



Securing the Future

WITH PHYSICAL IDENTITY AND ACCESS MANAGEMENT

CONTENTS

- 03** Introduction
- 04** Physical Identity and Access Management:
Bridging the stakeholder gap
- 05** Physical Identity and Access Management:
Why it matters
- 06** HID Global's HID SAFE Enterprise:
Next-generation security
- 07** HID SAFE Enterprise: Features
- 08** What does HID SAFE Enterprise mean
for your organization?
- 10** Conclusion



INTRODUCTION

Identity—the data and information you have about a person that help to establish who the person is, their role in the organization and level of trust.

Today's organizations are tasked with managing the physical identities of not only their workforce but a range of third parties including contractors, vendors, customers and visitors.

Managing multiple identity types can be frustrating. Typically, identity data is kept in disparate systems, making it necessary to manage identities and their physical access manually, often by different teams (e.g. employees and contractors, security departments, general managers).

In the absence of an automated, integrated approach, these teams often duplicate each other's processes, leading to operations that are highly inefficient, while increasing the probability of errors and additional risks and liabilities. What's more, changing regulations and policies hinder an organization's efforts to remain compliant.

Additionally, risk landscapes are changing faster than ever. As security threats present themselves in new ways—increasing the risk to customers, employees and the general public—organizations struggle to predict future risks. In response to this changing landscape, the need for physical access and identity management systems is increasing exponentially.



A SURVEY OF IT LEADERS SHOWS KEY IDENTITY CHALLENGES FACED TODAY



said physical access is enforced manually, which makes it vulnerable to human error¹



said integration between physical and logical security systems could improve¹



said that when an employee or contractor is terminated, they're not certain their identity and access are removed properly¹

PHYSICAL ACCESS AND IDENTITY MANAGEMENT: STAKEHOLDERS

Physical Identity and Access Management (PIAM) breaks down traditional organizational silos to transform communities of stakeholders involved in identity management such as employees and contractors, security departments and process managers in HR, IT, Facilities, Reception, Contractor Administration, etc.

STAKEHOLDERS	RESPONSIBLE FOR
Employees and Contractors	On/Off-boarding Badging Approvals
Security Department	Access requests Visitor pre-registration
Managers: HR & IT Facilities Line managers	Visitor management Area owners Contract owners Delegate

PIAM

Empowers employees, contractors or tenants to handle their common security needs

Connects disparate systems together, providing control of physical identity and access management functions

Enables stakeholders within your organization to own and manage their security functions





PHYSICAL ACCESS AND IDENTITY MANAGEMENT: WHY IT MATTERS

In addition to automating key processes and simplifying the control of all physical identities across an organization, PIAM helps to:



Reduce costs by leveraging existing physical/IT infrastructure and automating manual processes that reduce errors.



Minimize risk by vetting and authorizing identities based on role, location and other organizational policies.



Ensure compliance with regulatory and security requirements through real-time reporting.



Foster customer centricity by automating security business processes; helping customers initiate and track their own requests.

PIAM enables organizations to centrally manage the lifecycle of identities such as permanent and temporary employees, contractors and visitors. Ultimately, it ensures synchronized and compliant on/off-boarding of identities; decreasing the likelihood of a security risk while lowering operational costs.

HID GLOBAL'S HID SAFE™ ENTERPRISE: NEXT-GENERATION SECURITY

HID Global's HID SAFE™ Enterprise is a web-based solution that allows organizations to manage the lifecycle of identities and their authorization for physical access. It is a highly scalable platform that automates key processes and simplifies control of all identities—employees, contractors, vendors and visitors—across an organization to ensure each identity has the right access, to the right areas, for the right length of time.

By adopting a unified approach to physical security management, HID SAFE Enterprise seamlessly manages identities, their physical access and their correlation with physical security events in a multi-stakeholder environment while providing real-time compliance.

KEY BENEFITS:



Reduce operating costs by automating identity/access management



Centralize physical access control of all identities across disparate physical access control systems (PACS)



Minimize risk around manually enforcing provisioning policies



Reduce delays in on/off-boarding identities and their physical access in PACS



Demonstrate compliance with regulations such as Sarbanes-Oxley



Gain useful analytics and reporting with regular updates

HID SAFE™ ENTERPRISE: FEATURES

HID SAFE Enterprise provides a comprehensive range of features, including:



Centrally manages all types of identities of interest to physical security, i.e. permanent and temporary employees, contractors, visitors and vendors.



Allows users to **create virtual zones of related access levels** across disparate systems and locations.



Provides a central location to **search and assign access levels to an identity** across disparate systems.



Access profile feature allows users to **automate assigning of physical access using common conditions**, i.e. role-/location-based access.



The urgent termination feature **allows authorized personnel to immediately terminate physical access**, avoiding delays of terminations by HR personnel.



Complete audit trail of all transactions executed within the system and between SAFE and external systems.



Allows users to create spatial hierarchy of locations (sites), the underlying buildings, floors and the associated areas for **better access management**.



Pre-defined reports on physical identities and their access, including identities by type and status access.





WHAT DOES HID SAFE™ ENTERPRISE MEAN FOR YOUR ORGANIZATION?

HID SAFE Enterprise by HID Global takes risk management and mitigation far beyond the capabilities of traditional access control systems.



Reduced Costs: HID SAFE Enterprise provides immediate operating cost reduction by leveraging existing physical/IT infrastructure to automate manual processes that reduce errors.



Mitigated Risks: A centralized platform with policy-based workflows closes loopholes, forces accountability through logs and enforces identity access based on role and location, as well as organizational and regulatory policies.



Demonstrable Compliance: Logs who has access to what, when, and why; logs can be formatted and scheduled based on regulatory requirements.



Advanced Analytics: Robust reporting informs security teams of activity in on-boarding and badging access manager and visitor manager. It includes status, activity monitoring, diagnostics, and compliance.



Predictive Security: Logs are leveraged with predictive analytic techniques to transform security data into critical knowledge and actionable insights called IOCs; enabling organizations to take preventive action against possible threats.



Customer Centricity: HID SAFE Enterprise supports stakeholders by automating many of the security business processes that help internal customers initiate and track their own requests.

WHAT DOES HID SAFE™ ENTERPRISE MEAN FOR YOUR ORGANIZATION?

HID SAFE Enterprise brings siloed areas together to streamline major identity management tasks like on-boarding and badging, visitor management, access management and compliance.



CONCLUSION

HID Global's HID SAFE™ Enterprise is an ideal choice for effective, off-the-shelf physical identity and access management. It enables busy organizations to connect disparate physical security, IT and operational systems; automate manual security processes; and reduce both costs and risks.

Organizations of all types, across Fortune 100, financial, government and real estate vertical markets, have turned their investment in HID SAFE Enterprise into a strong and sustainable ROI.

Key benefits of HID SAFE Enterprise



Cost: Immediate operating cost reduction by manual processes that reduce errors.



Risk Mitigation: Enables the proper vetting and authorizing of identities based on role, location and other organizational policies.



Regulatory Compliance: Process and approval automation provides consistent policy management.

Learn more about
HID SAFE™ Solutions





© 2019 HID Global, Incorporated. All rights reserved. HID Global and the HID Global logo are registered trademarks of HID Global Incorporated in the United States and/or other countries. Product modules are subject to change and some modules cannot be purchased independently; please contact your sales representative for more information. All other trademarks are the property of their respective owners.
2019-06-12-hid-safe-enterprise-eb-en PLT-04023

Sources:

1. Based on an IDG Research Services survey of 101 IT security leaders at organizations with 1,000 or more employees

