CHAPTER 6: MANAGE USER RIGHTS AND PROFILES

Objectives

The objectives are:

- Explain how authentication works in Microsoft Dynamics® NAV
- Explain the concepts of the superuser, roles, and permissions
- Manage security for RoleTailored client users
- Create, assign, and work with user profiles for the RoleTailored client
- Create a new role and assign permissions to it
- Apply security filters in Microsoft Dynamics NAV with Microsoft® SQL Server®
- Manage security for Classic client users
- Perform user-specific setup
- Use Microsoft® Active Directory® with Microsoft Dynamics NAV

Introduction

An enterprise business solution must have a built-in security system that protects the database and the information that it contains from being accessed by unauthorized people. It must also allow the application administrator to specify what authorized users are allowed to do in the database—whether they can:

- Read data
- Insert data
- Modify data
- Delete data
- Execute data

(The five database actions are referred to as RIMDEX in short.)

The minimum acceptable level of security requires that each user is assigned an ID and a password. This ensures that only authorized personnel can gain access to the database. This is database-level security.

A medium level of security enables you to limit users' access to only certain types of information stored in the database. In other words, they can only gain access to particular tables in the database. This is table-level security.
A high level of security enables you to limit users' access to only specified records stored in the tables. This is record-level security and is available using Microsoft Dynamics® NAV with Microsoft® SQL Server®.

Along with logins and SQL Server security filters, companies can control user access to Microsoft Dynamics NAV data by means of roles and permissions. Additionally, administrators can set up and assign users to profiles for use in the RoleTailored client.

The responsibility of the application administrator is to manage the security system.

**Authentication**

With several security systems interacting, the terminology can be confusing, so before explaining how the Microsoft Dynamics NAV security system works, it is necessary to clarify two key concepts:

- **Authentication**: The process by which the system validates the user's identity. This can be done by having users enter an ID and password when they log on. Microsoft Dynamics NAV supports two kinds of authentication: Windows authentication and database server authentication.

- **Login**: When a user has identified himself or herself and has been recognized by the system, he or she is granted access to the parts of the system for which he or she has permission.

If the user has logged on to the system with Microsoft Windows authentication, then he or she has been assigned a Windows login.

If the user has logged on to the system with database server authentication, then he or she has been assigned a database login.

**Windows Authentication**

One of the main features of Windows security is the single sign-on system. Microsoft Dynamics NAV supports this feature and can also use more of the features contained in the Active Directory security system.

The Windows single sign-on and the unified login supported by Windows are the same. This lesson refers to both of these systems as Windows authentication.

With Windows authentication, when users try to connect with the server to open a database, they do not have to supply a user ID or password. Microsoft Dynamics NAV automatically asks Windows to confirm whether this user, who has already logged on to the network, has a valid Windows account and whether this account gives the user the right to access this particular server.
If the user is allowed to access the server, then Microsoft Dynamics NAV checks to see if he or she has been assigned a Windows login within Microsoft Dynamics NAV. If the user has a Windows login, he or she will be granted access to the database.

The user is granted access to Microsoft Dynamics NAV and given the permissions specified for that Windows user and those specified for any Windows groups of which he or she is a member.

If the user does not have a valid Windows account or if his or her account does not include permission to log on to the Microsoft Dynamics NAV database, authentication fails and the user receives an error message.

The Windows authentication system includes the following security features:

- Secure validation and encryption of passwords
- A time limit on passwords
- Minimum password length
- Account lockout after an invalid password is entered

**Database Server Authentication**

With Microsoft SQL Server 2005/2008, you can set the system up so the database logins also have to adhere to Active Directory policies regarding password expiration and minimum password requirements.

If the server does not support Windows authentication, then database server authentication must be used. It is also used when the network administrator has chosen not to use Windows authentication. The application administrator decides which kind of authentication each individual user must use by assigning each user or group a Windows login or a database login.

If you have decided to use database server authentication, you must assign each user a database login. This entails creating a user ID and password for the user within Microsoft Dynamics NAV, which the user must enter correctly when accessing a database. You must have superuser permissions to create the database logins.

In Microsoft Dynamics NAV with Microsoft SQL Server, the database server authentication is based on Microsoft's SQL Server authentication. For more information, refer to the "Demonstration: Apply SQL Server Security Filters" lesson in this course.

**NOTE:** The RoleTailored client requires Windows logins and does not support database logins.
Test Your Knowledge: Introduction and Authentication

Fill in the blanks to test your knowledge of this section.

1. The minimum acceptable level of security is called ___________ -level security.

2. ___________ -level security is a medium level of security that enables you to limit access to certain data.

3. A high level of security referred to as ______ -level security is available with the SQL Server.

4. ______ refers to when a user identifies oneself, and is recognized by the system, thus allowing access.

5. Authentication is the process by which the system validates the user's ______.

Security Setup Overview

Microsoft Dynamics NAV gives you complete control over the information that each user can access. You can create users, give them roles and modify the permissions of these users and roles from within Microsoft Dynamics NAV.

To create users in Microsoft Dynamics NAV, you must give them an identity within the database that allows them to log on to the system. When the user has logged into the database, they are able to perform tasks in accordance with the permissions that they have been allocated.

Some of the security set up is handled differently based on the Microsoft Dynamics NAV client. Described herein are the central concepts of the Microsoft Dynamics NAV security system.

NOTE: All administration of security set up (logins, roles, and permissions) is performed through the Classic client, regardless of the client to be used. In this content, it is performed in the Microsoft Dynamics NAV 2009 Classic with Microsoft SQL Server client.

Initiate the Security System

The Microsoft Dynamics NAV security system is initiated when you create the first login. The first login must therefore be for a superuser who is given the SUPER role. The superuser then owns and administers all access to this database from within Microsoft Dynamics NAV. Until you create a superuser, any user with access to the system can carry out any transactions in a Microsoft Dynamics NAV database.
Chapter 6: Manage User Rights and Profiles

One of the first things the superuser must do is create user IDs for the other people who will have access to the database and assign roles to these users. Permissions are allocated at company level in Microsoft Dynamics NAV.

