



Automating User Provisioning with Tivoli Identity Manager (TIM)

Leveraging knowledge of people
to create business value

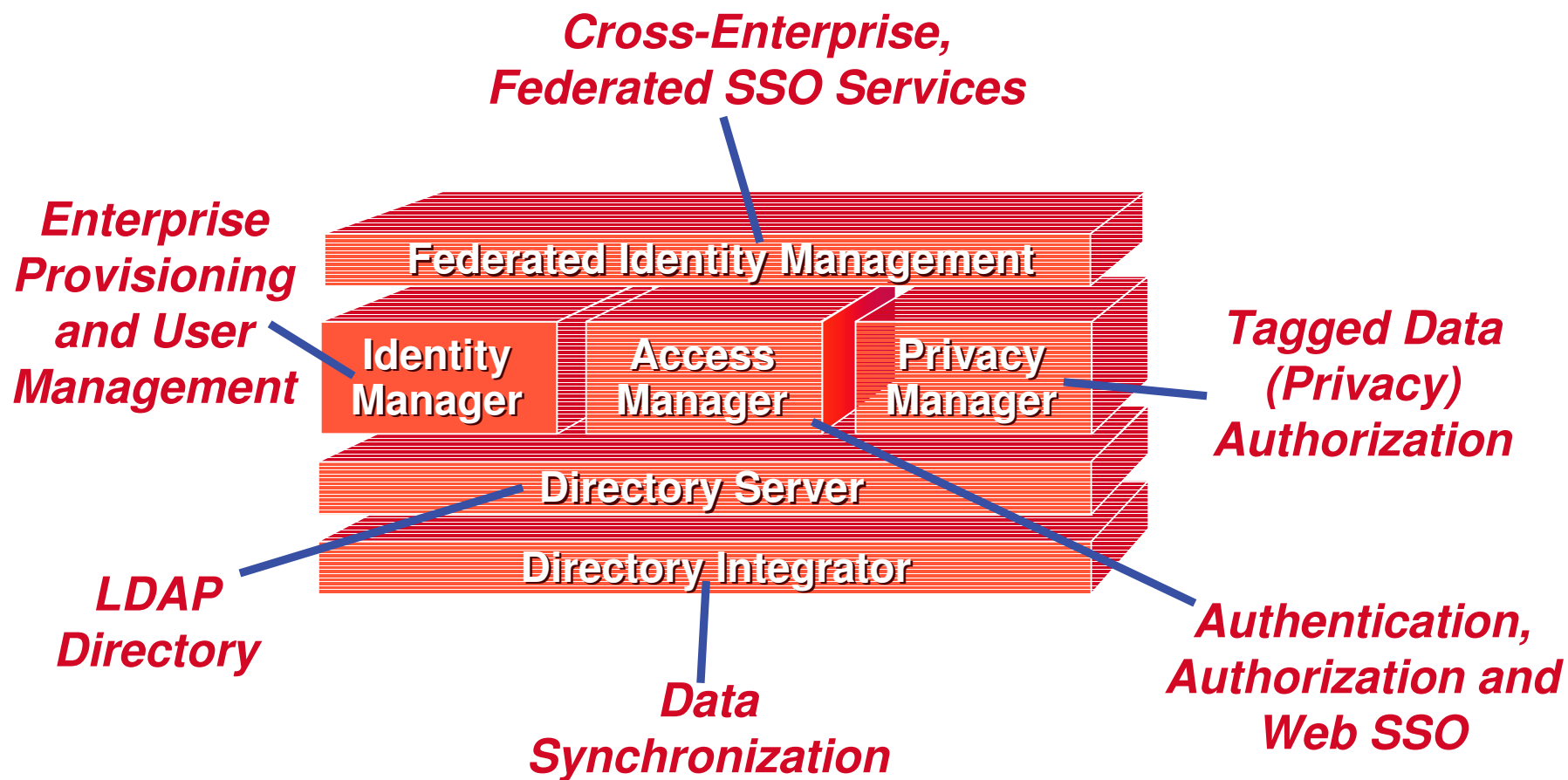
*Daniel TumSuden, CISSP
Technical Security Evangelist - Americas
danhere@us.ibm.com*



 e-business software

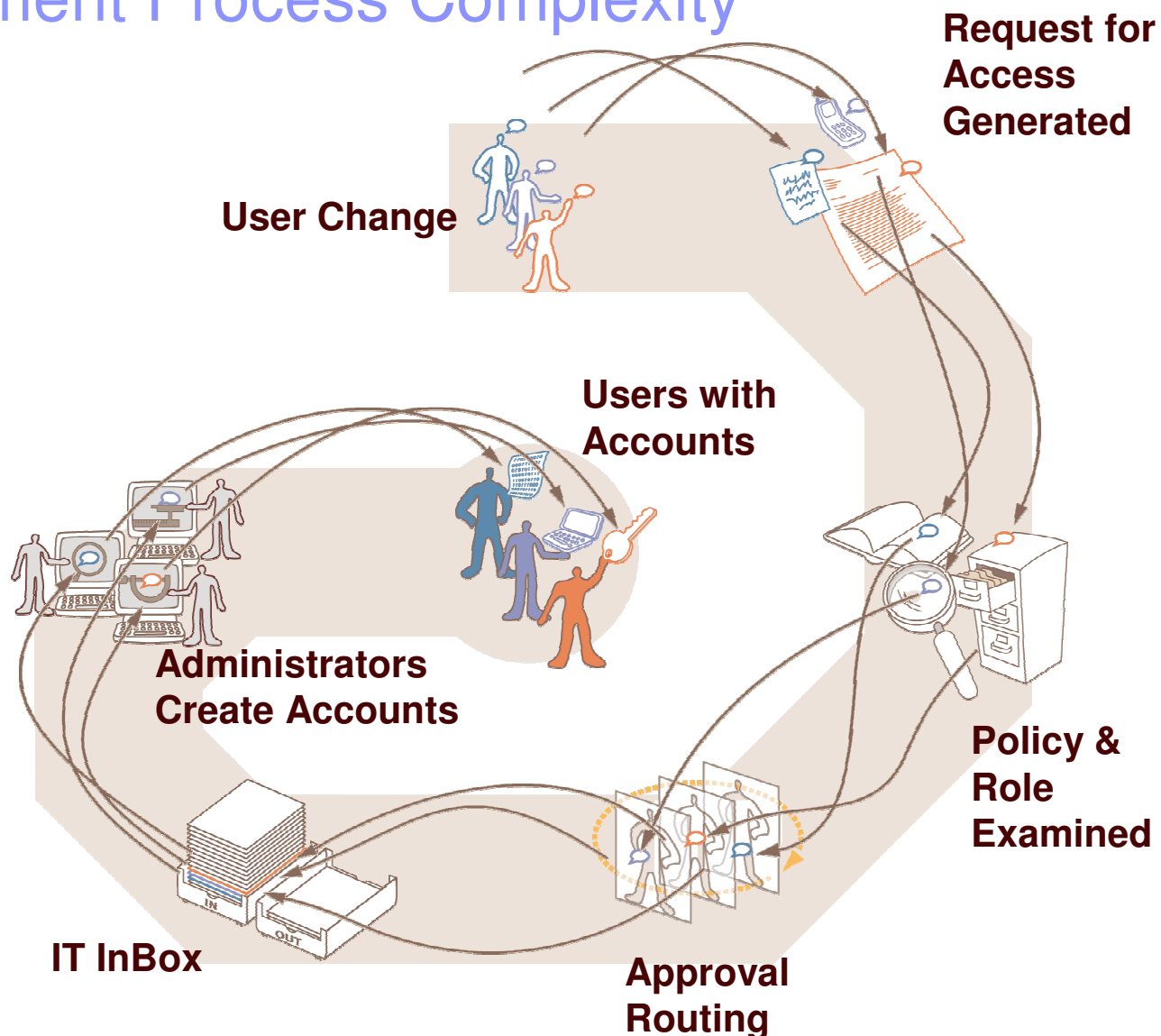
© 2004 IBM Corporation

IBM's Integrated Identity Management Solutions



Security Management Process Complexity

- Elapsed turn-on time: up to 7 days per user
- Account turn-off performance: 30-60% of accounts are invalid
- FTE User Admin only handles 300-500 users
- 40% of Helpdesk spent on Password Resets



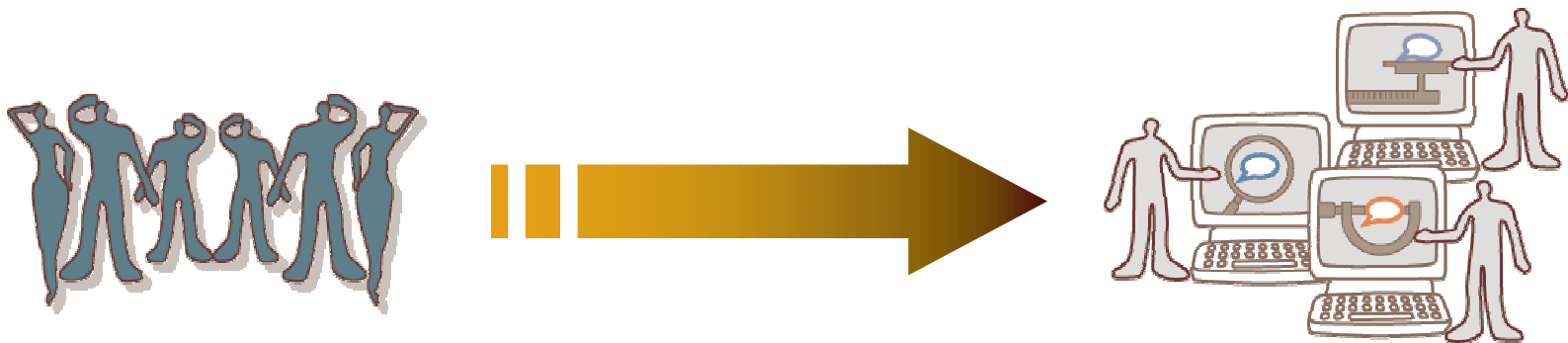
Identity Management and Compliance

	Major Wall Street Mutual Fund Company
Need:	Fulfill Requirements for Sarbanes-Oxley Preparation Audit; Determine source of customer retention issues
Result:	<ul style="list-style-type: none">Discovered 900 former brokers who still had accounts activeDiscovered 1 of these brokers had been accessing customer accounts internally...

