



IBM Tivoli Identity Manager Overview

April 2011

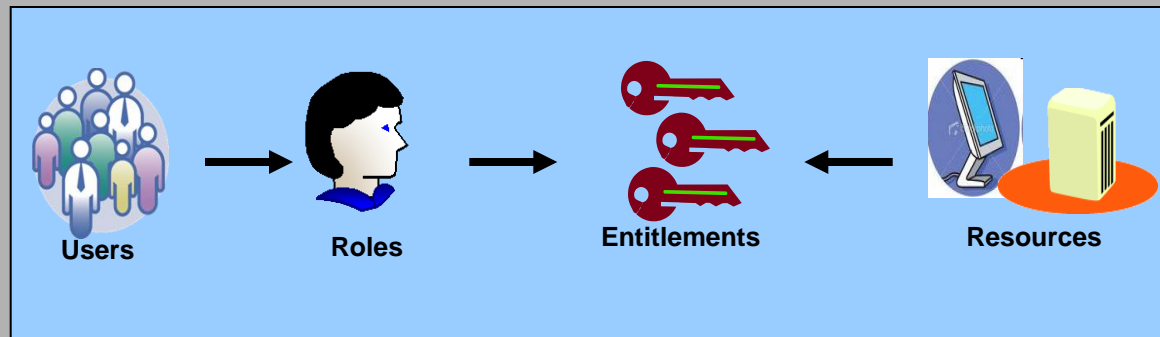


Agenda

- Why Tivoli Identity Manager**
- Identity and Access Assurance**
- TIM Overview**
- Role management and modeling**
- Compliance and audit**

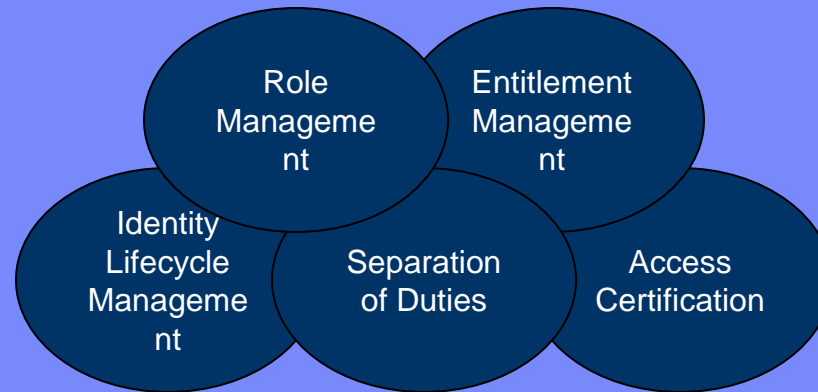
Why Tivoli Identity Manager

- ❑ **User provisioning products deliver value, but deployments can stall without scalable administration**
 - Role and entitlement management can deliver an abstraction to manage administration and access
- ❑ **Web access management solutions fail when not integrated to offer business context**
 - Entitlement management can provide business context (e.g. location, data classification, time of day, etc...) for access control policies
- ❑ **Inability to manage business conflicts that arise due to granting of user access**
 - Separation of duty policies can manage access conflict
- ❑ **Lack of flexible and continuous validation of user access and remediation**
 - Access certification tightly integrated with user provisioning can deliver validation and remediation of user access
- ❑ **Poor integration with security information and event management for user activity monitoring**
 - Log collection is good, integrated suspension of access based on abnormal activity is better
- ❑ **Desire for more integrated/holistic policy-based governance around IAM**



