Managing RACF with Tivoli User Administration and Security Management

Vanguard Enterprise Security Expo 2000

Bruce R. Wells
SecureWay OS/390 Security Server
Poughkeepsie, New York

(914) 435-7498
brwells@us.ibm.com

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

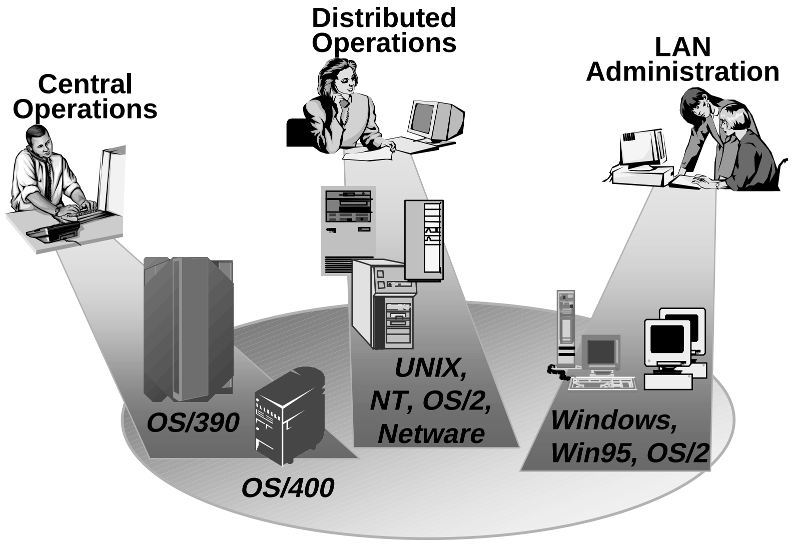
The following are trademarks or registered trademarks of other companies or institutions:

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

Agenda

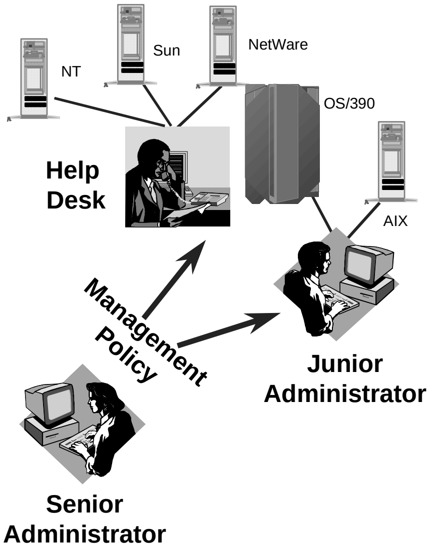
- Overview
- Tivoli User Administration
- Tivoli Security Management
- Role Based Security
- Sources for Additional Information

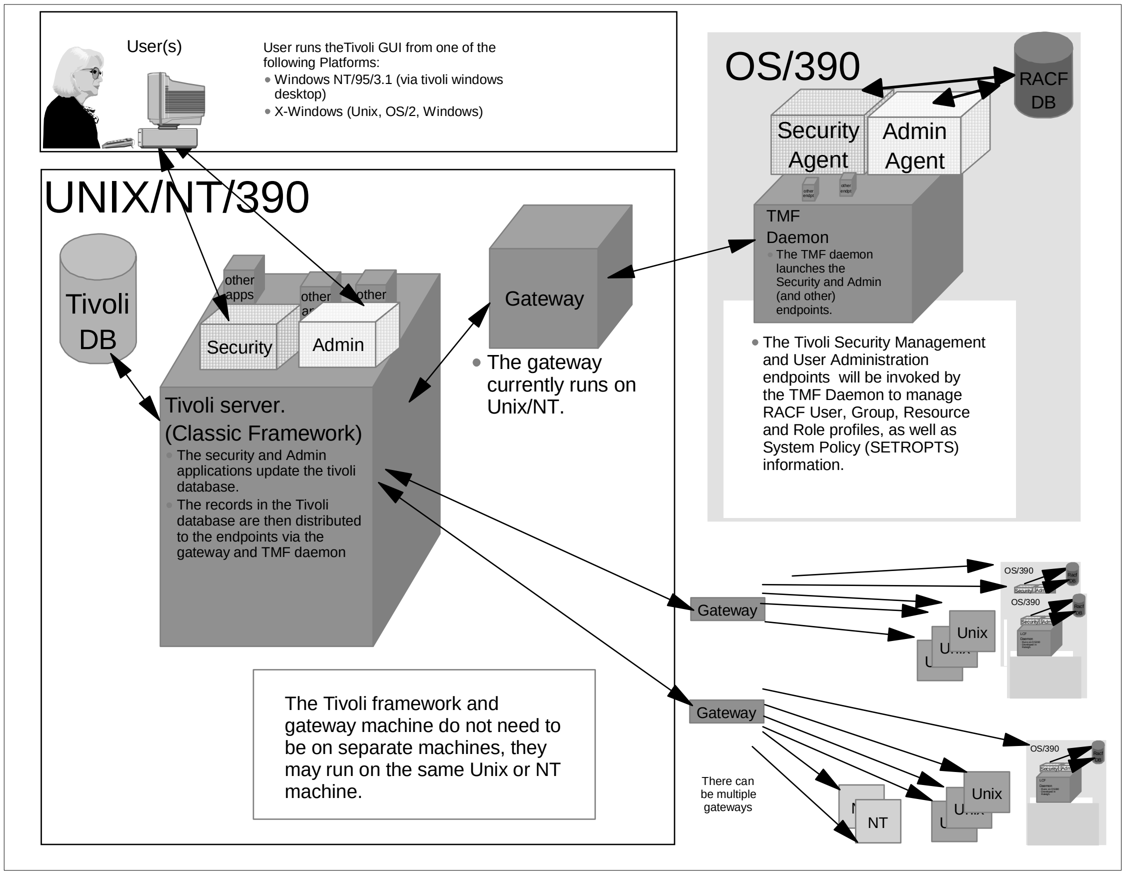
The Problem: Islands of Management



The Tivoli Approach

- Management by Policy
- Secure delegation - decentralized administration
- Single Tivoli interface shields Administrators from multi-platform complexity
- Single Action Management reduces errors, increases productivity
- Manage multiple instances of the same security model





User runs theTivoli GUI from one of the following Platforms:

- Windows NT/95/3.1 (via tivoli windows desktop)
- X-Windows (Unix, OS/2, Windows)

Tivoli server.
(Classic Framework)

- The security and Admin applications update the tivoli database.
- The records in the Tivoli database are then distributed to the endpoints via the gateway and TMF daemon

- The gateway currently runs on Unix/NT.

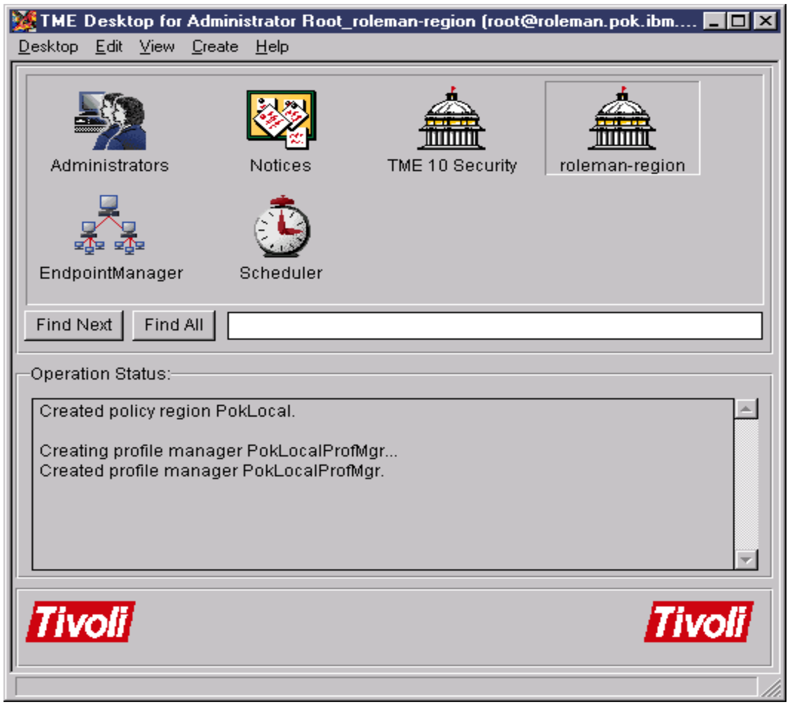
- The TMF daemon launches the Security and Admin (and other) endpoints.

