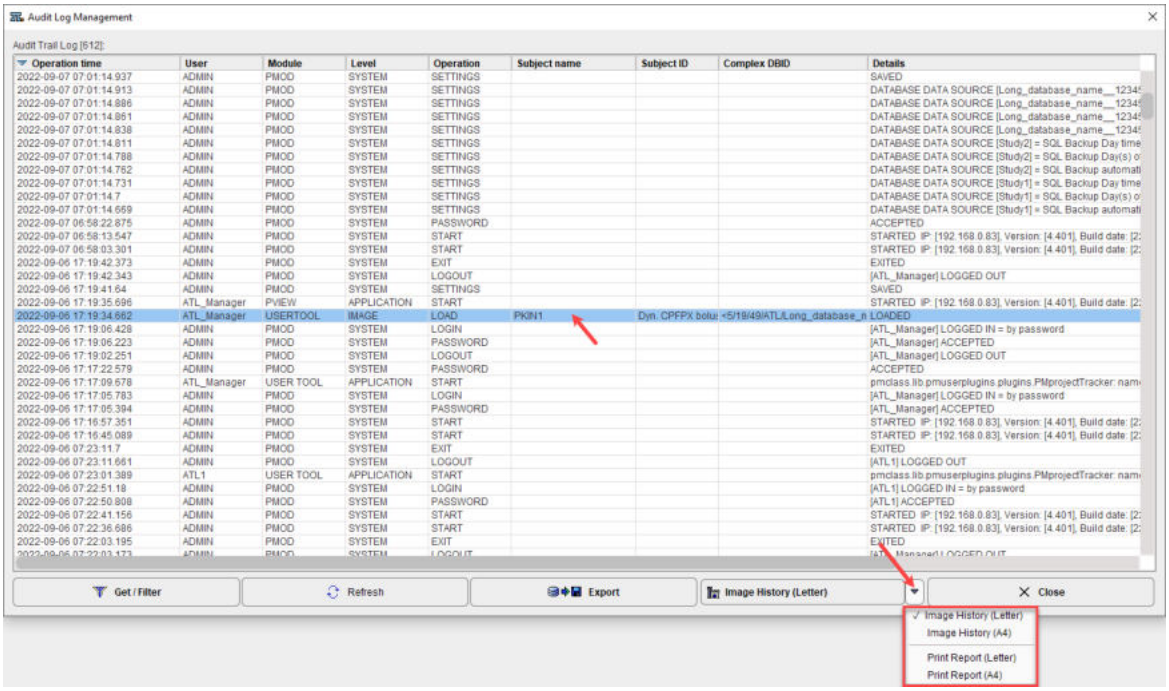
In both cases there is a selection to switch between different Audit trail databases. For instance, an institution could use annual Audit databases. For each year it would create a new database, and then switch logging to this new database. With the switch above, the administrator can inspect the current Audit database, but also the old ones.

The advantage of the **Config** window is that an **Audit Log Statistics** is available for the selected Audit database:

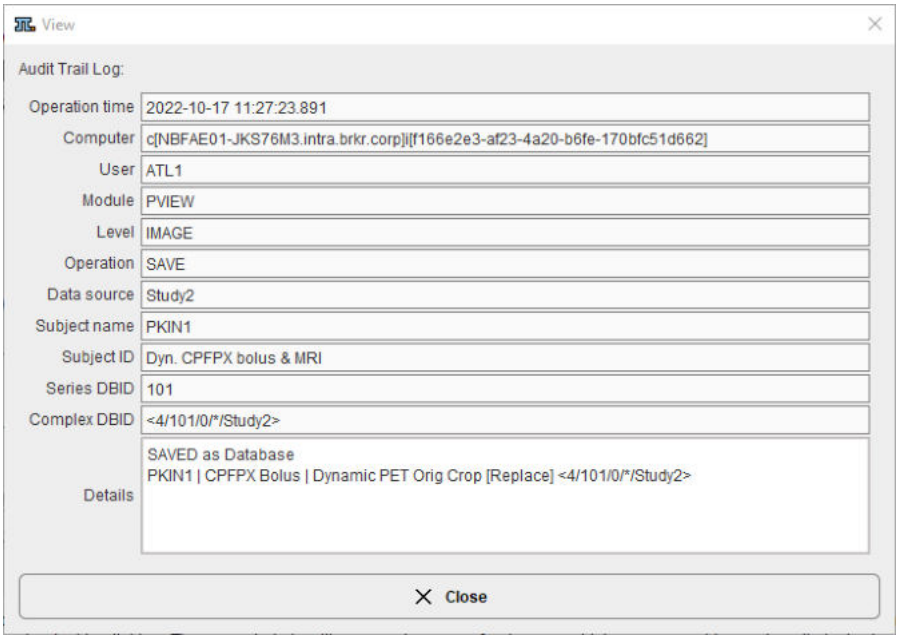


Audit Log

Activating the **View Audit log** button opens the **Audit Log Management** as illustrated below.

