OS/390 Security Server meets Tivoli
Managing RACF with Tivoli
Vanguard Enterprise Security Expo '99
June 6-11, 1999 Session 139

Paul de Graaff
IBM International Technical Support Organisation
Poughkeepsie, New York

(914) 433-1389
graaff@us.ibm.com

THE POWER TO MANAGE. ANYTHING. ANYWHERE.

Disclaimer

The information contained in this document is distributed on an "as is" basis without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Trademarks

The following are trademarks of International Business Machines Corporation:

CICS
DB2
IBM
IMS
DFSMS
Open Edition
OS/390
MVS/ESA
RACF
HiperBatch
PSF
System/390
VTAM

The following are trademarks or registered trademarks of other companies or institutions:

Open Software Foundation	Open Software Foundation, Inc.
OSF	
DCE	
Distributed Computing Environment	
NetWare	Novell
NT	Microsoft Corporation

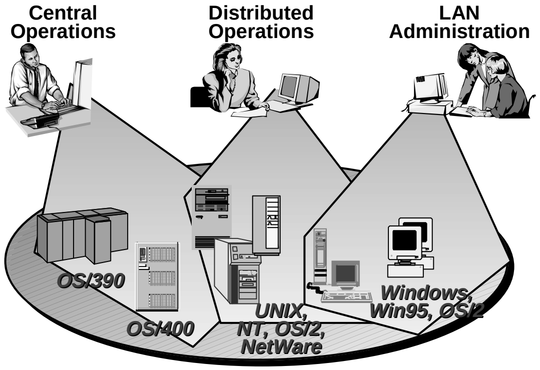
Agenda

- □ Challenges in Security Management
- □ Tivoli Architecture and Security Offerings
- □ Role Based Security
- □ Getting Started
- □ Benefits
- □ Screenshots of GUI interface

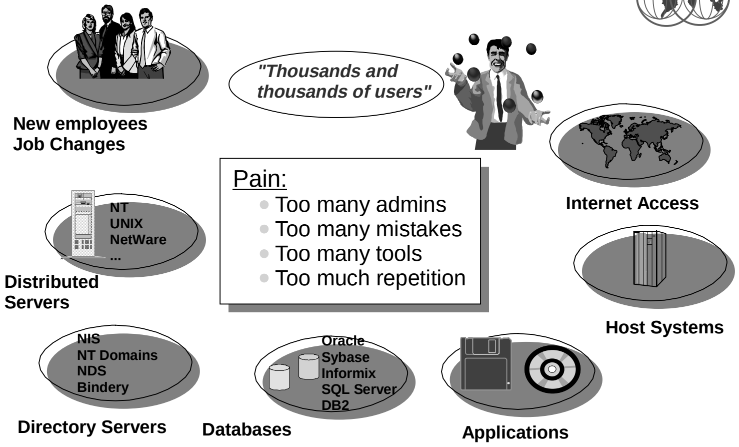
Agenda

- ☛ Challenges in Security Management
- □ Tivoli Architecture and Security Offerings
- □ Role Based Security
- □ Getting Started
- □ Benefits
- □ Screenshots of GUI interface

Management Problem…
…..*Islands of Management*



Managing *users* is very complex in the truly distributed environment

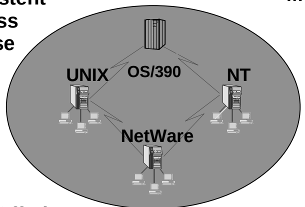


Pain:
- Too many admins
- Too many mistakes
- Too many tools
- Too much repetition

Managing *security* is very complex

The Challenge:

Establish, Implement, and Enforce a Consistent Security Policy across your Entire Enterprise

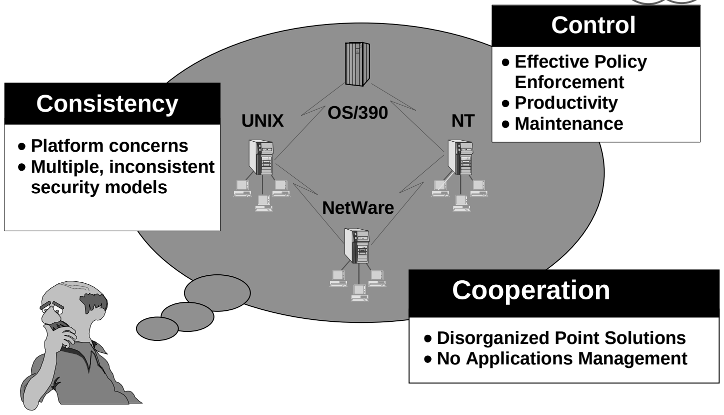


The Dilemma:

Different Security Tools & Models
- ➤ I/A
- ➤ Access Control
- ➤ Virus Protection
- ➤ Alarm/Monitoring
- ➤ Intrusion Detection

The Result:
- ➤ Fragmented Offerings
- ➤ Too many Points of Failure ... the customer becomes the integrator
- ➤ Increased Training Costs
- ➤ Security needs are not linked to the needs of the business
- ➤ Lack of consistent security policy

Distributed Security: Customer Goals



Consistency

- Platform concerns
- Multiple, inconsistent security models

Control

- Effective Policy Enforcement
- Productivity
- Maintenance

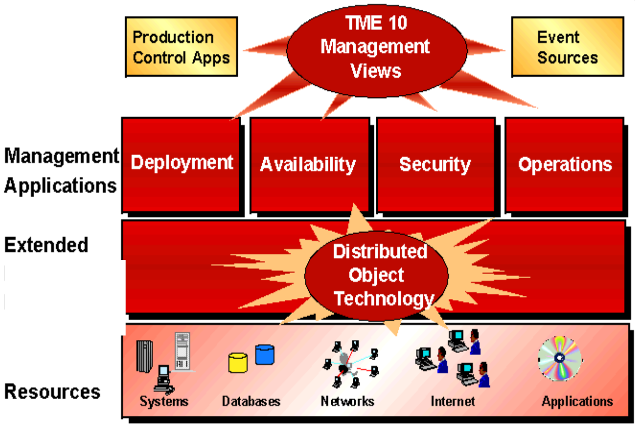
Cooperation

- Disorganized Point Solutions
- No Applications Management

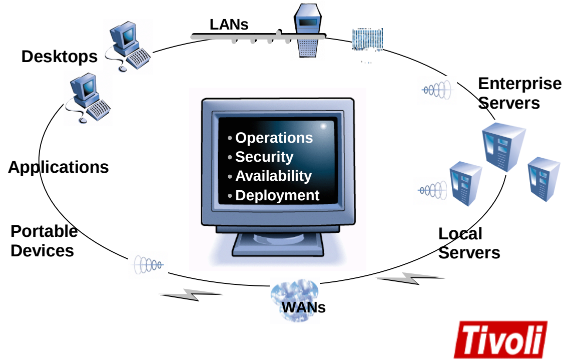
Agenda

- □ Challenges in Security Management
- Tivoli's Architecture and Security Offerings
- □ Role Based Security
- □ Getting Started
- □ Benefits
- □ Screenshots of GUI interface

