

Role mining

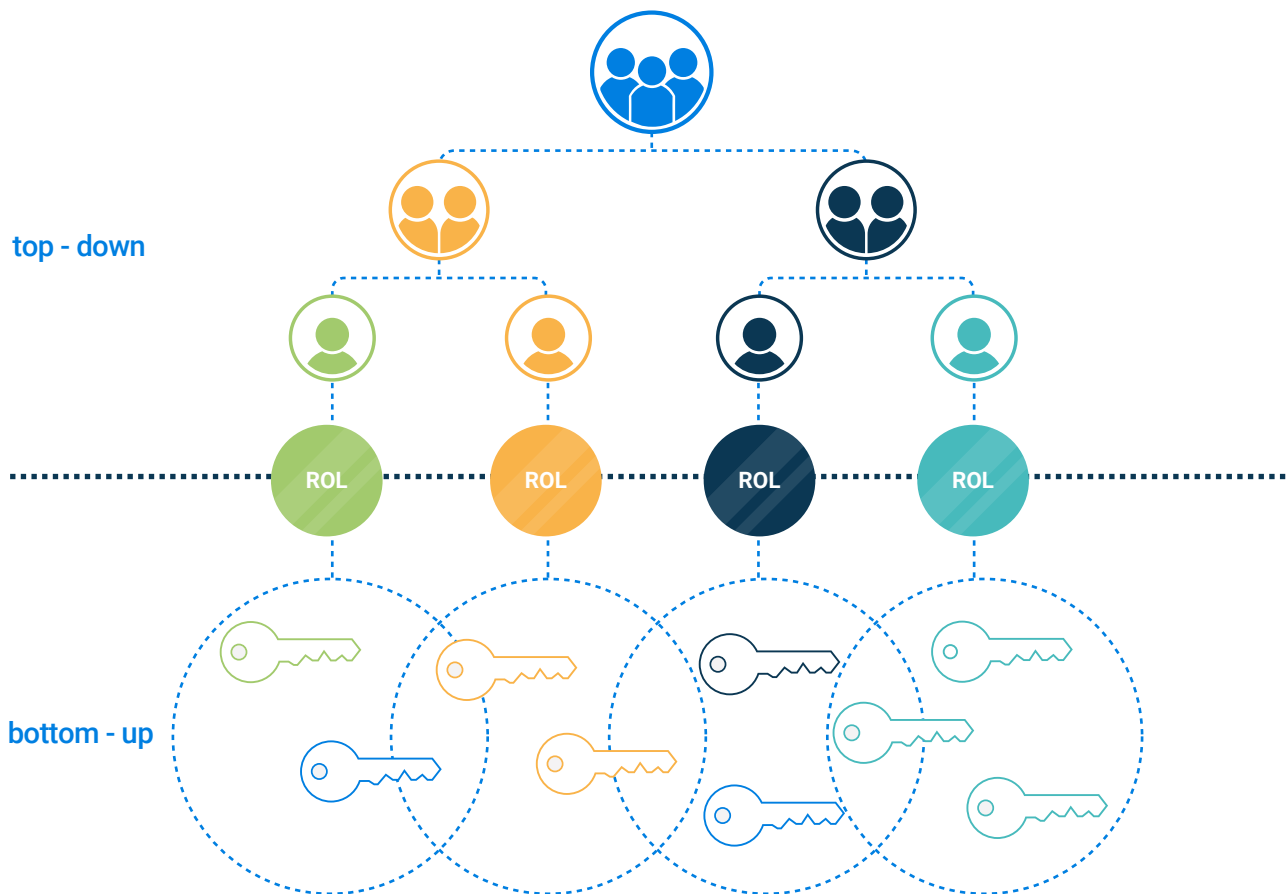
Many customers combine the rollout of HelloID with the implementation of Role Based Access Control (RBAC). Based on clear roles and corresponding business rules, this allows you to easily and automatically manage the access rights of all users. Of course, this requires a smooth and fast RBAC implementation. Tools4ever developed a pragmatic role mining approach specifically for this purpose.



In RBAC, every user is linked to one or more clear roles, often related to someone's function, department and/or location. For each role, the corresponding access rights are recorded in business rules, allowing us to automatically provide users with the same role with the right rights. If someone's role changes, the rights are also automatically adjusted. However, many customers are reluctant to implement RBAC. How do you build such a complete scheme with sometimes hundreds of roles and rights? How do you involve key players in that process? And won't your model be outdated by the time you're done? We solve this at Tools4ever with our role mining approach. A clear step-by-step plan with which we translate existing data from HR systems and (Active) Directory directly into an initial RBAC model. Role mining prevents us from having to develop such a model from scratch. Instead, we have an excellent starting point with roles and business rules from which we can further improve and refine the model. Tools4ever uses technical tools in combination with further analysis steps. Thus, together with the client in an efficient process, we arrive at an initial and immediately usable RBAC implementation.

Role mining approach

- 1 Inventory of existing roles:** We collect top-down the different roles as registered within HR.
- 2 Inventory of existing rights (groups):** We distil bottom-up from the applications and IT systems - such as an (Azure) Active Directory - the currently actually assigned rights and groups.
- 3 Designing RBAC concept:** We match the information from steps 1 and 2. We discover patterns in authorisations based on the collected information and process these in an initial concept with roles and associated business rules.
- 4 Evaluation of the concept with stakeholders such as department managers:** Inaccuracies and contamination (e.g. due to previous accumulation of rights) are identified. Based on this, we adapt the concept to an initial usable model.
- 5** The result is a first baseline version of the role model, which can be applied operationally. From here, the model can be built on, regularly updated and adjusted according to new insights.



Integrated approach with birth rights and options

By default, we recommend limiting the RBAC model to so-called birth rights, the 'standard' rights belonging to someone's primary role. We then manage individual exceptions such as special applications or access to project folders as options via the HelloID Service Automation module. This allows users - or their managers - to request online access to applications or folders via automated self-service workflows. HelloID thereby ensures that the correct approval steps are completed and the rights are subsequently activated in the IT environment. Risky mistakes are thus prevented and automated configuration rules ensure that the service catalogue is automatically kept up-to-date.

Want to know more about the Tool4ever role mining approach?

So, for organisations that do not yet have a role model, we combine the unique combination of HR and user network data to implement an initial RBAC model via role mining. Role mining requires analysis, verification and consultation in addition to technical tools to develop such a baseline. Points of attention include removing existing errors, contamination and rights stacking. Our business consultants have extensive experience in this and will help you in a clear, defined consultancy process to quickly realise a baseline RBAC model via role mining.