CASE STUDY

Šumperk Hospital: Secure and automated identity governance

Šumperk Hospital is a general hospital providing extensive inpatient and outpatient care. With nearly 2,000 employees and almost 200 external partners and students, the hospital operates in a complex environment where accurate and timely permission settings are critical for both security and operational continuity.

The challenge

The hospital's HR system was not integrated with Microsoft Active Directory (AD), as identity and user account management was handled largely manually. This resulted in several issues:

- User account administration was complicated and time-consuming.
- AD accounts were created, updated, and disabled manually based on email or paper requests.
- Requests for new system permissions were processed through an internal HelpDesk, slowing down operations.
- Manual changes were slow to implement and prone to human error.
- Due to the risk of errors, accounts and access rights had to be reviewed manually at regular intervals.

The solution

To address all of these challenges, we deployed an IDM solution that serves as an integration layer between the HR system and Active Directory. The system manages access through:

- daily synchronization of data from the Vema Cloud HR system,
- automated account creation, updates, and deactivation in AD,
- permission management in target systems through AD groups,
- a dedicated UI for access requests and approvals,
- self-service password reset with SMS code verification,
- a complete audit trail of all relevant operations and changes.

2 075
total managed identities

1 671
application and business roles

18
applications with AD-managed access

1 400+
monthly role requests

Key solution features:

- If an individual has multiple employment contracts, they are managed as a single identity.
- Manages employees, contractors, and students.
- Access rights can be tied to specific employment contracts or to a defined time period.
- Approvers can assign delegates to act on their behalf during absences.
- When a user's name changes, a new username is prepared, IDM delays activation by 7 days, and notifies the user so they can prepare for the change.
- Reports on user access, compliance, approved access requests, and application/role owners. Furthermore, IDM sends daily event summaries and monitors the HR system for any changes.

> *The IDM has brought significant time savings for our IT team, reduced error rates, and provided a clear audit trail for managing the lifecycle of users and their access rights. We also value the constructive cooperation with the Orchitech team and their fast response to urgent situations.*

— Josef Loupanec. Head of IT, Šumperk Hospital

The outcomes

- **Reduced error rates and IT workload** through automated identity lifecycle management. Changes in HR data are reflected in AD, and when a contract ends, the system immediately revokes all associated permissions.
- **Enhanced control and security, and easier audit** through clear and fully auditable entitlement management. For every access right, it is possible to demonstrate exactly who requested it, who approved it, which contract it relates to, and its duration.
- **Less pressure on IT support** thanks to a self-service portal. Users can handle routine tasks themselves, meaning IT no longer needs to manually process every access change or password reset.

The deployment of the IDM system at Šumperk Hospital demonstrates how automated Identity Management can fundamentally simplify IT operations while boosting security and auditability. By integrating the HR system directly to Active Directory, the hospital has minimised manual intervention, accelerated access management, and prepared the organisation for evolving legislative requirements.

About client

Šumperk Hospital is a general hospital serving a catchment area of up to 200,000 residents. It hospitalises over 20,000 patients annually and performs approximately 8,000 surgeries. The hospital employs nearly 2,000 staff and works with nearly 200 external contractors and students.

Co-funded by the European Union

MINISTRY OF REGIONAL DEVELOPMENT CZ

The IDM system was procured through a public tender as part of project CZ.06.01.01/00/22_003/0000038 - "Podpora kybernetické bezpečnosti pro Nemocnici Šumperk a.s." and this project was funded by the EU.

About Orchitech

We help IT departments:

- manage and secure the identities of employees and external workers efficiently,
- automate routine tasks,
- save time and reduce costs,
- eliminate audit-related stress through instant visibility and control.

Our solutions help organizations comply with legislative requirements, including GDPR, NIS2, and other regulations. We have been active in the market for over 18 years, successfully delivering more than 100 projects for approximately 50 clients across sectors.

https://orchi.tech/ +420 216 216 850 info@orchitech.cz

orchitech