- The Tivoli Security Management and User Administration endpoints will be invoked by the TMF Daemon to manage RACF User, Group, Resource and Role profiles, as well as System Policy (SETROPTS) information.

The Tivoli framework and gateway machine do not need to be on separate machines, they may run on the same Unix or NT machine.

There can be multiple gateways

The Tivoli Desktop



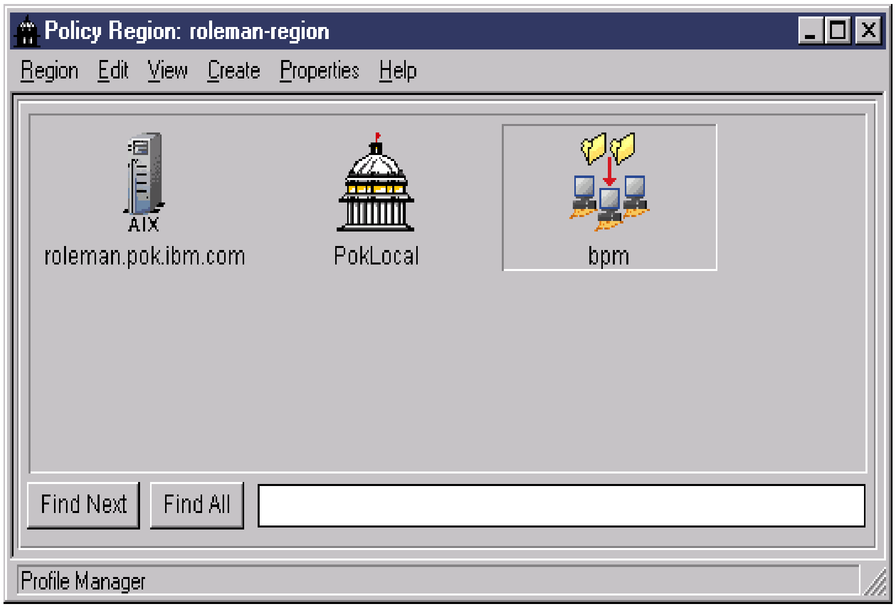
```
Created policy region PokLocal.

Creating profile manager PokLocalProfMgr...
Created profile manager PokLocalProfMgr.
```

- This is the main tivoli desktop. What you see depends on your administrative authority. These are all functions provided by the framework.

The icons you see are

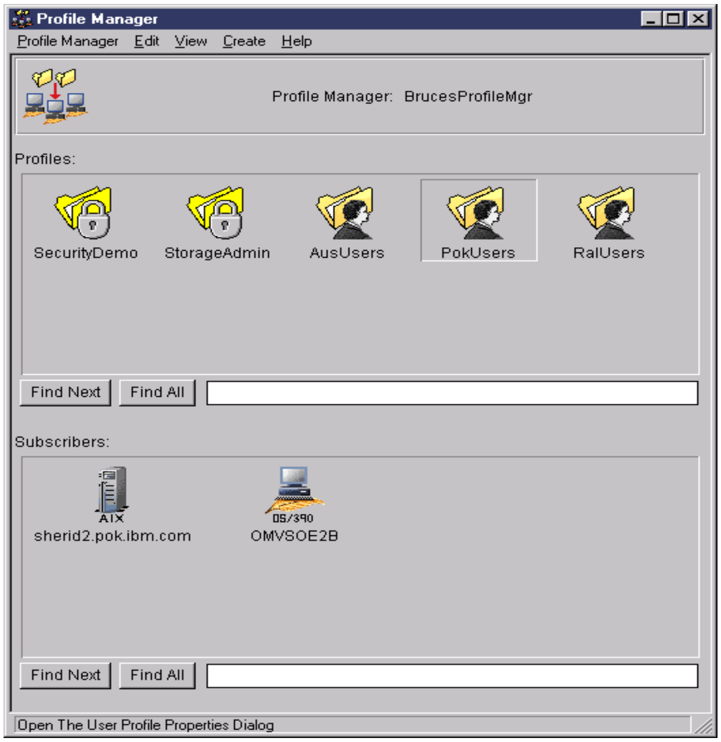
- Administrators. Defines your login names, your roles, what notice groups you can see, etc. For RACF, these are mapped to RACF user IDs using profiles in the TMEADMIN class.
- Notices. Interface into notice goups
- UserLocator: Only if User Administration is installed. Allows you to quickly locate a user record.
- Policy regions: collections of hosts and profile managers
- Endpoint Manager. Defines which endpoints are serviced by which gateways
- Scheduler. Automated jobs and tasks.

A Policy Region



- View into a policy region
- A policy region is a collection of objects which share certain policy characteristics
- You can limit the types of resources which can be contained in a given policy region
- Administrative rights can be granted to manage the resources within a policy region
- Policy regions can be nested, and used for decentralized administration
- A profile manager is selected

A Profile Manager

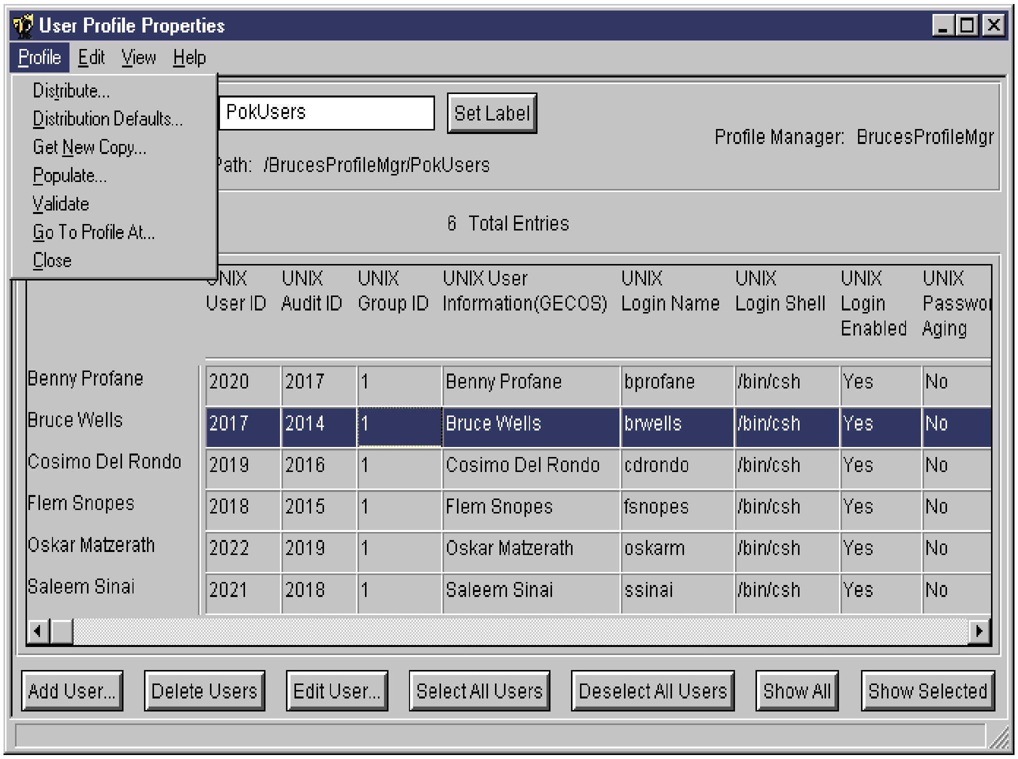


Profile Manager: BrucesProfileMgr

Open The User Profile Properties Dialog

- A collection of Tivoli User Adminsitration (TUA) and Tivoli Security Managemnt (TSM) profiles in a profile manager.
- Other applications will allow for other profile types on the "Create ..." pulldown
- subscribers are set at the profile manager level
- Subscribers can be actual endpoints, or other profile managers
- You can distribute data at the level of profile manager, or at the profile level
- We will look inside a user profile