Microsoft Dynamics NAV allows only users that have been given the SUPER or SECURITY roles to administer security. These Microsoft Dynamics NAV users can only grant to other users permissions that they themselves possess.

**Demonstration: Create a Superuser**

**Scenario**: Simon, the Systems Implementer/Consultant at CRONUS, is setting up a new Microsoft Dynamics NAV installation with the RoleTailored client.

Simon sets up a Windows Login for the Administrator—the company's superuser—and then assigns it to the SUPER role before setting up security for other users.

**NOTE**: Delete the Windows login for the Administrator if it already exists.

**Steps: Create a Superuser**

Follow these steps to assign the standard SUPER role to a superuser with a Windows Login:

1. On the Tools menu, point to Security and then click Windows Logins.
2. In the User ID field, enter Administrator.
3. Click the next line and then re-select the line.
4. Click Roles.
5. In the Role ID field, click the look-up arrow and then select the SUPER role.
6. With SUPER selected in the Roles window, click Role and then select Permissions.

The Permissions window holds the groups of permissions that are given to the standard superuser in the database.

**FIGURE 6.1 PERMISSIONS GIVEN TO THE SUPER ROLE**
Steps: Assign the SUPER Role

Follow these steps to assign the SUPER role to the superuser:

1. Close the Permissions window.
2. With the SUPER role selected in the Roles window, click OK.
3. Click the next line.

A superuser is now created in the database, and the SUPER role is assigned to that user.

The superuser only needs to be assigned a single role, because the SUPER role has permissions to everything in the system. All other users, however, need to be assigned at least two or more roles.

As a default, the roles apply to all the companies in the database, but they can be restricted to apply to only a particular company. To do this, in the Roles window, enter the name of the company in the Company Name field.

To have permissions apply to several (but not all) companies, set up one line for each company (each line starting with the same role ID). If you specify that the permissions a user has only apply to a particular company in the database, the user in question will only be able to see that company.

4. Close the open windows.

Standard Roles

Standard security roles for use in the Classic client can be found in the demo CRONUS International, Ltd. company. Security roles for use in the RoleTailored client must be imported. The import process is described in the "Security Set Up for RoleTailored Client" lesson.

Standard roles for use in the Classic client are process-driven, such as FA-FIXED ASSET, EDIT, which includes permissions to edit Fixed Assets. These roles are used in conjunction with other roles to encompass all processes that a user needs to perform.

In contrast, standard roles for use in the RoleTailored client are role-driven, such as Bookkeeper, which includes permissions necessary to work in the Bookkeeper profile. Additional roles can be added to the user for processes not covered in the Bookkeeper role.

Before assigning roles to users, review the standard roles. You can use these roles as they are, modify them, or set up completely different ones. The process of creating a new role is described in the "Create a New Role" demonstration.

NOTE: The standard roles provided for the RoleTailored client are offered as samples and may need to be modified to meet the needs of your company.
Roles and Permissions

Each role in Microsoft Dynamics NAV describes a set of access permissions to the objects in the following table.

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Data</td>
<td>The actual data stored in the tables.</td>
</tr>
<tr>
<td>Table</td>
<td>The tables themselves.</td>
</tr>
<tr>
<td>Form</td>
<td>The forms used to view and enter data.</td>
</tr>
<tr>
<td>Report</td>
<td>The reports used to present the data.</td>
</tr>
<tr>
<td>Dataport</td>
<td>The dataports used to import and export data.</td>
</tr>
<tr>
<td>Codeunit</td>
<td>The codeunits used in the database.</td>
</tr>
<tr>
<td>XMLport</td>
<td>The XMLports used to import and export data in XML format.</td>
</tr>
<tr>
<td>MenuSuite</td>
<td>The object that contains the menus displayed in the navigation pane.</td>
</tr>
<tr>
<td>Page</td>
<td>The pages used to view and enter data.</td>
</tr>
<tr>
<td>System</td>
<td>The system tables in the database that allow the user to make backups, change the license file, and so on.</td>
</tr>
</tbody>
</table>

The following table shows the various permission types that a role can have on an object.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>You can read this object.</td>
</tr>
<tr>
<td>Insert</td>
<td>You can insert data into this object.</td>
</tr>
<tr>
<td>Modify</td>
<td>You can modify data in this object.</td>
</tr>
<tr>
<td>Delete</td>
<td>You can delete data from this object.</td>
</tr>
<tr>
<td>Execute</td>
<td>You can run this object.</td>
</tr>
</tbody>
</table>

The following table shows the options that appear in the permissions fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;blank&gt;</td>
<td>Not selected (the field is empty), and you do not have this permission.</td>
</tr>
<tr>
<td>Yes</td>
<td>This permission is granted, and you have full access to this object. You can always, for example, read this object.</td>
</tr>
</tbody>
</table>
### Special Standard Roles

The following table describes the permissions of special standard roles in Microsoft Dynamics NAV.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>This role can use fundamental (but not high security) tables and functions. The permissions the user gains with this role can only be used in the tables that users normally have access to, such as the navigation pane menu. Assign this role to all Classic client users (except SUPERUSER) because this is a prerequisite for all other roles you assign to them.</td>
</tr>
<tr>
<td>BASIC</td>
<td>This role can use fundamental (but not high security) tables, system table, and functions. The permissions the user gains with this role can only be used in the tables that users normally have access to, such as the navigation pane menu. Assign this role to all RoleTailored client users (except SUPERUSER) because this is a prerequisite for all other roles you assign to them.</td>
</tr>
</tbody>
</table>
Chapter 6: Manage User Rights and Profiles

