

This document is for informational purposes. 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 in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

ORACLE®
FUSION MIDDLEWARE **11g**


ORACLE®

Introduction to Identity and Access Management

Mark Wilcox

Product Manager, Directory Services

March 2010



How would you define Identity and Access Management?

What is Identity and Access Management?

- Tools and processes for managing user identities, credentials and privileges

Why Should I Care?

- Make your employees and customers more productive and happy by making sure they don't waste time dealing with forgotten passwords and have proper access to the tools and services they are entitled to
- Maintain compliance with regulation
- Ensure operational security – in particular remove the danger of access from people who no longer work for you

The 50,000 Foot View

- Centralized Credential Service
- Centralized Identity Attribute Service
- Centralized Group (Role) Service
- Web Single Sign-On
- Desktop Single Sign-On (Enterprise SSO)
- User Self-Service
- Account Reconciliation
- User Management (Provisioning)
- Access Management

The 30,000 Foot View

- LDAP – Standard protocol for credentials, user and group/role
 - Typically deployed as a mix of storage and virtualization
 - Virtualization lets you take advantage of data managed in database-based systems like HR
- Web-SSO
 - SAML is standard but primarily still reserved for “inter-domains”
 - Multiple vendors maintain proprietary SSO systems
- Desktop SSO
 - Software that Auto-fill username/password forms under central management
 - Kerberos/Windows Native Authentication

The 30,000 Foot View Cont.

- **User Self-Service**
 - Enable password reset, update
 - Enable users and supervisors to manage access
- **Account Reconciliation**
 - Map actual access with expected access
 - Manage orphan/rogue accounts
- **User Management (Provisioning)**
 - Manage user access via triggers such as HR status change
 - Supports workflow including management approvals
 - Can support non-IT resources like mobile phones or office space

The 30,000 Foot View Cont.

- Access Management
 - Coarse Grained – Only employees can see this website
 - Fine-Grained – Only an employ's manager can click this button
 - Risk management – deny access based on abnormal behavior (e.g. someone trying to move money from an account from a foreign IP address)
 - Adjust authentication type based on application requirement - email (username/password), salary (require one-time password)

Managing Audit Report

- Many regulations (SOX, HIPPA, etc) require audits for compliance
- At least - user management system should support attestation reports and orphan accounts
- Ideal – integrated audit system that can integrate with common report generators

Cloud – IDM the Next Generation

- More and more services will be accessed via external Web applications
 - Google Apps, Oracle CRM onDemand, Line of Business Specialists (e.g. restaurant supply management)
- Make sure partner supports SAML or at very least ability to import LDAP data
- Do not forget to include these systems into audit reports

Who should use IDM?

- Everyone performs IDM
- Small – can utilize native tools in the OS
- Large – leverage vendors to use tools and expertise to insure compliance and improve efficiency
- As you grow – add the tools that help accomplish your business or meet compliance



Question and Answers

Conclusion

- Everyone does identity management
- As you grow – importance of management increases to keep people productive, protect the network and maintain compliance
- Take advantage of existing software instead of trying to roll your own