Identity Manager from One Identity (OI)

Optimized administration of authorizations and processes

One Identity Manager enables the central administration of identities - including their authorizations - and promotes the automation of the processes related to them. Identity Manager enables companies to satisfy increasingly complex security and IT governance requirements, while ensuring that access management is consistently aligned with business needs.

Enterprise access management is more demanding than ever

Access and authorization management in companies is a considerable time and cost factor; the implementation and maintenance of an identity and access management solution involves a significant investment. The technical landscape of organizations is ever-changing, and the number of remote employees has never been greater. More than ever, users need to be able to access their necessary data and applications from anywhere in a targeted and secure manner. Furthermore, applicable security regulations and current legal requirements must be taken into consideration at the same time. An IT department cannot meet these requirements by individual, non-integrated local solutions and manual processes.

Automated provisioning of user identities and authorizations

Identity Manager from One Identity reduces the complexity of access management through central administration and automation of processes by bundling all security-relevant policies and processes in one place. With the help of the dashboard function, for example, on-demand or routine confirmations can be scheduled and the status of group or distribution lists can be displayed in a clear overview. Central administration and automation of processes reduces the workload in the IT department. One Identity Manager transforms the IT department from an access management bottleneck to a business enabler. Employees of the individual business units are responsible and empowered to implement processes in the most effective and efficient way.

Self-service access portal and password manager

The self-service access portal is a special feature of Identity Manager, because no one knows better when they need access to certain applications than the employees themselves. Based on predefined approval processes and workflows, users can use the "online shopping cart" to request access rights and authorizations, as well as inclusion in group and distribution lists. Additionally, the functional scope of Identity Manager can be expanded with the help of numerous supplementary modules. For example, Password Manager allows employees to independently reset the passwords of their user accounts after the company-specific password policies for the various user roles have been centrally defined and stored. This

saves money and improves user satisfaction, as there is no need to go to the IT department for simple password management

Product characteristics & features

- Modular and scalable IAM solution
- SAP-certified
- Existing SAP applications can be easily integrated and extended
- Cloud-based add-on service for hybrid and SaaS applications
- Dashboard for planning on-demand and routine confirmations
- Self-service access portal for employees
- Numerous extensions available (Password Manager, Starling Connect, Active Roles, Multi-factor Authentication etc.)

Your benefits at a glance

- Administration of access to local, cloud and hybrid resources
- Reduced risk by ensuring that users only have access to applications they need
- Adherence to audit and compliance requirements with the help of stored guidelines for (re-)certification
- Transfer of access decisions into the right hands (business level)
- Reduced IT workload through self-service access portal
- High system compatibility, which supports building on existing infrastructures with appropriate expansion

„In many companies, access management ties up too many personnel resources for a system landscape that is often quite heterogeneous and hybrid, especially in the IT department. By centralizing administration and automating processes, One Identity Manager significantly reduces the cost and complexity of access management. Identity Manager empowers organizations to ensure they provide the access level actually required for employees in accordance with the company’s security regulations. This applies throughout the entire identity lifecycle, regardless of whether the user is joining, changing or leaving the company."

Gerald Appel (Team Lead One Identity)