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY</td>
<td>This role has access to the tables and functions related to security information (users, permissions). Users within this role can grant permissions to others, but only those permissions they themselves have. Therefore, if you want to create an &quot;area superuser,&quot; give the person the SECURITY role plus permissions for the areas (such as Purchases &amp; Payables) in which they can grant and revoke permissions for other users.</td>
</tr>
<tr>
<td>SUPER</td>
<td>This role can read, use, change, and delete all data and all application objects (that your license permits). Microsoft Dynamics NAV requires that at least one user is assigned this role in each database. You cannot alter the permissions that have been granted to this role.</td>
</tr>
<tr>
<td>SUPER (DATA)</td>
<td>This role can read, use, change, and delete all data. This is a role that you usually assign to an accounting manager or another person who can access all the data, but who does not need to make changes in the program.</td>
</tr>
<tr>
<td>SUPER (NAVIPANE)</td>
<td>This role can create navigation pane menus with the navigation pane designer. For example, managers who need to design menus for their staff.</td>
</tr>
</tbody>
</table>

**System Access Roles**

Any user who is not a superuser must be assigned the ALL or BASIC role in addition to roles/permissions that give access to the required areas of the program. The ALL or BASIC role provides fundamental permissions to:

- Log on
- Access the navigation pane menus
- Move around in the program

These roles do not permit access to tables, table data, forms, and so on without further permissions, so there is no logic in assigning it only to a user.

A user who administrates security in only certain areas (such as department managers who administer security for their own departments) must be assigned at least three roles: ALL or BASIC, SECURITY, and the role that provides access to the relevant areas of the database (such as Sales & Receivables).

There is no point in granting permissions to areas that the license file does not include. However, granting such permissions does not cause any problems. Remember to change or add to the permissions if Microsoft Dynamics NAV is customized or additional application areas are purchased.
NOTE: Assign the ALL role only to users accessing the Classic client and the BASIC role only to users accessing the RoleTailored client.

Synchronization

The heart of the security system in Microsoft Dynamics NAV with Microsoft SQL Server is the synchronization process. This process ensures that the information contained in the Users window in Microsoft Dynamics NAV corresponds with the information contained in the SQL Server security system.

SQL Server database user accounts contain information about the permissions that the users have to the objects contained in the database. The information for managing permissions to Microsoft Dynamics NAV objects is contained and administered within Microsoft Dynamics NAV.

Every time a change is made to the Microsoft Dynamics NAV security system, the security system must be synchronized with SQL Server.

To synchronize the security system, click Tools, point to Security, and then click Synchronize All Logins. Individual logins can also be synchronized using the Synchronize Single Login menu item. However, this menu item is only available when a login is selected in the Windows Logins window.

To synchronize the security system, the administrator must have permission to access the Microsoft Dynamics NAV security system.

Security Setup for RoleTailored Client

In the RoleTailored client, assign roles to users based on the area that they must access:

- Role Center
- Departments

To execute most of the tasks in the Role Center, a user must be set up with a Windows Login and then assigned one of 22 predefined standard security roles, in addition to the BASIC special standard role. These roles are imported into Microsoft Dynamics NAV from XML files using the RIM toolkit data migration functionality.

To execute tasks in the Departments menu, a user must be assigned standard security roles, in addition to the BASIC role.

NOTE: The BASIC role is in the XML file so the data migration process must be completed for any user in the RoleTailored client.
Procedure: Import Roles for the RoleTailored Client

Microsoft Dynamics NAV 2009 requires the import of 22 predefined Standard Security roles and permissions that grant users access to tables and table data relevant to the RoleTailored client.

To import and apply roles for the RoleTailored client, follow these steps:

1. In the navigation pane, click **Administration**.
2. Click **Application Setup**, then **Company Setup**, and then click **Data Migration**.
3. In the **Table ID** field, click the look-up arrow and then select 2000000004, **User Role**.
4. Click **Migration** and then select **Migration Fields**.
5. On the Name line, select the **Include** check box.
6. Click **OK** to close the **Migration Fields** window.
7. Click **Functions** and then select **Import from XML**.
8. Browse to and open the **Company Settings** folder (Program Files/Microsoft Dynamics NAV/60/Classic).
9. Click the **UserRoles.xml** file and then click **Open**.
10. Click **OK** when the Setup Data is successfully imported.
11. Click **Migration** and then select **Apply Migration Data**.

Procedure: Import Permissions for the RoleTailored Client

To import and apply permissions for the RoleTailored client, follow these steps:

1. In the **Migration Overview** window, click the next line.
2. In the **Table ID** field, click the look-up arrow and then select 2000000005, **Permission**.
3. Click **Migration** and then select **Migration Fields**.
4. Select the **Include** check box for each field.
5. Click **OK** to close the **Migration Fields** window.
6. Click **Functions** and then select **Import from XML**.
7. In the **Company Settings** folder (Program Files/Microsoft Dynamics NAV/60/Classic), click the **UserRolePermissions.xml** file and then click **Open**.
8. Click **OK** when the Setup Data is successfully imported.
9. Click **Migration** and then select **Apply Migration Data**.
10. Close the **Migration Overview** window.
NOTE: This XML file contains the permissions for the BASIC role only. Permissions for all other roles must be downloaded from PartnerSource and then imported into Microsoft Dynamics NAV 2009 following the same steps listed in the above procedure. You must download and import two separate files: Sample_Roles & Permissions_part1.XML and Sample_Roles & Permissions_part2.XML

Windows Logins

You can add a Windows user or group to the list of Windows logins that can access the system. Users that have been given a Windows login must use Windows authentication to gain access to the database.

The Windows Users & Groups window lists all of the Windows users and groups available in the current forest of domains and domain trees. This window is only available if both the domain controller is running on Windows 2000 Server or Windows Server 2003, and the clients are running on Windows 2000/XP or have been Active Directory enabled. However, if you are running a Windows NT network, you can type in the names of the Windows users and groups in the Windows Logins window. Remember to use the Domainname\Username format.

In Microsoft Dynamics NAV with Microsoft SQL Server, the users' Windows account must be entered in the Windows Login table before any SQL permissions can be assigned to that user in the SQL database.

Demonstration: Set Up Security Access to a Role Center

Every user is assigned a job-related profile by the system administrator. The profile provides a Role Center and one or more menus that give users access to the tasks, lists, reports, and documents that they need most often.

Before assigning profiles, set up the user with the proper security access to that Role Center.

