



**2nd Annual**  
**MidPoint Community Meetup**

**Micro-Certifications in midPoint**

# Agenda

- Introduction to certifications
- Certification Campaigns
- Micro-certifications
- Micro-certification use cases
- Configuration structure
- Demo



# Introduction to Certification Campaigns

- automation is always the goal in IGA
- not everything can be automated
- solution is in managed requests and approvals
- **main problem**
  - *users ask for access to be granted but never to be revoked*
- **solution ???**



# Certification Campaigns

- they serve as counterbalance to access requests
- why they are essential
  - economic reasons
    - saving money on licenses
  - security
    - principle of least privilege
- ***problems with certification campaigns***
  - ***large number of reviewer items***
  - ***disconnected from the event that required provisioning***
  - ***often result in default responses***
- ***solution ???***



## Micro-Certifications/Ad-Hoc Certifications

- connected to the relevant events
- continuous
- automated (as automated as possible)
- relieve the load from periodic certification campaigns significantly



## Mover Role Membership Provisioning

- employee moves from one department to another
  - organization role change triggers ad-hoc certification
  - accesses are evaluated
    - based on risk level
    - based on origin of the role
    - other criteria



## Balancing Granting Automatic Access to Low Risk Roles

- user requests access
  - access is automatically granted
  - this action triggers ad-hoc certification to revoke the access
  - in case the access is unnecessary, it is removed
- benefits
  - no waiting period for access for justified provisioning
  - unjustified access is deprovisioned in reasonable time
  - very suitable for low risk accesses



## High-Risk Role Membership Evaluation

- main high risk role exists
- it induces other roles
- the main role is changed
  - new inducement is added
  - this event triggers ad-hoc certification of all main role assignees/members
- this adds another security layer



## Configuration Structure

- certification campaign definition
  - remediation definition with style automated
  - adHoc: true
- policy rule induced in policy or archetype
  - specifications set in policy constraints
  - policy actions reference the certification campaign
- policy or archetype with the policy rule assigned to the target object (e.g. user)
- action specified in policy constraint triggers campaign
  - reviewers, stages, strategies are set in the campaign definition





# DEMO

# Evolveum

## Thank you for your attention

Feel free to ask your questions now!



2nd Annual MidPoint Community Meetup