

User's & Security

- a very fine-grained level of detail in assigning permissions.
- User-level security allows the database administrator to group users with similar needs into common pools. Permission can then be granted to work group instead of to individual users, easing the administration of permissions.

The best practices for securing your system users, roles,& permissions are based on the following ideas:

1. Rethink your roles
2. Know the defaults
3. Evaluate your elevated permissions

The importance of User's, Roles and Permissions

- **Users** are the **people**
- **Roles** are their **Functions**,and
- **Permissions** define what **Authorizations** those functions have.

Sample page for creating user account

Clear		Show		Top		Previous		Next		Bottom		Add		Update		Delete		+			
Email Address		accounting@costules.co										Password									
Name	Accounting Department										Access Code										
Phone											Phone-Mobile										
Date Format	[Select]										Date Separator										
Shortcut Prefix	Alt										Shortcut Exclusions		fcvhta								
Language	[Select]										Tooltips?		<input type="checkbox"/> Enable								
Restrict Access to Modules	ca,g,ar,ap,im										Active		<input checked="" type="checkbox"/> Activate?								
Reference											Asset Id										
Changed Password	0										Single Session Only?		<input type="checkbox"/> Yes								
Security Question																					
Answer																					
Custom Security Model	[Select]										Access from Location Only?		<input type="checkbox"/> Yes								
Self-customization	<input checked="" type="checkbox"/> Restrict																				

Sample page for the list of system Users

Users	
<div> <div><</div> <div>></div> </div> <div>50</div> <div>></div> <div>></div>	
Name ↑ Access Code	Email Address Restrict Access to Modules
Accounting Department	accounting@costuless.com ca,gl,ar,ap,im
Accounts	accounts@dreamapps.com cafav,cahome, ar, ap, gl, ca
Adeline Dura	adel@dreamapps.com
Ai-ai Abapo	cecille.abapo@dreamapps.com
Asok Chattopadhyay	asok@dreamapps.com
Boss	boss@dreamapps.com
u	
Connecticom Global Network, Inc	training@connecticom.com zx, ca, ar, ap, gl, op, po, im, sa
u	
Cost U Less	demo@costuless.com ca,pd,gl,ar,ap,op,po,im,es,cx,cs,sa
Distribution	aiai@mol.com ca,gl,ar,ap,
Julie Ngau	julie@dreamapps.com esx,cauploaddoc,cafav,cahome, pd,ar, ap, gl, op, no, im, sa, ca, cf, es, ex

Roles

- This is a principle by which developers create a systems that limit access or restrict operations according to a user's defined role within a system. This is also often called **role-based** principle to ensure that authorized users do not gain access to privileged information.

Sample page for Roles definition

Home

System Administration

Accounting Department

cecille.abapo@dreamapps.com

DreamApps PH

User

Roles

Access-Control

Limits

Groups

Teams

Visibility

Managers

Locations

Accounts

Define the Role of the specific user in here:

Clear

Show

Top

Previous

Next

Bottom

Add

Update

Delete

+

Role

User

Active

☒

Activate?

Accountant

Customer

Designer

Employee

Manager

Merchant

Site

Supplier

Tenant

User

<

>

50

>

>

Role #

Target En

User

Roles

Name

Active

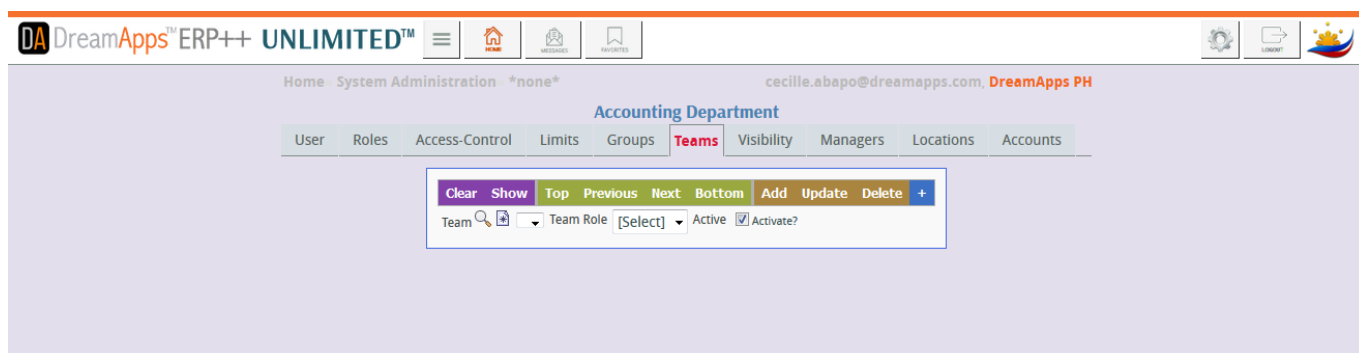
☒

Teams

- After you have defined the Team, you can link the Team member to the Team and Role. By doing

so, you can access to any of the transaction entry by **Team**.

