System Security

Property Management Solutions for Over 30 Years

Overview

This document covers the functions available in System Security.

- Basic System Security information
- Access Groups – Tab 2 (page 2)
- Users – Tab 3 (page 3)
- Database Directories – Tab 4 (page 5)
- Examples of limiting access (page 6)

System Security

System Security sets up the User registration license consisting of the protected Company name that prints on all reports, the unit limit, and which features (network, commercial, maintenance) are enabled. After registration the database is used to establish user security authorization parameters that restrict access to selected modules and functions. This is done by setting up and assigning Access Groups to a User. A User's access to functions and ability to post transactions can be limited by setting transaction posting parameters for that User.

Access to System Security requires a password. The initial password is provided by Customer Support when you register the software. At that time (and from then on) you can, at your discretion, change the system security password.

Prior to registration it is not necessary to enter a User Name or Password to get into the PROMAS Landmaster databases (Residential Demonstration, Practice Demonstration). When you call to register you will be provided with a password to get into the System Security database and assisted thru the process of entering your protected company name, unit limit and identify the options you will have available.

After entering the registration parameters you can set up your user ID's, passwords and file security for your users. Once you register, a user name and password is required.

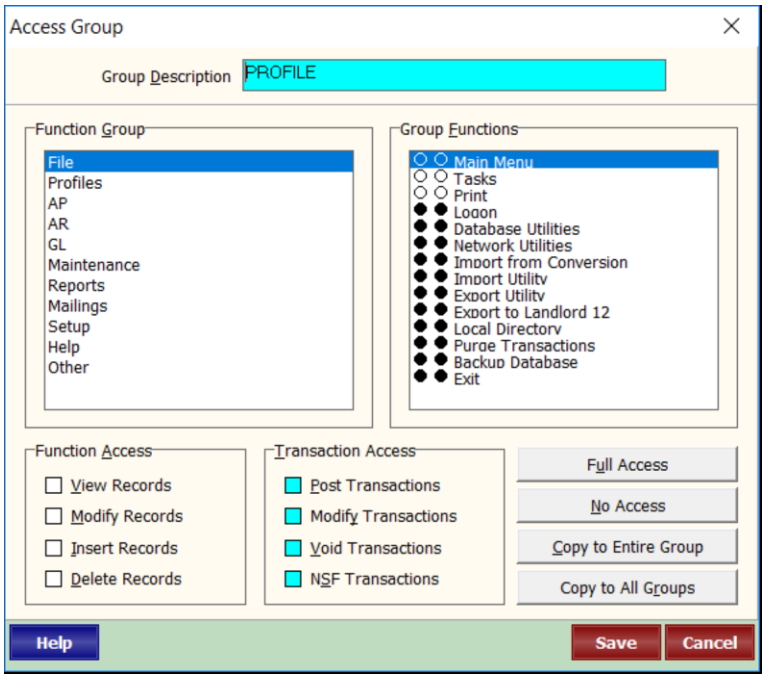
Each database can be set up so that the security parameters are different.

Using the security features is optional. If you want to either have a record of who posted each transaction or limit access to some functions depending on the user, you must set up security.

Access Groups – Tab 2

An access group identifies the functions that the user has access to and is the means for limiting what a user is allowed to do. An access group is assigned to a user when that user should not have full access to all functions.

The name chosen for the Access Group is assigned to users on the Users tab in System Security.



Function Group
Each major function group is listed. When one is highlighted, the functions for that group are listed under Group Functions.

Group Functions
Each function for the highlighted function group is listed with two circles. One of the circles indicates function access and one indicates transaction access. When the circle is filled in, that function has full access. When the circle is empty, that function has no access. If it is partially filled in there is partial access. The functions/transactions that are enabled are listed below. Note that the highlight bar makes the background the reverse shading.

Function Access
Each of the functions can be enabled or disabled.

- View Records – view only
- Modify Records – view and modify
- Insert Records
- Delete Records

Full Access
Clicking the Full Access button will mark all checkboxes in Function Access for the highlighted Group Functions and move the selection bar to the next line.

No Access
Clicking the No Access button will unmark all checkboxes in Function Access for the highlighted Group Function and move the selection bar to the next line. A function marked No Access (none of the checkboxes marked) will not be displayed on the task bar nor listed on the drop down list.

