

Best Practices for NAV Easy Security setup

When doing setup of permissions in NAV is there many different ways to approach the task. This document will try to give some guidelines of the best way to maintain and create permissions.

When starting a new installation is the roles delivered from Microsoft a good base. Even when the roles are having errors and are missing your customizations and add-ons, the general concept is working. By using the Recorder is it easy to fix the problems in the base roles or build new when needed for special processes.

What Company to use for Easy Security data

Security is best maintained in a company that can be controlled with specific permissions, this mean a company that is not used for other purposes than security setup. This can allow a person in the IT department working on security to have full permissions in that company since no data is confidential.

The data in the company have to contain setup for add-ons and customization to use the recorder properly. The best way is typically to use a CRONUS demonstration company that has been renamed without CRONUS as the first part of the Company Name. With the data in the demo company is it often possible to record all scenarios without using actual data.

By using a company with only limited data, this company can also easily be moved between different databases. This makes it easy to backup and work on permissions in different databases (Live or Test) but still maintaining a good backup of the security setup.

Even Restore Points and Recordings can be exported and imported is a lot of other data being used when publishing permissions. Without maintaining all the data in the company will Object Level Security, Role Groups, Company Groups and features in the Role Builder not work the same way if reinstalled in a new company.

A CRONUS company should not be used for maintaining security. Based on the special permissions in a company starting with CRONUS will recordings not always be correct. The message from Easy Security will also warn the user about this when running processes in Easy Security.

Maintaining Logins

Logins is best maintained by using groups of roles. This makes it easy to get an overview of the high level permissions for a user. Instead of 50 individual roles is maybe only a few Role Groups needed. By making groups like "BASE", "SALES", "ACCOUNTING" and " WAREHOUSE" are the groups referring to functional areas. When later adding another customization or add-on requiring more roles for a user, it only would affect the Role Group and not each individual user. Certifying users with Sarbanes-Oxley is also easier when using the Role Groups, compared to many individual roles.

Role Groups can also be nested by Including Role Groups inside a Role Group. This can be used for build a setup with a user only having 1 Role Groups in each Company.

The “SUPER” or “SUPER (DATA)” should normally not be included in Role Groups since these are really important and needs to be visible directly under the Login.

A Role Group “BASE” is very useful to add permissions that all users need. The Role “ALL” and “BASIC” can be included in the Role Group. But also Roles required by add-ons to be added to every user can be added to the Role Group.

If many users work in a similar role in a company and need the same permissions the “Permissions as User ID” should be used. This allows for only maintaining one user and has all the other warehouse employees be similar for example.

Company Groups can save a lot of complexity by having multiple test companies in a single Company Group. New test companies are typically created on a regular basis and adding the permissions to users would only be adding the Company in the Company Group and then publish permissions.

Maintaining Roles

Roles should be maintained as small tasks to allow easily modifying and adding permissions when new customization or add-ons are added to the database. Using a recording for a change in process, a small Role can easily be updated.

The 0 permissions for objects should not be used in many different roles. This permission is so powerful that trying to control object level permissions when this is scatter in many different roles is very difficult.

If a role is a complete set of permissions a user needs for doing all the work in a day will several roles be created for each type of user in a company. This will turn into a nightmare for maintenance because of hundreds or even thousands of permissions are repeated again and again in each role. The Role Groups should be used instead to maintain this by building a Role Group with multiple smaller Roles.

If a new customization or add-on is added a small recording can be created with the changes. This recording can then be added to the Roles affected by the changes. In this way is it easy to track changes and even reverse permissions added if a mistake happens.

Security Filters

Using Security Filters with Easy Security is not different that using base NAV permissions. There are some limitations of the implementation in NAV. Permissions are always added, that will cause a Security Filter to be removed in permissions to the same table are given from another role. This makes it very hard to use for tables like G/L Entries or similar where permissions is given from many roles.

A Security Filter is normally also user specific but the setup within a Role is not making it available by user. This will cause a lot of very similar roles to be created based on different Security Filters needed.

A feature to support this in a much better way is considered for a future version of Easy Security.