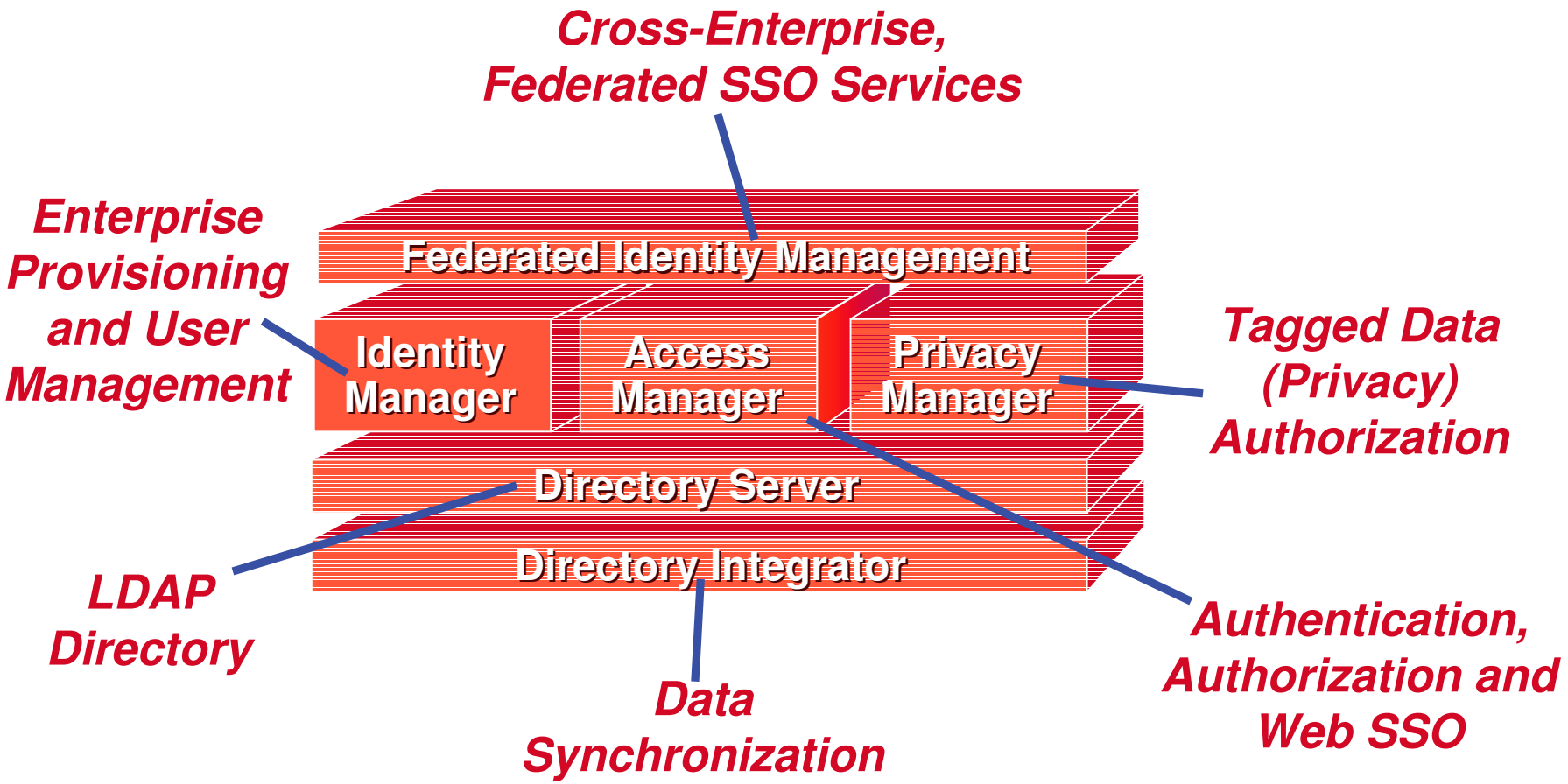
Automating User Provisioning
with
Tivoli Identity Manager (TIM)

Leveraging knowledge of people to create business value

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

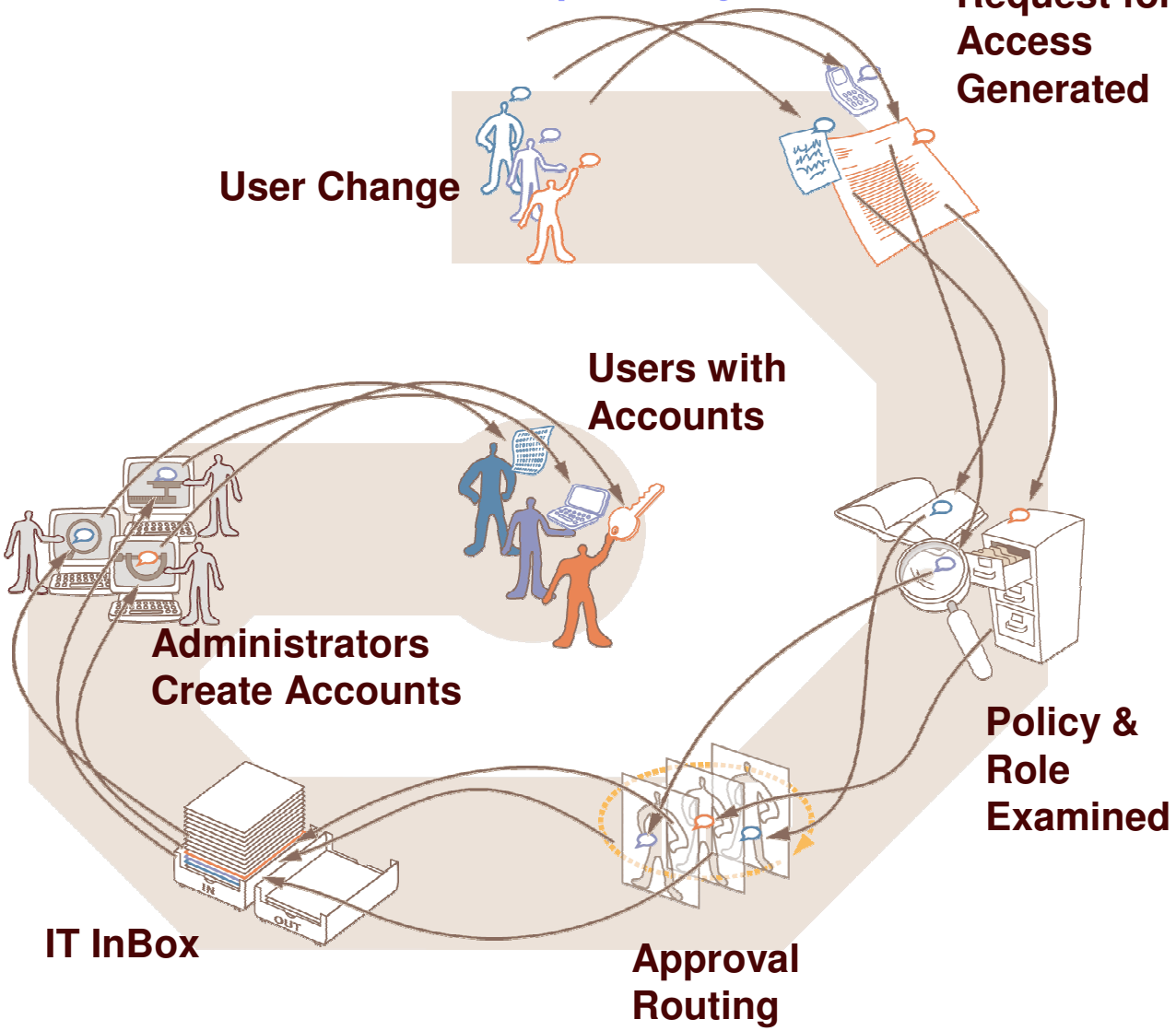
e business software

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:	▪ **Discovered 900 former brokers who still had accounts active** ▪ **Discovered 1 of these brokers had been accessing customer accounts internally…**

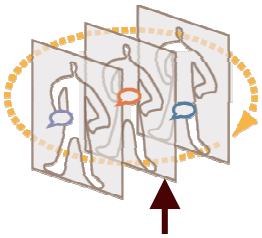
User Provisioning Controls Access Privileges

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

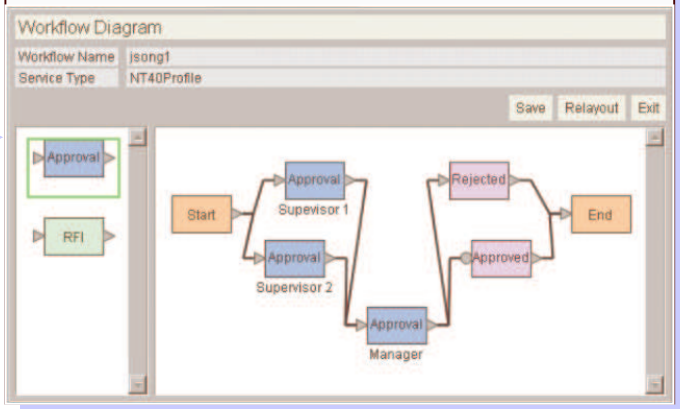
Enterprise Identity Needs

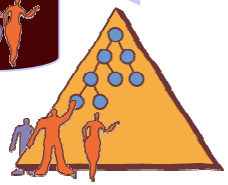
Identity change (add/del/mod) → Access policy evaluated → Approvals gathered → Accounts updated

Detect and correct local privilege settings



TIM

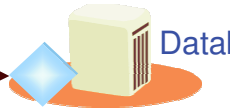




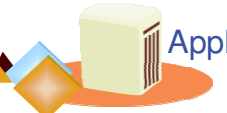
HR Systems/ Identity Stores

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

Operating Systems



Databases



Applications

Now Network Identities Too!

Password Management

Reduce costs in the helpdesk

User self-service of passwords across all systems

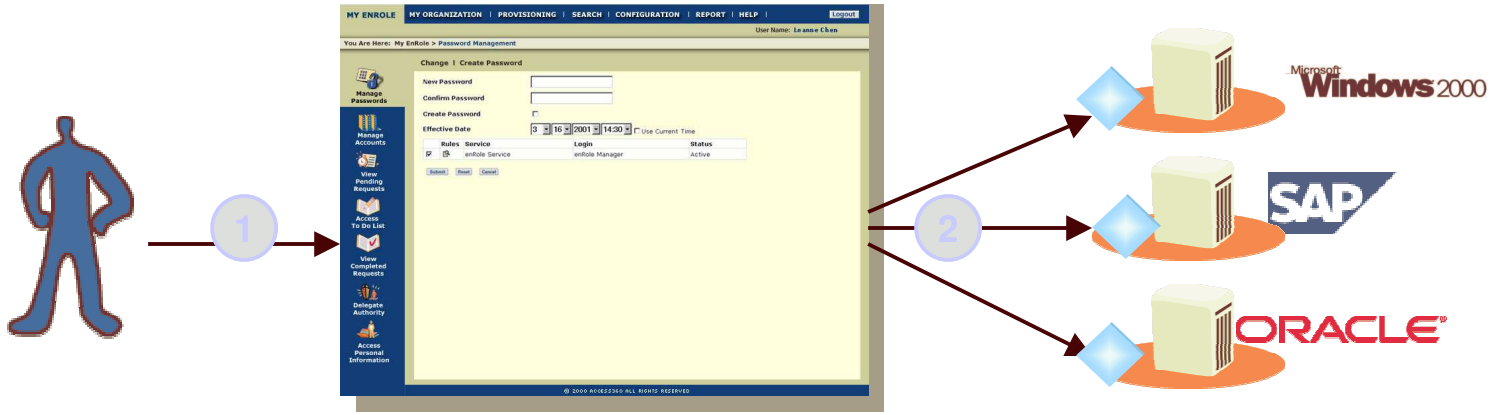
Password Rule Checking

- **Verifies compliance with target requirements**
- **Add rules across all resources**

Challenge-Response system for forgotten passwords

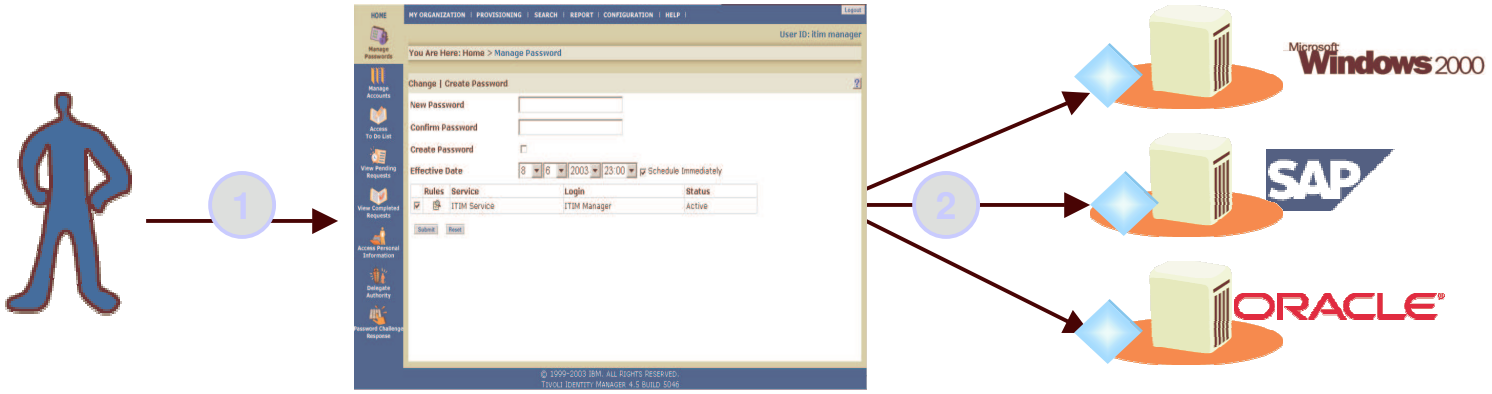
Help Desk costs $20-per-call for password resets
Gartner Group

