

# Security

Microsoft Business Solutions-Navision:  
SQL Server Option

## Synchronizing Security in Navision 4.0 SP2

White Paper

2006

# Table of Contents

## **Security Synchronization in Microsoft Business Solutions-Navision**

<b>4.0 SP2 .....</b>	<b>3</b>
When to Synchronize the Security System.....	4
<b>Standard Security .....</b>	<b>5</b>
Synchronizing the Standard Security Model .....	6
<b>Enhanced Security .....</b>	<b>7</b>
Synchronizing the Enhanced Security Model .....	7
<b>Selecting the Security Model.....</b>	<b>9</b>
After Changing the Security Model.....	10
Converting the Database .....	10
<b>Attaching xp_ndo to SQL Server .....</b>	<b>12</b>

## *Security Synchronization in Microsoft Business Solutions-Navision 4.0 SP2*

Navision contains a comprehensive security system that enables you to manage the access that all of your users have to the objects and data in your Navision database. As this database is stored on SQL Server, the Navision security system and SQL Server's own security system must work in harmony to ensure that only authorized users can gain access to the database. The Navision security system therefore contains a synchronization mechanism that ensures that the information contained in the Navision security system corresponds with the information contained in the SQL Server security system.

Navision 4.0 SP2 allows you to specify the level of security that you want to implement in each database. You can choose between two different security models:

- **Standard Security**
- **Enhanced Security**

The main difference between these two security models is the way in which they synchronize the Navision security system with SQL Server and the way that they integrate the Navision security system with Windows authentication.

The security system is not synchronized automatically when you:

- **Change the security model.**
- **Restore a backup.**
- **Convert a database.**
- **Update the executable files.**
- **Update the application.**

To change the security model used in the database, you must be:

- **A member of the sysadmin server role on SQL Server or be a member of the db\_owner database role for the database in question.**
- **Assigned the SUPER role in Navision.**

Furthermore, if you want to change security models, you must ensure that both of the extended stored procedures that come with Navision have been added to the instance of SQL Server that you are using. These extended stored procedures are called:

- **xp\_ndo\_enumusergroups**
- **xp\_ndo\_enumusersids**

These extended stored procedures are part of the xp\_ndo.dll that comes on the Navision product CD. For more information about installing the extended stored procedures, see the section Attaching xp\_ndo to SQL Server or read the Readme.txt file that is stored with the dll on the product CD.

The main differences between the two security models are listed in the following table:

<b>Feature</b>	<b>Standard Security</b>	<b>Enhanced Security</b>
Synchronization Performance	Fast	Slower If you have several companies and many users in the same database, the synchronization process will be slower with Enhanced Security.
Windows groups displayed	Local domain + forest of domains	Local domain only
Logins required in Navision	Windows groups and individual Windows users	Windows Groups + the members of each group and individual Windows users
Granularity of Synchronization	Entire security system	Entire security system and individual logins.
Automatic synchronization when you insert, modify or delete a Windows login or a database login in Navision.	Yes	No
Required Extended Stored Procedure	xp_ndo_enumusersids	xp_ndo_enumusergroups

## When to Synchronize the Security System

The Navision security system must be synchronized with SQL Server every time you:

- **Change the security model.**
- **Change the users, permissions or roles that have been created in Navision.**
- **Restore a backup.**
- **Convert a database.**
- **Modify an object in the database**

Every time you modify an object in the database or modify the permissions that an object has to other database objects, you must correspondingly update all the roles and users who have permission to access this object and then you must synchronize these roles and users.