Identity and Access Assurance

Identity and Access Management Governance



User Provisioning

Access Management

Security Information &
Event Management

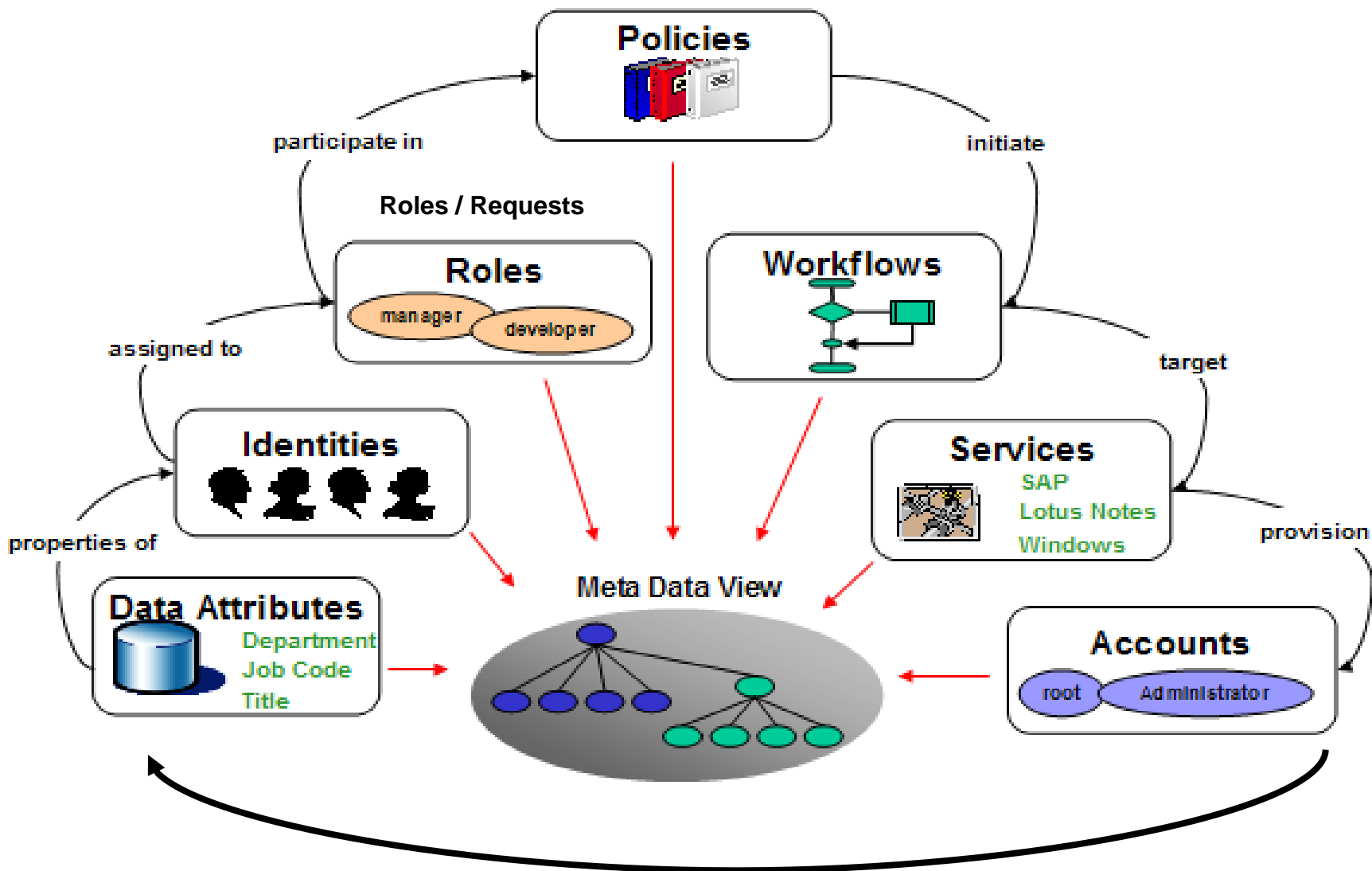
Directory Services

Policy Management

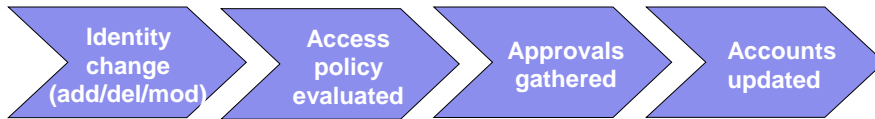
- **Identity and Access Assurance governs and enforces access while providing the closed loop to audit/compliance**

Tivoli Identity Manager Overview

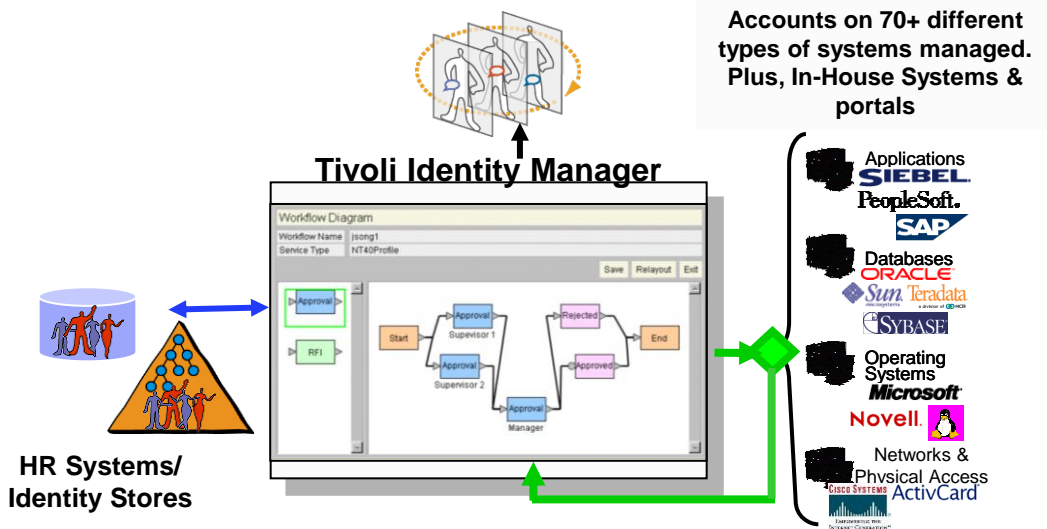
Tivoli Identity Manager – How it works



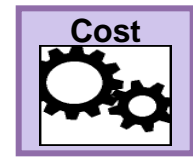
Tivoli Identity Manager automates, audits, and remediates user access rights across your IT infrastructure



Detect and correct local privilege settings

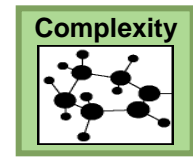


- Know the **people** behind the accounts and **why** they have the access they do
- Automate user privileges lifecycle across entire IT infrastructure
- Fix non-compliant accounts
- Match your workflow processes



