MODULE 2: MANAGE USER RIGHTS AND PROFILES

Module Overview

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 the following in the database:

- 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.

It is the responsibility of the application administrator to manage the security system. To control user access, the application consultant can use several tools provided by Microsoft Dynamics® NAV. Along with logons and SQL Server® security filters, companies can control user access to Microsoft Dynamics NAV data by means of permission sets and permissions. Additionally, administrators can set up and assign users to profiles for use in the Windows client.

Objectives

The objectives are:

- Explain how authentication works in Microsoft Dynamics NAV.
- Manage security for Windows client users.
- Set up a new user.
- Explain the concepts of permission sets and permissions.
- Create a new permission set, and assign permissions to it.
Application Setup in Microsoft Dynamics® NAV 2013

- Apply security filters in Microsoft Dynamics NAV.
- Perform user-specific setup.
- Create, assign, and work with user profiles.
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 three credential authorization mechanisms: Windows®, Username, and NavUserPassword authentication.
- Logon: 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.

**Note:** You specify which credential type is used for a particular Microsoft Dynamics NAV Server instance by modifying the relevant Windows client configuration file and Microsoft NAV Server instance configuration.

**Note:** All users of a given Microsoft Dynamics NAV Server instance must be using the same credential type.

Windows Authentication

With this credential type, users are authenticated using their Windows credentials (Active Directory®, the local workgroup, or just the local computer’s users and groups). Before you create a Windows user in the Windows client, there must already be a corresponding user or group in Windows.

Windows users, because they are authenticated through Windows, are not prompted for credentials when they start the Windows client.

Username Authentication

With this setting, the user is prompted for username/password credentials when starting the Windows client. These credentials are then validated against Windows authentication by Microsoft Dynamics NAV Server. Security certificates are required to protect the passing of credentials across a wide area network.

This setting should typically be used when the Microsoft Dynamics NAV Server computer is part of the authenticating Active Directory domain, but the computer where the Windows client is installed is not.
NavUserPassword Authentication

With this setting, authentication is managed by Microsoft Dynamics NAV Server but is not based on Windows users or Active Directory. The user is prompted for username/password credentials when starting the Windows client. The credentials are then validated by an external mechanism. Security certificates are required to protect the passing of credentials.

This mode is intended for hosted environments – for example, where Microsoft Dynamics NAV is implemented in SQL Azure™.

Note: How to configure the credential type is described in the Installation and Configuration in Microsoft Dynamics NAV 2013 course.

Set Up User Rights

Microsoft Dynamics NAV gives you complete control over the information that each user can access. You can create users and grant them the appropriate permission sets from within Microsoft Dynamics NAV.

Procedure: Set Up a New User Card

When you create users in Microsoft Dynamics NAV, they receive an identity within the database that allows them to log on to the system. Depending on the authentication mechanism, separate procedures are followed for creating users.

Note: You can create users with only one of the available credential types or with multiple credential types. For example, you could create a user who would automatically be logged on to the Windows client without having to present credentials when the credential type is Windows, but would be prompted for a username (the value of the User Name field) and a password when the credential type is Username.

When users log on to the database, they can perform tasks in accordance with the permissions that they have been allocated.

Follow these steps to open the Users page.

1. In the navigation pane, click Departments.
2. Click Administration, and then click IT Administration.
3. On the IT Administration page, click General, and then click Users.
4. Click New to open a new User Card page.
Module 2: Manage User Rights and Profiles

General FastTab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter a unique short name to identify the user.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Enter the user’s full name (first name, last name).</td>
</tr>
<tr>
<td>State</td>
<td>Specify whether the user should initially be Enabled or Disabled.</td>
</tr>
<tr>
<td></td>
<td>This field is used to create new users using Username and NavUserPassword authentication.</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>Click a date, if you want to set a time limit on the user’s access.</td>
</tr>
<tr>
<td></td>
<td>This field is used to create new users using Username and NavUserPassword authentication.</td>
</tr>
</tbody>
</table>

Windows Integrated Security FastTab

Do one of the following:

- Type the name of a valid Active Directory user in the Windows User Name field, using the format domain\username.
- Alternatively, view the options by clicking the Windows User Name field, then click Allow for the Session, and then use the Active Directory Select User or Group dialog box to identify a Windows user.

