Security Intelligence.
Think Integrated.

IBM Security Identity Manager

Introduction for Technical Sales

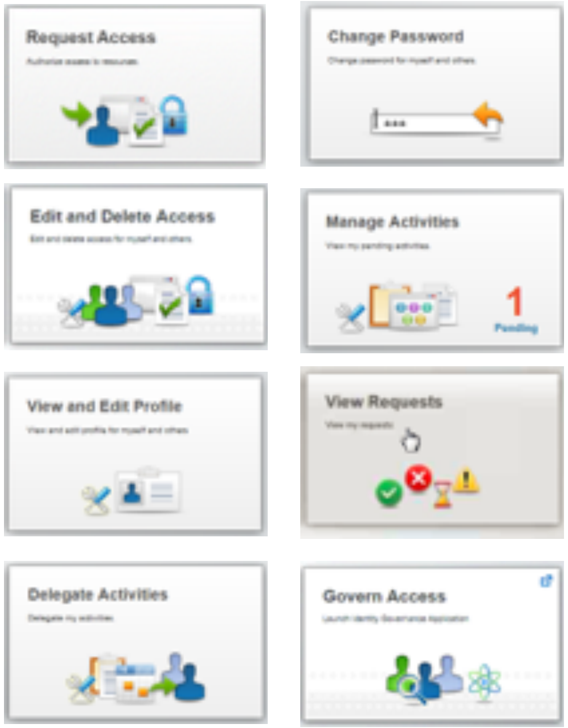
Agenda

- Identity Management update
- Privileged Identity Management update
- Functional Overview
- Market and Licensing Information

Security Identity Manager

IBM Security Identity Manager simplifies deployment and improves user experience

IBM Security Identity Manager



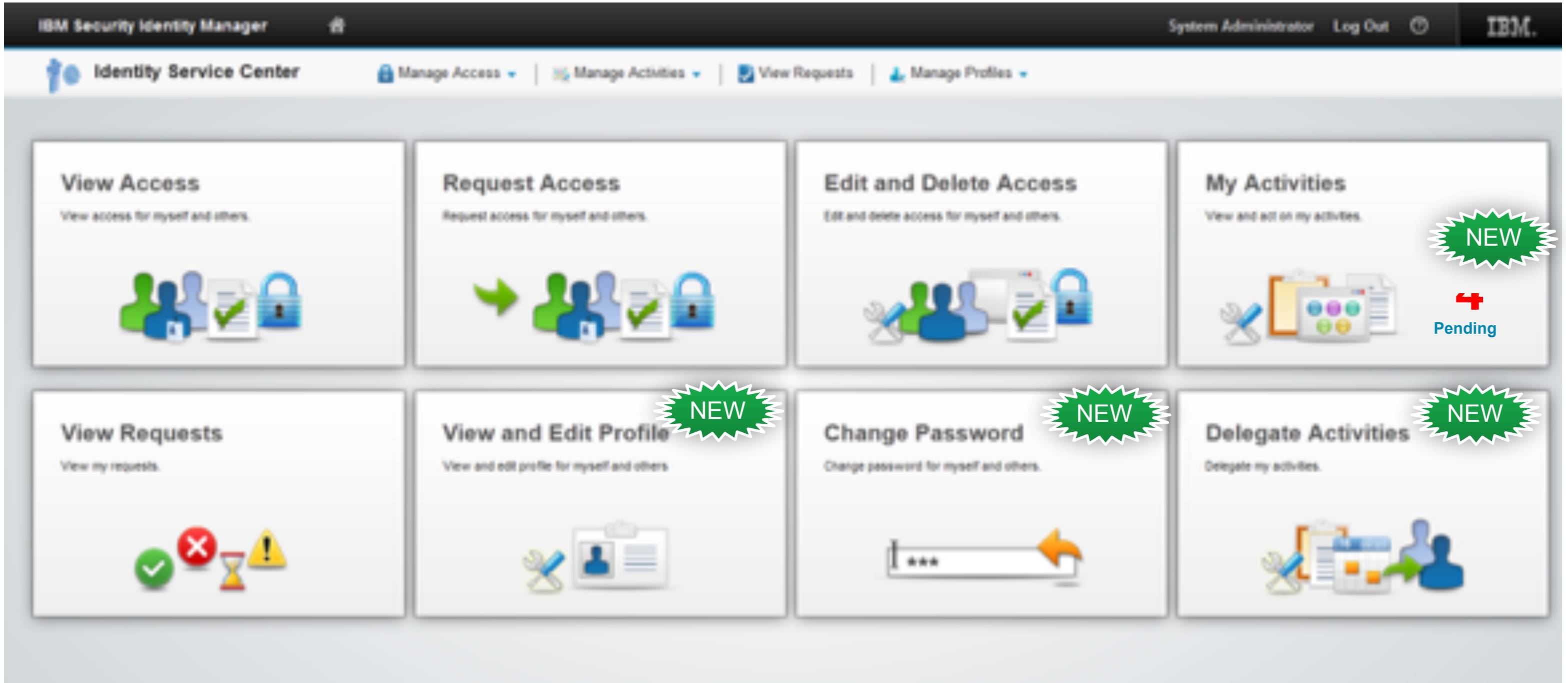
Request Access
Authorize access to resources
Change Password
Change password for myself and others
Edit and Delete Access
Edit and delete access for myself and others
Manage Activities
View my pending activities
1
Pending
View and Edit Profile
View and edit profile for myself and others
View Requests
View my requests
Delegate Activities
Delegate my activities
Govern Access
Launch Identity Governance Application

NEW!