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



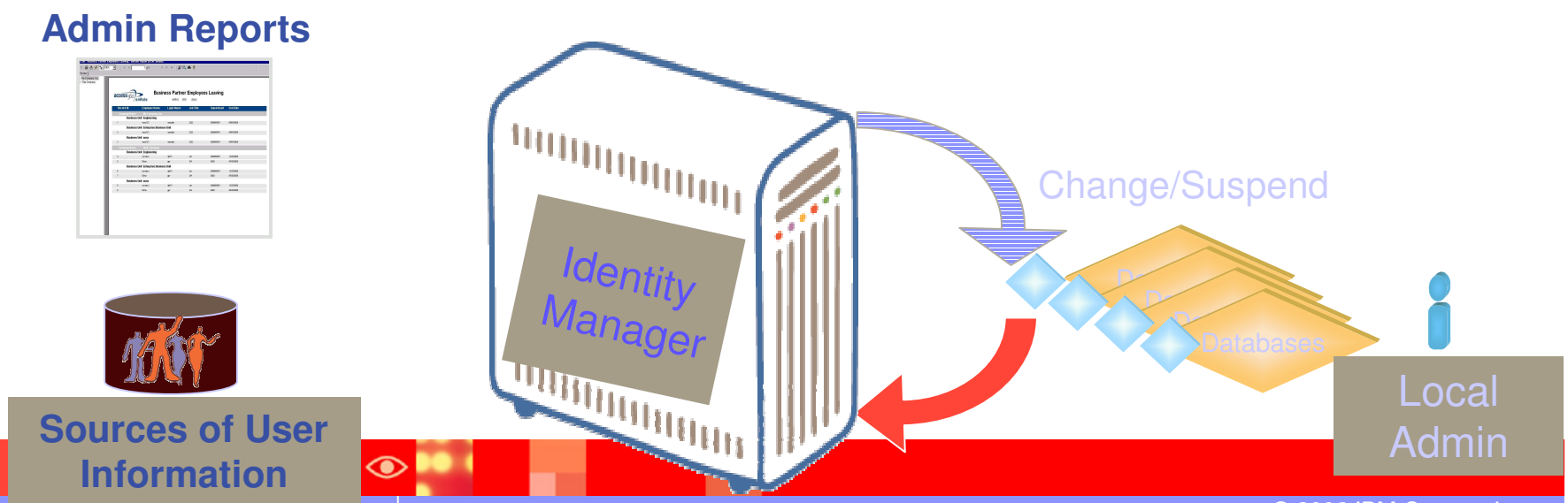
Self Service Reduces Help Desk Calls

- 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



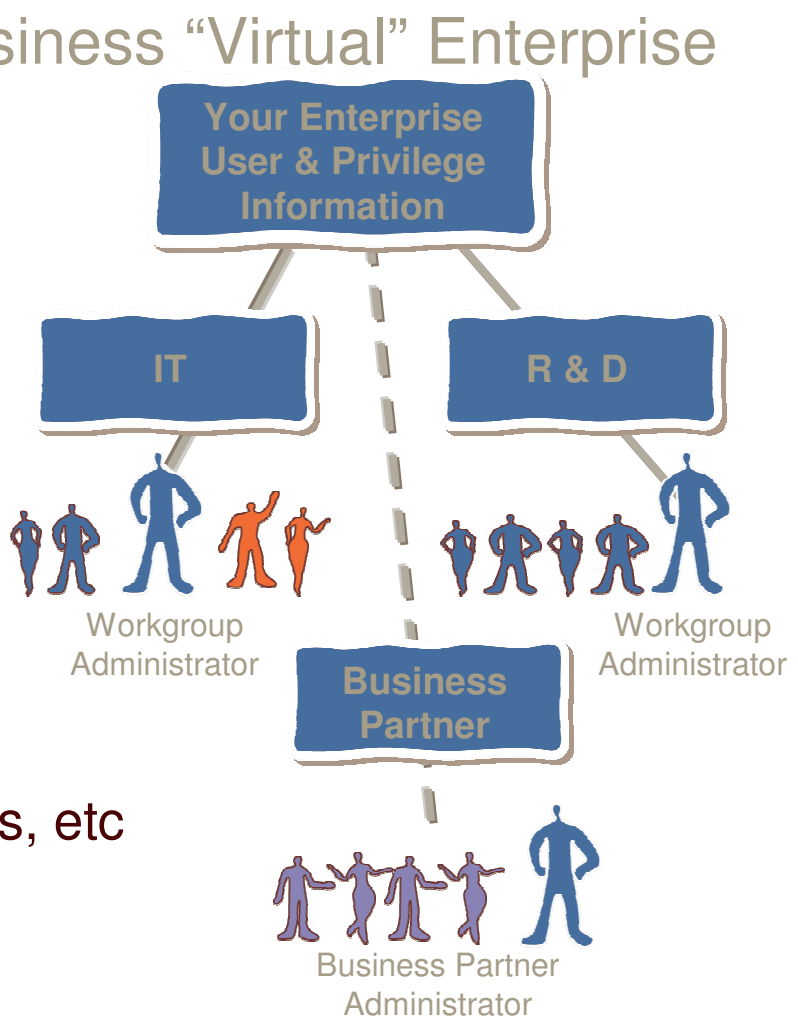
Access Rights Accountability

- 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



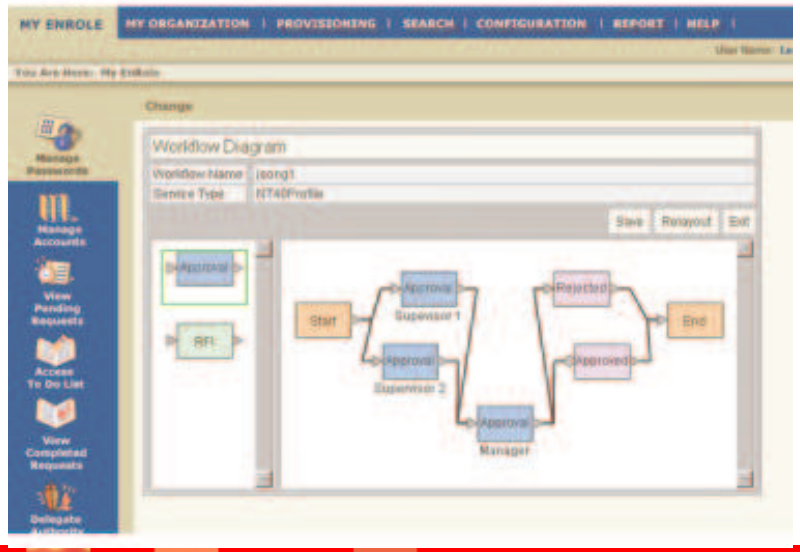
Delegated Administration Reduces Admin Overhead

- "Junior" administrators can control people and attributes
- Can restrict internal TIM resources
  - Services, Provisioning Policies, Reports, etc

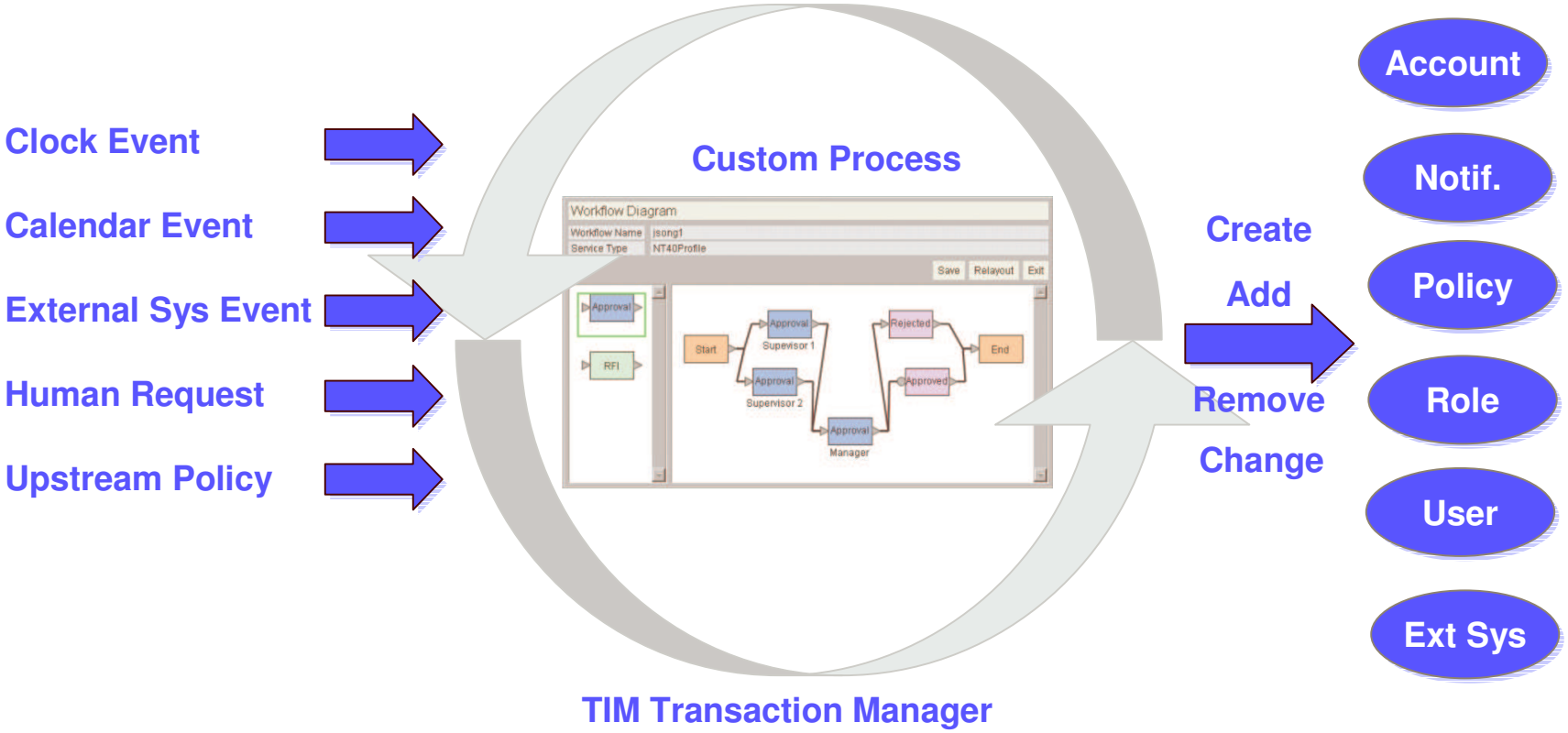


Access Request Approval Automation

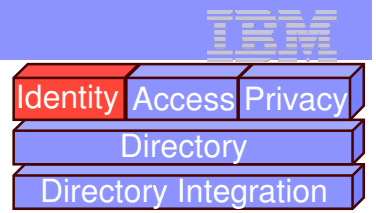
- Reduce elapsed time to establish and remove accounts.
- Decrease administrative burden.
  - Pain point with large majority of our clients
- Automate delegated or centralized approval and decision-making processes.
- Reduce mundane data-entry tasks.

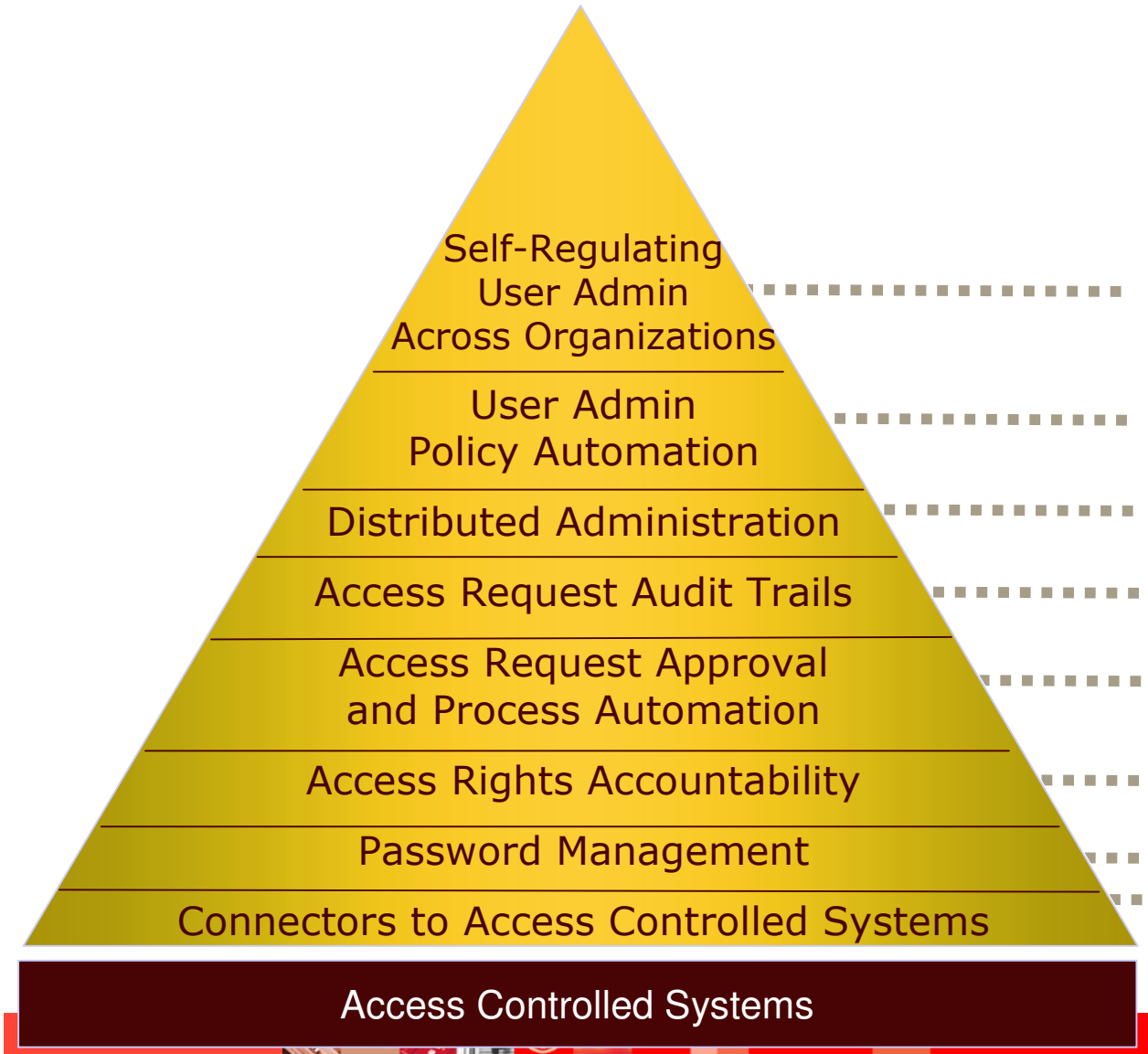


Identity Lifecycle Creation and Management



Provisioning Value Pyramid





Extend security automation to business partners

Enforce security policies proactively, automate based on roles and rules

Manage distributed sets of users

Ease support of security audits

Cut elapsed turn-on time, automate routine admin tasks, eliminate errors

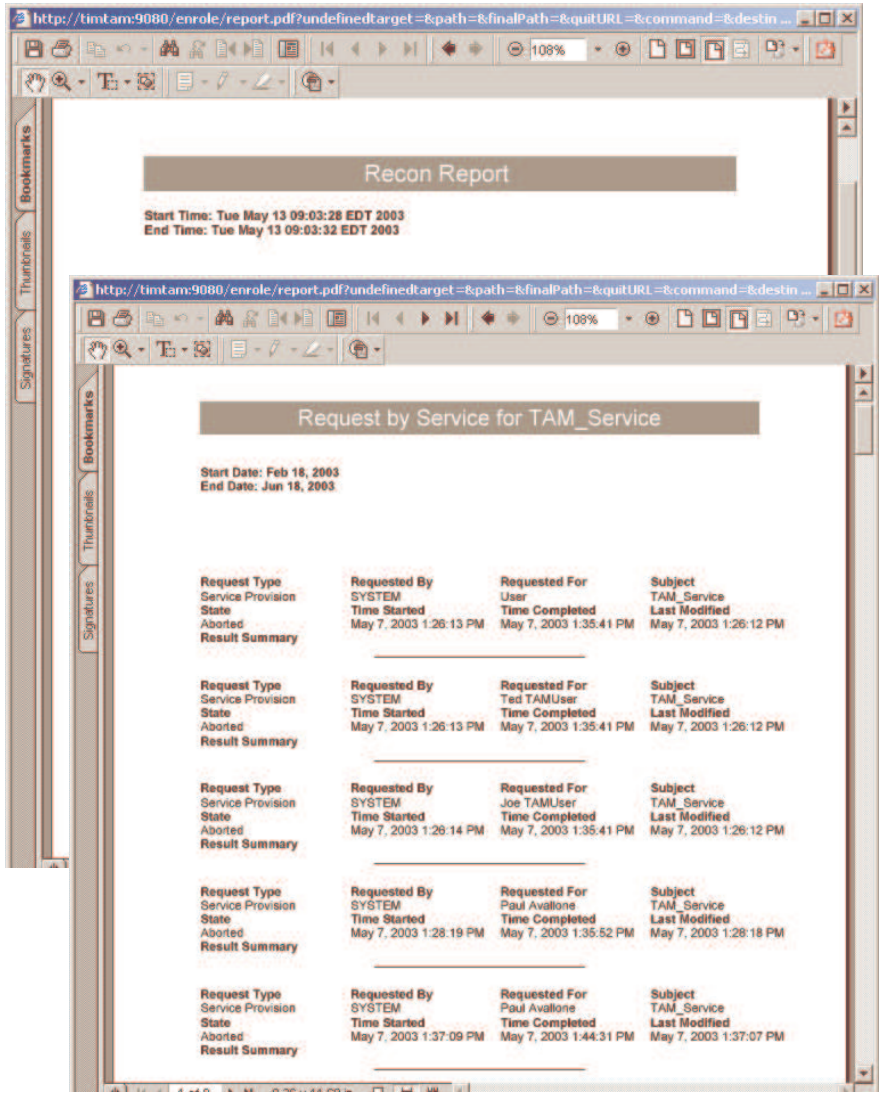
Eliminate backdoors, know who has access to what