User Profile Table View



PokUsers

Path: /BrucesProfileMgr/PokUsers

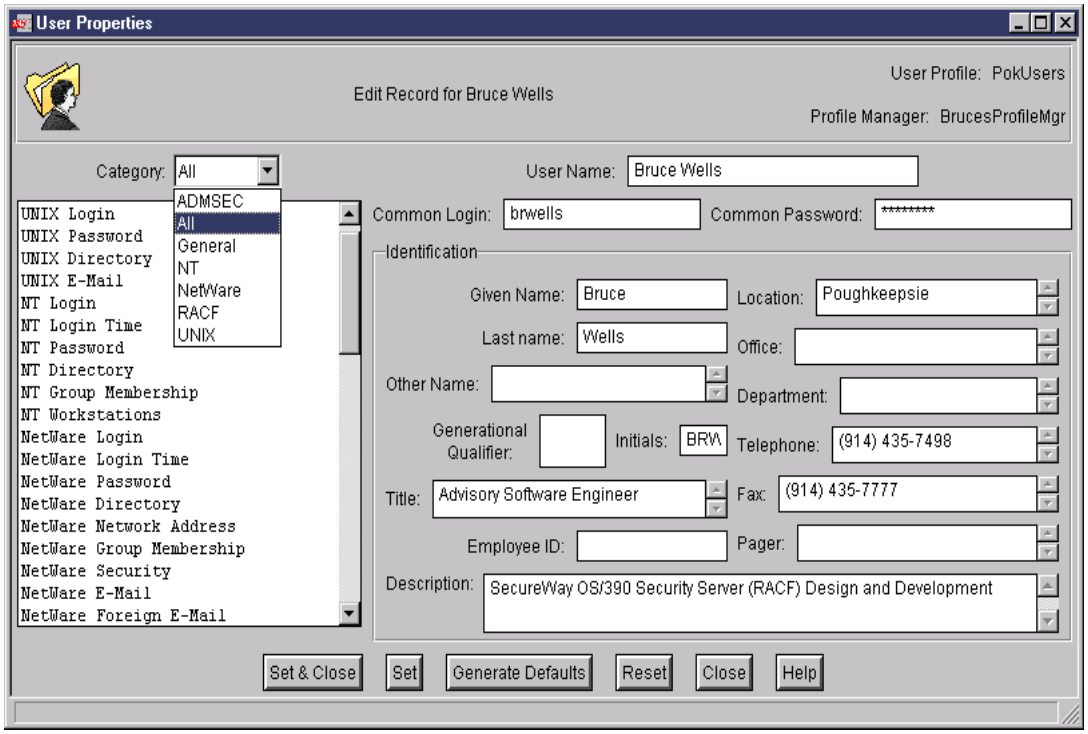
Profile Manager: BrucesProfileMgr

6 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 Passwo Aging
Benny Profane	2020	2017	1	Benny Profane	bprofane	/bin/csh	Yes	No
Bruce Wells	2017	2014	1	Bruce Wells	brwells	/bin/csh	Yes	No
Cosimo Del Rondo	2019	2016	1	Cosimo Del Rondo	cdrondo	/bin/csh	Yes	No
Flem Snopes	2018	2015	1	Flem Snopes	fsnopes	/bin/csh	Yes	No
Oskar Matzerath	2022	2019	1	Oskar Matzerath	oskarm	/bin/csh	Yes	No
Saleem Sinai	2021	2018	1	Saleem Sinai	ssinai	/bin/csh	Yes	No

- This is the table view of the user records defined within this profile
- The pull down menus allow various profile-oriented operations like populate, distribute, validate, etc
- double-clicking a row will get us into the gui view for that user record

User Record Main Panel



User Properties

Edit Record for Bruce Wells

User Profile: PokUsers

Profile Manager: BrucesProfileMgr

Category: All

User Name: Bruce Wells

Common Login: brwells

Common Password: ********

Identification

Given Name: Bruce

Location: Poughkeepsie

Last name: Wells

Office:

Other Name:

Department:

Generational Qualifier:

Initials: BRW

Telephone: (914) 435-7498

Title: Advisory Software Engineer

Fax: (914) 435-7777

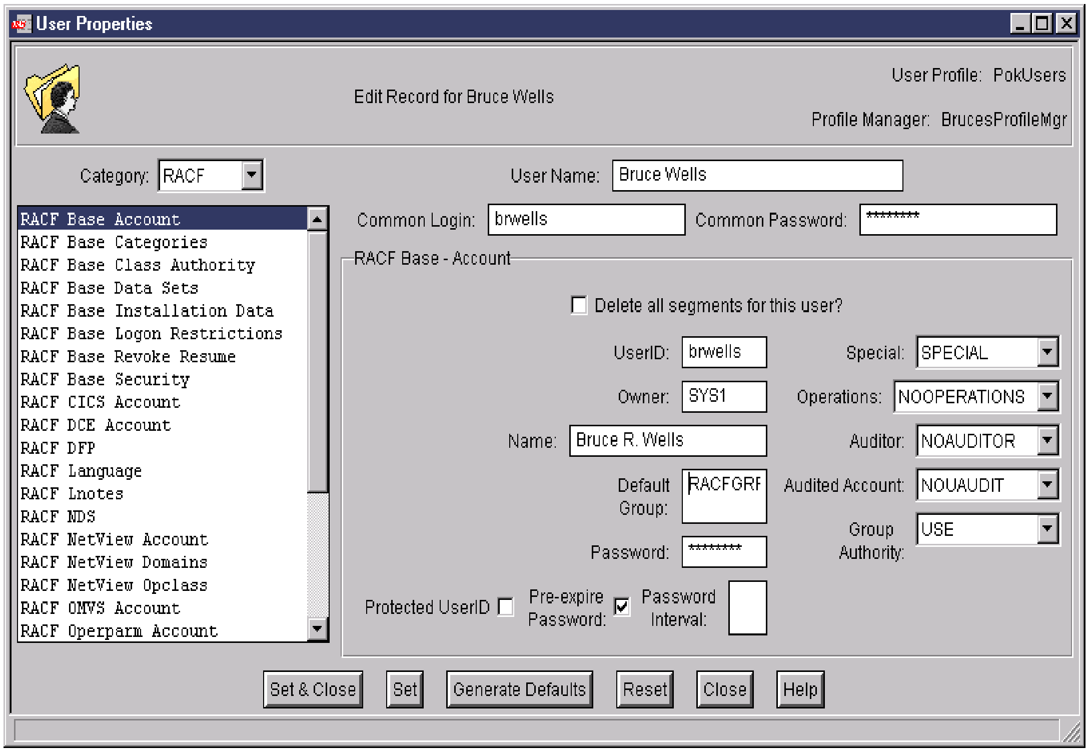
Employee ID:

Pager:

Description: SecureWay OS/390 Security Server (RACF) Design and Development

- This is the first panel you see.
- You can enter a common user ID and password to be used across all accounts on all platforms
- Or you can define endpoint-specific info
- There are separate categories for all kinds of endpoint types
- A commandline interface (for both TUA and TSM) can also be used to manipulate profiles and properties.
- The default view is "All’, which displays all the subcategories in the list on the left.
- We select "RACF" and see the next slide ....

RACF Basic Data Panel



User Properties

Edit Record for Bruce Wells

User Profile: PokUsers

Profile Manager: BrucesProfileMgr

Category: RACF

User Name: Bruce Wells

Common Login: brwells

Common Password: ********

RACF Base - Account

□ Delete all segments for this user?

