

HID Solves Global Identity Management Challenges for Financial Services Company



“Physical identity and access management (PIAM) deployments are increasing due to technology and product development, compliance mandates, a greater desire to manage alternative user populations such as on-premises visitors and contractors, and a sharp emphasis on timely and secure access.”
- Gartner ¹

¹ Gartner Research; *Physical Identity and Access Management*; Feb 2012

Solution:

- HID SAFE™ Enterprise

Our client is an American multinational financial services corporation that facilitates electronic funds transfers throughout the world. They have about 13,000 identities (employee and non-employee) across 80 office locations in 40 countries, and were managing these identities using multiple locally-maintained access control systems.

Challenges

When the use of these multiple disparate access control systems and devices became increasingly complicated, our client resorted to manual processes to automate access provisioning. Not only were their processes inefficient, but they also increased their risk exposure. A change was necessary to improve their situation, so they began their search for a new solution to manage their physical security infrastructure. The challenges and limitations faced by our client's situation were leveraged to identify key requirements needed to manage their physical identities and access, which included:

Interoperability of Authoritative and Security Systems

Our client's security team lacked a consolidated view into the physical security infrastructure of the organization, resulting from a lack of standardized global policies, reporting, planning processes, common documentation and tools to protect people, information and the facility in offices across their many global locations. A centralized, interoperable system would be required to manage the scope of their identities and physical access requirements.

Common System Architecture and Design

The complication described above was aggravated due to the employment of several identity-based systems, each containing multiple stakeholders. These systems store data for the same person but – due to lack of proper integration – data exchange happens through manual interactions. These solutions also had limited or no integration with authoritative and logical security systems. As a result, there were huge operational inefficiencies, delays and a high state of risk to potential security exceptions. To blunt these risks, future-focused integration capabilities would be required.

Managing Access Lifecycles for Multiple Stakeholders

Our client has multiple stakeholders (employees, visitors, contractors) who access the premises, and each person holds a varying risk profile and access requirement. Due to the manual nature of our client's access control operation, the entire process of onboarding, performing background checks, provisioning access, and off-boarding was slow, error-ridden and costly. Automation would be necessary to improve operating costs and increasing efficiency.

Common Notification and Escalation Procedures

Our client's approval lifecycle was manual and paper-based; therefore, it was extremely difficult to track the access-related activities. For instance, if an approver was not available, the identity had to wait multiple days to get access. To solve this problem, they would need standardized criteria for escalation, activation and communications.

Compliance with Industry Standards and Regulations

Our client's physical security systems managed identity, credential and access data but lacked the capability to automate the policies and processes for managing personal and property security. This required extensive manual intervention by the physical security team which caused delays and manual errors as well as a high level of effort from the team. Our client was looking for a 100% automated environment for reporting and assurance in accordance with government/industry compliance standards.

THE SOLUTION

The challenges mentioned above are exactly the issues that HID's SAFE solution solves best. Our client selected the HID SAFE™ Enterprise solution to provide their organization with a comprehensive view of their physical access operations and automate their existing processes associated with access and identity lifecycle management, resulting in faster processing times and better audit controls.

Integration and Interoperability of the Siloed Physical Security System

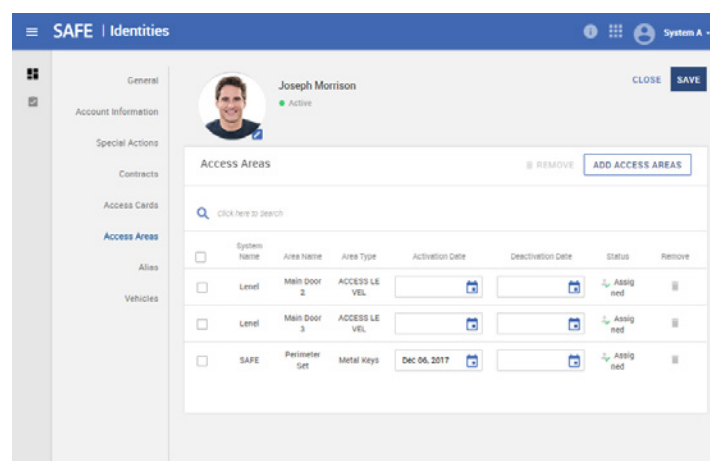
HID's SAFE Enterprise solution provides ready-to-use connectors (agents) which integrate with the external disparate Physical Access Control Systems (PACS) present at our client's sites (CCURE and Picture Perfect) and the authoritative Human Resource Management System (HRMS) to provide a common centralized security platform. With the ability to communicate across devices and systems, HID SAFE delivers our client a unified comprehensive view of security and provides seamless processing of identity information from the PACS to HID SAFE.

Automation of the Entire Physical Identity Lifecycle Management

HID SAFE Enterprise enabled our client's security managers to create and automate standard security processes and policies to grant, manage, revoke and provision physical security identities and access privileges across international sites/PACS.

Tracking Every Visitor with HID SAFE Visitor Manager

HID SAFE Visitor Manager provided our client with web-based, policy-driven software to securely manage visitors by automating different processes throughout the access lifecycle. HID SAFE Visitor Manager manages the visitor pre- registration, background checks, check-ins, badging and check-outs. It provides a highly efficient visitor management process and the ability to track and report every visitor's activity.



HID's SAFE solution has replaced our client's manual processes associated with automated on/off-boarding employees, visitors and contractors, card issuance, access assignments and provisioning access control, so new personnel can be operational in minutes. SAFE's improvement in efficiency ensures a 90% reduction in the card management process and abandons manual processes for identity-management – saving our client a huge sum in annual operation costs.

To summarize, the overall benefits of our financial services client utilizing SAFE Software from HID are:

- **Safer Premises:** SAFE provides a centralized administration of the entire access management process. Our client's security team now has a comprehensive unified view of their entire physical operation. This ensures that unwanted identities are not able to access organization premises.
- **Enhanced Operational Efficiencies:** With SAFE providing system interoperability and automation of the otherwise manual tasks, the physical access processes such as access approvals are completed within minutes, without delay – improving operational efficiencies.
- **Substantial Reduction in Operation Costs:** SAFE reduced manual interventions such as paper-based request forms, and it automated reports so that security and business units can analyze data quickly and, in turn, make informed business decisions. This has increased efficiency and significantly lowered processing times.
- **Auditing and Compliance:** SAFE delivered a 100% automated environment for Reporting and Assurance in accordance with government/industry compliance standards.
- **Comprehensive Reporting:** SAFE provides security managers with robust and full-featured reporting capabilities that can support workflow-embedded, scheduled and ad hoc reporting of identity and physical access events and activities. Configurable reports and dashboards promote efficient and appropriate operational decisions to better manage threats. Reports may also be sent to SAFE users based on events/triggers or on defined scheduling as delegated in the policy engine.

© 2018 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, and HID SAFE are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2018-08-02-cc-iams-hid-safe-nam-financial-srvcs-cs-en
PLT-04013