Scenario: Simon, the Systems Implementer/Consultant at CRONUS, needs to set up users with access to their relevant Role Centers in the RoleTailored client. He sets up Alicia Thornber, the Purchasing Agent, with access to the pre-defined Role Center for Purchasing Agent.

Steps: Set Up Security Access to a Role Center

Follow these steps to set up a user with access to a Role Center in the RoleTailored client:

1. On the Tools menu, point to Security and then click Windows Logins.
2. Insert a new line.
3. In the **ID** field, click the look-up arrow to access the **Windows Users & Groups** window.

4. Locate and select Alicia Thornber and then click **OK**.

5. Click off the line and then re-select the line for CONTOSO\alicia.

6. Click **Roles**.

7. In the **Role ID** field, enter **BASIC**.

8. Click the next line.

9. In the **Role ID** field, enter **PURCHASING AGENT**.

10. Click the next line.

11. Close the **Roles** window.

12. On the **Tools** menu, point to **Security** and then click **Synchronize Single Login**. Alternatively, click **Synchronize All Logins** if multiple logins have been set up without running the synchronize process.

13. If **Synchronize All Logins** was selected, click **Yes** in the dialog box to synchronize all logins.

14. Once the synchronize process has finished, close the **Windows Logins** window.

### Procedure: Review Roles Assigned to Windows Logins

To see the Windows logins that have been assigned a particular role in Microsoft Dynamics NAV, follow these steps:

1. On the **Tools** menu, point to **Security** and then click **Roles**.

2. Select the Microsoft Dynamics NAV role to review.

3. Click **Role** and then click **Windows Logins**; the **Windows Logins** window appears, listing the Windows logins that have been assigned this role in the database.

4. To assign a new Windows login to this role from this window, insert a new line, look up in the **Login ID** field, select the Windows login, and then click **OK**.

### Security Access to Departments

The Departments page in the RoleTailored client provides access to parts of the application that are not included in the personalized menus.

All users have access to the Departments menu. It is possible to navigate to everything in Microsoft Dynamics NAV that users have access to, including set up and configuration windows. Therefore, users need to be set up with standard security to limit access to all areas in the Departments menu.
This task can be accomplished using the following methods:

- Assign standard security Roles in addition to the personalized menu
- Add permissions from the standard security Roles to the personalized menu

**IMPORTANT:** While users can modify standard roles, it is recommended to create new roles based on the standard Microsoft Dynamics NAV roles since upgrades and updates can overwrite user changes. This can be done by copying permissions from an existing Microsoft Dynamics NAV role, pasting those permissions into a new role, and then making modifications.

**Demonstration: Set Up Security Access to Departments**

**Scenario:** Annie, the bookkeeper at CRONUS, has been asked to manage some of the XBRL financial reporting. The BOOKKEEPER role and Role Center profile do not accommodate these tasks, thus Annie will have to access the XBRL area from the Departments page.

When Simon sets up security access for Annie, he assigns the roles to access the Bookkeeper Role Center, and then the standard role relating to XBRL.

**Steps: Set Up Security Access to Departments**

Follow these steps to set up a user with access to a Role Center and the Departments page in the RoleTailored client:

1. On the **Tools** menu, point to **Security** and then click **Windows Logins**.
2. Insert a new line.
3. In the **ID** field, click the look-up arrow to access the **Windows Users & Groups** window.
4. Locate and select Annie Herriman and then click **OK**.
5. Click off the line and then re-select the line for CONTOSO\annie.
6. Click **Roles**.
7. In the **Role ID** field, enter **BASIC**.
8. Click the next line.
9. In the **Role ID** field, enter **BOOKKEEPER**.
10. Click the next line.
11. In the **Role ID** field, enter **G/L-XBRL, EDIT**.
12. Click the next line.
13. Close the **Roles** window.
14. On the **Tools** menu, point to **Security** and then click **Synchronize Single Login**.
**NOTE:** It is unnecessary to synchronize after each user is set up; all users can be synchronized simultaneously using the Synchronize All Logins function. Regardless of when it is done, always remember to run the synchronize process when security changes are made.
Lab 6.1 - Create a Windows Login and Assign Roles

The purpose of this lab is to reinforce your understanding of the process required to create a Windows login and assign it to the necessary roles.

Scenario

A new employee, Susan Burk, has accepted the role of Sales Order Processor at CRONUS International, Ltd. As the application administrator, it is your responsibility to set up Susan with security access to the RoleTailored client Microsoft Dynamics NAV as follows:

- Login type = Windows
- ID = CONTOSO\Susan
- Roles =
  - BASIC
  - ORDER PROCESSOR

At this time, Susan requires no access to the Departments page.

Complete the Windows Login security set up by running the synchronize process for this user only.

Challenge Yourself!

1. Create a Windows login for Susan as specified in the scenario.
2. Assign the Roles noted in the scenario.
3. Run the Synchronize process as noted in the scenario.

Need a Little Help?

1. Open the Windows Logins window and insert a new line.
2. Open the Windows Users & Groups window and then locate and select Susan Burk.
3. Open the Roles window.
4. Add the roles as noted in the scenario.
5. Synchronize the Windows login for this user only.

Step by Step

1. On the Tools menu, point to Security and then click Windows Logins.
2. On the toolbar, click New.
3. In the ID field, click the look-up arrow to access the Windows Users & Groups window.
4. Locate and select Susan Burk and then click **OK**.
5. Click off the line and then re-select the line for CONTOSO\susan.
6. Click **Roles**.
7. In the **Role ID** field, enter **BASIC**.
8. Click the next line.
9. In the **Role ID** field, enter **ORDER PROCESSOR**.
10. Click the next line.
11. Close the **Roles** windows.
12. On the **Tools** menu, point to **Security** and then click **Synchronize Single Login**.
13. Once the synchronize process has finished, close the **Windows Logins** window.

### User Profile Setup for the RoleTailored Client

For the RoleTailored client, Microsoft Dynamics NAV 2009 includes pre-defined Role Centers and Profiles to fit many of the fundamental roles in companies. Creating or modifying Role Centers is a development task, but the creation and assignment of Profiles is a setup task performed by an administrator. Typically Profiles are created and then the appropriate Role Center is assigned. Once users are set up, they are assigned to a Role Center through the Profile.