Security Identity Manager (SIM) Release Highlights

- V6.0.0.6 (software install) and V7.0.0.2 (virtual appliance)
- Improved Identity Service Center user interface for business managers and end users
  - New: Self-Service Password Management
  - New: Self-Service Profile Management
  - New: Delegation support
  - Updated: pending Activities alert
- Updated: Virtual appliance enhancements
- Customizations: RESTful APIs to streamline UI extensions for additional use cases
- Customer sponsored enhancements; adapter updates; platform updates

Identity Service Center – Home screen - updated



View Access

View access for myself and others.

Request Access

Request access for myself and others.

Edit and Delete Access

Edit and delete access for myself and others.

My Activities

View and act on my activities.

NEW

Pending

View Requests

View my requests.

View and Edit Profile

View and edit profile for myself and others

NEW

Change Password

Change password for myself and others.

NEW

Delegate Activities

Delegate my activities.

NEW

SIM V7.0.0.2 Virtual Appliance (VA) updates

- SNMP alerts for VA status
- Updated VA platform (“Mesa”)
  - KVM hypervisor support (Red Hat Linux)
  - VMware update - ESXi v5.5 support
- REST APIs for VA management
- Support for data tier migration from TIM v5.1 and SIM v6
  - Migration via Services engagement only – no automated upgrade, not customer upgradeable
  - Check white papers on developerWorks for customization compatibility:
    - Customization: https://ibm.biz/BdE338
    - SIM v6 vs. SIM v7: https://ibm.biz/BdE3wF

Note!

Recent SIM Adapter Updates – a sampling

Documentum: Support for V7

Microsoft Office 365: multi-domain support

PeopleSoft: Support for PeopleTools v8.5.4

Oracle eBusiness: Support for Oracle eBusiness Suite v12.2

BMC Remedy: Support for Remedy 8.1

SAP

- Support for JCo 3.0.11 and 3.0.12 (NetWeaver)
- New! Hana database adapter
- New! SAP App Server Enterprise Portal User Management Engine adapter

IBM Security Access Manager (formerly "TAM Combo") – support for maximum password age

... and much more - for latest adapter list, see:
http://www.ibm.com/support/docview.wss?uid=swg21687732

New customer-sponsored enhancements:

- Expanded self-approval governance
  - Option to enable explicit/manual self-approval
- A new workflow extension that pauses the activity for a certain amount of time
- Workflow designer enhancements
  - 3 new checkboxes on approval, RFI and work order node – Skip Escalation, No Timeout Action, Complete on Timeout
- Support Active Directory password complexity rules
  - A new 3 of 4 rule in out-of-the-box password rules
  - New password generator and validator module to make sure the password is compliant with the new rule

Identity Manager Platform support

Component	SIM 6.0.0.6	SIM VA 7.0.0.2
OS / Hypervisor	AIX 6.1, 7.1 RHEL 6.6, 7; SLES 10,11 Windows 2012 R2	VMware ESXi 5.0, 5.5 KVM
Database	10.1, 10.5 Oracle 11g , 12c	DB2 10.5 Oracle 12c
Directory Server	SDS 6.3.1, 6.4	same
Directory Integrator	TDI 7.1.1 (SDI 7.2 supported externally if licensed separately)	same
App Server	WAS 8.5.0.x, WAS 8.5.5.x	(Inside VA)
Reports	Cognos 10.2.1, 10.2.2	same
Browser	IE 10, 11 Firefox 24, 31 ESR Chrome 42 (ISC only)	same

Privileged Identity Manager

Latest IBM Security Privileged Identity Manager (PIM) delivers improved security and flexibility

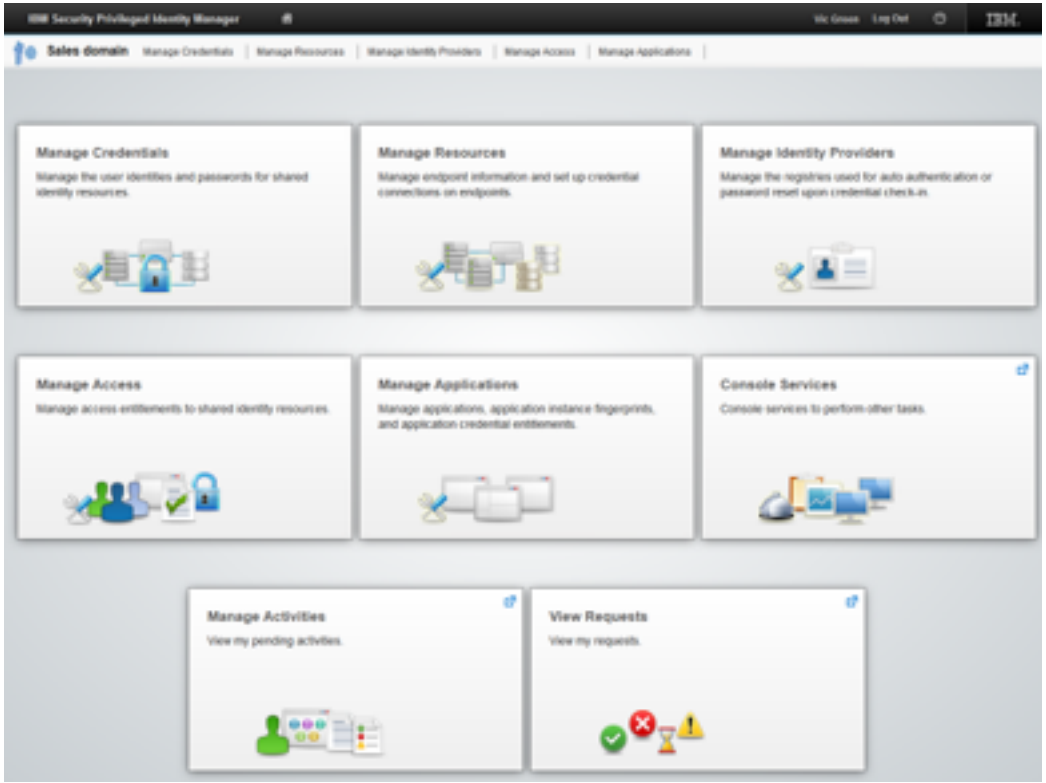
NEW!

