

# Physical and Logical Access Convergence with Oracle Identity Manager

*An Oracle White Paper*  
*October 2006*

**NOTE:**

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

# Physical and Logical Access Convergence with Oracle Identity Manager

Note.....	2
Introduction .....	4
Converging physical and logical access management.....	5
Physical access control systems .....	5
Oracle Identity Manager .....	5
Convergence use cases.....	6
Employee on-boarding .....	6
Role-based access control.....	7
Self-service and delegated administration .....	8
Employee access termination.....	8
Attestation.....	9
Case study.....	10
Components of the solution .....	10
Expected integration benefits .....	10
Conclusion.....	11

# Physical and Logical Access Convergence with Oracle Identity Manager

## INTRODUCTION

While IT security professionals have long appreciated the importance of physical security for IT resources, today there is growing interest in leveraging IT infrastructures in the delivery of physical security solutions. This concept is often referred to as physical and IT convergence, which the Alliance for Enterprise Security Risk Management (AESRM) defines as

*[the integration of] physical security devices for access control, monitoring and process control into the IT infrastructure.<sup>1</sup>*

Benefits cited by proponents of convergence include reduced operational costs, increased efficiencies, better use of technology investments and improved security. Convergence is a hot topic among security professionals today, and organizations such as the Open Security Exchange (<http://www.opensecurityexchange.com/>) and ASIS International (<http://www.asisonline.org/>) are actively supporting development and adoption of convergence strategies.

This paper describes a convergence approach involving the integration of physical access control systems with identity management solutions, specifically Oracle Identity Manager. This integration centralizes the management of access controls to both physical and logical (i.e., IT application-based) resources for users across the organization. This should be of particular interest to US government agencies subject to the HSPD-12 mandate to establish “a mandatory, Government-wide standard for secure and reliable forms of identification,” which are to be used for access control to secure federal facilities and information resources.<sup>2</sup> Other industries are facing similar pressures for increased accountability for security policies and processes related to physical and logical access control.

Oracle Identity Manager integrates with physical access control systems through connector technologies to provide centralized provisioning and privilege management, effecting what is referred to in this paper as the converged identity

**The converged identity environment is a solution for centrally managing user identities and access privileges across the physical and IT domains.**

---

<sup>1</sup> The Alliance for Enterprise Security Risk Management (AESRM), “Convergent Security Risks in Physical Security Systems and IT Infrastructures,” 2006.

<sup>2</sup> White House press release (<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>)

environment. Use cases and benefits of the converged identity environment as well as a customer case study are described.

## **CONVERGING PHYSICAL AND LOGICAL ACCESS MANAGEMENT**

When describing the convergence of physical and logical access management there are two domains to consider. Physical access management deals with the management of *cardholder* identities, and the rights of cardholders to enter specific buildings, floors, rooms, etc. Logical access management deals with the management of *user* identities, and the various application accounts, network accounts, and access privileges associated with these users.

In most large organizations, best practice for physical access management involves deployment of a physical access control system, and best practice for logical access management involves deployment of an enterprise identity management and account provisioning solution. This section describes each, and approaches for connecting the two to provide a converged identity environment.

### **Physical access control systems**

Physical access control systems are used by organizations' security departments to protect facilities. They provide a means of controlling access to secured locations by automatically granting access to cardholders who are authorized to enter a specified location. Physical access control systems can be integrated with other systems providing credential management, badging, video surveillance, alarm monitoring, and biometric enrollment. Leading physical access control vendors and products include Honeywell's Pro-Watch, Lenel's OnGuard, and Software House's C•CURE.

Most physical access control systems deployed today are managed independently of the organization's IT function. Physical access control systems which do leverage the corporate IT infrastructure often do so in a superficial way, for example, by using TCP/IP for communication with an administrative console. Typically, there is no commonality of the user identity managed in the physical access control system and the digital identities associated with the various applications deployed in the enterprise.

