© Gianni Camilleri

identiT

SECURING THE GATEWAY: MODERNIZING ACCESS AT PORT OF ANTWERP-BRUGES

REFERENCE CASE

TABLE OF CONTENTS

1. CHARTING A NEW COURSE: TRANSFORMING ACCESS MANAGEMENT AT THE PORT OF ANTWERP-BRUGES

Port of Antwerp-Bruges, one of Europe's largest and busiest ports, faced critical challenges with its legacy Access Management (AM) infrastructure. Their solution, Oracle Access Manager, lacked support for modern authentication standards such as OpenID Connect (OIDC), and a choice of Multi-Factor Authentication (MFA) solutions. Beyond its technical limitations, the platform offered an unclear roadmap for future enhancements, making it incompatible with the port's ambition to adopt Infrastructure as Code, enable federation with external identity providers, and design flexible, user-friendly authentication journeys.

IdentIT successfully delivered a comprehensive transformation to a modern Access Manager platform over four years. This ambitious project addressed several key objectives:

Advanced Security

Implementing modern authentication standards such as OpenID Connect and intelligent MFA, significantly enhancing the overall security posture while avoiding user inconvenience.

Seamless Migration

Transitioning from Oracle Access Manager to the new Access Manager with minimal disruption to end-users through carefully designed authentication journeys and a "blue-green" migration approach".

Integration of Legacy Applications

Utilizing reverse proxy logic and custom scripting to effectively integrate legacy applications into the modern AM environment, ensuring a unified Single Sign-On (SSO) experience.

Infrastructure Automation

Leveraging Infrastructure as Code (IaC) with Ansible and AWX, IdentIT dramatically reduced environment setup times, minimized human errors, and enabled rapid, secure deployments.

Enhanced Monitoring and Logging

Introducing robust centralized system monitoring through Grafana and Prometheus, alongside comprehensive audit logging via the ELK stack, significantly improved real-time visibility and enabled proactive incident prevention and faster resolution.

User Integration Amidst Mergers

To support the transition during the merger of Port of Antwerp and Port of Bruges, we implemented interim solutions that allowed the Access Management system to work seamlessly with both Active Directories. This approach ensured operational continuity and minimal disruption while Port of Antwerp-Bruges led the successful unification of the underlying directory infrastructure.

The project delivered measurable and impactful results, including significantly enhanced operational efficiency, robust security improvements, reduced operational costs, and an elevated user experience. Creative solutions, such as custom authentication scripting and advanced persistent cookie logic, overcame initial limitations within the new platform, demonstrating IdentIT's capability to innovate proactively.