Transaction Access
This feature is not implemented at this time. Use the [Limit to] in Users to limit transaction posting.

Copy to Entire Group
Clicking this button makes every function within the group the same as the highlighted one.

Copy to All Groups
Clicking this button makes every function in all groups the same as the highlighted one.

NOTE: To give full access and then limit some access, mark one function as full access, highlight it and then click Copy to All Groups. Then remove the access from the desired function.

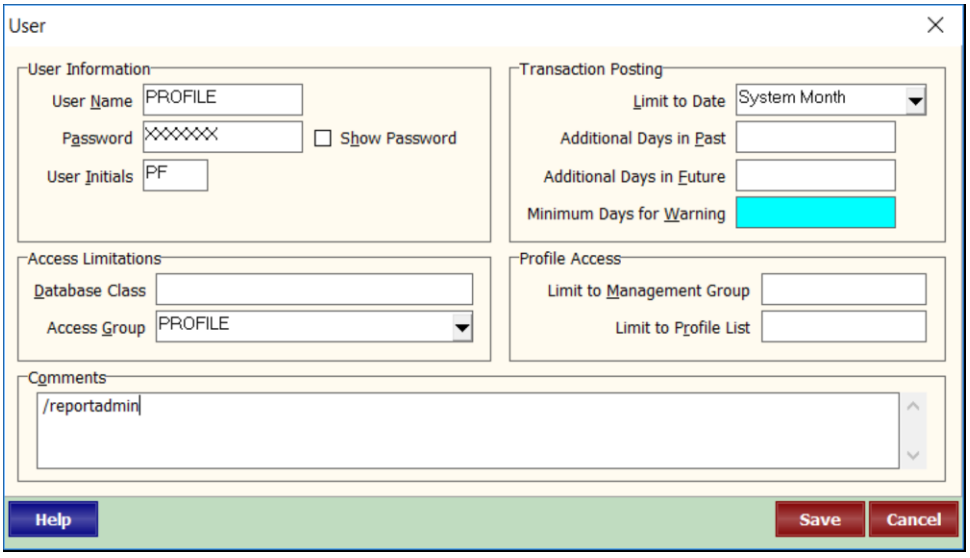
The buttons let you assign full access or no access to any function or group with just one click.

Users – Tab 3

Each person who uses the program should be set up as a user in the System Security database. Each user has a different User Name, Password and a set of initials. Each transaction that is posted is assigned the set of initials based on the User Name and Password entered on Logon.

To enter a new user

- On the User page, click New to create a new user or highlight a user name and click Edit. The User screen will display. Enter a **Name** and **Password** that will be used to log-on each time the user enters the program. Enter **Initials** that will be assigned to each transaction posted.
- To give the user access to the Manage reports function, click into the Comments field and type /reportadmin.
- To give the user access to modify reports and do backups under File, Backup Database click into the Comments field and type /admin. There can be no access groups assigned to the user for this to work.
- To prevent user from voiding any transactions click into the Comments field and type /novoid.



Database Class - Each database can have a Database Class assigned to it. If you have several databases, a user can be limited to only one database by assigning the Database Class of that database.

Access Group - You can assign a user to an access group which can be used to limit that user's access to functions.

Profile Access - The user can be limited to a management group and/or a Profile List. This restricts access to only those profiles that belong to the group selected.

