ManageEngine
Password Manager Pro

CASE STUDY

Europe's leading international bank relies on Password Manager Pro to manage privileged access

A bank, well known for its customer-centric approach and technological adoption, deploys Password Manager Pro to replace another solution, automating password management practices across geographically disparate IT divisions.

Background

Headquartered in Amsterdam, Netherlands, a reputed private bank offers a complete suite of financial products and services across multiple business lines, including asset management, private banking, retail banking, trade and commodity finance, treasury, and structured finance. To effectively serve its clientele, spread across the European Union, the bank has set up branches, IT divisions, and representative offices in Germany, Switzerland, Turkey, and Ukraine.

The business challenge

Banking and financial institutions regularly deal with huge amounts of sensitive data, which naturally demands adoption of top-notch IT security processes. In this lucrative, but highly competitive market, keeping up customers' trust is vital for survival and growth. Even a minor security glitch or data compromise can lead to a huge hit in the stock market, skyrocketing insurance claims and, above all, loss of customer trust.

In addition to ensuring data security, banking institutions are required to adopt the latest technical advancements to enhance user experience. As evident from a recent survey by Mckinsey & Company, one in three banking customers now use mobile phones for online banking. To keep up with this emerging global trend and ensure superior customer service, this bank in the Netherlands has set up a huge IT infrastructure.

The IT infrastructure of the bank is disparate, with many servers, databases, routers, switches, firewalls, point-of-sale machines, and several other embedded systems. Apart from deploying and maintaining these devices, the IT team is tasked with ensuring the security, performance, and availability of these systems, along-side compliance with various internal and external regulations.

With IT assets and technicians spread across multiple locations, the IT division of the bank increasingly felt the need for centralized administration and control of assets. In particular, they found it difficult to control privileged access to sensitive systems in the absence of centralized management of administrative credentials.

> **We found that Password Manager Pro possessed all required features, as well as proving to be extremely easy to use. In addition, our interactions with technical support during the evaluation process revealed that we have a sound technical support team to rely on. We then decided to go with Password Manager Pro without any second thoughts.**

Facing the classic password management problem, the IT team first deployed the open-source password manager KeePass. However, other IT teams in different branches started deploying similar password management solutions. While these solutions helped them consolidate the privileged credentials in a repository, the IT team faced coordination issues. They then realized the need for an enterprise-grade solution that could serve as a corporate-wide, single, centralized repository and also take care of automating the entire life cycle of privileged password management.

"We wanted a solution that provides strong encryption, assigns and enforces usage of strong passwords through a policy, periodically rotates passwords automatically, allows secure sharing of passwords among technicians, audits all actions, and readily integrates with enterprise IT infrastructure and applications. In particular, integration with Active Directory for user provisioningand single sign-on was crucial. The online password managers we were using then did not fulfill these critical requirements," recalled the IT infrastructure administrator of the bank.

The solution

Apart from the previously listed requirements, the security division also wanted all communications to take place through a secure channel. They expected the solution not to be exposed to the internet, to possess advanced security features, offer uninterrupted access and disaster recovery provisions, and conform to their internal security standards.

With very clear and well-defined objectives, the IT team started to evaluate the top password management solutions on the market, including ManageEngine Password Manager Pro. After a series of rigorous evaluations and internal testing phases, the team decided to deploy Password Manager Pro.

"We found that Password Manager Pro possessed all required features, as well as proving to be extremely easy to use. In addition, our interactions with technical support during the evaluation process revealed that we have a sound technical support team to rely on. We then decided to go with Password Manager Pro without any second thoughts," said the IT system administrator of the bank.

> **"All access to IT assets—applications that contain sensitive data-is now being closely and constantly monitored. With the session recording provisions in Password Manager Pro, we are now able to track all the operations performed on our critical assets."**

The Password Manager Pro difference

The IT team was able to deploy the solution to production within a couple of days. The ability to integrate with Active Directory helped the team to complete user provisioning in less than an hour. They deployed the primary server in the Netherlands and the secondary in Germany, with constant data replication between the two.

With the solution up and running on their premises, the team started making the best use of the product's rich feature set. The following are some of the features proving to be useful for the bank:

- The ability to designate individual technicians as password administrators, and allow them to add and share passwords with other technicians and end-users, which helps streamline the account consolidation process.
- A provision to restrict access to passwords based on job roles, which helps establish tight access controls.
- Remote password synchronization to help assign strong, unique passwords for IT resources.
- Request-release workflows, which help enforce an additional layer of control over sensitive passwords.
- A single sign-on mechanism, which helps with seamless authentication and automated user provisioning and de-provisioning processes.
- The option to store personal passwords and have user-level encryption keys.
- The option to launch secure and reliable Windows RDP, SSH, and Telnet sessions directly from a browser.

> **"Administrative passwords that grant unlimited access privileges to IT assets are now totally protected. Technicians get access to passwords only on a need-to-know basis."**

- Instant email notifications and comprehensive auditing to help track who has access to what IT assets.
- High-availability architecture that provides uninterrupted access to administrative passwords for users who are geographically separated (across the Netherlands and Germany).
- Scheduled and live data backup for disaster recovery.
- Integration with RSA SecurID, which serves as the second level of authentication.

> **"Password Manager Pro has undoubtedly enhanced the security of our IT infrastructure. We are very pleased and look forward to deriving full benefits."**

The IT division of the bank now feels that Password Manager Pro has helped take IT security to the next level. "Administrative passwords that grant unlimited access privileges to IT assets are now totally protected. Technicians get access to passwords only on a need-to-know basis," the IT system administrator of the bank pointed out.

"All access to IT assets—applications that contain sensitive data—is now being closely and constantly monitored. With the session recording provisions in Password Manager Pro, we are now able to track all the operations performed on our critical assets. Password Manager Pro has undoubtedly enhanced the security of our IT infrastructure. We are very pleased and look forward to deriving full benefits," declared the IT system administrator.

Before Password Manager Pro	After Password Manager Pro
No provision to periodically change passwords on critical systems.	Provision to automatically change passwords based on policy.
Insecure sharing practices that could lead to security issues.	Secure and fully-controlled sharing practices.
Lack of proper records on who has access to what systems and applications.	Comprehensive audit trails and session recordings of entire privileged accesses.
Lack of centralized control and coordination between teams that are geographically distant.	Centralized control and effortless coordination.
Lack of high availability and disaster recovery provisions.	High-availability architecture, even between locations that are geographically distant. Live backups of data.

About Password Manager Pro

Password Manager Pro is a comprehensive privileged account management solution, which helps enterprises secure sensitive accounts, the keys to privileged resources by enforcing password management best practices such as centralized password storage, use of strong passwords, regular password resets, and controlling user access to shared passwords across your organization. For more information, or to try it out, check out https://passwordmanagerpro.com

About ManageEngine

As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget. ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our 90+ products and free tools cover everything your IT needs, at prices you can afford. From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimize your IT. For more information, visit www.manageengine.com

ManageEngine

Zoho Corporation
4141 Hacienda Drive, Pleasanton,
CA 94588, USA
Phone: +1-925-924-9500
Email: sales@manageengine.com