CHAPTER 4: SECURITY

Objectives

The objectives are:

- Describe the elements of Role Based Security in Microsoft Dynamics® AX.
- Setup a new user.
- Assign roles to a user.
- Assign a security role to a user.
- Edit duties assigned to a role.
- Edit privileges assigned to a duty.
- Edit permissions assigned to a privilege.
- Search for roles with access to a menu item.

Introduction

Role based security provides an extensible framework for defining access to the Microsoft Dynamics AX application and data.

A security role relates to a job role that an end-user has within an organization. The role includes duties, privileges and permissions required to perform the tasks required in that role.

The maintenance of roles and duties is typically undertaken by the system administrator in the rich client.

The maintenance of privileges and permissions is typically undertaken by a developer in the developer workspace.

The framework and related tools assist the security administrator to ensure the system is secure.

Definitions

Role based security is designed with the following base concepts.

An end-user is given one or more **security roles.** A security role represents a behavior pattern that a person in the organization can play. An example is the Accounts receivable manager. A security role includes one or more duties.

A **duty** is a responsibility to perform one or more tasks. Examples of the Accounts receivable manager's duties are to maintain the customer master and inquire into the chart of accounts. A duty includes one or more privileges

Privileges specify the access that is required to perform a duty. For example, the duty of maintaining the customer master requires privileges to maintain customers and maintain customer bank accounts. A privilege includes one or more permissions.

Permissions include the access level to one or more securable objects that are required to perform the function associated with an **entry point**. For example, the privilege of maintaining customers requires permissions that give full control to the customer form accessed through the entry point of a display menu item. It also requires full control to create a new address accessed through the entry point of an action menu item.

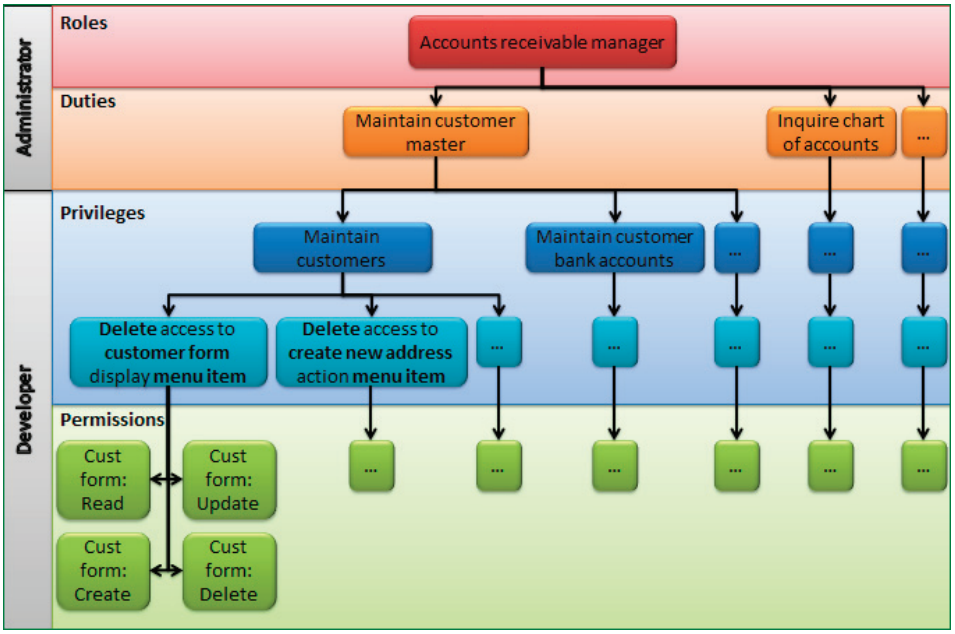

FIGURE 4.1 SECURITY EXAMPLE

Entry Points

An entry point is the element that is triggered by a user action to start a particular function. There are three different categories of entry points in Microsoft Dynamics AX:

- **Menu items** point to forms, reports and classes that an end-user can access from the rich client.
- **Web content items** point to URLs and actions that an end-user can access from the Enterprise Portal.
- **Service operations** are used in document service classes in the Application Integration Framework (AIF). AIF exchanges data with external systems by sending and receiving XML documents.