### **Oracle Identity Manager**

Oracle Identity Manager, a component of Oracle Identity Management, is a solution for managing users' identities, credentials, and access to resources throughout the enterprise. Oracle Identity Manager achieves this by automating the business processes associated with managing account creation, access privileges, credentials, and resource responsibilities. Oracle Identity Manager provides administrative and self-service interfaces for managing identities and requesting resource privileges, an integrated, rule-driven workflow capability and pre-configured connectors for supporting resources such as e-mail systems, enterprise applications and remote access networks. Also included is a facility called the

**Today, most organizations manage cardholders in their physical access control systems and users of their IT systems independently.**

Adapter Factory, which automates the development and maintenance of customized connectors.

**Oracle Identity Manager is an enterprise user identity management and provisioning solution that integrates with a wide variety of applications. By integrating Oracle Identity Manager with physical access control systems, sites can implement the converged identity environment.**

Oracle Identity Management is deployed today by a number of large enterprises to manage access to a wide variety of enterprise applications. Through connector technology, Oracle Identity Manager can also manage the identities maintained in a physical access control system. Identities managed can include those of the administrative users (the security administrators who interact with the physical access control system through the application console), as well as the cardholders (the subjects of the physical access control system). This integration allows organizations to implement centralized, policy-based user administration across the physical and logical domains, effecting what is referred to in this paper as the converged identity environment.

## **CONVERGENCE USE CASES**

**The benefits of the converged identity environment can be understood by examining some use cases.**

A few use cases for integration of physical access controls and enterprise identity management serve to illustrate the benefits of the converged identity environment. The use cases examined include employee on-boarding, role-based access control implementation, self-service and delegated administration, employee access termination, and attestation of employee authorizations.

### **Employee on-boarding**

Employee on-boarding is often referred to as the “day one” problem. In order to do their jobs, employees typically require physical access to the facilities as well as secure access to a variety of enterprise and departmental applications such as e-mail, e-business applications and network remote access. Access provisioning across these systems needs to be coordinated throughout the new employment process, and errors or delays can result in reduced productivity.

Information about the employee is typically entered into the HR system during the pre-employment process. This includes identity information such as the employee’s name, department, job title, and manager. In the converged identity environment, this information can be sourced by Oracle Identity Manager and used to generate a cardholder record in the physical access control system. On the first day of work, the employee visits the badging office where a security administrator collects the additional information required to generate an identity card (badge) for that employee. This might include a photograph or collection of biometric information. Selected information collected during badging can then be recorded in Oracle Identity Manager where it can be used to trigger further automated account provisioning events.

**The converged identity environment automates the on-boarding of new employees.**

In this example, the converged identity environment provides a number of benefits to the employee on-boarding process. These include:

- Less work for the security staff, and less of an opportunity for errors such as misspellings to creep into the on-boarding process because identity information is automatically imported into the physical access control system.
- Coordination of physical security and IT events during the hiring process, ensuring that user accounts are created exactly when they are needed.
- Streamlined on-boarding of new employees, allowing them to “hit the ground running” with their accounts, credentials and access privileges in place.

### **Role-based access control**

Role-based access control (RBAC) is a method for controlling access entitlements through role memberships. In IT systems, role memberships are most commonly represented by group memberships. The chief advantage of the RBAC approach in practical application is that it allows administrators to grant and manage a default set of privileges across a population of users with similar access needs.

**Integrating physical access control with identity management can help organizations leverage their RBAC strategies.**

The converged identity environment makes it possible to manage role-based entitlements across the physical and logical access space. For example, organizational roles may be reflected in Oracle Identity Manager. Employee membership in roles may be driven by a number of sources such as the employee’s department and office location as reflected in the HR system. By applying business rules, Oracle Identity Manager automatically translates role memberships into application privileges and provisions the user for the necessary accounts and application-specific access control lists. In the same way, Oracle Identity Manager can also translate these roles into a discrete set of physical access privileges maintained in the physical access control system. As a result, if an employee changes departments and relocates to a different floor of a facility, his access privileges can be automatically updated in the physical access control system to grant him card-based access to that floor. This would be accomplished simply by updating the employee’s role membership in the identity management system. Another example might be the relocation of an entire department to a new floor of a facility. In this case, administrators can update the physical access privileges for all department members simply by changing the set of physical access privileges granted to that group in the identity management system.