Set Password

To create new users using Username and NavUser Password authentication, a password will be set up.

On the Navigate tab, click Set Password and specify a password for the user. At the first log on, the user is prompted to change the password.

User Permission Sets FastTab

A permission set is a collection of permissions that will give a user access to certain domains within the Microsoft Dynamics NAV database. One or more permission sets can be given to one user.

From this place it is possible to review or change the permissions granted per permission set.

**Note:** When you change the permissions, you will change the permissions belonging to a permission set and thus change it for every user that has been granted this permission set.
Permission Sets

Follow these steps to review the permissions to the objects granted by a permission set.

1. In the navigation pane, click Departments.
2. Click Administration, and then click IT Administration.
3. On the IT Administration page, click General and then click Permission Sets.
4. On the Navigate tab of the Permission Sets page, click Permissions.

Object Types

Each permission set 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>Report</td>
<td>The reports used to present the 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. This is a legacy object from versions prior to Microsoft Dynamics NAV 2013.</td>
</tr>
<tr>
<td>Page</td>
<td>The pages used to view and enter data.</td>
</tr>
<tr>
<td>Query</td>
<td>The query used to retrieve data from multiple tables and combine in a single dataset.</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>

Permission Types

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>
</tbody>
</table>
Module 2: Manage User Rights and Profiles

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>

**Permission Options**

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>
| Indirect   | This permission is granted indirectly. An indirect permission allows you to, for example, read the object through another object that you have permission to use, such as a codeunit or a page.  
Example: You have permission to run Codeunit 80, Sales-Post. The Sales-Post codeunit performs many tasks. One of these is to modify Table 39, Purchase Line. When you run the Sales-Post codeunit, Microsoft Dynamics NAV checks whether you have permission to modify the Purchase Line table or not.  
• If you do not have permission to modify the Purchase Line table, the codeunit cannot complete its tasks and you receive an error message.  
• If you have permission to modify the Purchase Line table, the codeunit runs successfully. However, you do not need to have full access to the Purchase Line table to run the codeunit.  
• If you have indirect permission to modify the entries in the Purchase Line table, the Sales-Post codeunit runs successfully.  
When you have indirect permission, you can only modify the Purchase Line table when you run the Sales-Post codeunit or another object that has permission to modify the Purchase Line table. |

**Security Filters**

Microsoft Dynamics NAV 2013 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.

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

**Note:** When you apply a security filter to a permission set, you modify that permission set. This means that all the other users who have been assigned that permission set 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 permission set, consider creating new permission sets before changing any of the standard permission sets. You might also want to create new permission sets that contain security filters which reflect the security needs of your company. Each department may need its own permission set each with its own individual security filters.

**Merge Security Filters**

When you choose a process-driven security approach, 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 permission set in the current database and receives permissions from each of these permission sets. The permissions that the user possesses are the sum of all the permissions specified for all the permission sets the user has been assigned.

If more than one permission set gives the user permissions to access data from the same table, the security filter specified for this table in one permission set will have no effect if another permission set 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 permission sets that give permission to the same table and both permission sets 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.

With a role-driven security setup, objects only appear once in the permissions of a user, which means that merging security filters is not necessary.
Module 2: Manage User Rights and Profiles

**Special Permission Sets**

Permission sets can be either process-driven or role-driven. Process-driven permission sets, such as FA-FIXED ASSET, EDIT, which includes permissions to edit fixed assets, are used in conjunction with other permission sets to encompass all processes that a user needs to perform. Role-driven permission sets, such as Bookkeeper, include permissions necessary to work in the Bookkeeper profile. Additional permission sets can be added to the user for processes not covered in the Bookkeeper role.

A number of predefined permission sets are provided by default in the Windows client. Before assigning permission sets to users, review the predefined permission sets. You can use these permission sets as they are, modify them, or set up completely different ones.