IBM Security Privileged Identity Manager

- **Improved enterprise integration: external authentication support**
  Now supports use of Microsoft Active Directory (single domain) for user authentication
- **Improved ease of use with expanded Privileged Identity Service Center support of entitlement management**
- **Improved flexibility: application credential password management**
  The optional PIM for Applications now supports scheduled password updates of managed credentials
- **Enhanced customization support**
  New published REST APIs better support customer application integration initiatives.
- **Enhanced security: RFID authentication**
  Supports RFIDeas' RFID authentication solution
- **Quicker time to value with additional SSO profiles**
  New SSO profiles for
  - SQL Server Management Studio 2008
  - Secure CRT
  - DB2 Admin Tool *(July)*

PIM user experience: Initial Service Center Integration

- Focus on PIM administrative functions
  - Checkout functions better via SSO using PIM Access Agent, therefore no end user Service Center interaction at present



Manage Credentials

Manage the user identities and passwords for shared identity resources.

Manage Resources

Manage endpoint information and set up credential connections on endpoints.

Manage Identity Providers

Manage the registries used for auto authentication or password reset upon credential check-in.

Manage Access

Manage access entitlements to shared identity resources.

Manage Applications

Manage applications, application instance fingerprints, and application credential entitlements.

Console Services

Console services to perform other tasks.

Manage Activities

View my pending activities.

View Requests

View my requests.

PIM VA – Administrative and Security enhancements

- Certificate management enhancements: Allows upload and management of a centralized trust store using a web UI
- Use of Active Directory (single domain) for user authentication
- Support of RFIDeas’ RFID badges for second factor authentication
- REST APIs for user and credential management

Privileged Identity Manager Platform support

Component	PIM VA v2.0.1
OS / Hypervisor	VMware ESXi 5.0, 5.5
Database	DB2 10.1, 10.5
Directory Server	SDS 6.3.1, 6.4
Directory Integrator	TDI 7.1.1
App Server	[inside the VA]
Reports	Cognos 10.2.1
Access Agent client	Windows 7, 8.1 Server 2008, 2012
Browser	IE 10, 11 Firefox 24, 31 ESR

Security Intelligence.
Think Integrated.

ISIM Functional Overview

Managing
WHO has ACCESS to WHAT

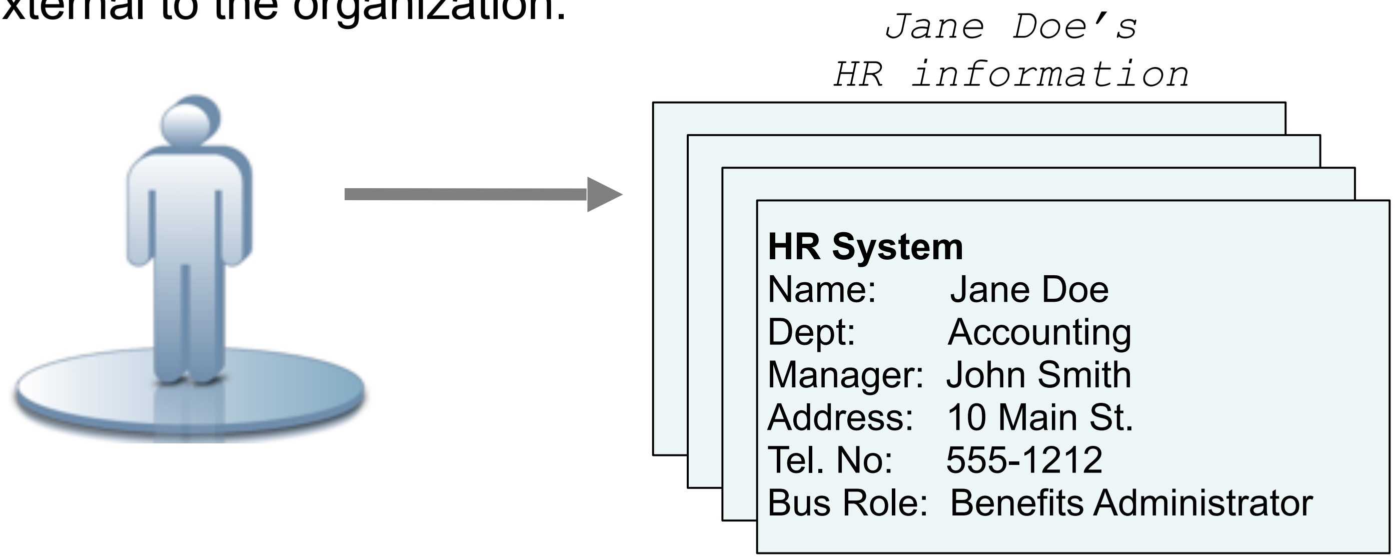
People	Policy	Resources

The *Who* in Identity Management

Who → Users → people who need access to resources.

Users can be internal or external to the organization.