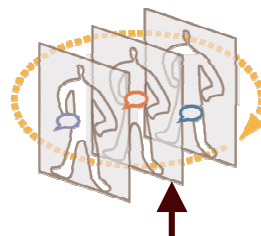


User Provisioning Controls Access Privileges

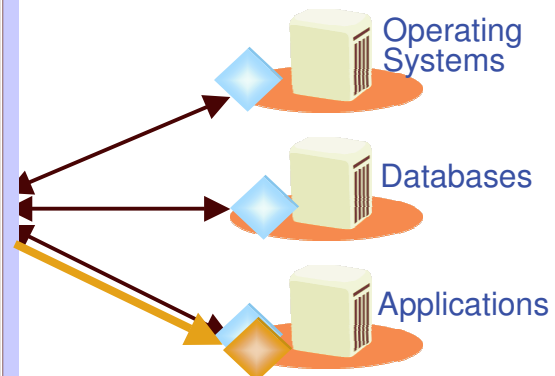
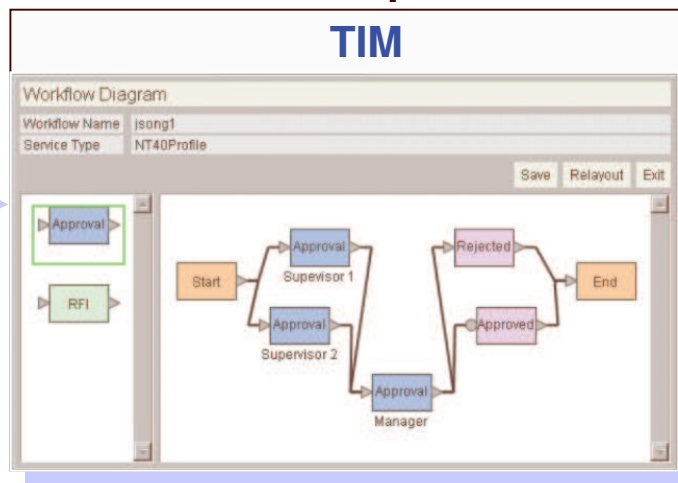
Know the valid users
Know what users are entitled to access
Control who gets access to what



Enterprise Identity Needs



Accounts on 70 different types of systems managed. Plus, In-House Systems & portals



Now Network Identities Too!





Password Management

Reduce costs in the helpdesk

User self-service of passwords across all systems

Password Rule Checking

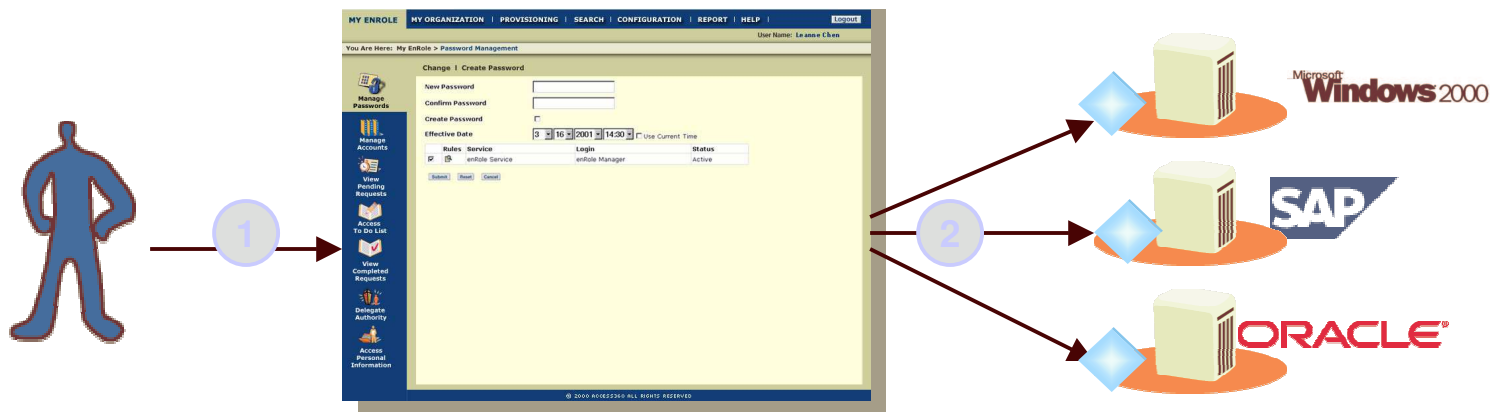
- Verifies compliance with target requirements

- Add rules across all resources

Challenge-Response system for forgotten passwords

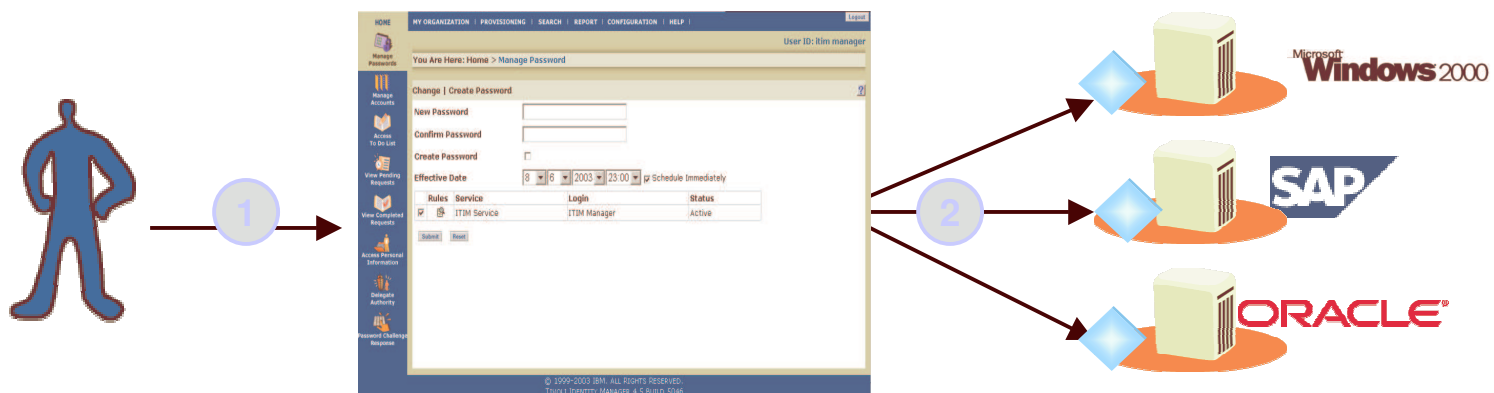
Help Desk costs \$20-per-call for password resets
Gartner Group

Employees request an average of 3-4 reset per year
Meta Group



Self Service Reduces Help Desk Calls

- Users may service all of their own attributes (address, title, etc)
Challenge response for password reset
- Changes can be reviewed and approved through workflow
- Password sync for TIM services
- Reverse password sync for Windows and/or Access Manager users



Access Rights Accountability



- Improve security by automatically finding, flagging, and/or removing invalid accounts
- Audit actual user access rights against privilege rules.
 - Know who has access to what
 - Know when access rights are violated
 - Evaluate/Audit changes made by local administrators

Admin Reports

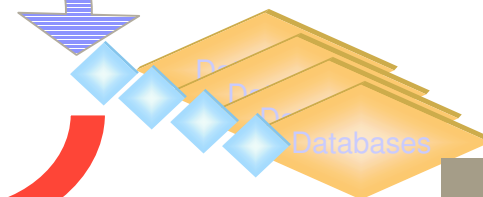
Business Partner	Employee ID	Employee Name	Employee Title	Employee Department	Employee Location	Employee Status
Business Partner 1	1000000001	John Doe	Software Engineer	Development	New York	Active
Business Partner 1	1000000002	Jane Smith	Product Manager	Marketing	New York	Active
Business Partner 1	1000000003	Bob Johnson	Sales Representative	Sales	New York	Active
Business Partner 1	1000000004	Alice Brown	Customer Support	Support	New York	Active
Business Partner 1	1000000005	Charlie White	Quality Assurance	QA	New York	Active