For example, when Alicia, the Purchasing Agent opens the RoleTailored client, she sees the Purchasing Agent Role Center, which has been customized to help her carry out her daily tasks. This Role Center was assigned to her login through the Purchasing Agent profile.

Explained herein are the various processes related to working with user profiles. For information about exporting and importing profiles, refer to F1 help.

**NOTE**: Profiles can be managed in either the RoleTailored client or the Classic client. In this content, it is managed in the RoleTailored client.

### Procedure: Create a Profile

The Profile Card is used to create unique profiles for end-users. Each profile is associated with a Role Center that can then be configured to suit the specific needs for the user. Often profiles are associated with a job title in a company.

To create a profile, follow these steps:

1. Open the RoleTailored client.
2. In the navigation pane, click the **Departments** button.
3. Click **Administration** and then click **Application Setup**.
4. On the **Application Setup** page, click **RoleTailored Client** and then click **Profiles**.
5. Click **New** to create a new record.

![FIGURE 6.2 PROFILE CARD](image)

6. In the **Profile ID** field, type a short, appropriate name that describes the intended role of the user.

7. If necessary, in the **Owner ID** field, click the **Edit** button to view all available logins.

8. Select a Windows user login and then click **OK**.

9. In the **Description** field, type a description of the Profile ID, for example, Order Processor.

10. In the **Role Center ID** field, click the drop-down arrow to view all available Role Centers.

11. Select a Role Center and click **OK**.

12. Select the **Default Role Center** check box to make this the default Profile ID for all users. This is optional.

13. Click **OK** to close the Profile Card.

**Procedure: Assign a Profile to a New User**

The User Personalization Card is used to assign newly configured profiles to end-users. An end-user cannot access their new profile until this step has been completed. This task must be completed by an administrator.

To assign a profile to a new user, follow these steps:

1. On the **Application Setup** page, click **RoleTailored Client** and then click **User Personalization**.

2. Click **New**.

![FIGURE 6.3 USER PERSONALIZATION CARD FOR A NEW USER PROFILE SET UP](image)
3. In the **User ID** field, click the **Edit** button.
4. Select the line for the relevant user and then click **OK**.
5. In the **Profile ID** field, enter the correct profile for this user.
6. In the **Language ID** field, enter an appropriate language ID, or leave this field blank.
7. In the **Company** field, enter a company for which this user/profile combination is relevant.
8. Click **OK** to close the User Personalization Card.

**Procedure: Copy a Profile**

Use the Copy Profile function to create a copy of an existing profile.

To copy a profile, follow these steps:

1. On the **Application Setup** page, click **RoleTailored Client** and then click **Profiles**.
2. Open the **Profile Card** of the profile to copy.
3. On the **Actions** menu, point to **Functions** and then click **Copy Profile**.
4. In the **New Profile ID** field, type a short, descriptive name of the new profile.
5. Click **OK** to copy the profile, and then close the **Profile Card** of the copied profile.

The new profile with the same information as the copied profile is added to the Profiles List. Update the profile information as needed.
Lab 6.2 - Assign a Profile

The purpose of this lab is to reinforce your understanding of the process required to assign profiles to users.

Scenario

Previously, a Windows login was created and security roles were assigned to the new Sales Order Processor at CRONUS, Susan Burk.

As the application administrator, it is now your responsibility to assign the Sales Order Processor profile to her User ID. Set up her profile with the English language and access to the CRONUS International Ltd. company.

Challenge Yourself!

Assign the Profile to Susan's Windows login as specified in the scenario.

Need a Little Help?

1. Open the User Personalization Card and insert a new line.
2. Select the Windows login for Susan.
3. Assign the profile, language, and company as specified in the scenario.

Step by Step

1. In the navigation pane, click the Departments button.
2. Click Administration and then click Application Setup.
3. On the Application Setup page, click RoleTailored Client and then click User Personalization.
4. Click New.
5. In the User ID field, click the Edit button.
6. Select the line for CONTOSO\Susan and then click OK.
7. In the Profile ID field, enter ORDER PROCESSOR.
8. In the Language ID field, enter 1033.
9. In the Company field, enter CRONUS International Ltd.
10. Click OK to close the User Personalization Card.
Demonstration: Create a New Role

If the existing roles do not meet the needs of the organization, create new ones or modify permissions of existing roles.

Scenario: CRONUS needs a new role called G/L Accounts Only. Later, the administrator must modify the role with a restriction to delete data in G/L Accounts. Later again, the role is extended to have reading rights to payment terms and finance charge terms.

NOTE: The processes in this lesson must be performed in the Microsoft Dynamics NAV 2009 Classic with Microsoft SQL Server client.

Steps: Create the New Role and Grant Permissions

Follow these steps to create the G/L Accounts Only role:

1. Open the Microsoft Dynamics NAV 2009 Classic with Microsoft SQL Server client.
2. On the Tools menu, point to Security and then click Roles.
3. Insert a new line.
4. In the Role ID field, type G/L Accounts Only.
5. In the Name field, type Works in G/L accounts.
6. Press ENTER or click the next line to accept the new role. Then click the new role again.
7. Click Role and then click Permissions. The Permissions window for this new role appears. Because this is a new role, the window will be empty.
8. In the Object Type field, ensure that Table Data is selected as the type of object you want to grant permission for.
9. In the Object ID field, enter 15, G/L Account as the specific instance of that object.
10. Accept the default of Yes in all permissions.

FIGURE 6.4 PERMISSIONS GIVEN TO G/L ACCOUNTS ONLY ROLE

Steps: Restrict the Permissions of the New Role

Follow these steps to restrict the deletion permissions of the G/L Accounts Only role:

1. In the Permissions window for the G/L Accounts Only role, clear the Yes value in the Delete Permission column.

FIGURE 6.5 DELETE PERMISSION REMOVED FOR G/L ACCOUNT TABLE

2. Click the next line.
Steps: Extend the Permissions of the New Role

You can also give permissions to multiple objects. This is a useful time-saving feature if you want to radically modify the permissions that apply to a role.