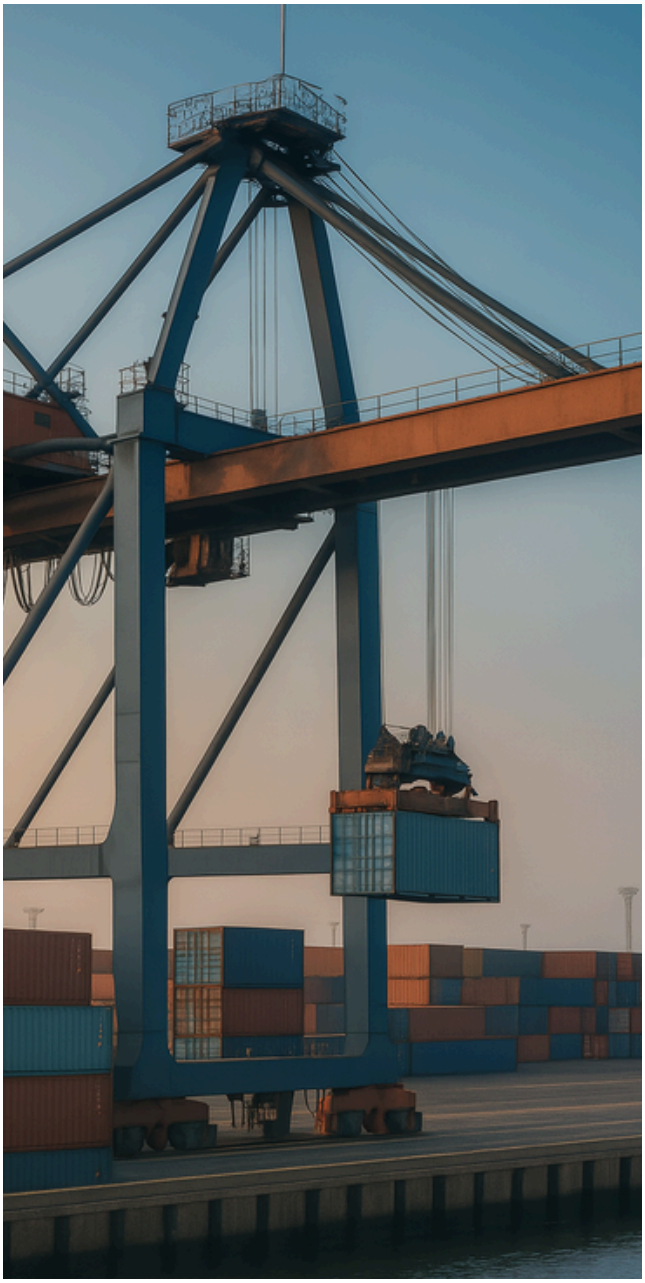
Moving forward, Port of Antwerp-Bruges's AM infrastructure is scalable, adaptable, and demonstrably resilient—successfully withstanding annual datacenter failover tests without impacting components of the new Access Management platform. This ensures continued secure, efficient, and user-friendly access management, even under adverse conditions.

Ultimately, establishing a single digital gateway significantly streamlined access management, enhancing both security oversight and governance. Furthermore, the robust DevOps pipeline and automation substantially accelerated the safe deployment of new features and updates from test to production, supporting continuous innovation and operational agility.

2. IMPLEMENTATION IN ACTION: PHASES OF MODERNIZATION

Proof of Concept (PoC) to Minimum Viable Product (MVP)

Initially, a targeted Proof of Concept was executed to validate the Access Manager solution, rapidly transitioning into a Minimum Viable Product due to its successful demonstration of immediate value. Early success boosted stakeholder confidence and clearly set the project's trajectory.



User Datastore Migration

A crucial phase was migrating user data from Oracle LDAP to a new directory server, also LDAP based. Using custom-developed Python scripts, IdentIT executed a highly efficient "blue-green" migration strategy, ensuring a no-downtime rollover by introducing a brief user data freeze during the migration. This approach, combined with robust rollback capabilities, safeguarded business continuity.

To ensure a smooth and reversible migration, IdentIT adopted a blue-green strategy—a deliberate choice to mitigate risk. This approach allowed the old and new environments to run side-by-side, making it possible to switch back if needed without disrupting users.

During the actual user migration, a brief freeze was introduced in the legacy Oracle system to prevent any data changes. At that moment, IdentIT exported the user data and transformed it via a custom Python script into the new AM solution format. This carefully orchestrated window ensured data integrity and business continuity while minimizing downtime.

Legacy Integration & Authentication

Legacy Systems Integration

To accommodate numerous legacy applications not natively supporting modern authentication protocols, Web Agents were employed effectively. These agents enabled comprehensive Single Sign-On (SSO) integration, with specific legacy applications gradually upgraded to support SAML and OIDC, further consolidating and modernizing the AM ecosystem.

MFA & Advanced Authentication

Implementing Multi-Factor Authentication (MFA) was central to enhancing security without compromising user experience. IdentIT initially offered email-based MFA and Authenticator apps (Google and Microsoft Authenticator). Intelligent authentication logic and persistent cookies were integrated, intelligently determining MFA requirements based on context, dramatically reducing user fatigue while still preserving security posture.