Reduce Costs

- Self-service password reset
- Automated user provisioning



Manage Complexity

- Consistent security policy
- Quickly integrate new users & apps

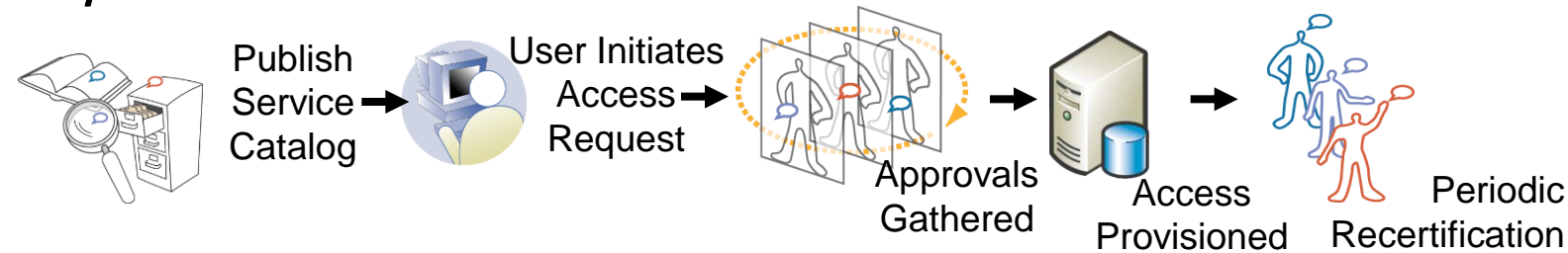


Address Compliance

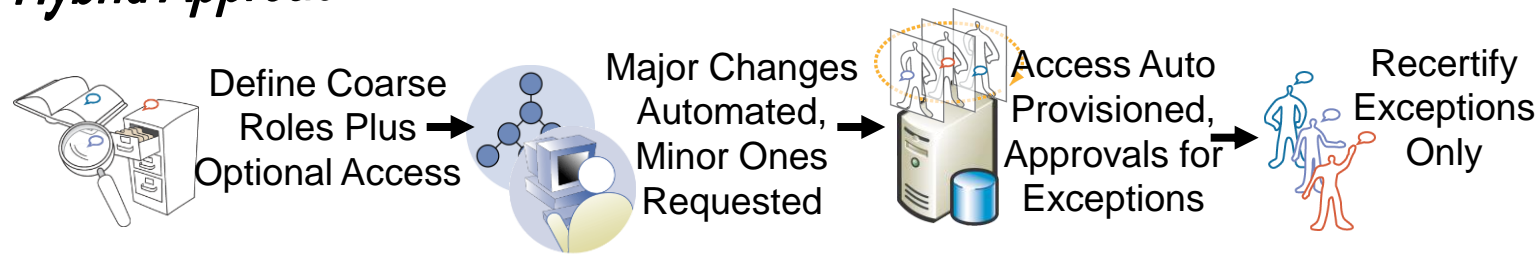
- Closed-loop provisioning
- Access rights audit & reports