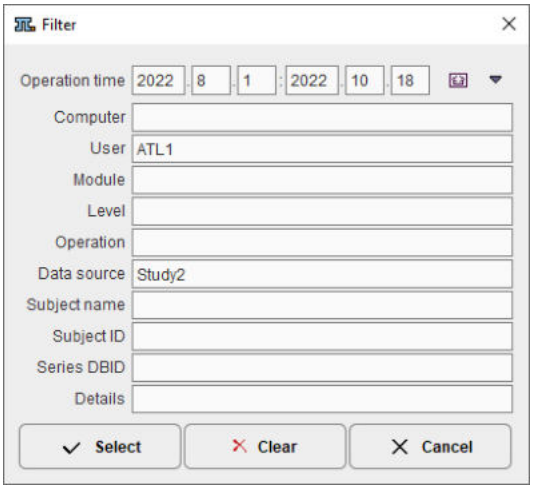


Each relevant event generates one or more entries in the Audit log. For instance, when the VOI statistics are saved the system saves the VOI definitions also and logs this action. Similar, the transformation is saved when matched image is saved. The details of a log entry can be seen by double-clicking. The example below illustrates the entry of a data set which was created by setting all pixel values below zero by zero.



Audit Trail Report

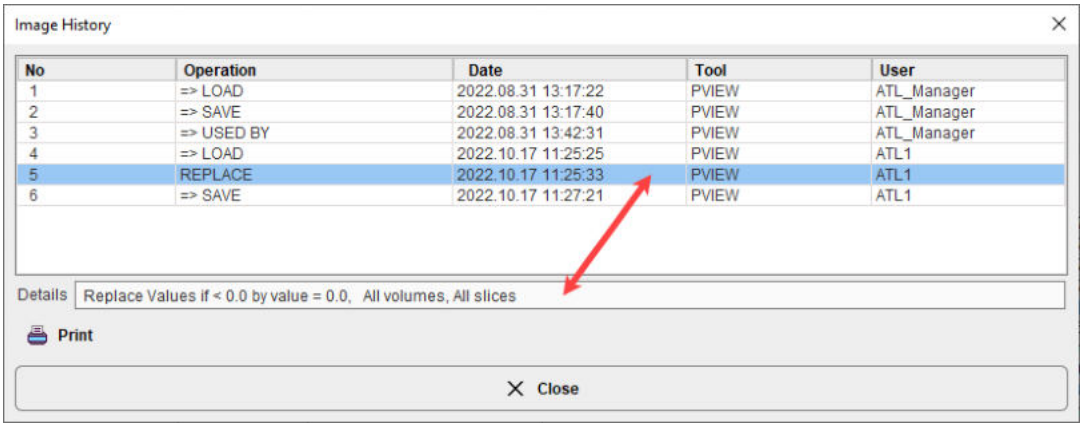
The first task for creating a meaningful audit trail report is defining an appropriate filter so that only relevant information will be listed. The filtering criteria can be changed with the **Get/Filter** button. After setting the filter as in the example below, only the operations of user **ATL1** in the **Study2** database will be shown in the list.



Once the list has been filtered, it can be printed as a report with the **Print Report** button, either with the **A4** or the **Letter** format. For reasons of performance, the maximum number of print pages is restricted to 100.

Image History

When an **IMAGE** (Level) **SAVE** (Operation) event is selected in the list, the **Image History** button becomes active. It can be selected to show the entire history of this saved data set, for example:



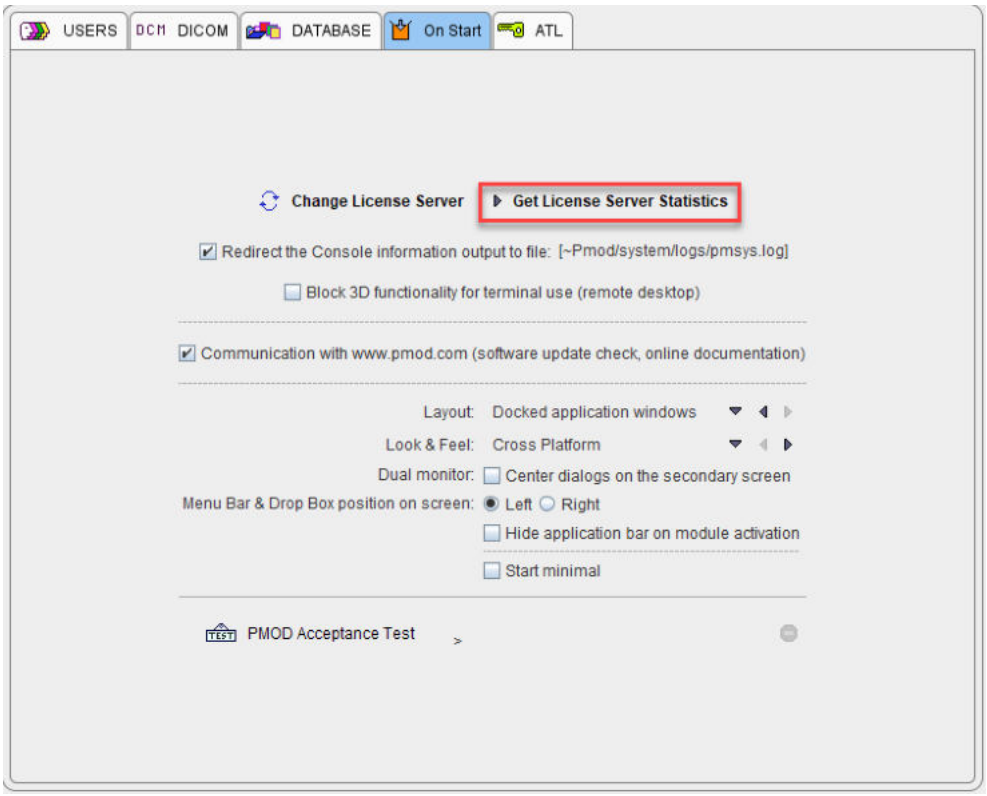
The detail information of an operation can be seen in the **Details** area after clicking at an operation. The **Print** button allows printing the history as a report wherein the operation details are listed.

3.3 Annual Maintenance

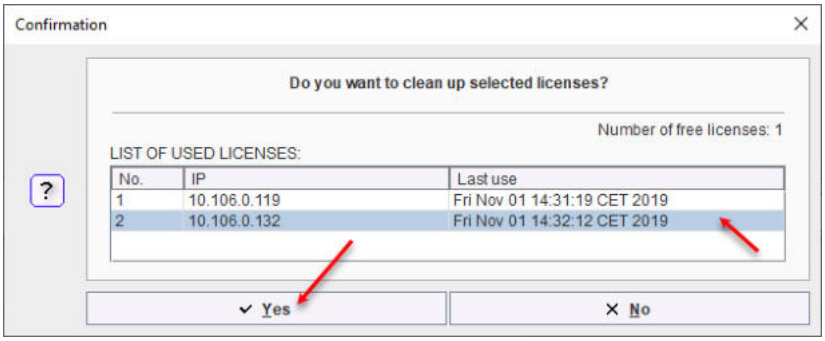
It is recommended to create a new, dedicated database and switch audit trail log to it each year.

3.4 Licenses Control

The license usage is available for inspection on the **Users Configuration** window, on the **On start** tab:



The activation of the **Get License Server Statistics** opens a dialog window similar to the one shown below:



This dialog window allows disconnecting one or all of the clients currently connected. To do so, in the **LIST OF USED LICENSES**, select the entrie(s) based on the **IP** information and activate the **Yes** button. The selected clients are disconnected from the license server. A confirmation window will display a successful operation.

Note: The client is only removed from license pool, not killed instantly. So it can reconnect to license server in few minutes if there are still spare licenses.

4 Data Processing

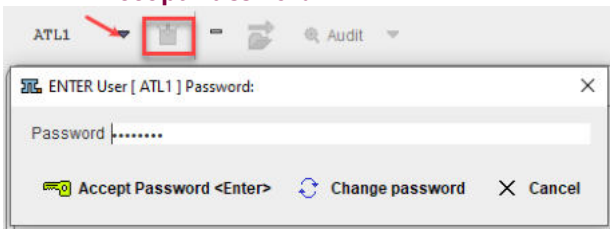
From the data processing point of view there are only a few differences to the normal operation of PMOD, which are explained below. Therefore, the user is referred to the standard User Guides for the explanations of the PMOD functionality.

4.1 Starting the PMOD Client

On a client system PMOD is started for data processing by the script *RunPmodClient* as described in the Client Installation 25 section.