- **Update the executable files.**
- **Update the application.**

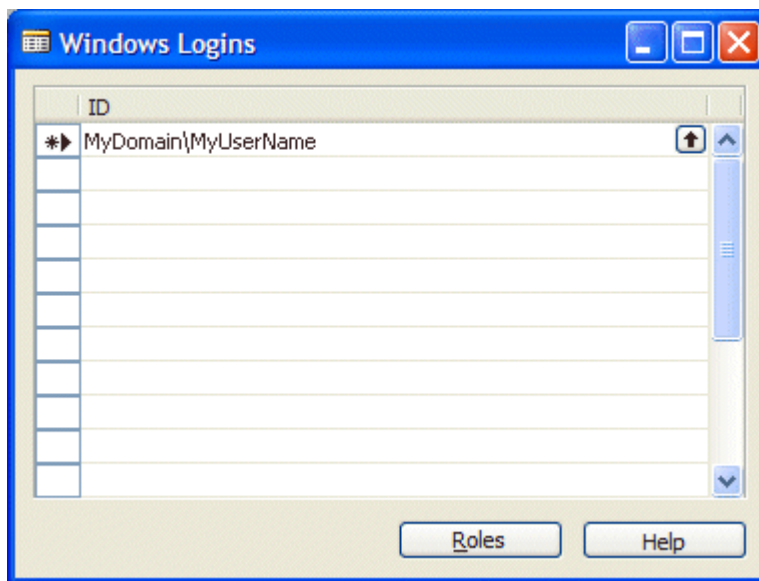
## Standard Security

The Standard Security model only allows you to synchronize the entire security system when you update the permissions system in Navision.

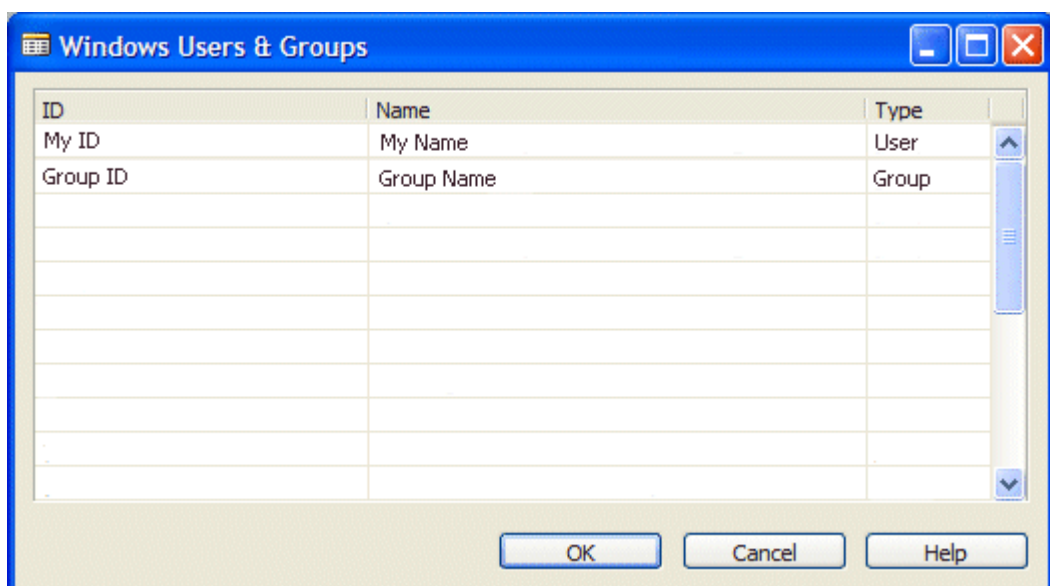
When you are using Standard Security, you can enter a Windows group in the **Windows Logins** window and assign it a role in Navision. All the users who are members of this windows group are then automatically assigned this role in Navision.

To create a Windows login:

1. Click Tools, Security, Windows Logins to open the **Windows Logins** window.



2. In the **ID** field, click the AssistButton to open the **Windows Users & Groups** window.



3. In the **Windows Users & Groups** window, select the user or group that you want to create a login for in Navision.  
Alternatively, you can just enter the Windows login of the user or group directly into the **Windows Logins** window if you know it.

With the Standard Security model, the **Windows Users & Groups** window lists all of the Windows groups and users that you can see in Active Directory as well as the local groups on your computer.