- Employees
- Customers
- Business Partners
- Citizens



Jane Doe's HR information

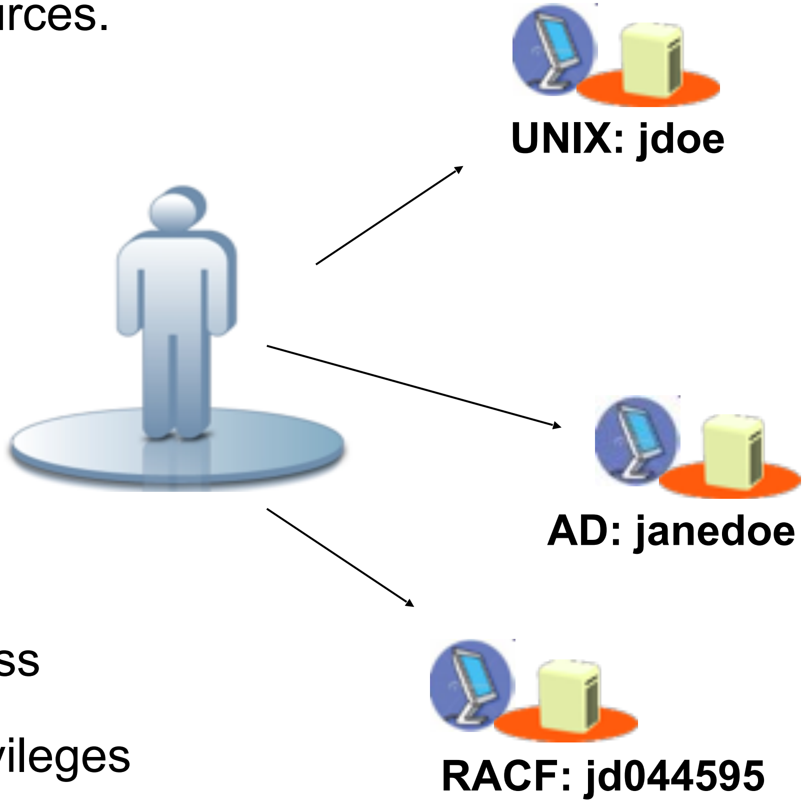
HR System
Name: Jane Doe
Dept: Accounting
Manager: John Smith
Address: 10 Main St.
Tel. No: 555-1212
Bus Role: Benefits Administrator

The *What* in Identity Management

What → Accounts → give people access to resources.

Examples of Resources:

Operating Systems	UNIX, Windows
Databases	DB2, Oracle
Applications	SAP, Lotus Notes
Directories	LDAP, Active Directory



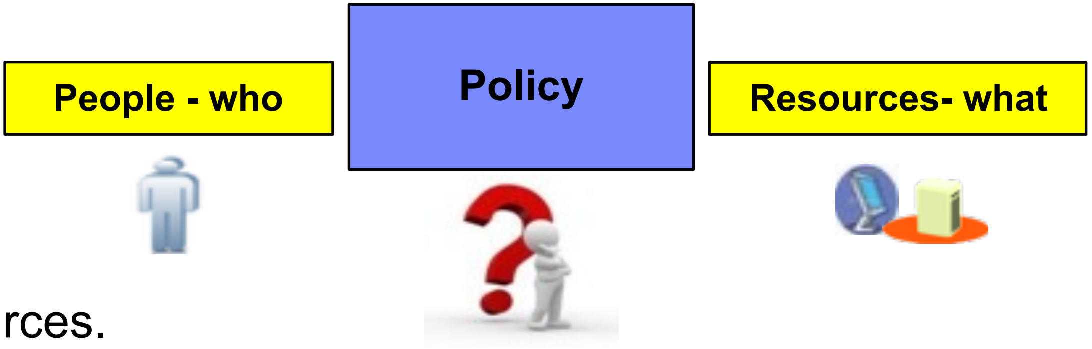
The user account generally consists of:

- A user ID
- Password
- Group or role assignments

grant initial access

grant access/privileges

How is Access granted …



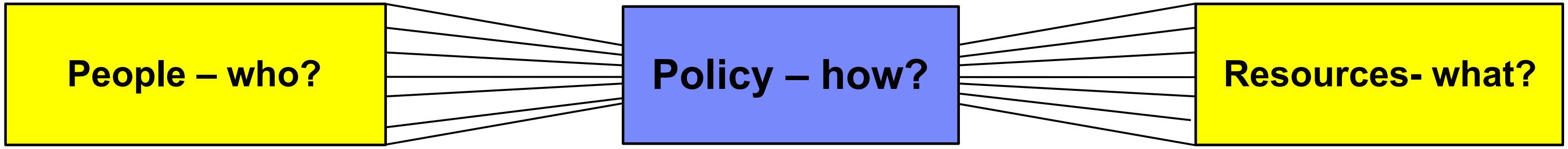
People - who

Policy

Resources- what

- Policy defines who can access resources.
- Policy is made up of membership and entitlements
- Workflow and Approvals define the business process and ensure that the right people are given the right access.
- Policy Membership can be defined through Roles
  - Business Roles – collections of users by job function
  - Application Roles – collection of resources or entitlements.
- Membership - Individual vs. Group
  - Examples of group Membership: Active Directory group policies, SAP authorizations
- Access can be regularly recertified to ensure continued business need

Identity Manager connects Who to What through How



People – who?

Policy – how?