Reduce helpdesk load by up to 40%

Administer web and legacy environments consistently

TIM Reporting Tools and 3rd Party Integration

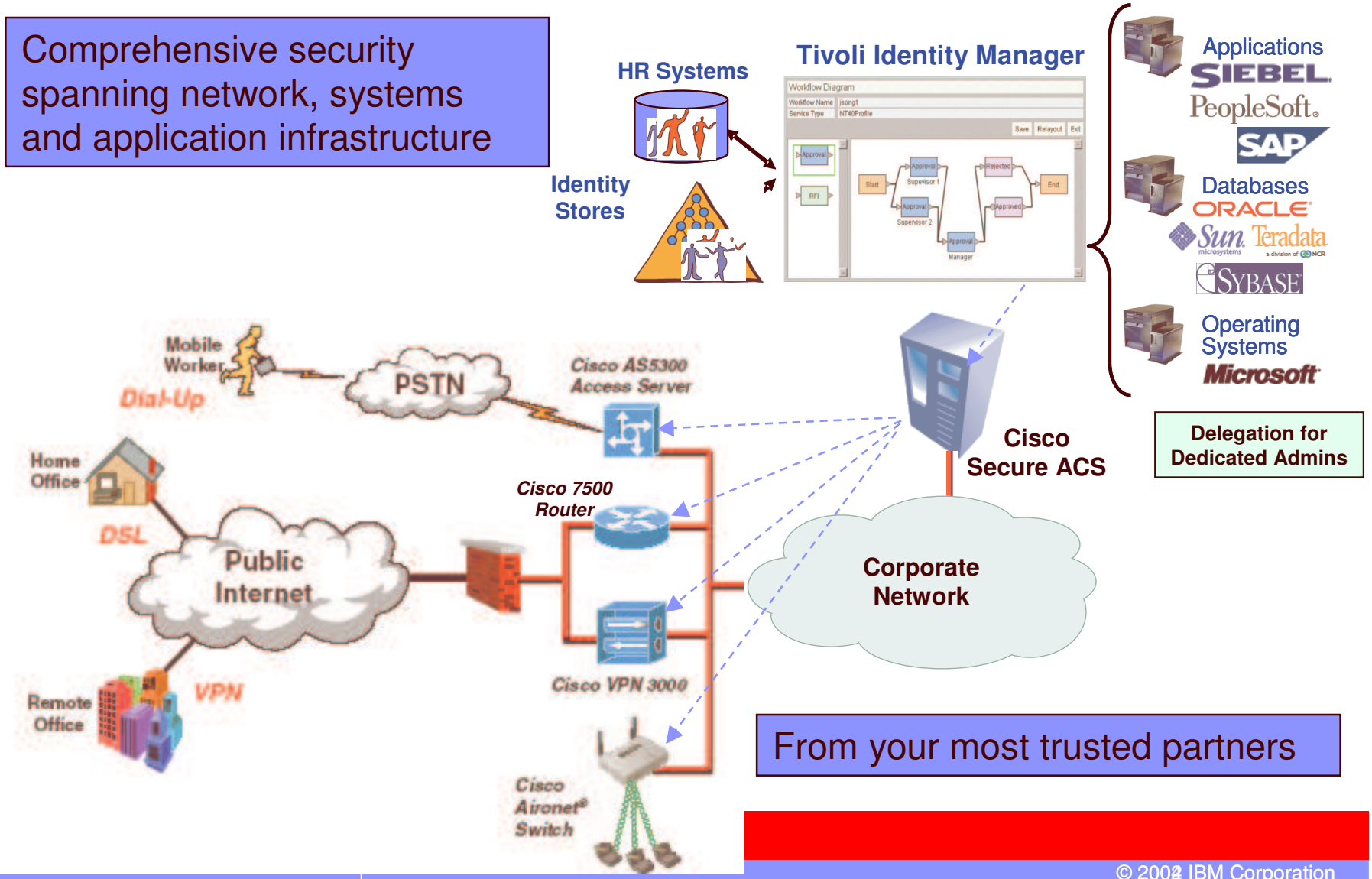
- Default and Custom Reports
- Access Control over Report Info
- Acrobat Format for Easy Viewing
- Crystal/Actuate Reports



IBM and Cisco: Teamed to reduce operating costs

TIM can manage network identities too!

Comprehensive security spanning network, systems and application infrastructure



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:

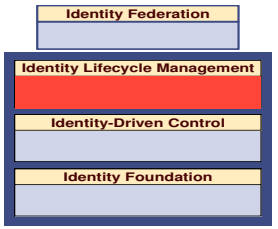
- Automate the administration of user access rights for 65,000+ users
- Manage security of access privileges across 100's of systems
- Insure security policy enforced across enterprise in an auditable fashion for regulation compliance

Exploiting the Power of Identity Management:

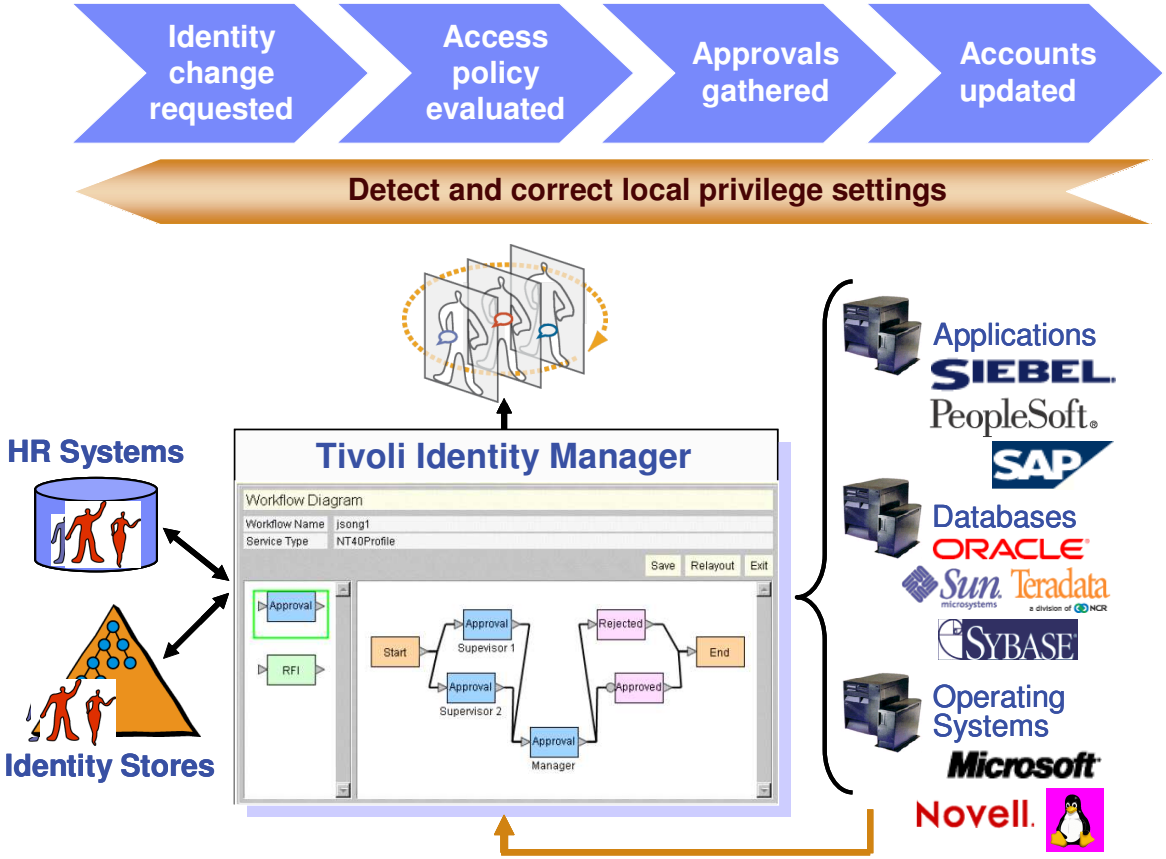
- Same staff now manages 3X the user population
- Centralized reporting to insure regulatory compliance

"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



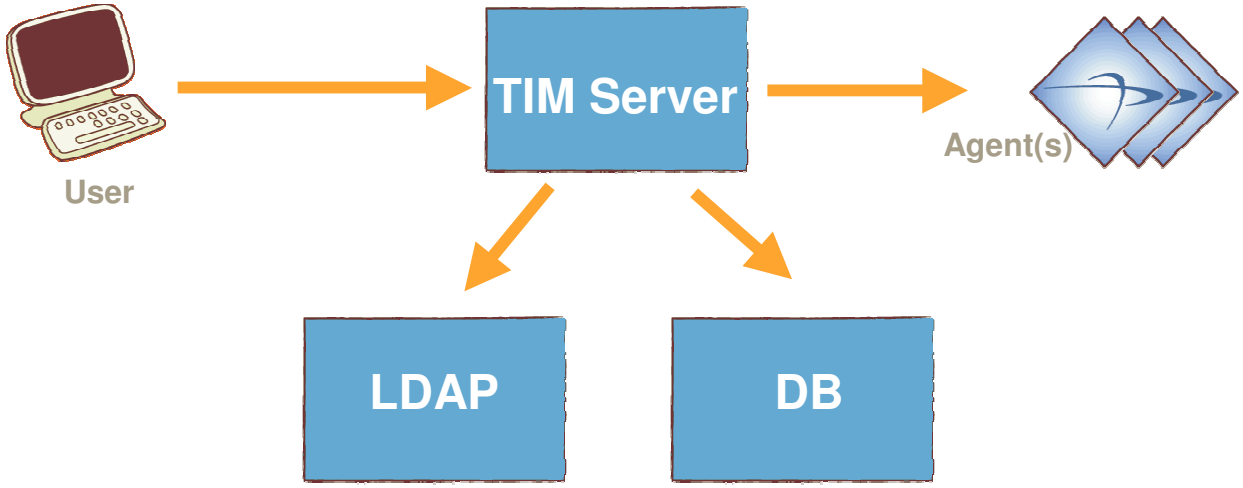
- **Password sync & self-service**
- **Customizable self-registration**
- Security policy automation with **Lifecycle Management**
- **Extensive workflow** customizability for custom provisioning processes
- **Adhoc reporting** kit with third party reporting tool integration
- **Extensive, open APIs** 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



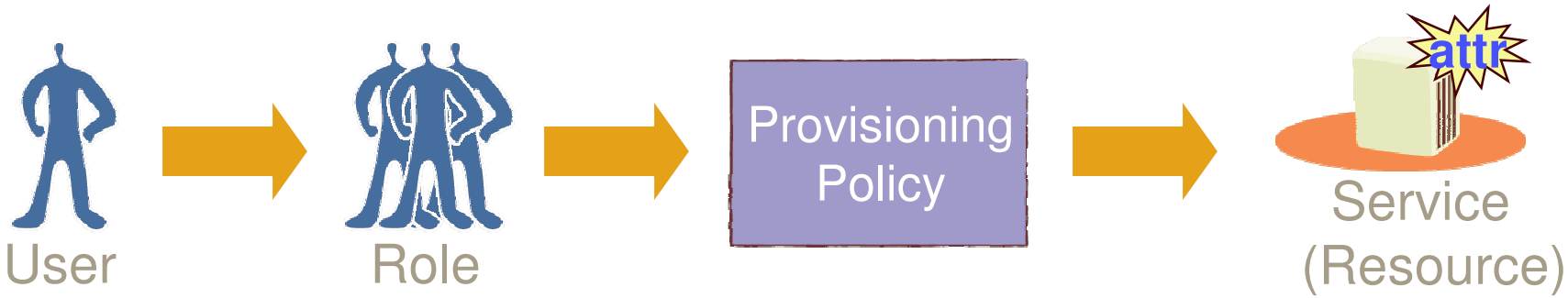
TIM Connector operations

- 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

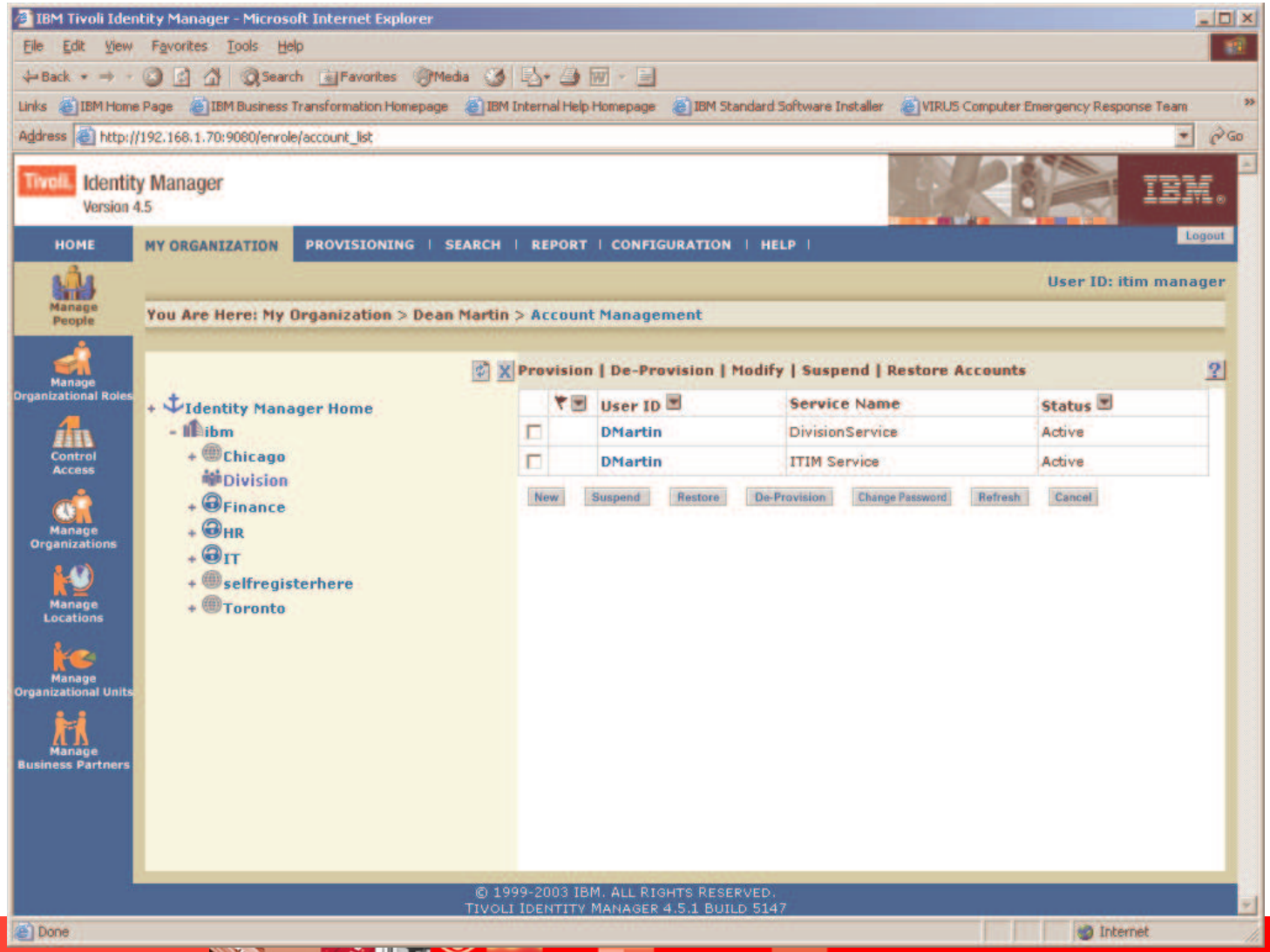
- A role is a collection of users with a common responsibility
- Roles are defined statically or dynamically
- Dynamic roles defined based on LDAP attribute.
- Provisioning based on role membership