Follow these steps to extend the permissions of the G/L Accounts Only role to also include read permissions in the Payment Terms and Finance Charge Terms tables:

1. In the Permissions window for the G/L Accounts Only role, click All Objects.
2. In the Read Permission column for the Payment Terms table, enter Yes.
3. In the Read Permission column for the Finance Charge Terms table, enter Yes.
4. Click OK to save the selections.

If your database is running on SQL Server, you can also apply security filters as a part of the role. For more information, refer to the "Apply SQL Server Security Filters" demonstration in this course.

5. Close all open windows.
Demonstration: Apply SQL Server Security Filters

Microsoft Dynamics NAV 2009 with Microsoft SQL Server supports record-level security and allows you to tailor the security system to meet the needs of your organization. You may, for example, want some of your employees to be able to read, edit, and enter information in the accounts of a particular customer or of a particular department. This is done by applying security filters that limit the access your users have to the records stored in specific tables in the database.

Security filters can only be applied to tables and the records that they contain. In the following demonstration, security filters are applied that limit the access a user has to the entries in the database. The filters applied are based on Department (Global Dimension 1). After the filters have been applied, the user can only see the accounts and entries that have to do with the Sales department.

Scenario: The existing G/L-ACCOUNT role in the CRONUS company must be extended to include security filters.

Steps: Apply the Security Filter to the G/L-ACCOUNT Role

Follow these steps to apply the security filter:

1. On the Tools menu, point to Security and then click Roles.
2. Select the G/L-ACCOUNT role, click Role, and then select Permissions.
3. Select the G/L Account table.
4. In the Security Filter field, click the Edit button to open the Table Filter window.
5. In the Field field, click the look-up arrow and select Global Dimension 1 Filter in the list that appears.
6. In the Filter field, enter Sales.
7. Click OK to apply the filter.
8. Close the Permissions window.
You have now applied the security filter to the G/L-ACCOUNT role.

When a user who has the G/L-ACCOUNT role opens the Chart of Accounts window, there is less information displayed in the Net Change and Balance fields.

**Steps: Apply the Security Filter to the G/L Entry Table**

The G/L entries are stored in a separate table. Therefore, you must remember to apply the same filter to the G/L Entry table. You must apply the filter to both tables to ensure that the user does not gain access to entries that are not specified in the filter applied to the G/L Account table. This ensures that the user can only see the accounts and the entries that comply with the security filter. Security permissions and filters are table specific.

When applying the security filter to the G/L Entry table, you must select Department Code in the Field field.

To apply the same filter to the G/L Entry table:

1. With the G/L-ACCOUNT role selected, click Role, and then click Permissions; the Permissions window for that role appears.
2. Select the G/L Entry table.
3. In the Security Filter field, click the Edit button to open the Table Filter window.
4. In the Field field, click the look-up arrow and select Global Dimension 1 Code.
5. In the Filter field, enter Sales.
6. Click OK to apply the filter.

![G/L Account Read G/L accounts and entries - Permissions](image)

**FIGURE 6.8 SECURITY ALSO APPLIED TO G/L ENTRY TABLE**

7. Close the open windows.
Review the Result in the General Ledger Entries Window

You have now applied a security filter to the G/L-ACCOUNT role. After you have applied this security filter, the users who have this role can only see the G/L accounts and ledger entries that relate to the Sales department (Global Dimension 1). G/L Account 8530 contains ledger entries that relate to all the departments. After you have applied the security filter, the users who have the G/L-ACCOUNT role can only see 14 of these entries, namely those relating to the SALES dimension.

These changes only take affect the next time the users who have been assigned this role in the database log on. If any are currently logged on, their permissions are not affected by this security filter.

IMPORTANT: When you apply a security filter to a role, you modify that role. This means that all the other users who have been assigned that role will have their permissions changed as well.

If you do not want these modified permissions to apply to all the other users who have been assigned this role, consider creating new security roles before changing any of the standard security roles. You might also want to create new roles that contain security filters, which reflect the security needs of your company. Each department may need its own set of security roles each with their own individual security filters.
Merge Security Filters

Setting up one security filter does not ensure that the user can only see those records specified in the filter. Each user generally has more than one role in the current database and receives permissions from each of these roles. The permissions that the user possesses are the sum of all the permissions specified for all the roles the user has been assigned.

If more than one role gives the user permissions to access data from the same table, the security filter specified for this table in one role will have no effect if another role gives the user permissions to perform the same operations on the same table but without any security filter. Not applying a security filter means that the user can, for example, read all the entries in that table.

In the same way, if the user has two roles that give permission to the same table and both roles have security filters applied to them, it is the sum of these filters that is applied. This means that if one filter specifies that the user must only be able to read entries 1 to 10, and the other filter specifies entries 5 to 20, the user will be able to read entries 1 to 20.

Security Setup for Classic Client

Security set up in the Classic client is different than the set up in the RoleTailored client as follows:

- Database Logins can be used
- ALL role is used rather than the BASIC role
- Standard security roles are used; not the imported roles
- Profiles are not assigned to users

Windows logins can be used in the Classic client and are assigned roles the same as demonstrated for the RoleTailored client. In addition, SQL Security filters can be set in the Microsoft Dynamics NAV 2009 Classic with Microsoft SQL Server client. The biggest difference in set up is the use of Database Logins.

Creating a database login involves giving the user a User ID and one or more roles that contain the permissions appropriate to their position within your organization.

Both the Database Logins window and the process of creating a database login will be different depending on the Classic client version of Microsoft Dynamics NAV that you are using:

- Database Server
- Microsoft SQL Server

In this lesson, only the Database Login set up is described for the Microsoft Dynamics NAV Classic with Microsoft SQL Server client. For more information about setting up security in the Database Server, refer to the F1 help.
Procedure: Create Database Logins on SQL Server

Before you can give a user a database login, an administrator must give the user a login (using SQL Server authentication) on the SQL Server that they will be using.

