



SAP Customer Stories eBook

See how six organizations simplify IAM for SAP and other platforms with a certified solution from One Identity



Today, employees expect to get **access to the information they need** to do their jobs from anywhere and at any time, regardless of the target system or application.

However, this kind of seamless access requires the universal implementation of an identity and access management (IAM) solution across an organization's IT infrastructures and software platforms—which can be significantly challenging. In addition to having to speed onboarding and deprovisioning, IT departments must also standardize roles and maintain compliance with corporate and government-imposed security and privacy regulations.

Implementation of an effective IAM solution becomes even more complicated when business-critical platforms like SAP are involved. That's because SAP has its own security and access governance requirements, and it's typically managed by a dedicated team that's separate from the one responsible for the corporate IAM program.

Why struggle with IAM, especially when it comes to SAP? One Identity Manager is a comprehensive IAM solution that's certified by SAP to work seamlessly with the growing portfolio of SAP modules. With Identity Manager, you can dramatically simplify and improve user lifecycle management, governance and authentication for all your SAP implementations across production, test, development and even sandbox environments. And because Identity Manager also interoperates with cross-platform applications and hybrid architectures, you can use it as your central IAM solution to protect all your systems and data.

With One Identity, **you can:**



Use one console to manage SAP accounts across enterprise systems.



Bring all IT resources under governance by associating an SAP account with standard user corporate identities.



Scale your IAM environment to include hundreds of millions of SAP objects.



Verify and enforce SAP-optimized segregation of duties.



Deliver SAP-specialized workflows and business logic within enterprise governance.



Accelerate deployments and reduce complexity by integrating your IAM environment with SAP cloud applications using One Identity Starling Connect instead of complex interfaces.



Replace manual workflows for provisioning and other basic tasks with standardized and automated processes.



Facilitate single sign-on.

On the following pages, read how the following six organizations are improving and simplifying IAM for their IT environments that include SAP:

Table of Contents

- 4 Union Investment**
One Identity Manager and One Identity Starling Connect
- 5 Jemena**
One Identity Manager and One Identity Starling Connect
- 6 The Otto Group IT**
One Identity Manager
- 7 Swiss National Accident Insurance Fund (SUVA)**
One Identity Manager, One Identity Starling Connect and One Identity Services
- 8 Franke**
One Identity Manager and One Identity Starling Connect
- 9 BHF-Bank**
One Identity Manager and One Identity Starling Connect



Customer Profile

Company: Union Investment

Industry: Finance & Insurance

Country: Germany

Employees: 2,700

Solution: One Identity Manager and One Identity Starling Connect

Partner: iC Consult

“We chose One Identity Manager because it is flexible. You can customize your own connectors, and it delivers standard connectors to different systems like SAP.”

Dieter Fromm, Project Manager for Infrastructure Projects, Union Investment

Investing wisely in identity management

Union Investment provides same-day system access and meets tougher auditing standards with a single identity management solution

Today, Union Investment ...

increases control and insight over who has access to data about €257 billion in assets stored in systems including SAP. The company also simplifies regulatory compliance, cuts risk and speeds provisioning from up to four days to just one because it takes one minute to set up a new user profile. **Union Investment achieves this by:**



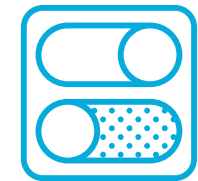
Giving the right people the right access

- Administrators create user profiles for SAP and other systems based on 360 standardized roles.
- People are granted access only to the systems and data they need to complete their work.



Enforcing the right level of control

- Administrators can see who has access to what data.
- Digital audit trails detail users' lifecycles of system access for at least 10 years.



Using the right processes

- The provisioning and deprovisioning of 10,000 Active Directory accounts are now automated processes instead of manual.
- Administrators manage access to 70 systems based on standard user profiles and employee roles.
- Compliance with national and GDPR requirements is easier.



Customer Profile

Company: Jemena

Industry: Utility

Country: Australia

Employees: 2,500

Solution: One Identity Manager and One Identity Starling Connect

“Identity Manager would talk to each system [including SAP] in whatever schema the system understood. ...Not only can we ensure that we’re compliant with Identity Manager, we can also demonstrate that compliance.”

Phil Duncanson, General Manager, IT Application Management, Jemena

Enhancing auditing and compliance automatically

Jemena in Australia mitigates access management risks with automated attestation processes

Today, Jemena ...

boosts security, increases efficiency and reduces risk associated with managing access to SAP ERP, Active Directory and 18 other business applications used by 2,000 permanent staff as well as 1,500 temporary employees whose roles frequently change. **Jemena achieves this by:**



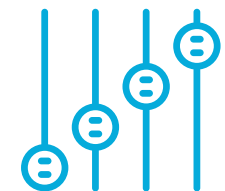
Giving the right people the right access

- Stakeholders across the organization teamed up to establish standardized roles in SAP modules and four other systems, along with standardized Active Directory group memberships.
- To ensure only authorized individuals have access to resources, the team also created 20 standard attestation policies across eight target systems including SAP.