With the Standard Security model, every time you create, modify or delete a Windows login or a database login, the security system is automatically synchronized. However, if you add, alter or delete a role in the Navision security system, you must manually synchronize the security system.

The synchronization of the security system is performed faster with Standard Security than it is with Enhanced Security. Standard Security could be preferable if you have several companies in the same database and need to update the security system on a regular basis.

### **Synchronizing the Standard Security Model**

If you are using the Standard Security model, you can only synchronize the entire security system.

To synchronize the entire security system, click Tools, Security, Synchronize All and the entire security system is synchronized.

When you are using the Standard Security model, synchronizing the entire security system is not a very lengthy process.

## Enhanced Security

The Enhanced Security model has a more refined synchronization system.

Enhanced Security allows you to:

- **Synchronize individual users one at a time.**  
When you modify the permissions of a particular user, you can select that user and synchronize them.
- **Synchronize the entire security system at once.**

When you are using Enhanced Security, you can enter a Windows group in the **Windows Logins** window and assign it a role in Navision. However, you must also enter all of the individual users who are members of this Windows group in the **Windows Logins** window. You do not need to assign these individual logins any permissions in Navision as they receive their permissions by virtue of their membership of the Windows group that you added earlier. However, you can assign them any extra permissions that they might need in Navision.

When you are using Enhanced Security, the **Windows Users & Groups** window only lists all of the Windows groups and users that are visible to you in Active Directory. You cannot see any local groups on your computer.

### Important

All of the Navision users must therefore be members of the current domain.

With the Enhanced Security model, every time you create, modify or delete a Windows login or a database login, the security system is **not** automatically synchronized. You **must** remember to synchronize the security system yourself – no message is displayed!

Furthermore, if you have implemented Enhanced Security, synchronizing the entire security system can be a lengthy process and is considerably slower than Standard Security. We therefore recommend that no other users are logged on to the database when you synchronize the entire security system.

## Synchronizing the Enhanced Security Model

If you are using the Enhanced Security model, you can synchronize:

- **a single user**
- **all (the entire security system).**

To synchronize a user:

1. Click Tools, Security, Windows Logins to open the **Windows Logins** window.
2. Select the Windows login that you want to synchronize. You can only synchronize one login at a time.
3. Click Tools, Security, Synchronize Single Login to synchronize that login.  
You can also open the **Database Logins** window and synchronize the database logins one at a time.

To synchronize the entire security system:

1. Click Tools, Security, Synchronize All and the entire security system is synchronized.

### **Note**

Synchronizing the entire security system can take a considerable time.