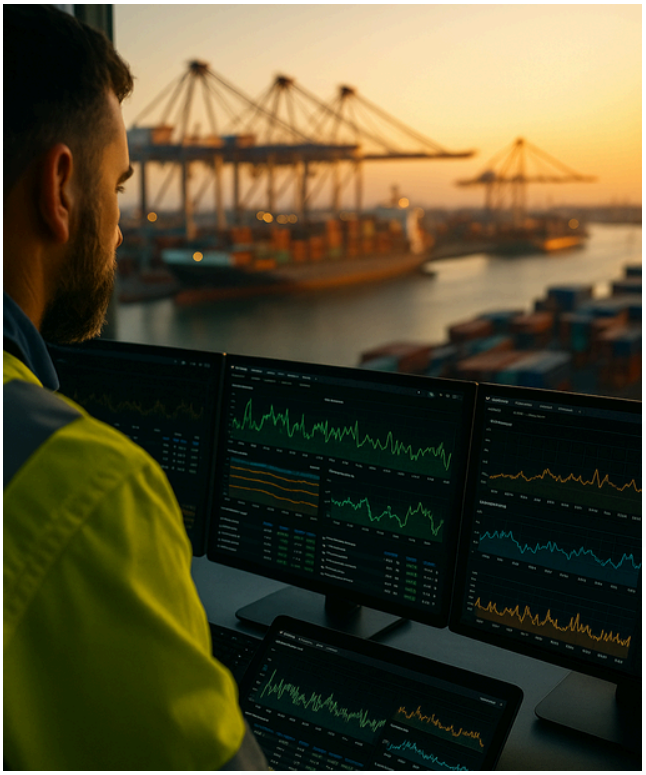
By consolidating multiple authentication points into a single digital gateway, we significantly enhanced security management and oversight. The unified gateway provided centralized authentication and authorization policies, enabling stronger security governance and compliance.

"We proactively addressed MFA fatigue by implementing context-based policies and persistent cookies, significantly enhancing user experience without compromising security."

Automation & Infrastructure as Code

Central to project agility and reliability was the use of automation through Ansible and AWX for Infrastructure as Code (IaC). By combining Port of Antwerp-Bruges's existing Ansible roles—for server provisioning and firewall configuration—with IdentIT's custom roles for configuring the platform's stack, we enabled streamlined full-stack deployments. This collaboration significantly accelerated deployment cycles and minimized human error.

Leveraging this robust automation within the DevOps pipeline streamlined and secured transitions from test to production environments, dramatically reducing deployment time and associated risks.



Monitoring & Logging Improvements

Enhanced monitoring was established through Grafana dashboards combined with Prometheus endpoints provided by the AM solution, enabling real-time visibility into system performance and behavior. This configuration provided unprecedented visibility, real-time anomaly alerts, and facilitated swift incident resolution, significantly improving overall system resilience. While a centralized ELK stack for logging was initially implemented, the logging strategy is currently being revisited to better align with evolving operational needs.

"During a virtual switch failure impacting storage, our real-time monitoring provided immediate alerts, allowing swift response and prevention of broader system issues."

Ports of Antwerp and Bruges Integration

IdentIT managed the complexity introduced by the merger between Port of Antwerp and Port of Bruges through a carefully phased integration strategy. Initially, separate authentication realms were established within the platform to support both user directories, ensuring operational continuity during the transition. Once the directories were unified into a single Active Directory, authentication flows were streamlined across all applications. This not only reduced integration complexity per application, but also significantly improved the reliability of Joiner-Mover-Leaver (JML) processes—ensuring consistent and secure user lifecycle management. Thanks to modular Ansible code, updates and changes could be rolled out efficiently across both environments without duplicating effort, paving the way for long-term maintainability.

External User Authentication Improvements

External user authentication, involving employees from third-party companies, saw substantial security enhancements. Authentication journeys were standardized to include MFA, while initial pilots with federated identity providers, such as Azure, successfully demonstrated secure, federated authentication capabilities. This laid the foundation for broader adoption and user-friendly authentication experiences for external users.

