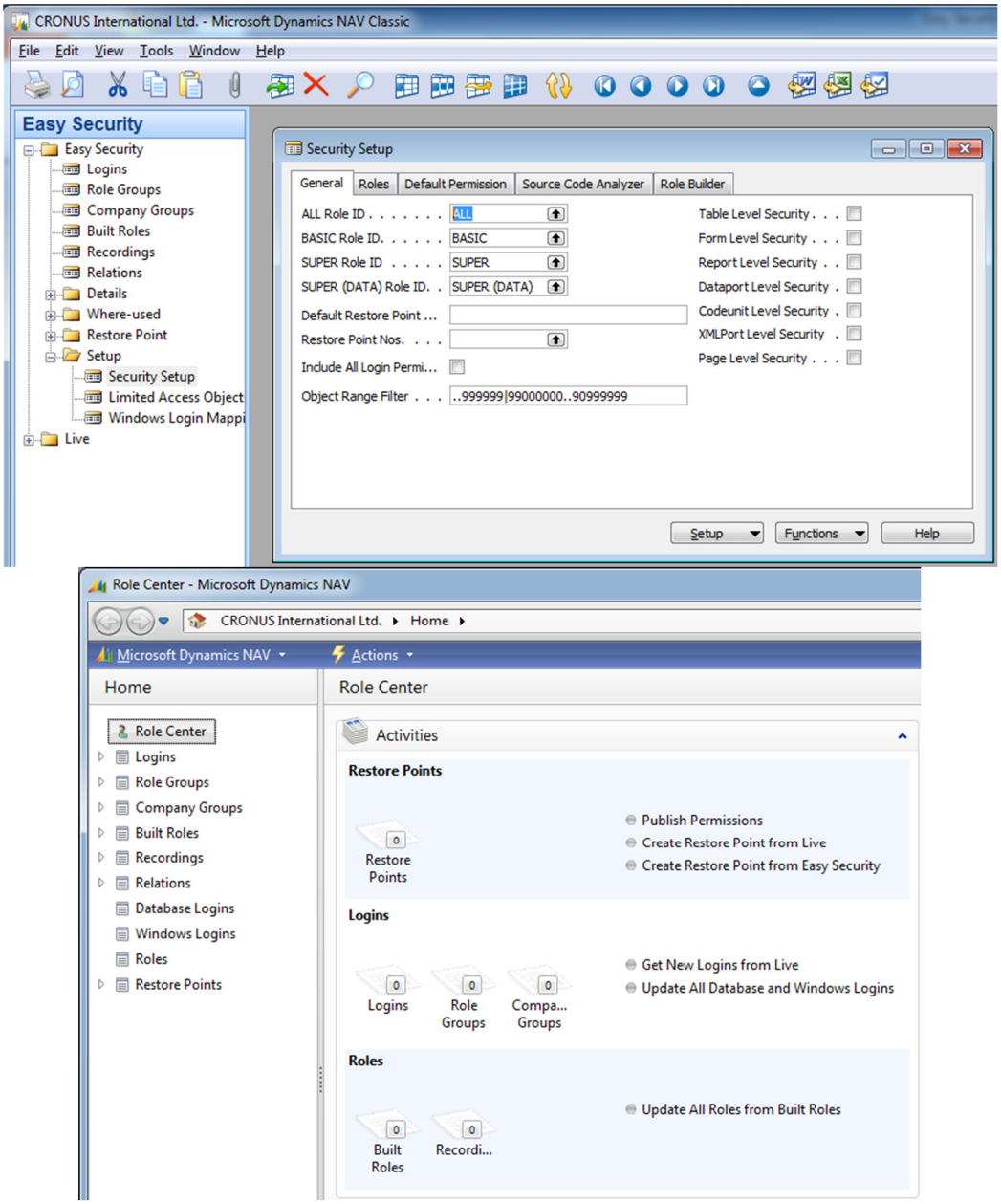
The technical side of NAV Easy Security

NAV Easy Security is a solution to maintain permissions for Microsoft Dynamics NAV. Permissions can be maintained from the RoleTailored Client or the Classic Client. Below is a screen shot of the menu and Security Setup from the Classic Client and the Role Center from the RoleTailored Client.



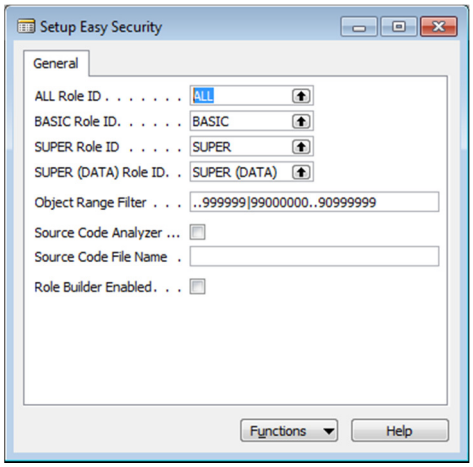
Maintaining permission from the RoleTailored Client is possible when using the “Standard” security model in the SQL database. Only setup of new users and synchronize after import of new objects requires using the Classic Client.