Permissions

Permissions refer to the access levels that can be applied to the securable objects. This could include any tables, fields, forms, reports or server side methods that are accessible through an entry point.

Permissions are maintained by a developer in the Application Object Tree (AOT).

Access levels available are:

AOT name	Label	Description
No Access	No Access	Does not provide any access to data.
Read	View	An end-user can view data.
Update	Edit	An end-user can view and edit data.
Create	Create	An end-user can view, edit and create new data.
Correct	Correction	An end-user can view, edit, create new and correct date-effective records without creating new records.
Delete	Full control	An end-user can view, edit, create new and delete data.

Permissions that give access to reports or classes need only to have access or not have access. By convention, reports are typically given read access and classes are typically given delete access.

Permissions that give access to tables or fields can make use of all access levels. Possible permission levels are defined on the entry point target. For example, a form might allow permission levels to read, update, create or delete. The level to be granted to an end-user is defined on the permission.

Privileges

A **Privilege** is a group of related permissions that are required to perform a duty.

Privileges can be assigned directly to roles. However, for easier administrative maintenance and to use the Segregation of Duties feature, it is recommended to group privileges into duties and assign duties to roles.

Privileges are typically maintained by a developer in the AOT however they can also be maintained by a system administrator in the rich client.

A best practice is for privileges to be maintained in the AOT and to assign privileges to duties.

Duties

Duties are a group of related privileges required to perform a task.

Duties are grouped into the following six **Process Cycles.**

- Conversion cycle
- Cost accounting cycle
- Expenditure cycle
- Human capital management cycle
- Information technology cycle
- Revenue cycle

Process cycles are used in the rich client to make it easier for a system administrator to view and find related duties when setting up security.

Roles

Roles are a group of duties that are required by an end-user to do his or her job based on the end-user's role in the organization.

Roles can be organized into a **role hierarchy**. Roles can contain sub-roles and inherit the permissions from the sub-role. For example, the accounting manager role could be defined as a combination of the manager role and the accountant role. A role hierarchy reduces the need for duplicating security access that makes access change management simpler.

Set Up a New User

Users are setup in the rich client. They are typically imported from Active Directory.

A user is assigned multiple roles. An internal user is assigned the following two roles in addition to functional roles:

- The **System user** role provides access to basic functionality and tools so that a user can access and use base functions in Microsoft Dynamics AX.
- The **Employee** role provides access to base functionality that all internal roles can use. This includes employee self-service on the Enterprise Portal.

Procedure: Import User from Active Directory

Scenario: Tony Krijnen has just started with Contoso in the Accounts Receivable Department. Chris, the Information Technology (IT) engineer, is responsible for setting up new users and assigning security. Chris has already set up Tony as a user in Active Directory and now he needs to give him access to Microsoft Dynamics AX.

1. Open the Microsoft Dynamics AX client.
2. Open the **Users** form. **System Administration > Common > Users > Users**.
3. Click **New > Import** in the Action Pane.
4. Click **Next**.
5. Select the domain name **contoso.com**.
6. Enter **Tony** for the first name.
7. Click **Next**.
8. Click **Select all**.
9. Click **Next**.
10. Click **Next**.
11. Select only **System User** and **Employee** roles. Chris is not yet sure what level of access Tony needs.
12. Click **Next**.
13. Select **Accounts receivable administrator** profile in **Same profile in all companies**. This defines Tony's role center.
14. Click **Next**.
15. Click **Finish**.

Procedure: Give user access to SharePoint

Tony will also need access to SharePoint in order to view his roll center page. The following procedure will give Tony access to the SharePoint Enterprise Portal site.

1. Open Internet Explorer
2. Click **Site Actions > Site Permissions**
3. Click **Grant Permissions**
4. In the **Users\Groups** box, enter **Tony**
5. Click **Check Names**
6. Check **Full Control**
7. Click **OK**

Assign a User to a Role

Roles are typically maintained by the system administrator in the rich client however they can also be maintained by a developer in the AOT.

The **Security roles** form available in the rich client displays all roles defined in the application and the duties associated with each role.

This form can be accessed from **System Administration > Setup > Security > Security roles**.