The TIM Provisioning Model

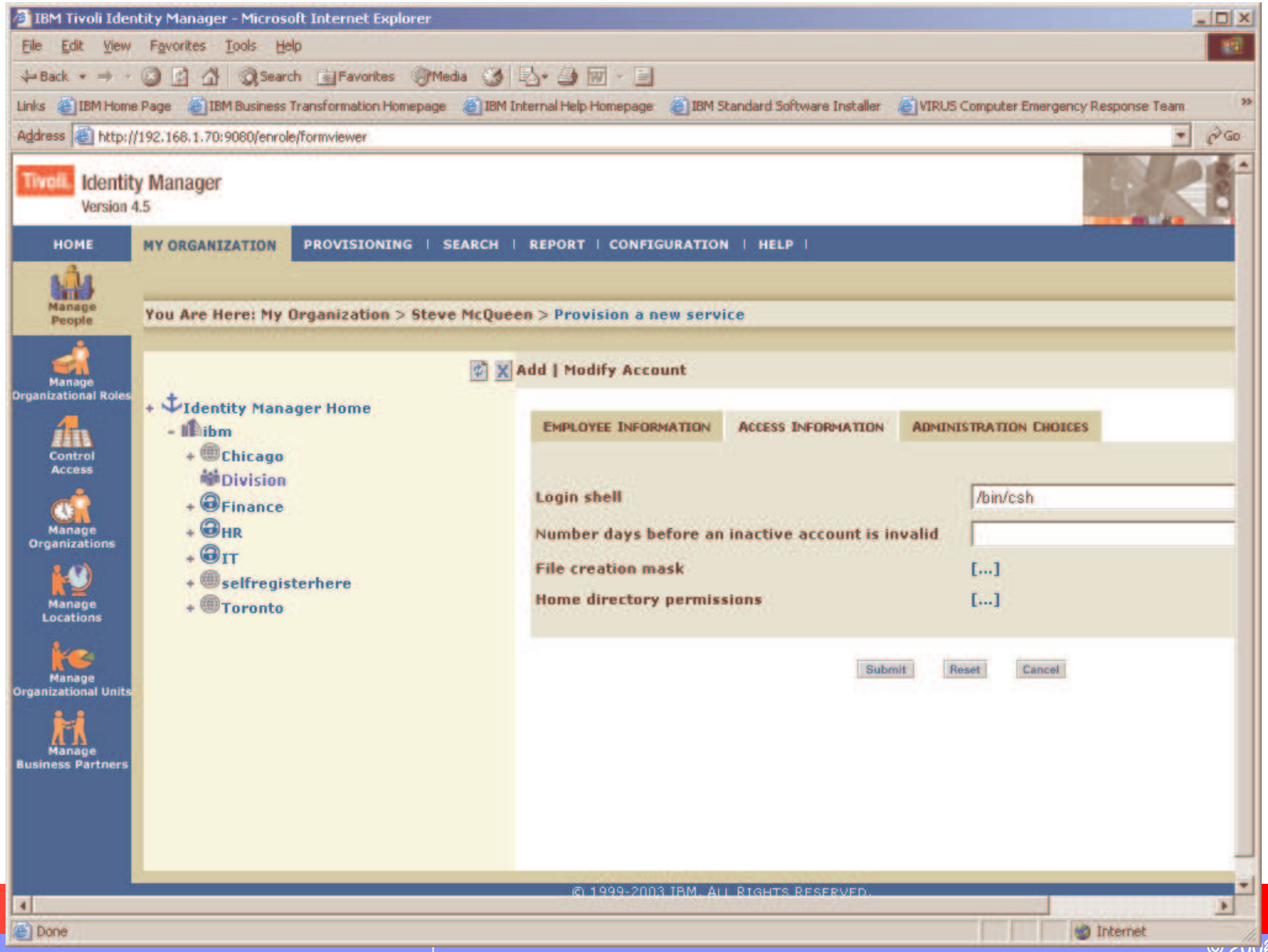


- Users assigned to roles based on responsibilities
- Role members are provisioned to resource(s) via a Provisioning Policy
- Provisioning Policies can also define attributes for a user

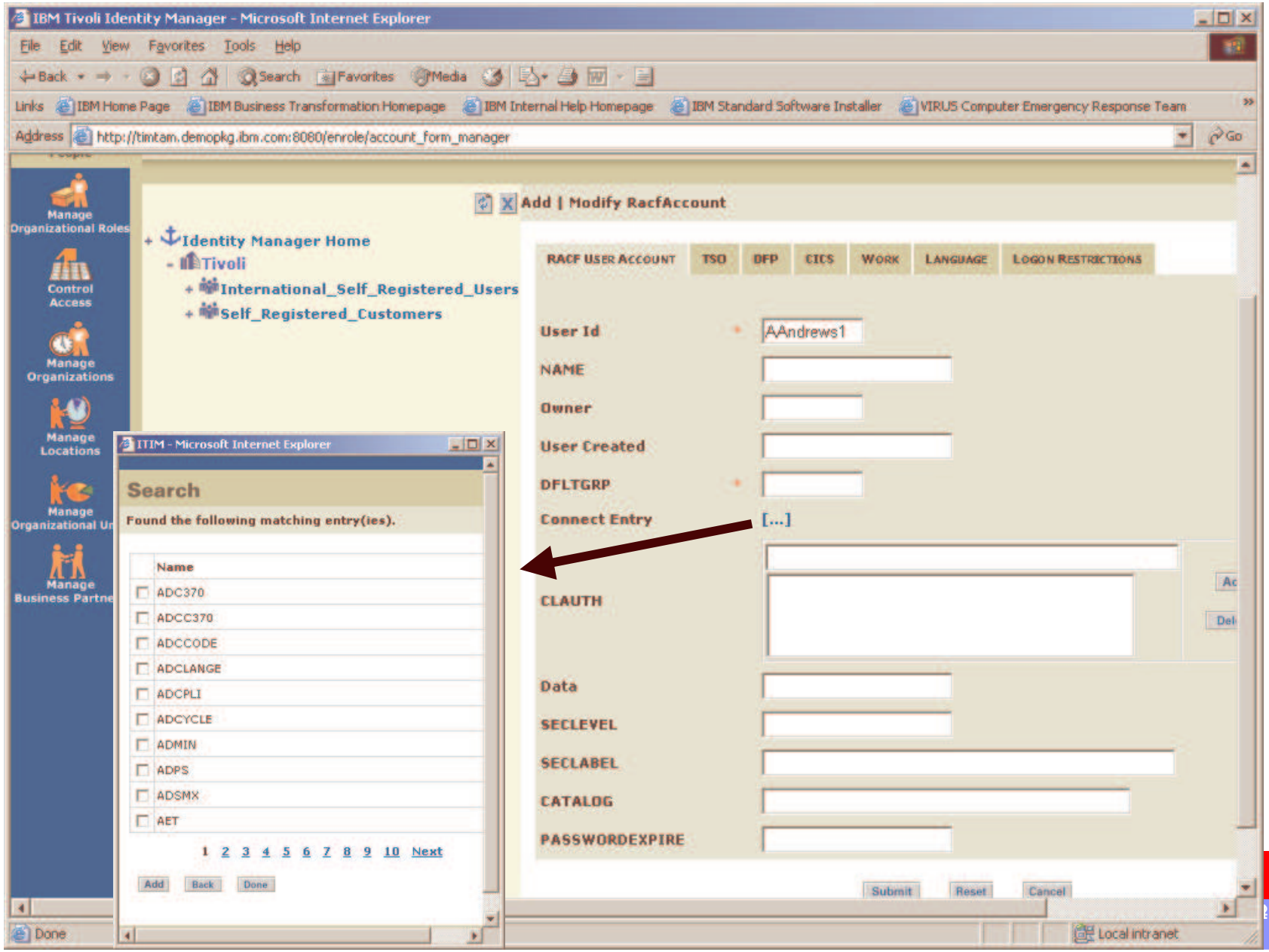
System of Record



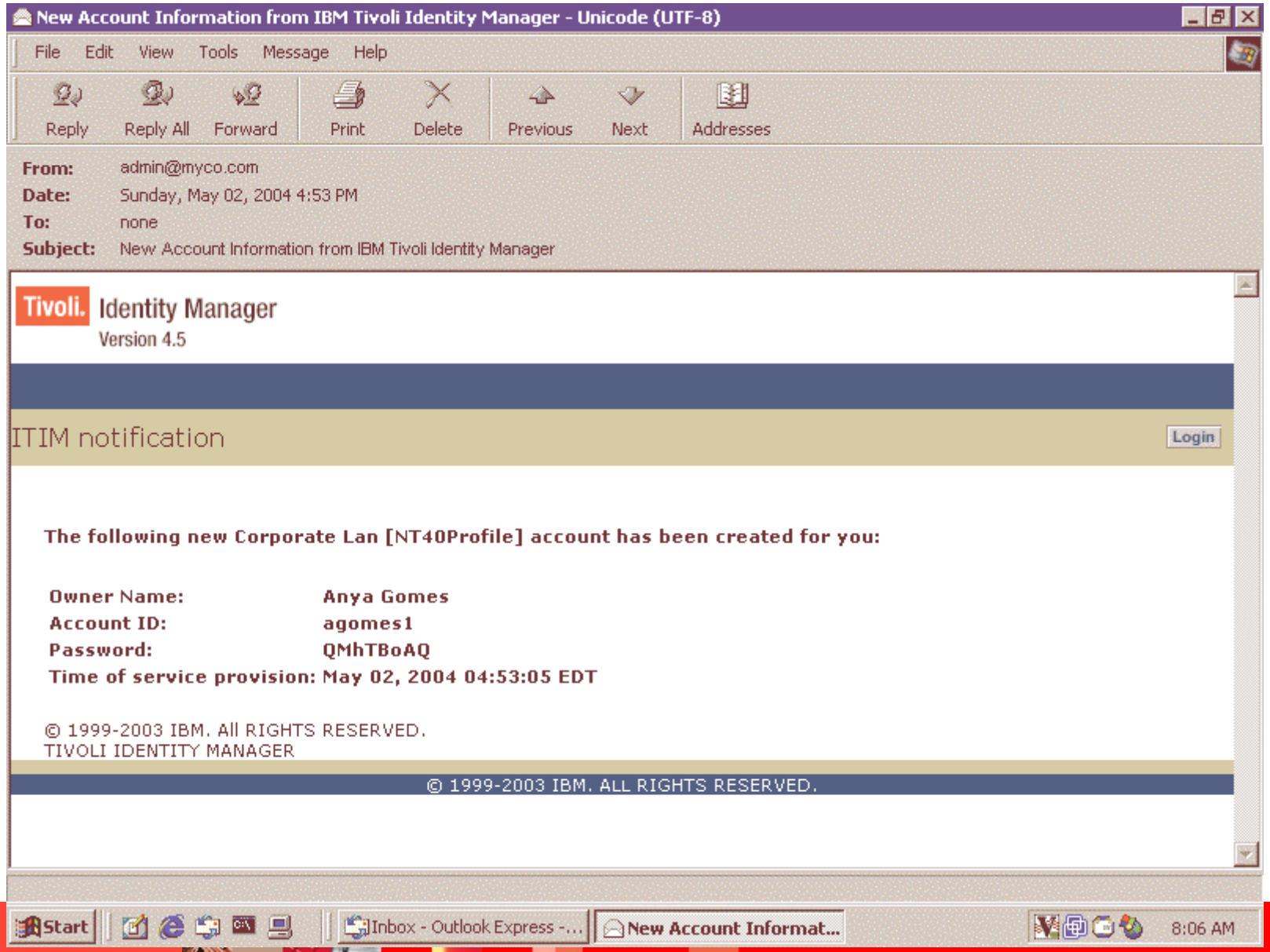
UNIX/Linux Account



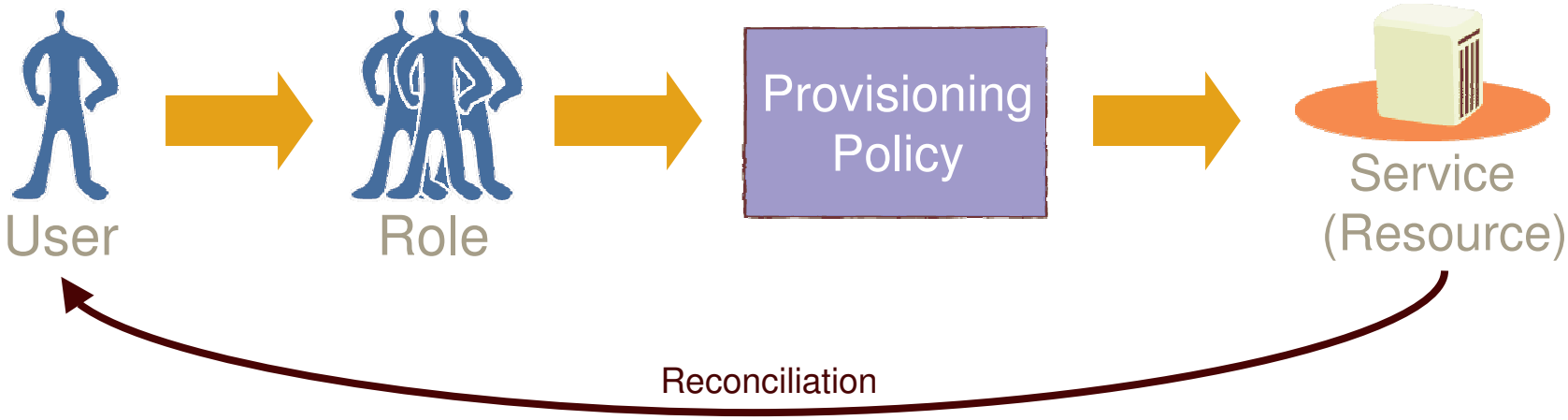
RACF Account



Email interaction



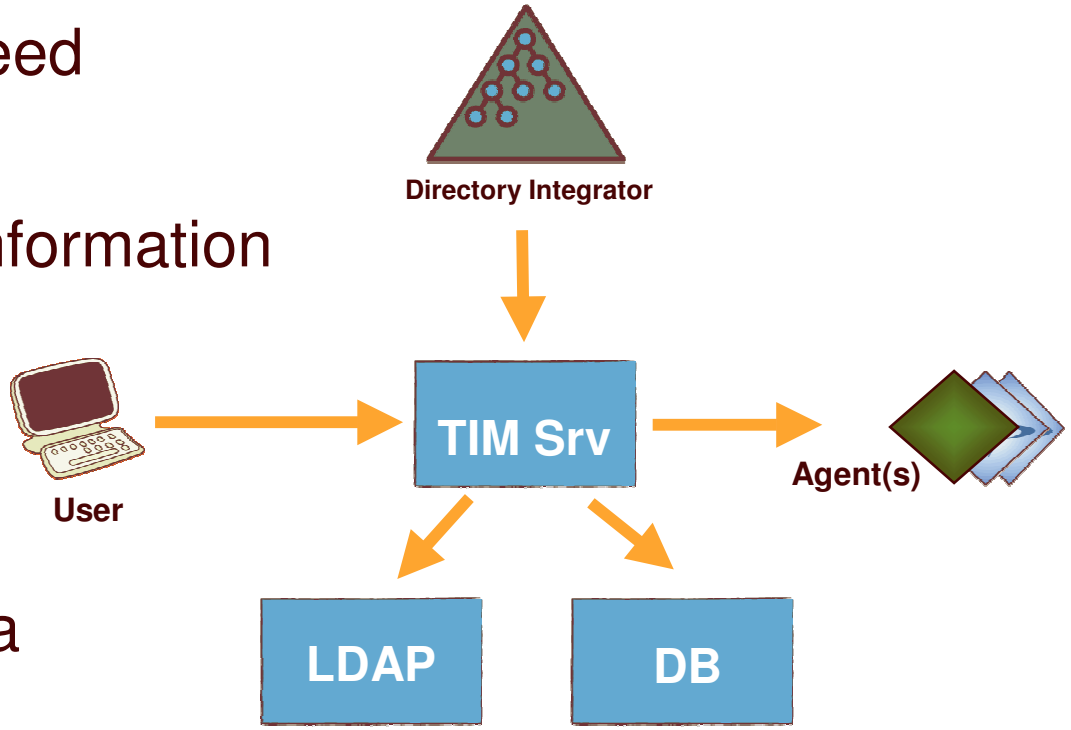
Reconciliation Compares "What Is" to "What Should Be"