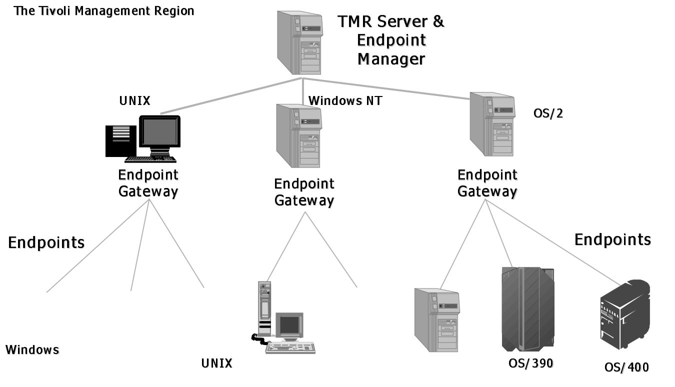
Tivoli Architecture



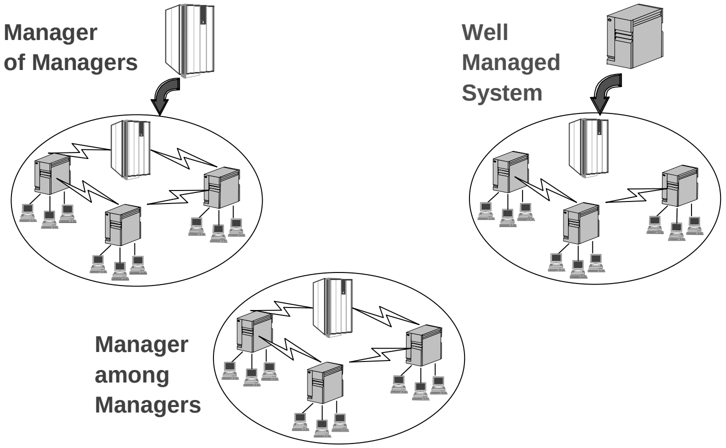
Single-action Management



Tivoli Management Architecture



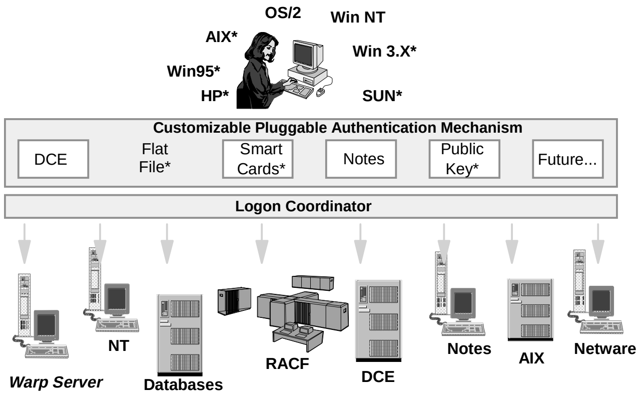
Role of OS/390



Tivoli's Security Offerings

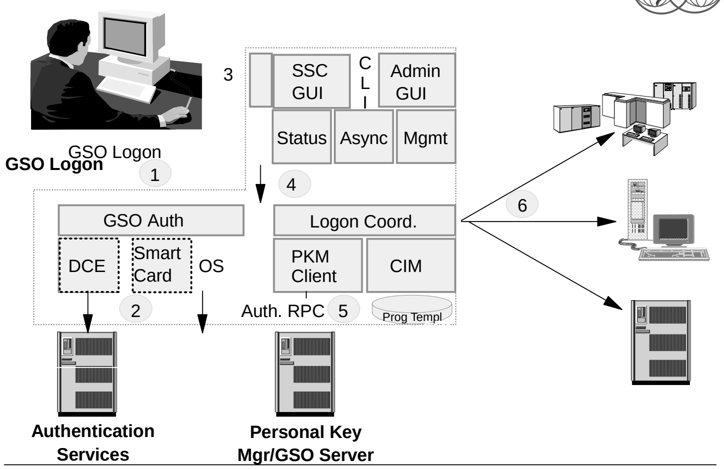
- Tivoli Global Signon (GSO)
- Tivoli User Administration
- Tivoli Security Management

Global Sign-on Framework



*Future Support

Global Sign-on Architecture



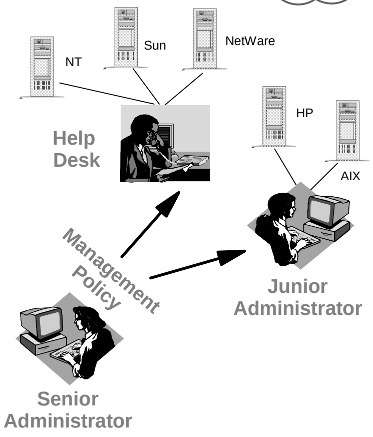
GSO Logon
GSO Logon
1
3
SSC GUI
C L I
Admin GUI
Status
Async
Mgmt
4
GSO Auth
DCE
Smart Card
OS
2
Logon Coord.
PKM Client
CIM
Auth. RPC
5
Prog Templ
6
Authentication Services
Personal Key Mgr/GSO Server

User Administration

- A single Tivoli user profile can define a user on many different platforms, applications and directories
  - RACF, OS/400, various UNIX implementations, Lotus Notes, Windows NT, NetWare, LDAP
- Supports all RACF user segments
- Extensible through Tivoli's Application Extension Facility
- Implementation of Default and Validation Policy

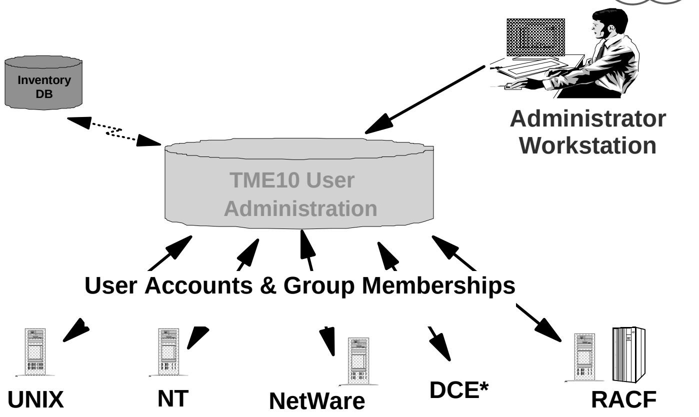
The Tivoli Approach

- Tivoli interface shields administrators from multi-platform complexity
- Object-based architecture provides tremendous scalability
- Management-by-policy ensures organizational compliance
- Secure delegation enables distributed responsibility



NT
Sun
NetWare
HP
AIX
Help Desk
Management Policy
Junior Administrator
Senior Administrator

The Tivoli Solution: Single-Action Mgmt



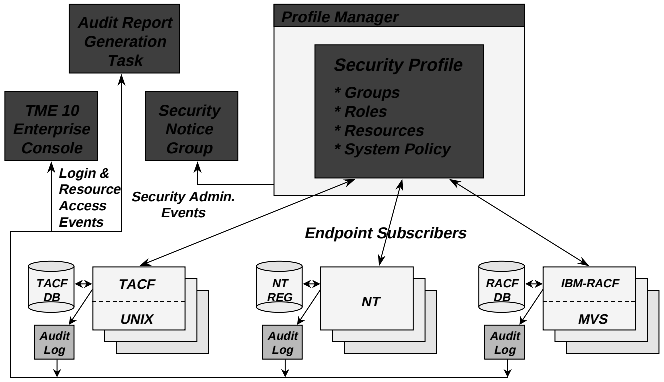
Inventory DB
Administrator Workstation
TME10 User Administration
User Accounts & Group Memberships
UNIX
NT
NetWare
DCE*
RACF

Security Management

- Implements a role based security model
  - new ROLE class in RACF
- Enforces a consistent Security Policy
- Utilizes native security where sufficient
  - RACF updates implemented through R-admin
  - No changes for user interaction
- Enhances UNIX Security