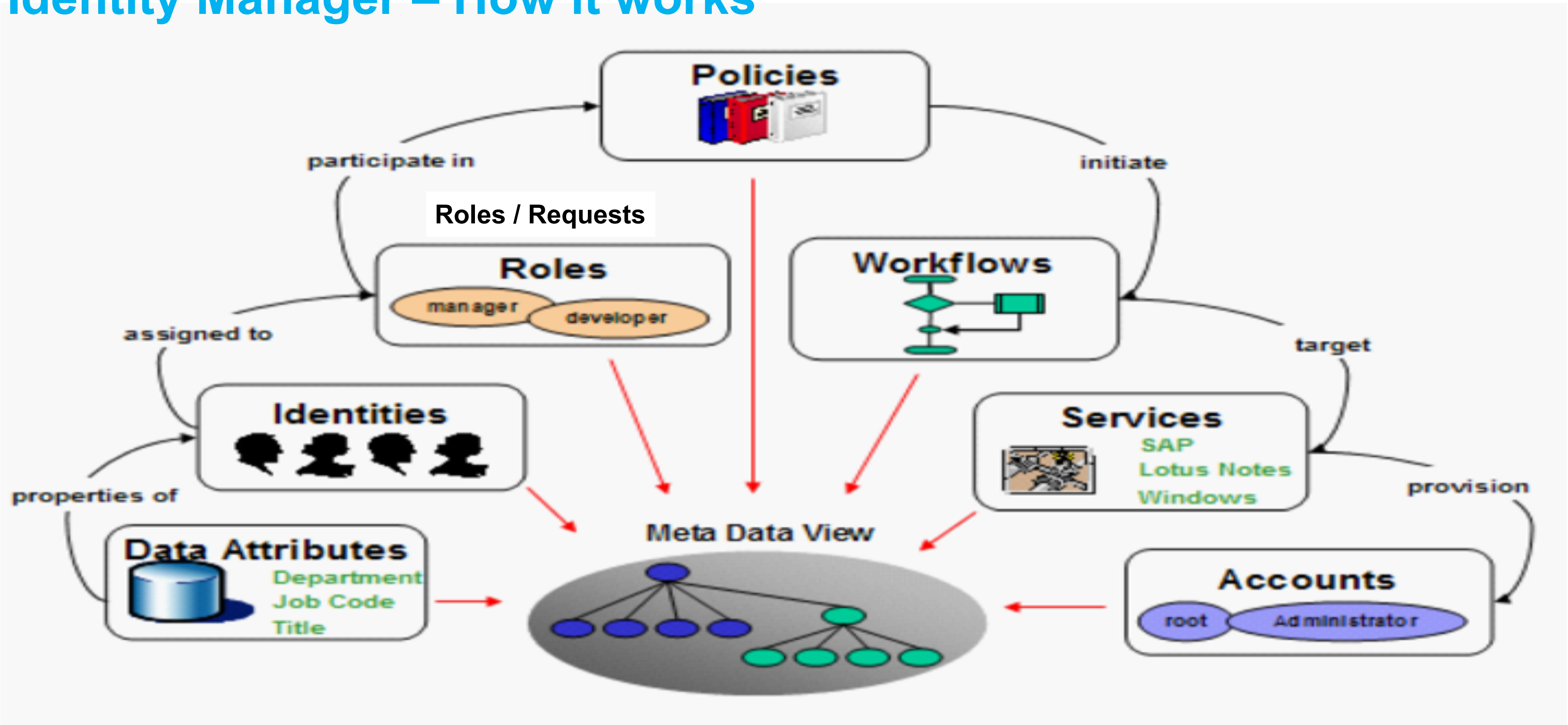
Resources- what?

- Manages existing user identities
- Help automate the creation of new identity
- Maintains enterprise wide Identity records for reports and audits.

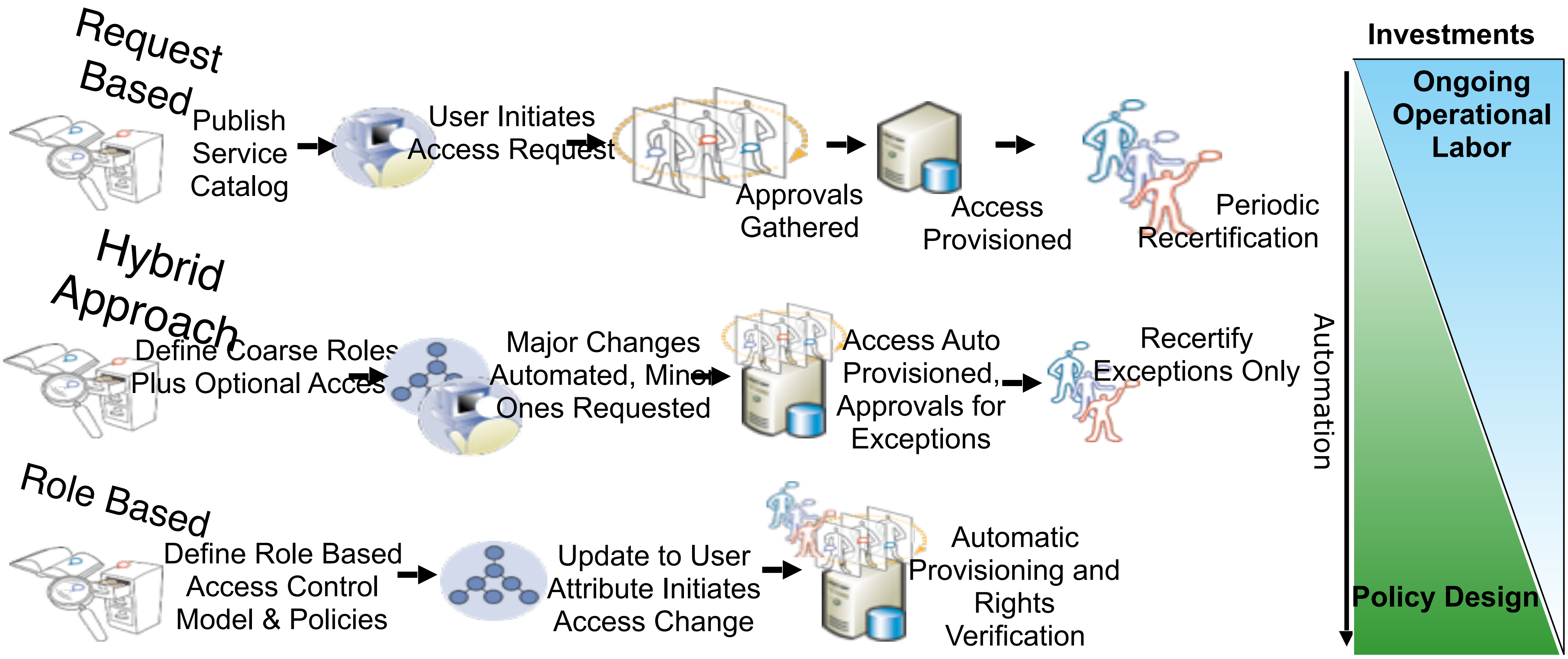
- Help maintain a unique identity-entitlement map for the enterprise