New roles can be created from the **security roles** page.

Roles and associated duties can also be viewed in the **security** node in the AOT.

Security Roles Form

The **security roles** form displays the following information:

- All existing **Roles** are listed in the left pane of the form.
- The **AOT name** for the selected role is displayed at the top center of the form together with the name and description. The AOT name is the object name displayed in the AOT.
- The R**ole content** pane in the bottom center of the form displays the duties that are associated with the selected role.
- The **FactBox** pane contains three FactBoxes that contain related information.
  - **Roles with selected duty** display other roles that contain the duty currently selected in the Role content pane.
  - **Privileges in selected role** displays a list of privileges associated with the selected role.
  - **Users with selected role** displays a list of all users assigned the selected role.

- The **Action Pane** includes various actions including creating or deleting roles, assigning users to a role and overriding permissions currently granted to a role.

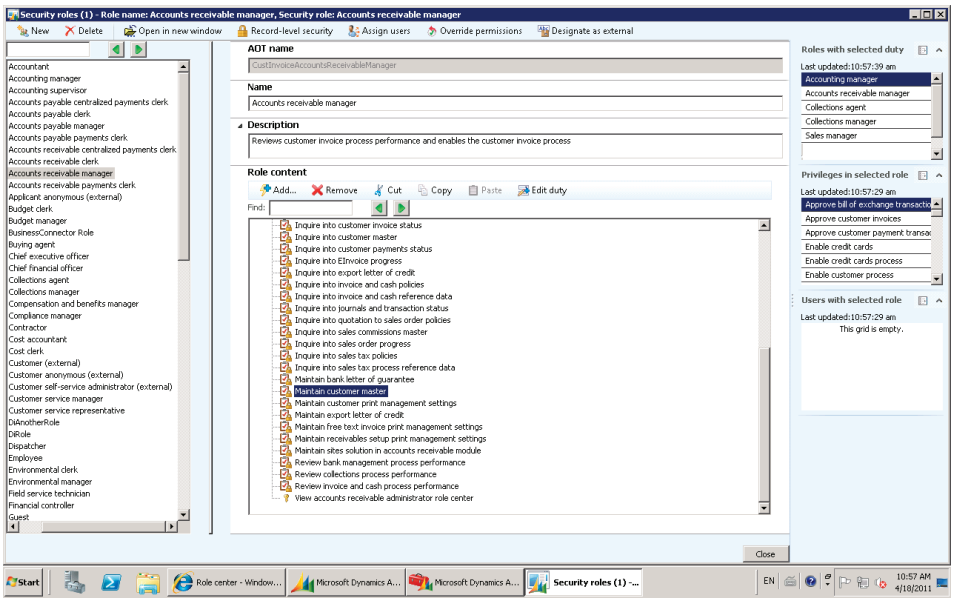

FIGURE 4.2 SECURITY ROLES FORM

Procedure: Add Roles to an Existing User

Scenario: Chris is advised that Tony Krijnen is the new Accounts receivable manager. He needs to assign that role to Tony's user account.

1. Open the Microsoft Dynamics AX client.
2. Go to **System Administration > Common > Users > Users**.
3. Double-click Tony Krijnen in the grid to edit his record.
4. Click **Assign roles** in the **User's role** section of the form.
5. Select **Accounts receivable manager** and click **OK**.
6. Click **Start > Power button options > Switch User**.

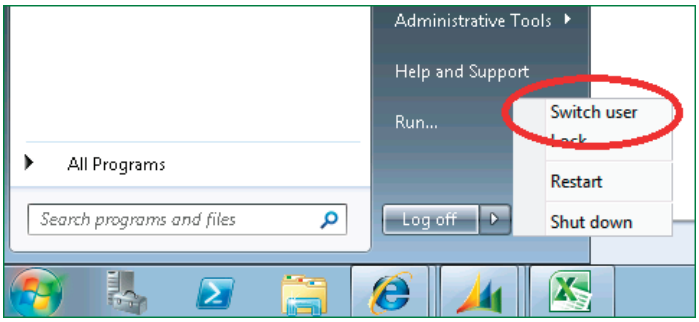

FIGURE 4.3 SWITCH USER

7. Press **Ctrl-Alt-Delete** to log on.
8. Click **Other User**.

9. Log on as **Tony**, password **Pa$$w0rd**.
10. Run the Dynamics AX client.
11. View the changes in Tony's access.
12. Switch user back to Administrator

Security Roles in the AOT

You can also view and edit roles in the **Security > Roles** node in the AOT. You can right-click the Roles node to add a new role, and drag-and-drop duties from the **Security > Duties** node to add duties to a role.