TIM offers multiple ways to administer user access rights

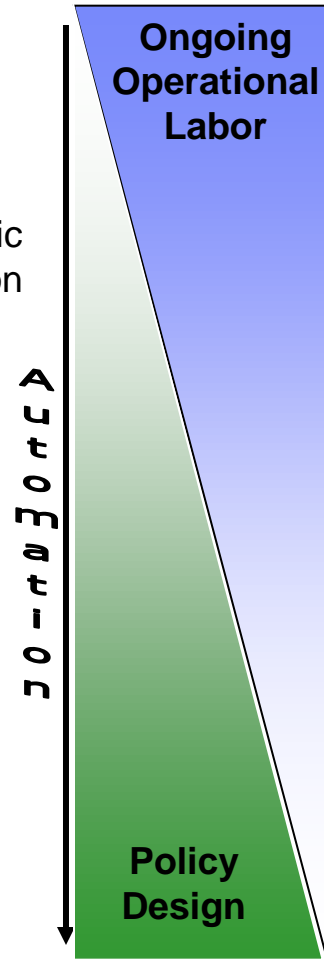
Request Based



Hybrid Approach



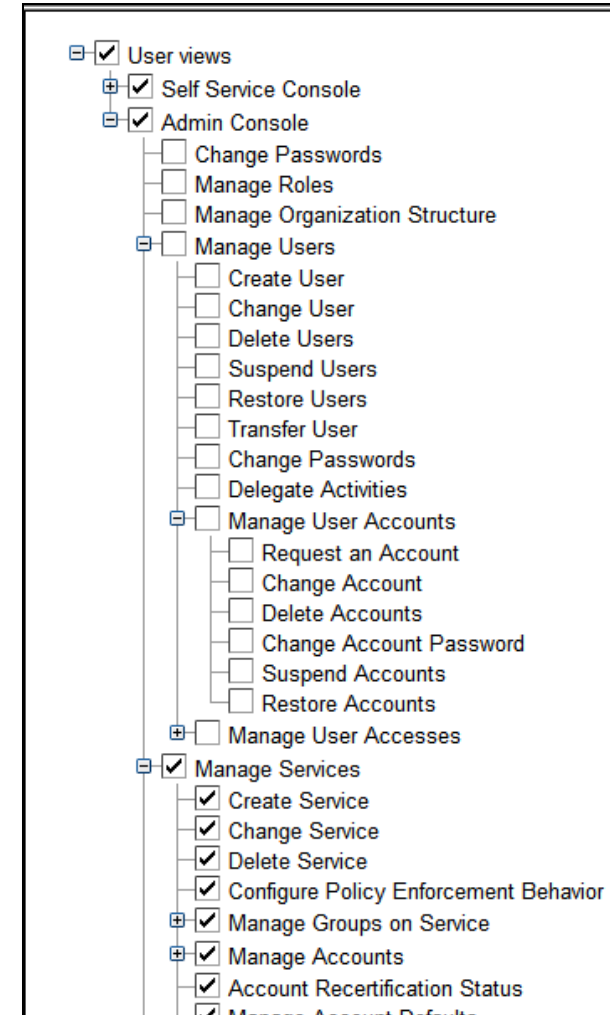
Role Based



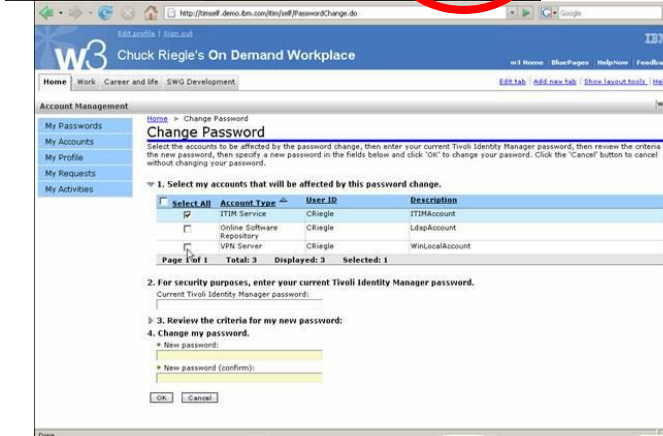
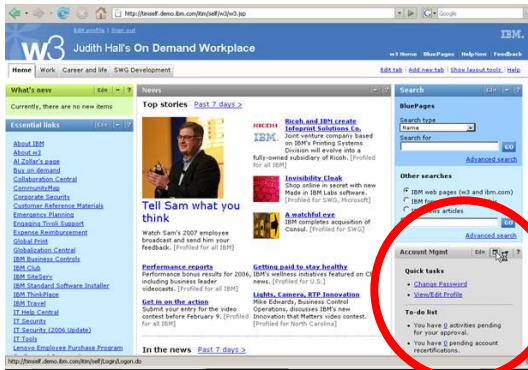
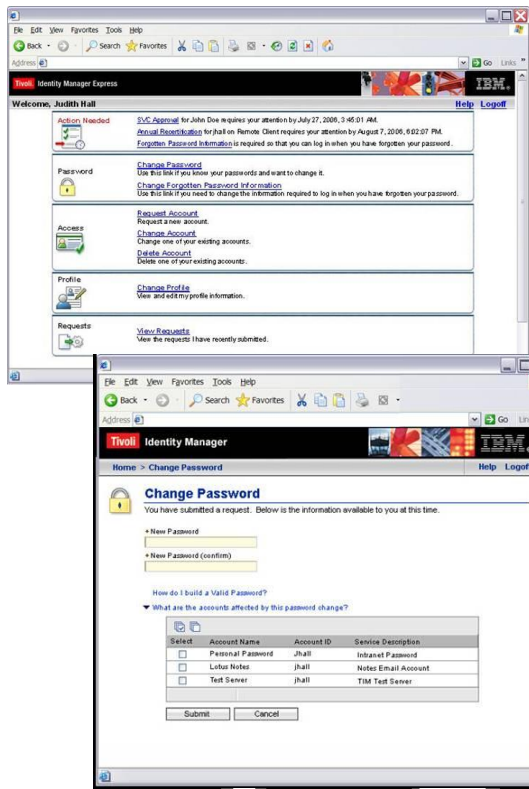
TIM makes it easy - Tailored user interface views for IT and business users - console

Console

- Designed with more than just system administrators in mind**
 - TIM administrators
 - Help desk assistants
 - Service/Application owners
 - Managers
 - Auditors
 - End users
- Customize default user views and security settings or create additional views unique for users in your organization**
- Intuitive user interface shows users only what they need to do their jobs**



Tailored UI's - Customizable Self-Service User Interface - Accelerates ROI



- Self-Service for end-users
 - Request Access
 - Reset Password
 - Approvals
- Customizable
 - Update via style sheets
 - Portal-friendly
- Upgrade-friendly
 - Customizations maintained
 - New features added