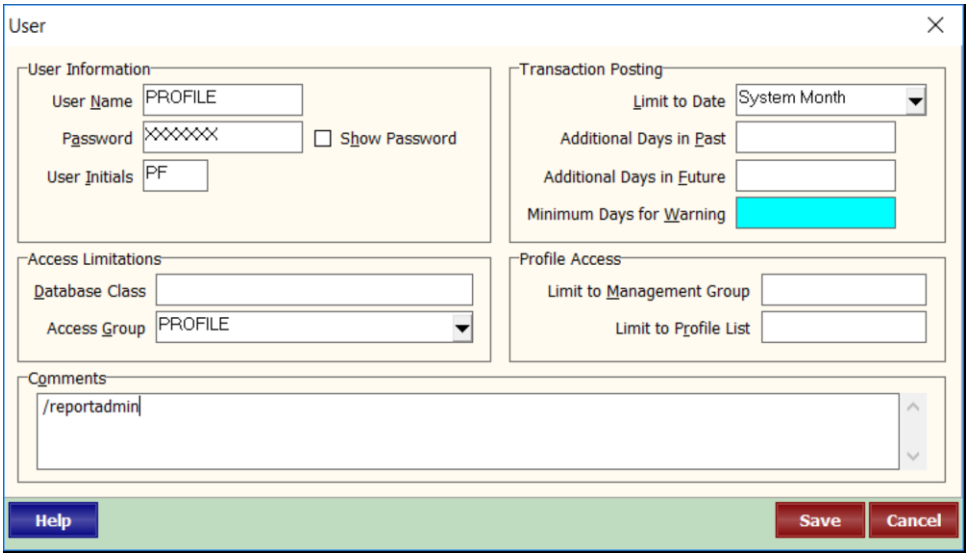
Transaction Posting –
Limit To - This field lets you prevent this user from posting transactions outside of a specified period. The options include:

- Never - user cannot post transactions
- System Day - limits posting to the computer system clock day
- System Month - limits posting to days in the computer system month
- System Year - limits posting to days in the computer system year
- Example: If the Limit To field is set to System Month and the computer system date is April 4, 2006, the user can only post transactions with posting dates of April 2006.

Additional Days in the Past and Additional Days in the Future modify the Limit To Date parameter. If both were set to 1 and the Limit is System Day, this user could post transactions dated yesterday, today and tomorrow.

The <<Reports, Manage Reports>> function lets you copy a current report and make changes to it, then save it as a new report. It shows on the Reports screen. To have access to the Manage Reports function, the User profile in System Security must be set up in one of two ways. In the Options field:

- /admin with no access group enables report manager and the backup functions
- /reportadmin enables the report manager



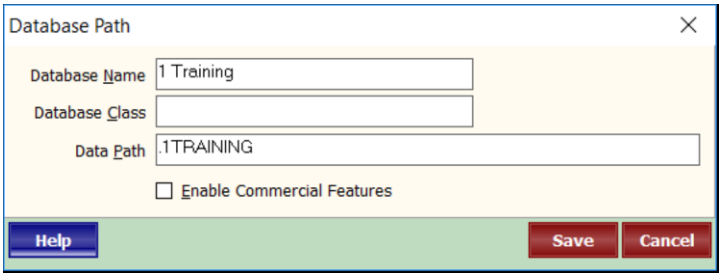
Database Directories – Tab 4

The two databases that are activated at registration are your primary database and the Rental Demonstration database, which is used for training and testing.

To start with a database with basic account codes, pre-defined statement styles, and other setup basics, create a folder at the Drive Letter\Path (e.g. F:|RPROMAS) and copy the LL12_Database from the Data QuickStart folder into that folder. Then follow the startup directions.

Add an Additional Database

- Select the System Security database on the Logon screen.
- Enter the System Security password, established at registration.
- Select Tab 4 – Database Directories.
- Click the <New Database> button.
- Leave the Database Class field blank.
- Enter a Database Name
- Enter the Data Path in one of the following formats
    - .foldername -- e.g. .myfolder (the period preceeding the folder name takes the place of the drive letter and the rpromas folder)
    - Drive Letter\Path\foldername -- e.g. F:\RPROMAS\MyFolder



If your license is for anything other than unlimited you can maintain up to three separate databases. An unlimited license lets you define an unlimited number of databases.

Multiple Databases

In general one database is sufficient for most users since multiple sets of books can be maintained within a single database. Instances where you might want to consider separate databases include:

- Keeping self-owned properties separate from managed properties
- Maintaining the company books
- keeping the financial records for more than one association
- processing responsibility (posting receipts, writing checks, etc) is functionally separate, i.e. bookkeeper 1 does all processing for one set and bookkeeper 2 does all processing for another set.

