Introduction to Local Admin Provisioning

After more than 20 years of experience delivering numerous IAM (IGA) projects & solutions, OPNS observed that, aside from the typical control perimeter of an IAM solution, there are (tens of) thousands of computers that fall into a "grey zone" and follow different rules and processes.

A well-known example are all AD domain-joined Windows machines, being workstations (laptops, desktops, VDI machines…) or servers.

For various valid reasons some staff require, permanently or temporarily, the so-called **Local Administrator privilege** on a single machine or a group of machines. This can be a requirement for:

- a specific user on a specific machine; typical use cases are IT developers on "their" respective workstation.
- a team on a set of servers; for example, a project team installing SW on servers in a LAB environment.

Unfortunately, in most cases, managing Local Admin privileges for Windows machines is performed through parallel request/approve/implement processes, bypassing well designed & controlled IAM processes...

Consequences are:

- End-user experience: no single place where to request access rights (some access rights are requested through IAM, some others, like Local Admin, are requested through another channel).
- No central place where to look for ALL access rights granted to a user (→ control risk).
- Lack of integrated solution to revoke such rights when a lifecycle event affects the user, for example when his department and/or job function is changing in the organization.
- No inclusion in any Access Review process → Local Admin rights survive "under the radar".
- No participation in the IAM (RBAC) role model → no method to automatically manage such a privilege for staff that meets conditions (grant) or not (revoke).
- Extra workload put on the AD team that must manage all Local Admin requests, control & revoke previously assigned rights, provide reports… all without the benefits of existing IAM processes.
- In a worst-case scenario, granting the privilege happens through "Administrator" credentials of the machine being shared! This is a far cry, from a security point of view, compared to granting equivalent rights through the user's AD account…

Local Admin Provisioning integrates the local "Administrators" group of every domain-joined computer into NetIQ IDM role catalogue. As such, requesting/approving and revoking the Local Admin privilege on any such computer becomes a standard feature available through the NetIQ IDM self-service portal, and comes with all associated benefits like reporting, access review campaigns (through NetIQ Identity Governance) etc…

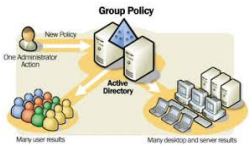
Local Admin Provisioning sits side-by-side with your AD Group Policy Objects (GPO), complementing them with the possibility to have granular control, through standard IAM processes, over individual members of any domain-joined computer's local "Administrators" group.

Local Admin Provisioning extends the reach of IDM to every Windows computer in your AD domain!

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

Implementing **Local Admin Provisioning** in your NetIQ IDM + AD environment is simple and easy:

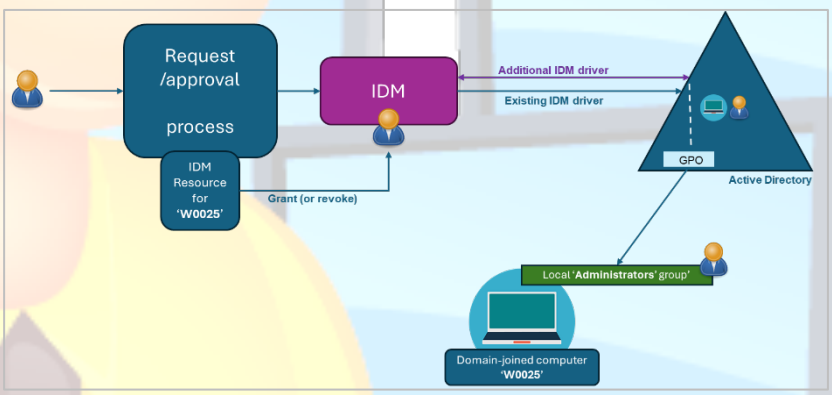
- **Pre-requisite**: you have an operational IDM-to-AD driver in place, and that driver is configured to support the standard IDM Resource-to-AD group provisioning process.
- **Deploy the Local Admin Provisioning driver**. This driver sits alongside your existing AD provisioning driver, without any interference (no change on your existing AD driver).
- **Optional: deploy the custom request form**. This form enables end-users to request "Admin" rights for AD domain-joined computers. The custom form is designed to offer 2 options:
  - request for "My computer" (computer ID pre-configured* if available).
  - request for "Another computer" (select computer ID from a list).



- **Prepare your AD environment**.
  - Create an OU for Local Admin objects created by the IDM driver.
  - Deploy the new GPO and, only if needed, adapt your existing "Restricted Groups" GPO.
  - Optional: add the smart discovery process* in Users' login script.

: an optional process can dynamically discover which workstation "belongs" to each AD user. When this process is activated the custom request form knows which Computer ID to indicate in the IDM Resource if requesting admin rights on "My computer".

Once the setup is done, in a matter of a couple of hours, you'll benefit from auto-created IDM Resources that are requestable, directly or through IDM roles, all through the NetIQ IDM workflow sub-system.



When the "Local Admin" Resource is granted to an IDM user, provisioning actions will result in the AD account of the user being a member of the local "Administrators" group of the specified computer. There is no need to share any other "Administrator" credentials with the user!

Because it all works through standard NetIQ IDM processes, and because it leverages your existing IDM-to-AD provisioning driver, you immediately benefit from all associated features you have deployed such as, for example, reporting, access reviews, de-provisioning and more.

Local Admin Provisioning 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. **Local Admin Provisioning** 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