Help Desk costs \$20-per-call for password resets

Gartner Group

Employees request an average of 3-4 resets per year

Meta Group

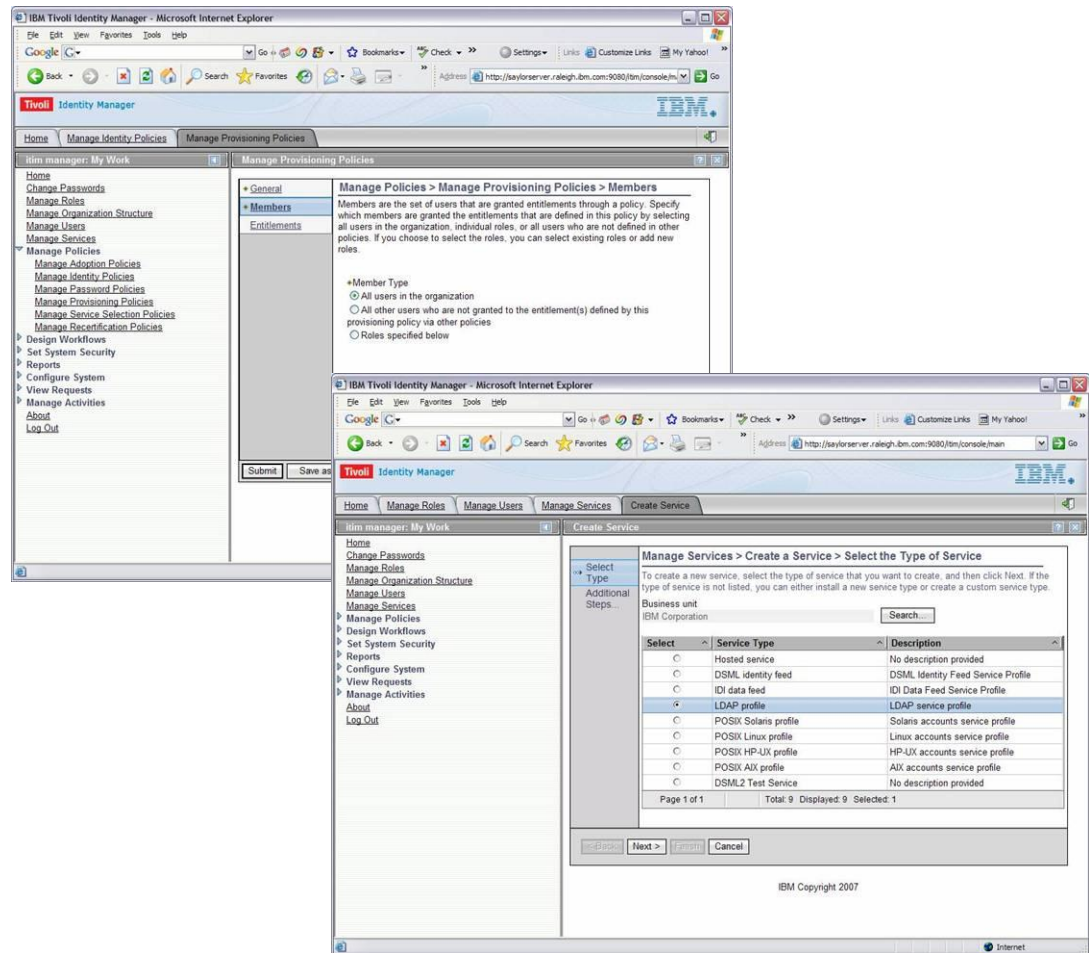
Simplified policy, workflow, and configuration reduces setup time and training

□ Wizards helps users build:

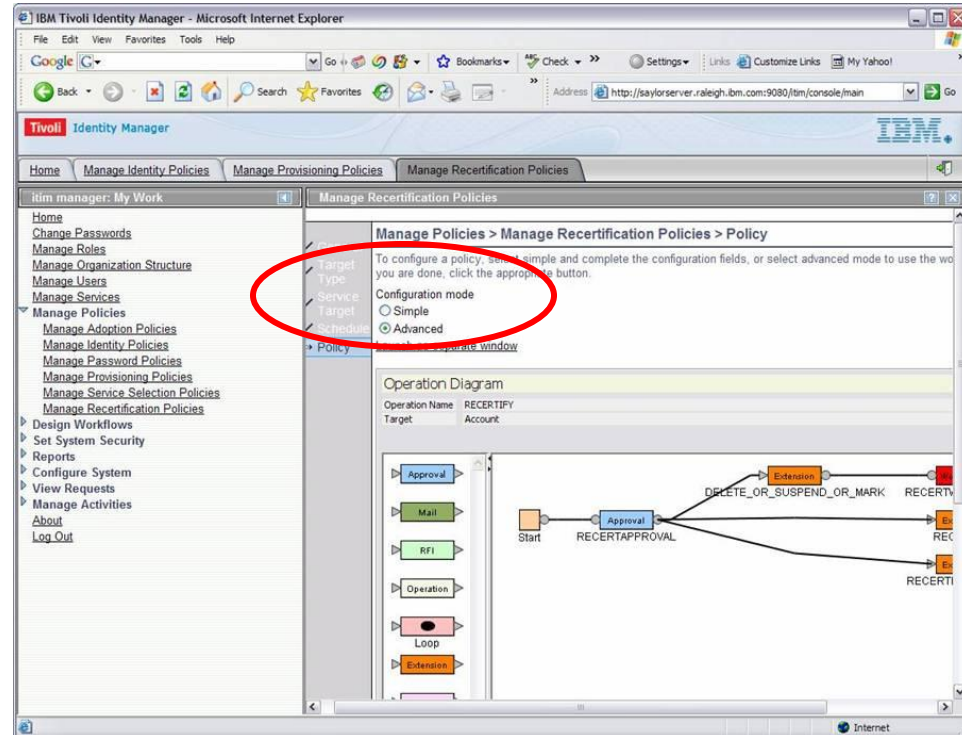
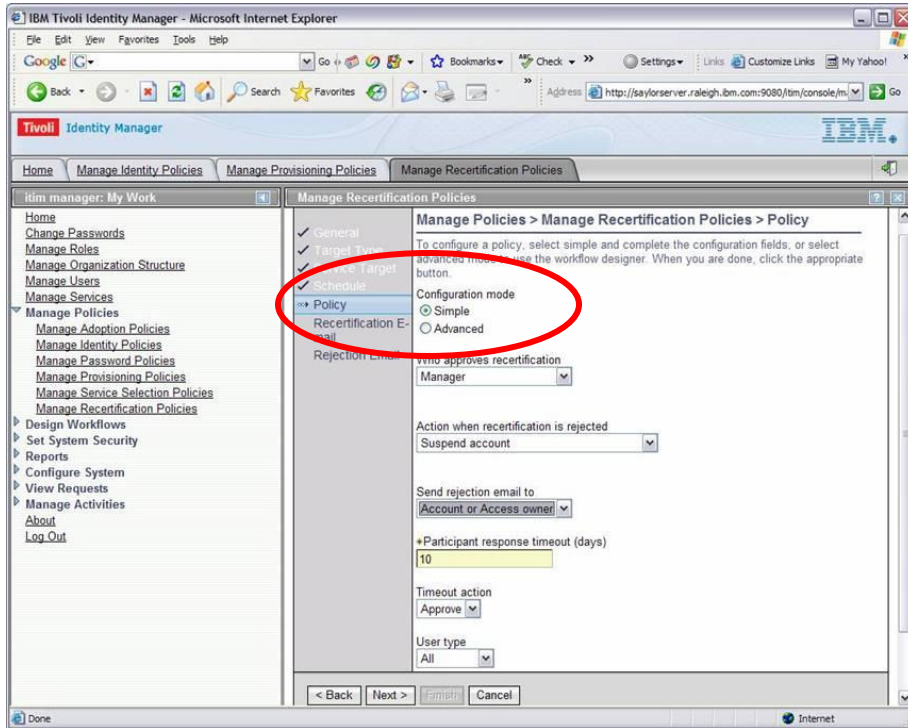
- Approval workflows
- Request for Information Nodes
- Email Nodes
- Adoption Policies
- Recertification Policies
- Identity Feeds
- Service Definitions