- 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

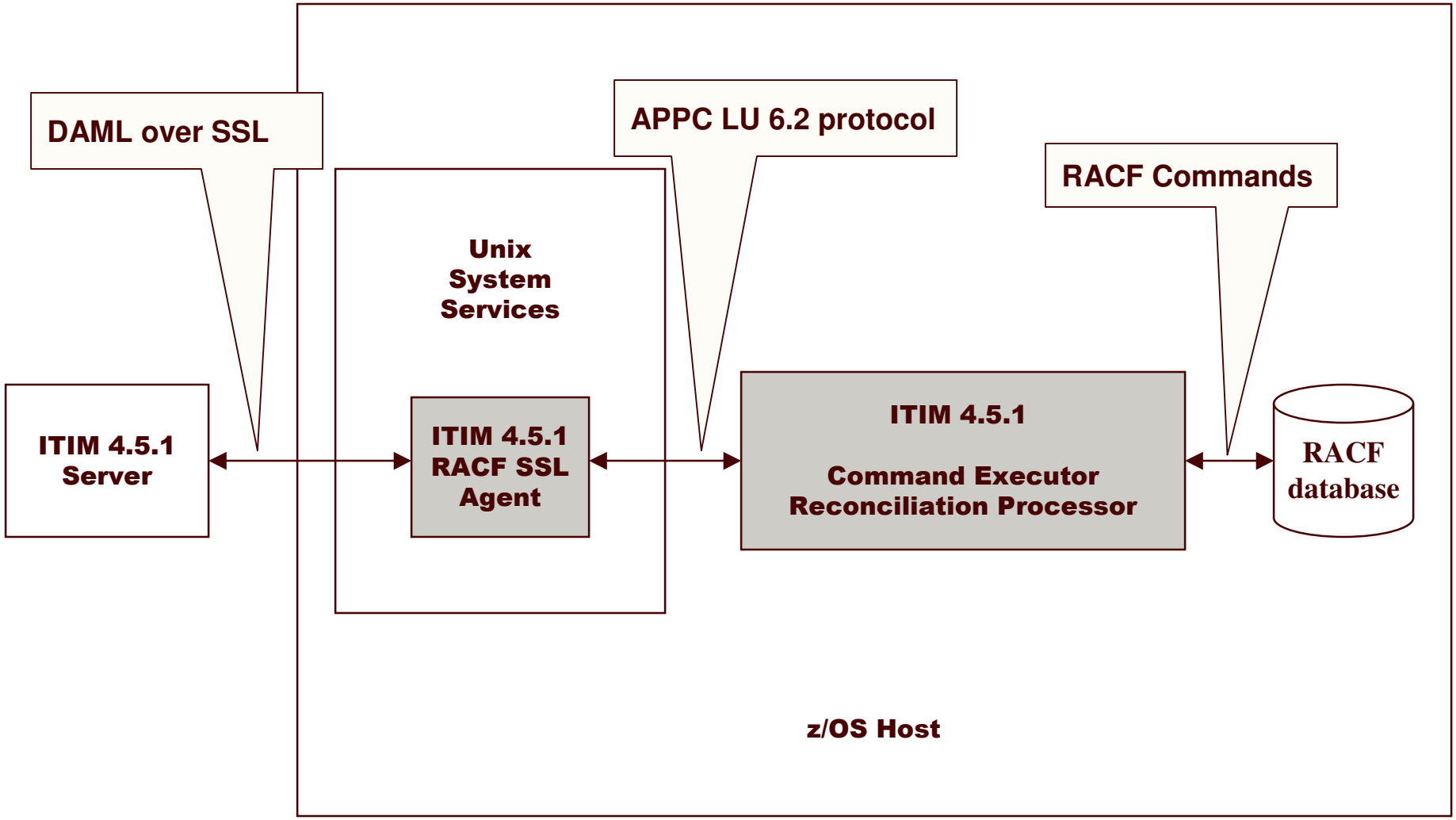
Help Desk Systems

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



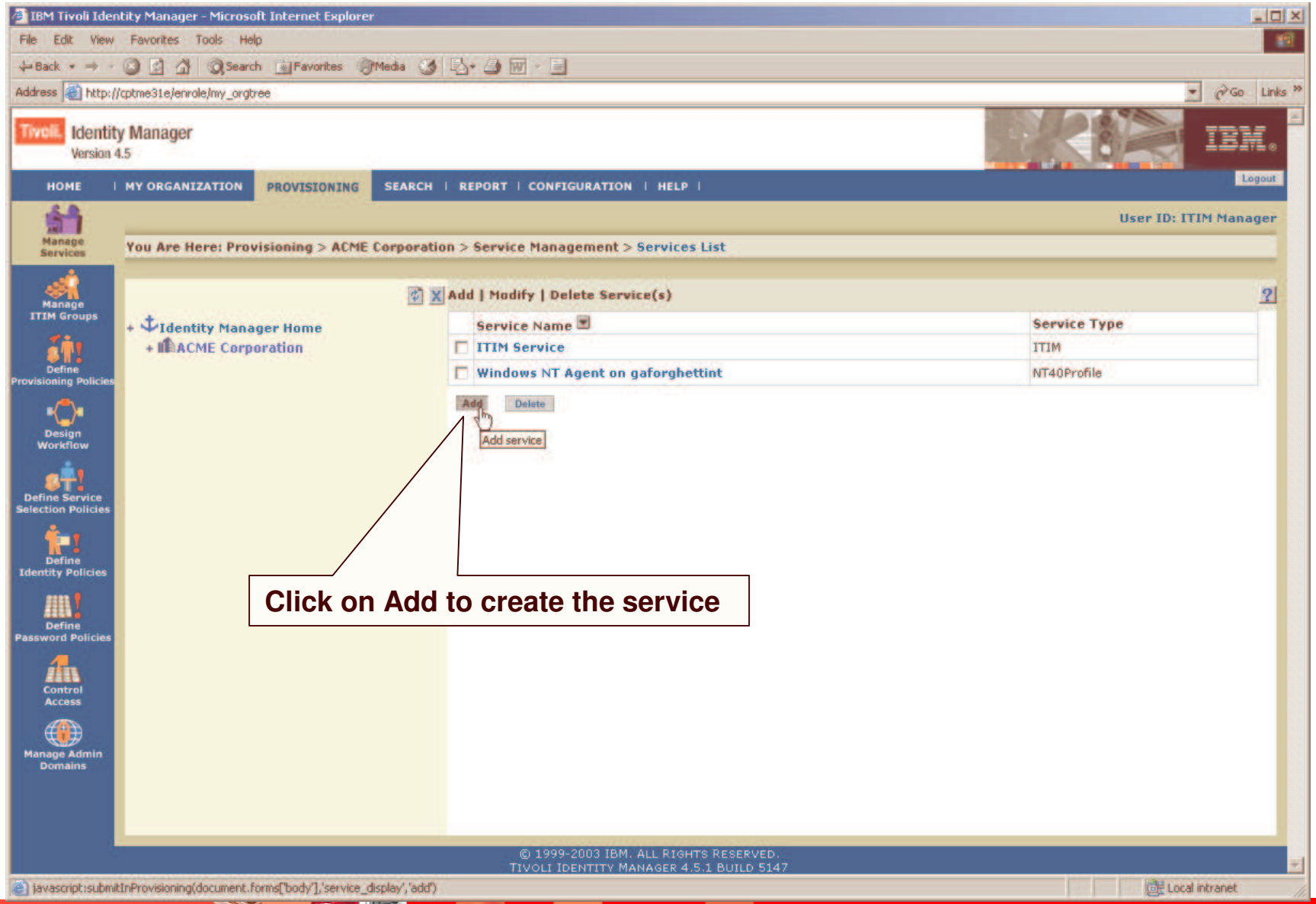
ITIM 4.5.1 RACF SSL Agent Overview

- **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

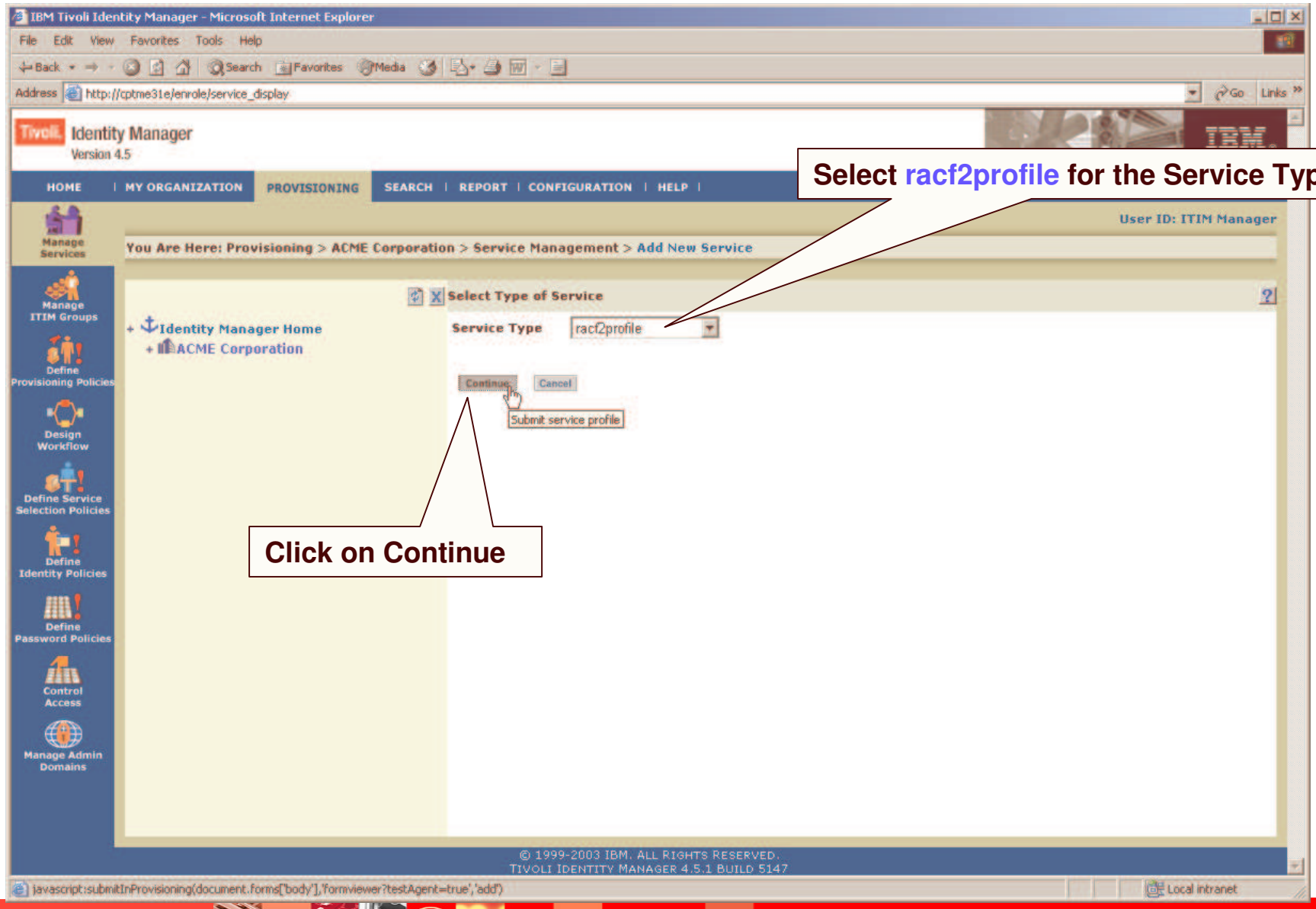
ITIM RACF SSL Agent Key Install/Configuration steps

- 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



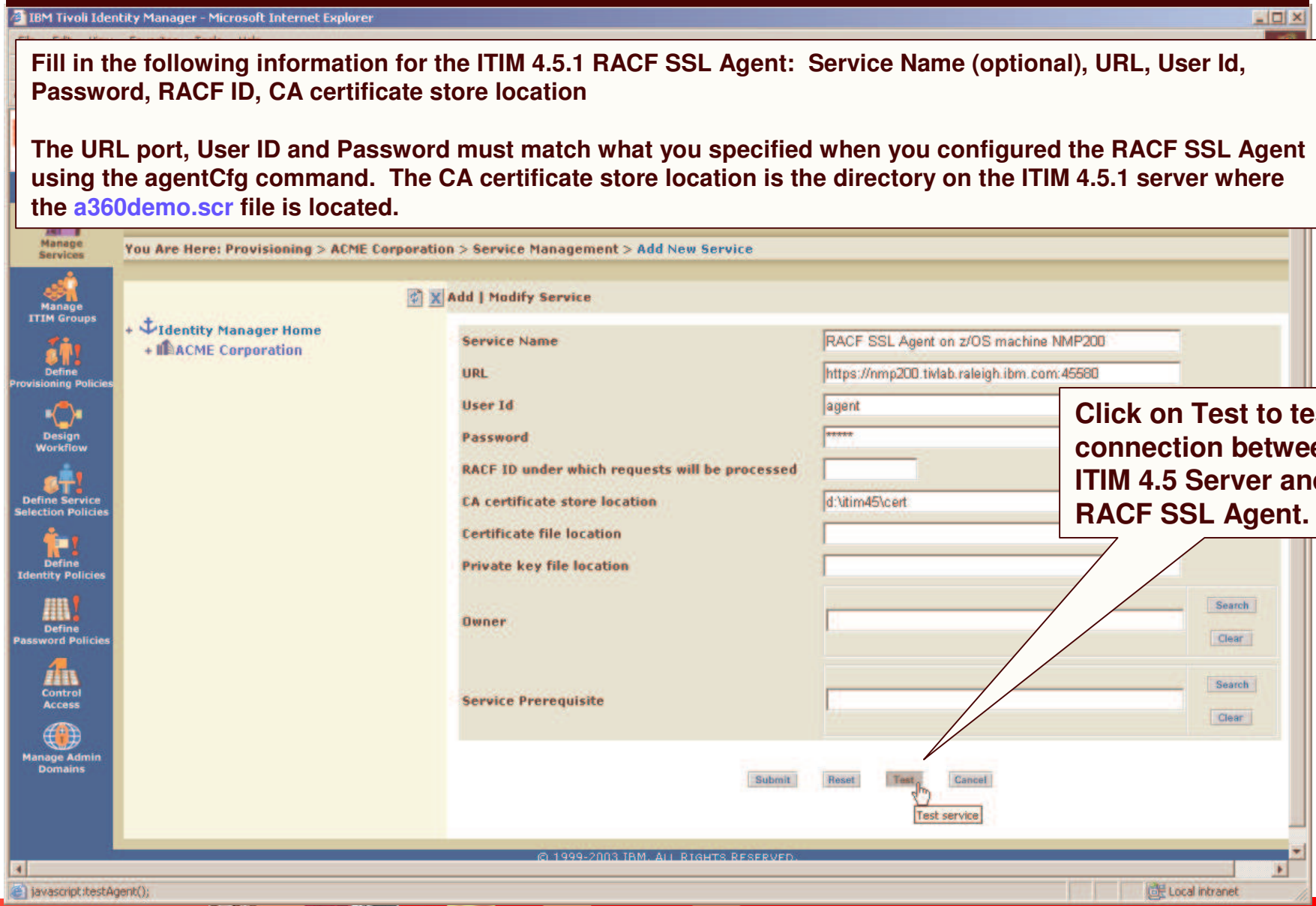
Create Service for ITIM 4.5.1 RACF SSL Agent