3 TANGIBLE OUTCOMES: EFFICIENCY, SECURITY, AND EXPERIENCE

The transformation at Port of Antwerp-Bruges delivered significant, measurable improvements across multiple dimensions. By modernizing the AM infrastructure and streamlining authentication processes, we achieved notable gains in operational efficiency, strengthened security posture, and dramatically enhanced the user experience. Below, we highlight key outcomes demonstrating the practical impact of this strategic initiative.

Enhanced Security

Prior to the migration, Port of Antwerp-Bruges faced limitations including the absence of robust real-time monitoring and insufficient authentication security. The implementation of the new platform delivered:

- Advanced Multi-Factor Authentication (MFA) with context-based triggers.
- Centralized monitoring using Grafana and Prometheus, coupled with detailed audit logging via the ELK stack, enhanced the team's ability to swiftly detect, respond to, and resolve incidents, greatly improving overall system reliability.
- Improved overall security posture and resilience against threats.

These enhancements also contributed to improved compliance with key regulatory frameworks. For instance, the combination of real-time monitoring, access control, and audit logging supports the technical measures outlined in NIS2 Article 21, which requires essential infrastructure operators—such as major ports—to implement appropriate and proportionate cybersecurity controls. Additionally, sector-specific obligations around identity verification, traceability, and secure access in port environments are easier to fulfil with centralized governance and reliable MFA mechanisms in place.

Operational Efficiency

The extensive use of Infrastructure as Code (IaC) and automation through Ansible and AWX has delivered significant measurable outcomes:

- Deployment Automation: Reduced AM environment setup time from hours to approximately twenty minutes.
- Operational Support Efficiency: Decrease in support tickets related to password resets, access issues, and manual configuration errors.
- Cost Reduction: Significant reduction in manual operational tasks, minimizing resource allocation and lowering operational costs.

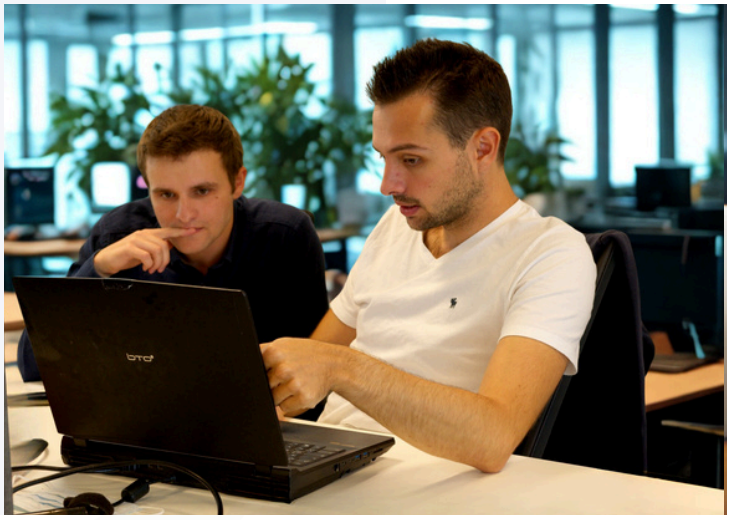
User Experience

Intelligent MFA logic significantly enhanced user satisfaction by reducing authentication fatigue, while still achieving strong security posture:

- Context-aware MFA significantly reduced the number of times users had to authenticate.
- Persistent cookies allowed streamlined, secure user sessions, further minimizing disruptions and providing a frictionless user experience.
- Positive feedback from users indicating higher satisfaction and productivity due to smoother authentication processes.

4. KEY CHALLENGES AND TAILORED SOLUTIONS

Throughout the project, IdentIT encountered a number of technical and operational challenges—some related to the platform, others stemming from organizational complexity. Each was addressed with custom-fit solutions designed to ensure long-term maintainability, scalability, and security.



Persistent Cookie Security

Challenge: The default persistent cookie functionality of the platform lacked crucial validation and security features, posing potential security risks.

Solution: IdentIT implemented custom scripts and authentication nodes to enhance security. These included cookie invalidation triggers tied to password changes, account locks, or account deletions, as well as conditional IP and device checks to ensure cookie authenticity and security.

