

Access Management

Manage physical access permissions organisation-wide and across all sites, regardless of the systems in place.



The ID-ware Access Management Module centralises the granting and withdrawal of physical access rights in different legacy systems. It also increases traceability of all actions, ensuring compliance with both corporate and official regulations.

Does your organisation operate across multiple locations with various unconnected systems (such as access control, parking management, etc.)? Managing authorisations across these systems can often be challenging, time-consuming, and costly. Additionally, maintaining a clear overview of all authorisations within the organisation can become increasingly complex and incorrect authorisations are a security risk.

The ID-ware Access Management Module allows physical access permissions to be managed organisation-wide and across all sites, regardless of the systems in place.

The outcome of this consolidation: an efficient, streamlined solution with numerous benefits.

Function Overview

Automatic Assignment of Authorisations (Rule Engine)

Via its Rule Engine, the ID-ware Access Management Module will evaluate the complexity of conditions and attributes for each person and automatically assign their access permissions.

Dynamic Permission Models

You have flexibility to create highly detailed & dynamic permission models eliminating the need for pre-defined roles (like with role-based access systems).

Integration with HR Systems

In high security environments where assigning permissions manually is a challenge, you can simplify and re-risk the process based on employee attributes integrated with HR systems.

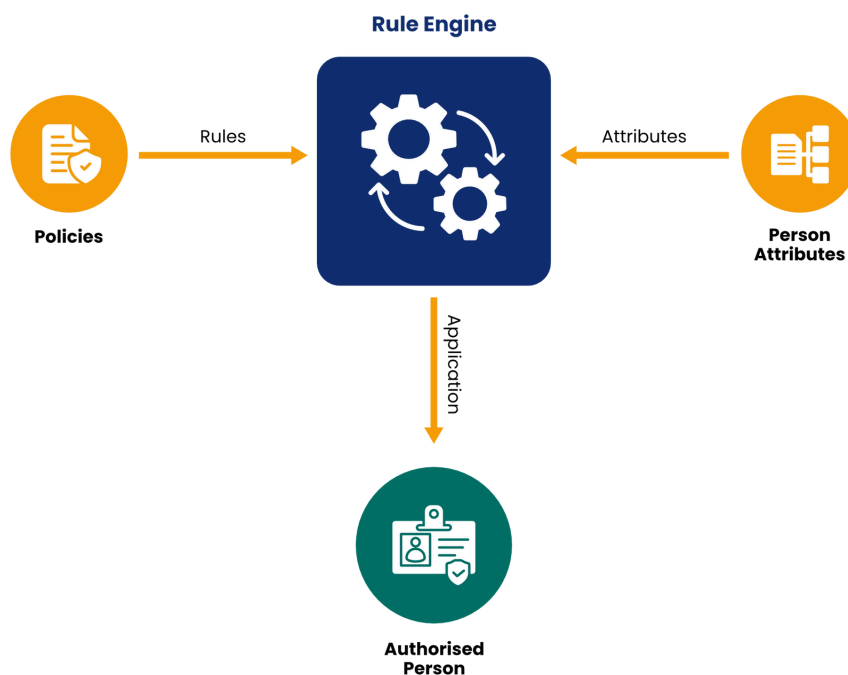
Automatic Adaptation of Changes

It will automatically adapt to changes, based on attributes or time-based needs ensuring permissions remain accurate without your manual intervention.

Workflow Engine

You can create individual workflows for requesting, approving and assignment of authorisations to persons: from non-interactive with automatic approval up to complex models requiring approval by managers, asset owners or verifiers.





The Rule Engine evaluates the complexity of conditions and person attributes and automatically assigns their access permissions.

Key Benefits



Centralisation

Centralised, cross-site access management: Automated process for assignment/withdrawal of authorisations



Risk reduction

Increased traceability, i.e. compliance with company & official policies as well as centralised reporting



Workflows

Multi-level workflows for request and approval of authorisations



Overview

Full overview of all authorisations anytime (cross-site & cross-system)