---

**Note:** The provided default permission sets are all process driven. Role-driven permission sets must be created new by the Microsoft Dynamics NAV Partner.

**Note:** While users can modify the default provided permission sets, it is recommended to create new permission sets based on the defaults since upgrades and updates can overwrite user changes. This can be done by copying permissions from an existing Microsoft Dynamics NAV permission set, pasting those permissions into a new permission set, and then making modifications.

---

The following table describes the permissions of special predefined permission sets in Microsoft Dynamics NAV.

<table>
<thead>
<tr>
<th>Permission Set</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASIC</td>
<td>This permission set can use fundamental (but not high security) tables, system table, and functions. The permissions the user gains with this permission set can only be used in the tables that users normally have access to, such as the navigation pane menu.</td>
</tr>
<tr>
<td>SECURITY</td>
<td>This permission set has access to the tables and functions related to security information (users, permissions). Users within this permission set can grant permissions to others, but only those permissions they themselves have. Therefore, if you want to create an “area superuser,” 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>
</tbody>
</table>
**Application Setup in Microsoft Dynamics® NAV 2013**

<table>
<thead>
<tr>
<th>Permission Set</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUPER</td>
<td>This permission set 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. This user is then responsible for creating additional users and for assigning appropriate permission sets to those users. You cannot alter the permissions that have been granted to this role.</td>
</tr>
</tbody>
</table>

**Note:** When a user creates a Microsoft Dynamics NAV database, that user is automatically assigned the SUPER permission set in the Microsoft Dynamics NAV security system.

**Note:** Before starting to set security filters and/or permission sets, always make sure that one user authentication remains as “SUPER” to prevent locking access to parts of the database, which can only be enabled by the ‘SUPER Access Permission Set’.

| SUPER (DATA)         | This permission set can read, use, change, and delete all data. This is a permission set 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. |

**System Access Permission Set**

Any user who is not a superuser must be assigned the BASIC permission set in addition to permission sets and permissions that give access to the required areas of the program. The BASIC permission set provides fundamental permissions to:

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

This permission set does 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 administrate security for their own departments) must be assigned at least three roles: BASIC, SECURITY, and the role that provides access to the relevant areas of the database (such as Sales & Receivables).
Module 2: Manage User Rights and Profiles

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.

Create a New Permission Set

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

Demonstration: Create the New Permission Set and Grant Permissions

Scenario: CRONUS International, Ltd. needs a new permission set called G/L Accounts Only.

Demonstration Steps

1. Create the G/L Accounts Only permission set.
   a. In the navigation pane, click Departments.
   b. Click Administration, and then click IT Administration.
   c. On the IT Administration page, click General and then click Permission Sets.
   d. Click New on the Home tab to insert a new line.
   e. In the Permission Set field, type "G/L Accounts Only".
   f. In the Name field, type "Works in G/L accounts".
   g. Press ENTER or click the next line to accept the new permission set.
   h. Then click the new permission set again.
   i. On the Navigate tab of the Permission Sets page, click Permissions. The Permissions page for this new permission set appears. Because this is a new permission set, the window will be empty.
   j. In the Object Type field, ensure that Table Data is selected as the type of object for which you want to grant permission.
   k. In the Object ID field, enter 15, G/L Account as the specific instance of that object.
   l. Accept the default of Yes in all permissions.
Demonstration: Restrict the Permissions of the New Permission Set

Scenario: Later, the administrator must modify the permission set with a restriction to delete data in G/L Accounts.

Demonstration Steps

1. Restrict the deletion permissions of the G/L Accounts Only role.
   a. On the Permissions page for the G/L Accounts Only permission set, clear the Yes value in the Delete Permission field.
   b. Click the next line.
Demonstration: Extend the Permissions of the New Permission Set

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 permission set.