Enforcing the right level of control

- IT staff can quickly see who has access to what data from “one version of the truth.”
- Jemena is using its identity and access management policies and roles as a foundation for wider corporate security solutions.



Using the right processes

- Jemena replaced manual provisioning, deprovisioning and attestation workflows with automated processes.
- Having IT and business stakeholders collaborate on standardizing access improves overall outcomes.

otto group

Customer Profile

Company: The Otto Group IT

Industry: Retail, Finance, Logistics

Country: Germany

Employees: 53,000

Solution: One Identity Manager

"The key objective of our IAM program was to streamline IAM workloads. We couldn't have done it without Identity Manager. The flexibility of the solution and the ease with which it can be customized means it can satisfy even the most demanding user base."

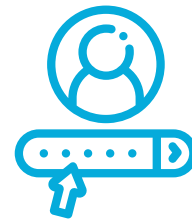
Malte Krüß, IAM Architect at Otto Group IT

Accelerating digital initiatives across 30 countries

The Otto Group IT reduces error, streamlines processes and improves security through automation with Identity Manager

Today, Otto Group IT...

has the IAM solution it needs to easily embrace new cloud technologies and further its digital transformation. By implementing a nimble identity governance and administration solution, the company boosts staff efficiency, simplifies provisioning and adds rich attestation capabilities on critical systems. **Otto Group achieves this by:**



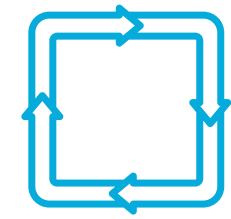
Giving the right people the right access

- With appropriately scoped approvals and an authorization paradigm, Otto Group IT streamlines and improves the user experience while reducing risk.
- Efficiently and compliantly governing access for more than 25,000 users allows the company to serve more than 70,000 IAM transactions a day.



Enforcing the right level of control

- Otto Group IT significantly reduces human error and risks associated with manual processes for onboarding, modifying and terminating users and subsidiary companies.
- The company helps ensure compliance, security and accuracy by removing IT from the process and enabling line-of-business personnel to perform attestations on their own.



Using the right processes

- Automated identity lifecycle management processes, including self-service for access requests, approval and provisioning are streamlined across all managed companies.
- Otto Group IT can now design interfaces and processes that end users embrace.



suva

Customer Profile

Company: Swiss National Accident Insurance Fund (Suva)

Industry: Insurance

Country: Switzerland

Employees: 4,200

Solution: One Identity Manager, One Identity Starling Connect and One Identity Services

“Identity Manager was the right choice. I particularly liked the availability of an SAP standard connector that would enable integration of our SAP modules.”

Sebastian Goodrick, Head of Identity and Access Management, Swiss National Accident Insurance Fund (Suva)

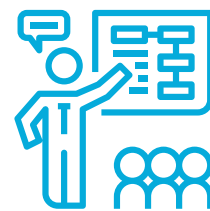
Delivering more than just protection against accidents

Swiss National Accident Insurance Fund takes the pain out of access management

Today, Suva ...

has a future-proof IAM solution that improves security and IT staff efficiency.

Suva is also lowering operating costs and projecting a complete return on investment within four years. **Suva achieves this by:**



Giving the right people the right access

- Seven hundred business roles, each with predefined access privileges, now provide a standardized framework for IAM.
- Employees' application access is based on the roles they are assigned to.



Enforcing the right level of control

- Employees' application and data access privileges are automatically provisioned and deprovisioned when changes are made in SAP.
- Security is improved because today one IT team—instead of many—controls IAM.



Using the right processes

- Suva replaced siloed IAM processes with seamless, standardized workflows facilitated by one comprehensive solution.
- IT staff can now use their standard IT development platform—Microsoft .NET—to customize Identity Manager as needed.



FRANKE

Customer Profile

Company: Franke Holding AG

Industry: Manufacturing

Country: Switzerland

Employees: 9,000

Solution: One Identity Manager and One Identity Starling Connect

Partner: Devoteam

“We now have complete control of nearly 100 percent of our user accounts of the onboarded target systems.”

**Aristeidis Matsokis,
Business Process Specialist, Franke**

Franke gains control of identity management

Global manufacturer turns challenging environment into an efficient global management system

Today, Franke ...

has improved IT security, cost savings and efficiency with its IAM solution. Provisioning and deprovisioning access to global on-premises and cloud-based systems take just 30 minutes of effort. And domain name changes involving SAP, Active Directory and other global systems take just minutes instead of weeks or months. **Franke achieves this by:**



Gives the right people the right access

- Provisioning and deprovisioning are automated based on standard roles and a consolidated view of employee and user data from disparate identity and HR systems.
- Orphaned accounts were identified and eliminated.