Sources of User Information



Change/Suspend



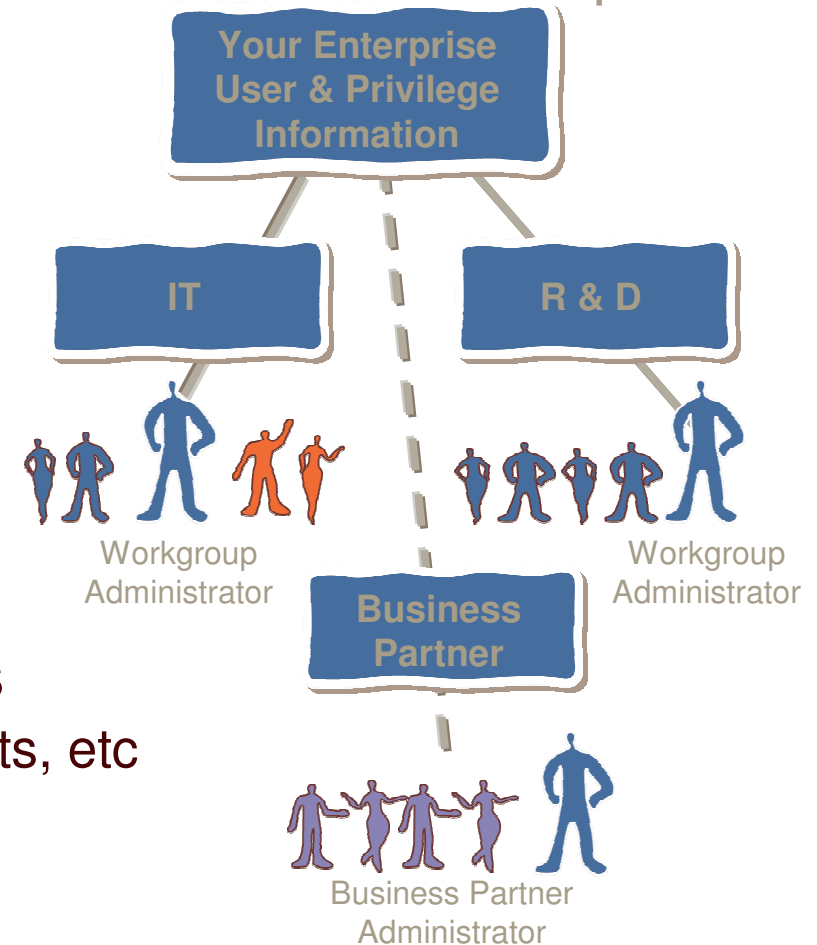
Local Admin

Delegated Administration Reduces Admin Overhead

e-Business “Virtual” Enterprise

- “Junior” administrators can control people and attributes

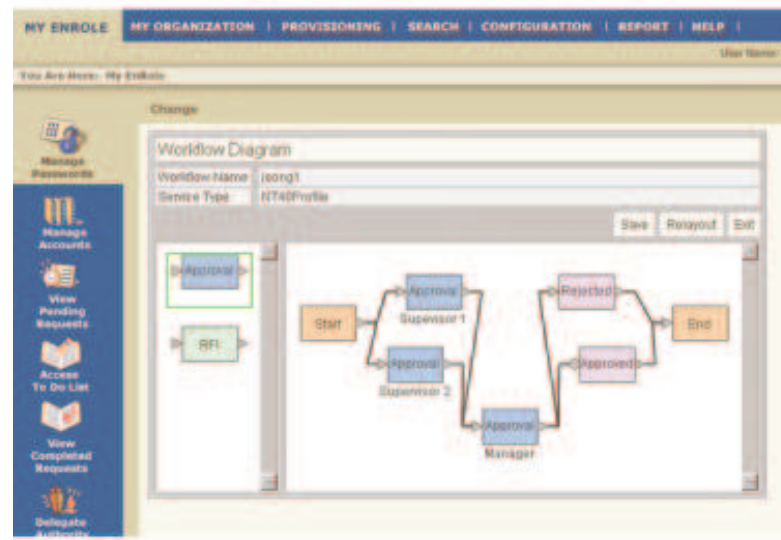
- Can restrict internal TIM resources
 - Services, Provisioning Policies, Reports, etc



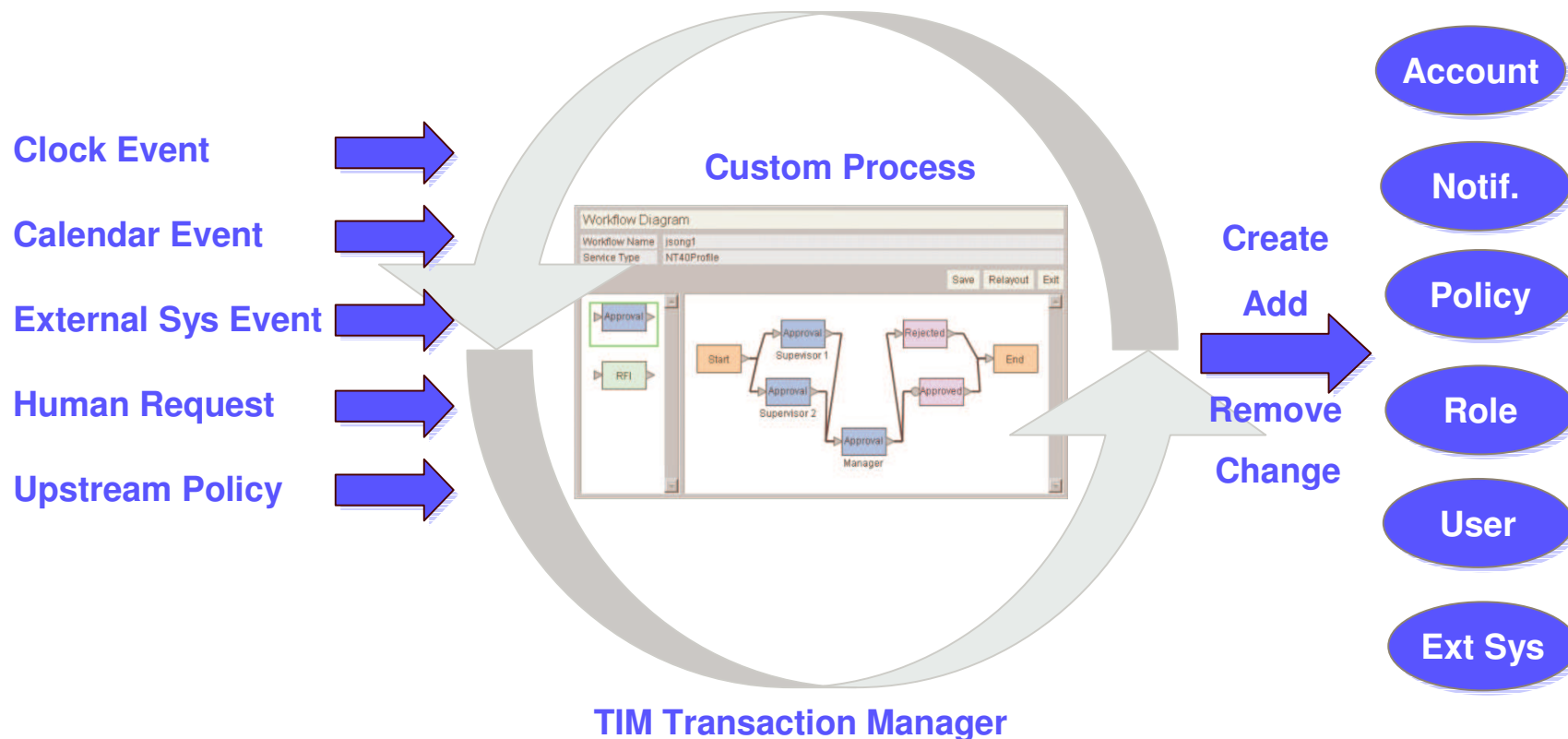


Access Request Approval Automation

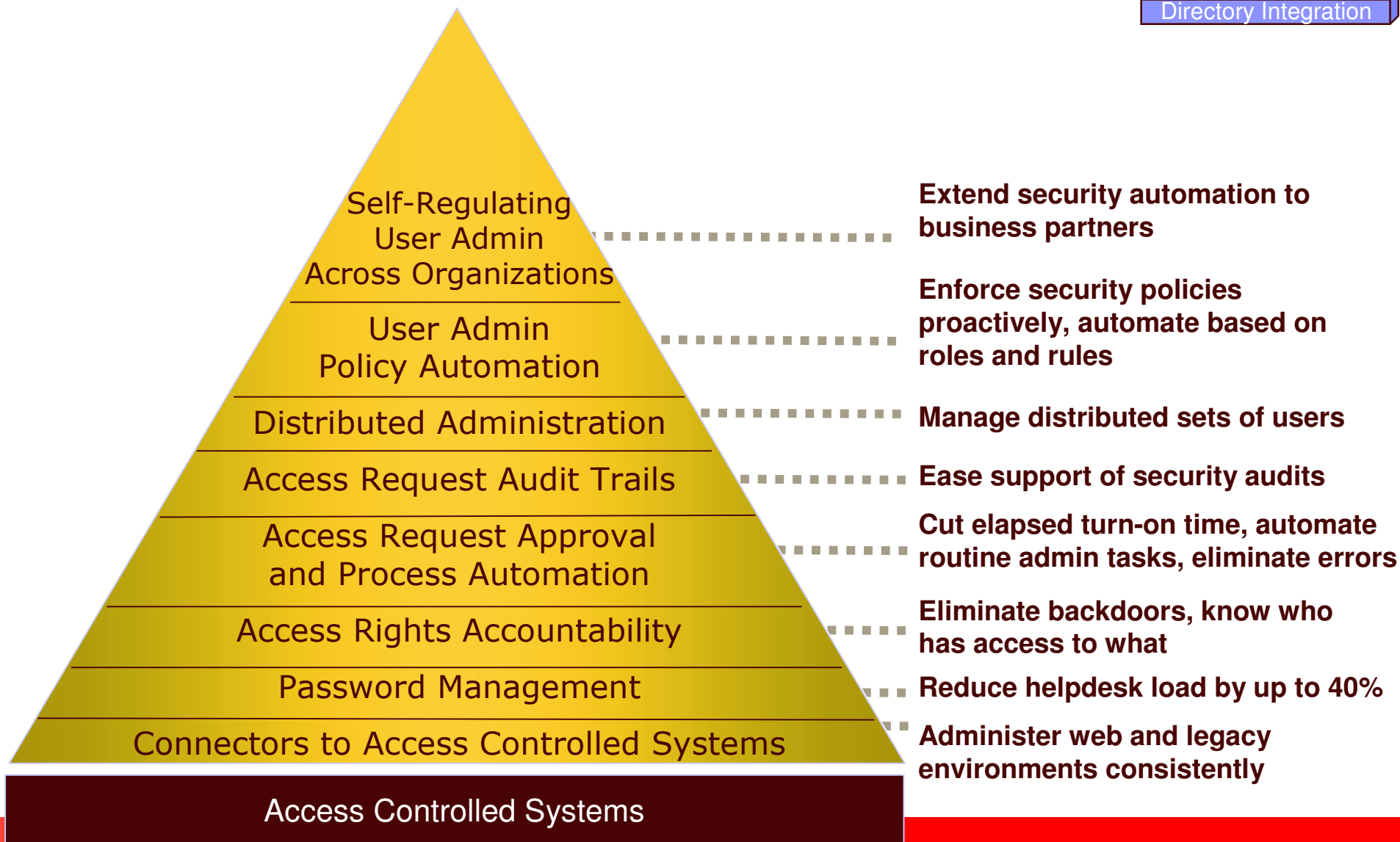
- Reduce elapsed time to establish and remove accounts.
- Decrease administrative burden.
 - Pain point with large majority of our clients
- Automate delegated or centralized approval and decision-making processes.
- Reduce mundane data-entry tasks.



