Copyright Notice

2017 P2 Energy Solutions. All rights reserved.  
No reproduction without written permission.

Version 1

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, P2 Energy Solutions, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

Any questions regarding this document should be forwarded to:

P2 Energy Solutions  
1670 Broadway, Suite 2800  
Denver, CO 80202  
United States
Table of Contents

Course Overview........................................................................................................................................... 4
- Security System Module Description ........................................................................................................ 4
- Course Description ...................................................................................................................................... 4
- Audience, Course Level and Prerequisites .................................................................................................. 4
- What You Will Learn .................................................................................................................................... 4

Lesson One: SETUP PROCEDURES .................................................................................................................. 5
- Functions Menu Descriptions Table ............................................................................................................ 5
- System Options ............................................................................................................................................. 6
- User Setup ................................................................................................................................................... 8
- Security Setup ............................................................................................................................................ 9

Lesson Two: MENUS, PASSWORDS AND LOCKS .............................................................................................. 11
- Menu Security Matrix Report ...................................................................................................................... 11
- Change Password ......................................................................................................................................... 12
- Lock Administration .................................................................................................................................... 13
- P2 Global Support ....................................................................................................................................... 13

Lesson Three: USER ACTION AUDIT TRAIL .................................................................................................. 14
- User Action Audit Trail Administration ......................................................................................................... 14
- User Action Audit Trail Report .................................................................................................................... 15
Course Overview

Security System Module Description

The IDEAS for Windows (IFW) System Security module is used to administer and report user security, and to view and remove table locks.

Specifically, this module is used to create, edit, inactivate or remove users, assign user passwords and grant access privileges. Access is granted to each user, by module at the menu option level, and may be modified from time to time as needed. (The IDEAS Enhanced Security module can further limit access privileges.) A simple report function allows users to preview and print reports of access privileges.

System options are available to enter rules governing passwords and login attempts, establish audit trails, “turn on” Enhanced Security, and view the number of user licenses that have been purchased.

A lock administration function allows users to view and remove table locks (a normal part of system processing) in the unlikely event they are not automatically removed at the close of a given process.

Course Description

This class provides an overview of the IDEAS System Security module and then covers setup procedures, menu and password security, locks, and user action audit trail administration.

Audience, Course Level and Prerequisites

This basic level class is recommended for those who are responsible for IDEAS user setup and security. Prerequisites for this course are the Core New User Training sequence: IDEAS User Interface Navigation and Introduction to IDEAS Architecture.

What You Will Learn

- Security System Overview
- Security System Setup Procedures
  - System Options
  - User Setup
  - Security Setup
- Menus, Passwords and Locks
- User Action Audit Trail Administration
Lesson One: SETUP PROCEDURES

To set up IFW for operating the System Security module, complete the following steps in the order listed below. Each step requires that you select a function from a drop-down menu and complete the screen(s) that IFW displays. Please see the Screen-By-Screen Instructions section for detailed instructions on how to complete each screen.

Functions Menu

<table>
<thead>
<tr>
<th>TO ACCESS FROM THE FUNCTIONS DROP-DOWN MENU:</th>
<th>USE THE FUNCTION TO:</th>
</tr>
</thead>
</table>
| Click on **System Options**.               | Define rules governing passwords, logins, audit trails and enhanced security.  
                                            | View number of user licenses.           |
| Click on **User Setup**.                   | Establish new users and passwords, inactivate or remove existing users.       |
| Click on **Security Setup**.               | Assign menu access to new users or edit access of existing users.             |
| Click on **Report**.                       | Easily generate reports of access privileges by module(s) and user(s).        |

Optional during initial setup
### TO ACCESS FROM THE FUNCTIONS DROP-DOWN MENU:

<table>
<thead>
<tr>
<th>Function</th>
<th>Use the Function To:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Password</strong></td>
<td>Change the password associated with the default administrative user.</td>
</tr>
<tr>
<td></td>
<td><em>Optional during initial setup</em></td>
</tr>
<tr>
<td><strong>Lock Administration</strong></td>
<td>View information regarding locked rows within tables. Remove locks.</td>
</tr>
<tr>
<td></td>
<td><em>Not required for initial setup</em></td>
</tr>
</tbody>
</table>

### System Options

![System Options](image)

- Minimum Password Length: 5
- Allow Password Re-use After: 3
- Maximum Login Attempts: 10
- Enforce Complex Passwords: *not checked*
- Inactivate Users: *not checked*
- Chartmaster Audit Trail: *not checked*
- Journal Corrections Audit Trail: *not checked*
- Login Tracking: *not checked*
- Allow Master Login: *not checked*
- Enhanced Security: not selected
- User Licenses: 10

Current Encryption Level is Strong.

- Apply Strong Encryption
- Apply Standard Encryption

[Save] [Close]
Use System Options for the following functions:

- **Minimum Password Length** – Select a minimum password length from 0 to 10 characters. The default is 0, which means that passwords have no minimum length requirements.

- **Allow Password Reuse After** – If passwords are to expire, this option requires that 0 to 10 new passwords be created before a previously used password can be used again.

- **Maximum Login Attempts** – Use this function to define 0 to 10 login attempts that can be made before the user is exited from the module.

- **Inactivate Users** – Used with the Maximum Login Attempts, this option automatically inactivates any user failing to successfully log in after the maximum permitted login attempts. Inactive users must be reactivated in the User Setup screen.

- **Chartmaster Audit Trail** – Select this option to activate an audit trail of General Ledger Chartmaster activity. Several reports are available on the Utilities menu of the General Ledger module.

- **Journal Corrections Audit Trail** – Select this option to activate an audit trail of General Ledger Journal Corrections. The Journal Corrections Log is available on the Utilities menu of the General Ledger module.

- **Login Tracking** – Select this option to track user logins. The Login Tracking report is available on the Utilities menu of the General Ledger module.

- **Allow Master Login** – Select this option to accept the System.Master login.

- **Enhanced Security** – Select this option to activate the IFW Enhanced Security module, if licensed.

- **User Licenses** – Displays the number of user licenses and may not be altered.
User Setup

Before processing can begin in any IFW module, users must first be created and given permission to access that module through the Function menu in the System Security module.

Use the User Setup function to define initial IFW users, and establish passwords and password expirations for them. Later this function can be used to edit, inactivate or remove users.

- **User** – To create new users, type in a name up to 20 alphanumeric characters in length. The User ID is not case sensitive.
- **Password** – Enter a password for this user up to 10 alphanumeric characters in length. Passwords will not display. Passwords are also *not* case sensitive.
- **Confirm Password** – Re-enter the password.
  **Note:** When existing Users are edited, passwords need to be reconfirmed before the system will allow any change to be saved.
- **Status** – By default, the system assumes new users are active. User status may be changed at any time by selecting the appropriate **Active** or **Inactive** button.
- **Options** – Users can be required to change passwords every *X* number of days. To activate this, enter the number of days in the **Days until password expires** text box. Alternatively, select the **Password never expires** check box to set passwords to never expire. To force a password change, select the **Change Password on Next Login** check box.

Click **Save** to save the information and clear the screen for additional entries. Click **Delete** to permanently remove a user.
Security Setup

Use the Security Setup function to grant users access to some or all menus within licensed IFW modules. When IFW is installed, a default administrative user named System.Master is automatically created.

Initially, security is copied from this user and then access privileges for individual users or user groups will be modified based on access needs. Users with the same access needs may be copied from one to another with no further editing necessary.

- **Username** – Select the user for whom you want to create or edit security.
- **Copy Security from User** – Select a user with similar access needs/restrictions to copy security from. Normally this is used only during initial setup of a user’s access privileges.

