

Understanding Power Enterprise User Setup

Controlling user access to power enterprise is vital in a business environment. You have to understand the elements that are available to you.

Each person who uses the system (a user) has to log into the system to use it. Users have their own unique access, which is password controlled. You should ensure that users understand that they should **NEVER** give their passwords out to anyone else.

For specialized user such as administrator or managers, you can of course set access levels individually.

You specify the ability to create, edit, and delete each master file individually. The reason for this separate mechanism is that whenever a user uses a master file record, such as a customer or Vendor record, the data entry field allows authorized users to access that master file's maintenance functions. For details about this data entry,

User creation process is sub-divided into two:

1. Creating the user
2. Assigning right and privileges

User Creation

Creating a user in power enterprise is a simple function all you need to do is to log in to the system with a user that possess the administrative privilege or its equivalents.

Then follow this path:

System Setup >>> Company Setup>>>User Setup >>> New

Specify unique user identifier for the user in the User ID Section, Full User name in the User Name section and fill the other information as appropriate.

Note: A default password is to be specified for every user created, which can be reset by the user upon successful log in.

Assigning right and privilege

Creating a user alone does not give a full privilege to the system, a newly created user must be assigned privilege and access to certain functions within the application. To access this function, follow this path:

System Setup >>> Company Setup>>>Security Setup >>> New

Understanding the Access right and privilege

The security architecture of power enterprise is built around four functions:

1. **View** : Ability to see the function upon successful log on
2. **Add** : Ability to add a new record
3. **Edit** : Ability to modify an existing record
4. **Delete** : Ability to delete an existing record

The security setup is then modularized base on the functional modules within the application; there by checking and un-checking the appropriate boxes signifies granting and denying access to those functions.

Also you can specify a default page for each user to restrict access to certain information on the dash board of the application below is some of the standard default pages:

1. Default.aspx (Default for all user if nothing is specified)
2. DefaultBlank.aspx (A blank default page)
3. Default1.aspx (A default page that show the financial status of the company)
4. DefaultCrm.aspx (A default page for the CRM Module)

Also granting the Admin functions under the admin section overrides any form of setup in the preceding sections.

It must be noted that creating several users without enforcing each user to log on to the system without the use of the generic user id is not a best practice as these goes a long way in defeating the drill down audit trail of who does what on the system.