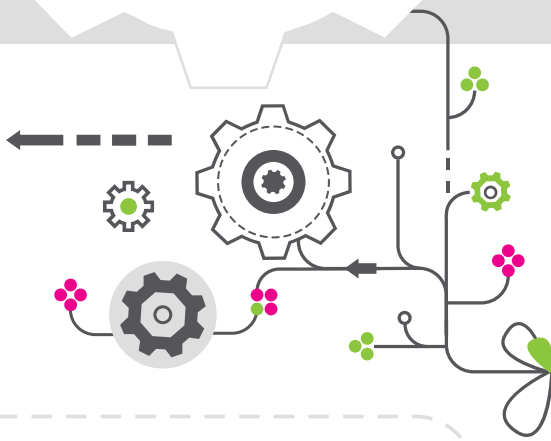
Case study

University of South Bohemia: Effective Identity Governance with Wren:IDM

The University of South Bohemia in České Budějovice needed a new, reliable IDM solution for an environment with thousands of students, regular student enrollments, and a multitude of systems, as the original solution was no longer sustainable. Orchitech won the tender with the Wren:IDM solution thanks to its flexibility, speed, transparent costs, and ability to adapt to the university's specific processes.

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice



When the old solution falls short

The original IDM system from Novell no longer met the needs of the University of South Bohemia.

The implementation of processes had become outdated, prone to errors, and any configuration adjustments were difficult. *"In the original setup, reconciliation—comparing the desired and actual system states—was virtually impossible when the system desynchronized for any reason,"* explains Mr. Marek, Head of IT Infrastructure Management at UoSB. Additionally, the vendor changed its pricing model to charge per identity. With tens of thousands of identities, this made the licensing prohibitively expensive. As a result, UoSB had to change its system.

This presented an opportunity to implement processes according to current needs and introduce several improvements. *"The University anticipated that transitioning to a new system would be beneficial. The primary criterion for the new system, however, was TCO, aiming to reduce costs compared to the original solution,"* says Mr. Marek.

Total Cost of Ownership

As part of the supplier selection process, UoSB calculated 5-year total costs, including licensing fees, maintenance, support, and development work for up to 1,000 MH. A key requirement was the transfer of complete configurations to avoid vendor lock-in. That is also why an open-source platform was favored. Orchitech's solution provided transparent pricing, allowing the university to acquire the new system for the cost of just one year of licensing support for the previous solution.

Orchitech won the tender and delivered a solution based on Wren:IDM, the open-source successor to OpenIDM. The flexibility of Wren:IDM also allowed for the easy implementation of requirements specific to the university environment, including a fully customized user interface.

> *We now have a completely new system that is more reliable, faster, more predictable, and easier to recover in case of failures. Whether it's catching up on changes from the source systems or verifying and reconciling the state in the target systems.*

— Jan Marek
Head of IT Infrastructure Management Unit
University of South Bohemia

Problems detected during implementation

During the implementation, we used synchronization in "dry run" mode to uncover several data consistency issues that persisted from the original IDM:

- In Active Directory, we identified numerous attribute inconsistencies (e.g., trailing spaces in names, commas in DN, etc.).
- Username conventions sometimes generated names longer than 20 characters, exceeding AD limits (the original IDM, shortened names without errors).
- Passwords had discrepancies because the password policies of the original IDM were not aligned with AD requirements, resulting in data mismatches between the original IDM and AD.
- Other inaccuracies in email addresses generated by the original IDM that were not according to the required algorithm. The new IDM corrected these issues.
- LDAP for FreeRADIUS contained multi-valued records in attributes that should have been single-valued. The original IDM did not flag this, leading to potential misinterpretation of some accounts.
- Certain systems enforced referential integrity, which the IDM needed to respect by correctly ordering record creation and modification. As this was primarily not done, several errors appeared in the original IDM's operations and the data was not properly synchronized.

By identifying these issues early, we resolved them through data cleanup and IDM script adjustments, ensuring a smooth transition to production.

Specifics of the solution

- **70 000 identities** (15 000 active)

5 source systems:

- IS/STAG study agenda system
- EGJE HR system
- Lifelong learning platform
- Card system
- Facilities and classroom registers

10 managed systems:

- MS Active Directory
- LDAP
- PostgreSQL DB
- RADIUS LDAP
- Card system
- Library system
- and others

Maintaining continuity upon leaving the university

Users can continue to access certain services for a period after leaving the University, such as their university email account. We addressed this by introducing configurable grace periods. These periods are specific to different identity types and can be adjusted as needed. For each identity, a retention period is calculated upon termination. Only after this period expires is the identity fully terminated, and access is blocked. Additional processes, such as email forwarding to a personal account, are also linked to the calculated retention period.

Personal data shredding

Identity management is inherently well-suited for the automated handling of personal data in managed systems, particularly for often overlooked data disposal processes required by GDPR and by individual national data protection laws and also regularly audited by data protection offices.