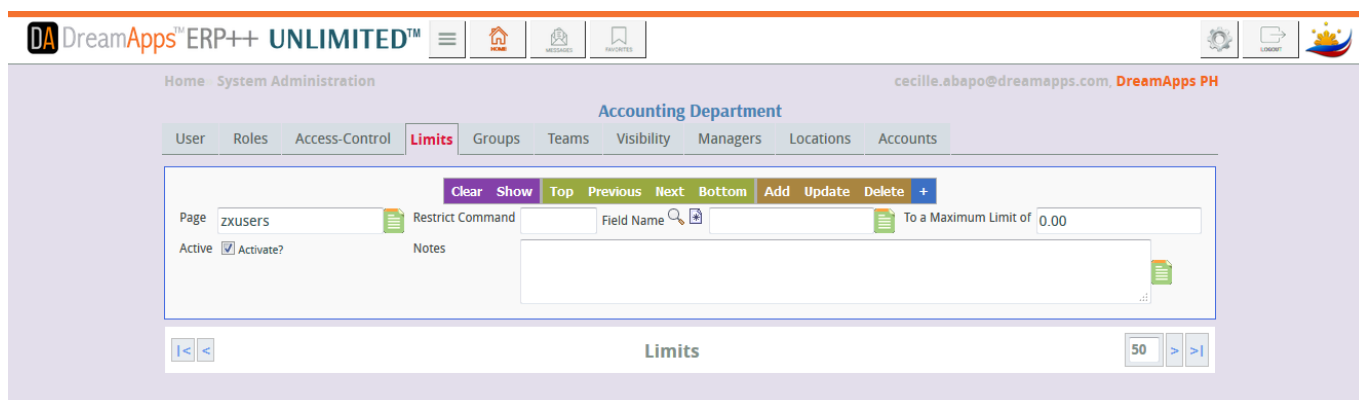
Sample page for creating by Teams



Limits

- The function on user Limit is activated for a particular transaction type only if you have set any limit for at least one user for one transaction type.

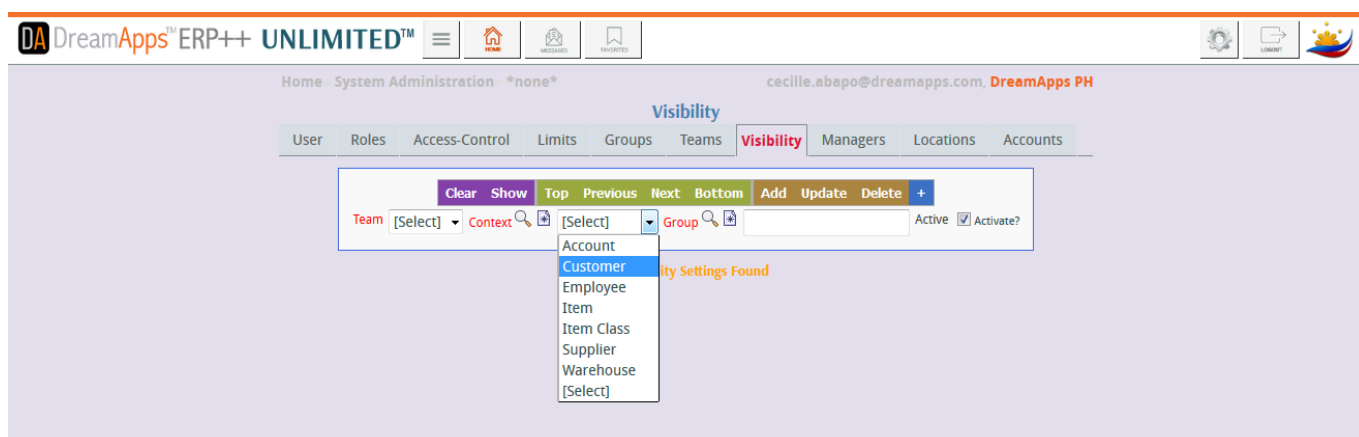
Sample page for activating Limits



Visibility

- Once you set up any value for a particular context, all users not satisfying the condition will be barred from viewing any record in all lists in the system.

Sample page for setting visibility



From:

<http://wiki.dreamapps.com/wiki/> - **DreamApps Wiki**

Permanent link:

http://wiki.dreamapps.com/wiki/doku.php?id=new:user_and_security&rev=1474098230

Last update: **2016/09/17 07:43**