UserID: brwells

Owner: SYS1

Name: Bruce R. Wells

Default Group: RACFGRF

Password: ********

Protected UserID □

Pre-expire Password: ☑

Password Interval:

Special: SPECIAL

Operations: NOOPERATIONS

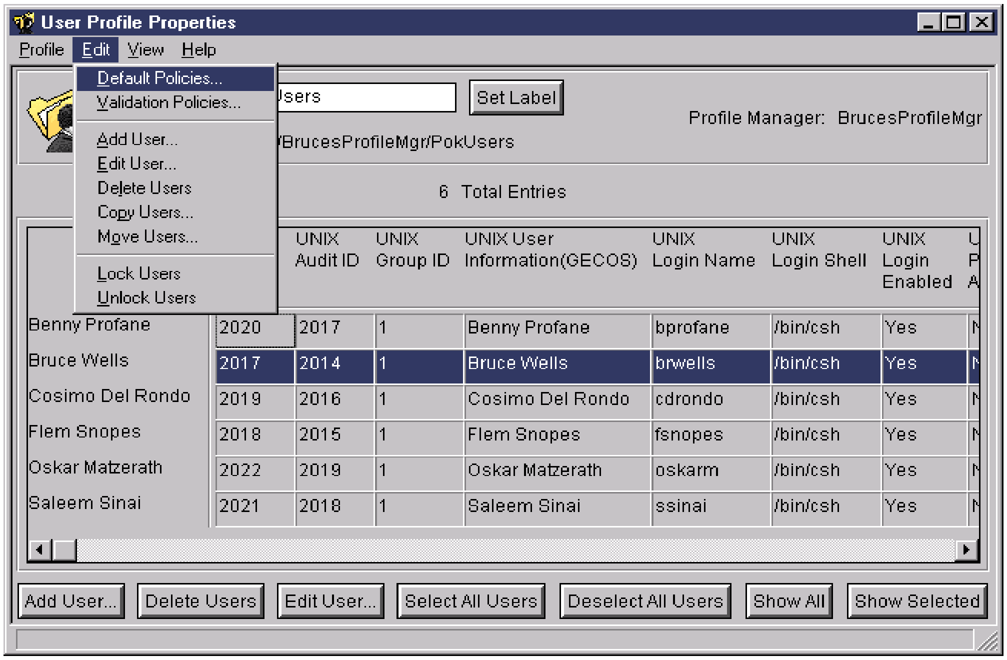
Auditor: NOAUDITOR

Audited Account: NOUAUDIT

Group Authority: USE

- This is the RACF Base Account panel
- There are subcategories for every RACF user profile segment
- Note that the common password and login name can be overridden with RACF specifics

Editing Default Policy



sers

Profile Manager: BrucesProfileMgr

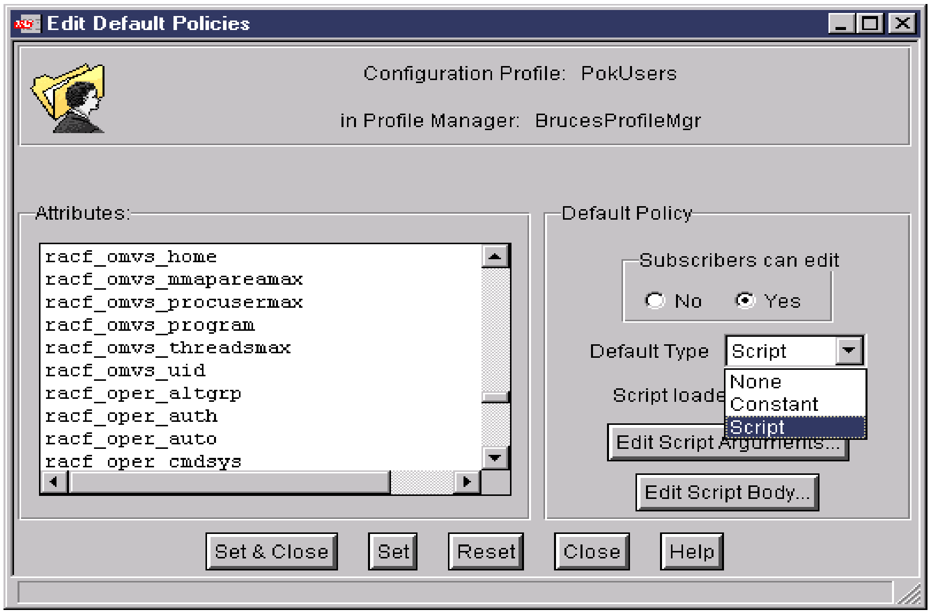
/BrucesProfileMgr/PokUsers

6 Total Entries

		UNIX Audit ID	UNIX Group ID	UNIX User Information(GECOS)	UNIX Login Name	UNIX Login Shell	UNIX Login Enabled	U P A
Benny Profane	2020	2017	1	Benny Profane	bprofane	/bin/csh	Yes	N
Bruce Wells	2017	2014	1	Bruce Wells	brwells	/bin/csh	Yes	N
Cosimo Del Rondo	2019	2016	1	Cosimo Del Rondo	cdrondo	/bin/csh	Yes	N
Flem Snopes	2018	2015	1	Flem Snopes	fsnopes	/bin/csh	Yes	N
Oskar Matzerath	2022	2019	1	Oskar Matzerath	oskarm	/bin/csh	Yes	N
Saleem Sinai	2021	2018	1	Saleem Sinai	ssinai	/bin/csh	Yes	N

- One of the most powerful features of Tivoli is the ability to apply default policy and enforce validation policy
- Get to these functions using the Edit pull-down menu

Editing Default Policy ...



Edit Default Policies

Configuration Profile: PokUsers

in Profile Manager: BrucesProfileMgr

Attributes:

```
racf_omvs_home
racf_omvs_mmapareamax
racf_omvs_procusermax
racf_omvs_program
racf_omvs_threadsmax
racf_omvs_uid
racf_oper_altgrp
racf_oper_auth
racf_oper_auto
racf_oper_cmdsys
```