Traceability

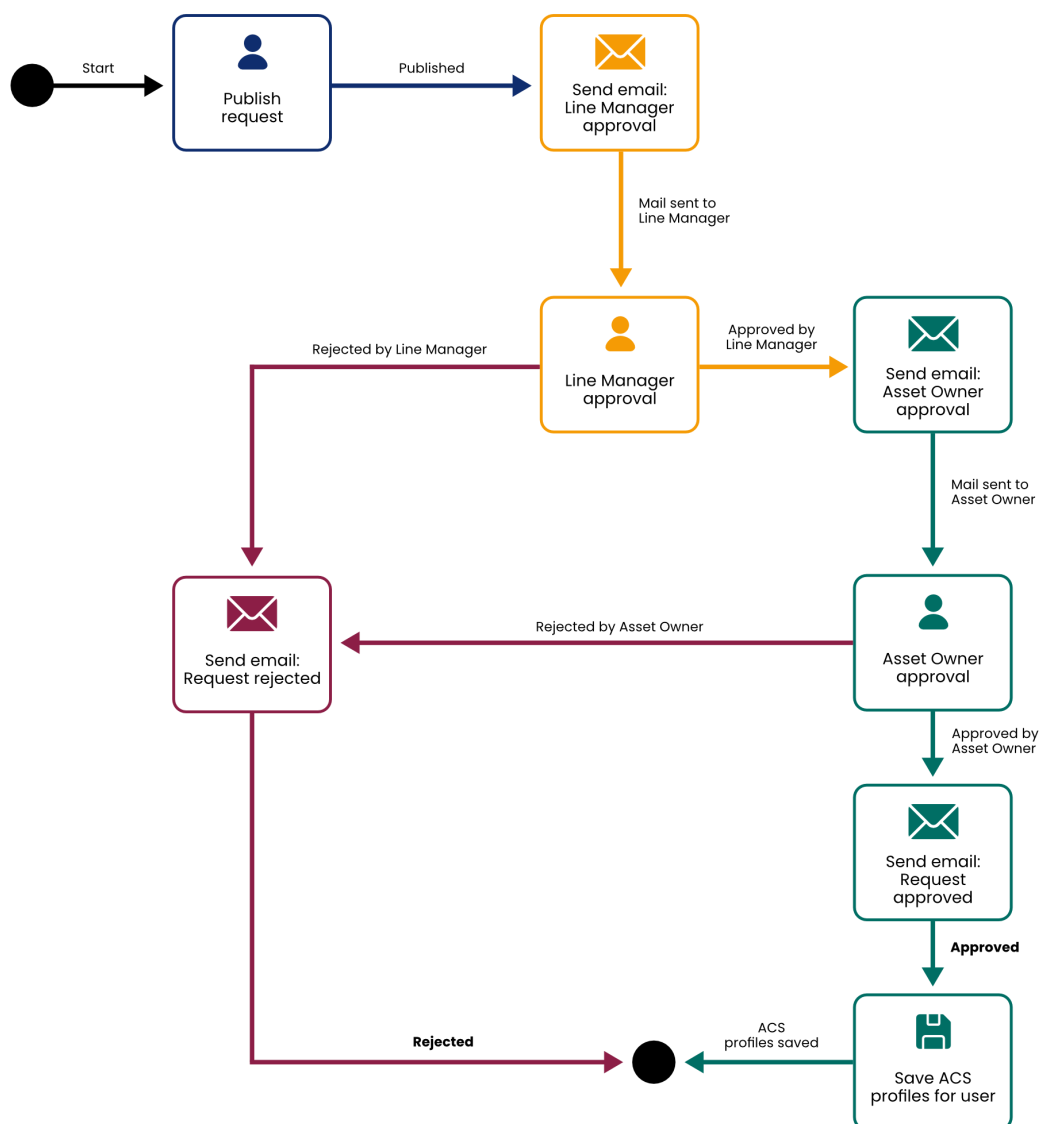
Increased traceability, i.e. compliance with company & official policies



Cost reduction

Cost reduction due to reduced administration effort (streamlined process)

Workflow Example



Your workflow models can be connected to specific locations and access control profiles. By configuring the Workflow Engine, you can ensure compliance with both local policies and requirements, as well as cross-site policies.

About us

ID-ware is a leading global provider of Physical Identity and Access Management (PIAM) solutions. With over 20 years of experience, we are specialised experts for effective identification and authentication processes to support large-scale organisations.

Our innovative and secure products in connection with our strong principle of long-term partnerships make our customers profit from customised solutions for their complex environments.



Netherlands: +31 70 337 1500
Germany: +49 69 210 8555 60
UK: +44 20 8050 2648



info@id-ware.com