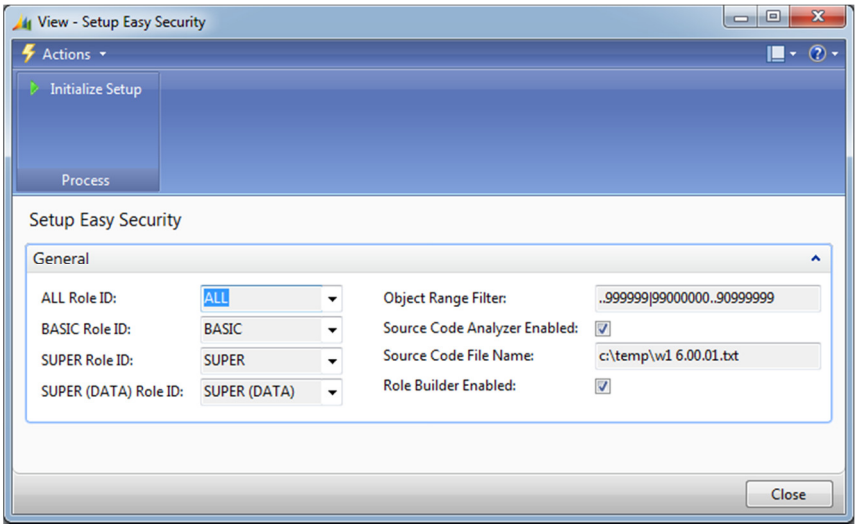
If the Enhanced security is used must all users must be synchronized from the Classic Client after permissions have being published. Also when adding or changing objects must a full synchronization of the users, be performed from the Classic Client.

Installation and Setup

The objects for NAV Easy Security are all new objects. This makes integration with the customer database very simple by importing the objects.

Set up of NAV Easy Security can be done from the RoleTailored or Classic Client. Open the Easy Security Setup and a wizard window opens. If using a different country version can it be necessary to lookup the different Role ID for ALL, BASIC, SUPER and SUPER (DATA). The Object Range Filter is used when searching for limited license permissions; because of the very large range (2,000,000,000 per object type) must a filter be applied. If an add-on is installed in the database using limited permissions, this range must be extended to include these objects.





If the Source Code Analyzer module has been purchased, the “Source Code Analyzer Enabled” must be checked and the path and filename entered for the current source code. The source code can be exported as a txt-file from the Object Designer in the Classic Client. This will normally require a Partner developer license. This can also be done later from within the application.

If the Role Builder module has been purchased, the “Role Builder Enabled” must be checked. This will create data in the Roles Details and related tables during the initialize process. This can also be done later from within the application.

Click on the “Initialize Setup” to finish the setup. This will run 3-10 minutes depending on the options selected. During the process multiple messages will appear to tell about the progress, just click ok on these messages. After this process is finished NAV Easy Security is ready to be used and the Setup Easy Security window can be closed.