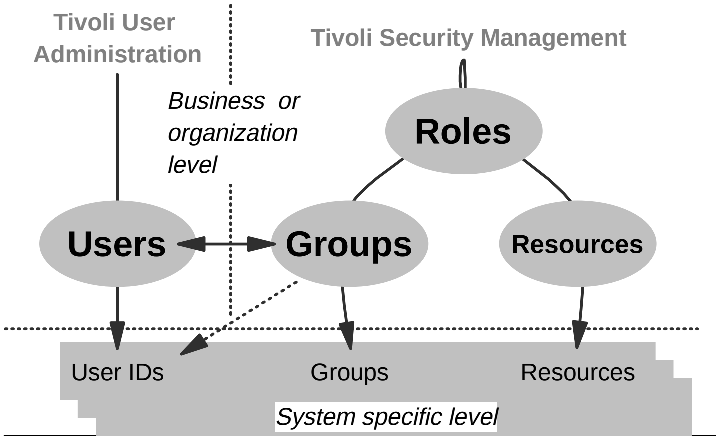
IBM Technical Support

Security Management Architecture



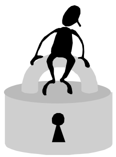
IBM Technical Support

Conceptual View


Tivoli User Administration
Tivoli Security Management
Business or organization level
Roles
Users
Groups
Resources
User IDs
Groups
Resources
System specific level

IBM Technical Support

An *Integrated* Tivoli Solution



TME 10 Security Management

- ★ **Centralized Policy Enforcement**
- ★ **Role-based Security Policy**
- ★ **Integrated Security in a Heterogeneous Environment**
- ★ **Robust Resource Access Control**
- ★ **Non-intrusive Architecture (no kernel modification)**

TME 10 User Administration

- ★ **Maintains Consistent Accounts / manages Common PW**
- ★ **Manages WinNT Accounts Across Multiple Domains**
- ★ **Single Action Management (Productivity)**
- ★ **Secure Granular Delegations to Remote Administrators**
- ★ **Integrated with TME 10 Security Management**

IBM Technical Support

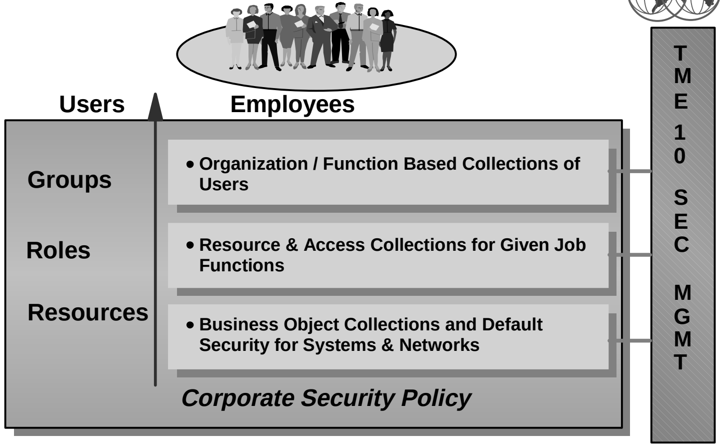
Agenda

- □ Challenges in Security Management
- □ Tivoli Architecture and Security Offerings
- ☛ Role Based Security
- □ Getting Started
- □ Benefits
- □ Screenshots of GUI interface

Key drivers for Role-Based Security

- □ High employee turnover
- □ High rate of reorganization / change
- □ Growth of organization
  - ➢ sheer volume of users
  - ➢ incredible "flux" of users
  - ➢ proliferation of user issues
- □ Complexity
- □ ROI of System Administration costs
- □ High Risk / cost of security breaches
- □ Changing ways of doing business ("coopetition" = competetion + cooperation)

Role-Based Resource Access Control



Users

Employees

Groups

Roles

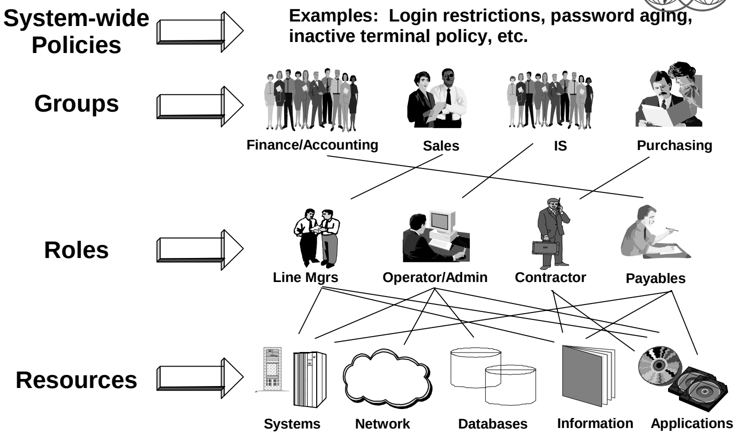
Resources

- Organization / Function Based Collections of Users
- Resource & Access Collections for Given Job Functions
- Business Object Collections and Default Security for Systems & Networks

Corporate Security Policy

TME 10 SEC MGMT

TME 10 Security Mgmt - Role-based Controls



System-wide Policies → Examples: Login restrictions, password aging, inactive terminal policy, etc.

Groups →

Roles →

Resources →

Agenda

- □ Challenges in Security Management
- □ Tivoli Architecture and Security Offerings
- □ Role Based Security
- ☛ Getting Started
- □ Benefits
- □ Screenshots of GUI interface

OS/390 Security Server Support

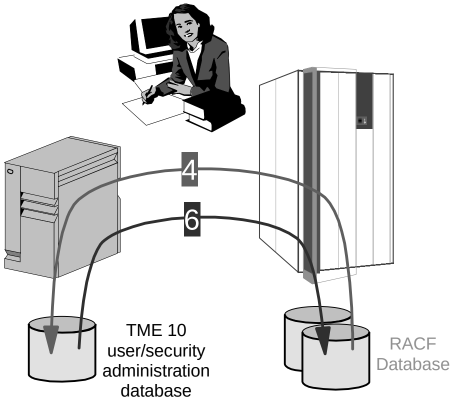
- □ Updated callable service - R_admin
- □ New general resource class - ROLE
- □ TME segment added to group, dataset, and general resource profiles
- □ Support shipped on OS/390 V1R3 and up
  - ➢ RACF PTFs: **UW90398, UW91102**
  - ➢ SAF PTFs: **UW90399, UW90463, UW91103**
  - ➢ In base of Version 2 Release 6

Dependencies

- □ The following Tivoli product sets must be installed at the 3.6+ level:
  - ➢ Tivoli Management Framework
  - ➢ Tivoli User Administration
  - ➢ Tivoli Security Management

Setting up Tivoli Security Administration

1. Create Tivoli User/Security administration profile
2. Create profile managers
   - ➢ *Create user profiles*
   - ➢ *Adding subscribers*
3. Set up TMEADMIN RACF profiles
4. Populate the profile
5. Modify entries
6. Distribute the profile



Getting Started

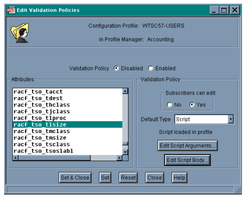
- Populate the Tivoli administration database with RACF data
  - Divide into manageable chunks
- Start with groups of a few hundred users requiring resources across all platforms such as administrators or managers
- Add custom classes to Tivoli to include them in roles

User accounts
and
access rights
Managers

Default and Validation Policy

- Default policies provide default values when creating a new record
- Validation policies flag impermissible values during the generation of records
- Policies are implemented as constants or shell scripts
- System Policy for generic policy (such as passwords)

```
#!/bin/sh
 #
 # Component Name: RacfTSOSizeVal
 #
 # $Date: 1998/03/03
 #
 # $Revision: 1.2 $
 #
 # Description: Provides a  point  of
 # modification to allow  a system  administrator to customize the policy
 # associated  with  RACF TSO Size .  When a
 # request to set the RACF TSO Size is made, it is validated  against
 # the policy implemented by this method.
 #
```



Edit Validation Policies

Configuration Profile: WTSC57-USERS

in Profile Manager: Accounting

Validation Policy ● Disabled ○ Enabled

Attributes:

```
racf_tso_tacct
racf_tso_tdest
racf_tso_thclass
racf_tso_tjclass
racf_tso_tlproc
racf_tso_tlsize
racf_tso_tmclass
racf_tso_tmsize
racf_tso_tsclass
racf_tso_tsoslabl
```