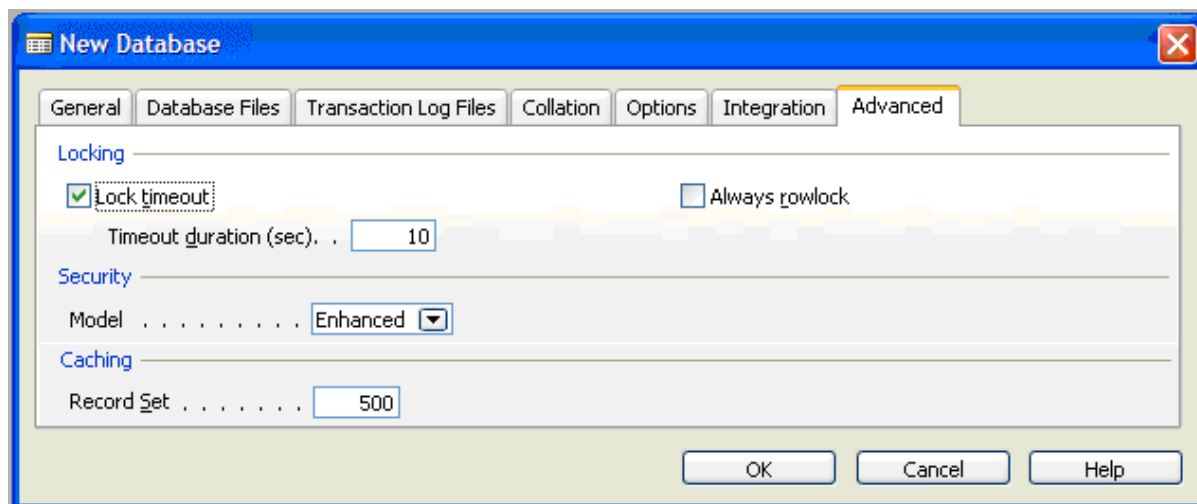
### **Important**

When you are altering the permissions of users or roles in Navision, make sure that none of the users whose permissions you are altering or who have been assigned the role you are altering are logged on to the database. When you are synchronizing the entire security system, make sure that you are the only user in the database.

## Selecting the Security Model

You can specify the security model that you want to use in a database when you create the database.

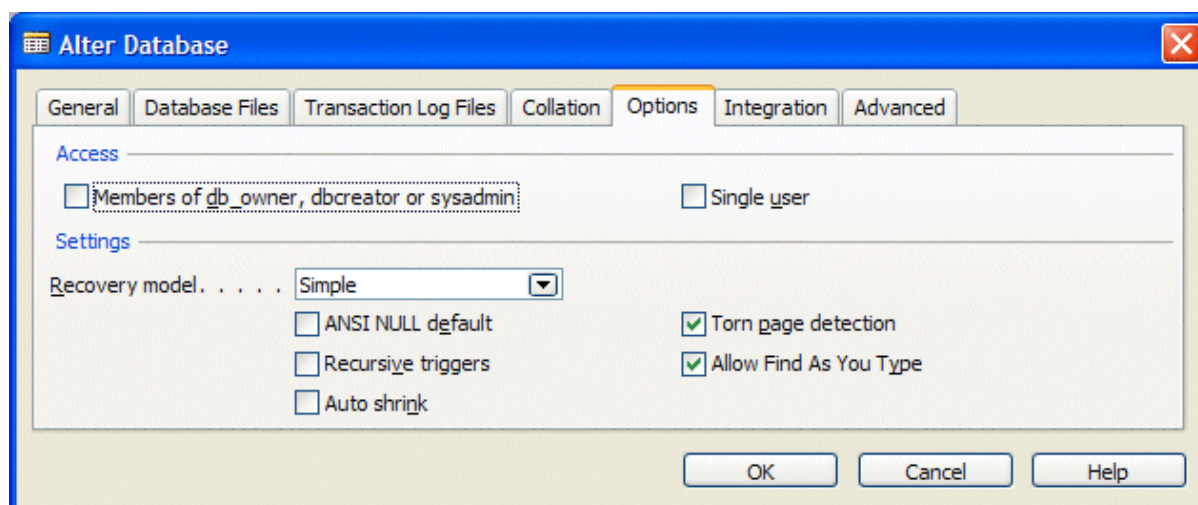
You specify the security model that you want to use in the advanced tab of the **New Database** window:



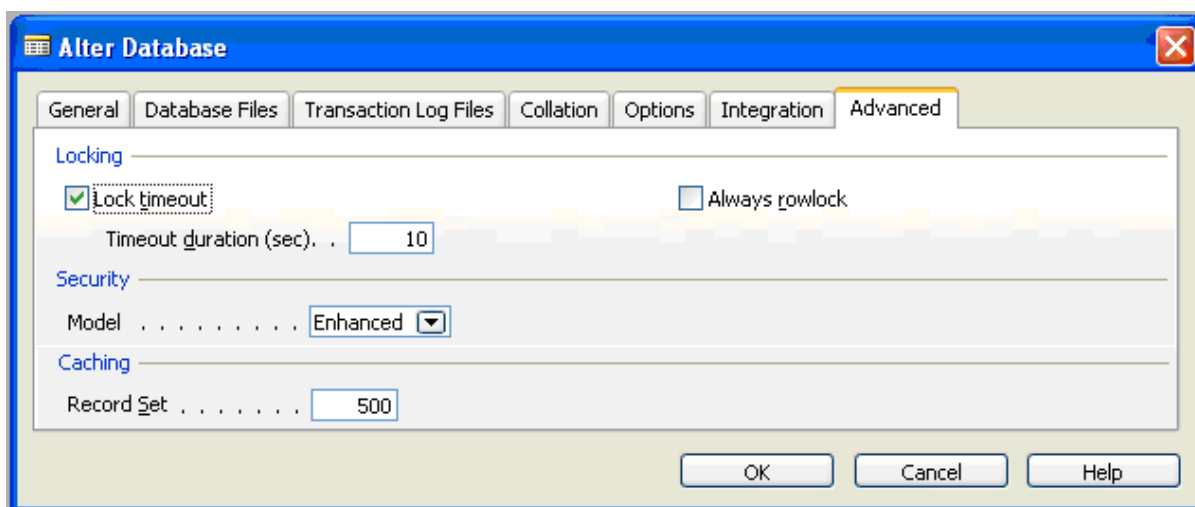
You can also change the security model that you want to use in the database in the **Alter Database** window.

To change the security model:

1. Ensure that no other users or tools, such as Microsoft SQL Server Management Studio, are using the database.
2. Close and reopen the database to ensure that you are the only user currently accessing the database.
3. Click File, Database, Alter to open the **Alter Database** window and click the **Options** tab:



4. Enter a check mark in the **Single user** field. This will prevent other users and tools from accessing the database.
5. Click the **Advanced** tab:



6. In the **Security Model** field, click the drop down list and select the security model that you want to implement in this database.
7. Click OK to alter the database and change the security model.

As mentioned earlier, you **must** synchronize the entire Navision security system with SQL Server after you change the security model.

#### Important

You **must** remove the check mark in the **Single user** field before you synchronize the entire Navision security system with SQL Server. If another user logs on to the database while you are synchronizing the security system, they will probably not have access to all the resources that they need.

### After Changing the Security Model

When you change from Enhanced Security to Standard Security, you can delete all the individual users who have been given a Windows Login in Navision as long as the Windows group(s) that they are a member of has the permissions they require. However, if any of the users have been assigned extra permissions you should not delete them from the **Windows Logins** window.

#### Important

When you change from Standard Security to Enhanced Security, you must give all the individual members of any Windows groups that have been entered in the **Windows Logins** window a Windows login of their own. You do not need to assign any permissions or roles to these logins in Navision. The Windows group that they belong to has already been assigned the permissions they need.

### Converting the Database

When you convert a database to Navision 4.0 SP2, it is automatically assigned a security model.

The following table lists the default values:

Conversion Path	Default Security Model
3.70 – 4.0 SP2	Standard Security
4.0 – 4.0 SP2	Enhanced Security

After you have converted the database, you can change the security model that the database uses.

When you restore a backup of a Navision 3.70 database into a Navision 4.0 database with enhanced security and when you convert a Navision 3.70 database to Navision 4.0 and select enhanced security, you must be aware of the following changes that were made to the Navision security system for Navision 4.0:

- **New objects have been added to the Permission table**

After you upgrade an old database to Navision 4.0, you must manually update the Permission table to include the new MenuSuite and XMLport objects.

To update the Permissions table:

1. Open the Object Designer, select table 2000000005, Permission and click Design.
  2. In the Table Designer window, select field number 3, Object Type and open the Properties window (Shift+F4).
  3. In the Properties window, ensure that XMLport and MenuSuite are added to the comma separated lists in the OptionString, OptionCaption and OptionCaptionML fields.
  4. Close, save and compile the table.
- **The implementation of permissions is more restrictive**  
In Navision 4.0, you must ensure that each user has explicit permission (either direct or indirect) to all the tables that they need to perform their tasks. This includes both system and application tables.

For example, in Navision a table can contain a flowfield that generates sums based on values that are stored in another table. In this case, the user must have permission to read both tables or they will not be allowed to read the first table.

This means that it might be necessary to change the permissions for some of the existing roles.