Advantages of leveraging the converged identity environment to implement role-based access control include:

- Ability to leverage business roles to automate the provisioning of new users with an initial set of physical and logical access privileges.
- Ability to quickly grant and revoke users’ access to areas of the facility based on their role memberships as managed in the identity management system.

- Ease of managing entitlements such as access to buildings, floors or security zones for a collection of users.

### **Self-service and delegated administration**

Oracle Identity Manager implements self-service and delegated administration to facilitate user identity management. Self-service administration provides end users with an intuitive application interface for managing aspects of their identity profiles, viewing current accounts and entitlements, and requesting access to resources. Delegated administration provides a mechanism for administrators to designate selected users as administrators of collections of users, thus allowing administrative activities to scale across large, dispersed user populations.

The self-service and delegated administration features of Oracle Identity Manager can be leveraged in the converged identity environment. When an employee uses these interfaces to submit a request, it can travel through a rule-driven approval process based on his job level, department, functional manager, etc. For example, an employee may require access to an off-site facility for a temporary assignment. In most organizations today, this need would be addressed through a manual process involving e-mails or telephone calls to the appropriate security administrator. Leveraging identity convergence, however, allows the employee to request physical access privileges through the same familiar self-service administration interface he uses to manage account access privileges. The request may need to be approved by his manager, the manager responsible for the floor, and a security administrator. This approval process is automated and mediated by Oracle Identity Manager. Once the employee's request has traveled through the process, if approved, his updated privileges are automatically reflected in the physical access control system.

**Self-service and delegated administration capabilities help organizations more effectively manage employees' physical access privileges.**

As demonstrated here, benefits of using self-service and delegated administration to manage physical access privileges in the converged identity environment include:

- Enforcement of a defined process for requesting and granting access to facilities across the enterprise, with tracking and auditing capabilities.
- Automatic granting of access in the physical access control system once the necessary approvals have been granted.
- Quicker and easier access for employees to physical facilities who have a legitimate business need.

### **Employee access termination**

There are circumstances when administrators may need to quickly revoke or suspend a user's access privileges to an organization's resources. This can happen in termination situations, or in the case of a compromised credential. Implementing the converged identity environment with identity management makes it possible to respond to these needs immediately across both the physical and logical domains.

**Rapid response to events such as employee terminations and lost credentials is crucial. In the converged identity environment, access can be suspended immediately across the physical and logical security domains.**

For example, an employee who retained her badge on termination might continue to have access to the facility for hours or even days while this information was processed and updated in the physical access control system. Such processing delays represent a potential security vulnerability. Another example where rapid suspension of a user's access privileges might be necessary occurs in organizations using smartcard credentials for both physical and logical access. In this case, loss of a card can provide an unscrupulous person with the means to not just enter the facility but also access the company's IT resources. Integration of the physical access control system with identity management allows organizations to respond to these events immediately, suspending physical access and IT account access, with a single action.

Benefits of being able to rapidly suspend a user's physical and IT account access through the converged identity environment include:

- Reduced overhead on the part of the security administrators in responding to events such as employee terminations and lost user credentials.
- Improved security through immediate response across the physical and logical domains to events such as employee terminations or lost credentials.

### **Attestation**

Attestation is a process by which managers and resource owners periodically verify the access rights and privileges of users. Attestation processes are typically defined and implemented to support requirements such as regulatory compliance. Oracle Identity Manager supports periodic and automated attestation processes. For example, managers can periodically receive notifications to review the list of accounts and resources granted to a direct report. If an employee no longer reports to that manager, she can refer the review and approval to another manager. The entire process happens according to a pre-determined schedule and is tracked and auditable.

**Implementing attestation in the converged identity environment establishes accountability over physical access rights and prevents privilege creep.**

The converged identity environment permits these automated attestation processes to be applied to physical resources such as facility, floor or door access. For example, managers can periodically receive a notification to review and approve a list of the areas of a facility to which their reports have access. This addresses the problem of "privilege creep" that occurs when users retain access rights to areas of the facility they no longer need, and can be useful in satisfying regulatory compliance requirements.