When a PMOD client is started, the name of the current user is retrieved from the AD and one of the following actions happens:

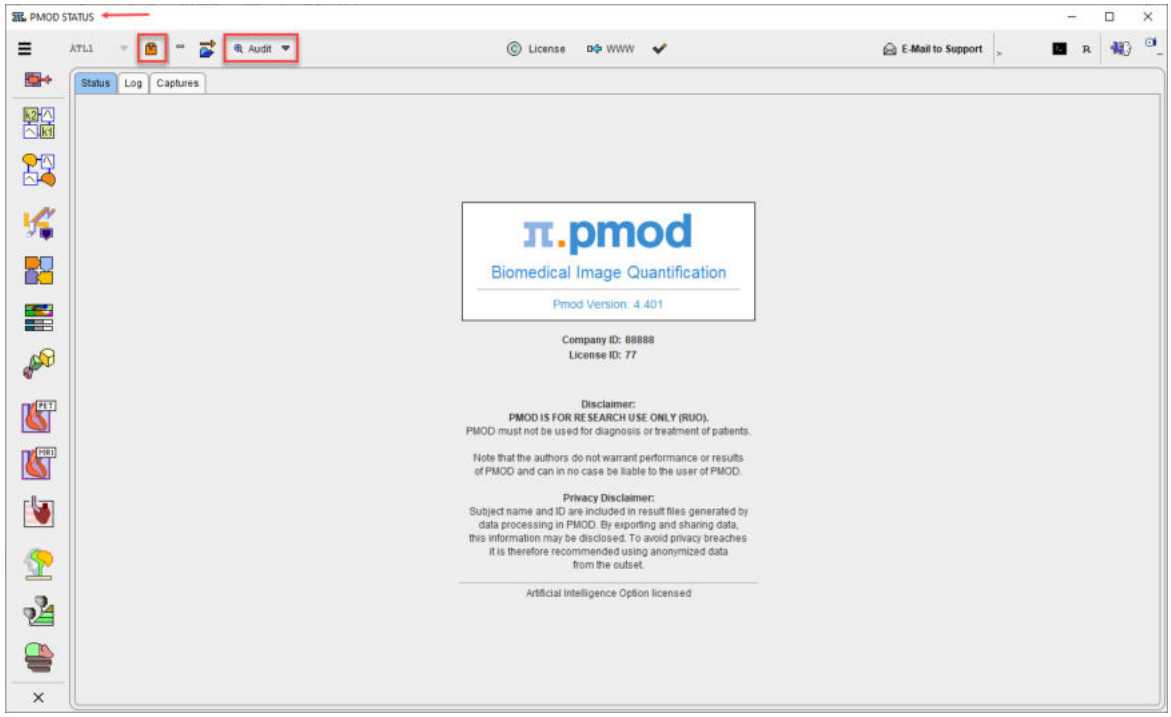
1. If the name of the user logged into the operating system is found in the PMOD user list as an OS user name, PMOD starts automatically. In this case, no logout is possible, just exit of PMOD.
2. If the AD user name is not found in the PMOD user list as an OS user name, the user has to select among the users without OS association. Then he has to enter the correct password and activate **Accept Password**.



The **Change password** button in window can be employed for changing the user password.

3. If there are no user names without OS association in PMOD, only the **Config** tool can be opened by the administrator. In this case all PMOD tools remain disabled.

The PMOD dock looks similar to a standard PMOD installation. There is an indication in the PMOD Status window, the mandatory log in and the presence of the **Audit** button (active or grayed out, depending of the user configuration) which alerts the user that he is working in an ATL environment.



The **Audit** button serves for starting the inspection of the Audit log. This button is only active if the user has been assigned a corresponding right in the setup 16.

The **Configuration** button allows starting the configuration of the PMOD ATL Server installation. It will always require the administrator password, independent of the user who is logged in.

Note that log in to PMOD is disabled if logging to the audit trail database is not possible. In this case only the the configuration tool can be opened by the PMOD administrator.