Identity Lifecycle Creation and Management



Provisioning Value Pyramid



TIM Reporting Tools and 3rd Party Integration

- Default and Custom Reports
- Access Control over Report Info
- Acrobat Format for Easy Viewing
- Crystal/Actuate Reports

The screenshot shows two overlapping browser windows displaying PDF reports. The top window shows a 'Recon Report' with the following details:

- Start Time: Tue May 13 09:03:26 EDT 2003
- End Time: Tue May 13 09:03:32 EDT 2003

The bottom window shows a 'Request by Service for TAM_Service' report with the following details:

- Start Date: Feb 16, 2003
- End Date: Jun 18, 2003

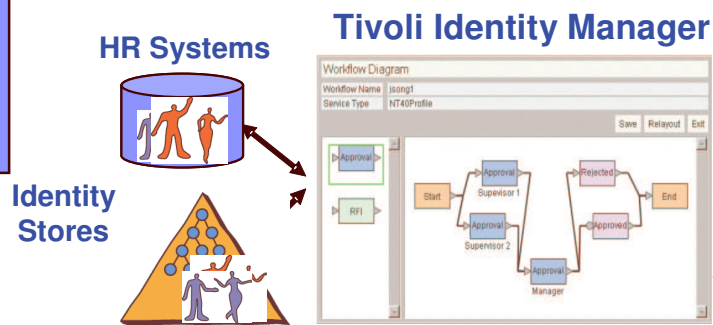
The report content is organized into a table with the following columns:

Request Type	Requested By	Requested For	Subject
Service Provision	SYSTEM	User	TAM_Service
State		Time Completed	Last Modified
Aborted	May 7, 2003 1:26:13 PM	May 7, 2003 1:35:41 PM	May 7, 2003 1:26:12 PM
Result Summary			
Service Provision	SYSTEM	Ted TAMUser	TAM_Service
State		Time Completed	Last Modified
Aborted	May 7, 2003 1:26:13 PM	May 7, 2003 1:35:41 PM	May 7, 2003 1:26:12 PM
Result Summary			
Service Provision	SYSTEM	Joe TAMUser	TAM_Service
State		Time Completed	Last Modified
Aborted	May 7, 2003 1:26:14 PM	May 7, 2003 1:35:41 PM	May 7, 2003 1:26:12 PM
Result Summary			
Service Provision	SYSTEM	Paul Avalons	TAM_Service
State		Time Completed	Last Modified
Aborted	May 7, 2003 1:26:19 PM	May 7, 2003 1:35:52 PM	May 7, 2003 1:26:18 PM
Result Summary			
Service Provision	SYSTEM	Paul Avalons	TAM_Service
State		Time Completed	Last Modified
Aborted	May 7, 2003 1:37:09 PM	May 7, 2003 1:44:31 PM	May 7, 2003 1:37:07 PM
Result Summary			

IBM and Cisco: Teamed to reduce operating costs

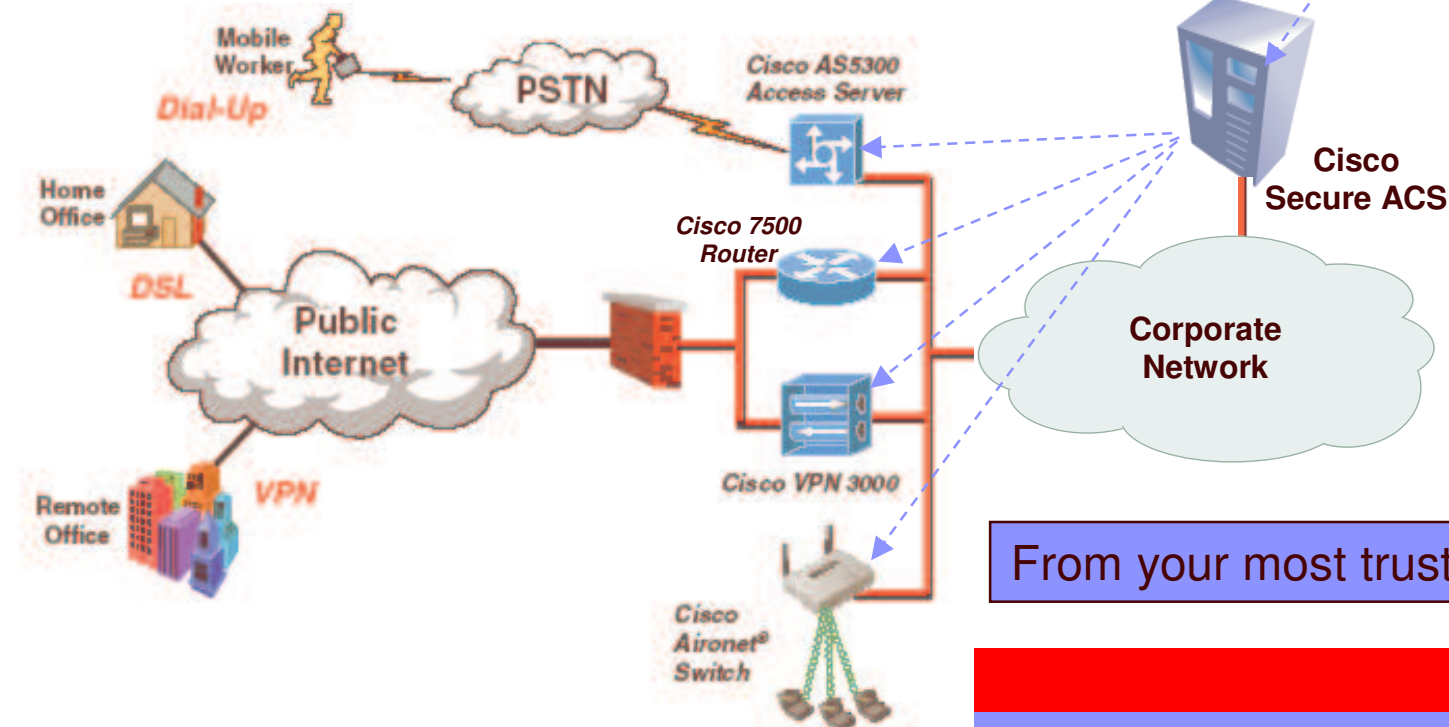
TIM can manage network identities too!

Comprehensive security spanning network, systems and application infrastructure



- Applications
 - SIEBEL
 - PeopleSoft.
 - SAP
- Databases
 - ORACLE
 - Sun microsystems
 - Teradata
 - SYBASE
- Operating Systems
 - Microsoft

Delegation for Dedicated Admins



From your most trusted partners

Proven Return on Investment



Prudential Financial – Serves institutional and individual companies worldwide with over \$590 billion in total assets under management and administration

Business Initiative:

- Automate the administration of user access rights for 65,000+ users
- Manage security of access privileges across 100's of systems
- Insure security policy enforced across enterprise in an auditable fashion for regulation compliance

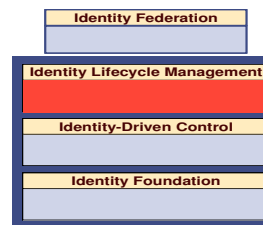
Exploiting the Power of Identity Management:

- Same staff now manages 3X the user population
- Centralized reporting to insure regulatory compliance

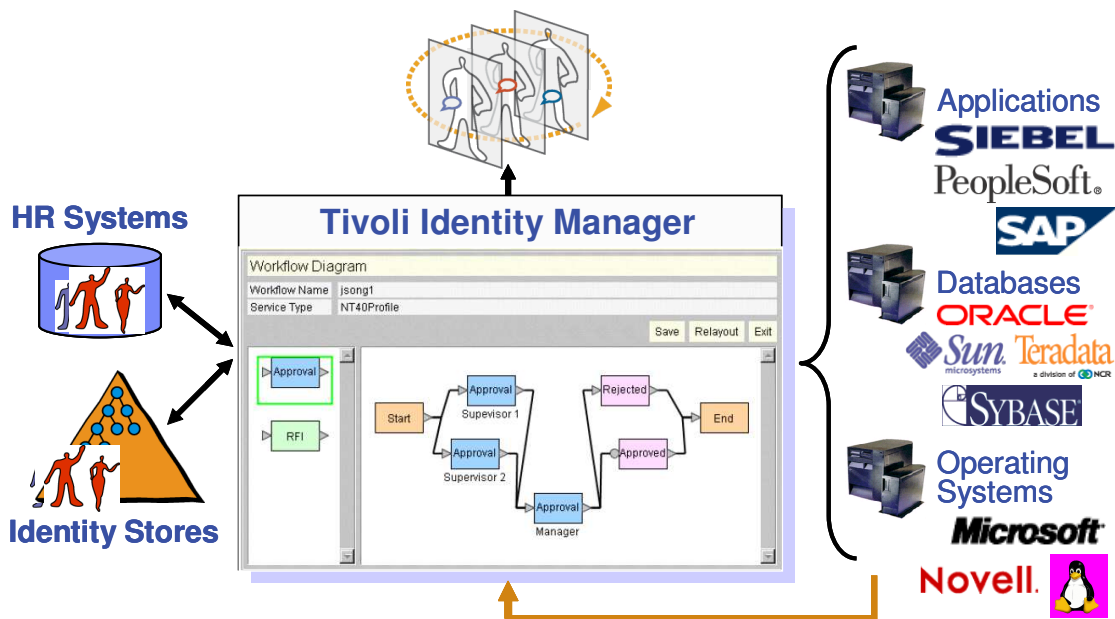
"Our manual system was expensive and cumbersome to maintain. Identity Manager [enRole] enables us to lower our administrative costs, improve our service levels, and deliver new products and tools to our customers quickly and securely," Laura Gashlin, Vice President, Information Systems for the US Consumer Group at Prudential Financial.



Tivoli Identity Manager – Functional Summary



- Password sync & self-service
- Customizable self-registration
- Security policy automation with Lifecycle Management
- Extensive workflow customizability for custom provisioning processes
- Adhoc reporting kit with third party reporting tool integration
- Extensive, open APIs for integration and extension
- Packaged with Tivoli Directory Integrator for quick creation of custom connectors and identity feeds
- Policy enforcement for proactive regulatory compliance
- Translation to nine languages for international support



Tivoli Identity Manager

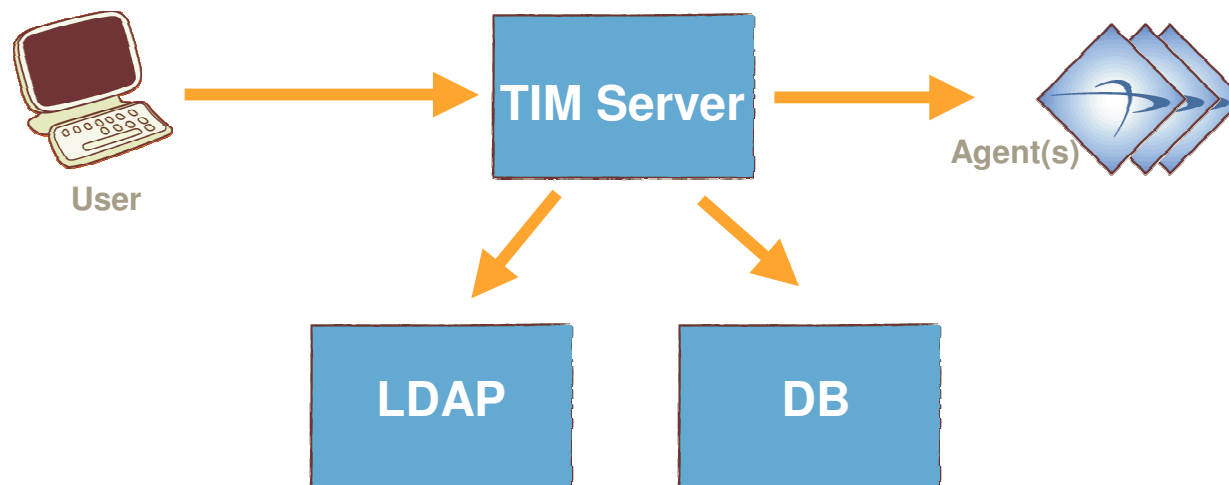
—

How does it work?