Demonstration Steps

1. Extend the permissions of the G/L Accounts Only permission set to also include read permissions in the Payment Terms and Finance Charge Terms tables.
   a. On the Permissions page for the G/L Accounts Only permission set, on the Actions tab, click All Permissions.
   b. In the Read Permission field for the Payment Terms table, enter Yes.
   c. In the Read Permission field for the Finance Charge Terms table, enter Yes.
   d. Click OK to save the selections.
   e. Close all open windows.

![FIGURE 2.3: READ PERMISSION ADDED FOR PAYMENT TERMS AND FINANCE CHARGE TERMS TABLE DATA]

Apply Security Filters

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 permission set in the CRONUS company must be extended to include security filters.

Demonstration: Apply the Security Filter to the G/L-ACCOUNT Permission Set

Demonstration Steps

1. Apply the security filter.
   a. In the navigation pane, click Departments.
   b. Click Administration, and then click IT Administration.
   c. On the IT Administration page, click General and then click Permission Sets.
   d. On the Permission Sets page, select the G/L-ACCOUNT permission set.
   e. On the Navigate tab, click Permissions.
   f. On the Permissions page, select the G/L Account table and then, on the Security Filter field, click AssistEdit.
   g. On the Table Filter page, click the Field Number field to view the options.
   h. On the Field Lookup page, select Global Dimension 1 Filter and click OK.
   i. On the Table Filter page, fill in SALES in the Field Filter field.
   j. Click OK to apply the filter.

FIGURE 2.4: SECURITY FILTER ADDED TO THE PERMISSION SET CONCERNING THE G/L ACCOUNT TABLE
You have now applied the security filter to the G/L-ACCOUNT permission set.

When a user who has the G/L-ACCOUNT permission set opens the Chart of Accounts window, less information appears in the Net Change and Balance fields.

**Demonstration: 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.

**Demonstration Steps**

1. Apply the security filter.
   a. In the navigation pane, click Departments.
   b. Click Administration, and then click IT Administration.
   c. On the IT Administration page, click General and then click Permission Sets.
   d. On the Permission Sets page, select the G/L-ACCOUNT permission set.
   e. On the Navigate tab, click Permissions.
   f. On the Permissions page, select the G/L Entry table and, on the Security Filter field, click AssistEdit.
   g. On the Table Filter page, click the Field Number field to view the options.
   h. On the Field Lookup page, select Global Dimension 1 Code and click OK.
   i. On the Table Filter page, in the Field Filter field, enter SALES.
   j. Click OK to apply the filter.
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.
User-Specific Setup

With Microsoft Dynamics NAV, you can put time limits on user IDs. Time limits can be set to either the user IDs in Microsoft Dynamics NAV or to the passwords within the Windows domain, when using Windows authentication. Alternatively, the User Setup page provides the possibility to restrict when a particular user is allowed to post to a particular company. In addition, the Time Registers page allows the program to register the amount of time that an individual user works in the 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.

User Setup Page

Follow these steps to open the User Setup page.

1. In the navigation pane, click Departments.
2. Click Administration, and then click Application Setup.
3. On the Application Setup page, click Users and then click User Setup.

![FIGURE 2.7: USER SETUP PAGE]

The fields shown in the following table are included in the User Setup page.

<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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Posting From and Allow Posting To</td>
<td>Enter the period (starting and ending date) in which the user will be allowed to post. <strong>Note:</strong> 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 choice made in the General Ledger Setup page.</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, Purchase Resp. Ctr. Filter and Service Resp. Ctr. Filter</td>
<td>Enter the code for the responsibility center to which you want to assign the user. Click the field to see the responsibility centers that have been created. This responsibility center will be the default responsibility center when the user respectively creates new sales, purchase, or service documents. The user only sees sales, purchase or 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>

You can also use the User Setup page to complete the setup on document approval and time sheet management. These fields will be discussed in detail in the appropriate courseware.

**User Time Registers**

If the Register Time field in the User Setup page contains a check mark, the 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.
Module 2: Manage User Rights and Profiles

This page displays the time use registers for users. Each time the user leaves the program, the lines are generated automatically, containing information about the user ID, date, and number of minutes worked.