Validation Policy

Subscribers can edit ○ No ● Yes

Default Type: Script

Script loaded in profile

Implementing Role-based security

□ RACF already allowed for grouping of users and resources

➢ Restricted to grouping resources of the same class (like GCICSTRN)

□ Requires planning and synchronizing with other platforms (NT, UNIX) to define a consistent model

□ Ability to add your own resources for management through Tivoli AEF (user-defined classes)

Agenda

□ Challenges in Security Management

□ Tivoli Architecture and Security Offerings

□ Role Based Security

□ Getting Started

☛ Benefits

□ Screenshots of GUI interface

Benefits

- Tivoli Customers
  - Ability to manage RACF access using a role-based model
  - Manage RACF profiles from the Tivoli desktop
  - Ability for password changes to take effect on RACF
  - Common point of administration across the enterprise

Benefits

- OS/390 Customers
  - Allow helpdesk personnel to reset user passwords without requiring SPECIAL or OWNER attribute
  - Ability to set a password which is not marked as expired
  - Allow installations to code to an API that has the same abilities as all commands for users, groups and resources

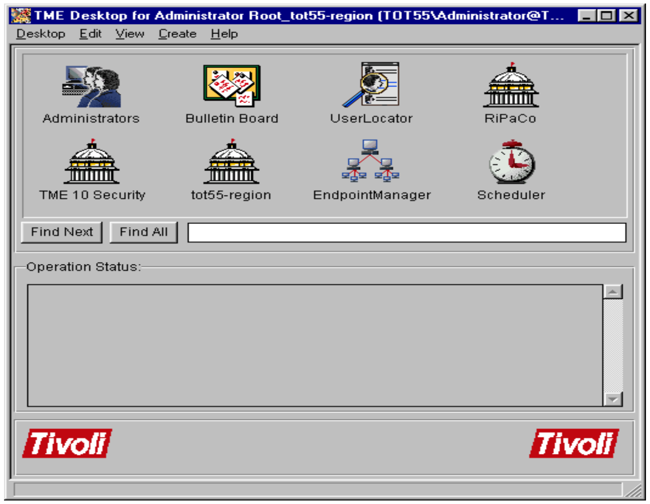
Other benefits

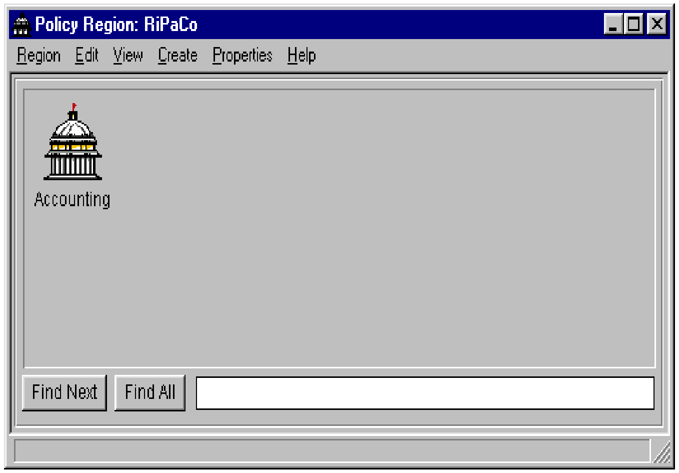
- Password management, reset password across platforms
  - Tivoli wpasswd command
  - Onepassword web tool
- Execute RACF commands from management workstation
- Administrative actions tracked in a Notices database
- Integration with other Tivoli management products
  - Tivoli Enterprise Console - event correlation across security systems
  - Tivoli Distributed Monitoring for Security Alarming (Watchdog !)
- Full message text returned (with SAF and RACF return and reason codes where appropriate)

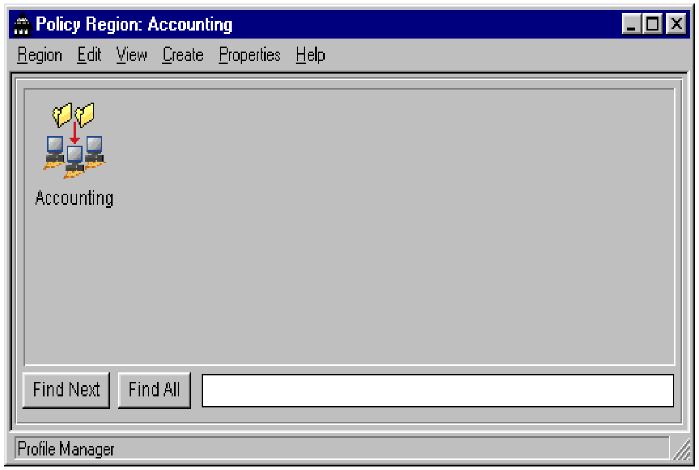
Agenda

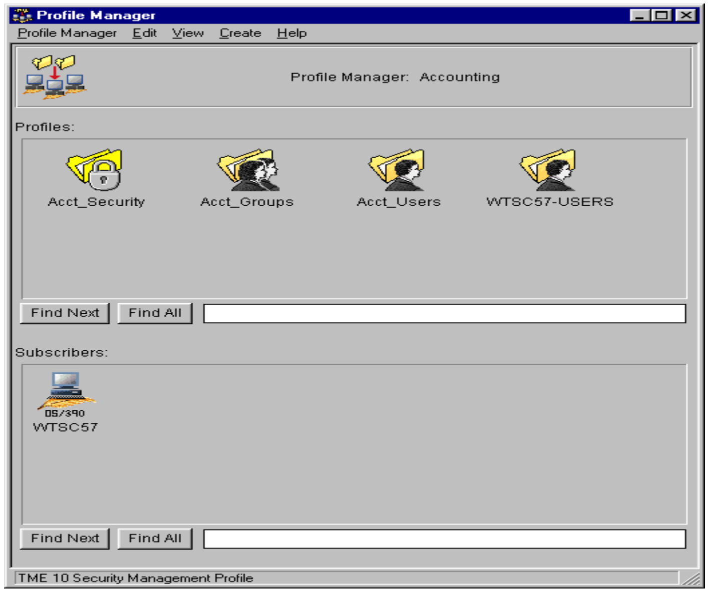
- Challenges in Security Management
- Tivoli Architecture and Security Offerings
- Role Based Security
- Getting Started
- Benefits

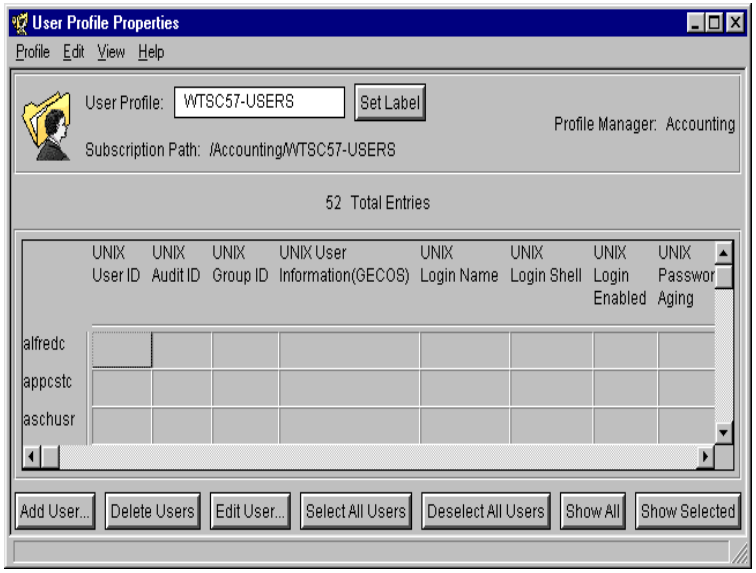
☛ Screenshots of GUI interface


TME Desktop for Administrator Root_tot55-region (TOT55\Administrator@T...
Desktop Edit View Create Help
Administrators
Bulletin Board
UserLocator
RiPaCo
TME 10 Security
tot55-region
EndpointManager
Scheduler
Find Next
Find All
Operation Status:
Tivoli
Tivoli