4.2 Data Processing

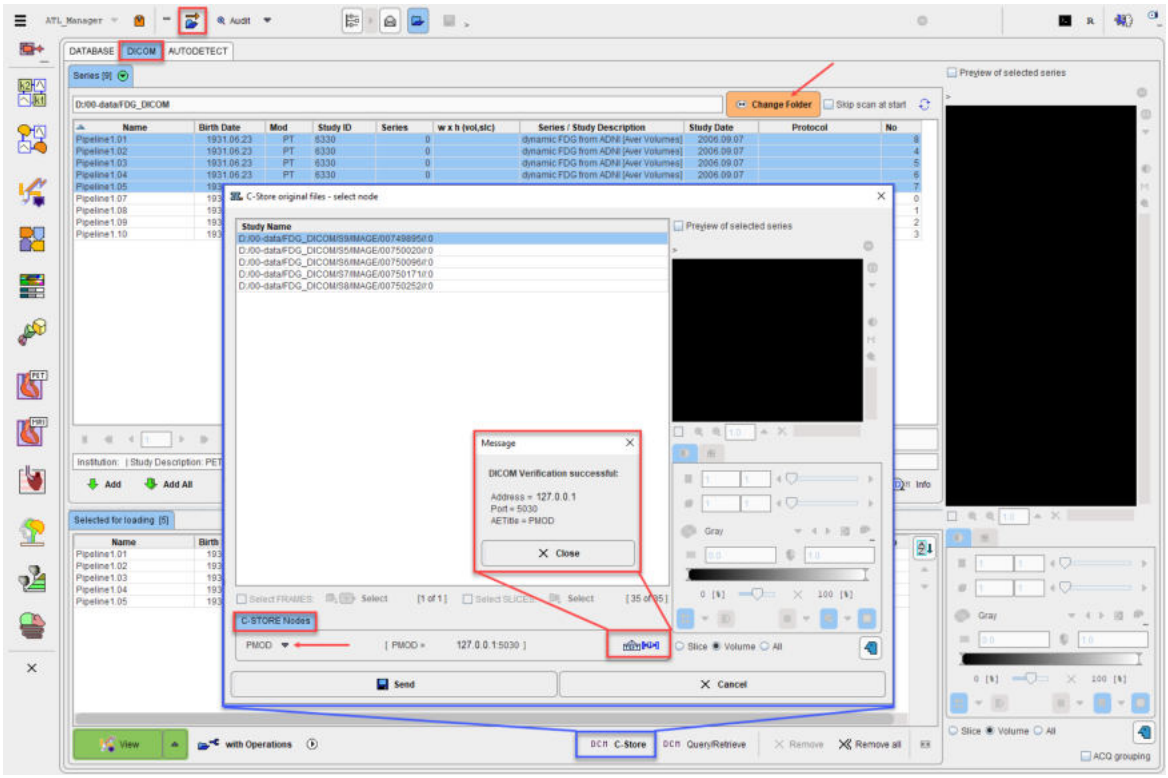
Data processing with an ATL client is exactly the same as with a standard PMOD instance except for the following differences:

1. A user will not see all available databases, just the ones for which he has been authorized.
2. A user can not delete from database, unless he has been assigned this privilege.
3. All loading and saving operations in all PMOD tools are logged to the Audit Trail.
4. When image data are loaded from a database, the ImageHistory of these images are loaded as well. New data processing steps are appended to this ImageHistory, so that there is a full data processing record in the ImageHistory.
5. When image data are saved, the complete ImageHistory is automatically saved. Both operations are recorded in the Audit Trail, so that the data transformations can be easily tracked and reported.
6. When VOI statistics is performed and the result saved, the VOIs are automatically saved.

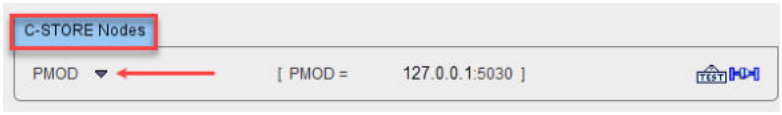
4.3 DICOM Data Import

If DICOM data are available on a disk (flash disk, DVD, hard disk), they can easily be sent to the DICOM server, which will add them to the **Import** database.

Start the unified data loader and select the **DICOM** tab. Use the **Change Folder** button to browse the file system to the directory where the data resides. If the data is organized as DICOM part 10 offline files, there will be a DICOMDIR file at the root of the directory tree which contains the image access information. Please **Select** this directory and the image series on the device will be listed as in the illustration below.



Select the image series you want to import in the list, and use the **Add** button to bring them to the **Selected for loading** area. Use the **DCM C-Store** button to initiate sending of the images to the DICOM server running on the ATL server machine. A dialog window appears for selecting the sending target which should equal the proper node.