However, lines can also be created manually.

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.

User Profile Setup

For the Windows client, Microsoft Dynamics NAV 2013 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.
Application Setup in Microsoft Dynamics® NAV 2013

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

**Note:** Before assigning profiles, set up the user with the proper security access to the corresponding Role Center page and to the objects (tasks, lists, reports, and documents) that can be found in the corresponding Home section on the navigation pane.

**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. In the navigation pane, click **Departments**.
2. Click **Administration**, and then click **Application Setup**.
3. On the **Application Setup** page, click **RoleTailored Client** and then click **Profiles**.
4. Click **New** to create a new **Profile Card**.

![FIGURE 2.9: NEW PROFILE CARD WINDOW](image)

The fields shown in the following table are included in the Profile Card page.
## Module 2: Manage User Rights and Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile ID</td>
<td>Type a short, appropriate name that describes the intended role of the user.</td>
</tr>
<tr>
<td>Owner ID</td>
<td>Click <strong>AssistEdit</strong> to view all available users. Select a user, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of the Profile ID, for example, &quot;Order Processor&quot;.</td>
</tr>
<tr>
<td>Role Center ID</td>
<td>Click the field to view all available Role Centers. Select the <strong>Role Center</strong>, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Default Role Center</td>
<td>Select the check box to make this the default Profile ID for all users. This is optional.</td>
</tr>
<tr>
<td>Use Record Notes and Use Page Notes</td>
<td>Select the check box if you want to activate the OneNote integration on a record and/or page level.</td>
</tr>
<tr>
<td>Record Notebook and Page Notebook</td>
<td>Indicate the location of the OneNote Notebook for a record and/or page.</td>
</tr>
</tbody>
</table>

**Note:** See online help for how to Set Up OneNote Integration for a Group of Users.

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

The User Personalization Card is used to assign newly configured profiles to end users. End users 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. In the **navigation** pane, click **Departments**.
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**.
The fields shown in the following table are included in the User Personalization page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Click AssistEdit, select the line for the relevant user, and then click OK.</td>
</tr>
<tr>
<td>Profile ID</td>
<td>Enter the relevant user, and then click OK.</td>
</tr>
<tr>
<td>Language ID</td>
<td>Enter an appropriate language ID or leave this field blank.</td>
</tr>
<tr>
<td>Company</td>
<td>Enter a company for which this user/profile combination is relevant.</td>
</tr>
</tbody>
</table>

**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. In the navigation pane, click Departments.
2. Click Administration, and then click Application Setup.
3. On the Application Setup page, click RoleTailored Client and then click Profiles.
4. Select the line of the profile to copy.
5. On the Actions tab, click Copy Profile.
6. In the New Profile ID field, type a short, descriptive name of the new profile.
7. Click OK to copy the profile and a new line is created.

The new profile with the same information as the copied profile is added to the Profiles page. Update the profile information as needed.
Best Practices

Superuser Responsibilities

The Microsoft Dynamics NAV security system is initiated when you create the first logon. The first logon 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.

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 permission sets 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.

Process-Driven vs. Role-Driven Setup

FIGURE 2.11: USER SETUP OVERVIEW

When new users need to be created and security needs to be set up for these users, the application administrator can use two different approaches in mapping out the user security requirements:
Application Setup in Microsoft Dynamics® NAV 2013

- Process-driven approach: The application administrator lists the different tasks a user needs to perform within the different Microsoft Dynamics NAV 2013 database. Typically, the administrator will use the default process-driven permission sets available in the system and the user will not be assigned a profile, thus he or she will be using the default Role Center.

- Role-driven approach: The application consultant looks at the job description, the role a user has been given within the company. Typically, the consultant will use the default role-driven permission sets, to be downloaded and imported within the Microsoft Dynamics NAV 2013 database. Also, the user will be assigned a profile that is aligned with his company role and the role-driven permission set.

Note: A user’s profile will determine the user’s Home menu (containing the Role Center page and other most used pages from job-related application areas), but it is the permission set that will determine whether a user can access these pages, data, and functions. It is up to the application administrator to make sure the profiles and permission sets are in perfect alignment.