The TIM components

- TIM Server handles most operations
 - Provisioning, Workflow, Self-Service and Admin Operations
- LDAP stores all person and account information
- Database mainly stores audit information
- Agents (connectors) perform operations on target system



TIM Connector operations

- Reconcile
- Add
 - Allows custom rules
 - Out-of-the-box checks for duplicate
- Change
 - Attribute change
 - Group Membership
 - Password
- Suspend
- Delete

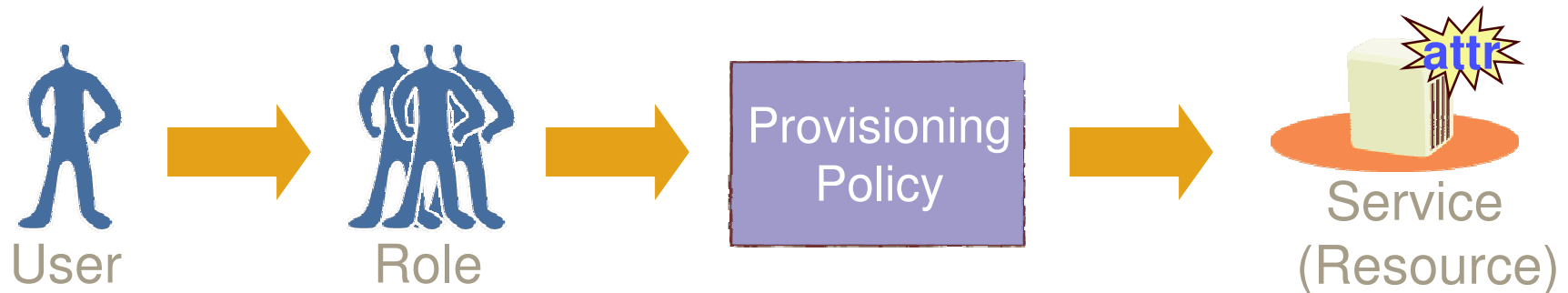


TIM Uses Roles for Easy Deployment and Administration

- A role is a collection of users with a common responsibility
- Roles are defined statically or dynamically
- Dynamic roles defined based on LDAP attribute.
- Provisioning based on role membership



The TIM Provisioning Model



- Users assigned to roles based on responsibilities
- Role members are provisioned to resource(s) via a Provisioning Policy
- Provisioning Policies can also define attributes for a user

System of Record

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `http://192.168.1.70:9080/enrole/account_list`. The page title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer".

The interface includes a navigation menu with the following items: HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, HELP, and a Logout button. The user ID is identified as "itim manager".

The main content area displays the breadcrumb "You Are Here: My Organization > Dean Martin > Account Management". Below this, there is a table with columns for "User ID", "Service Name", and "Status". The table contains two rows of data:

User ID	Service Name	Status
<input type="checkbox"/> DMartin	DivisionService	Active
<input type="checkbox"/> DMartin	ITIM Service	Active

Below the table, there are several action buttons: New, Suspend, Restore, De-Provision, Change Password, Refresh, and Cancel.

At the bottom of the page, the copyright information reads: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

UNIX/Linux Account

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL `http://192.168.1.70:9060/enrole/formviewer`. The page title is "Identity Manager Version 4.5". The navigation menu includes "HOME", "MY ORGANIZATION", "PROVISIONING", "SEARCH", "REPORT", "CONFIGURATION", and "HELP". The breadcrumb trail indicates the current path: "You Are Here: My Organization > Steve McQueen > Provision a new service".

The main content area is titled "Add | Modify Account" and features three tabs: "EMPLOYEE INFORMATION", "ACCESS INFORMATION", and "ADMINISTRATION CHOICES". The "ADMINISTRATION CHOICES" tab is active, showing the following configuration options:

- Login shell:**
- Number days before an inactive account is invalid:**
- File creation mask:**
- Home directory permissions:**

At the bottom of the form are three buttons: "Submit", "Reset", and "Cancel". The footer of the page contains the copyright notice: "© 1999-2003 IBM. ALL RIGHTS RESERVED."

RACF Account

IBM Tivoli Identity Manager - Microsoft Internet Explorer

Address: http://tintam.demopkg.ibm.com:8080/enrole/account_form_manager

Add | Modify RacfAccount

TABS: RACF USER ACCOUNT | TSO | DFP | CICS | WORK | LANGUAGE | LOGON RESTRICTIONS

User Id: AAndrews1

NAME: []

Owner: []

User Created: []

DFLTGRP: []

Connect Entry: [...]

CLAUTH: []

Data: []

SECLEVEL: []

SECLABEL: []

CATALOG: []

PASSWORDEXPIRE: []

Buttons: Submit, Reset, Cancel

Search Window:

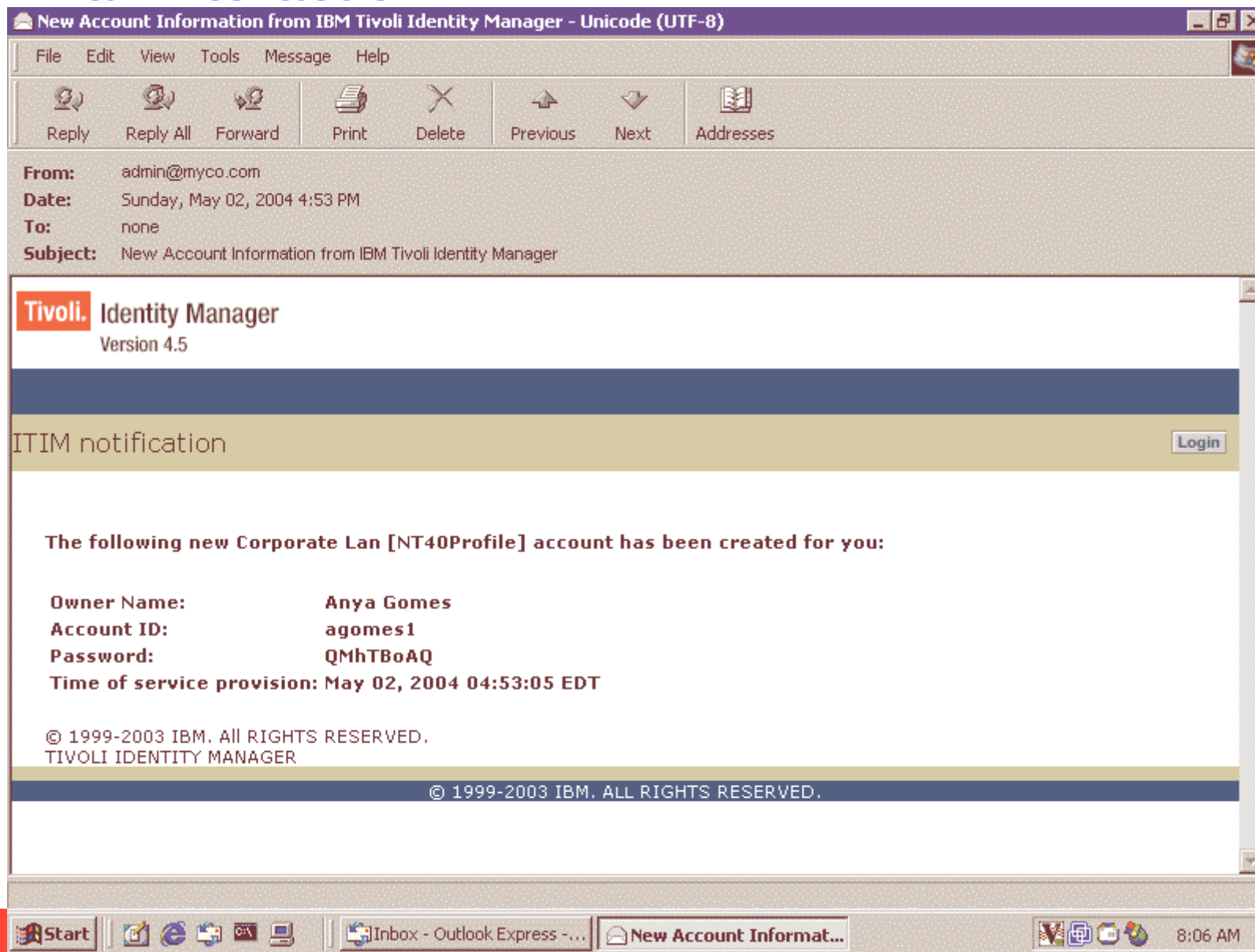
Found the following matching entry(ies).