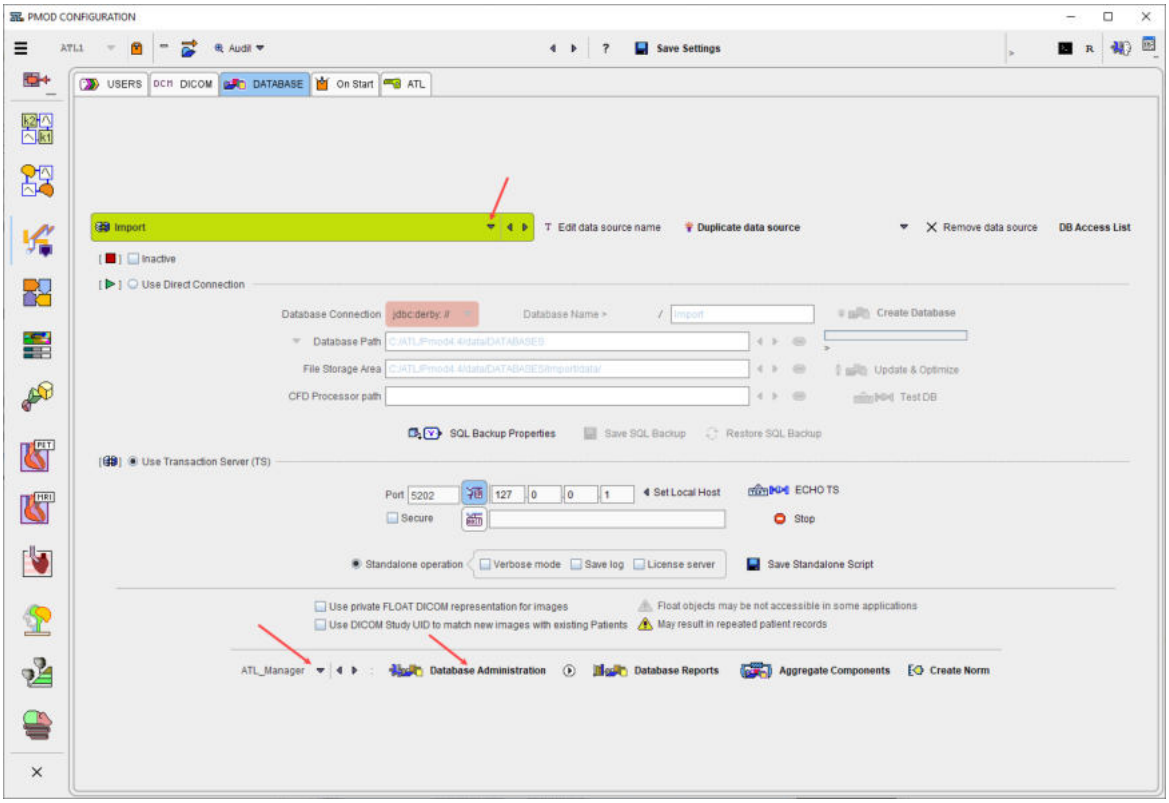
Start sending the images with the **Send** button. After the acknowledgment of a successful transfer has appeared the images are available in the **Import** database.

4.4 Data Migration

The **ATL_Manager** will be in charge for moving the data from the **Import** database to the target study database, in the example below **Study2**. This task can be done in two ways. Note that all of these actions will be documented in the Audit log.

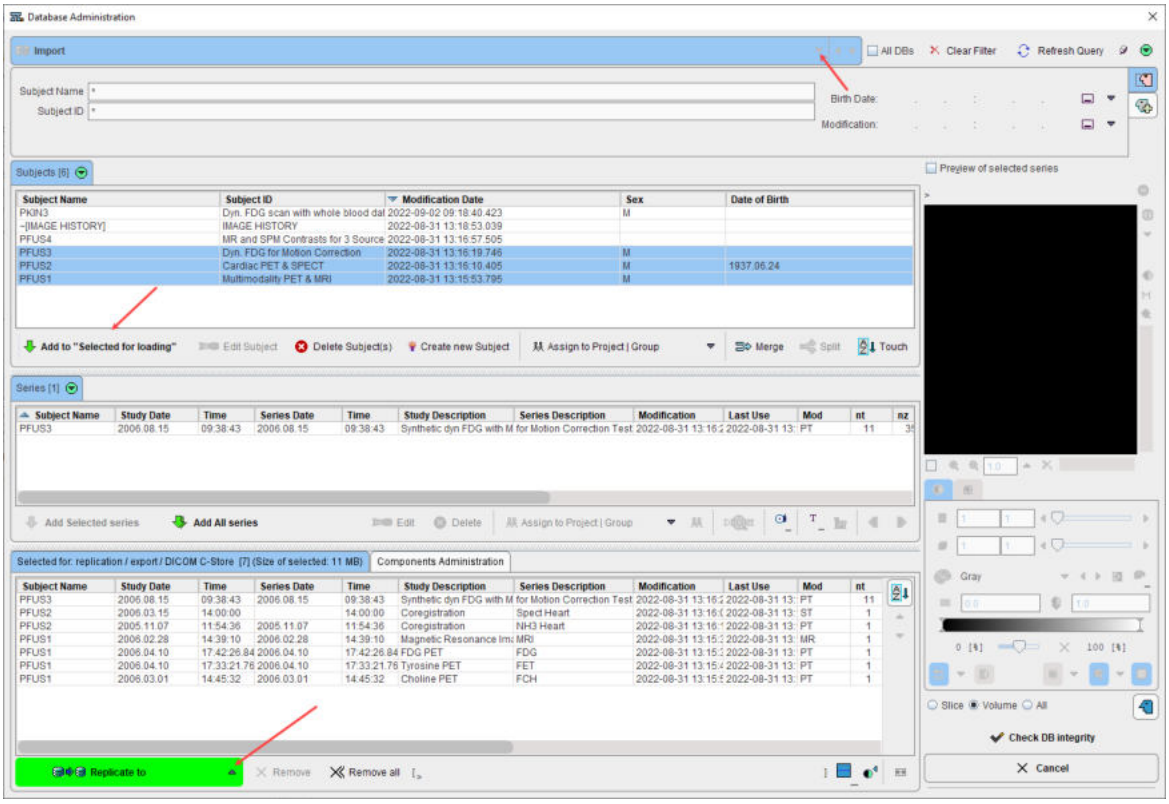
Moving Data in the Config Window (requires Administrator Password)

Start the **Configuration** utility and select the **DATABASE** tab. Make sure that the correct user **ATL_Manager** is selected, and activate the **Database Administration** button.