NOTE**: You might need to refresh elements in the AOT so that the changes made in the rich client are visible. In the developer workspace, navigate to **Tools** menu > **Caches > Refresh Elements.

Change Duties on a Role

The system administrator maintains the assignment of duties to roles in the rich client; however this can also be maintained by a developer in the AOT.

Duties can be added or removed from a role in the **Security roles** form available in the rich client.

This form can be accessed from **System Administration > Setup > Security > Security roles.**

Duties assigned to a role can also be edited in the **security** node of the AOT.

Procedure: Add Duties to an Existing Role

Scenario: Tony Krijnen will be working closely with service related customers so he needs access to view service orders which is not included in the standard Accounts receivable manager role. Chris is asked to add service order access to the Accounts receivable manager role.

1. Open the **Rich client**.
2. Go to **System Administration > Setup > Security > Security roles**.
3. Click **Accounts receivable manager** in the list of roles on the left side of the form.
4. Click the **Add** button in the **Role content** section in the center of the form to add a new duty.
5. Expand the **Conversion cycle** process cycle.
6. Select the **Inquire into service orders** privilege.
7. Click **Close**.
8. Click **Start > Power button options > Switch User**.
9. Press **Ctrl-Alt-Delete** to log on.
10. Click **Other User**.

11. Log on as **Tony**, password **Pa$$w0rd**.
12. Run the Dynamics AX client.
13. View the changes in Tony's access.
14. Switch user back to Administrator.

Adding Duties to a Role in the AOT

Duties can also be assigned to a role in the **Security > Roles** node in the AOT. You can also drag-and-drop duties from the **Security > Duties** node to a **role**.

***NOTE**: You might need to refresh elements in the AOT so the changes made in the rich client are visible. In the developer workspace, navigate to **Tools** menu > **Caches > Refresh Elements**.*

Change Privileges on a Duty

The assignment of privileges to duties is maintained by a developer in the **security node** of the AOT.

The **Security privileges** form available in the rich client displays all duties defined in the application and the privileges associated with each duty. Duties are grouped by **process cycle**. Privileges cannot be added to a duty from here.

This form can be accessed from **System Administration > Setup > Security > Security privileges.**

Procedure: Add a Privilege to a Duty

Scenario: Chris, the IT Manager, is asked to add access to the Service order margin report for everyone with access to view service orders. Chris realizes the best way to do this is to add a privilege with permission to access the report to the Inquire on service order duty.

1. Open the AOT.
2. Expand the **security > duties > smaServiceOrderProgressInquire** node.
3. Open a second AOT.
4. Expand the **security > privileges > smaServiceOrderMarginGenerate** node.
5. Drag-and-drop the privilege to the duty.
6. Click **Start > Power button options > Switch User**
7. Press **Ctrl-Alt-Delete** to log on
8. Click **Other User**
9. Log on as **Tony**, password **Pa$$w0rd**.

10. Run the Dynamics AX client.
11. View the changes in Tony's access.
12. Switch user back to Administrator

Security Privileges Form: Duties

The **security privileges** form displays information about the privileges and permissions associated with a duty in the rich client.

Both duties and privileges can be viewed in this form. When a duty is selected, the form includes the following information:

- All existing **Duties** are listed in the left pane of the form. Duties are grouped by **Process cycle**.
- The **AOT name** for the selected duty is displayed at the top center of the form together with the name and description. The AOT name is the object name displayed in the AOT.
- The **Privileges** pane in the bottom center of the form displays the privileges that are associated with the selected duty.
- The **FactBox** pane contains three FactBoxes that display related information.
  - **Roles with selected duty** display other roles containing the duty that is currently selected.
  - **Privileges with selected permission(s)** is only used when this form is used to view a privilege.
  - **Users' assistance hint** provides help for a system administrator editing security from this form.