Follow these steps to create database logins for users on the SQL Server version:

1. Set up the user on the SQL Server using SQL Server authentication and assign a complex password.
2. Open the Microsoft Dynamics NAV 2009 Classic with Microsoft SQL Server client.
3. On the Tools menu, point to Security and then click Database Logins.

4. In the User ID field, enter the same Login name used in the SQL Server.
5. In the Name field, enter the name of the user to whom this ID belongs.
6. In the Expiration Date field, enter a final date on which the user will be able to log on to Microsoft Dynamics NAV. This is optional.

It is unnecessary to enter a password here because that has already been done on the SQL Server. When the user wishes to access a Microsoft Dynamics NAV database, they will have to enter both their user ID and the password that the administrator entered on the SQL Server.
Chapter 6: Manage User Rights and Profiles

Procedure: Assign Roles to Database Logins

Follow these steps to assign a role to a database login:

1. On the Tools menu, point to Security and then click Database Logins.
2. Select the database login for which to assign Roles.
3. Click Roles; the Roles window opens.
4. In the Role ID field, click the look-up arrow.
5. Select the role and then click OK.
6. Repeat steps 3-5 to add more roles.

Procedure: Assign Database Logins to a Role

Sometimes database logins are set up first and then assigned roles at a later time. You can assign roles to existing users directly from the Roles window.

Follow these steps to assign a database login to a role:

1. On the Tools menu, point to Security and then click Roles; the Roles window appears.
2. Select the role for which to assign database logins.
3. Click Role and then select Database Logins; the Database Logins window appears listing the database logins that have been assigned this role in the database.
4. In the User ID field, click the look-up arrow.
5. Select the database login and then click OK.
6. Repeat steps 3-5 to add more database logins to this role.

User-Specific Setup

Microsoft Dynamics NAV allows you to put time limits on user IDs. If using Windows authentication, you can also put a time limit on passwords within the Windows domain. If you have the required permissions, you can always delete a user's login from the system or cancel all their permissions. Alternatively, you can specify a limited time period during which a particular user ID is allowed to post in the program.

After you have created a user ID, you can specify that the user with that ID can only post during certain time periods (for example, June 1 to June 15) and that the program must keep track of the amount of time the user has been working in each company.

This can be used, for example, for accountants who post entries for other users, to document the amount of time they spent working on the accounts of the various companies. The User Setup and User Time Register windows are used for this.
Procedure: Set Up Users

In the User Setup page, define when each user is allowed to post and whether the program records the amount of time that each user was logged on. You can also assign responsibility centers to the user.

To enter users, follow these steps:

1. Open the RoleTailored client.
2. In the navigation pane, click the Departments button.
3. Click Administration and then click Application Setup.
4. On the Application Setup page, click Users and then click User Setup.
5. Click New.
6. Fill in the fields according to the guidelines in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Enter the user ID for which you want to set up conditions. The user must have been set up already. If you cannot remember the user ID, look up in the User ID field to see a list of the user IDs that have been set up in the current database.</td>
</tr>
<tr>
<td>Allow Posting From</td>
<td>Enter the date on which the user will be allowed to start posting.</td>
</tr>
<tr>
<td>Allow Posting To</td>
<td>Enter the last date on which the user will be allowed to post.</td>
</tr>
<tr>
<td>Register Time</td>
<td>If you want to register the amount of time a user works on the company, enter a check mark by clicking the field or pressing the spacebar.</td>
</tr>
<tr>
<td>Sales Resp. Ctr. Filter</td>
<td>Enter the code for the responsibility center to which you want to assign the user. Look up in the field to see the responsibility centers that have been created. This responsibility center will be the default responsibility center when the user creates new sales documents. The user only sees sales orders created from his or her responsibility center. If you leave this field blank, the default responsibility center in Customer or Company Information (in order of priority) will be used.</td>
</tr>
<tr>
<td>Purchase Resp. Ctr. Filter</td>
<td>Enter the code for the responsibility center to which you want to assign the user. Look up in the field to see the responsibility centers that have been created. This responsibility center will be the default responsibility center when the user creates new purchase documents. The user only sees purchase orders created from his or her responsibility center. If you leave this field blank, the default responsibility center in Customer or Company Information (in order of priority) will be used.</td>
</tr>
<tr>
<td>Service Resp. Ctr. Filter</td>
<td>Enter the code for the responsibility center to which you want to assign the user. Look up in the field to see the responsibility centers that have been created. This responsibility center will be the default responsibility center when the user creates new service documents. The user only sees service orders created from his or her responsibility center. If you leave this field blank, the default responsibility center in Customer or Company Information (in order of priority) will be used.</td>
</tr>
</tbody>
</table>

**NOTE:** Other fields for posting periods are found on the General Ledger Setup page. These periods refer to the entire company and thus apply to all users. Anything entered for a particular user in the User Setup page takes precedence over the general choices made in the General Ledger Setup page.
User Time Registers

If the **Register Time** field in the **User Setup** page contains a check mark, the **User Time Registers** page will contain information about when and how long individual users have been logged on to the company.

To open the **User Time Registers** page, on the **Application Setup** page, click **Users**, and then click **Time Registers**.

![User Time Registers](image)

**FIGURE 6.12 USER TIME REGISTER USED TO RECORD THE AMOUNT OF TIME USERS SPEND LOGGED ON TO THE DATABASE**

This page displays the time use registers for users. The lines are generated automatically, but you can also enter information in them.

Time use is registered in whole minutes, rounded to the nearest minute. The program creates one line for each user, each day. If the same user uses the company more than once in a day, the line displays the total time used on that day.

If a user finishes using the company after midnight, the time use will be registered to the date when work began—not the date it was completed.
Active Directory Security

If your network and clients are using Active Directory or are Active Directory enabled, you have access to extra security features. You are able to give roles within Microsoft Dynamics NAV to Windows users and groups. You can also make Microsoft Dynamics NAV roles members of Windows security groups. However, the individual permissions granted to the roles can only be administered from within Microsoft Dynamics NAV.

The Active Directory service gives Microsoft Dynamics NAV several new security features. These include allowing administrators to:

- Grant or deny users access to Microsoft Dynamics NAV by simply adding them to or deleting them from a Windows security group.
- Grant other people in the organization the power to create and administer users and groups (for example heads of departments).

