



CASE STUDY

Switzerland's Most Trusted Media Voice Streamlines Password Management Using Securden

With Securden, Radio Fribourg SA has eliminated the complexity of fragmented password management. Teams collaborate more efficiently, access systems securely, and operate with improved productivity and peace of mind.



INDUSTRY
Media & Broadcasting

LOCATED
Switzerland

Quick facts

REQUIREMENT

- Centralized, encrypted credential storage to replace scattered spreadsheets
- Granular, role-based access controls for internal and external users
- Automated password generation and rotation
- Comprehensive audit logging for compliance
- Time-limited, workflow-based access for external vendors and freelancers
- Secure remote access for distributed teams

THE SOLUTION

Securden Password Vault for Enterprises

RESULTS

- Eliminated fragmented password management and informal sharing
- Enhanced security, accountability, and compliance
- Improved operational efficiency and collaboration
- Reduced risk of unauthorized access with temporary, monitored permissions
- Quick adoption and positive user experience across teams



The Background

Founded in 1988 and headquartered in Villars-sur-Glâne, Radio Fribourg SA stands as one of Switzerland's most respected and influential media organizations. Renowned for its unwavering commitment to credibility and independence, Radio Fribourg serves as a vital voice for the Fribourg region, offering high-quality radio and television broadcasting in both French and German. Its bilingual programming not only reflects the region's unique cultural heritage but also fosters inclusivity and dialogue among diverse audiences.

The organization is also at the forefront of media innovation, actively collaborating with partners such as MediaParc SA and MediaPub SA to create a dynamic hub for creative exchange and technological advancement. With a daily reach of over 155,000 listeners, Radio Fribourg continues to set the standard for excellence, trust, and forward-thinking in Swiss media.

The Business Challenge

For a technology-driven media house like Radio Fribourg SA, every credential—whether for a playout server, CMS, signage controller, or podcast

platform—is vital to seamless operations. The station's intricate IT ecosystem underpins a diverse range of core systems, including audio playout automation, visual signage controls, and financial and content management platforms.

For operational efficiency, credentials for these systems were managed in local Excel spreadsheets and shared within departments. While this approach facilitated day-to-day workflows, it did not include access controls or audit trails, making it challenging to track who accessed which systems and when. Role-based access was handled informally, so team members with access to these spreadsheets could log into various systems, including those with administrator privileges.

This setup highlighted an opportunity to further enhance security and accountability as the organization continued to grow and modernize.

The IT team observed that identical passwords were often used across both internal and external user accounts, including service accounts for critical systems such as the CMS, FTP, and streaming servers. In addition, usernames and passwords were sometimes hard coded into display firmware and scheduling software, leading to password reuse across multiple platforms.

This approach to credential management introduced potential security risks, such as increased exposure to

cyber threats and the possibility of internal misuse or credential leaks. As Laurent Meuwly explains:

“Our approach to password management created challenges in maintaining security and oversight. When unauthorized access attempts occurred or unusual activity was detected, the absence of centralized control and comprehensive logging made it difficult to identify the source of the issue or to quickly revoke compromised credentials.”

LAURENT MEUWLY, IT MANAGER, RADIOFR.

In addition to internal teams, external vendors and freelancers needed access to different systems for tasks such as maintenance, content collaboration, or platform development. However, without an established approval workflow or controlled access privileges, this external access was primarily unmanaged and lacked oversight.

“Without access permissions or time-limited credentials, contractors retained access long after their contracts were up, creating a persistent security risk for us,”

LAURENT MEUWLY, IT MANAGER, RADIOFR.

To fix above hiccups, the Swiss media entity sought a password management solution that would offer role-based access control, centralized credential management, secure storage, and time-limited access for external users. By deploying a password manager, the station aimed at bolstering IT security and gaining adherence to compliance standards.

Identifying The Right Solution

When Radio Fribourg began overhauling their password management methods, they evaluated multiple password manager offerings. Some of the prominent players they reviewed include Psono,

1Password, Dashlane, NordPass, and Pass Securium. Scalability, ease of use, and security were some cornerstone principles they were after.