Policy Region: RiPaCo
Region Edit View Create Properties Help
Accounting
Find Next
Find All


Policy Region: Accounting
Region Edit View Create Properties Help
Accounting
Find Next
Find All
Profile Manager


Profile Manager
Profile Manager Edit View Create Help
Profile Manager: Accounting
Profiles:
Acct_Security
Acct_Groups
Acct_Users
WTSC57-USERS
Find Next
Find All
Subscribers:
OS/390
WTSC57
Find Next
Find All
TME 10 Security Management Profile



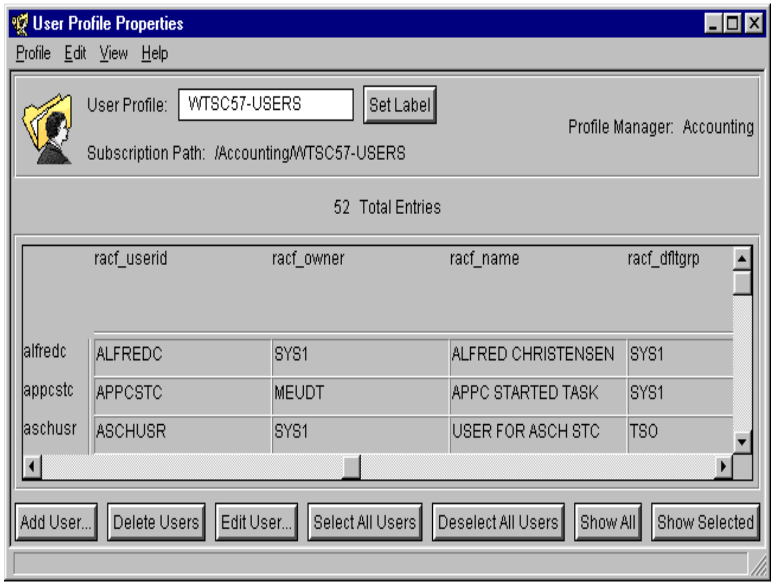
User Profile: WTSC57-USERS

Subscription Path: /Accounting/WTSC57-USERS

Profile Manager: Accounting

52 Total Entries

	UNIX User ID	UNIX Audit ID	UNIX Group ID	UNIX User Information(GECOS)	UNIX Login Name	UNIX Login Shell	UNIX Login Enabled	UNIX Passwor Aging
alfredc								
appcstc								
aschusr								



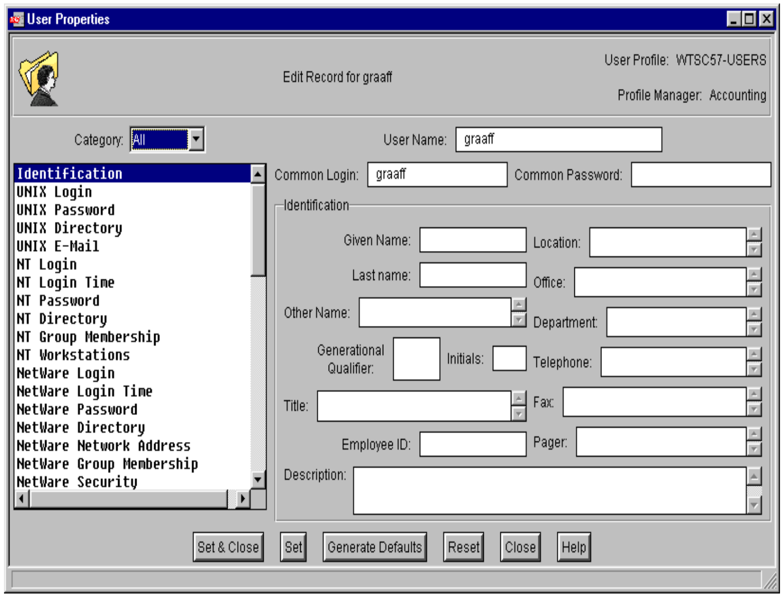
User Profile: WTSC57-USERS

Subscription Path: /Accounting/WTSC57-USERS

Profile Manager: Accounting

52 Total Entries

	racf_userid	racf_owner	racf_name	racf_dfltgrp
alfredc	ALFREDC	SYS1	ALFRED CHRISTENSEN	SYS1
appcstc	APPCSTC	MEUDT	APPC STARTED TASK	SYS1
aschusr	ASCHUSR	SYS1	USER FOR ASCH STC	TSO



Edit Record for graaff

User Profile: WTSC57-USERS

Profile Manager: Accounting

Category: All

User Name: graaff

Common Login: graaff

Common Password:

Identification

Given Name:

Location:

Last name:

Office:

Other Name:

Department:

Generational Qualifier:

Initials:

Telephone:

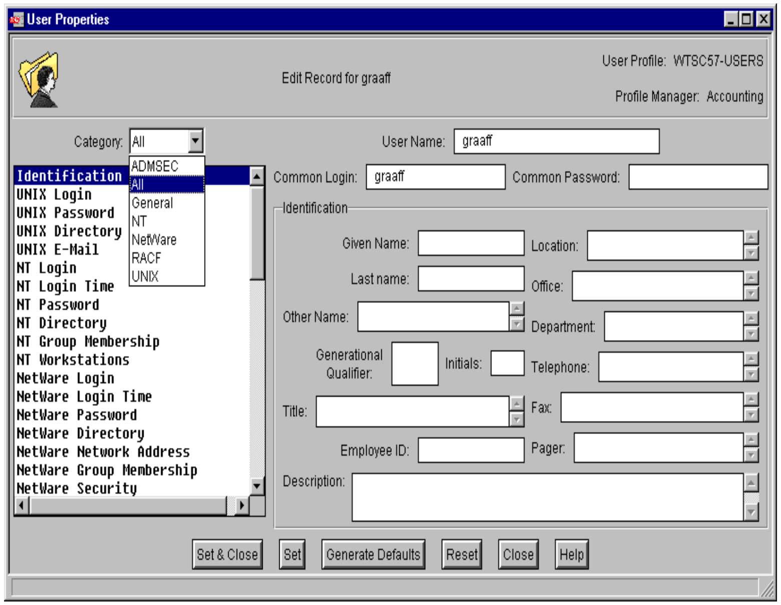
Title:

Fax:

Employee ID:

Pager:

Description:



Edit Record for graaff

User Profile: WTSC57-USERS

Profile Manager: Accounting

Category: All

User Name: graaff

Common Login: graaff

Common Password:

Identification

Given Name:

Location:

Last name:

Office:

Other Name:

Department:

Generational Qualifier:

Initials:

Telephone:

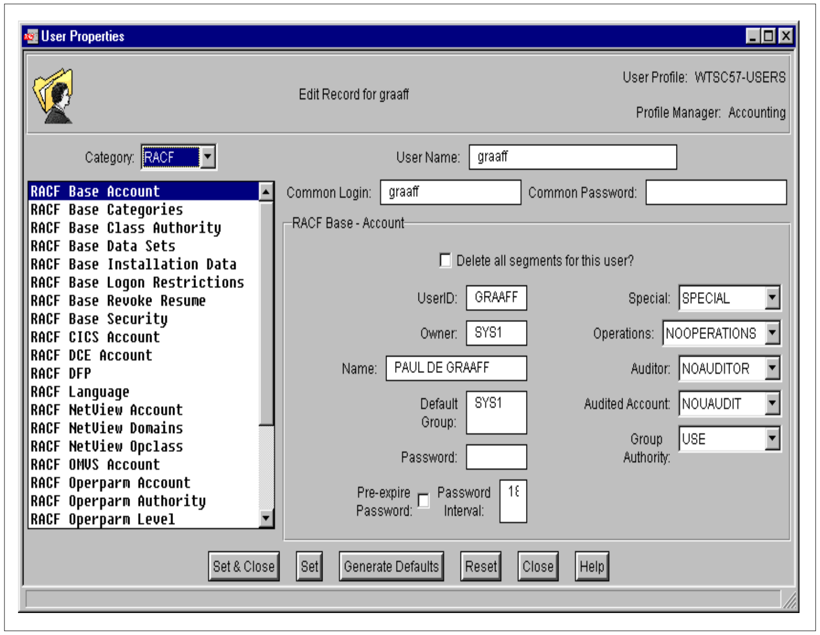
Title:

Fax:

Employee ID:

Pager:

Description:



User Properties

Edit Record for graaff

User Profile: WTSC57-USERS

Profile Manager: Accounting

Category: RACF

User Name: graaff

Common Login: graaff

Common Password:

```
RACF Base Account
RACF Base Categories
RACF Base Class Authority
RACF Base Data Sets
RACF Base Installation Data
RACF Base Logon Restrictions
RACF Base Revoke Resume
RACF Base Security
RACF CICS Account
RACF DCE Account
RACF DFP
RACF Language
RACF NetView Account
RACF NetView Domains
RACF NetView Opclass
RACF OMVS Account
RACF Operparm Account
RACF Operparm Authority
RACF Operparm Level
```

RACF Base - Account

☐ Delete all segments for this user?

UserID: GRAAFF

Owner: SYS1

Name: PAUL DE GRAAFF

Default Group: SYS1

Password:

Pre-expire Password: ☐

Password Interval: 1ε

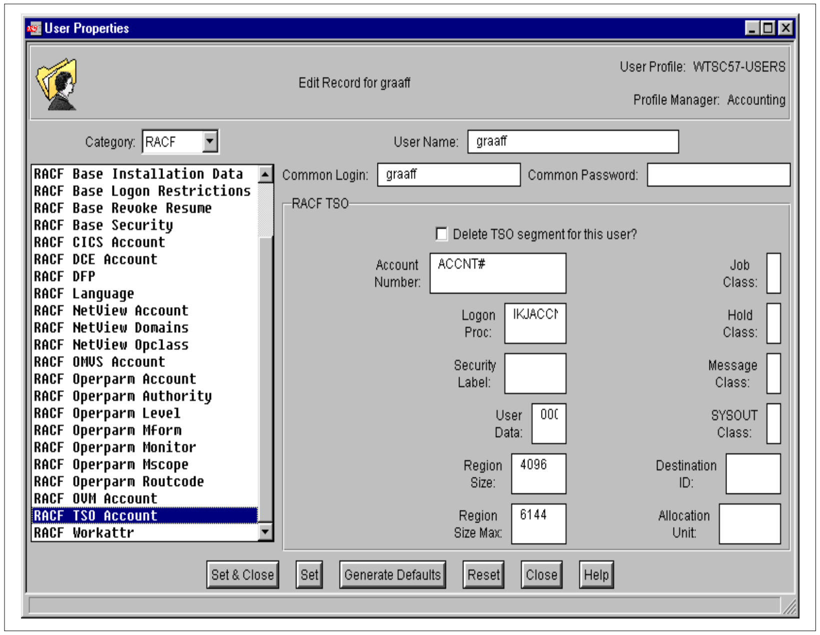
Special: SPECIAL

Operations: NOOPERATIONS

Auditor: NOAUDITOR

Audited Account: NOUAUDIT

Group Authority: USE



User Properties

Edit Record for graaff

User Profile: WTSC57-USERS

Profile Manager: Accounting

Category: RACF

User Name: graaff

Common Login: graaff

Common Password:

```
RACF Base Installation Data
RACF Base Logon Restrictions
RACF Base Revoke Resume
RACF Base Security
RACF CICS Account
RACF DCE Account
RACF DFP
RACF Language
RACF NetView Account
RACF NetView Domains
RACF NetView Opclass
RACF OMVS Account
RACF Operparm Account
RACF Operparm Authority
RACF Operparm Level
RACF Operparm MForm
RACF Operparm Monitor
RACF Operparm Mscope
RACF Operparm Routcode
RACF OVM Account
RACF TSO Account
RACF Workattr
```

RACF TSO

☐ Delete TSO segment for this user?

Account Number: ACCNT#

Logon Proc: IKJACCN

Security Label:

User Data: 000

Region Size: 4096

Region Size Max: 6144

Job Class:

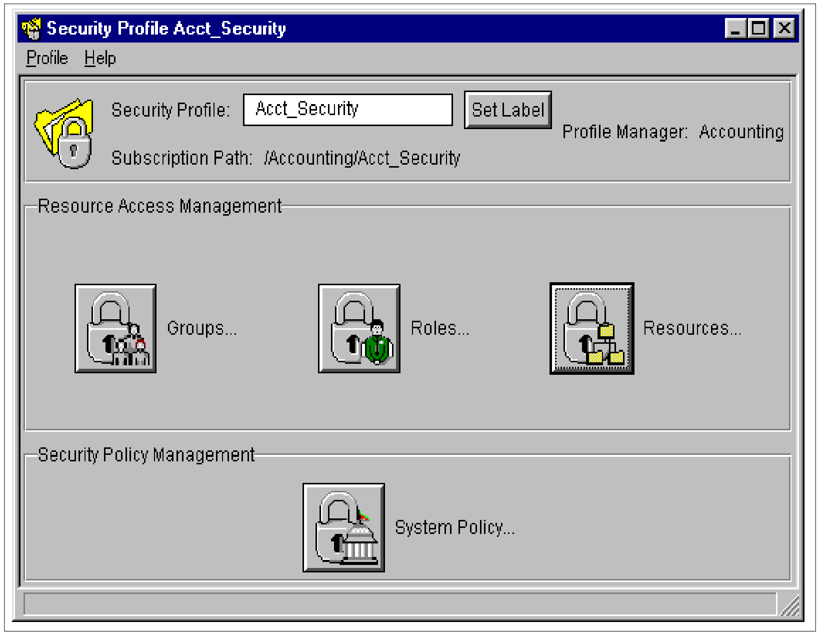
Hold Class:

Message Class:

SYSOUT Class:

Destination ID:

Allocation Unit:

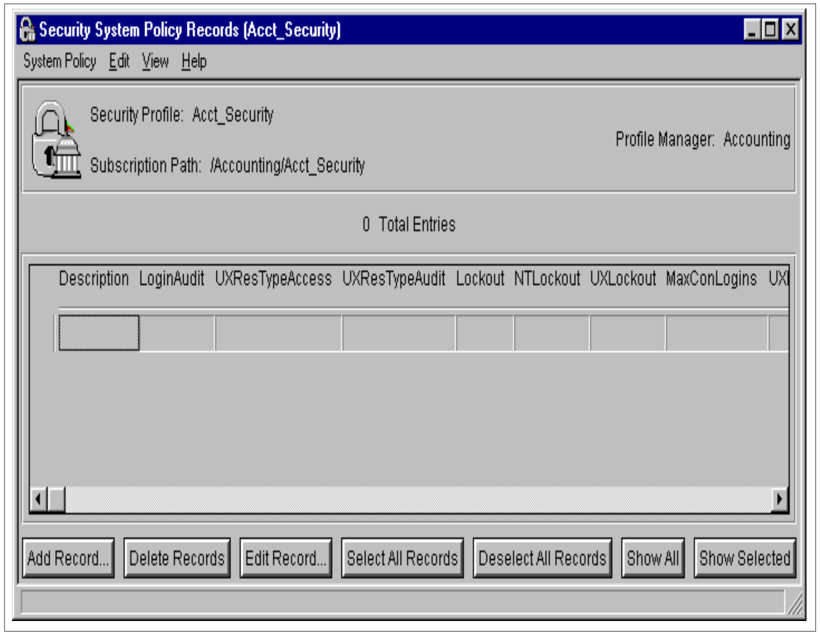


Security Profile Acct_Security

Security Profile: Acct_Security

Profile Manager: Accounting

Subscription Path: /Accounting/Acct_Security



Security System Policy Records (Acct_Security)

