Module 8
Security

By Kitti Upariphutthiphong
Technical Consultant, ecoSoft™
kittiu@gmail.com
Module Objectives

- Set up Users and Roles
- Understanding about System / Client / Organization
- Understanding about Role Security and Data Security
What we face?

In a real ERP implementation, there are many people, i.e., General Manager, Accounting Manager, Warehouse Manager, Accounting staff, warehouse staff, shipping staff, and so on) involved in operating the system.

Because every individual has his or her own responsibilities in the organization, the system should help the organization manage the access rights to information and perform activities in the system.
Data Layers

- **System**
  - System Definition
  - Shared Setup

- **Client**
  - Client/Org Definition
  - Shared Setup

- **Organization**
  - Transactions
Module 8.1
Role Security
**Access Levels**

Security Access

=  
User (role) login to the ADempiere  
What Functions they have the right to access

**Role**

**User Level**
1. Client  
2. Organization  
3. Client + Organization  
4. System

**Data Access Level**
1. All  
2. Client only  
3. Client + Organization  
4. Organization  
5. System only  
6. System + Client

Note: give default access to features, but can always overwrite.
Example Scenario on **Default** Access Level

<table>
<thead>
<tr>
<th>Object</th>
<th>Data Access Level</th>
<th>System</th>
<th>Client + Org</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>![System icon]</td>
<td>System</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Calendar icon]</td>
<td>System + Client</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>![Client icon]</td>
<td>Client + Organization</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>![Settings icon]</td>
<td>All</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Configuring Role Access Rights

Role Level

Optional
- Access all Orgs
- Maintain Change Log
- Show accounting
- Can Report
- Can Export

Org Access
- Window Access
- Process Access
- Form Access
- Task Access
- Doc Action Access
Create new user

- Login to ADempiere as **Client**
  - Username: GardenAdmin
  - Password: GardenAdmin
  - Role: GardenWorld Admin
  - Client: GardenWorld
  - Organization: Fertilizer

- Create 2 new users
  - Open **User** window
  - Create new users with following information

<table>
<thead>
<tr>
<th>Field</th>
<th>1st user</th>
<th>2nd user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Name</td>
<td>Daniel</td>
<td>Moses</td>
</tr>
<tr>
<td>Search Key</td>
<td>Daniel</td>
<td>Moses</td>
</tr>
<tr>
<td>Password</td>
<td>123456</td>
<td>123456</td>
</tr>
</tbody>
</table>

These users are not yet connected to any role, so they still cannot access the system quite yet. If you try to login, there will be no role selection in the login dialog.
Create new roles

- Create 2 new roles
  - Open **Role** window
  - Create new roles with following information

<table>
<thead>
<tr>
<th>Field</th>
<th>1st Role</th>
<th>2nd Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Name</td>
<td>All Access</td>
<td>Restricted Access</td>
</tr>
<tr>
<td>User Level</td>
<td>Client + Organization</td>
<td>Organization</td>
</tr>
<tr>
<td>Manual</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Preference Level</td>
<td>Client</td>
<td>Organization</td>
</tr>
<tr>
<td>Maintain Change Log</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Show Accounting</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Access all Orgs</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Can Report</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can Export</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- For the All Access role, select all of the checkboxes in the Allow Info in Role fields group.

  **All Access** role (which has the Manual checkbox deselected), the Window Access, Process Access, Form Access, Workflow Access, Task Access, and Document Action Access will be granted automatically, based on User Level selection.
Assign User to new role

- **Assign user to role** **All Access**
  - Open Role window
  - With Role = All Access selected
  - Click on User Assignment tab
  - Click New
    - Organization: *
    - User: Daniel
  - Click Save

- **Assign user to role** **Restricted Access**
  - Open Role window
  - With Role = Restricted Access selected
  - Click on User Assignment tab
  - Click New
    - Organization: *
    - User: Moses
  - Click Save
  - At this point, user Moses still cannot login as it has no Organization assigned yet.

- **Assign user to role** **Restricted Access**
  - With Role = Restricted Access selected

- Click on Org Access tab
- Click New
  - Organization: Fertilizer
- Click Save

At this point we already created 2 roles.

**All Access** role will have access to every org and every role feature, i.e., Maintain Change Log, Show Accounting (Accounting Tab, Post Account button, etc.), Can Report (view and print report), Car Export (export data out of the system).

**Restricted Access** role can access only access Fertilizer org and have no access to any window / form / process yet.
Assign Window Access to a role

• Assign 2 windows to **Restricted Access** role.
  – Open **Role** window
  – With Role = **Restricted Access** selected, click on **Window Access** tab.
  – Assign following windows.

<table>
<thead>
<tr>
<th>Field</th>
<th>1st data</th>
<th>2nd data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Org</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Window</td>
<td>Purchase Order</td>
<td>Material Receipt</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Selected</td>
<td>Selected</td>
</tr>
</tbody>
</table>

• Test login with **Restricted Access** role and see the change.
  – Logoff and login again,
    - **Name**: Moses
    - **Password**: 123456
    - **Role**: Restricted Access
  – View the Menu, now you will see the 2 windows.