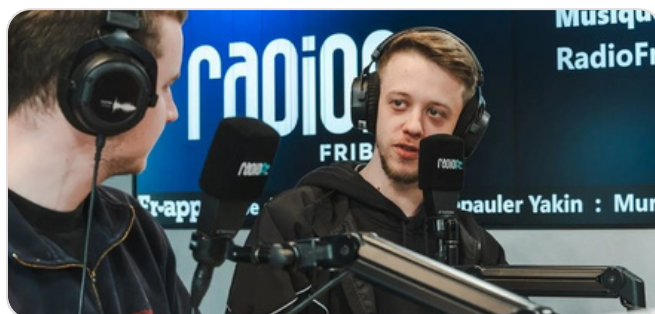
Further, they were looking for an intuitive interface that would be deemed attractive to both their IT and non-IT users. Say for instance, Nordpass fell short when it came to group management functionality. And Psono had inadequate user experience, ultimately retarding its organization-wide adoption.

“The solutions we evaluated provided isolated solutions, missing the bigger picture. While they focused just on storing and sharing passwords, our IT team was looking for a comprehensive package that included robust group management features”

LAURENT MEUWLY, IT MANAGER, RADIOFR.

Securden emerged as a strong contender for Radio Fribourg SA as it offered exceptional group management functionality. They were able to segment access rights based on roles and responsibilities. Sensitive credentials were being shared with other team members while simultaneously enforcing stricter control over who could access what.

Also, the user interface of Securden was simple and straightforward without infusing the need for extensive training. They easily scaled the solution to teams beyond IT.



Every playout, CMS and signage credential now sits behind one vault.

Below is a set of targeted solutions Radio Fribourg SA was looking for within Securden:

- ✓ **Centralized, Encrypted Vault:** Secure and encrypted storage of all credentials to eliminate the risks of scattered and informal management.
- ✓ **Granular Role-Based Access:** Assign permissions precisely based on roles and responsibilities. Ensure users and external collaborators only access what they need, when they need it.
- ✓ **Automated Password Generation and Rotation:** Enforce strong and unique passwords and automated rotation to remove the dangers of weak or reused credentials.
- ✓ **Comprehensive Audit Logging:** Log every access event to gain full visibility and traceability for compliance.
- ✓ **Time-Limited and Workflow-Based Access:** Provide time-limited access to external vendors and freelancers. Ensure automated expiry and approval workflows to close the door on lingering risks.
- ✓ **Secure Remote Access:** Enable teams and remote contributors across multiple locations to safely connect to sensitive platforms and systems.

“Setting up Securden was a breeze, thanks to the thorough documentation and quick support we received. It has streamlined the entire password lifecycle—creation, rotation, and deletion—greatly reducing manual work and the chances of making mistakes. Users have adjusted their habits and now feel comfortable creating unique passwords for every platform. The quick and responsive support we received further ensured a smooth and hassle-free transition,”

LAURENT MEUWLY, IT MANAGER, RADIOFR.

The Results



By implementing Securden Password Vault, Radio Fribourg SA achieved a secure and efficient password management system perfectly aligned with its complex,

IT infrastructure. The centralized vault now safeguards all critical credentials—from playout servers and CMS platforms to signage controllers and podcast systems—ensuring that passwords are no longer scattered or shared informally.

Role-based access controls provide precise, need-to-know permissions for each team member and external contributor, with time-limited access for contractors, significantly reducing security risks.

Automated password generation and enforced rotation have strengthened overall credential hygiene, eliminating weak or reused passwords embedded in essential systems.

Comprehensive audit trails deliver full visibility into access events, empowering the IT team to monitor usage, quickly detect anomalies, and maintain accountability across multiple sites and remote users.