Name	Select
<input type="checkbox"/> ADC370	
<input type="checkbox"/> ADCC370	
<input type="checkbox"/> ADCCODE	
<input type="checkbox"/> ADCLANGE	
<input type="checkbox"/> ADCPLI	
<input type="checkbox"/> ADCYCLE	
<input type="checkbox"/> ADMIN	
<input type="checkbox"/> ADPS	
<input type="checkbox"/> ADSMX	
<input type="checkbox"/> AET	

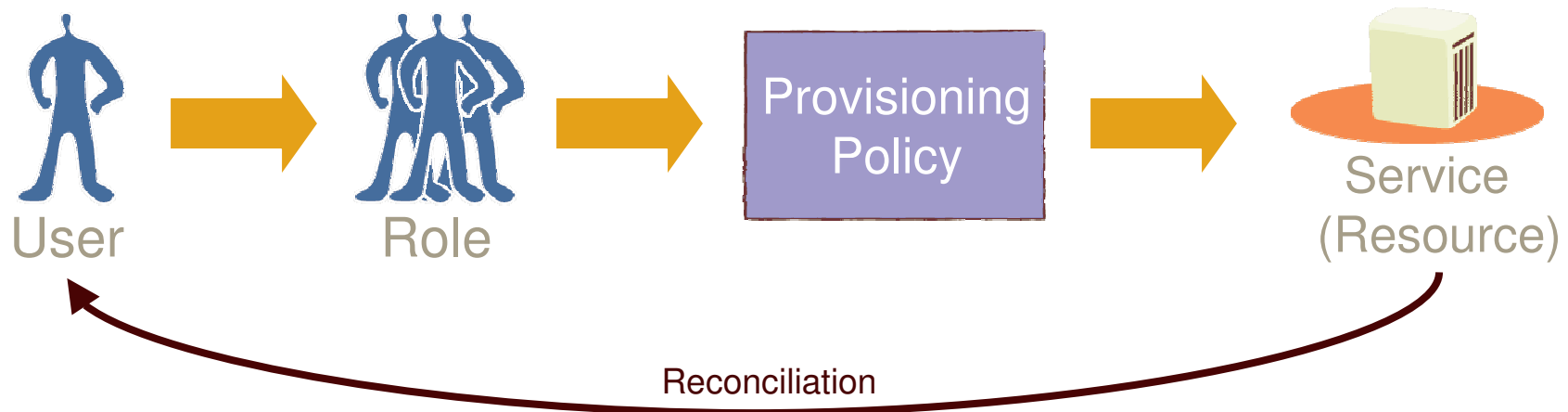
1 2 3 4 5 6 7 8 9 10 Next

Buttons: Add, Back, Done

Email interaction



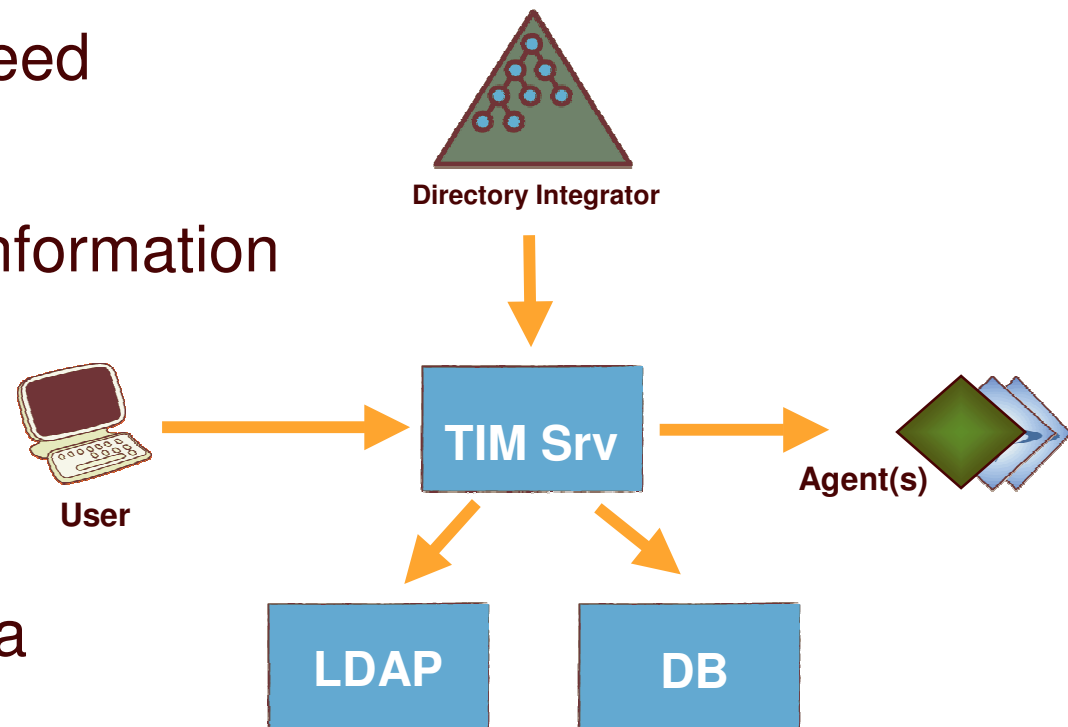
Reconciliation Compares “What Is” to “What Should Be”



- Policy enforced during reconciliation (i.e. permissions on resource)
 - TIM identifies unauthorized changes made by local admin
 - ✓ Policy determines whether to flag, notify, correct, or suspend account
- Reconciliation identifies orphan accounts
 - Adopted, suspended, restored or de-provisioned

IDI Simplifies Integration with Existing Environments

- Authoritative Identity Feed
- Bulk Loading of User Information
- Custom Agent
- Synchronization of Data
- IDI Included, but not required



Java API's Integrate with Existing Systems

Corporate Portals



Account mgmt
Password sync

Provisioning front-end application



Provisioning requests



Approvals



IVR Systems



Password resets

Opening/closing
of help desk tickets



Help Desk Systems

Tivoli Identity Manager

—

How does the RACF integration work?

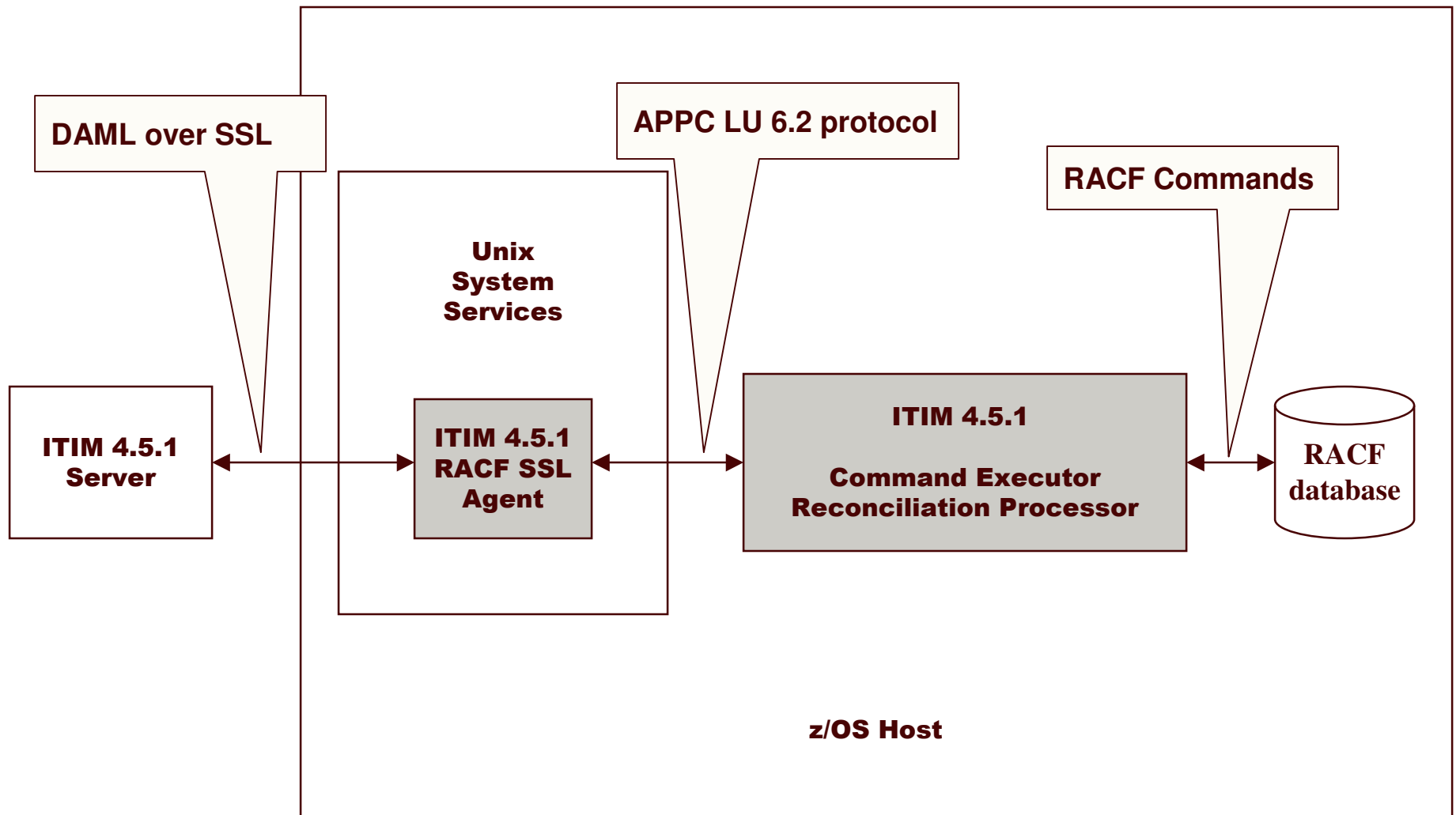


ITIM 4.5.1 RACF SSL Agent Overview

- **The ITIM 4.5.1 RACF SSL Agent performs the provisioning of RACF user accounts on your systems running the z/OS operating system**
 - ◆ **Add, Modify, Delete and Extract user account information**
- **It communicates with the ITIM 4.5.1 Server using SSL and converts Directory Access Markup language (DAML) requests from the ITIM 4.5.1 Server into RACF commands**
- **The ITIM 4.5.1 RACF SSL Agent consists of 3 components:**
 1. **Agent proper**
 2. **Command Executor**
 3. **Reconciliation Processor**



ITIM 4.5.1 RACF SSL Agent Configuration



ITIM 4.5.1 RACF SSL Agent Overview

◆ **Agent proper**

- ◆ Runs in Unix System Services
- ◆ Receives and processes requests from the ITIM 4.5.1 Server over SSL
- ◆ Sends the requests to the Command Executor over APPC
- ◆ Receives the results from the Command Executor over APPC and forwards them to the ITIM 4.5.1 Server over SSL

◆ **Command Executor**

- ◆ Runs in the APPC/MVS environment
- ◆ REXX exec that operates as an APPC/MVS transaction triggered from requests from the Agent proper

◆ **Reconciliation Processor**

- ◆ Runs in the APPC/MVS environment
- ◆ C programs that operate as an APPC/MVS transaction triggered from requests from the Agent proper - (parses IRRDBU00 output)
- ◆ Runs the RACF data base unload utility (IRRDBU00) or can be provided with an input file generated from the RACF database unload utility



ITIM RACF SSL Agent Key Install/Configuration steps

- ◆ **Install the ITIM RACF SSL Agent code**
- ◆ **Configure the ITIM Unix System Services component**
- ◆ **Configure the ITIM z/OS and APPC pieces**
- ◆ **Install certificate/key for SSL trust**
- ◆ **Insure that the ASCH and APPC started tasks are running**
- ◆ **Start the ITIM 4.5.1 RACF SSL Agent**
- ◆ **Install the ITIM 4.5.1 RACF SSL Agent profile on the ITIM 4.5.1 Server**
- ◆ **Configure the ITIM 4.5.1 Server to communicate with the ITIM 4.5.1 RACF SSL Agent and test the connection**



Create Service for ITIM 4.5.1 RACF SSL Agent

The screenshot shows the IBM Tivoli Identity Manager 4.5.1 web interface. The browser window title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer". The address bar shows "http://cptme31e/enrole/my_orgtree". The page header includes "Tivoli Identity Manager Version 4.5" and a navigation menu with "HOME", "MY ORGANIZATION", "PROVISIONING", "SEARCH", "REPORT", "CONFIGURATION", and "HELP". The user is logged in as "User ID: ITIM Manager".