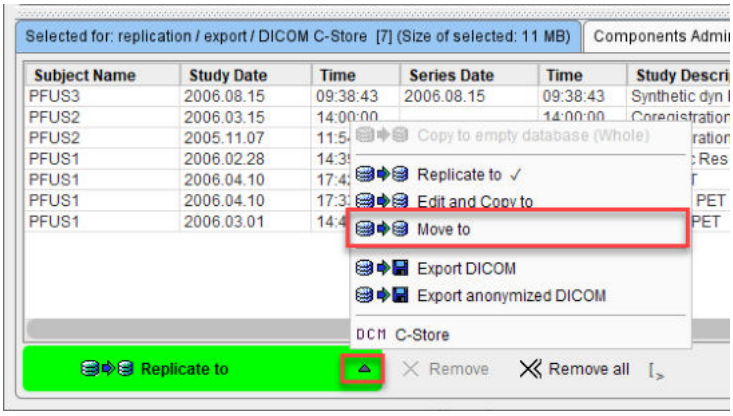


In the appearing **Database Administration** make sure that the **Import** database is selected. If it is not selected, activate the **Components Administration** tab, switch the database to **Import**, and the select the **Selected for:/replication/ ..** tab.

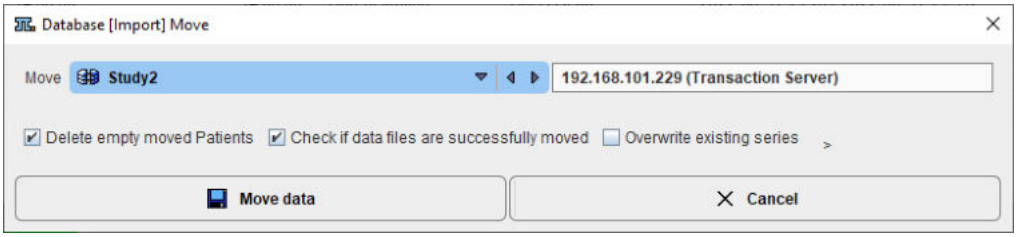
Then select the subjects to move to the **Study2** database, and activate **Set as "Selected for Loading"**. This brings all related images to the **Selected for:/replication/ ..** tab.



In order to remove the data after being copied switch **Replicate to** to **Move to**.



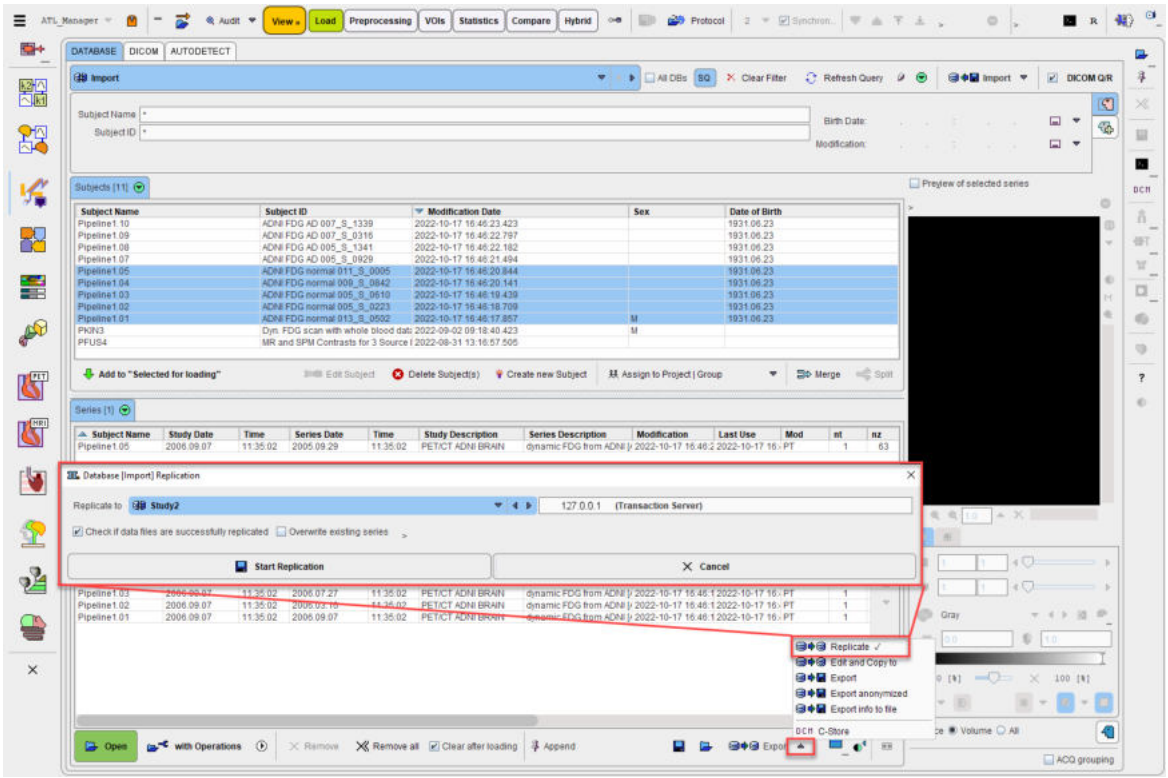
A dialog window appears for the specification of the target database. Make sure that the right **Move to** database is selected, and then migrate the data with the **Move data** button.