However, specific challenges arise in university settings, such as students enrolling in consecutive programs or employees returning after just one semester off. Immediate disposal would disrupt data continuity across the organization's systems.

Therefore, in the case of UoSB, it is initially replaced by pseudonymization, which erases unnecessary personal data while still allowing correlation via a hashed unique identifier. This enables identity restoration through HR systems. Final disposal, including the complete deletion of the identity and related links, occurs only after the set period for that identity type has expired.

Management of guest identities

Universities typically experience high turnover of identities. Beyond students, this includes conference guests and external collaborators who require specific access. This mostly includes WiFi connection and access cards. Therefore, the IDM system supports the management of temporary—or guest—identities.

Administrators at each faculty of UoSB can manage these identities, setting restrictions such as maximum validity or username prefixes. University administrators can oversee guest identities across all faculties.

Once a guest identity is created, the IDM system handles the entire lifecycle, granting necessary access and ensuring timely revocation of rights.

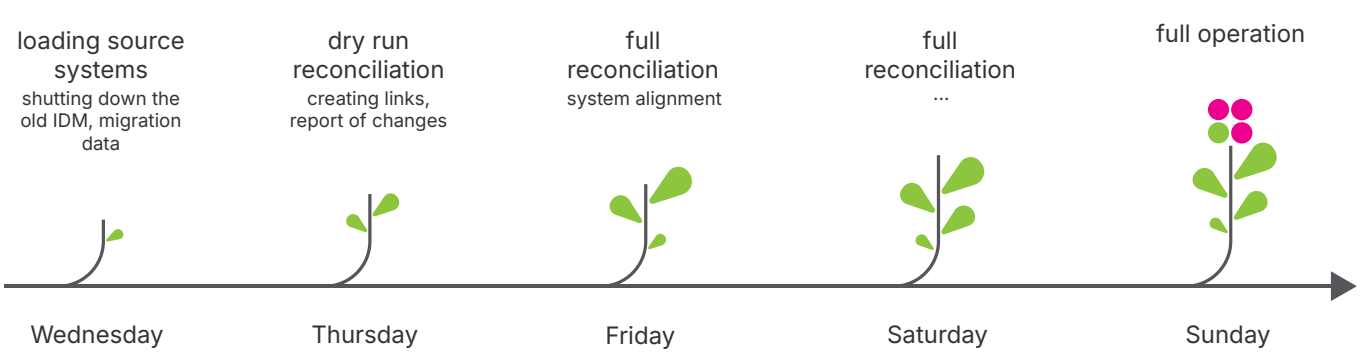
Migration

Thanks to careful preparation, the complete production migration was carried out in less than a week. The migration to the new IDM was completed without any downtime and without impacting end-users. After the migration, the error rate in processing IDM processes dropped dramatically.

Migration statistics:

- **14 000** correctly matched valid accounts
- **33 000** disabled accounts without owners (accounts of former students)
- **80** incorrectly enabled accounts (accounts that should have been disabled but were not)
- **8** missing accounts (accounts that should exist but did not)

Migration process:



Benefits for the University

The project aimed to improve reliability, reduce operating costs, and gain full control over the identity lifecycle across the university infrastructure. All these goals were successfully achieved.

The Wren:IDM implementation at the University of South Bohemia showed that modern identity management can significantly improve operational efficiency, security, and the long-term sustainability of the IT environment, even in an organization with highly specific requirements and a large number of identities.

> *IDM deployed by Orchitech has impressed us with its speed and reliability. According to the RT system, we now handle 80% fewer requests. The remaining 20% are mostly just forgotten passwords. The solution covered all our needs, and was delivered in the promised timeframe.*

— Jan Marek
Head of IT Infrastructure Management Unit
University of South Bohemia

80 % fewer
incidents related to identity and access management

Lower TCO
thanks to the open-source system and transparent business model

IT workload reduction
most identity-related processes are now fully automated

Readiness
for audits and compliance with regulatory requirements

Are you interested in how IDM can help your organization?

We'd be happy to share more experiences from the academic, public, and private sectors.

About the client

The University of South Bohemia in České Budějovice is among the 10 largest universities in the Czech Republic. It has over 10,000 students, with hundreds of staff involved in their education.

IAM at the university is challenging not only due to the number of identities but also because of the regular influx and departure of students at the start and end of each academic term.

The university has been collaborating with Orchitech since 2014.

About Orchitech

We help IT departments to:

- Automate routine tasks
- Save time and costs
- Efficiently manage and secure identities of employees and external workers
- End audit-related stress thanks to instant oversight

Our solutions ensure compliance with legislative requirements, including GDPR, NIS2, and other EU regulations. Since 2008 we have delivered over 100 projects for 50 clients in public and private sectors.

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

orchitech