- The **Action Pane** includes various actions including creating, deleting, copying or pasting duties and permissions.

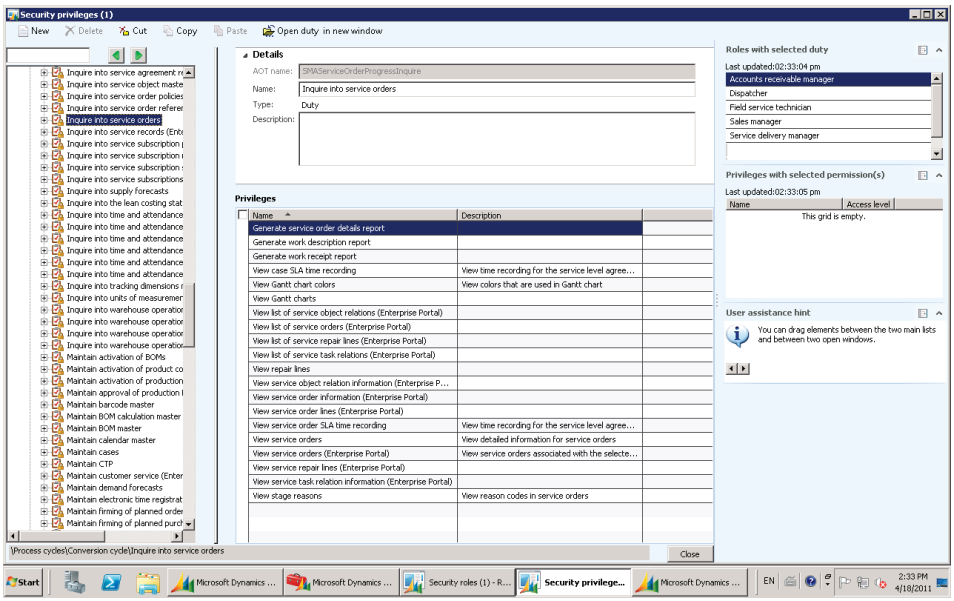

FIGURE 4.4 SECURITY PRIVILEGES FORM

Security Privileges Form: Privileges

When an end-user expands a duty in the tree, a list of privileges associated with the duty displays on the left side of the form. When a privilege is selected, the form includes the following information:

- The **AOT name** for the selected privilege is displayed at the top center of the form together with the name and description. The AOT name is the object name displayed in the AOT.
- The **Permission** pane in the bottom center of the form displays the permissions that are associated with the selected privilege.
- The **FactBox** pane contains three FactBoxes that display related information.
  - **Roles with selected duty** display other roles that contain the duty that is currently selected.
  - **Privileges with selected permission(s)** displays a list of privileges associated with the selected role.
  - **Users' assistance hint** provides help for a system administrator editing security from this form.

- The **Action Pane** includes various actions including creating, deleting, coping or pasting duties and permissions.

Assign a Permission to a Privilege

The assignment of permissions to privileges is typically maintained by a developer in the AOT; however this can also be maintained by a system administrator in the **Security privileges** form in the rich client.

Menu items and web content items can be dragged-and-dropped onto the entry point node on a privilege in the AOT. The permission level is set on the properties.

Procedure: View Permissions

Scenario: Chris wants to view the permissions included in the privilege Maintain customer records (financials) which is assigned to the duty Maintain customers.

1. Open the AOT.
2. Expand the **security > privileges > custTableMaintain > Entry points** node. Chris can view all of the menu items and web content items that this privilege permits access to.
3. Click **CustTable** and view the **Properties.** The properties show the object type is a MenuItemDisplay, the object name is CustTable and the access level is Delete.
4. Collapse **Privileges** and **Security**.
5. Expand **Forms > CustTable > Permissions**. The possible access types are listed and include read, update, create and delete.

Investigate Access

Auditing security can be a difficult task. Security tools are provided to assist in this process.

The **security roles** and **security privilege** forms in the rich client provide FactBoxes that give further information about the relationships between permissions, privileges, duties and roles.