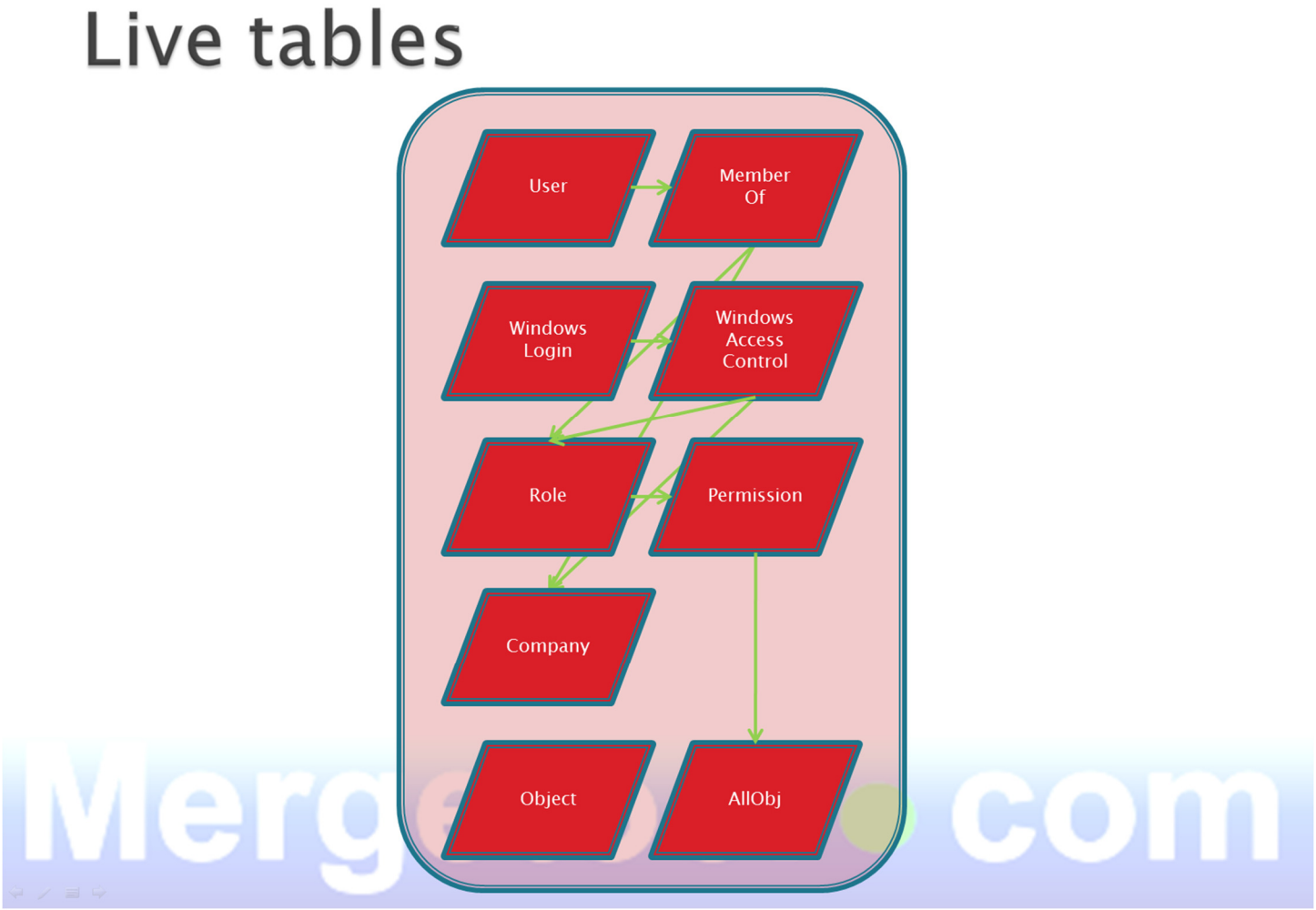
Table structure

NAV Easy Security is based on a process of working with permissions offline. To allow this is the tables in the live system (referred to as “Live” in the following) associated with permissions copied to a new set of tables (referred to as “Easy Security” in the following). This copy always happens through a Restore Point. A Restore Point (referred to as “Restore Point” in the following) can be created both from “Live” and “Easy Security” tables and a “Restore Point” can be written to “Easy Security” and partially to “Live”.

Below are 3 drawings of the different tables, each group of nine tables contains a similar field structure. Some of the tables in “Easy Security” and “Restore Point” have been renamed to make a more consistent naming.