When a user needs to have more access than given by a single default role-driven permission set, you can create new role-driven permission sets and profiles.

When a user has more than one role within the company or within different companies in the same database, you can create a new profile, design a new role center, and create a new aligned permission set.
Module 2: Manage User Rights and Profiles

Lab: Set Up New Users

Scenario

Simon, the System Implementer/Consultant at CRONUS, needs to set up users with access to both their relevant Role Centers and other application areas through Departments. All users will work in the English language. CRONUS uses Windows authentication as credential type. (Windows ID: CONTOSO\Name)

He sets up the following users:

1. A new employee, Susan Burk, has accepted the role of Sales Order Processor and is responsible for the maintenance of customer data at CRONUS International, Ltd.
2. Alicia, the purchasing agent, is responsible for the maintenance of vendor data.
3. Cassie, the bookkeeper at CRONUS, has been asked to manage some of the XBRL financial reporting. The BOOKKEEPER permission set and Role Center profile do not accommodate these tasks, thus Cassie will have to access the XBRL area from the Departments page.

Exercise 1: Susan

Task 1: Susan

High Level Steps

1. Create a user for Susan, using Windows authentication as specified in the scenario.
2. Assign the appropriate permission sets.
3. Assign the profile to Susan's user ID.

Detailed Steps

1. Create a user for Susan, using Windows authentication as specified in the scenario.
   a. In the navigation pane, click Departments.
   b. Click Administration and then click IT Administration.
   c. On the IT Administration page, click General and then click Users.
   d. Click New to open a new User Card.
   e. In the Windows User Name field, type “CONTOSO\Susan”.
2. Assign the appropriate permission sets.
   a. Go to the User Permission Sets FastTab.
   b. Add a new line and, in the Permission Set field, enter BASIC.
Application Setup in Microsoft Dynamics® NAV 2013

c. Add a new line and, in the Permission Set field, enter S&R-CUSTOMER, EDIT.
d. Click the next line.
e. Click OK to close the User Card.

3. Assign the profile to Susan’s user ID.
   a. In the navigation pane, click Departments.
   b. Click Administration, and then click Application Setup.
   c. On the Application Setup page, click RoleTailored Client, and then click User Personalization.
   d. Click New.
   e. In the User ID field, click the AssistEdit (...) button.
   f. Select the line for CONTOSO\Susan, and then click OK.
   g. In the Profile ID field, enter ORDER PROCESSOR.
   h. In the Language ID field, enter 1033.
   i. In the Company field, enter CRONUS International Ltd.
   j. Click OK to close the user personalization card.

Exercise 2: Alicia

Task 1: Alicia

High Level Steps

1. Create a user for Alicia, using Windows authentication as specified in the scenario.
2. Assign the appropriate permission sets.
3. Assign the profile to Alicia’s user ID.

Detailed Steps

1. Create a user for Alicia, using Windows authentication as specified in the scenario.
   a. In the navigation pane, click Departments.
   b. Click Administration, and then click IT Administration.
   c. On the IT Administration page, click General and then click Users.
   d. Click New to open a new User Card.
   e. In the Windows User Name field, type “CONTOSO\Alicia”.
2. Assign the appropriate permission sets.
   a. Go to the User Permission Sets FastTab.
   b. Add a new line and, in the Permission Set field, enter BASIC.
   c. Add a new line and, in the Permission Set field, enter P&P-VENDOR, EDIT.
Module 2: Manage User Rights and Profiles

d. Click the next line.
e. Click OK to close the User Card.

3. Assign the profile to Alicia's user ID.
a. In the navigation pane, click Departments.
b. Click Administration, and then click Application Setup.
c. On the Application Setup page, click RoleTailored Client, and then click User Personalization.
d. Click New.
e. In the User ID field, click the AssistEdit (…) button.
f. Select the line for CONTOSO\Alicia, and then click OK.
g. In the Profile ID field, enter PURCHASING AGENT.
h. In the Language ID field, enter 1033.
i. In the Company field, enter CRONUS International Ltd.
j. Click OK to close the user personalization card.