Replicating Data in the Viewing Tool

Data replication can also be done directly in the viewing tool PVIEW. There are two requirements: the database **Load** page is configured and that the user has access rights to both databases and that he is allowed to delete in the **Import** database.

1. On the database **Load** page select the **Import** database
2. Select the subject(s) to move to the **Study2** database.
3. Activate **Add to "Selected for Loading"** to prepare the images for replication.
4. Activate the **Replicate** button.
5. In the appearing **Database[Import] Replication** window select the target database **Replicate to Study2** and **Start Replication**. The replication is confirmed.
6. To clean up remove the data from the **Import** database by the **Delete Subject(s)** button.


Database [Import] Replication
Replicate to
Study2
127.0.0.1 (Transaction Server)
Check if data files are successfully replicated
Overwrite existing series
Start Replication
Cancel
Replicate
Edit and Copy to
Export
Export anonymized
Export info to file
DCM C-Store

5 Appendix

Transaction Servers

	Audit Trail Log & License Server	Import Database	Study Database 1	Study Database 2
DB Name				
Port				
IP Address				
Encryption				
Users (d = delete)				

DICOM Server

Definition	Value
Application Entity Title	
Port	
IP Address	
Encryption	
User on **USERS** tab *)	
Import Database	

*) a user is required to define the saving behavior of the DICOM server.

6 PMOD Disclaimer

PMOD is a software
FOR RESEARCH USE ONLY (RUO)
and must not be used for diagnosis or treatment of patients.

7 PMOD Copyright Notice

Copyright © 1996-2022 PMOD Technologies LLC.
All rights reserved.

The PMOD software contains proprietary information of PMOD Technologies LLC; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development the program may change and no longer exactly correspond to this document. The information and intellectual property contained herein is confidential between PMOD Technologies LLC and the client and remains the exclusive property of PMOD Technologies LLC. If you find any problems in the document, please report them to us in writing. PMOD Technologies LLC does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of PMOD Technologies LLC.

PMOD Technologies LLC
Industriestrasse 26
8117 Fällanden
Switzerland
support@pmod.com
http://www.pmod.com

- A -

Administrator Password Change 22
Advanced DICOM Server Options 20
Annual Maintenance 30
Appendix 9, 38
ATL Client Systems 8
ATL Server System 8
Audit Trail 6
Audit Trail Configuration 11, 25
Audit Trail Database Creation 12
Audit Trail Inspection 27

- C -

Client Installation 25, 32
Client Script Generation 21

- D -

Data Migration 34
Data Processing 32, 33
Data Protection 6
Database Access Rights 22
Database Cleanup 15
DICOM Client Configuration 18
DICOM Data Import 33
DICOM Server Configuration 17
DICOM Server Definition 18

- I -

Installation 8

- L -

Licenses Control 30

- M -

Maintenance Operations 27

- O -

Overview Tables 9

- P -

PMOD ATL Server Installation and Configuration 8
PMOD Audit Trail Network License 5
PMOD Copyright Notice 40
PMOD Software Installation 9
Purpose 5

- S -

Starting of the Servers 22
Starting PMOD for System Configuration 9
Starting the PMOD Client 32
Stopping/Starting of the Servers 27
Study Database Configuration 13
Study Database Creation 13
System Configuration 11
System Organization 5, 6
System Setup 8

- T -

Transaction Server for Audit Trail and Licensing 13, 21
Transaction Servers for Study Databases 14

- U -

User Administration System 8
User Authentication 6
User Configuration 16
User Creation 16, 32