Photo: University of South Bohemia in České Budějovice.

University of South Bohemia: Efective Identity Management with Wren:IDM

70 000 identities (15 000 active identities)

5 source systems

- IS/STAG study agenda system
- EGJE personnel system
- Lifelong learning system
- Card system
- Building and classroom registers

8 managed systems

- Active Directory
- LDAP
- Aleph
- DB
- RADIUS LDAP
- ...

reference

> 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 within the promised timeframe.

Ing. Jan Marek
Head of IT Infrastructure Management Unit, University of South Bohemia

challenge

When the initial solution is not enough

The original IdM system from Novell no longer met the needs of the University of South Bohemia (UoSB).

The implementation of processes had become outdated, prone to errors, and any configuration adjustments were difficult.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 Unit 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. The University was therefore compelled to change the system.

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

Orchitech won the tender and delivered a solution based on Wren:IDM, the open-source successor to OpenIDM. “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 system or verifying and reconciling the state in the target system (e.g., LDAP, AD),” continues Mr. Marek. The flexibility of Wren:IDM also allowed for the easy implementation of requirements specific to the university environment, including a fully customized user interface.

Total Cost of Ownership

As part of the supplier selection process, UoSB calculated five-year total costs, including licensing fees, maintenance, support, and development work for up to 1,000 man-hours. A key requirement was the transfer of complete configurations to avoid vendor lock-in, which is why we favored an open-source platform. 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.

Ing. Jan Marek
Head of IT Infrastructure Management Unit at University of South Bohemia

solution

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. Data shredding is also mandated by the Czech Office for Personal Data Protection (ÚOOÚ).
However, specific challenges arise in university settings, such as students enrolling in consecutive programs or employees returning for just one semester. Immediate disposal would disrupt data continuity across the organization’s systems. Therefore, 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, such as WiFi and access cards. Therefore, the IdM system supports the management of temporary, or guest, identities.
Administrators at each faculty 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 handles the entire lifecycle, granting necessary access and ensuring timely revocation. However, implementing the new solution required us to address and permanently resolve several issues of the previous system.

Maintaining continuity after university departure

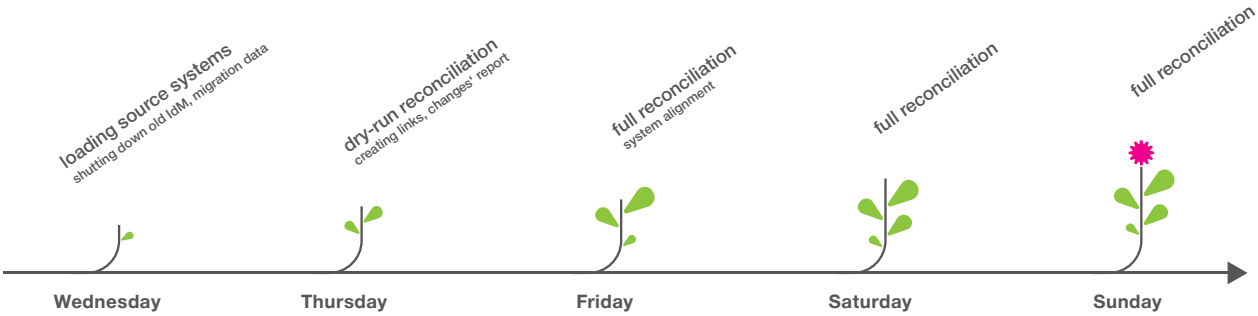
Users can continue to access certain services for a period after leaving the university, such as their university email account. We addressed this by introducing configurable grace periods. These periods are specific to different identity types and can be adjusted as needed. For each identity, a retention 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.

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 unsynchronized data.

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



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.

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)

About University of South Bohemia

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.

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

About us

We help IT departments manage identities and access, addressing one of the four critical components of organizational security. Our solutions reduce the costs associated with identity management, eliminate the stress of audit, and allow IT to focus on strategic business objectives.

With our support, you can effectively manage and secure the identities of employees, external workers, students, and customers. Our portfolio ranges from minimalistic solutions that adress immediate challenges to robust systems that fully cover all company processes.

Over the years, we have successfully completed more than 150 projects for around 50 clients, and we take pride in our long-term partnerships, many of which have lasted over 10 years.

orchitech

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