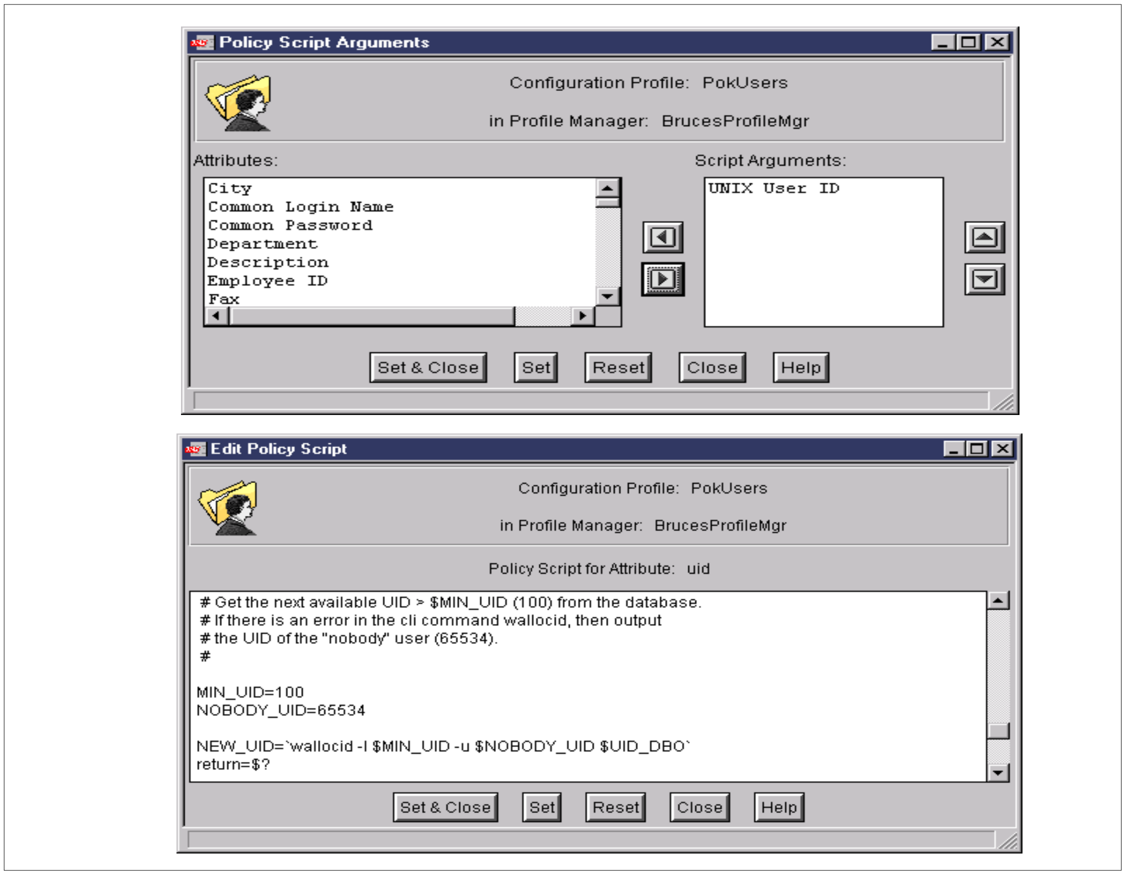
Default Policy

Subscribers can edit ○ No ● Yes

Default Type: Script

Script loade

- This is the default policy view. It’s pretty much the same as the validation policy view.
- Select the property on the left, and then view/set its policy attributes on the right
- When a new user is created, Tivoli will search for and execute default policy for every user attribute. This can take a while, so it behooves you to scope the number of properties associated with a user record where possible.
- When you select script for type of policy, you can create the script right here using these dialogs
- You select the arguments of the script, and can then edit the script (next slide)
- Works the same for all apps (including TSM)



Configuration Profile: PokUsers

in Profile Manager: BrucesProfileMgr

Attributes:

City
Common Login Name
Common Password
Department
Description
Employee ID
Fax

Script Arguments:

UNIX User ID

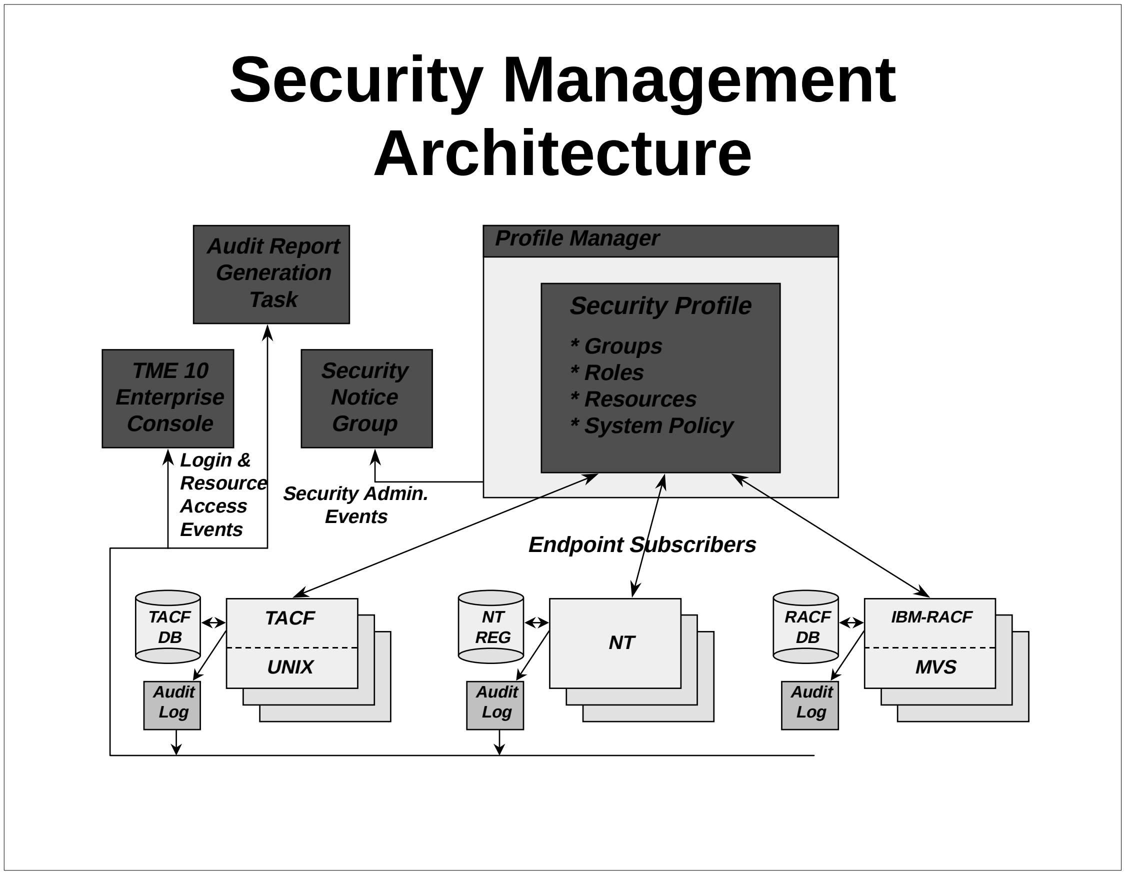
Configuration Profile: PokUsers

in Profile Manager: BrucesProfileMgr

Policy Script for Attribute: uid

```
 # Get the next available UID > $MIN_UID (100) from the database.
 # If there is an error in the cli command wallocid, then output
 # the UID of the "nobody" user (65534).
 #

MIN_UID=100
NOBODY_UID=65534

NEW_UID=`wallocid -l $MIN_UID -u $NOBODY_UID $UID_DBO`
return=$?
```

- The top dialog allows you to choose the script arguments from the set of user profile attributes. For example, for the RACF OMVS UID, you could pass in the base unix UID, and have your script echo that as its output
- The bottom dialog allows you to edit the script body. This example (partially shown) takes the user name as input, and using a side file, assigns the next unused UID value for this user
- Default policy is applied when you save the record, or when you click the "generate defaults" button
- Validation policy is applied when you save the record, or when you populate new records (can be used to enforce policy as you migrate endpoint data into Tivoli)