Create Service for ITIM 4.5.1 RACF SSL Agent

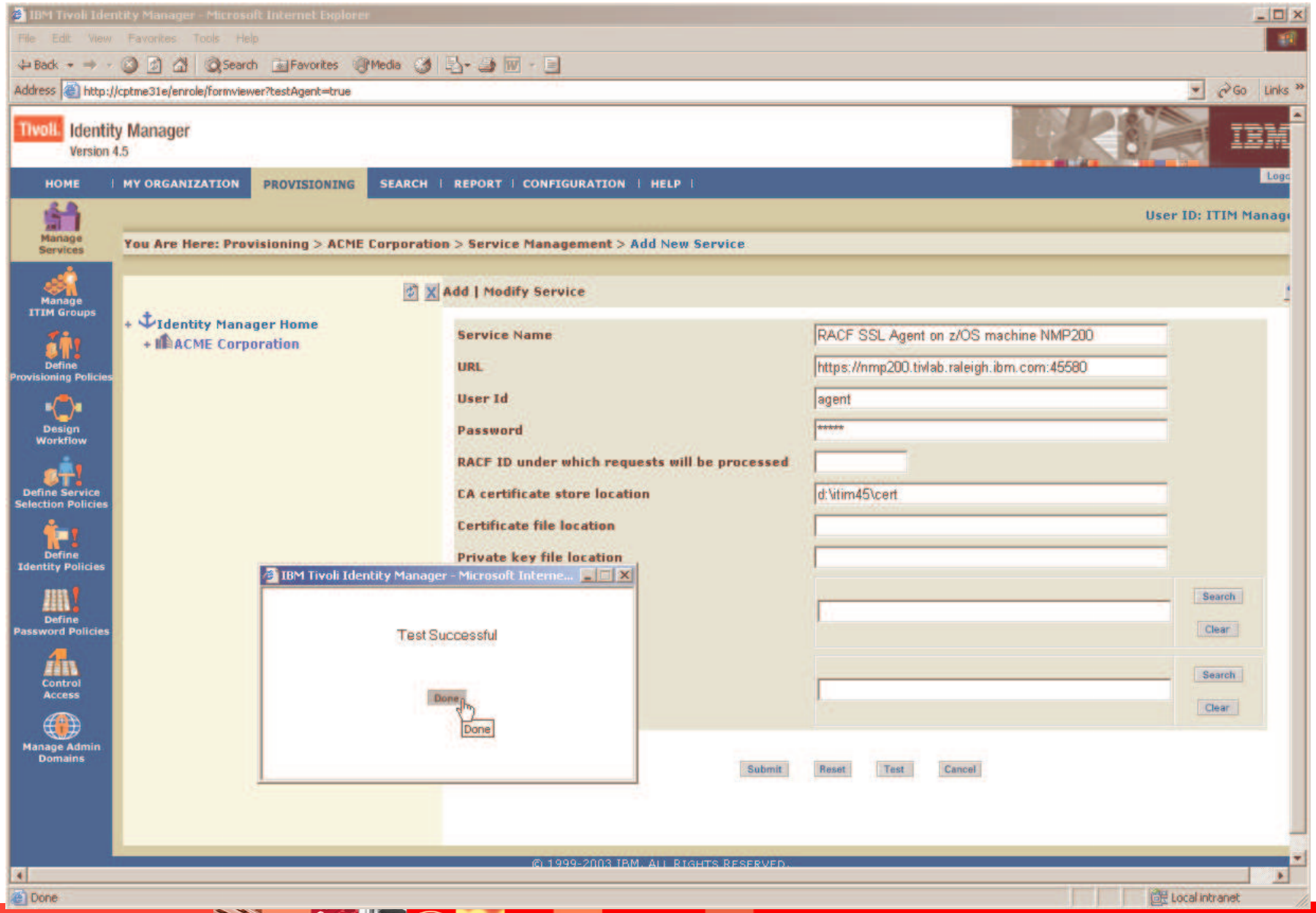
Fill in the following information for the ITIM 4.5.1 RACF SSL Agent: Service Name (optional), URL, User Id, Password, RACF ID, CA certificate store location

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.

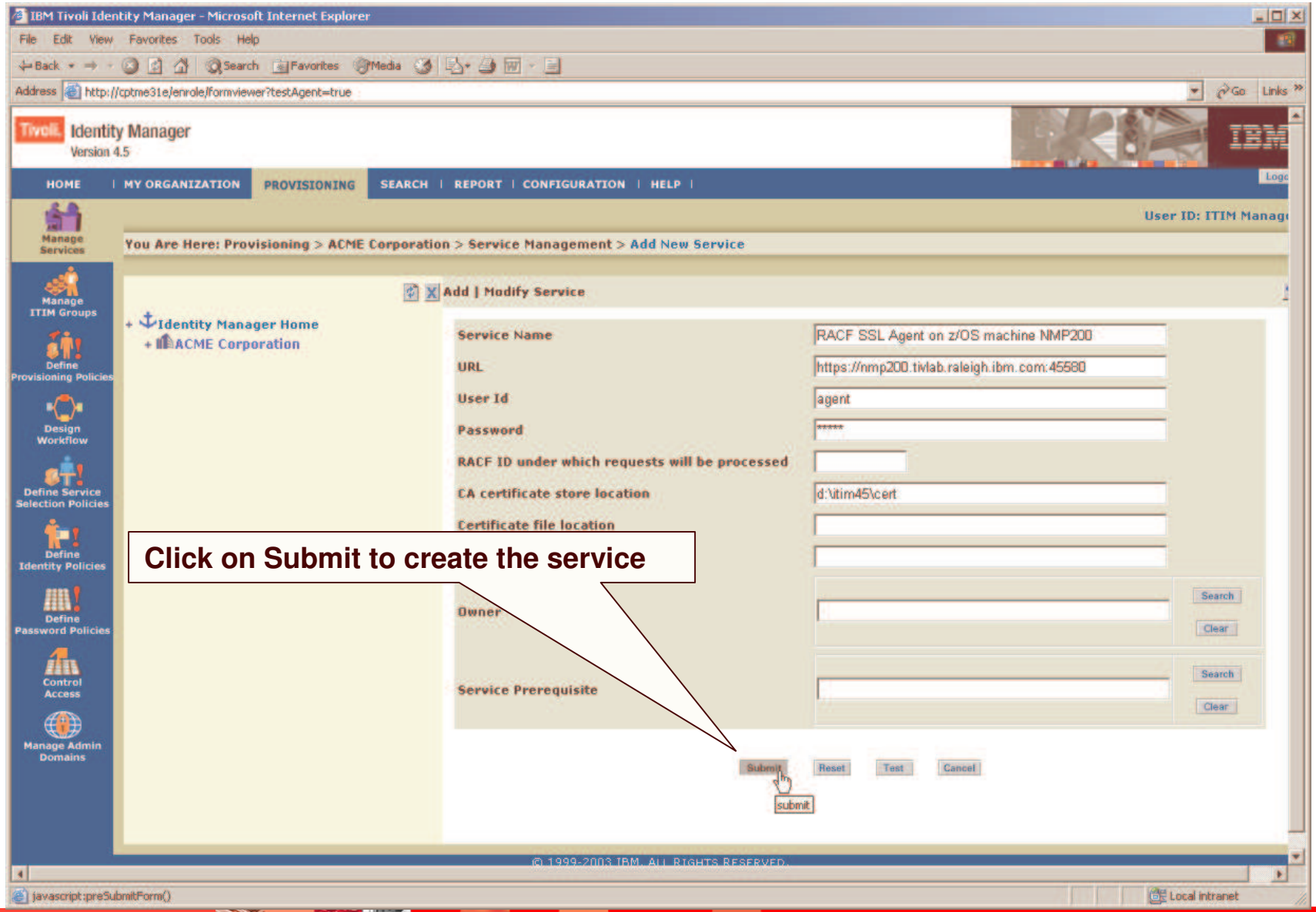


Click on Test to test the connection between the ITIM 4.5 Server and the RACF SSL Agent.

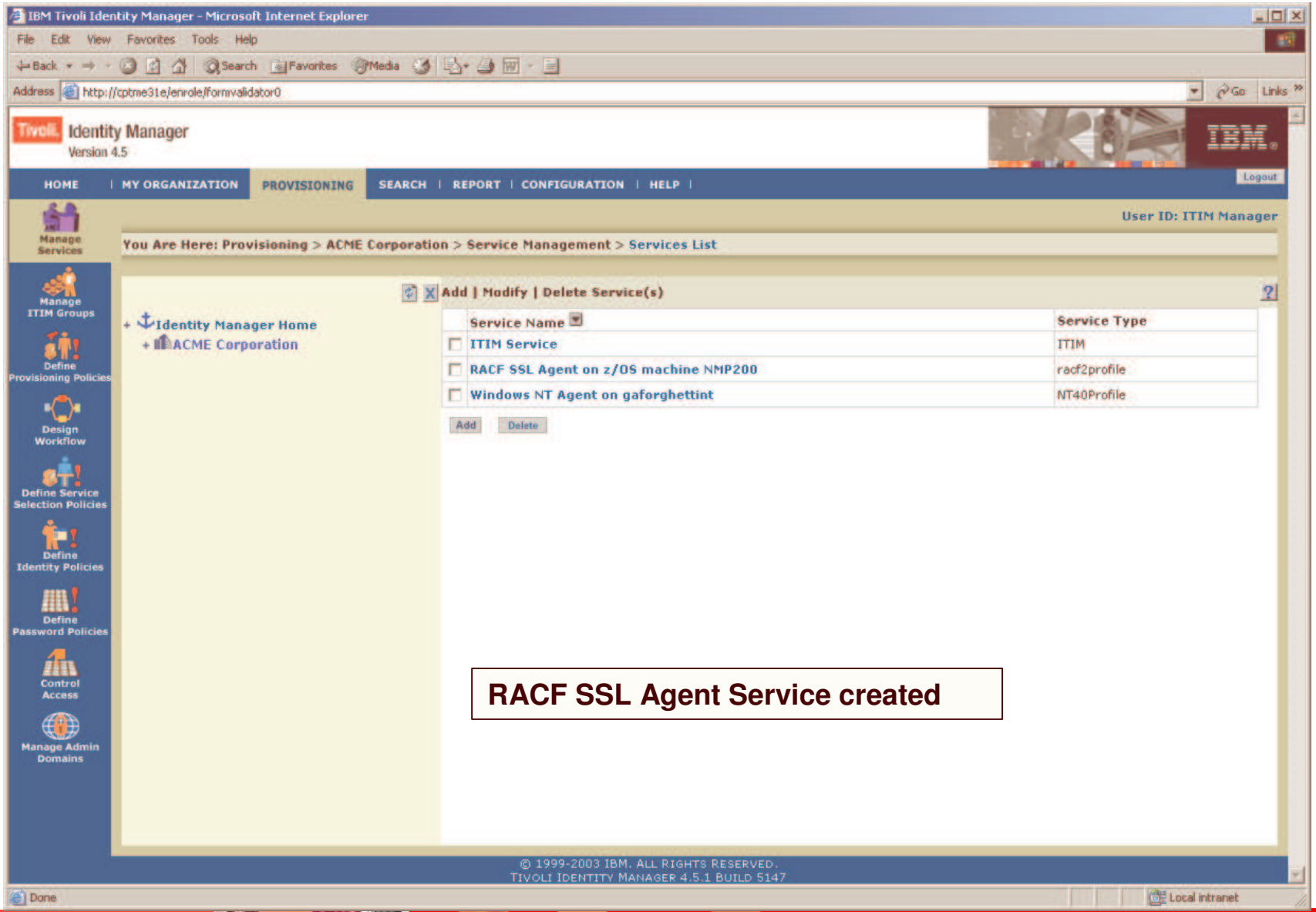
Test Service for ITIM 4.5.1 RACF SSL Agent



Create Service for ITIM 4.5.1 RACF SSL Agent



Create Service for ITIM 4.5.1 RACF SSL Agent



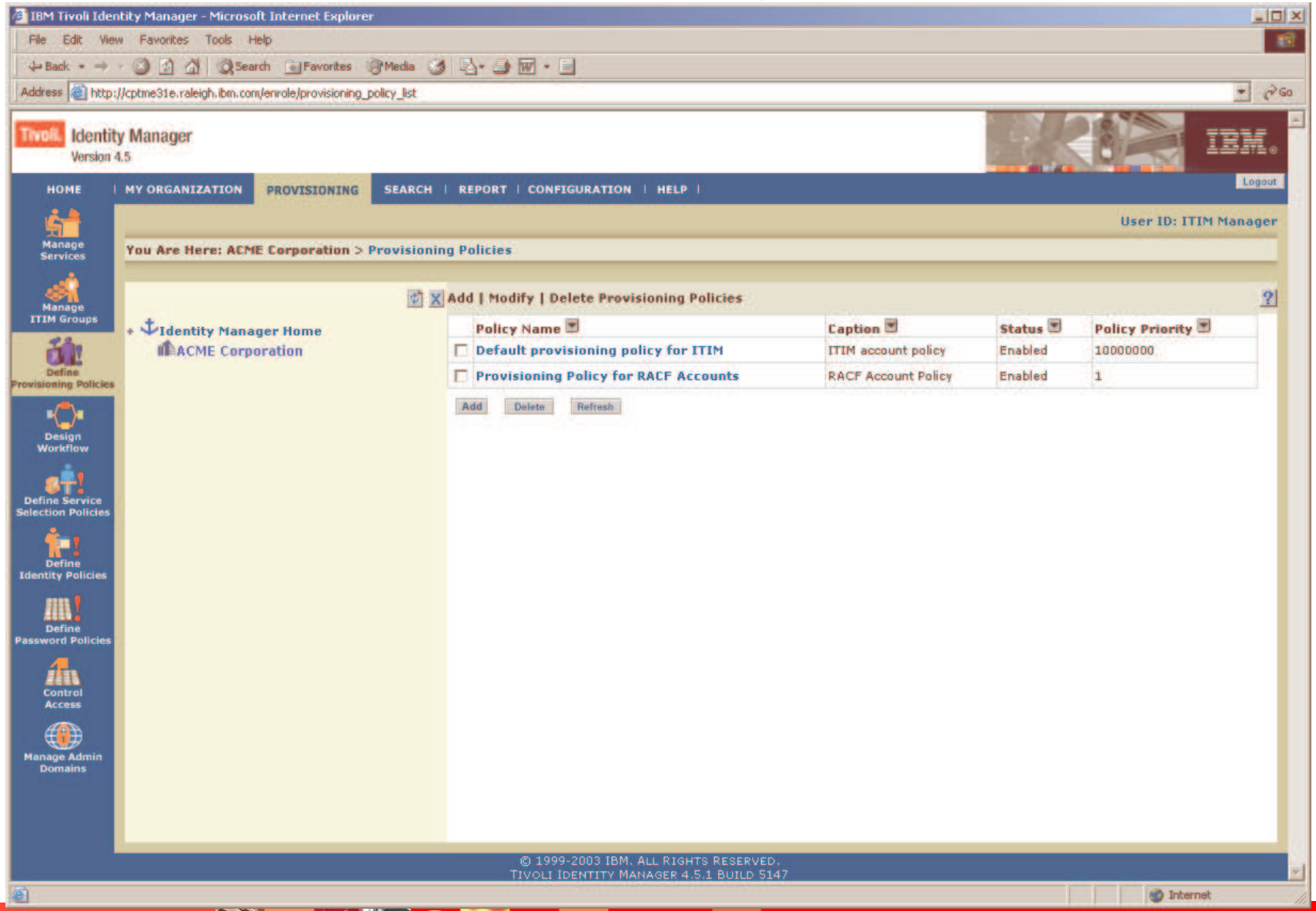
RACF SSL Agent Service created

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

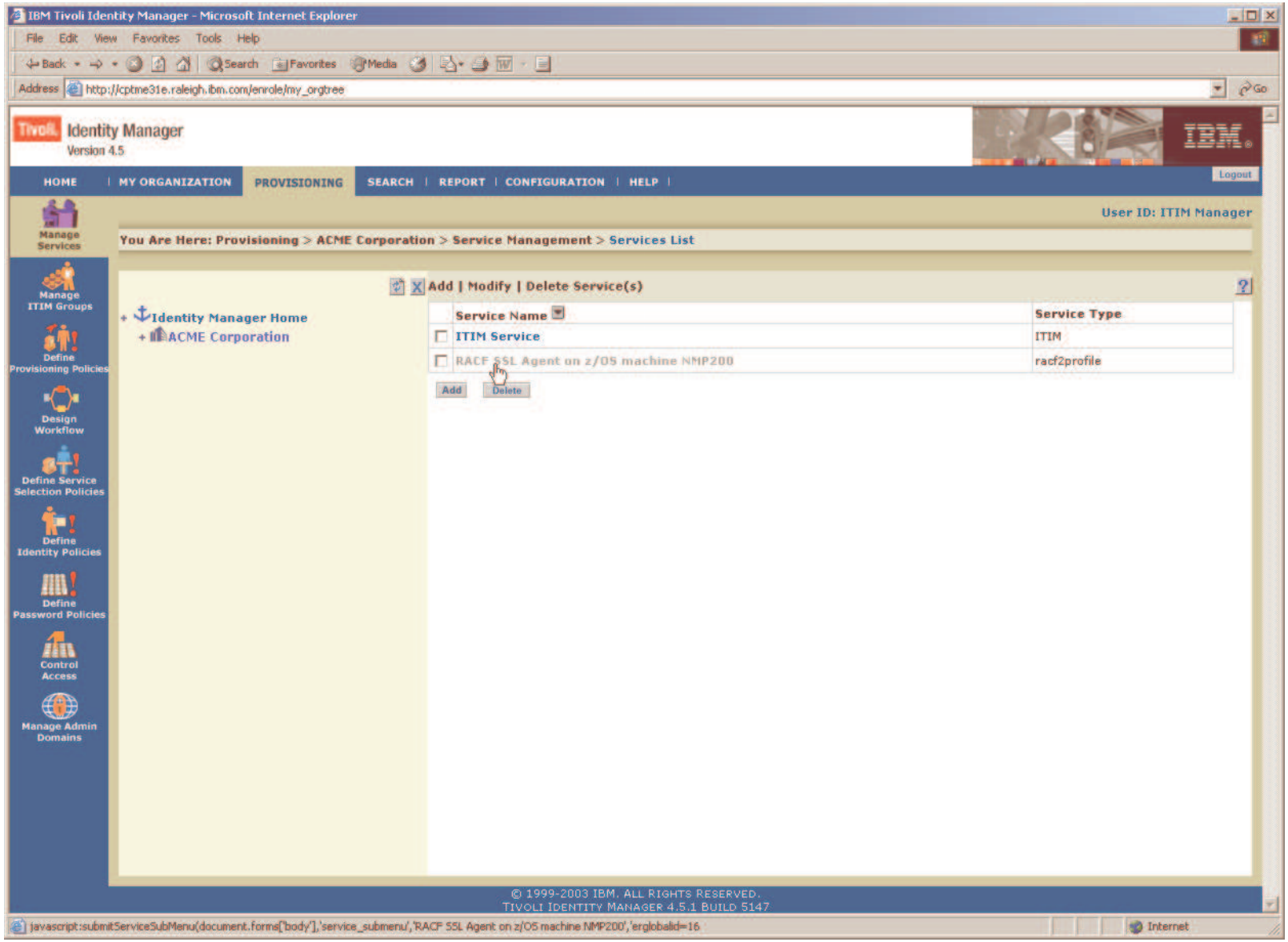
But, before creating or deleting users, you must first:

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

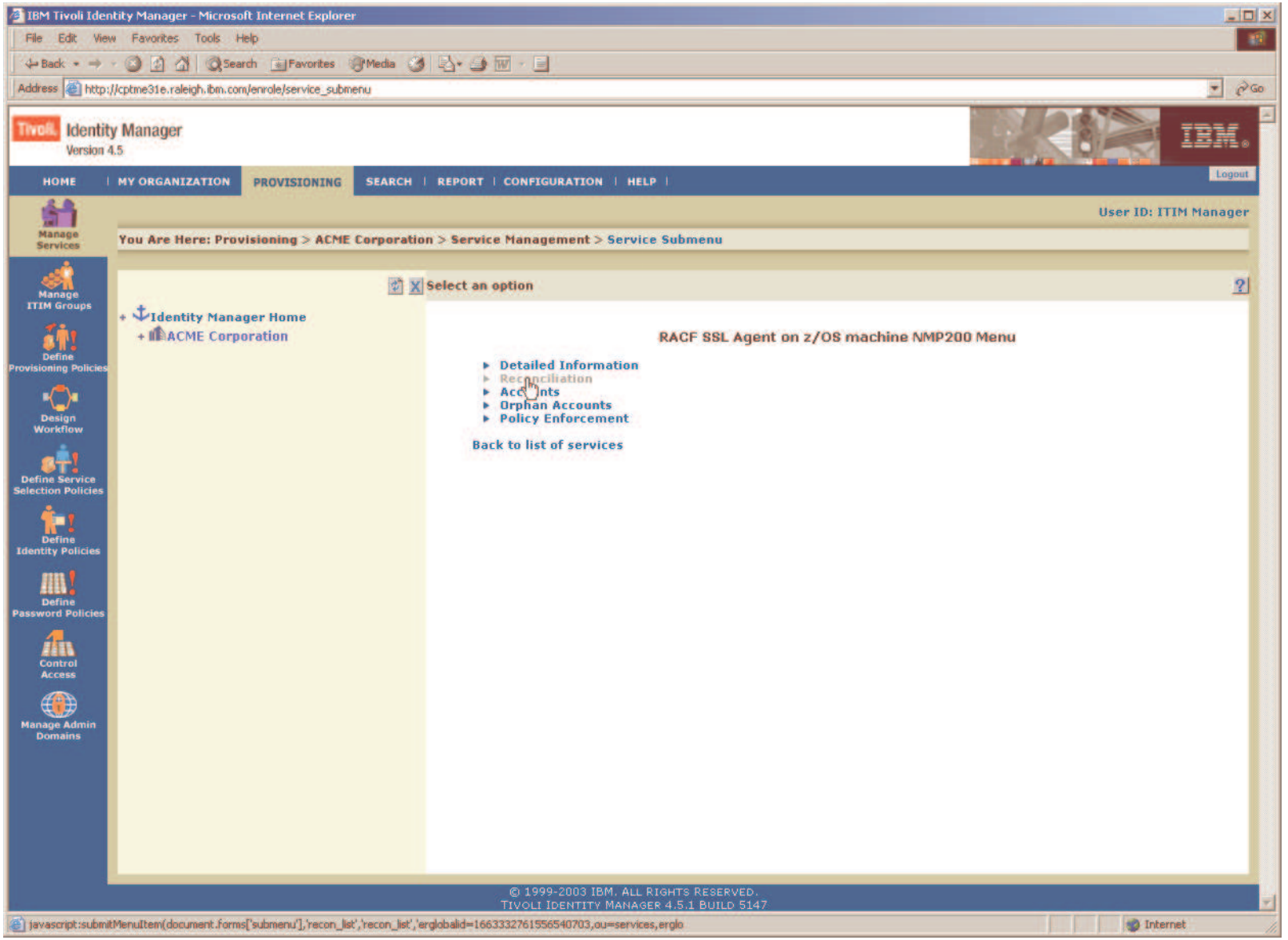
Create Provisioning Policy for RACF Accounts