□ No need for programming or scripting for simple configuration options

- Defaults to “simple” configuration
- Toggle to “advanced” option to meet complex needs



Make the “simple things simple” ...while still allowing for advanced customization (Recertification Policy example)



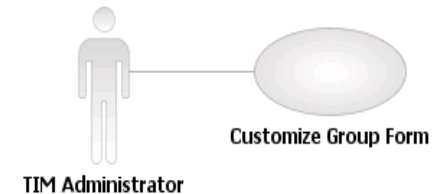
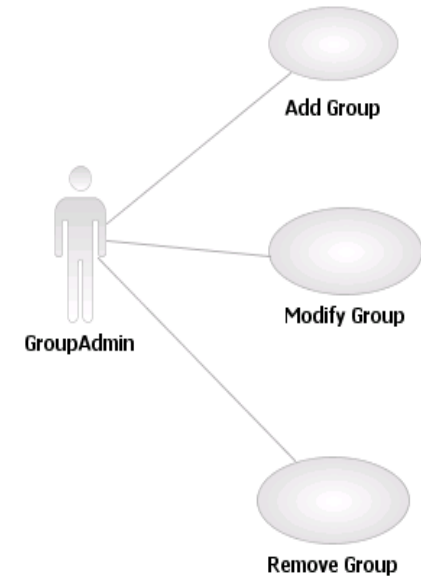
Group management simplifies and reduces cost of user administration

Customer challenge – business delay

- Business delay while TIM administrator waits for native application owner to create group, then TIM reconciliation with target system before users can be assigned to groups

Answer: TIM group management

- Administration of groups on the provisioning target
 - Create New Groups
 - Delete existing Groups
 - Modify – add, remove members
- Nesting of groups supported for those targets that support nesting
- Eligible provisioning targets
 - LDAP, Active Directory, Unix (AIX, HP-UX, Solaris) and Linux (RHEL and SuSE)
 - Additional targets via TIM adapter updates



Manage Groups > Create Group > General Information	
General Information	To create a group of type Windows Active Directory Groups on OFN Active Directory service, type the name of the group and any other information on the form. Then click Next.
Access Information	
Group Membership	
*Group unique name	<input type="text" value="ProjectA"/>
Common Name	<input type="text" value="Project A"/>
Container	<input type="text" value="ou=ofn"/> <input type="button" value="Search..."/> <input type="button" value="Clear"/>
Group Type	<input type="text" value="Security"/>
Group Scope	<input type="text" value="Local"/>
Member of	

Role Management

Role management:

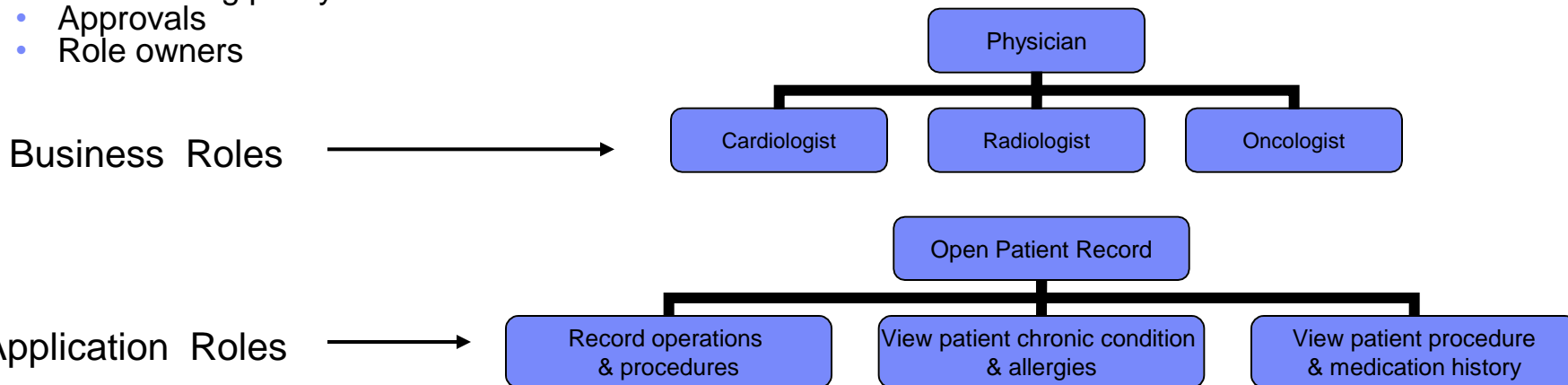
Role hierarchy simplifies and expands automation of user access

□ Business challenge

- Administration of user access can be increasingly complex and time consuming through the direct user-permission mapping

□ TIM capabilities

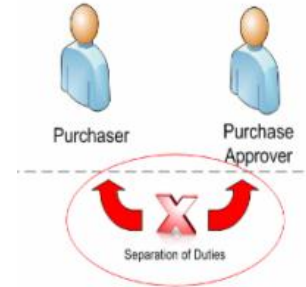
- Establish parent/child role relationship and apply inheritance through role membership
 - Add or remove roles as members to other roles
- Parent roles can have multiple children
 - Physician = parent role
 - Cardiologist, Radiologist = child roles
- Child roles can have multiple parents
 - Cardiologist = child role
 - Physician, Health care practitioner, Employee = parent roles
- Inheritance flows to all objects that use roles
 - Provisioning policy
 - Approvals
 - Role owners



Separation of duties enhances security and compliance

□ Business challenge

- Avoiding business conflicts that could heighten their risk exposure
 - e.g. same person making purchases is also allowed to approve them
- Exclude users from having access rights that create a business conflict



□ TIM capabilities

- Provides preventative and detective control over role conflicts by creating/modifying/deleting SoD policies that exclude users from having membership to conflicting roles
 - User cannot be a member of Role A and Role B
 - User may not have membership to more than N roles within accounts receivable process
- Upon assigning or requesting access, TIM detects if a conflicting rule exists and prevents a violation from occurring
- Can support exemptions via approval workflow process when a violation is detected
- Violation and exemptions auditing via reports, which helps prevent or highlight inappropriate use of privileges

Separation of Duty Policy Violations

The request when adding members to the role Log Receipt of Medications on February 16, 2009 has caused separation of duty policy violations.

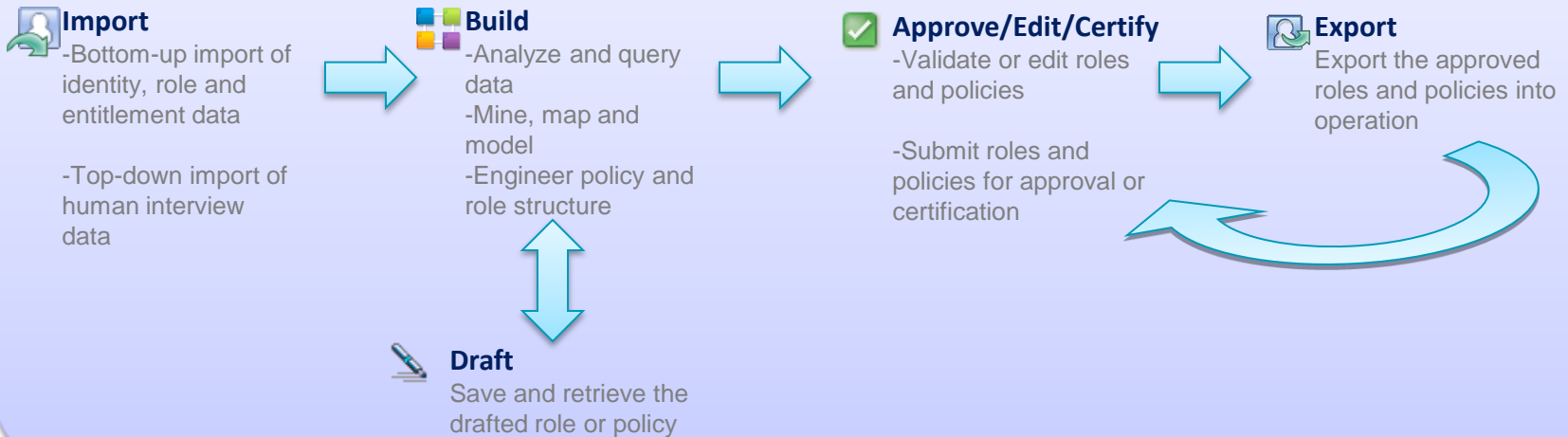
Separation of Duty Policy Violation Details

The separation of duty policy violation details are specified in the following table. Click Submit to add members to this role with separation of duty policy violations.