Security Management Architecture

Audit Report Generation Task

Profile Manager

Security Profile

* Groups
* Roles
* Resources
* System Policy

TME 10 Enterprise Console

Security Notice Group

Login & Resource Access Events

Security Admin. Events

Endpoint Subscribers

TACF DB

TACF

UNIX

Audit Log

NT REG

NT

Audit Log

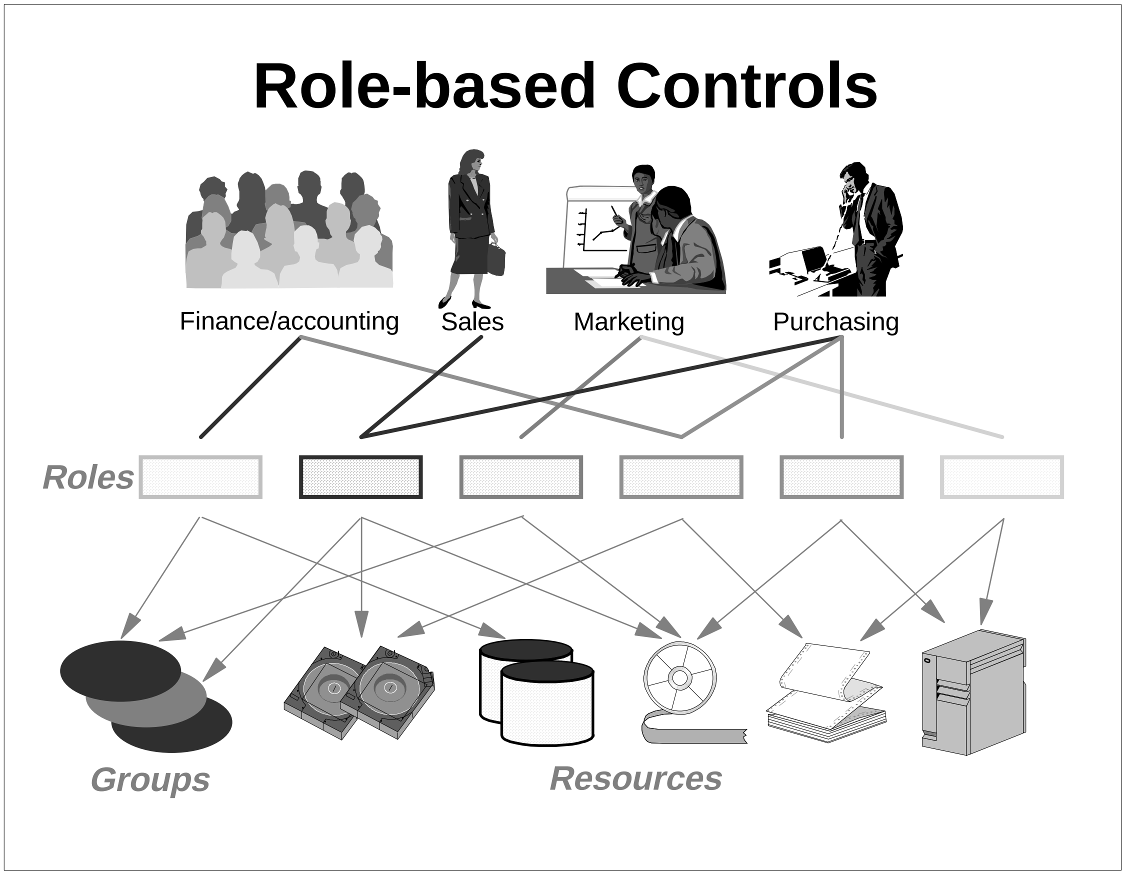
RACF DB

IBM-RACF

MVS

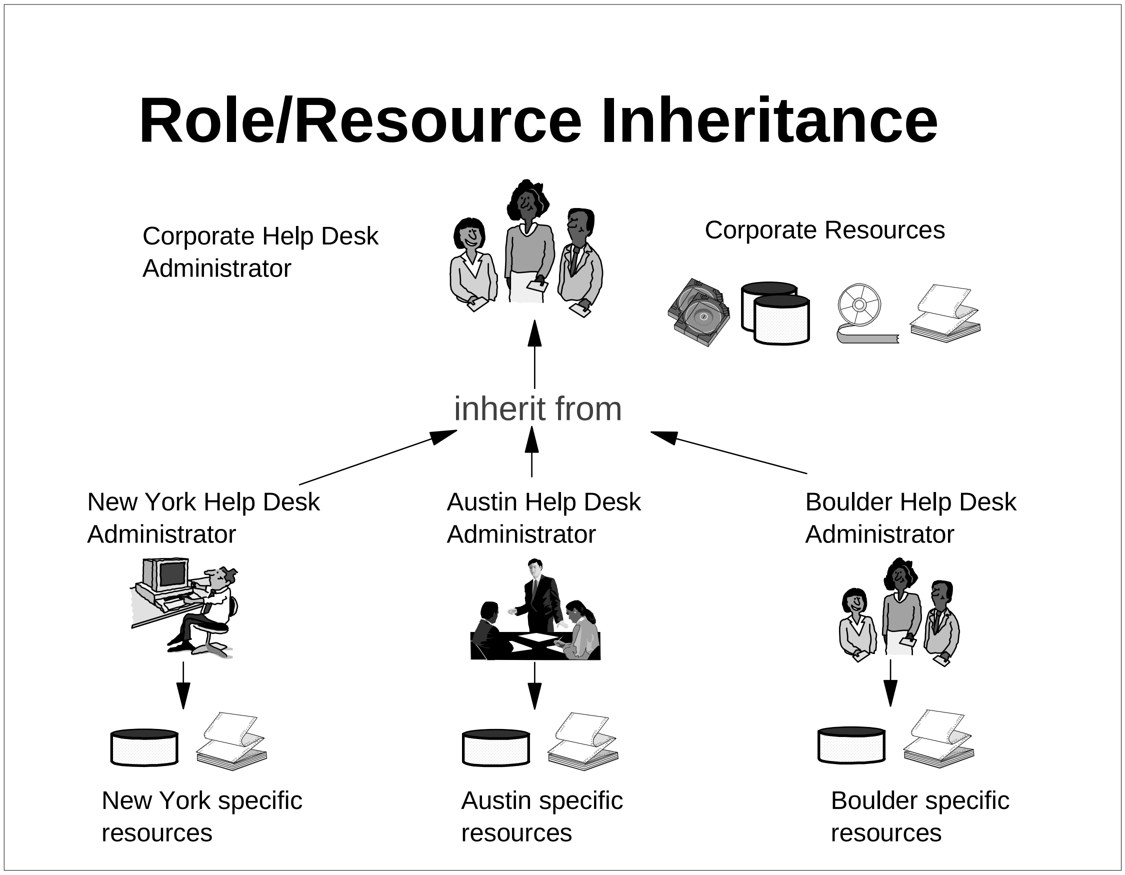
Audit Log

- Securty Management profiles contain 4 different types of record
- The RACF audit log (SMF) is not as yet integrated in with the other auditing, though certainly it could be using tivoli jobs.
- RACF events (operator messages) can be sent to Tivoli Event Console using NetView
- TSM provides a layer of security on top of native UNIX (the TACF product)



Role-based Controls

- A major feature of TSM is the ability to define role-based access control
- A role is represented as a textual description of a job function (E.G. Sales Representative).
- Within each role is a list of resources, and their permissions, which a given job function requires. The role also contains the groups which require these resources
- A role can be implemented somewhat by a racf group except
- It’s not cross-platform
- There’s no quick way to determine what resources the group has access to (need to run an offline utility)
- Inheritance (next slide) is not supported



Role/Resource Inheritance

Corporate Help Desk Administrator

Corporate Resources

inherit from

New York Help Desk Administrator

Austin Help Desk Administrator

Boulder Help Desk Administrator

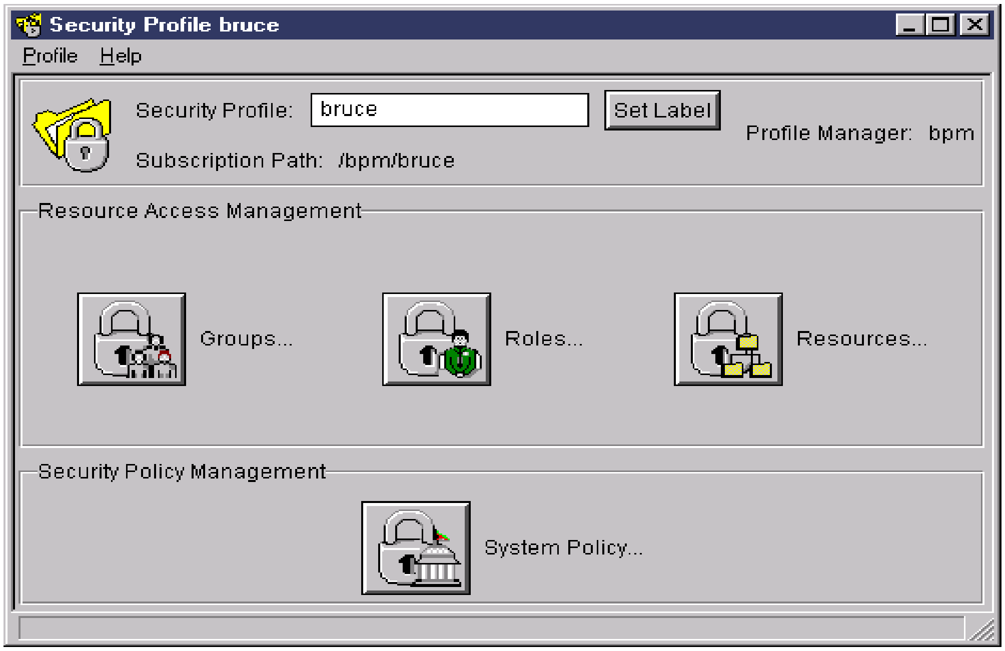
New York specific resources

Austin specific resources

Boulder specific resources

- TSM roles can designate a parent role from which resource access is inherited
- Only the differences need be specified in the child (can add resources, or override permission to parent’s resources). This saves work.
- A given role can have many children, but only one parent
- Note that RACF groups have an administrative hierarchy (group tree), but not an authorization hierarchy