Cross-domain Single Sign-On (SSO)

Challenge: The platform initially lacked sufficient documentation and capabilities to easily handle complex cross-domain authentication scenarios, complicating seamless user experience across different domain environments.

Solution: Leveraging custom scripting and the strategic deployment of Web Agents, IdentIT successfully resolved these complex SSO scenarios, enabling secure and seamless access across multiple domains.

OAuth Client Configuration Limitations

Challenge: Initially, the platform's OAuth configurations lacked granular client-level customizations, complicating the management of diverse OAuth client settings.

Solution: With the platform's later enhancements (OAuth provider overrides and advanced property fields), extensive custom scripting was significantly reduced, allowing precise, per-client OAuth configuration adjustments and streamlined client management.

Data Hygiene During Merger Integration

Challenge: During the integration of user directories following the merger with the Port of Bruges, data quality issues delayed progress. Inconsistent or incomplete user records made it difficult to unify authentication flows.

Solution: IdentIT built flexible, multi-realm support into their Ansible automation and gave POA the time and space to clean and consolidate their Active Directory. Once unified, integration was seamless—and far more sustainable.

These tailored solutions effectively addressed specific limitations, enhancing the overall functionality and flexibility of the AM solution.

"The platform's enhancements, especially in federation capabilities and authentication customization, allowed us to overcome initial platform limitations effectively."

5. NAVIGATING FORWARD
SECURING A FUTURE-PROOF AM INFRASTRUCTURE

The AM transformation at Port of Antwerp-Bruges delivered extensive operational, security, and user experience improvements. Automation and Infrastructure as Code significantly streamlined processes, reducing deployment times and operational errors. Enhanced security measures, including intelligent MFA and comprehensive real-time monitoring, elevated the port's security posture. We addressed technical obstacles through tailored solutions, resulting in a robust, scalable AM infrastructure prepared to meet future requirements.

Next Steps for Continuous Improvements

Looking forward, Port of Antwerp-Bruges aims to further refine its AM infrastructure by expanding federated authentication capabilities, notably with additional external identity providers. Ongoing optimization of automation workflows and continual enhancement of monitoring and alerting systems are planned. Additionally, proactive training and enablement for Port of Antwerp-Bruges's internal teams will ensure sustainable management and adaptation of the AM solution to future operational and technological needs.

GLOSSARY OF TECHNICAL TERMS

- Ansible: An open-source automation tool that allows IT administrators to configure systems, deploy software, and orchestrate advanced IT tasks using simple scripts.
- Web Agent: A component used to integrate legacy web applications with modern authentication frameworks, enabling secure access management.
- Blue-Green Migration: A strategy involving running two identical production environments (Blue and Green), allowing safe and quick migrations or updates by switching traffic seamlessly between them.
- ELK Stack (Elasticsearch, Logstash, Kibana): A centralized logging system used for collecting, analyzing, and visualizing log data in real-time.
- Grafana: A data visualization and monitoring tool used to display real-time metrics and generate alerts from diverse data sources.
- IaC (Infrastructure as Code): The practice of managing and provisioning computing infrastructure through machine-readable definition files, improving consistency and reliability.
- LDAP (Lightweight Directory Access Protocol): A protocol used to access and maintain distributed directory information services over an IP network.
- MFA (Multi-Factor Authentication): An authentication method requiring users to present multiple verification factors to gain access to a system, enhancing security.
- OAuth (Open Authorization): An open-standard authorization framework allowing secure, limited access to user resources without sharing credentials.
- OIDC (OpenID Connect): A modern authentication protocol enabling secure identity verification based on OAuth 2.0 standards, widely used for single sign-on (SSO).
- Persistent Cookie: A browser cookie that remains on a user's device for an extended period, allowing users to remain authenticated across multiple sessions without repeatedly logging in.
- Single Sign-On (SSO): An authentication process enabling users to securely authenticate with multiple applications and services using just one set of credentials.
- Web Agents: Software components integrated into web servers to enforce access management policies, crucial for integrating legacy systems into modern AM solutions.