- Manages existing entitlements, membership and accounts.
- Help automate the creation of new entitlements.
- Maintains an enterprise wide entitlement records for reports and audits.

Identity Manager – How it works



Identity Manager offers multiple ways to administer user access rights



Request Based

Publish Service Catalog → User Initiates Access Request → Approvals Gathered → Access Provisioned → Periodic Recertification

Hybrid Approach

Define Coarse Roles Plus Optional Access → Major Changes Automated, Minor Ones Requested → Access Auto Provisioned, Approvals for Exceptions → Recertify Exceptions Only

Role Based

Define Role Based Access Control Model & Policies → Update to User Attribute Initiates Access Change → Automatic Provisioning and Rights Verification

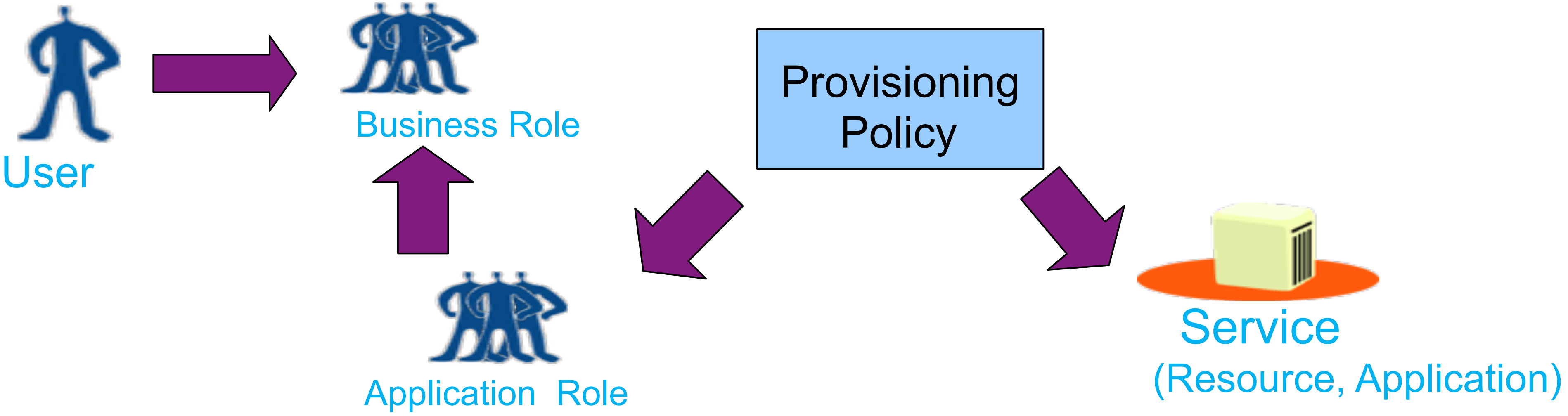
Investments

Ongoing Operational Labor

Policy Design

Automation

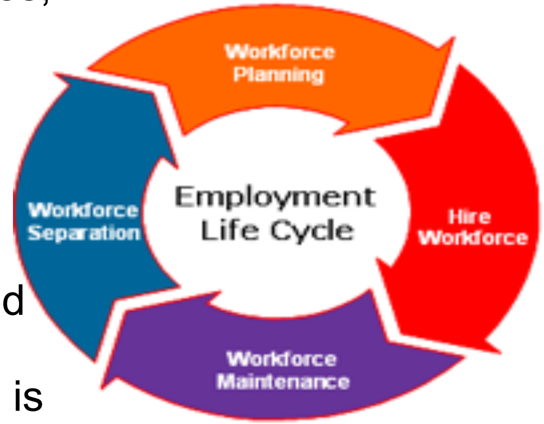
Provisioning model with role hierarchy



- **Provisioning policies administer access to resources through user membership and access rights**
  - Users can be assigned to roles based on their responsibilities
  - Roles, accounts and groups are then assigned as members of provisioning policies

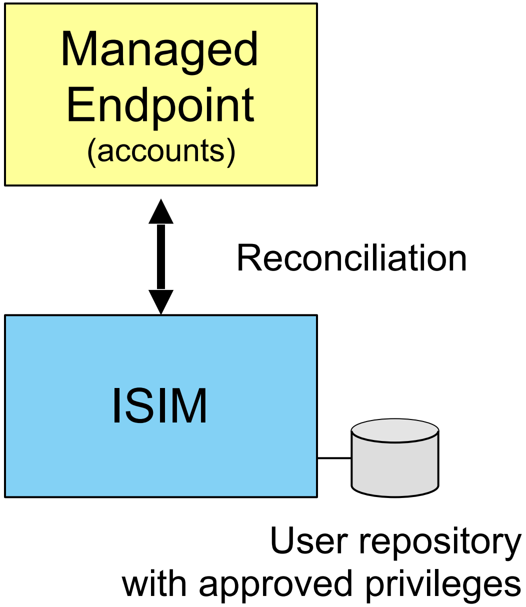
User Provisioning – User lifecycle management

