# Introduction to Auto-Group

After more than 20 years of experience delivering numerous IAM (IGA) projects & solutions, OPNS observed some missing automation supporting valuable use-cases. One such example, unfortunately rather complex or sensitive to implement, is about "grouping" of Users enabling common operations on all users "belonging" to the same group. Standard IAM products, once installed out-of-the-box, do support the concept but all the logic behind it still requires design, coding, testing and other activities related to SW development.

The most obvious example is related to the position of the user in the organization chart, being a member of a department or another. In real-life, the simple fact to be member of a department leads to multiple actions in an Identity Management solution like NetIQ IDM; one such action is about assigning a business role related to that department, triggering further actions downstream through provisioning connectors. Then, if the user moves from one department to another, his associated business role will be updated automatically; such a feature provides real business value and improves overall security.
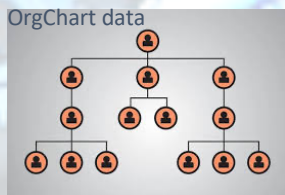
Besides the department a User belongs to, the same concept is applicable to other characteristics like the "User Type" (employee/contractor/…), the "Job Code" (Project manager/Sys Admin/…) and/or any other characteristics that directly influence access rights.

Creating & updating memberships for all these groups, then create associated NetIQ IDM roles, assign all these roles and maintain all relationships is not a simple task; a good level of automation is recommended to free-up time, avoid human errors, and keep pace with fresh data continuously changing the environment. For this challenge OPNS created **Auto-Group**, enabling full automation right inside your NetIQ IDM platform.

Auto-Group offers multiple features to automate many time-consuming tasks like:

- Creation of groups based on reference data (OrgChart …)

- Set users member of their group(s)

- Update group memberships as the data is changed

- Maintain **nested groups** up to date as the OrgChart evolves

- Update nested group memberships

- Create a container (sub-OU) in the role catalogue for each group (e.g. if group = department) and set the ACL for visibility restricted to the group members

- Create a role for each group ("department" or "job code" or …) and assign that role to the group

  o *This auto-assigns a default role to any member of the group.*

- Optionally: delete groups when the associated reference data doesn't exist anymore
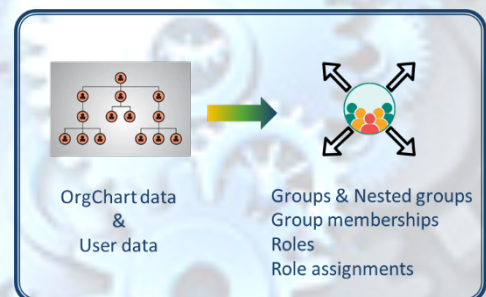
Auto-Group both automates time-consuming tasks and prepares your IDM environment in a smart way, enabling common use-cases to be deployed in a snap!

OPNS S.A. – N.V.
Brussels – Belgium
www.opns.net
info@opns.net
mir.iam@opns.net

Mir.IAM
*Identity project & solutions
straight to the point*

In essence Auto-Group has three main functions:

- **Create groups** based on reference data. This behavior is configured through Auto-Group's driver GCVs, where you can define prefix and suffix to group names (and description), placement of the groups in a dedicated container (OU), creation of nested groups (in case you have parent-child relationships between your reference data) and more.

- **Populate group memberships**. This is done based on user attributes that may or may not contain values corresponding to the reference data used to create the groups. This is quite like what eDirectory Dynamic Groups can offer, but Auto-Group static groups bring 3 main advantages:

    o Extensive use of Dynamic Groups in large environments has strong limitations and performance impacts. With (tens of) thousands of users and possibly dozens to hundreds of Dynamic Groups, your eDirectory will have difficulties coping with the resulting stress.

    o Dynamic Groups can't be natively nested, meaning you can't effectively use them to have a complete 'OrgChart' modelized into groups. To the contrary, static groups can be nested.

    o When Role-to-group associations is used (a handy function of RBPM), there is a delay before a role is effectively granted (or revoked) to current (or past) group members. Also, the more your environment is sizeable (referring to first bullet above), the more this delay must be increased to make sure RBPM has time to refresh all Dynamic Groups in one refresh cycle. With static groups a role-to-group grant or revoked is processed without any extra delay.

- **Create placeholders** in NetIQ IDM Role catalogue. With this capability you have:

    o A ready to use container (OU) where to place roles only visible by members of the group (typical use = one such container per "department group")

    Role

    o A ready to use role, already assigned to the group, and where you can link resources and/or child roles that will then be auto-assigned to each group member (use-cases = one default role per "department group" and/or one default role per "job function group")

Note: Auto-Group comes together with our "Reciprocal attributes" solution to automatically maintain all the 4 eDir attributes that makes a group membership 100% effective (the 2 attributes on the user and the 2 attributes on the group), with full support of nested groups! The next version will come together with a package to add to your AD connector in case you want to mirror auto-created eDir groups in AD, all automatically.

Auto-Group is part of ***Mir.IAM***, our overarching framework for a maturity level 5 IAM. We base our IAM projects on ***Mir.IAM***, which comes with a solution blueprint, an MVP, a project methodology and all components required to succeed fact and efficiently. Some of our ***Mir.IAM*** sub-components are packaged & available separately as a product, further designed to enrich any existing NetIQ solution. **Auto-Group** is only one of these products; contact or visit us to discover other surprisingly smart ***Mir.IAM*** sub-components!

OPNS S.A. – N.V.
Brussels – Belgium
www.opns.net
info@opns.net
mir.iam@opns.net