Person Name ^	Rule ^	Roles in Conflict
Judith Hill	Controlled Substances Inventory Mgmt	Log Receipt of Medications, Dispense Medication App Authority

Role Management: modeling and lifecycle management of roles and policies

Collaborative Role and Policy Governance



Role Modeling Assistant and Role Management Assistant

- Import data from interviews and data sources
- Analyze and engineer roles
- Approve, edit or certify roles
- Export roles into Tivoli Identity Manager for operational usage



User recertification delivers consumable compliance

Challenge: enabling access validation to those who can responsibly and accurately make that decision

- **Holistic recertification of a user's roles, account and groups for an approver in bulk fashion**
- **Recertifier specifies a separate decision for each resource and submits a consolidated response**
 - Preview prior to submission
 - Save incremental progress as draft
- **A User Recertification Policy defines a user population, schedule, resource targets, and workflow**
 - Can create recertification policies governing all accesses a user has, or a logical subset
 - Workflow can be defined using either Simple or Advanced modes
 - Simple workflow options include approval participant, rejection notification recipient (if any), rejection action, due date, overdue behavior (new), and notification templates

Review Request

Review the details of this request. To complete this activity, select the appropriate action, enter information in the comments field, and click OK. To review other activities without completing this request at this time, click Cancel.

Request Detail

Date submitted: November 11, 2008 6:59:44 AM
 Request type: Recertification Policy
 Requested for: Eastern US Sales
 Requested by: IBM Tivoli Identity Manager System
 Due date: November 21, 2008 6:59:45 AM
 Instruction summary: Recertification Approval

Instruction Detail

Reviewer Action

Indicate whether or not Eastern US Sales still requires each of the following roles:

Roles	Description	Still Required	All None
Sales Role		<input type="radio"/> Yes <input type="radio"/> No	

Indicate whether or not Eastern US Sales still requires each of the following accounts and groups:

Accounts and Groups	Description	Still Required	All None
<input type="checkbox"/> eussales on ITIM Service		<input type="radio"/> Yes <input type="radio"/> No	
<input type="checkbox"/> eussales on Sales Applications (Linux)		<input type="radio"/> Yes <input type="radio"/> No	All None
<input type="checkbox"/> Sales Demo Group		<input type="radio"/> Yes <input type="radio"/> No	

Reviewer Comments

Enter comments:

TIM reporting system facilitates audit requirements and integrates reporting across Tivoli

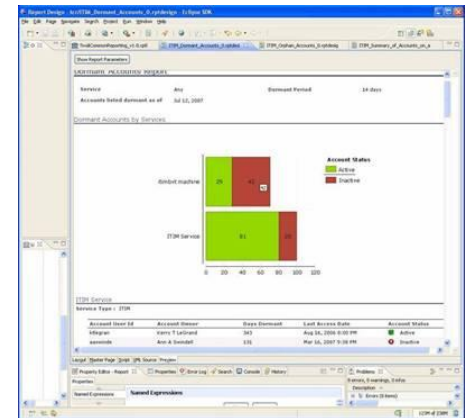
□ TIM Reporting

- Aimed at the IT Administrator
- Uses TIM reporting database and schema
- Supports large PDF reports
- BIRT designs for TIM reports



□ Tivoli Common Reporting Module

- Report Administration
 - Import of TIM report pack, report scheduling, accessible via email and URL
- Report customization using the Eclipse BIRT designer
- Common Console for Report Viewing



Tivoli Identity Manager integration breadth *and* depth is key to achieving rapid value

Broad Support for Prepackaged Adapters

Applications & Messaging

Amdocs ClarifyCRM 12.0 on AIX using DB2*
Documentum eServer *
 Lotus Notes/Domino
 Windows AD/ Exchange
 Novell e-Directory (NDS)
Novell GroupWise
Oracle E-Business Suite
PeopleTools
SAP GRC
SAP Netweaver
SAP AS Java
Siebel
 * **Peregrine Service Center**
Remedy
 Quickplace*
 LDAP-based Applications
 * Command Line-based Applications
 Universal Provisioning
 * **JDEdwards**
 * Tandem
 IBM Rational Clearcase

Relational Database

IBM DB2/UDB
 Informix Dynamic Server
 Oracle
 Microsoft SQL Server
 Sybase
 * **RDBMS Based Apps**

Ready for Tivoli

Citrix Password Manager
 Cyber-Ark Network Vault for Passwords
 Actividentity Trinity Secure Sign-on
 Passlogix v-GO Provisioning Manager
 Aveksa Access Governance
 Sailpoint Identity IQ
 CA Eurekify Discovery and Audit
 SecurIT R-Man

Authentication & Security

IBM RACF zOS*
 IBM Tivoli Access Manager
 IBM TAM ESSO
 IBM Desktop Password
 * Reset Assistant
 * CA ACF2
CA Top Secret
 Entrust PKI*
 RSA Authentication
 Manager*
 * CA Siteminder
 Cisco UCM

Operating Systems

HP-UX
 HP-UX NIS*
 IBM AIX*
IBM i5/OS
 OpenVMS*
 RedHat Enterprise Linux
 Sun Solaris
 Sun Solaris NIS*
 SuSE Linux Enterprise Server
 Windows Local

*Requires local adapter
 * Custom Implementation required
 •BOLD = Appl. adapter
 •BOLD = 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



Thank
YOU