- Customer Challenge:
  - Frequent employee churn, job changes
  - Too time consuming to manually provision access for new employees, change accounts due to job changes, deprovision access upon employee termination
  - Exacerbated by mergers (increased change) or IT staff shortage (insufficient resources to manually manage changes)
- Solution:
  - ISIM can automatically provision accounts for new employees based on employee assignment to a role (e.g. Emergency room nurse),
  - ISIM can automatically change privileges when the employee’s role is changed.
  - “Zero day de-provisioning” is also supported



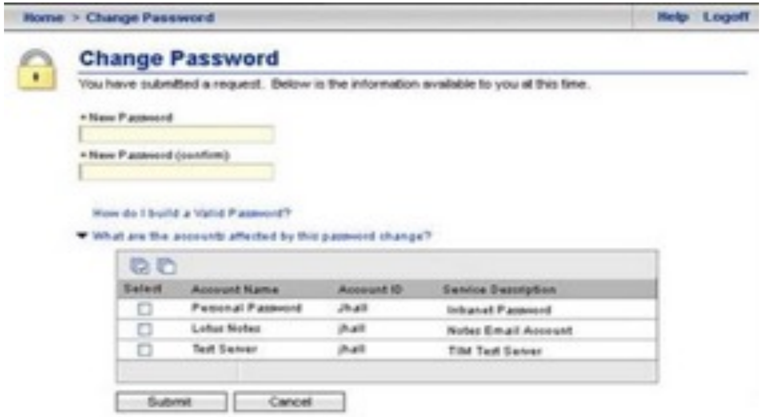
Account reconciliation – enforcing access policy

- **Customer Challenge:**
  - When employees leave or change jobs, their application and system accounts are not terminated
  - Dormant and “orphan” accounts result in higher license costs, and expose organization to security breaches
  - Compliance audit failure could result
- **IBM Solution:**
  - ISIM can automatically reconcile “known good” ISIM users to accounts on target applications and systems.
  - Orphan accounts are recognized and can be automatically suspended.
- **Benefit**: accounts available only for valid users – lower IT admin costs, improved security



Centralized password management - enhances security and reduces help desk costs

- Customer Challenge:
  - High Help Desk costs to support employee forgotten password requests
  - Need to expire passwords regularly and enforce password format for security
  - Account breach may raise awareness of weaknesses
- ISIM solution:
  - Self-service password management across all systems
    - Apply targeted or global password rules
    - Verify compliance with target systems
  - Password synchronization
    - Propagate and intercept
  - Challenge/response questions for forgotten user ids and/or passwords
    - User or site defined questions
    - Email notification
  - Integration with SAM E-SSO
    - Desktop password reset/unlock at Windows logon prompt
    - Provisioning user access to SAM E-SSO



Change Password

You have submitted a request. Below is the information available to you at this time.

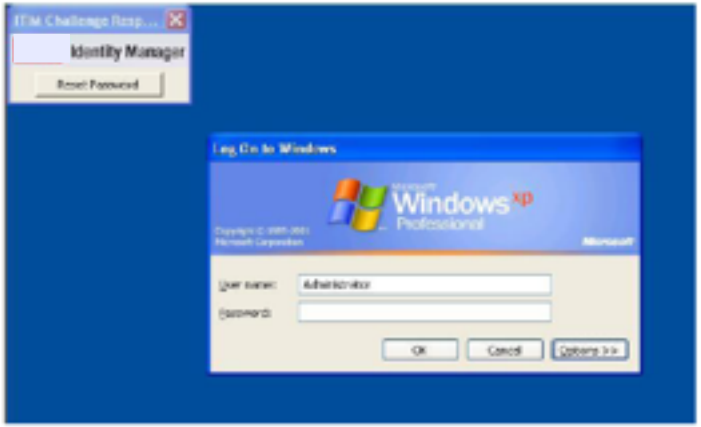
* New Password

* New Password (confirm)

How do I build a Valid Password?

What are the accounts affected by this password change?

Select	Account Name	Account ID	Service Description
□	Personal Password	JHall	Intranet Password
□	Lotus Notes	jhall	Notes Email Account
□	Test Server	jhall	TIM Test Server



User name: Administrator

Password:

Adapter portfolio: integration breadth and depth for rapid value

Broad Support for Prepackaged Adapters

Applications & Messaging

- Blackberry Ent. Server
- Cognos
- Command line-based applications
- Documentum eServer
- Google Apps
- LDAP-based applications
- Lotus Notes/Domino
- Microsoft Lync
- Microsoft Office365
- Microsoft Sharepoint
- Novell eDirectory
- Novell Groupwise
- Oracle E-Business Suite
- Oracle PeopleTools
- Rational Clearquest
- Rational Jazz Server
- Remedy
- Salesforce.com
- SAP GRC
- SAP Netweaver
- SAP AS Java
- Siebel
- Windows AD/ Exchange

Authentication & Security

- CA Top Secret
- CA ACF2
- Cisco UCM
- Desktop Password Reset Assistant
- Entrust PKI
- IBM Security Access Mgr
- IBM SAM-ESSO
- RACF zOS
- RSA Authentication Mgr

Partner Offered Integrations

- Approva BizRights
- Citrix Pwd Mgr
- Cryptovision PKI
- ActivIdentity
- Lawson
- SecurIT R-Man
- JD Edwards
- Epic
- Meditech
- Tandem
- BMC Remedy
- Zimbra Mail

Operating Systems

- HP-UX
- IBM AIX
- IBM i/OS
- Red Hat Linux
- Solaris
- Suse Linux
- Windows Local

Databases

- DB2/UDB
- Oracle
- MS SQL Server
- Sybase

Requires local adapter
Application adapter
Host adapter

Fast, adaptable tooling for custom Adapters

- Quickly integrate with home-grown applications
- Easy wizard-driven templates reduces development time by 75%
- Requires fewer specialized skills

Deep support, beyond a ‘check-box’, for critical infrastructure and business applications

Security Intelligence.
Think Integrated.