Benefits of leveraging the converged identity environment to implement attestation for the physical access environment include:

- A traceable, auditable means of verifying periodic physical access approvals.
- Avoidance of employee privilege creep where employees retain access to areas of the facility indefinitely.

- Potentially improved compliance with regulatory and internal audit requirements.

## CASE STUDY

A leading global investment banking, securities and investment management firm integrated their Oracle Identity Manager deployment with their Honeywell ProWatch physical access control system with the aid of their implementation partner, SENA Systems.

A leading global investment banking, securities and investment management firm wanted an integrated solution for controlling access to a variety of enterprise applications as well as to their facilities. Their requirement was for a centralized, authoritative and auditable solution for all infrastructure accounts, physical assets and technology applications to better meet internal policy and external regulatory requirements. Other goals of the project were reducing administrative labor costs via increasing end user self-service functionality, and implementing a flexible and extensible account provisioning solution that allowed for continued growth with the organization.

### Components of the solution

SENA Systems (<http://www.senasystems.com/>) is an Identity and Access Management (I&AM) focused consulting organization providing the full spectrum of services to enable customers to plan, assess, select, implement and integrate complete I&AM projects. With a record of successful delivery of over 150 I&AM engagements with Fortune 500 companies, SENA offers services to its clients in the Americas and Europe and has a Development Center based in Pune India.

The company deployed an identity management and physical access integration solution with their implementation partner, SENA Systems. The solution consisted of Oracle Identity Manager, preconfigured and custom connectors to various enterprise IT systems, and a custom connectivity solution for the firm's Honeywell ProWatch physical access control system. This project was implemented in two stages. In stage one, simple connectivity was deployed to allow administrators to disable door access through the identity management system. Stage two implemented further integration with the physical access control system, allowing automatic provisioning of users to the physical access control system and dynamic control of physical access privileges.

SENA Systems leveraged the Adapter Factory, a feature of Oracle Identity Manager, to implement the Honeywell ProWatch connector. The Adapter Factory is a Java code generator coupled with a graphical user interface that provides an environment for rapid deployment and automatic maintenance of custom application connectors, therefore reducing the costs of deployment and maintenance of a provisioning solution. Application engineers from SENA Systems worked closely with Honeywell engineers to develop the connector.

### Expected integration benefits

The financial services firm expects to realize a number of benefits from integrating its physical access control systems into their Oracle Identity Manager deployment. These include:

- Reduced security risks through the immediate removal of user access from physical access to facilities and logical access to core IT resources.
- Automation of user access rights management with minimal manual intervention.

- Who-has-what reporting capability across infrastructure targets, including Microsoft Active Directory and Exchange, RSA ACE/Servers, Honeywell ProWatch, CA-ACF2 mainframe environments and Kerberos servers.
- Ability to leverage automation to clean up incorrect and outdated identity data as part of the deployment process.

Ultimately these benefits are expected to translate into improved security with lower overall operational costs.

## CONCLUSION

Organizations today are under increasing pressures to improve control over their physical and logical security environments. Motivations for this include the desire to improve overall security, mandates to reduce operational costs and improve efficiencies, and the need to comply with regulations and directives such as HSPD-12. Physical and IT convergence seeks to deliver these benefits by integrating physical security devices into the IT infrastructure.

Oracle Identity Manager supports the deployment of convergent solutions through connector-based integration with physical access control systems. This provides a converged identity environment where there is a single point of administration for physical and logical identities throughout the organization. Benefits of the converged identity environment include improved compliance, enhanced security and improved process efficiencies. Customers are leveraging Oracle Identity Manager to implement convergence solutions today.

**Oracle Identity Management's best-in-class suite of IdM solutions delivers the industry's only hot-pluggable middleware, allowing enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources both within and beyond the firewall. Find out more about Oracle Identity Management at <http://www.oracle.com/identity/>.**



Physical and Logical Access Convergence with Oracle Identity Manager  
October 2006  
Author: Michael P. Mesaros

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.

Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
[oracle.com](http://oracle.com)

Copyright © 2006, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.