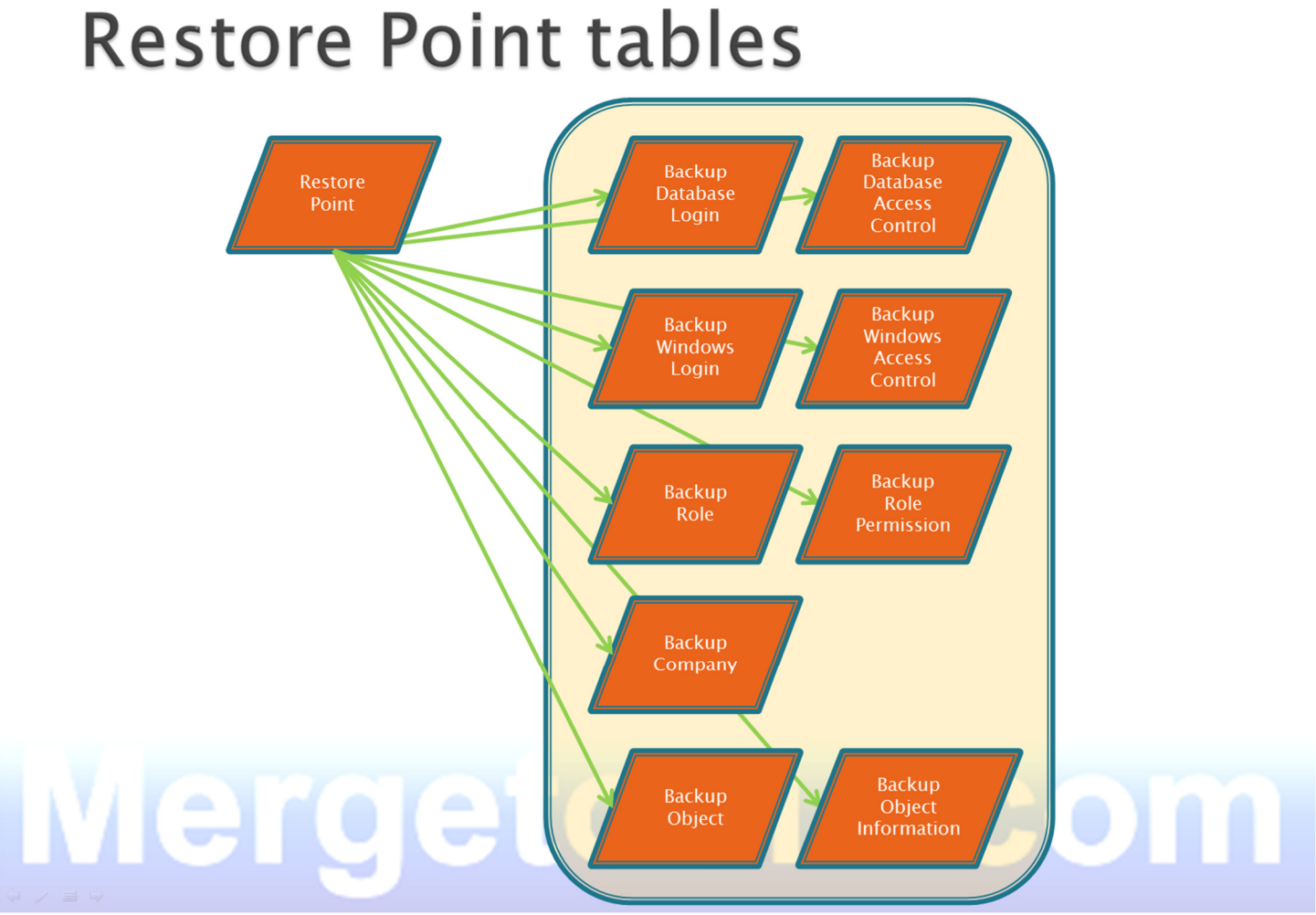
Live tables

The “Live” tables for permissions are all global to all companies. The information stored in these tables is available to be viewed in every company in the database. The “Easy Security” and “Restore Point” tables are not global to all companies, this allow for limiting access to the definitions of logins and roles.



Restore Point tables

The “Restore Point” is used to save complete permissions, both from “Live” and “Easy Security”. The tables have been renamed to use the consistent naming in NAV Easy Security, but are similar to the “Live” tables except a version field is part of the primary key.



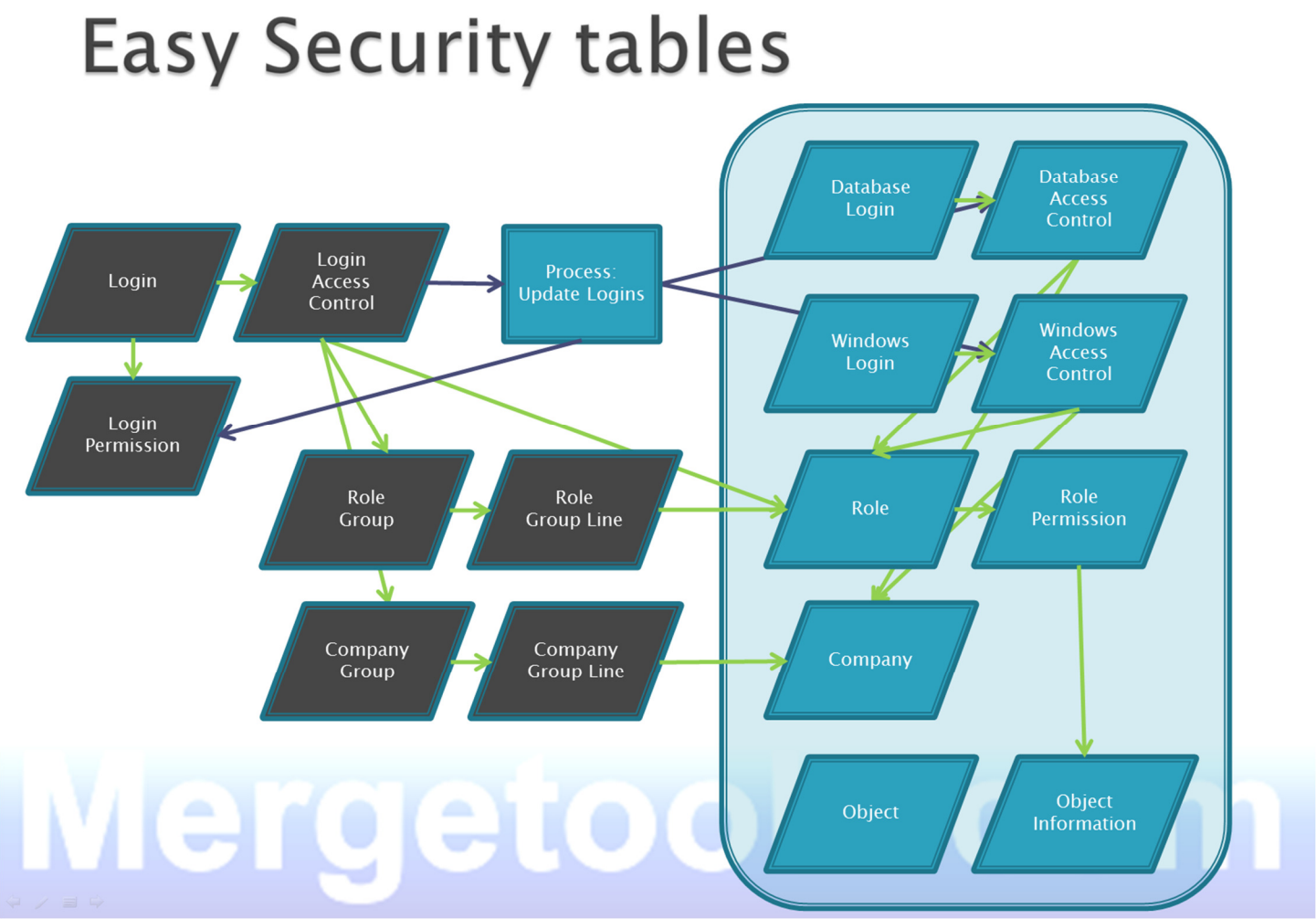
In the Windows Login table is a field User ID added. When moving a Restore Point from one domain to another is lookup of names not possible. This can be solved by adding the Windows Login SID to the Windows Login Mapping table with the appropriate information. After the information is added, logins will use the nicer names.

