

Swiss Post secures identities at national scale with One Identity

Swiss Post keeps Switzerland connected. Identity Manager by One Identity keeps its access secure.



Country: **Switzerland**

Employees: **45,000**

Industry: **Postal Services**

Website: www.post.ch

Challenges

Swiss Post operates critical infrastructure across Switzerland, which makes identity security both a business and national concern. The organization faces risks from cyberattacks, supply chain vulnerabilities, fraud, and social engineering targeting its digital channels.

Internally, identity governance was also becoming difficult to manage at scale. Provisioning access rights and managing identities relied heavily on manual processes, with limited tracking and visibility. With roughly 45,000 employees, many different user types and a large application landscape, Swiss Post needed a way to bring structure, transparency, and control to access management.

Products Featured

- Identity Manager by One Identity

Solutions Featured

- Identity governance and administration

Results

- Accelerated employee onboarding and offboarding
- Reduced manual IT requests and support tickets
- Increased visibility for managers and application owners
- Strengthened security through automated approvals and access recertification

Solutions

Swiss Post implemented Identity Manager by One Identity to modernize its identity governance and administration (IGA) program. The platform gave the organization a scalable governance framework with the flexibility to handle diverse applications and user populations.

Swiss Post introduced a structured onboarding process for applications, including entitlement definition, ownership assignment, risk classification, approval workflows and yearly access recertification. This gave managers and application owners clearer visibility into who has access to what, while automation reduced manual effort and helped strengthen security and compliance.

The Story

Swiss Post is responsible for keeping Switzerland connected. As the country's national postal service, it delivers letters and parcels across the nation while also operating services in logistics and finance. With about 45,000 employees and a wide array of applications and user types to manage, securing access at scale is a huge task.

For Marco Soliva, Product Manager for identity and access management (IAM) Services at Swiss Post, finding an IGA solution that could handle that complexity was essential.

“We have a large number of applications and user types. Identity Manager allows us to manage all this variety.”

*Marco Soliva
Product Manager for identity and access
management (IAM) Service, Swiss Post*

Swiss Post chose Identity Manager by One Identity for its governance capabilities, flexibility and scalability. Those qualities were essential for an organization operating critical infrastructure, where security and compliance need to be balanced with efficiency and a seamless user experience.

Managing thousands of identities and countless access needs

Like many large organizations, Swiss Post was facing a growing number of security challenges: cyberattacks targeting critical infrastructure, supply chain vulnerabilities and fraud attempts.

Before Identity Manager, Swiss Post's identity governance processes were heavily manual and difficult to track. Provisioning access rights and managing identities required significant administrative effort, making it harder to maintain visibility and consistency across the organization.

The move to Identity Manager helped Swiss Post bring automation and visibility to those processes.

A governance model built for a complex application landscape

Today, onboarding a new application follows a defined workflow. Swiss Post works with application owners to identify entitlements and establish ownership. From there, approval workflows and recertification requirements are put in place based on risk level, ensuring access is governed appropriately from the start.

That structure has also improved visibility for business stakeholders. Application owners can easily see who has access to their systems, making it easier to maintain oversight and accountability.

Faster onboarding, fewer IT tickets, more visibility

Swiss Post has accelerated employee onboarding and offboarding, reduced the number of manual IT tickets, and improved transparency for managers and application owners. Automating approval workflows and access reviews has also helped reduce risk while supporting compliance requirements.

One area where Swiss Post has found the right balance is access recertification. Rather than overwhelming stakeholders with frequent reviews, the organization performs annual recertification checks for highly critical roles.

“If you do [recertification checks] too often, people get used to it and click it away. When we do it once a year, then they pay attention to this recertification, and I think this had been quite effective.”

From an IT service to a business enabler

Looking back on the project, Soliva says one lesson stands out above all others: define governance before automation.

“If you automate something you don’t know, then you have a mess in the end.”

He also emphasizes the importance of stakeholder engagement throughout the process. For Swiss Post, identity governance is not simply an IT function. The team learned that success comes from helping stakeholders understand the value IAM creates for the business – improving security and compliance while enabling people to do their jobs efficiently and securely.

“We explain to stakeholders what value we generate for the business: compliance and security so that stakeholders from the business can perform their business processes in a secure way”

*Marco Soliva
Swiss Post*

With Identity Manager, Swiss Post has built the governance foundation needed to manage access across a complex organization while supporting the security, compliance and operational requirements that come with delivering essential services to millions of people every day.

About One Identity

One Identity delivers trusted identity security for enterprises worldwide to protect every identity, human and non-human. With flexible deployment options and subscription terms, from self-managed to fully managed, our solutions plug directly into an organization’s identity fabric to strengthen the identity perimeter, reduce breach risk and keep governance and compliance aligned at scale. Headquartered in Cork, Ireland, and trusted by 80 of the Fortune 100, One Identity is a leading provider of integrated identity governance and administration (IGA) and privileged access management (PAM) for identity security without compromise. Learn more at www.oneidentity.com.