Active Directory security also supports Windows authentication.

Active Directory and Microsoft Dynamics NAV

To take full advantage of the features provided by the Active Directory security system, the Microsoft Dynamics NAV client computers and the domain controller must all either be running on Microsoft Windows Server 2003, Microsoft Windows Vista, Microsoft Windows XP, or otherwise have access to Active Directory.

If your Microsoft Dynamics NAV client computers do not have access to Active Directory, they will not be able to see the Windows Users & Groups window.

Active Directory allows the administrator to give administrative permissions to other users, thereby delegating large areas of responsibility to other members of the organization. This feature makes administering Microsoft Dynamics NAV more flexible. Other users, such as department managers, can administer all the groups that they need within their department from the Microsoft Management Console.

With Active Directory, you can make Windows user members of specific security groups that have already been given roles within Microsoft Dynamics NAV. You can control access to and permissions within Microsoft Dynamics NAV, without having to open the program, provided that the Windows security groups have been given the appropriate roles within Microsoft Dynamics NAV.

In an Active Directory environment, Microsoft Dynamics NAV allows you to create users and roles from Windows accounts and modify the rights of these users and roles. All Active Directory security groups are visible within Microsoft Dynamics NAV and can be given roles within Microsoft Dynamics NAV.
Procedure: Add Windows Users or Groups to a Microsoft Dynamics NAV Role

Active Directory allows you to give Windows users and groups a Microsoft Dynamics NAV role. Follow these steps:

1. On the Tools menu, point to Security and then click Roles.
2. Select the Microsoft Dynamics NAV role to assign, click Role, and then Windows Logins.
3. To add a Windows user or group to the list, select an empty row or create a row by clicking the New icon on the toolbar.
4. In the Login ID field, click the look-up arrow to open the Windows Logins window. This window contains a list of all the Windows users and groups that can log on to Microsoft Dynamics NAV.
5. Select the user or group to whom you want to give this Microsoft Dynamics NAV role and click OK.

This user or group will now be added to the list shown in the Windows Logins window for this role.

Procedure: Add Microsoft Dynamics NAV Roles to a Windows Security Group

Active Directory also allows you to make Microsoft Dynamics NAV logins and roles members of Windows security groups. Follow these steps:

1. On the Tools menu, point to Security and then click Windows Logins.
2. Select the Windows login to which you want to add a Microsoft Dynamics NAV role.
3. Click Roles.
4. Select an empty row, or create a row by clicking the New icon on the toolbar.
5. In the Role ID field, click the look-up arrow, select the relevant role from the Roles window, and then click OK.

This role and all the individual users that have been given this role will now be added to the selected Windows login.
Summary

Microsoft Dynamics NAV provides the tools for a company to effectively secure data in the system through the use of logins, roles, permissions, and SQL Server security filters. A secure environment is also managed through the use of data posting restrictions and time registries. In addition, the integration of the Microsoft Dynamics NAV security system with the Active Directory security system provides companies with an extra layer of security.

Application administrators will benefit from the concepts and demonstrations provided in this course before taking on the responsibility of setting up and managing the company's security system.
Test Your Knowledge

Test your knowledge with the following questions.

1. Which user must be created before all others in Microsoft Dynamics NAV?
   ( ) A Superuser
   ( ) A Database Administrator
   ( ) A Windows Domain Administrator
   ( ) A Windows Server 2003 Local Administrator

2. What are the benefits of giving a user single sign-on ability to log on to Microsoft Dynamics NAV? (Select all that apply)
   ( ) No need to supply a User ID and password when opening a database on another server
   ( ) When the user accesses Microsoft Dynamics NAV, the application checks to see if the user has a Windows login within the application
   ( ) The user will never need to enter a Windows or Microsoft Dynamics NAV credential to access ERP information
   ( ) If the user does not have a valid Windows account or if their account does not include permission to log on to the database, authentication fails

3. What happens when you apply a Security Filter to a role? (Select all that apply)
   ( ) It changes the role
   ( ) It does not change the permissions that other users with the same role have
   ( ) It changes the permissions for all users with the role
   ( ) It only changes the permissions for the users who subsequently get the role

4. Where can set up be performed to prevent a specific user's posting timeframe capabilities?
   ( ) General Ledger Setup page
   ( ) Users page
   ( ) User Setup page
   ( ) Database/Windows Logins window(s)
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: Introduction and Authentication

Fill in the blanks to test your knowledge of this section.

1. The minimum acceptable level of security is called database-level security.

2. Table-level security is a medium level of security that enables you to limit access to certain data.

3. A high level of security referred to as record-level security is available with the SQL Server.

4. Login refers to when a user identifies oneself, and is recognized by the system, thus allowing access.

5. Authentication is the process by which the system validates the user's identity.

Test Your Knowledge

1. Which user must be created before all others in Microsoft Dynamics NAV?
   - (●) A Superuser
   - ( ) A Database Administrator
   - ( ) A Windows Domain Administrator
   - ( ) A Windows Server 2003 Local Administrator

2. What are the benefits of giving a user single sign-on ability to log on to Microsoft Dynamics NAV? (Select all that apply)
   - (√) No need to supply a User ID and password when opening a database on another server
   - (√) When the user accesses Microsoft Dynamics NAV, the application checks to see if the user has a Windows login within the application
   - ( ) The user will never need to enter a Windows or Microsoft Dynamics NAV credential to access ERP information
   - (√) If the user does not have a valid Windows account or if their account does not include permission to log on to the database, authentication fails
3. What happens when you apply a Security Filter to a role? (Select all that apply)

   (√) It changes the role
   ( ) It does not change the permissions that other users with the same role have
   (√) It changes the permissions for all users with the role
   ( ) It only changes the permissions for the users who subsequently get the role

4. Where can setup be performed to prevent a specific user's posting timeframe capabilities?

   ( ) General Ledger Setup page
   ( ) Users page
   (●) User Setup page
   ( ) Database/Windows Logins window(s)