Easy Security tables

In “Easy Security” are several other tables than the standard nine tables available to maintain permissions in a more efficient interface. Database Logins and Windows Logins are maintained from a new table “Login” that allow assigning permissions as another user and many more features.

Roles can be grouped with a “Role Group” containing roles or other role groups. The same goes for companies that can be grouped with a “Company Group” containing multiple companies.

The Login Access Control allows adding both roles and group of roles to a login. Only company groups can be used in the access control. This is done to very easily handle renaming of a company or adding a second test company without changing all the access control for the logins. During the installation process is a group built for each company used in the existing permissions.



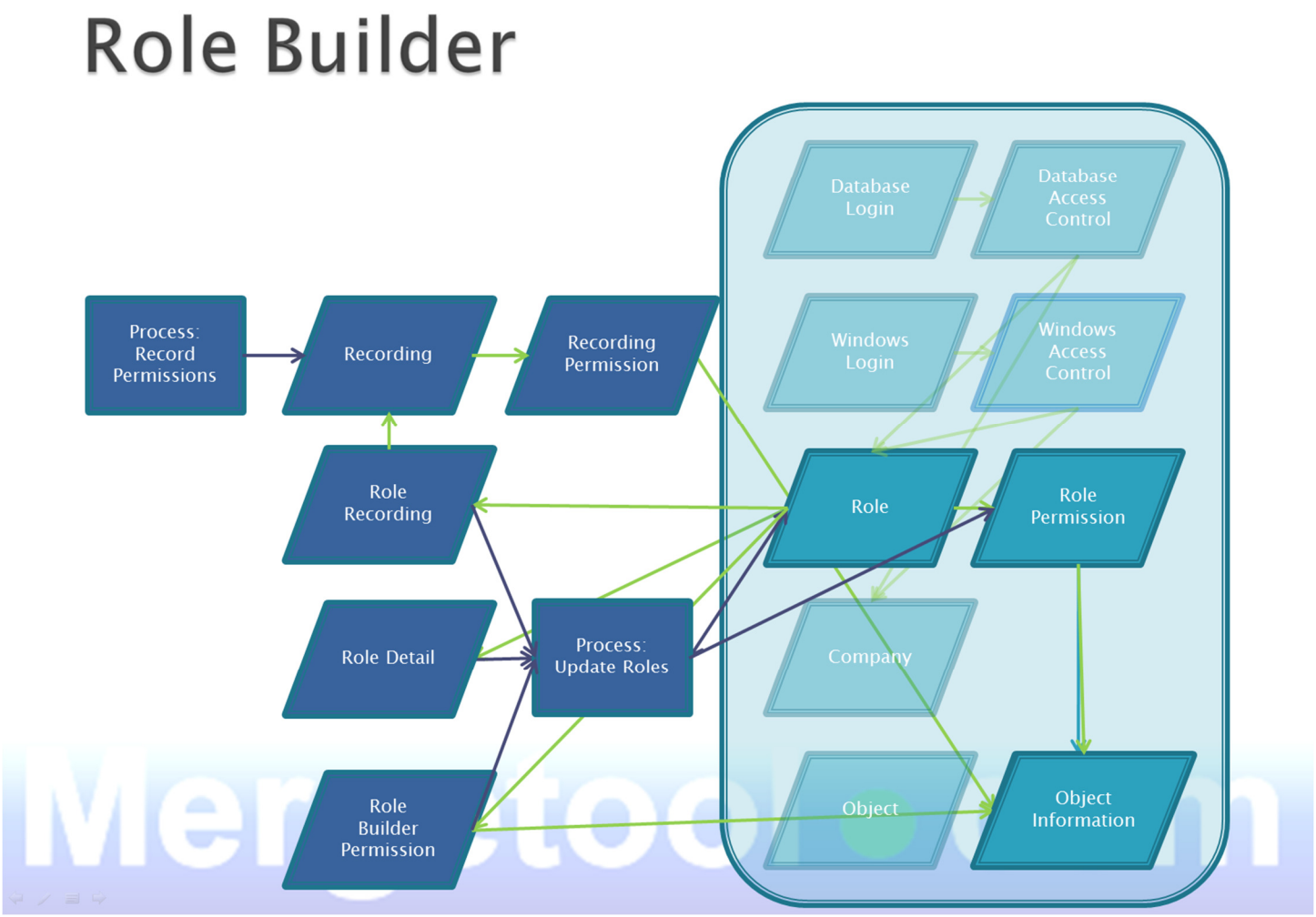
Login Permissions are created when updating the login in “Easy Security”. Only objects in the Limited Access Object table are by default included. This is done to limit the data created when updating logins, with a large installation with 200 users, 20 companies, using form, report and page level permissions could more than 20,000,000 records be deleted and created, potentially causing slow performance.

