Introduction to Role with Grace Period

After more than 20 years of experience delivering numerous IAM (IGA) projects & solutions, OPNS observed that, in some cases, it is desired to delay some specific actions that would otherwise happen immediately.

In essence an Identity Management provisioning engine, like NetIQ IDM, is designed to automate as fast as possible any action that should be executed in the provisioned systems through IDM provisioning drivers.

One possible action that happens at the "upper-level", before provisioning drivers are activated, is the revocation of a role; when this happens to a user, the NetIQ IDM role sub-system (RBPM) analyses the content of the Role (child roles, resources and ultimately entitlements) and triggers all required actions at "lower-level", typically the revocation of multiple access rights in one or more business application, each action being performed by a specific provisioning driver.

Many possible triggers exist to start the revocation of a Role as, for example:

- Data imported from an authoritative source (HR database…) updates the characteristics of a User in the IAM system, and pre-defined rules do re-evaluate all automatically assigned Roles. If the new User's characteristics do not meet criteria required for a particular Role, that Role is revoked.
    - Typical use-cases are when a user changes department and/or job function
- An access review campaign is finalized and enters in its last step: the remediation process. If automated, that process will revoke any Role indicated as "To remove" by the reviewer(s).
- An administrator and/or Service Desk employee enters the IAM console and manually revokes a Role.
- An external workflow system calls the IAM system (through an API) to revoke a Role.

In some cases, it is desired to delay the effective revocation of access rights related to a Role, granting extra time for the affected User to smoothly transition from the previous state to the new state.

One situation is when an employee changes job position but still needs to 'coach' another employee that is overtaking his previous job. For a week or two the employee still needs some or all his previous access rights to effectively support & coach his new colleague.

Another interesting use case is risk mitigation in business operations. Indeed, some risks are implied by human errors, for example when a Role was mistakenly revoked as part of an access review campaign or other processes. By granting a Grace Period the affected employee(s), being notified, has(have) time to react and the human error can be fixed before any associated access right in any application is effectively removed.

Role with Grace Period is designed to be easily deployed on top of any existing NetIQ IDM setup with an existing Role Catalogue. With **Role with Grace Period**, you can easily define which Role benefits from a Grace Period and which another Role does not.

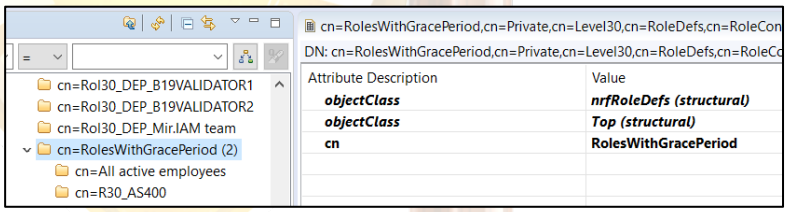
Role with Grace Period add-on for NetIQ IDM enables smooth business operations, facilitates the deployment of your RBAC Role model and reduces risk related to human errors.

In a nutshell what **Role with Grace Period** code does is:

- Carbon-copy granted Roles.
- Analyze transactions related to revocation of Roles.
- Keep the carbon-copy Role granted for the defined grace period and set a future revocation for it.
- Analyze transactions related to the grant of a Role and cancel any future revocation if required.
- Configurable: send notifications about the start of a grace period for a role.

So, when any event or process revokes a Role, and if that Role is being 'protected' by a Grace Period, **Role with Grace Period** will maintain the carbon-copy role granted for the specified number of days and, optionally, send a notification to the affected user.

Carbon-copy roles sit right in your Role Catalogue inside NetIQ IDM, and can be viewed, edited and deleted through the standard NetIQ IDM administration interfaces ("Identity Applications" portal and RBPM API).



G ⊆ R

Since v2.00 onwards, to support more advanced use-cases in the 'job position transition' use-case, **Role with Grace Period** now implement carbon-copy roles that are possibly more restrictive than the original roles. This advanced feature enables an employee to **keep a subset of previously granted access** during the grace period, for example only READ access to some business data instead of READ-WRITE, enabling that employee to effectively coach a colleague during the job transition but without enough rights to perform the job on his behalf.

Installing and configuring **Role with Grace Period** is an easy process requiring only basic knowledge of NetIQ IDM; its associated IDM driver is simply deployed side-by-side to other drivers in your driverset and can be stopped/started/audited independently of the RBPM driver itself; no impact at all on your current setup!

Role with Grace Period 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. **Role with Grace Period** is only one of these products; contact or visit us to discover other surprisingly smart ***Mir.IAM*** sub-components!