Market and Licensing Information

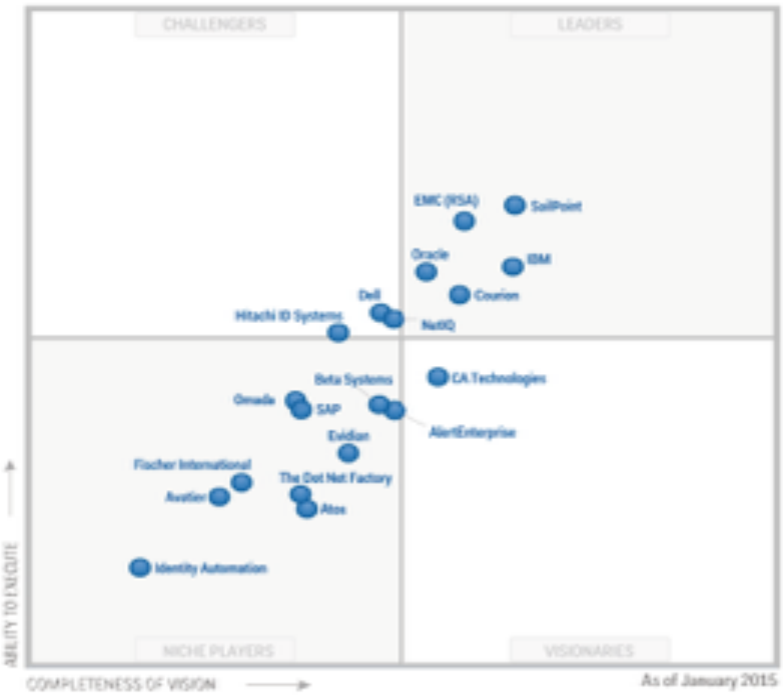
IBM is a Leader in the 2015 Gartner Magic Quadrant for Identity Governance and Administration

Gartner, Inc. Positions IBM as a LEADER in Identity Governance and Administration (IGA)

"The IGA market is transforming legacy, on-premises IAM products. IGA vendors are investing heavily to meet client needs in ease of use, mobility, business agility, and lower total cost of ownership. User provisioning and access governance functions continue to consolidate."

Gartner, Inc. "*Magic Quadrant for Identity Governance and Administration*" by Felix Gaehtgens, Brian Iverson, Steve Krapes, January 2015 Report #G00261633

Figure 1. Magic Quadrant for Identity Governance and Administration



Source: Gartner (January 2015)

Source: Gartner (January 2015)

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from http://www.gartner.com/technology/reprints.do?id=1-27CNZU9&ct=150112&st=sb.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

ISIM Software Licencing

- Licensing can be based on Users or Processors
  - Usually user-based pricing is the most cost-effective option

- User Value Unit (UVU) based pricing has 3 components
  - Base including “Infrastructure” (class A) adapters
  - Application edition add-on for application (class B) adapters
  - Host edition add-on for host (class C) adapters

- Processor Value Unit (PVU) based pricing
  - also known as “Unlimited User” pricing
  - includes entitlement for all adapters

PVU Sizing Considerations

- When priced by “PVU” there is no licence restriction on the number of users
  - Good for large number of users with relatively low activity
- Sizing (PVUs required) will be determined by:
  - Number of instances (ALL environments, HA/DR, separation of functionality)
  - Throughput (bound by CPU capacity for load)
  - Sub-capacity pricing is supported
- PVU count halved for non-production environments
  - Based on Sales Play being available for this
- COLD or WARM standby for HA/DR not counted in PVU calculation
  - Only where standby is turned off or not doing meaningful work while primary is active

UVU Sizing Considerations

- When priced by “UVU” there is no licence restriction on installed instances or processor cores
  - Good where user population is known in advance
  - S/W pricing not dependent on environments, architecture, load
    - Note that total solution cost will still be dependent on these

- Sizing (UVUs required) will be determined by:
  - Number of users that will access the system
    - Internal Users (Contractors and Employees of licensee)
    - External Users (NOT Contractors or Employees of licensee)
    - Infrequent Internal Users (Access less than 5 times a year)

User Value Unit Calculation

- Calculate number of “Users”
  - 1 “Internal User” = 1 “User”
  - 15 “External Users” = 1 “User”
    - Must be separate from internal users if mixed
  - 15 “Infrequent Internal Users” = 1 “User”
    - Must be tracked to prove low usage.

- Calculate UVUs based on number of “Users”
  - For 1 to 5,000 Users, 1.00 UVU per User
  - For 5,001 to 15K Users, 5,000 UVUs + 0.50 UVUs per User above 5K
  - For 15,001 to 50K Users, 10,000 UVUs + 0.30 UVUs per User above 15K
  - For 50,001 to 150K Users, 20,500 UVUs + 0.20 UVUs per User above 50K
  - For 150,001 to 500K Users, 40,500 UVUs + 0.10 UVUs per User above 150K
  - For 500,001 to 1M Users, 75,500 UVUs + 0.05 UVUs per User above 500K
  - For 1,000,001 to 3M Users, 100,500 UVUs + 0.025 UVUs per User above 1M
  - For greater than 3M Users, 150,500 UVUs + 0.01 UVUs per User above 3M

Questions ?