Security Profile Front End



Security Profile bruce

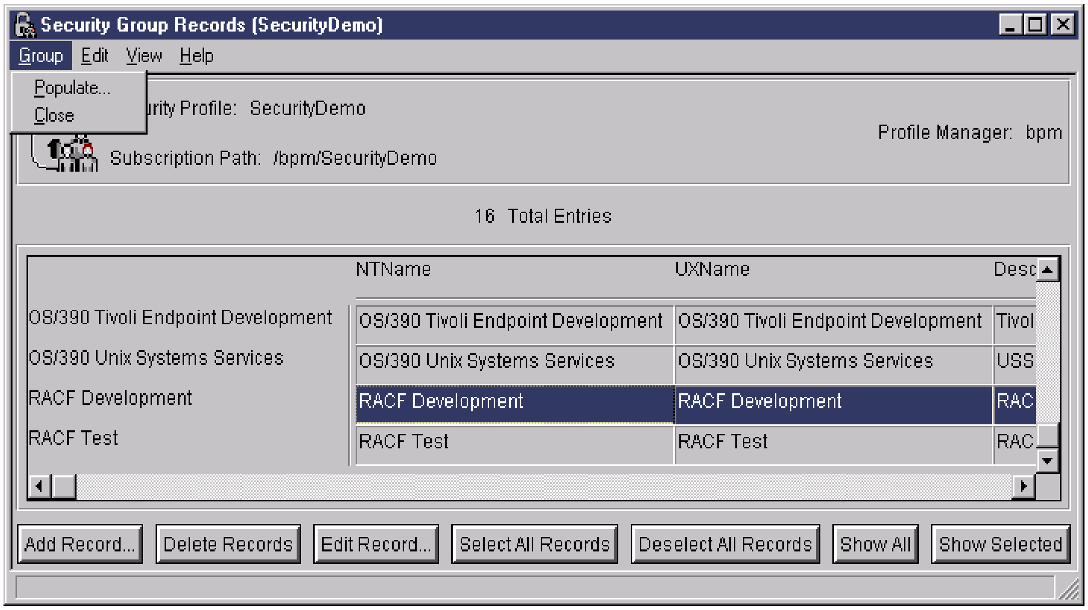
Security Profile: bruce

Subscription Path: /bpm/bruce

Profile Manager: bpm

- Double-clicking a security profile from the profile manager view results in this dialog
- Note that this differs from TUA, which showed a table view.
- Because TSM profiles contain 4 different record types, this "front-end" is required in order for TSM to display the correct dialogs for each record type.
- Populates and distributes can be done from this panel
- Profile validation can also be done
- The next dialog will be a table view similar to TUA
- Let’s click on Groups

Group Record Table View



urity Profile: SecurityDemo

Profile Manager: bpm

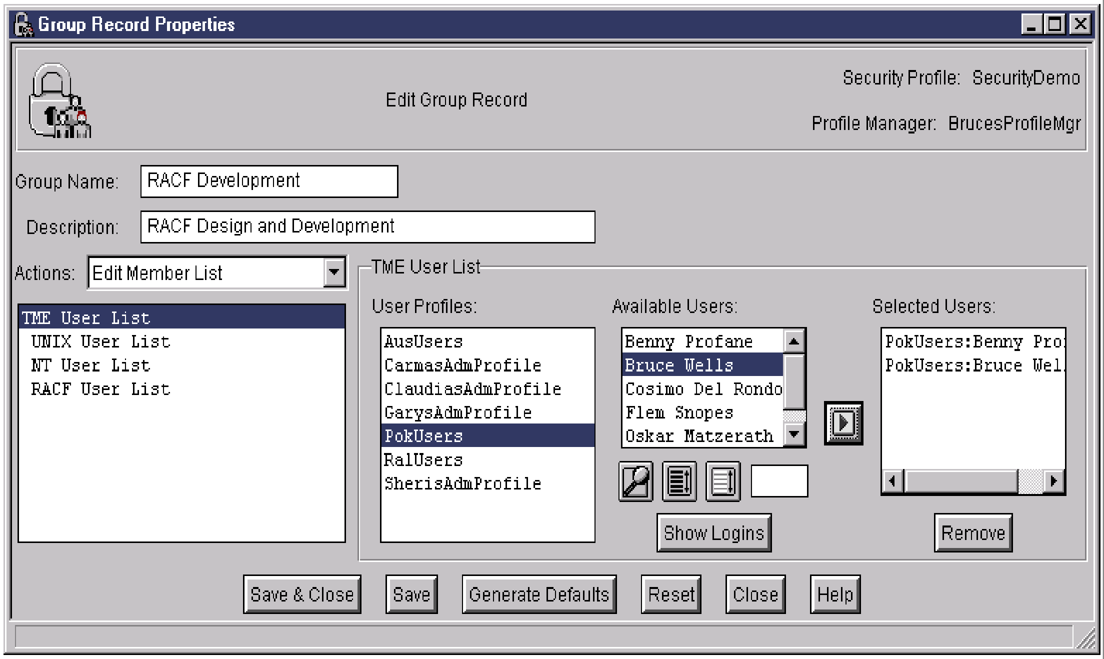
Subscription Path: /bpm/SecurityDemo

16 Total Entries

	NTName	UXName	Desc
OS/390 Tivoli Endpoint Development	OS/390 Tivoli Endpoint Development	OS/390 Tivoli Endpoint Development	Tivol
OS/390 Unix Systems Services	OS/390 Unix Systems Services	OS/390 Unix Systems Services	USS
RACF Development	RACF Development	RACF Development	RAC
RACF Test	RACF Test	RACF Test	RAC

- Like we saw for user admin, this shows a table view of the group records defined within this security profile.
- There are a set of pulldowns similar to what we see in all tivoli dialogs
- In TSM, you populate specific to the record type, though distribution is done at the profile level.
- Let’s double-click a group record and take a look inside

Editing Group Member List



Group Record Properties

Edit Group Record

Security Profile: SecurityDemo

Profile Manager: BrucesProfileMgr

Group Name: RACF Development

Description: RACF Design and Development

Actions: Edit Member List

TME User List

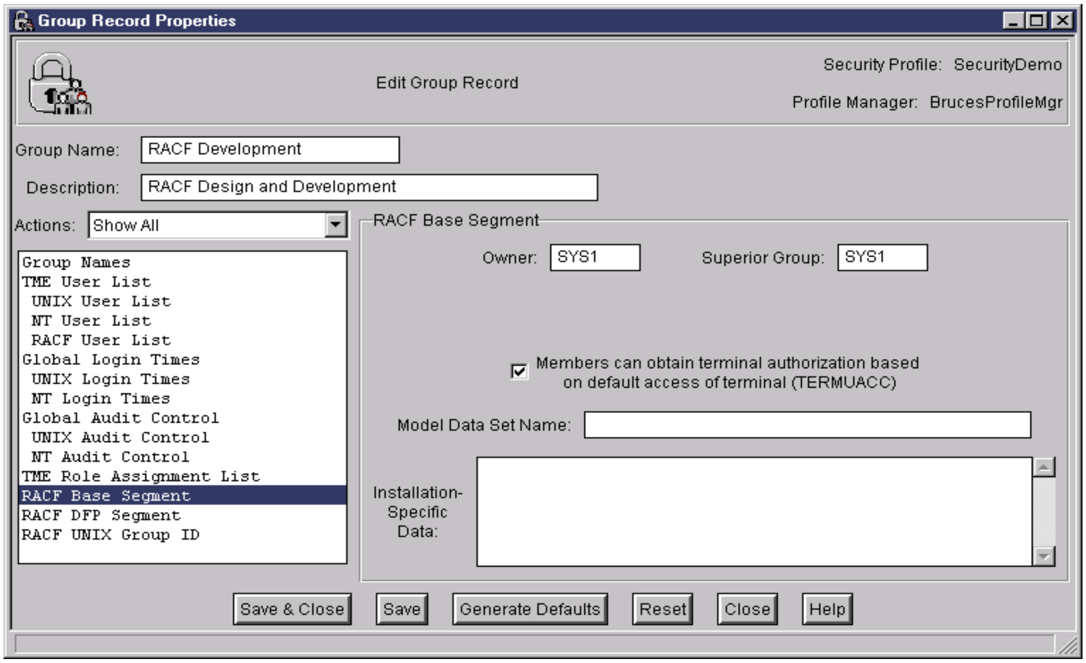
User Profiles:
- AusUsers
- CarmasAdmProfile
- ClaudiasAdmProfile
- GarysAdmProfile
- PokUsers
- RalUsers
- SherisAdmProfile