Enforces the right level of control

- For all employees across 66 subsidiaries, 40 countries and five continents, managers can quickly see who has access to what, along with who granted the access, when and why.



Uses the right processes

- Users access resources via single sign-on, and they reset passwords from a self-service portal.
- Managers can facilitate access changes for specific resources and individuals using a self-service portal.
- Employees and contractors can verify the appropriateness of their access privileges using a self-service portal.
- IT staff can scale Identity Manager to interoperate with any target system regardless of the API interface.

Customer Profile

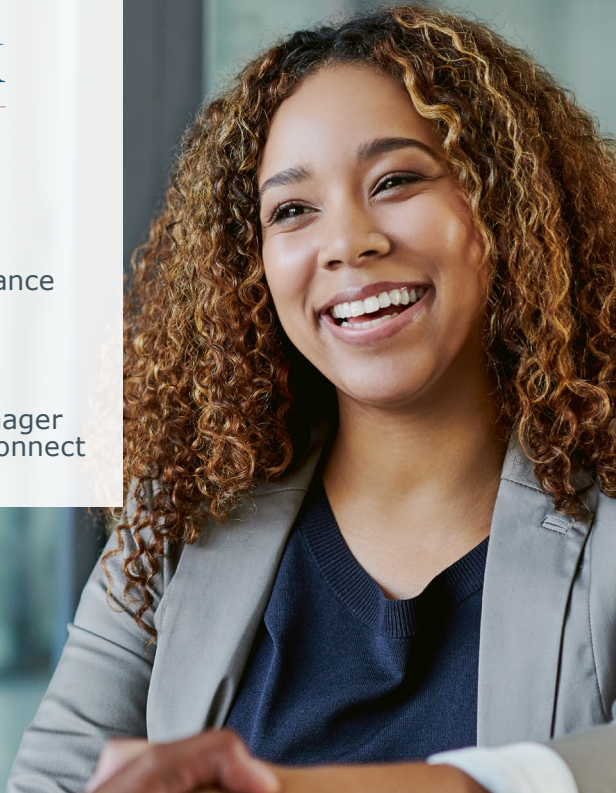
Company: BHF-BANK

Industry: Banking and Finance

Country: Germany

Employees: 1,100

Solution: One Identity Manager and One Identity Starling Connect



“We can provision users or systems up to 40 percent faster with Identity Manager thanks to its out-of-the-box functionalities.”

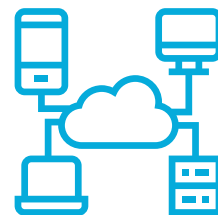
Frank Riewe, Head of Ecommerce and Web Development, BHF-BANK

German bank overcomes barriers to access management

BHF-BANK achieves 40 percent faster approval times for systems access and cuts administration time on identity management by 20 hours a week

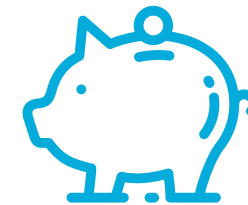
Today, BHF-BANK ...

has the IAM solution it needed to improve IT security and governance over its disparate systems that include SAP and significant numbers of proprietary applications. The company is also saving 20 hours each week in IAM management effort. **BHF-BANK achieves this by:**



Gives the right people the right access

- Thousands of internal and external users access digital resources based on standardized user profiles and roles.



Enforces the right level of control

- BHF-BANK now has a centralized IAM solution for 30 platforms including SAP systems, IBM mainframes and Oracle.
- Users visit a self-service “IT shop” to submit their own access requests—a process that takes about 30 seconds.



Uses the right processes

- Automated processes accelerate provisioning by 40 percent.
- Instead of manually creating custom user profiles for contractors in every system they need access to, IT staff use a standard temporary employee template.



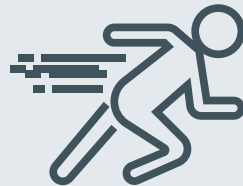
Industry experts recommend **One Identity** solutions for IAM

#GetIAMRight



Leader

Gartner February 2018 Magic Quadrant for Identity Governance and Administration



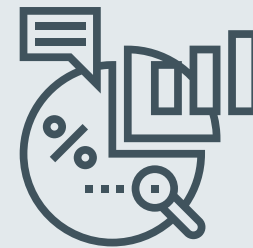
Challenger

in the Gartner Magic Quadrant for User Administration and Provisioning



Readers' Choice

Award winner for Governance, Risk and Compliance "Information Security magazine"



Comprehensive leader

and product leader in the KuppingerCole Leadership Compass for Access Management and Federation



Recommended

SAP-certified IAM solutions





[oneidentity.com](https://www.oneidentity.com)