Automation transforms access management— and boosts productivity

SKB-Bank provides secure system access in minutes and allows three full-time equivalents to focus on higher-value tasks with Identity Manager

Key Facts

- **Company**
  SKB-Bank

- **Industry**
  Financial Services

- **Country**
  Russia

- **Website**
  www.skbbank.ru

Challenges

- Changes to system access took one to two days to complete

- Access management needed three full-time equivalents (FTEs)

- Manual processes risked delays in setting up, amending and deactivating user accounts

- Resetting end-user passwords could take four to five hours

Results

- Secure system access granted in five minutes rather than days

- Automatic password resets minimise disruption to staff and boost productivity

- Access rights deactivated as soon as workers leave

- Three FTEs now have time to focus on high-value projects

- Audit reports generated in minutes

Solutions

- Identity Manager

SKB-Bank wanted to overhaul access management to make the identity lifecycle process of activating, deactivating and changing access rights more efficient. Processes were largely manual, involving written requests that needed to be signed off on by line managers and IT security staff before being handed over to IT personnel to implement.

By deploying Identity Manager, SKB-Bank has aligned access control with the business's need, providing secure access to systems in five minutes. Common activities like password resets are highly automatic and the bank has moved IT staff from access management tasks to high-value IT projects. The business now has control of authorisations and access to applications.

SKB-Bank provides a wide range of financial products and services, including consumer and corporate lending, international settlement services, and project finance. Headquartered in Ekaterinburg—Russia's fourth-largest city—the bank has approximately 4,850 employees, all of whom need access to IT.

Manual processes impact performance

Business users at SKB-Bank are assigned any number of the 700-plus job roles across the bank, which require access to specific business applications. Managing access to the applications for so many people was a major challenge at SKB-Bank. During any given week, more than 300 requests for access changes would be made. These could be for new starters to gain basic access rights, existing rights to be rescinded after someone left, or when staff changed roles.

"**Access can be securely granted in just five minutes with Identity Manager. That means no more waiting around for people who join the company.**"

Denis Uleiko
Chief information Security Officer, SKB-Bank

Requests for access changes often had to be written down on paper before being signed off on by line managers and IT security personnel, and then handed to the IT team. As a result, it could be one or two days before access was granted or changes were made. This not only caused potential delays for new starters or movers, but also exposed SKB-Bank to unnecessary risk as people who had left the organisation could still have access to its systems. Plus, three full-time equivalents (FTEs) worked on manually making access adjustments. Denis Uleiko, chief information security officer at SKB-Bank, says, "We wanted to move to automation and get to a point where we could streamline the whole access management process, providing access faster and at lower cost to the company."

A simpler route to automation

SKB-Bank chose Identity Manager after reviewing multiple identity and access management (IAM) solutions on the market. "Nothing could beat Identity Manager in terms of functionality," says Uleiko. "But, ultimately, we chose the Identity Manager solution because a proof of concept revealed it was simpler to manage and easier to implement than the competition."

Access rights given in minutes

The bank has realised several quick wins by implementing Identity Manager. A major benefit is the ability to automate access management for many of its job roles. SKB-Bank has automated management for approximately 40 percent of its 700-plus roles to date. New starters gain access to their core applications automatically, and line managers use the IT Shop web portal in Identity Manager to request any additional applications a new starter may require. Uleiko says, "Access can be securely granted in just five minutes with Identity Manager. That means no more waiting around for people who join the company. They can start being productive from the morning they begin working here."

New passwords issued more efficiently through automation

Resolving requests for password resets is now a simple task. "It could take four to five hours to reset passwords before," says Uleiko, "but with Identity Manager, it's seconds. A request comes in for a new password from a line manager for an employee and it's reset straightaway with no involvement by us."

> "It could take four to five hours to reset passwords before, but with Identity Manager, **it's seconds.**"
>
> Denis Uleiko, Chief information Security Officer, SKB-Bank

No more delays deactivating accounts

Access rights are automatically withdrawn when an employee leaves the bank. Comments Uleiko, "Access management is more secure with Identity Manager because there's no chance of a delay in withdrawing access rights or the risk of the task being overlooked in a manual setup. Once a staff member is taken out of the HR system, Identity Manager updates all access rights and the person's permissions are removed."

Three FTEs saved through automation

SKB-Bank could transfer IT staff working full time on access management to other tasks thanks to Identity Manager. "I reallocated three FTEs previously working on approving access requests to new roles," says Uleiko. "They are doing more interesting work and increasing our productivity."

Auditing reports ready in minutes

SKB-Bank is saving time complying with international audits by having data on system access readily available through Identity Manager. As part of the auditing process, the bank must provide authorities with data on new starters, people who have left and IT user accounts. Uleiko says, "It took a long time to manually gather the data on employees' IT accounts in the past, but we've cut that down and, in the future, I hope to generate the necessary auditing reports in minutes with Identity Manager."

> **"I hope to generate the necessary auditing reports in minutes with Identity Manager."**
>
> Denis Uleiko, Chief information Security Officer, SKB-Bank

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential—unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com.