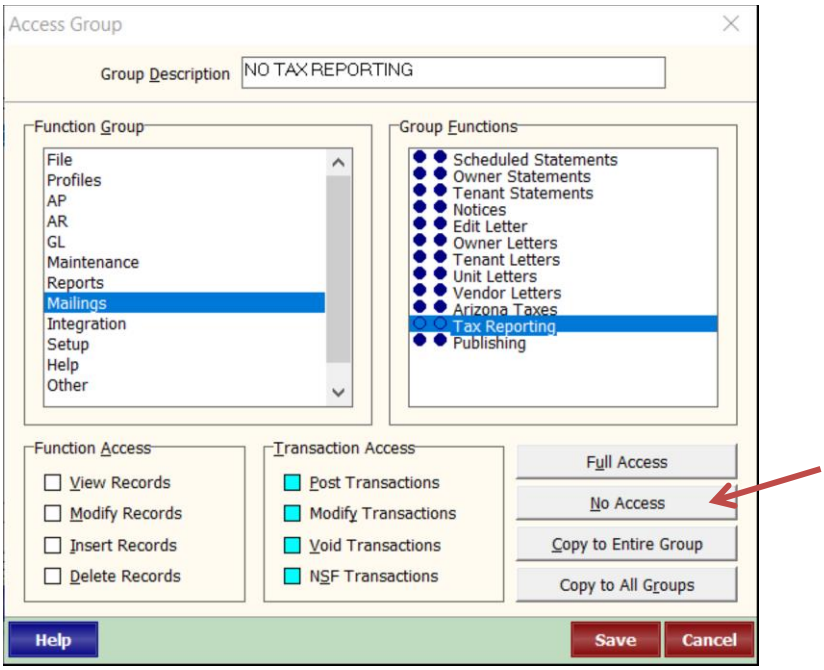
Limit Access to a Database

A user can be limited to specific databases by assigning a Database Class name to the database in System Security, Database Directories tab and then assigning the same Database Class to the user in System Security, Users tab.

Examples of Limiting Access to a User:

Limit access to tax reporting
On the Access Group tab create a new access group. Name it something like No Tax Reporting.

Go to the Mailings Function Group.
Highlight Tax Reporting.
Click on No Access.
Save. Then assign that access group to anyone who should not have access to tax reporting.



Limit to Tenant Receipts and Tenant History
You want to limit someone to only entering rent receipts and looking in tenant history, but don't want them to be able to void or edit transactions.

System Security, Access Groups – Set up an access group that has full access to:
- AR, Tenant Receipts
- AR, Tenant History
- File, Logon
- Profiles

System Security, Users
- Assign their user name to that access group and in the Limit To field choose System Date. That will limit them to posting and editing transactions for the system date only.

View Only Access

To set up a user with view only access:

1. Select the Access Groups tab
2. Click on New Group
3. Enter a Group Description Name (e.g. View Only)
4. Click on File in Function Group
5. Click on No Access to blank out the radio buttons
6. Click on Logon
7. Mark the View Records checkbox in Function Access
8. Click on Copy to All Groups
9. Click Save
10. Click on the Users tab
11. Enter a User Name, Password and Initials
12. Select the Access Group created above
13. Select Never Allow Posting in the Limit to Date field of Transaction Posting
14. Click Save

Changes to Profiles Only

1. Click on Profiles in Function Group
2. Mark the Modify, Insert and Delete Records checkboxes in Function Access
3. Click on Copy to Entire Group
4. Click Save.

Prevent Access to a Function

This will remove the speedbutton and menu item from the drop down list.

- First give full access to everything:

    1. Select the Access Group tab
    2. Click on New Group
    3. Enter a Group Description name
    4. Mark the View, Modify, Insert and Delete checkboxes in Function Access
    5. Click on Copy to All Groups

- Then to remove access to one function:
    1. Select the Function Group
    2. Highlight the Group Function
    3. Click on the No Access button
    4. Repeat steps 6-8 for each function you want removed.
    5. Click Save
    6. Click on the Users tab
    7. Enter a user name, password and initials
    8. Select the Access Group
    9. Click Save

Prevent Access to a Management Group

Limit to One of Two Mgmt groups

- In System Security, on the User Tab, edit the user and enter the Management Group ID in the Limit To field.

Prevent access to one group when there are more than two management groups.

- Set up a Profile List under <<Setup, Profile Lists>>.
- In System Security, on the User Tab, edit the user and enter the Profile List ID in the Limit To field.