Tools are also available within the AOT to view from a menu item, all related security roles and objects. This is useful if you need to know all users who have access to a particular form, report or action.

Procedure: View All Roles with Access to CustTable Form.

Scenario: Chris wants to know all roles that have access to the customer list page.

1. Open the AOT.
2. Expand the **Menu items > Display** node.
3. Right-click **CustTableListPage** and click **Add-ins > Security Tools > View related security roles**.
4. A list of all roles with access to the Customer table list page is displayed.

Lab 4.1 - Create a New Security Role

Scenario

June Low is employed in the new role of veterinary receptionist. June will be receiving patients at the front desk and will need access to maintain customer information and pet information. She will also need to view breeds and species. Chris, the IT Engineer, needs to create a new role for the veterinary receptionist and add duties so that she can access these areas of the application. June is already created in Microsoft Dynamics AX and is assigned the system user and employee roles. Chris needs to assign her the new role.

Challenge Yourself!

Create a new a new role and assign it to June with the following duties:

- Maintain customers
- Maintain pets

Maintaining pets requires the following privileges:

- Maintain pets
- View pet types

Step by Step

1. Open the **AOT**.
2. Expand **Security > Privileges**.
3. Right-click **Privileges** and select **New Privilege**.
4. In **Properties** change the name to **MaintainPets** and the label to **Maintain pets**.
5. Right-click **Privileges** and select **New Privilege**.
6. In **Properties** change the name to **ViewPetTypes** and the label to **View pet types**.
7. Expand Maintain pets to display **Entry points**.
8. Open a second **AOT**.
9. Expand **Menu items > Display**.
10. Drag-and-drop **vetCustPetTable** to the **entry points node** and specify **Delete** access in the property sheet.
11. Expand **View pet types** to display Entry points in the first AOT.
12. Drag-and-drop **vetSpeciesTable** to the entry points node and specify **Read** access in the property sheet.
13. Expand **Security > Duties**.
14. Right-click **Duties** and select **New Duty**.
15. Rename the new duty to **MaintainPets**.

16. Set the Label property to **Maintain pets**.
17. Drag-and-drop the **MaintainPets** privilege to the Maintain pets duty.
18. Drag-and-drop the **ViewPetTypes** privilege to the Maintain pets duty.
19. Expand **Security > Process cycles.**
20. Drag-and-drop the **Maintain pets duty** to the **TaxRevenue** cycle.
21. Open the **Security roles** form in the rich client.
22. Click **New**.
23. Specify the AOT name **VetReceptionist** and the description of the **Veterinary receptionist**.
24. Click the **Add** button.
25. Expand **Revenue cycle**.
26. Select **Maintain pets**.
27. Select **Inquire into customer master**.
28. Click **Close**.
29. Click **Assign users** in the **Action Pane**.
30. Select the **Vet Receptionist role**.
31. Click the **Manually assign** button.
32. Select **June** and click **Assign to role**.
33. Click **Close**.

Summary

This course showed how to set up a new user, assign a user to a role, change duties on a role, change privileges on a duty and assign permissions to a privilege.

Test Your Knowledge

1. Match the following item with the correct description:

_____ 1. A group of privileges _____ 2. A group of duties _____ 3. A group of permissions	a. Role b. Privilege c. Duty

2. What are the base roles which every internal employee should be assigned? (Select all that apply)

   ( ) System administrator

   ( ) System user

   ( ) Employee

   ( ) Vendor

3. Which of these are entry points? (Select all that apply)

   ( ) Web content items

   ( ) Menu items

   ( ) Forms

   ( ) Service operations

Quick Interaction: Lessons Learned

Take a moment and write down three key points you have learned from this chapter

1.

2.

3.

Solutions

Test Your Knowledge

1. Match the following item with the correct description:

__c__1. A group of privileges __a__2. A group of duties __b__3. A group of permissions	a. Role b. Privilege c. Duty

2. What are the base roles which every internal employee should be assigned? (Select all that apply)

   ( ) System administrator

   (√) System user

   (√) Employee

   ( ) Vendor

3. Which of these are entry points? (Select all that apply)

   (√) Web content items

   (√) Menu items

   ( ) Forms

   (√) Service operations