Click the **Copy** button at the bottom of the Pop-up window to complete the process and save the security from the selected source user to the target user (the Save button is not used at this time).

**Note:** The Copy function copies the security from the source Username to the target User for all modules and menus. User security copied from System.Master must be edited to remove access privileges that are not intended.
Security for new users is copied from existing users with similar access needs. Access privileges are then modified as necessary. During installation, a default administrative user (System.Master) is created with full access to all modules and is used as the initial template for new users.

Users will not have access to any screens until they have been given permission through the Menu Security Access function.

**Username** – Select the User for whom you want to edit security.

**Module ID** – Select the Module(s) where security needs to be edited.

**Menu Code** – Select a Menu Code to view and/or edit security for that menu. The associated Menu Options will display along with current Security Access settings.

**Security Access** settings are:

- **Y** – Yes, allow access
- **N** – No, do not allow access.

To change settings, click in the Security Access field for the Menu Option to be changed, highlight the selection and then type Y or N. Alternately, you can use the down arrow that appears in the Security Access field to select Y or N from the drop-down menu.

**Note:** Removing access to a Menu Option will inactivate the shortcut button to that Menu Option as well.
Lesson Two: MENUS, PASSWORDS AND LOCKS

Menu Security Matrix Report

The Matrix Report is a report of user access privileges to one or more modules. The report can be generated to display module-by-module access for Users or Roles. Use this report to preview or print a report of access privileges by user, module and function.

Enter the report description, choose to generate the report based on Users access or on user roles, select one or more module from the available list, and select one or more users. When all selections have been made, click Execute to generate the report.
Change Password

Use the Change Password function to change the password associated with the default administrative user.

Select the user name from the User drop-down list, at the Password and Confirm Password text boxes enter and confirm the new password, and then click Save.

You may also enter your Email ID as additional information.

Note: It is important to store a record of this password in a safe, secure place.
Lock Administration

Locks are created from time to time by IFW to enforce database rules. For example, a journal will be locked when the Journal Entry Correction function is used to prevent other users from attempting to work in that journal concurrently. Normally, locks are cleared by the system when it is appropriate to do so. Occasionally locks may not clear automatically. Lock Administration gives users the ability to manually remove them in this circumstance. Information reported on the screen assists users in determining if a lock should be deleted.

**P2 Global Support**

If questions arise, contact IDEAS International, Inc. support office for help.

**By Telephone**
North America: 1-844-732-2472 (1-844-REACH-P2)
APAC: +61 8-9241-0314

**By Email**
GCS@p2energysolutions.com
Lesson Three: USER ACTION AUDIT TRAIL

User Action Audit Trail Administration

The User Action Audit Trail Administration program allows you to define audit trail parameters for use throughout the system. This option should only be available to the system administrators.

The administrator can choose which types of activity should be monitored by selecting the appropriate Categories. The Categories essentially represent modules within the system, and certain database tables are associated with each Category. If a Category is selected for active monitoring, any activity that takes place within the associated tables will be tracked in the audit trail. The Track Record History option produces a snapshot of monitored records before and after modifications are made, and the Track Update Details option provides additional reporting capability to show the before and after values of the specific fields that are modified within the monitored records.
We strongly recommended that you perform regular purging of the User Action Audit Trail, as the size of the audit trail can become very large, affecting resources and performance. To assist with this maintenance, set the **Purge User Action Audit Trail Older Than** option to perform regular automatic purges based on date. The **Last Modified** field displays the last time the parameters in the User Action Audit Trail Administration screen were set.

The actual User Action Audit Trail data can be displayed by running the User Action Audit Trail Report.

**User Action Audit Trail Report**

The User Action Audit Trail Report generates an audit report by module and user. The report can be sorted by date or table, and it can include all types of transactions or a combination of the three transaction types. Users may choose to include all dates or specify dates, and they may also choose to include details in the report or a table key reference guide.