Role Builder

The Role Builder Module adds another way of maintaining and building roles. By using recordings and only adding a few permissions to either limit or add extra permissions. The Role Details is used to recreate Roles based on the Role Recordings and Role Builder Permissions. A few roles are special (like ALL and SUPER) and cannot be maintained in the Role Builder.

Recordings of permissions are done using the Client Monitor in the Classic Client. Before starting a recording should the database be closed and reopened to ensure the object cache is not loaded with objects. If this is not done the recorded permissions for objects can be missing.

Below is a diagram of the tables in Role Builder and the relations with the “Easy Security” tables.



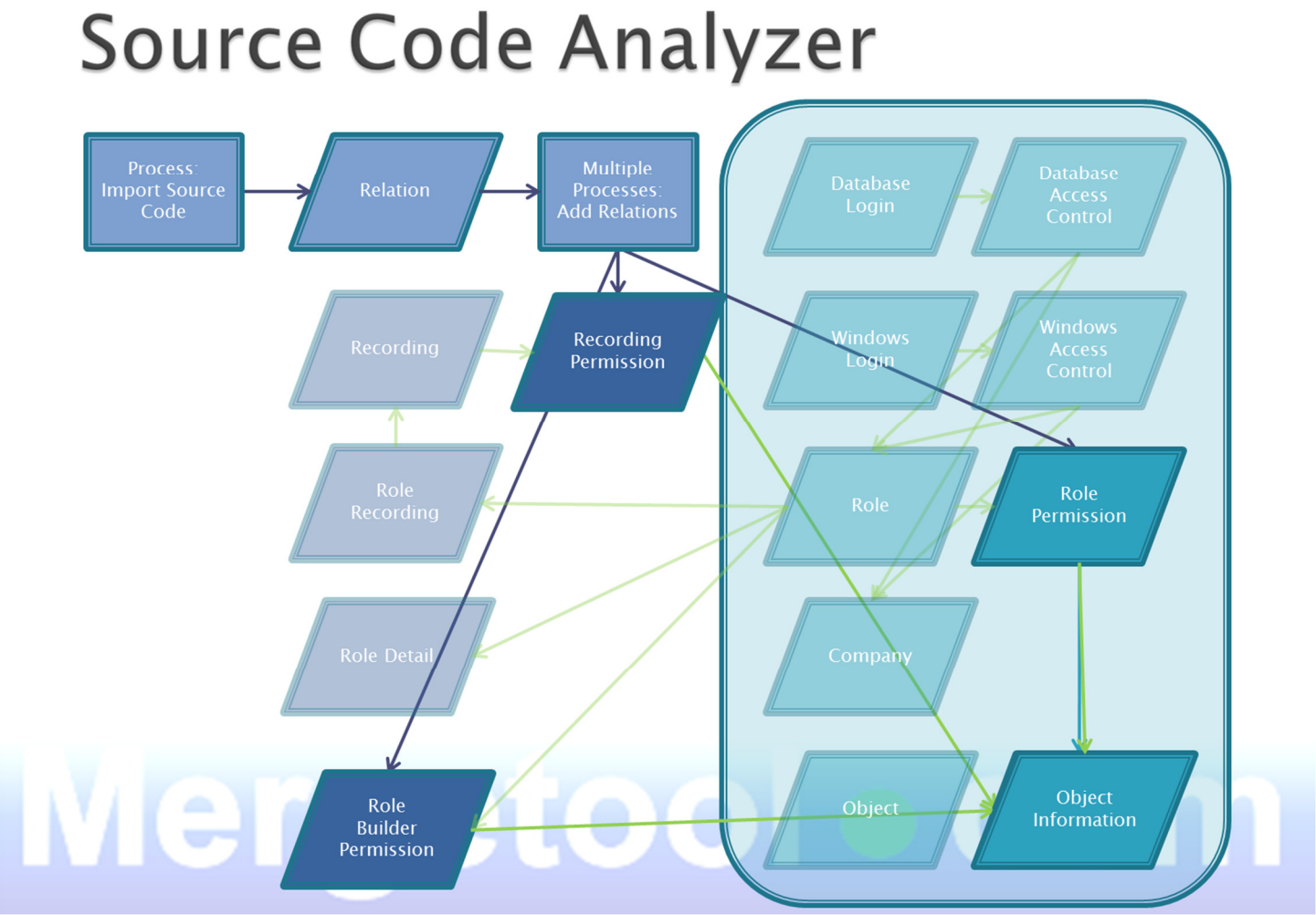
The Role can contain multiple Role Recordings and Role Builder Permissions. Recordings are added first to the Role Permissions and the Role Builder Permissions can be used to add or reduce the permissions in the role after the recordings are added. For example could this be used to remove access for the release codeunit (412) even if the recording included this.