Moreover, external partners and freelancers now request access for specific projects and timeframes, with each request moving through a structured approval process. Access is only enabled for the approved duration, after which it is promptly withdrawn, leaving no lingering permissions behind.

This ensures that third-party access is always temporary and purpose-driven, sharply reducing the risk of unauthorized entry.

Automated workflows not only streamline approvals but also guarantee that every access is justified and monitored.

This streamlined approach enhances operational efficiency while supporting Radio Fribourg SA's bilingual broadcasting and growing digital portfolio with robust security and compliance.

155,000+

DAILY LISTENERS

1988

BROADCASTING SINCE

2

LANGUAGES ON AIR

0

LINGERING CONTRACTOR
ACCESS



“

Our experience with Securden has been really positive overall. The team mainly uses Securden's access rights management features, which take away the stress of dealing with complicated passwords. One of the standout benefits is the user-friendly interface, which was a big factor in choosing Securden over other options. Plus, the ability to organize password storage into groups and automatically share passwords with group members has really boosted collaboration in our department.

LAURENT MEUWLY, IT MANAGER, RADIOFR.



About Securden



Securden is a leading provider of privileged access governance solutions that holistically combines the principle of least privilege with other critical security principles such as zero-trust and provide visibility into privileged activities to continuously monitor cyber risk to effectively prevent cyberattacks, malware & ransomware propagation, and insider exploitation.

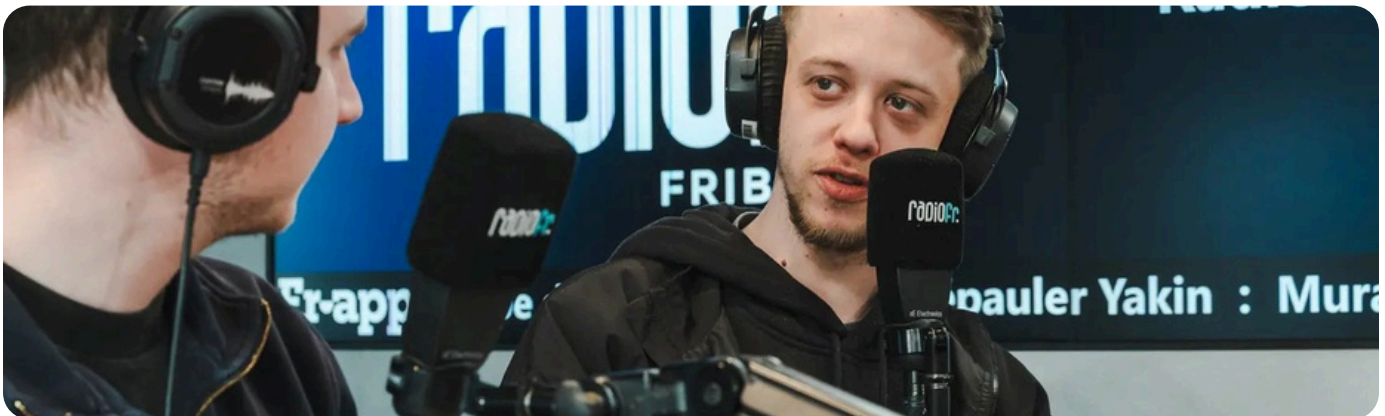
With simplicity and robustness in its core design, Securden offers a refreshing and intuitive panel of controls to govern privileged access across cloud, physical, and virtual environments. Here is a quick list of Securden's offerings:

- Password Vault for Enterprises
- Endpoint Privilege Manager
- Unified PAM

- Vendor PAM
- UnifiedPAM for MSPs
- Password Self-Service
- Secure Remote Access

The products have been built to be extremely scalable and secure. Securden is trusted by small businesses and large enterprises such as large banking and financial services, manufacturing companies,

government agencies, healthcare organizations, managed IT service providers, educational institutions, and security service provider. To learn more, visit www.securden.com



Enforce tight password security without slowing down operations

Try Securden Password Vault for Enterprises.

[REQUEST A DEMO](#)