• Test Printing Purchase Order Form
  – Open Purchase Order window.
  – With any opening Purchase Order, click on **Print Preview** button.
  – You will notice that report is not opened. This is because, this role still don’t have access right to the **Report Process** for this window.
  – Look at the bottom left of the window, a message is shown, **Cannot access Process 110**

**At this point, user only have access to the window, but not the underlining report process. Next step we will also assign the access to the Process**
Assign Process Access to a role

- Find out the Process name of Process ID 110
  - Logoff and login again,
    - **Name:** System
    - **Password:** System
    - **Role:** System Administrator
  - On Lookup window, click on Advanced tab
    - **Column:** Process (ID)
    - **Operator:** =
    - **Query Value:** 110
  - Click OK to search
  - The result show that the Search Key for this Process ID 110 is Rpt C_Order

- Assign Process to Restricted Access role
  - Logoff and login again,
    - **Name:** GardenAdmin
    - **Password:** GardenAdmin
    - **Role:** GardenWorld Admin
  - Open Role window
  - With **Role = Restricted Access** selected, click on Process Access tab.
  - Assign following process
    - **Organization:** *
    - **Process:** Rpt C_Order
    - **Read/Write:** Selected
  - Now, try to login as Restricted Access role again and test print preview a Purchase Order. **It should work!**

*We will not test for Workflow/Form/Document Action Access here. The same concept apply.*
Module 8.2
Data Access Restriction
Data Access Restriction

**Data Level**

Optional
- Encrypted Feature
- Obscure Feature

**Role Data Access**
- Personal Lock
- Record Access
- Table Access
- Column Access
- Report Access
- Export Access
Scenario 1

- Any user that can open Purchase Order window will see Document Types
  - MM Receipt
  - MM Receipt with Confirmation

- What if we want to restrict users in Restricted Access role to use only MM Receipt document type and not MM Receipt with Confirmation?
Restrict a Record Access to a Role

- Login to ADempiere as **Client Admin**
  - **Username:** GardenAdmin
  - **Password:** GardenAdmin
  - **Role:** GardenWorld Admin

- Enable **Personal Lock** to Admin
  - Open **Role** window.
  - Lookup for **Role = GardenWorld Admin**
  - Select **Personal Lock** field and Save change
  - Logout and re-login as GardenWorld Admin again.
  - Now, this GardenWorld Admin role will have Personal Lock icon in and opening window.

- Block the Document Type **MM Receipt with Confirmation** from **Restricted Access** role
  - Open **Document Type** window
  - With record **Document Type = MM Receipt** selected, click **Ctrl** button + **Personal Lock** icon

- A dialog will open, select **Role = Restricted Access** and click **OK**

- Now the Restriction to this record for the role is created.

- Login again as **Restricted Access** role
  - Open Purchase Order window, click **New**
  - Only **MM Receipt** is listed for DocType

This restriction apply only when **New** record. If you want to restrict all dependent records, also check **Dependent Entities** checkbox in Record Access Dialog.

2 ways to remove lock
- From the **Record Access Dialog**
- From **Role Data Access window | Record Access tab**
Scenario 2

• Suppose that you need to grant access to a Restricted Access role that can only read or view the Material Receipt window and cannot add or alter any information in this window.

• And we want to control this access in the Table level, not just interface layer, how do we do?

  (Interface Layer, we can still use Role’s Window Access to control)
Restrict a Table Access to a Role

- Login to ADempiere as **Client Admin**
  - **Username:** GardenAdmin
  - **Password:** GardenAdmin
  - **Role:** GardenWorld Admin

- Find the document's target table.
  - Opening the **Material Receipt** window and clicking on Record Info. In this case, the table name is **M_InOut**.

- Restrict the Table **M_InOut** from **Restricted Access** role
  - Open **Role Data Access** window
  - Click **Table Access** tab
  - Click **New**
    - **Table:** M_InOut_Shipment/Receipt
    - **Exclude checkbox:** Selected
    - **Access Type:** Accessing
    - **Read Only:** Selected
  - Click **Save**

- Re-Login again as **Restricted Access** role
  - Open **Material Receipt** window
  - Now, only **read-only access** and will not be able to alter or add any information.

*In addition, this **Role Data Access** window / **Table Access** tab can also use to restrict the access to **Report** and **Export** for the specified table and role.*

For **Report** restriction, choose **Access Type = Reporting**
For **Export** restriction, choose **Access Type = Exporting**
Scenario 3

- Well, what we need is just to make sure that this role cannot alter the Purchase Order's Date Ordered only. We need anyone who is connected with this role to use a default Date Ordered.

- How to we do that to Restricted Access role?
Restrict a Column Access to a Role

• Login to ADempiere as **Client Admin**
  – **Username**: GardenAdmin
  – **Password**: GardenAdmin
  – **Role**: GardenWorld Admin

• Restrict the Column Table **M_InOut** from **Restricted Access** role
  – Open **Role Data Access** window
  – Click **Column Access** tab
  – Click **New**
    ▪ **Table**: C_Order_Order
    ▪ **Column**: DataOrdered_Date Ordered
    ▪ **Exclude checkbox**: Selected
    ▪ **Read Only**: Selected
  – Click **Save**

• Re-Login again as **Restricted Access** role
  – Open **Purchase Order** window
  – Now, column **Date Ordered** will be read-only.
Test Your Knowledge

1. All Client will share the Same System Configuration but different Client Configuration?

2. A user in ADempiere can be assigned for more than 1 Role of the same client?

3. We can create a Client user that can access to all other Clients in ADempiere?

4. In Role window, what is Manual field used for? I.e., What different when it is Checked and it is Not Checked?

5. We can restrict a record access to a User?