Role Details and related tables and Recordings can be exported and imported easily moving data between a test and a live environment. A recording can be performed by a partner and imported at the customer site if the customer does not have purchased the license for the Client Monitor.

Source Code Analyzer

Updating permissions by adding table relations and flowfield definitions makes recordings and creating permissions in roles much easier. Only the primary tabledata permission needs to be added in the permissions and related tabledata permissions will be added from the source code. The process of scanning the source code is based on the actual code in the database. This ensures that customization and add-on also will be included. By using the Role Builder and Source Code Analyzer is it also possible to have a roles based on a recording that will be updated in the future if another add-on or customization is added.

Below is a diagram of the tables in Source Code Analyzer and the relations with the “Easy Security” and Role Builder tables.



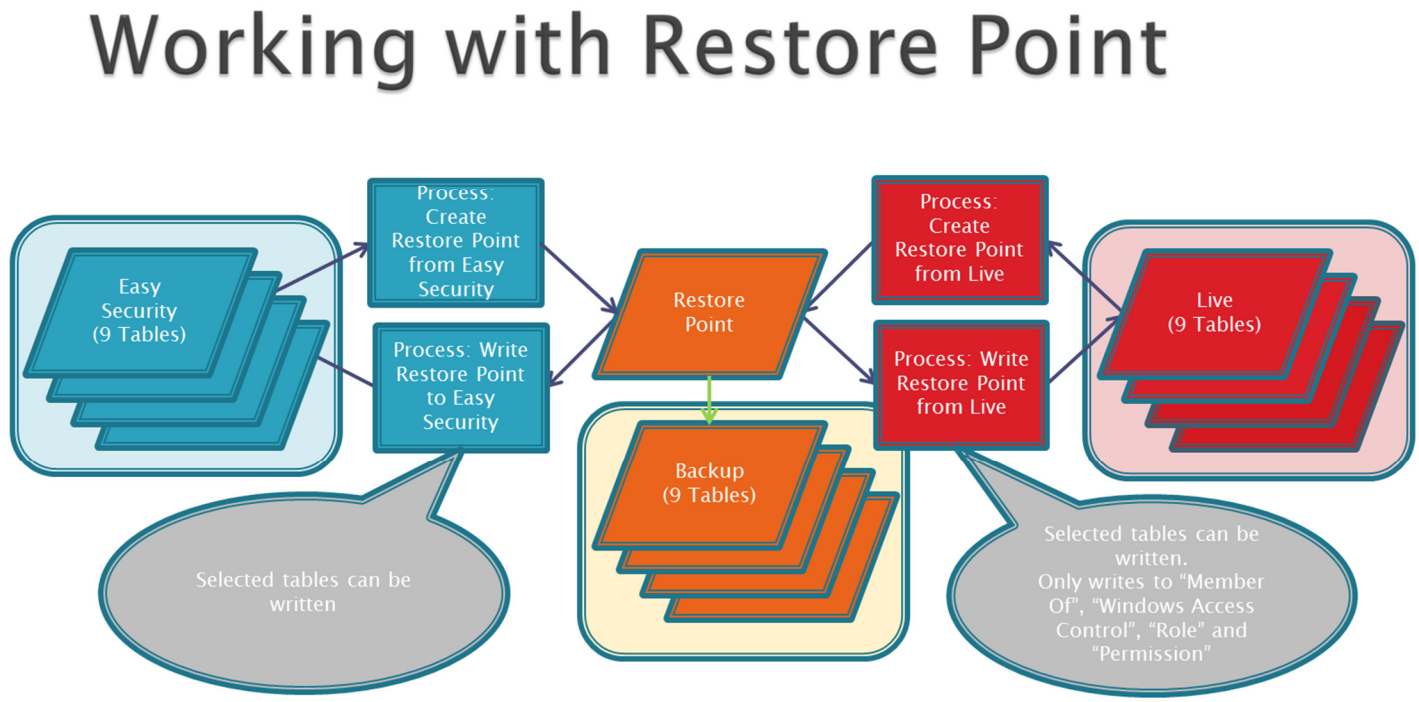
The Source Code Analyzer data can be created based on lookup into tables in “Easy Security” or “Live”. Only the relations based on Easy Security can be added to roles.