The main content area displays "You Are Here: Provisioning > ACME Corporation > Service Management > Services List". A window titled "Add | Modify | Delete Service(s)" is open, showing a table of services:

Service Name	Service Type
<input type="checkbox"/> ITIM Service	ITIM
<input type="checkbox"/> Windows NT Agent on gaforghettint	NT40Profile

Below the table are "Add" and "Delete" buttons. A callout box points to the "Add" button with the text "Click on Add to create the service".

At the bottom of the page, there is a copyright notice: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

Create Service for ITIM 4.5.1 RACF SSL Agent

The screenshot shows the IBM Tivoli Identity Manager 4.5.1 web interface. The browser address bar shows `http://cptme31e/enrole/service_display`. The page title is "Identity Manager Version 4.5". The navigation menu includes HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, and HELP. The user is logged in as "User ID: ITIM Manager". The breadcrumb trail is "You Are Here: Provisioning > ACME Corporation > Service Management > Add New Service". The main content area displays a "Select Type of Service" dialog box with a "Service Type" dropdown menu set to "racf2profile". Below the dropdown are "Continue" and "Cancel" buttons, and a "Submit service profile" button. A callout box points to the "racf2profile" selection with the text "Select racf2profile for the Service Type". Another callout box points to the "Continue" button with the text "Click on Continue". The footer of the page contains copyright information: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

Create Service for ITIM 4.5.1 RACF SSL Agent

Fill in the following information for the ITIM 4.5.1 RACF SSL Agent: Service Name (optional), URL, User Id, Password, RACF ID, CA certificate store location

The URL port, User ID and Password must match what you specified when you configured the RACF SSL Agent using the agentCfg command. The CA certificate store location is the directory on the ITIM 4.5.1 server where the [a360demo.scr](#) file is located.

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer". The page content includes a breadcrumb trail: "You Are Here: Provisioning > ACME Corporation > Service Management > Add New Service". The main form is titled "Add | Modify Service" and contains the following fields:

Service Name	RACF SSL Agent on z/OS machine NMP200
URL	https://nmp200.tivlab.raleigh.ibm.com:45580
User Id	agent
Password	*****
RACF ID under which requests will be processed	
CA certificate store location	d:\itim45\cert
Certificate file location	
Private key file location	
Owner	
Service Prerequisite	

At the bottom of the form are buttons for "Submit", "Reset", "Test", and "Cancel". A mouse cursor is hovering over the "Test" button, and a tooltip labeled "Test service" is visible. A callout box points to the "Test" button with the text: "Click on Test to test the connection between the ITIM 4.5 Server and the RACF SSL Agent." The footer of the page contains the copyright notice "© 1999-2003 IBM. ALL RIGHTS RESERVED." and the text "Local intranet".

Click on Test to test the connection between the ITIM 4.5 Server and the RACF SSL Agent.

Test Service for ITIM 4.5.1 RACF SSL Agent

The screenshot shows the IBM Tivoli Identity Manager 4.5.1 web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `http://cptme31e/enrole/formviewer?testAgent=true`. The page title is "Identity Manager Version 4.5". The navigation menu includes: HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, HELP. The user is logged in as "User ID: ITIM Manag".

The main content area displays "You Are Here: Provisioning > ACME Corporation > Service Management > Add New Service". The "Add | Modify Service" form is visible with the following fields:

- Service Name: RACF SSL Agent on z/OS machine NMP200
- URL: https://nmp200.tivlab.raleigh.ibm.com:45580
- User Id: agent
- Password: *****
- RACF ID under which requests will be processed: [Empty]
- CA certificate store location: d:\itim45\cert
- Certificate file location: [Empty]
- Private key file location: [Empty]

At the bottom of the form are buttons for "Submit", "Reset", "Test", and "Cancel". A "Test Successful" dialog box is overlaid on the form, containing the text "Test Successful" and two "Done" buttons. The status bar at the bottom of the browser shows "Local intranet".

Create Service for ITIM 4.5.1 RACF SSL Agent

The screenshot displays the IBM Tivoli Identity Manager 4.5.1 web interface. The browser title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer". The address bar shows the URL: `http://cptme31e/enrole/formviewer?testAgent=true`. The page header includes the Tivoli logo, "Identity Manager Version 4.5", and navigation tabs: HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, HELP. The user is logged in as "User ID: ITIM Manage".

The main content area shows the breadcrumb path: "You Are Here: Provisioning > ACME Corporation > Service Management > Add New Service". The form is titled "Add | Modify Service" and contains the following fields:

- Service Name: RACF SSL Agent on z/OS machine NMP200
- URL: `https://nmp200.tivlab.raleigh.ibm.com:45580`
- User Id: agent
- Password: *****
- RACF ID under which requests will be processed: [Empty]
- CA certificate store location: d:\itim45\cert
- Certificate file location: [Empty]
- Owner: [Empty]
- Service Prerequisite: [Empty]

Buttons for "Search" and "Clear" are present next to the Owner and Service Prerequisite fields. At the bottom of the form are buttons for "Submit", "Reset", "Test", and "Cancel". A callout box with the text "Click on Submit to create the service" points to the "Submit" button.

© 1999-2003 IBM. ALL RIGHTS RESERVED.

Local Intranet

Create Service for ITIM 4.5.1 RACF SSL Agent

IBM Tivoli Identity Manager - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://cptme31e/enrole/formvalidator0

Identity Manager Version 4.5

HOME | MY ORGANIZATION | PROVISIONING | SEARCH | REPORT | CONFIGURATION | HELP | Logout

User ID: ITIM Manager

You Are Here: Provisioning > ACME Corporation > Service Management > Services List

Manage Services

Manage ITIM Groups

Define Provisioning Policies

Design Workflow

Define Service Selection Policies

Define Identity Policies

Define Password Policies

Control Access

Manage Admin Domains

Add | Modify | Delete Service(s)

Service Name	Service Type
<input type="checkbox"/> ITIM Service	ITIM
<input type="checkbox"/> RACF SSL Agent on z/OS machine NMP200	racf2profile
<input type="checkbox"/> Windows NT Agent on gaforghettint	NT40Profile

Add Delete

RACF SSL Agent Service created

© 1999-2003 IBM. ALL RIGHTS RESERVED.
TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147

Done Local Intranet

Once installation and configuration of the ITIM Agent is complete, you are almost done.

But, before creating or deleting users, you must first:

- ✓ **Create a provisioning policy**
- ✓ **Perform a reconciliation.**



Create Provisioning Policy for RACF Accounts

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `http://cptne31e.raleigh.ibm.com/enrole/provisioning_policy_list`. The page title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer".

The application header includes the Tivoli logo, "Identity Manager Version 4.5", and a navigation menu with tabs: HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, HELP. A "Logout" link is visible in the top right. The user ID is "User ID: ITIM Manager".

The main content area displays "You Are Here: ACME Corporation > Provisioning Policies". Below this is a section titled "Add | Modify | Delete Provisioning Policies" with a table of existing policies:

Policy Name	Caption	Status	Policy Priority
<input type="checkbox"/> Default provisioning policy for ITIM	ITIM account policy	Enabled	10000000
<input type="checkbox"/> Provisioning Policy for RACF Accounts	RACF Account Policy	Enabled	1

Below the table are buttons for "Add", "Delete", and "Refresh".

The footer of the application contains the text: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

Perform a reconciliation

The screenshot shows the IBM Tivoli Identity Manager 4.5 web interface. The browser window title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer". The address bar shows the URL: `http://cptme31e.raleigh.ibm.com/enrole/my_orgtree`. The page header includes the Tivoli Identity Manager logo and version 4.5, along with navigation tabs: HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, and HELP. A "Logout" button is visible in the top right. The user ID is identified as "ITIM Manager".

The main content area displays a breadcrumb trail: "You Are Here: Provisioning > ACME Corporation > Service Management > Services List". Below this, there is a section titled "Add | Modify | Delete Service(s)". A table lists the services to be reconciled:

Service Name	Service Type
<input type="checkbox"/> ITIM Service	ITIM
<input type="checkbox"/> RACF SSL Agent on z/OS machine NMP200	racf2profile

Below the table are "Add" and "Delete" buttons. A mouse cursor is hovering over the "Delete" button for the "RACF SSL Agent on z/OS machine NMP200" service. The left sidebar contains various management options such as "Manage Services", "Manage ITIM Groups", "Define Provisioning Policies", "Design Workflow", "Define Service Selection Policies", "Define Identity Policies", "Define Password Policies", "Control Access", and "Manage Admin Domains".

At the bottom of the page, there is a copyright notice: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147". The status bar at the very bottom shows a JavaScript command: `javascript:submitServiceSubMenu(document.forms["body"],'service_submenu','RACF SSL Agent on z/OS machine NMP200','erglobalid=16`.

Perform a reconciliation

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer" and the address bar shows "http://cptme31e.raleigh.ibm.com/enrole/service_submenu".