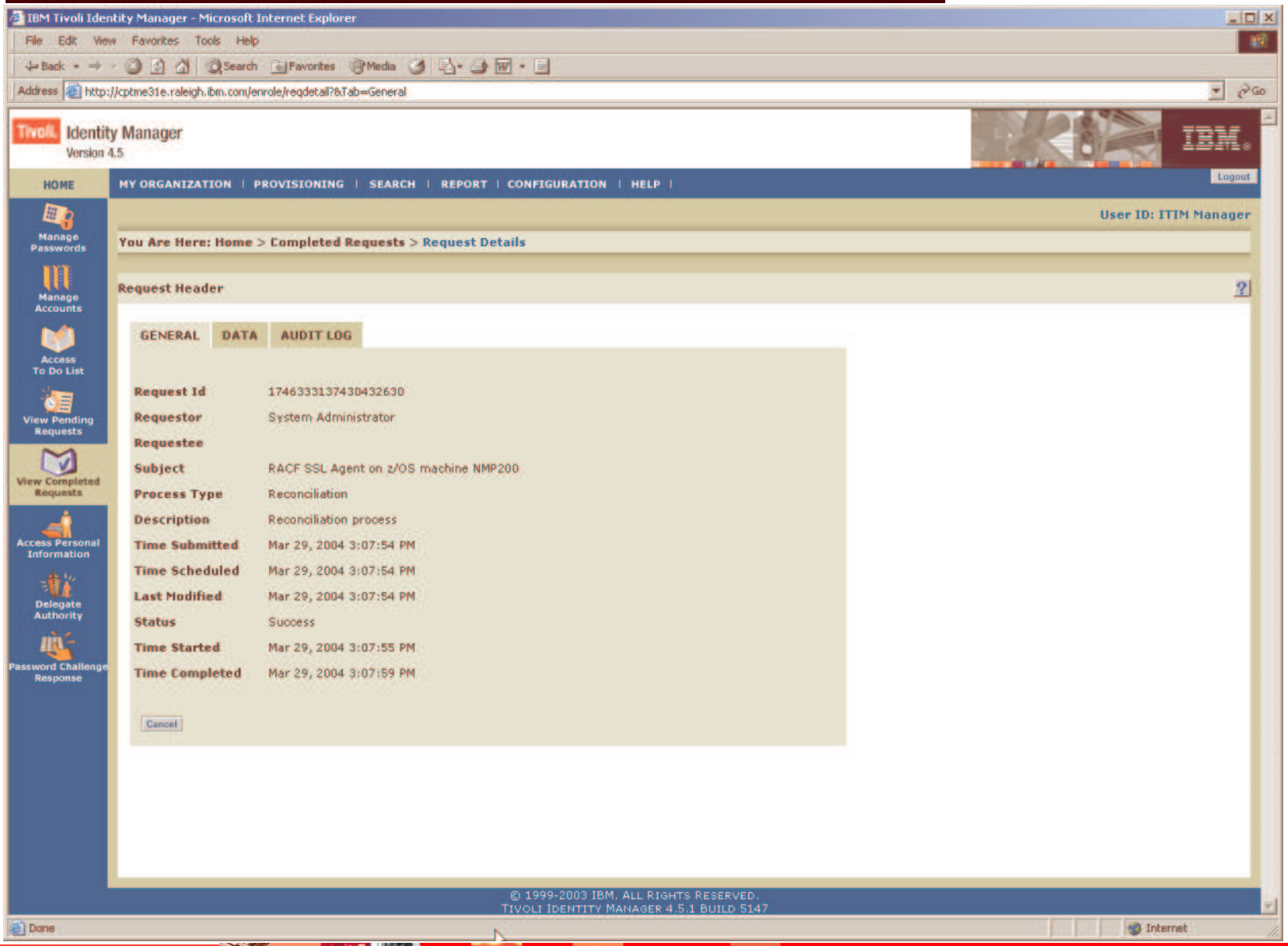
Perform a reconciliation



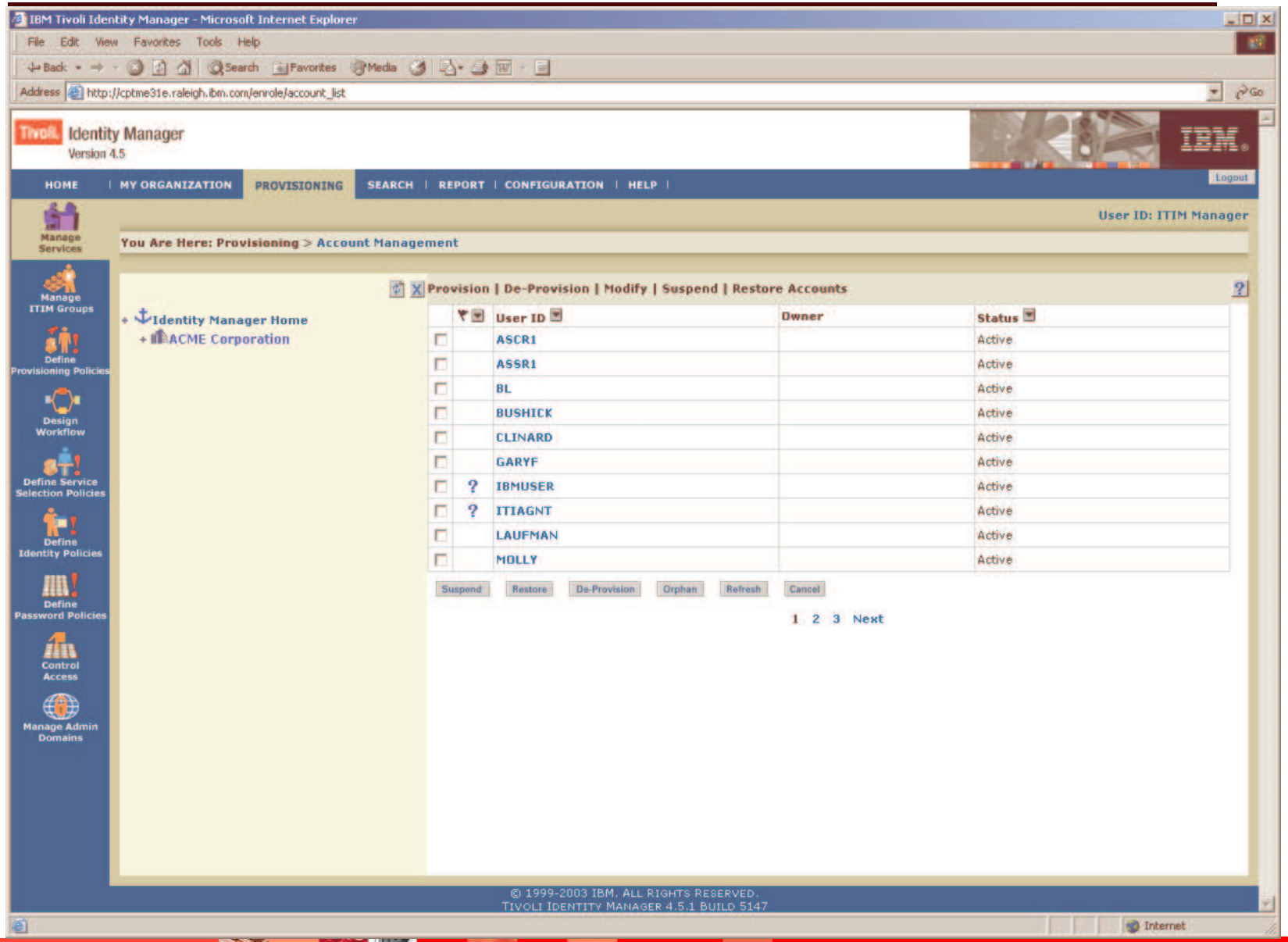
Perform a reconciliation



Verify reconciliation completed

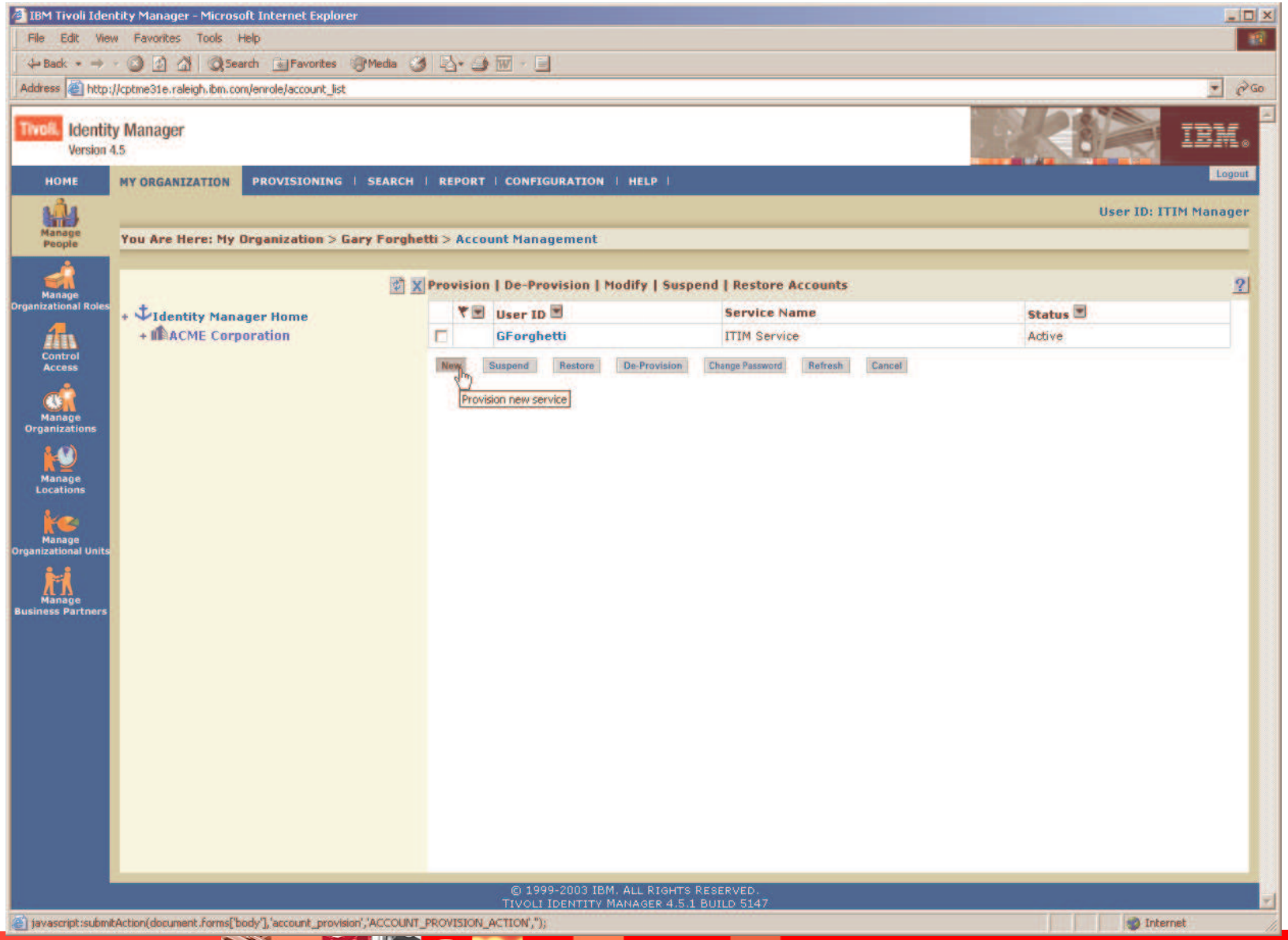


After reconciliation now have RACF data

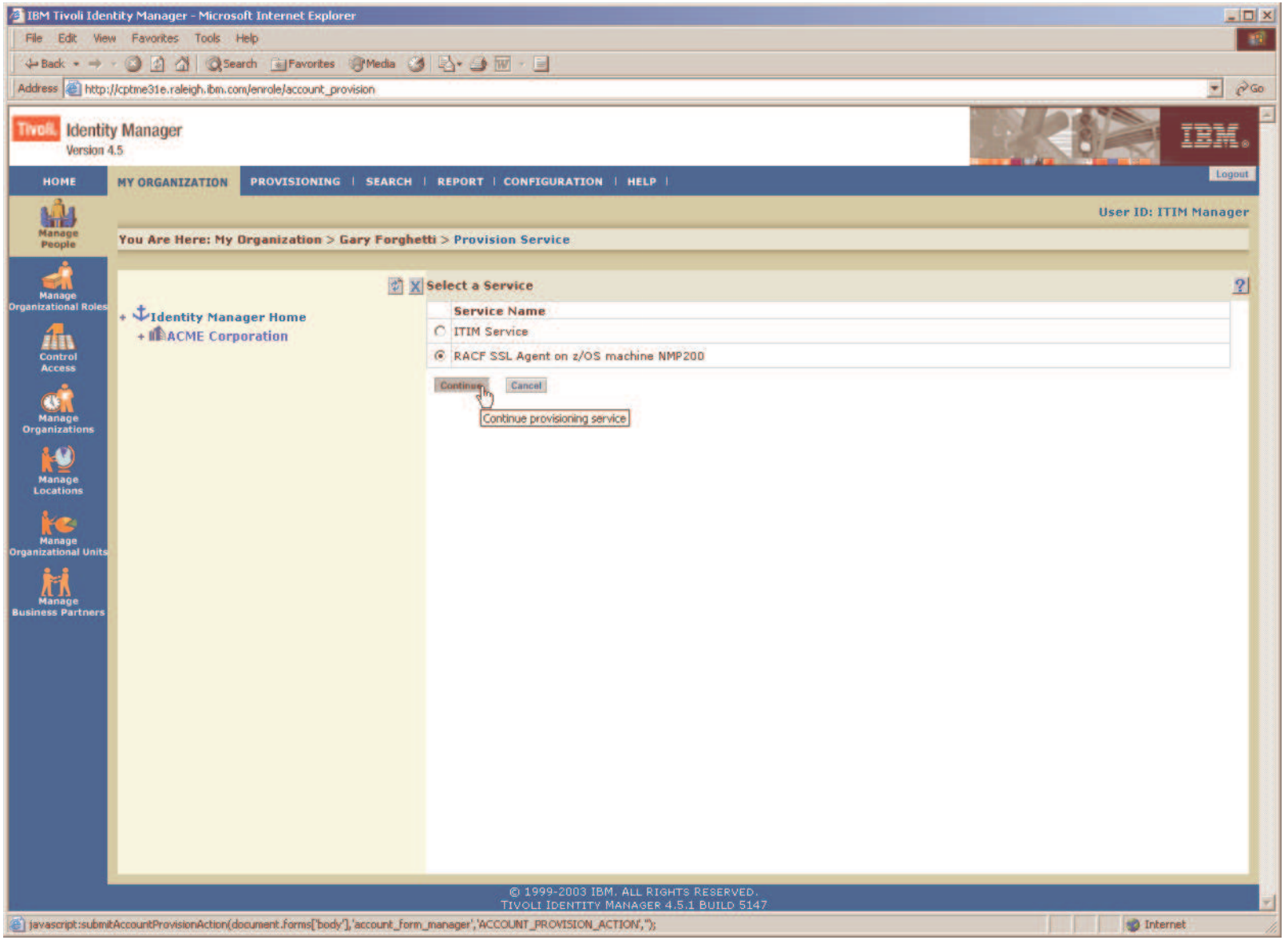


Create a new account (user ID)

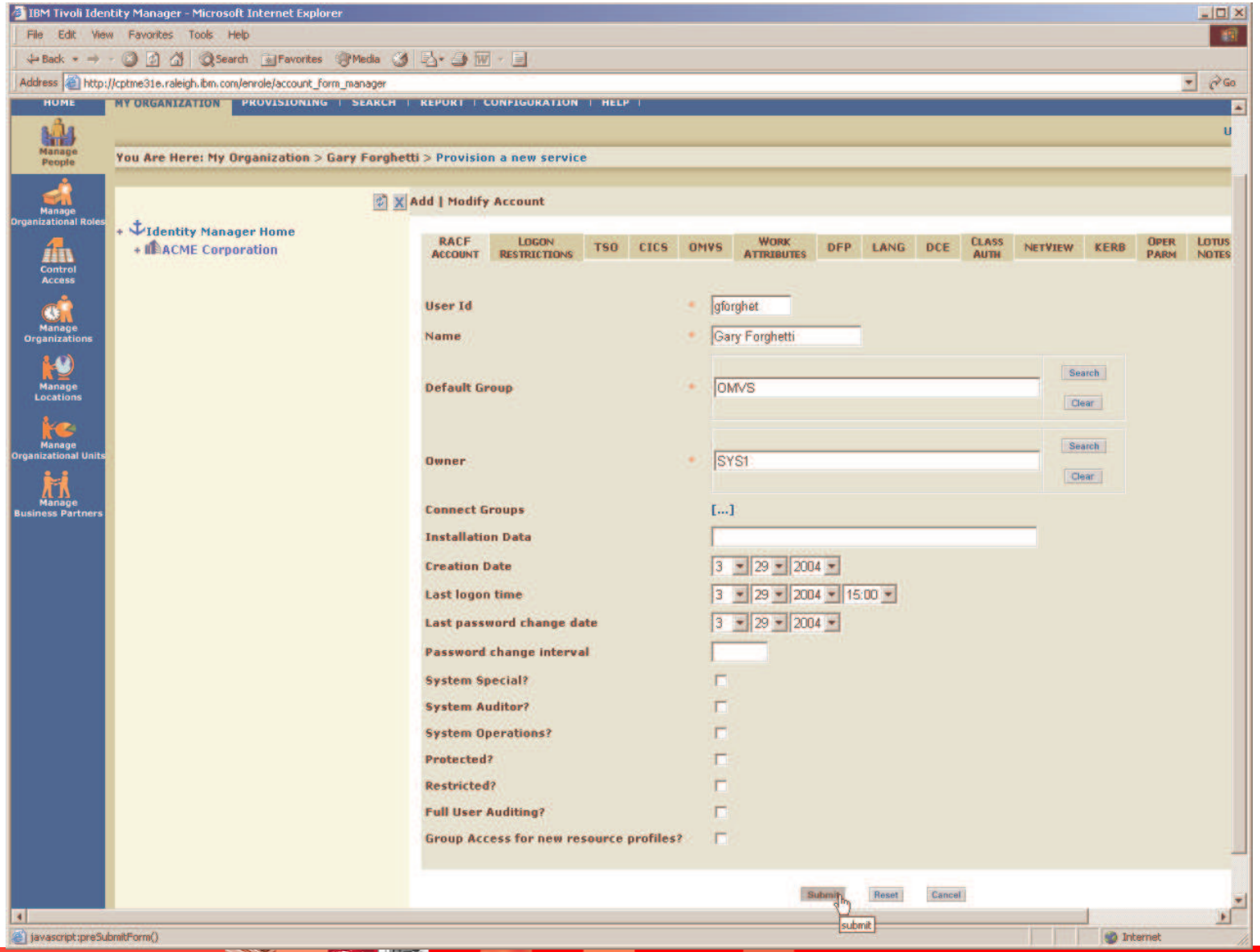
Create a new account



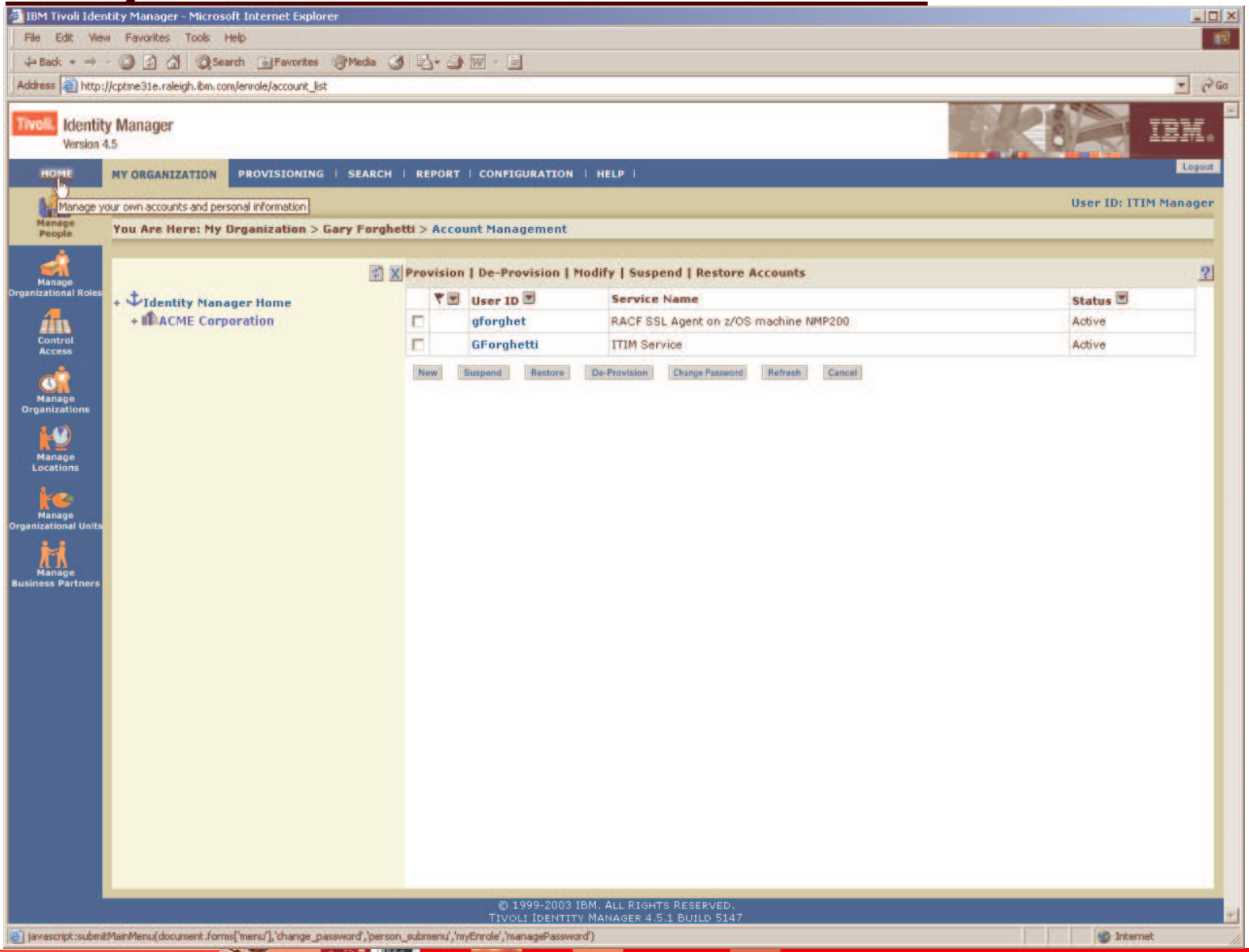
Create a new account



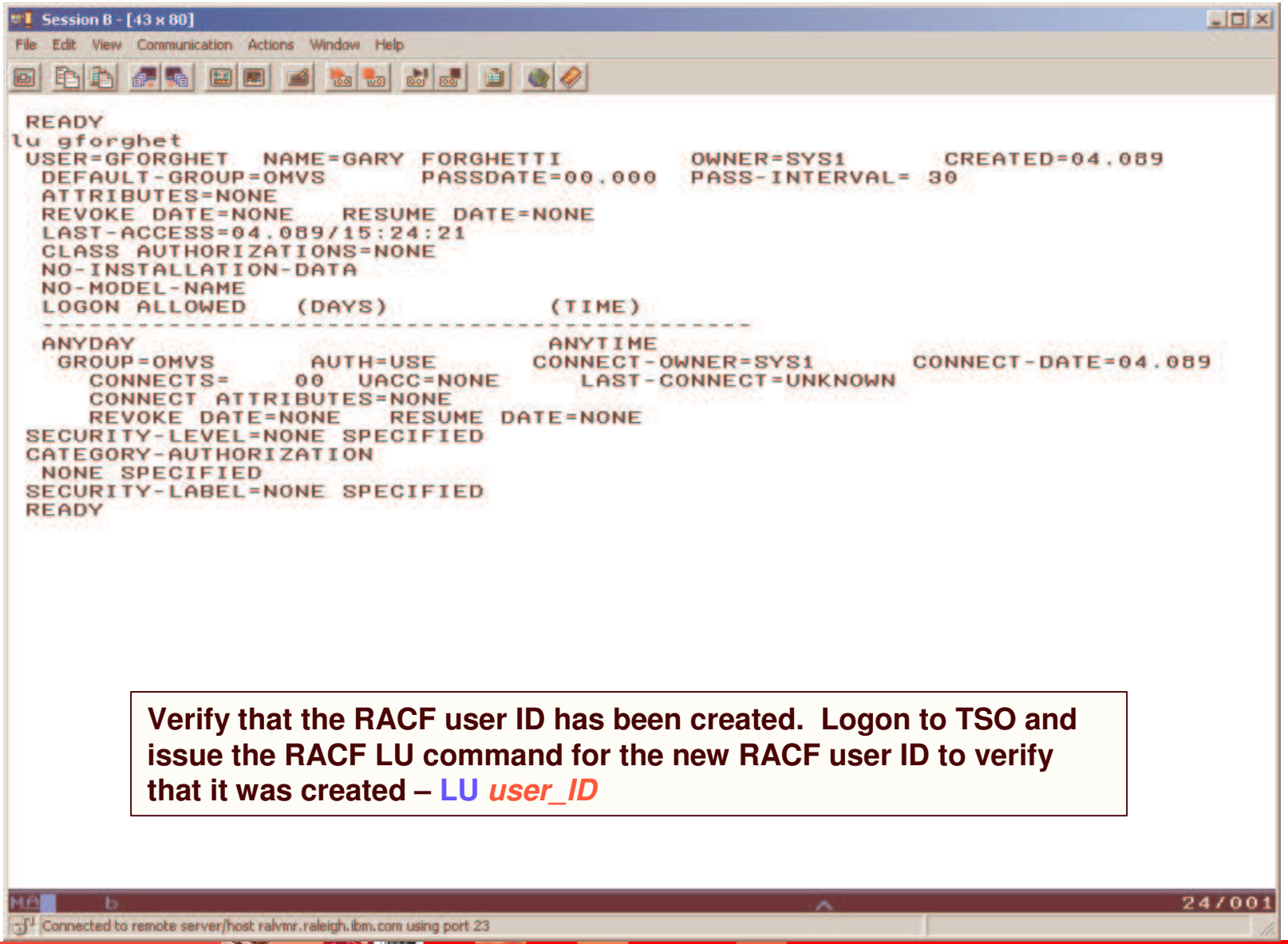
Create a new account



Gary now has a RACF account



The new account can be verified on RACF



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