Working offline with Restore Points

A very important part of NAV Easy Security is the ability to work with permissions without changing the actual users. The Easy Security tables can be changed and recreated without affecting the users in the database.

The tables in “Easy Security” and “Restore Point” are not used in the active companies and will have a limited number of records. Because of the many flowfields of the type COUNT is most of the tables very well indexed. This will cause publishing and similar operation to be a little slower, but the performance in the NAV Easy Security application is much better.

To move data from “Easy Security” to “Live” and the other ways is a “Restore Point” used the diagram below explains the process of moving the data between the tables.

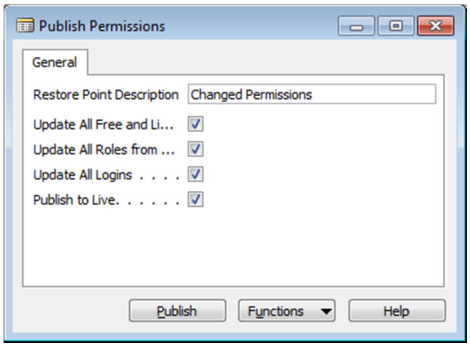


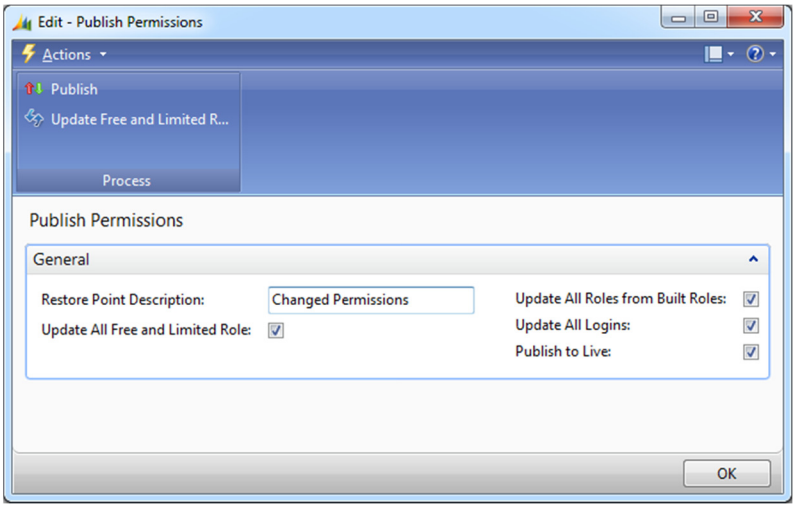
As the picture show is it only possible to move “Easy Security” to a “Restore Point” and a “Restore Point” to “Live” this ensures that no direct changes is done. Because every publishing of permissions build a restore point can it be reversed very easily to the state before the publishing.

A “Restore Point” can also be exported and imported to allow moving permissions from one server/database to another.

Publishing permissions

To publish permissions is a couple of steps required. The Publish Permissions window is making this very easy.





In most cases all steps should be processed. Click on the Publish after selecting the steps. The user doing the publishing of permission must be a SUPER user. The step Update All Roles from Roles Details require the Role Builder module has been purchased.

It is possible to only do a few steps or only creating a restore point by selecting the actions under functions.