The page header includes the "Tivoli Identity Manager Version 4.5" logo and an IBM logo. A navigation menu contains links for HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, and HELP. A "Logout" button is visible in the top right corner. The user ID is identified as "ITIM Manager".

The breadcrumb trail reads: "You Are Here: Provisioning > ACME Corporation > Service Management > Service Submenu".

The main content area is titled "Select an option" and displays the following menu items:

- + Identity Manager Home
- + ACME Corporation
- RACF SSL Agent on z/OS machine NMP200 Menu
 - ▶ Detailed Information
 - ▶ Reconciliation
 - ▶ Accounts
 - ▶ Orphan Accounts
 - ▶ Policy Enforcement
- Back to list of services

The left sidebar contains various management options: Manage Services, Manage ITIM Groups, Provisioning Policies, Design Workflow, Define Service Selection Policies, Define Identity Policies, Define Password Policies, Control Access, and Manage Admin Domains.

At the bottom of the page, there is a copyright notice: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

Verify reconciliation completed

The screenshot displays the IBM Tivoli Identity Manager web interface within a Microsoft Internet Explorer browser window. The browser's address bar shows the URL: `http://cptme31e.raleigh.ibm.com/enrole/reqdetail?Tab=General`. The page title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer".

The application header includes the "Tivoli Identity Manager Version 4.5" logo and a navigation menu with links for HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, and HELP. A "Logout" button is visible in the top right corner. The user is identified as "User ID: ITIM Manager".

The breadcrumb trail indicates the current location: "You Are Here: Home > Completed Requests > Request Details".

The main content area is titled "Request Header" and contains a tabbed interface with three tabs: GENERAL, DATA, and AUDIT LOG. The "GENERAL" tab is active, displaying the following request details:

Field	Value
Request Id	1746333137430432630
Requestor	System Administrator
Requestee	
Subject	RACF SSL Agent on z/OS machine NMP200
Process Type	Reconciliation
Description	Reconciliation process
Time Submitted	Mar 29, 2004 3:07:54 PM
Time Scheduled	Mar 29, 2004 3:07:54 PM
Last Modified	Mar 29, 2004 3:07:54 PM
Status	Success
Time Started	Mar 29, 2004 3:07:55 PM
Time Completed	Mar 29, 2004 3:07:59 PM

A "Cancel" button is located at the bottom left of the request details area.

The footer of the page contains the copyright information: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

After reconciliation now have RACF data

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `http://cptne31e.raleigh.ibm.com/enrole/account_list`. The page title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer". The interface includes a navigation menu with options like HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, and HELP. The current page is "Account Management" under the "PROVISIONING" tab. The user is logged in as "User ID: ITIM Manager".

The main content area displays a table of user accounts with the following columns: **User ID**, **Owner**, and **Status**. The table contains the following data:

<input type="checkbox"/>	User ID	Owner	Status
<input type="checkbox"/>	ASCR1		Active
<input type="checkbox"/>	ASSR1		Active
<input type="checkbox"/>	BL		Active
<input type="checkbox"/>	BUSHICK		Active
<input type="checkbox"/>	CLINARD		Active
<input type="checkbox"/>	GARYF		Active
<input type="checkbox"/>	? IBMUSER		Active
<input type="checkbox"/>	? ITIAGNT		Active
<input type="checkbox"/>	LAUFMAN		Active
<input type="checkbox"/>	MOLLY		Active

Below the table, there are buttons for "Suspend", "Restore", "De-Provision", "Orphan", "Refresh", and "Cancel". At the bottom of the table area, there are page navigation links: "1 2 3 Next".

At the bottom of the page, the copyright information reads: "© 1999-2003 IBM, ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

Create a new account (user ID)



Create a new account

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `http://cptme31e.raleigh.ibm.com/enrole/account_list`. The page title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer".

The interface includes a navigation menu with the following items: HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, HELP. A "Logout" button is visible in the top right corner. The user is logged in as "User ID: ITIM Manager".

The main content area displays a breadcrumb trail: "You Are Here: My Organization > Gary Forghetti > Account Management". Below this, there are several management options: "Manage People", "Organizational Roles", "Control Access", "Manage Organizations", "Manage Locations", "Manage Organizational Units", and "Manage Business Partners".

The central part of the interface shows a table with the following columns: "User ID", "Service Name", and "Status". A single row is visible with the following data:

User ID	Service Name	Status
GForghetti	ITIM Service	Active

Below the table, there are several action buttons: "New", "Suspend", "Restore", "De-Provision", "Change Password", "Refresh", and "Cancel". A tooltip is visible over the "New" button, displaying the text "Provision new service".

At the bottom of the page, there is a copyright notice: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

Create a new account

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer". The address bar shows the URL: `http://cptme31e.raleigh.ibm.com/enrole/account_provision`. The page header includes the Tivoli Identity Manager logo (Version 4.5) and a navigation menu with links for HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, and HELP. A "Logout" button is visible in the top right. The user is identified as "User ID: ITIM Manager".

The main content area shows a breadcrumb trail: "You Are Here: My Organization > Gary Forghetti > Provision Service". A "Select a Service" dialog box is open, displaying a list of services:

Service Name
<input type="radio"/> ITIM Service
<input checked="" type="radio"/> RACF SSL Agent on z/OS machine NMP200

Below the list are "Continue" and "Cancel" buttons. A mouse cursor is hovering over the "Continue" button, which has a tooltip that reads "Continue provisioning service".

The footer of the page contains the copyright notice: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147". The browser status bar shows the JavaScript code: `javascript:submitAccountProvisionAction(document.forms["body"], 'account_form_manager', 'ACCOUNT_PROVISION_ACTION', '');` and the "Internet" icon.

Create a new account

The screenshot shows the IBM Tivoli Identity Manager web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `http://cptne31e.raleigh.ibm.com/enrole/account_form_manager`. The page title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer".

The interface includes a navigation menu on the left with options like "Manage People", "Organizational Roles", "Control Access", "Manage Organizations", "Manage Locations", "Organizational Units", and "Business Partners". The main content area is titled "Add | Modify Account" and features a tabbed interface with various account attributes.

The "Add | Modify Account" form includes the following fields and options:

- RACF ACCOUNT** (selected tab)
- LOGON RESTRICTIONS**
- TSO**
- CICS**
- OMVS**
- WORK ATTRIBUTES**
- DFP**
- LANG**
- DCE**
- CLASS AUTH**
- NETVIEW**
- KERB**
- OPER PARM**
- LOTUS NOTES**

Form fields and values:

- User Id:** gforghet
- Name:** Gary Forghetti
- Default Group:** OMVS (with Search and Clear buttons)
- Owner:** SYS1 (with Search and Clear buttons)
- Connect Groups:** [...]
- Installation Data:** [Empty text box]
- Creation Date:** 3 / 29 / 2004
- Last logon time:** 3 / 29 / 2004 15:00
- Last password change date:** 3 / 29 / 2004
- Password change interval:** [Empty text box]
- System Special?:**
- System Auditor?:**
- System Operations?:**
- Protected?:**
- Restricted?:**
- Full User Auditing?:**
- Group Access for new resource profiles?:**

Buttons at the bottom of the form: Submit, Reset, Cancel. A mouse cursor is hovering over the Submit button.

Gary now has a RACF account

The screenshot shows the IBM Tivoli Identity Manager 4.5 web interface in a Microsoft Internet Explorer browser. The address bar shows the URL: `http://cptme31e.raleigh.ibm.com/enrole/account_list`. The page title is "IBM Tivoli Identity Manager - Microsoft Internet Explorer".

The interface includes a navigation menu with options: HOME, MY ORGANIZATION, PROVISIONING, SEARCH, REPORT, CONFIGURATION, HELP. The user is logged in as "User ID: ITIM Manager".

The main content area displays "You Are Here: My Organization > Gary Forghetti > Account Management". Below this, there is a table titled "Provision | De-Provision | Modify | Suspend | Restore Accounts" with the following data:

	User ID	Service Name	Status
<input type="checkbox"/>	gforghet	RACF SSL Agent on z/OS machine NMP200	Active
<input type="checkbox"/>	GForghetti	ITIM Service	Active

Below the table are several action buttons: New, Suspend, Restore, De-Provision, Change Password, Refresh, and Cancel.

At the bottom of the page, there is a copyright notice: "© 1999-2003 IBM. ALL RIGHTS RESERVED. TIVOLI IDENTITY MANAGER 4.5.1 BUILD 5147".

The new account can be verified on RACF

```
Session B - [43 x 80]
File Edit View Communication Actions Window Help
[Icons]
READY
lu gforghet
USER=GFORGHET  NAME=GARY FORGHETTI  OWNER=SYS1  CREATED=04.089
DEFAULT-GROUP=OMVS  PASSDATE=00.000  PASS-INTERVAL= 30
ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
LAST-ACCESS=04.089/15:24:21
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED  (DAYS)  (TIME)
-----
ANYDAY  ANYTIME
GROUP=OMVS  AUTH=USE  CONNECT-OWNER=SYS1  CONNECT-DATE=04.089
CONNECTS= 00  UACC=NONE  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
READY

MA b 24/001
Connected to remote server/host ralnvr.raleigh.ibm.com using port 23
```

Verify that the RACF user ID has been created. Logon to TSO and issue the RACF LU command for the new RACF user ID to verify that it was created – **LU *user_ID***

Etc., etc., etc.

- **You can now:**
 - ✓ **Delete users**
 - ✓ **Modify users**
 - ✓ **Modify or add segments**
 - ✓ **Incorporate HR feeds that trigger such actions**
 - ✓ **Incorporate Workflows for approval processing**
 - ✓ **Etc.**



Important manuals

- For complete install and configuration details refer to the **IBM Tivoli Identity Manager RACF SSL Agent Installation and Configuration Guide (SC32-1490-06)**
- Refer to the ***OS/390 V1R2.0 MVS Planning: APPC/MVS Management (GC28-1807-01)*** manual for more info on **APPC/MVS**



A Few Thoughts in Closing

IBM can help you protect, store, retain and comply to regulations, while at the same time helps you run your business more effectively

- Helps comply with government & business regulations, including Sarbanes-Oxley
- Automate IT processes and enhance the risk management program
- Retention and preservation of key business data
- Helps establish a compliance framework to address existing and potential new regulations

We deliver an end-to-end identity management approach to help you address compliance issues, while delivering business value through process automation