## Attaching xp\_ndo to SQL Server

As mentioned earlier, if you intend to switch between security models, you must install both of the extended stored procedures that come with Navision 4.0 SP2. One of the extended stored procedures is added automatically when you access SQL Server 2000 for the first time from a client that is also installed on the server computer. However, if you have previously accessed SQL Server with a Navision client the extended stored procedure is not added automatically.

If you are using SQL Server 2005, no extended stored procedure is added automatically and you must add them manually. The instructions for adding the extended stored procedures are contained in the `Readme.txt` file that comes with the extended stored procedures on the product CD.

To verify that the extended stored procedures have been added to an instance of SQL Server, check that the `xp_ndo.dll` file is stored in the following folders:

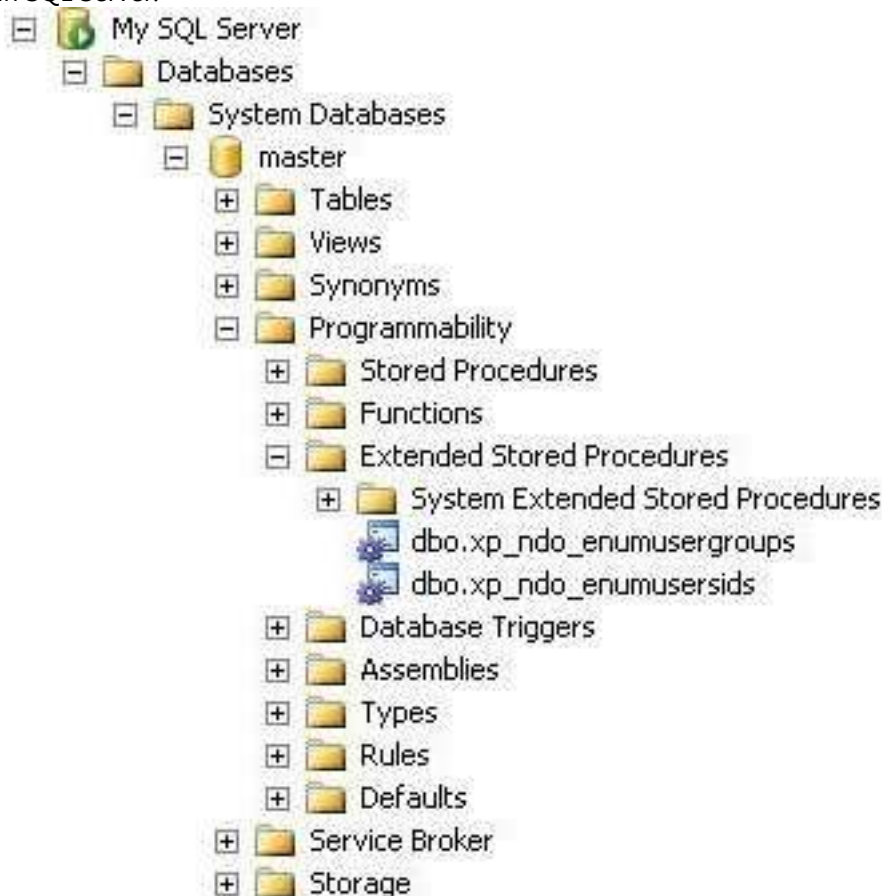
On SQL Server 2005 the default path is:

```
C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn.
```

On SQL Server 2000 the default path is:

```
C:\Program Files\Microsoft SQL Server\MSSQL\Binn.
```

You should also check that the extended stored procedures have been added to the master database in SQL Server:



The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, this document should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005 Microsoft Corporation. All rights reserved.

Microsoft, The Microsoft Dynamics Logo, [\[list all trademarked products\]](#), are either registered trademarks or trademarks of Microsoft Corporation or Microsoft Business Solutions ApS in the United States and/or other countries. Microsoft Business Solutions ApS is a subsidiary of Microsoft Corporation.

**Microsoft**