Exercise 3: Cassie

Task 1: Cassie

High Level Steps

1. Create a user for Cassie, using Windows authentication as specified in the scenario.
2. Assign the appropriate permission sets.
3. Assign the profile to Cassie's user ID as specified in the scenario.

Detailed Steps

1. Create a user for Cassie, using Windows authentication as specified in the scenario.
   a. In the navigation pane, click Departments.
   b. Click Administration, and then click IT Administration.
   c. On the IT Administration page, click General and then click Users.
   d. Click New to open a new User Card.
   e. In the Windows User Name field, type "CONTOSO\Cassie".
2. Assign the appropriate permission sets.
   a. Go to the User Permission Sets FastTab.
   b. Add a new line and, in the Permission Set field, enter BASIC.
   c. Add a new line, and enter G/L-XBRL, EDIT.
   d. Click the next line.
   e. Click OK to close the User Card.
3. Assign the profile to Cassie’s user ID as specified in the scenario.
   a. In the navigation pane, click Departments.
   b. Click Administration and then click Application Setup.
   c. On the Application Setup page, click RoleTailored Client, and then click User Personalization.
   d. Click New.
   e. In the User ID field, click the AssistEdit (...) button.
   f. Select the line for CONTOSO\Cassie, and then click OK.
   g. In the Profile ID field, enter BOOKKEEPER.
   h. In the Language ID field, enter 1033.
   i. In the Company field, enter CRONUS International Ltd.
   j. Click OK to close the user personalization card.
Module Review

Module Review and Takeaways

Microsoft Dynamics NAV provides the tools for a company to effectively secure data in the system through the use of logons, permission sets, permissions, and SQL Server security filters. A secure environment is also managed through the use of data posting restrictions and time registries.

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. What is the minimum acceptable level of security?
   - ( ) Table-level security
   - ( ) Database-level security
   - ( ) Record-level security
   - ( ) RIMDEX

2. Which security level limits access to certain data?
   - ( ) Table-level security
   - ( ) Database-level security
   - ( ) Record-level security
   - ( ) RIMDEX

3. Which of the following statements is incorrect?
   - ( ) Logon refers to when a user identifies oneself, and is recognized by the system, thus allowing access.
   - ( ) Authentication is the process by which the system validates the user’s identity.
   - ( ) The five database actions are referred to as RIMDEX in short.
Microsoft Dynamics NAV supports two credential authorization mechanisms: Windows authentication and NavUserPassword authentication.

4. 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

5. What happens when you apply a security filter to a permission?

   ( ) It changes the Role Center.
   ( ) It does not change the permissions that other users with the same role have.
   ( ) It changes the permissions for all users with the permission set.
   ( ) It only changes the permissions for the users who subsequently get the role.

6. 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)
Module 2: Manage User Rights and Profiles

Test Your Knowledge Solutions

Module Review and Takeaways

1. What is the minimum acceptable level of security?
   - ( ) Table-level security
   - (√) Database-level security
   - ( ) Record-level security
   - ( ) RIMDEX

2. Which security level limits access to certain data?
   - (√) Table-level security
   - ( ) Database-level security
   - ( ) Record-level security
   - ( ) RIMDEX

3. Which of the following statements is incorrect?
   - ( ) Logon refers to when a user identifies oneself, and is recognized by the system, thus allowing access.
   - ( ) Authentication is the process by which the system validates the user’s identity.
   - ( ) The five database actions are referred to as RIMDEX in short.
   - (√) Microsoft Dynamics NAV supports two credential authorization mechanisms: Windows authentication and NavUserPassword authentication.

4. 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
5. What happens when you apply a security filter to a permission?

( ) It changes the Role Center.

( ) It does not change the permissions that other users with the same role have.

(√) It changes the permissions for all users with the permission set.

( ) It only changes the permissions for the users who subsequently get the role.

6. 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)