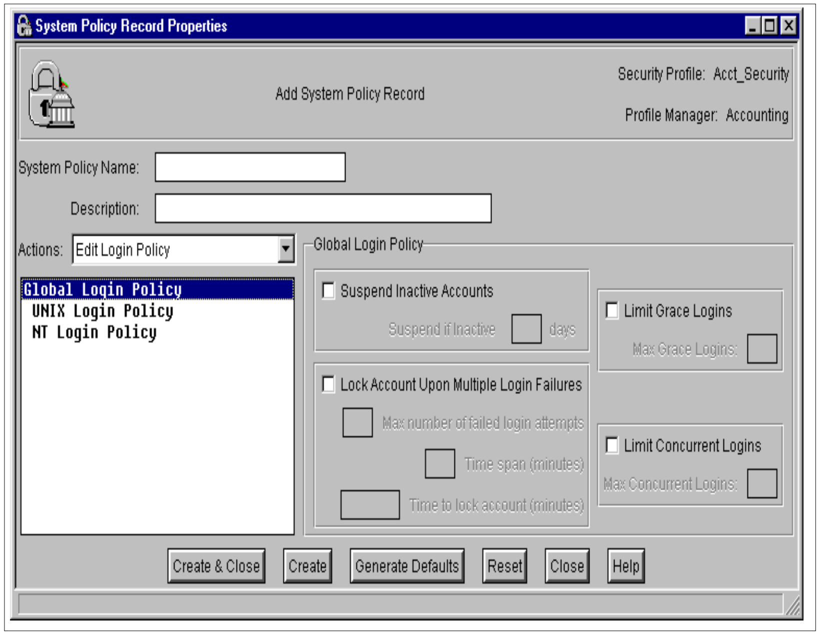
Security Profile: Acct_Security

Profile Manager: Accounting

Subscription Path: /Accounting/Acct_Security

0 Total Entries

Description	LoginAudit	UXResTypeAccess	UXResTypeAudit	Lockout	NTLockout	UXLockout	MaxConLogins	UX



System Policy Record Properties

Add System Policy Record

Security Profile: Acct_Security

Profile Manager: Accounting

System Policy Name:

Description:

Actions: Edit Login Policy

Global Login Policy
UNIX Login Policy
NT Login Policy

Global Login Policy

□ Suspend Inactive Accounts

Suspend if Inactive □ days

□ Lock Account Upon Multiple Login Failures

□ Max number of failed login attempts

□ Time span (minutes)

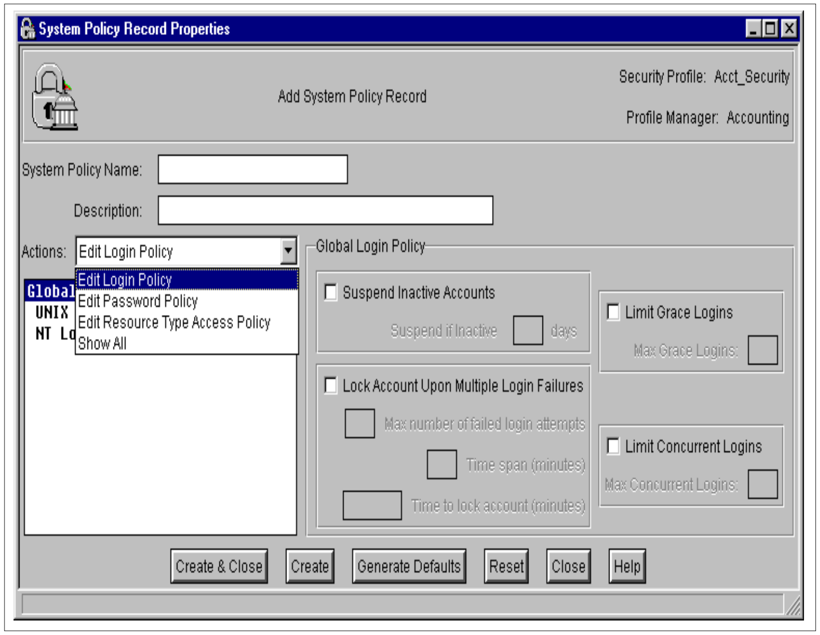
□ Time to lock account (minutes)

□ Limit Grace Logins

Max Grace Logins: □

□ Limit Concurrent Logins

Max Concurrent Logins: □



System Policy Record Properties

Add System Policy Record

Security Profile: Acct_Security

Profile Manager: Accounting

System Policy Name:

Description:

Actions: Edit Login Policy

Global
UNIX
NT Lo

Global Login Policy

□ Suspend Inactive Accounts

Suspend if Inactive □ days

□ Lock Account Upon Multiple Login Failures

□ Max number of failed login attempts

□ Time span (minutes)

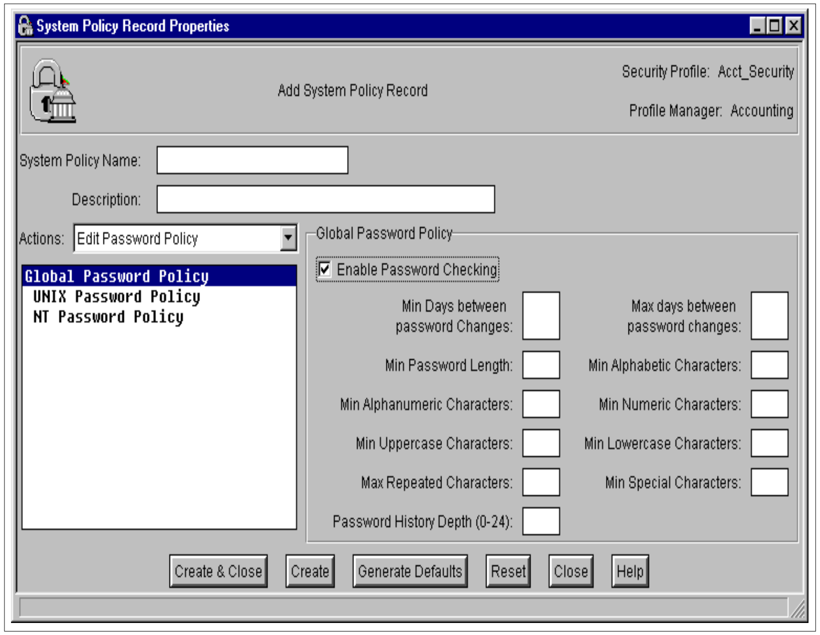
□ Time to lock account (minutes)

□ Limit Grace Logins

Max Grace Logins: □

□ Limit Concurrent Logins

Max Concurrent Logins: □



System Policy Record Properties

Add System Policy Record

Security Profile: Acct_Security

Profile Manager: Accounting

System Policy Name:

Description:

Actions: Edit Password Policy

Global Password Policy
UNIX Password Policy
NT Password Policy

Global Password Policy

☑ Enable Password Checking

Min Days between password Changes: □

Max days between password changes: □

Min Password Length: □

Min Alphabetic Characters: □

Min Alphanumeric Characters: □

Min Numeric Characters: □

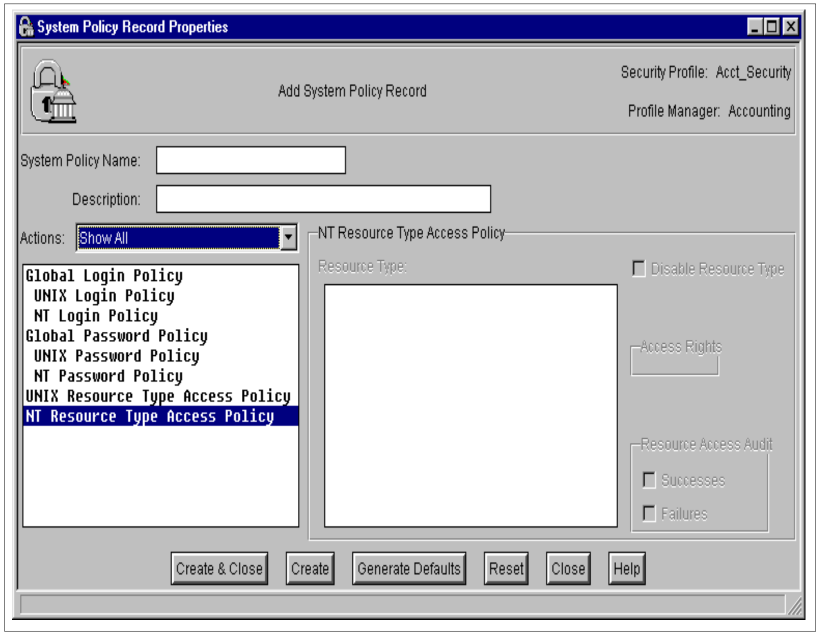
Min Uppercase Characters: □

Min Lowercase Characters: □

Max Repeated Characters: □

Min Special Characters: □

Password History Depth (0-24): □



System Policy Record Properties

Add System Policy Record

Security Profile: Acct_Security

Profile Manager: Accounting

System Policy Name:

Description:

Actions: Show All

Global Login Policy
UNIX Login Policy
NT Login Policy
Global Password Policy
UNIX Password Policy
NT Password Policy
UNIX Resource Type Access Policy
NT Resource Type Access Policy

NT Resource Type Access Policy

Resource Type:

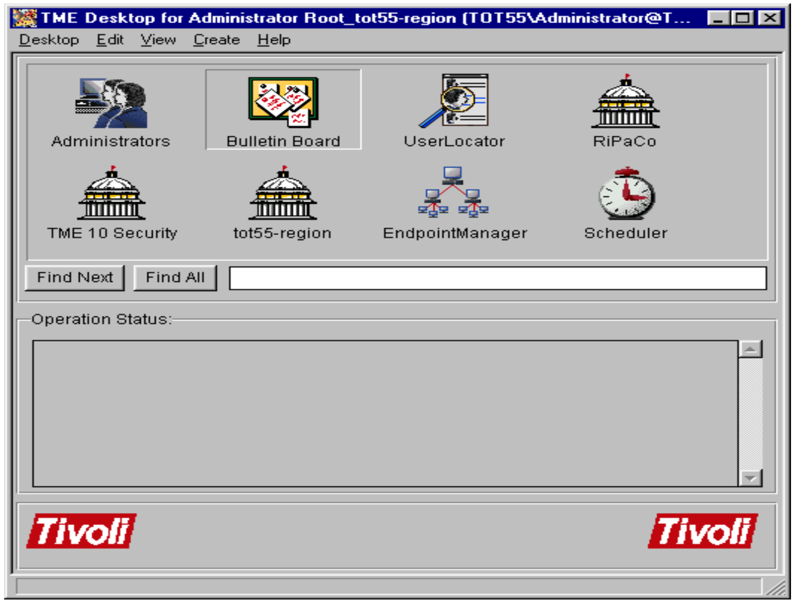
□ Disable Resource Type

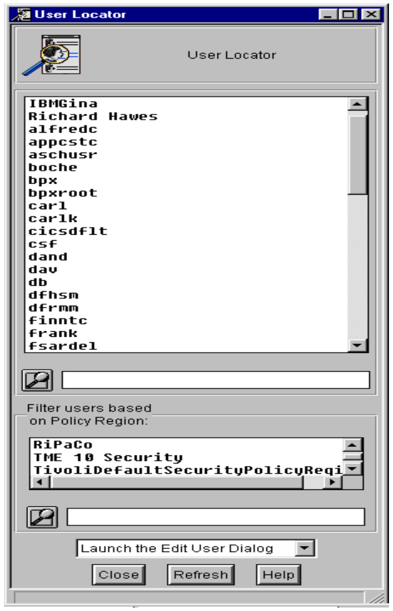
Access Rights

Resource Access Audit

□ Successes

□ Failures

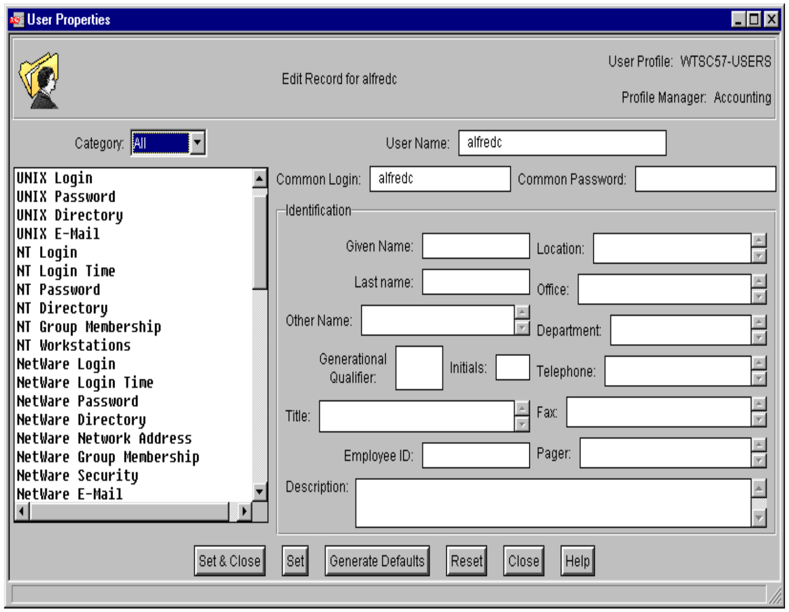




User Locator
User Locator
Filter users based on Policy Region:
Launch the Edit User Dialog
Close
Refresh
Help

```
IBMGina
Richard Hawes
alfredc
appcstc
aschusr
boche
bpx
bpxroot
carl
carlk
cicsdflt
csf
dand
dav
db
dfhsm
dfrmm
finntc
frank
fsardel
```

```
RiPaCo
TME 10 Security
TivoliDefaultSecurityPolicyRegi
```



Edit Record for alfredc

User Profile: WTSC57-USERS

Profile Manager: Accounting

Category: All

User Name: alfredc

Common Login: alfredc

Common Password:

Given Name:

Location:

Last name:

Office:

Other Name:

Department:

Generational Qualifier:

Initials:

Telephone:

Title:

Fax:

Employee ID:

Pager:

Description:

```
UNIX Login
UNIX Password
UNIX Directory
UNIX E-Mail
NT Login
NT Login Time
NT Password
NT Directory
NT Group Membership
NT Workstations
NetWare Login
NetWare Login Time
NetWare Password
NetWare Directory
NetWare Network Address
NetWare Group Membership
NetWare Security
NetWare E-Mail
```

To find out more

- □ Tivoli OS/390 and Enterprise Management Information
  - ➢ http://www.tivoli.com/os390
  - ➢ http://www.tivoli.com/o_products/html/body_products.html
- □ Redbooks - http://www.redbooks.ibm.com/solutions/tivoli
  - ➢ SG24-2015 Getting Started with TME 10 User Administration
  - ➢ SG24-5108 Tivoli User Administration Design Guide
  - ➢ SG24-2021 Introducing TME 10 Security Management
  - ➢ SG24-5101 Tivoli Security Management Design Guide
  - ➢ SG24-5339 Managing OS/390 Security Server with Tivoli