Available Users:
- Benny Profane
- Bruce Wells
- Cosimo Del Rondo
- Flem Snopes
- Oskar Matzerath

Selected Users:
- PokUsers:Benny Pro
- PokUsers:Bruce Wel

- You would really see the group names dialog first, but I clicked "Show All", and then displayed the TME user list
- This shows the TUA-defined users which are members of this group. Tivoli maintains the referential integrity between TUA and TSM profiles
- You can also define endpoint-specific users...those that aren’t defined within TUA
- When a group is distributed to RACF, the RACF user list will be fuly replaced by the user list known to TSM
- RACF connection attributes will not be modified, since they are not as yet supported in TSM, so you don’t need to worry about existing group authority being modified

Editing RACF Base Segment



Group Record Properties

Edit Group Record

Security Profile: SecurityDemo

Profile Manager: BrucesProfileMgr

Group Name: RACF Development

Description: RACF Design and Development

Actions: Show All

RACF Base Segment

Owner: SYS1

Superior Group: SYS1

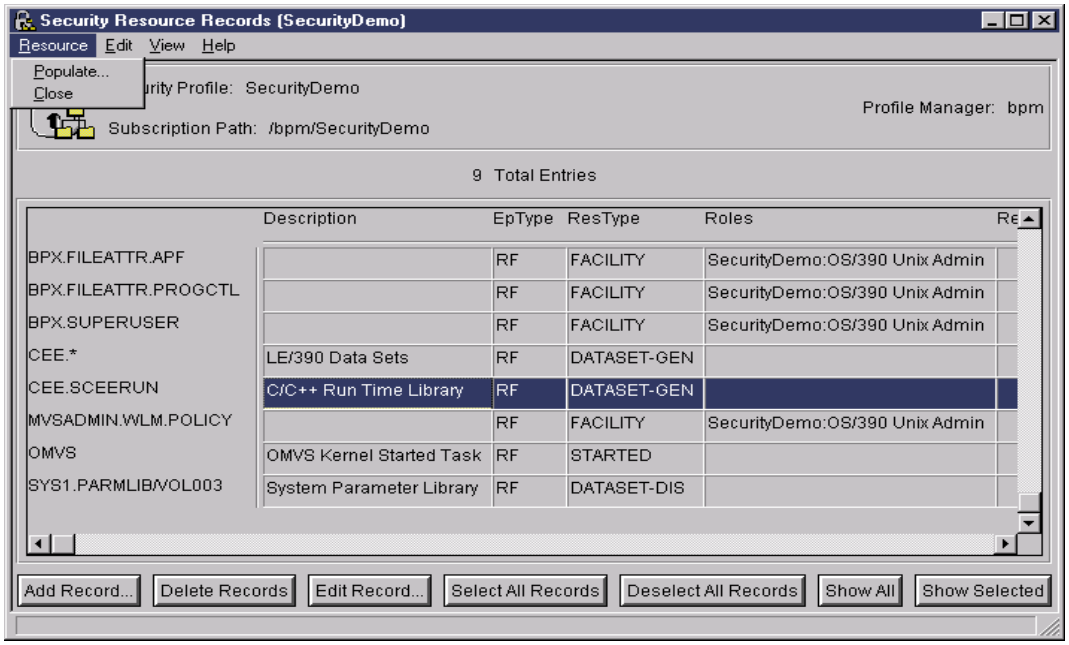
☑ Members can obtain terminal authorization based on default access of terminal (TERMUACC)

Model Data Set Name:

Installation-Specific Data:

- Note the RACF-specific dialogs defined for the group record
- This is the base segment dialog

Resource Record Table View



urity Profile: SecurityDemo

Subscription Path: /bpm/SecurityDemo

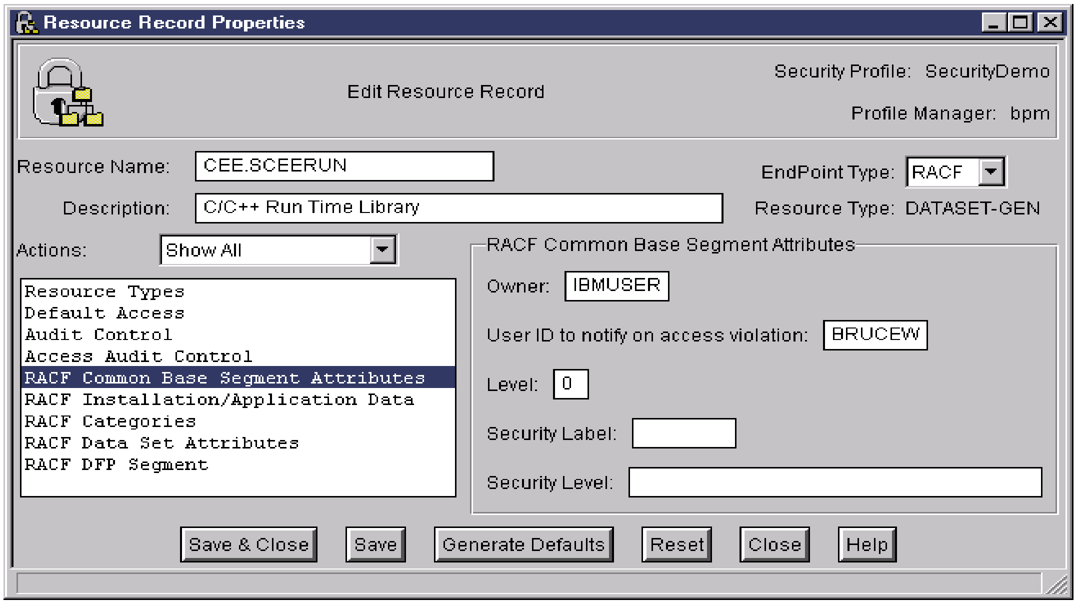
Profile Manager: bpm

9 Total Entries

	Description	EpType	ResType	Roles	Re
BPX.FILEATTR.APF		RF	FACILITY	SecurityDemo:OS/390 Unix Admin	
BPX.FILEATTR.PROGCTL		RF	FACILITY	SecurityDemo:OS/390 Unix Admin	
BPX.SUPERUSER		RF	FACILITY	SecurityDemo:OS/390 Unix Admin	
CEE.*	LE/390 Data Sets	RF	DATASET-GEN		
CEE.SCEERUN	C/C++ Run Time Library	RF	DATASET-GEN		
MVSADMIN.WLM.POLICY		RF	FACILITY	SecurityDemo:OS/390 Unix Admin	
OMVS	OMVS Kernel Started Task	RF	STARTED		
SYS1.PARMLIB/VOL003	System Parameter Library	RF	DATASET-DIS		

- Here is the resource table view
- In TSM, resources are endpoint-specific. There is no attempt to abstract them at a cross-platform level
- RACF profile names are capitalized automatically.
- Data sets are broken into two different categories for generic and discrete (this is not true for general resources)
- Discrete data sets can be qualified by volume
- Double-click to look inside...

Editing RACF Base Segment



Resource Record Properties

Edit Resource Record

Security Profile: SecurityDemo

Profile Manager: bpm

Resource Name: CEE.SCEERUN

EndPoint Type: RACF

Description: C/C++ Run Time Library

Resource Type: DATASET-GEN

Actions: Show All

```
Resource Types
Default Access
Audit Control
Access Audit Control
RACF Common Base Segment Attributes
RACF Installation/Application Data
RACF Categories
RACF Data Set Attributes
RACF DFP Segment
```

RACF Common Base Segment Attributes

Owner: IBMUSER

User ID to notify on access violation: BRUCEW

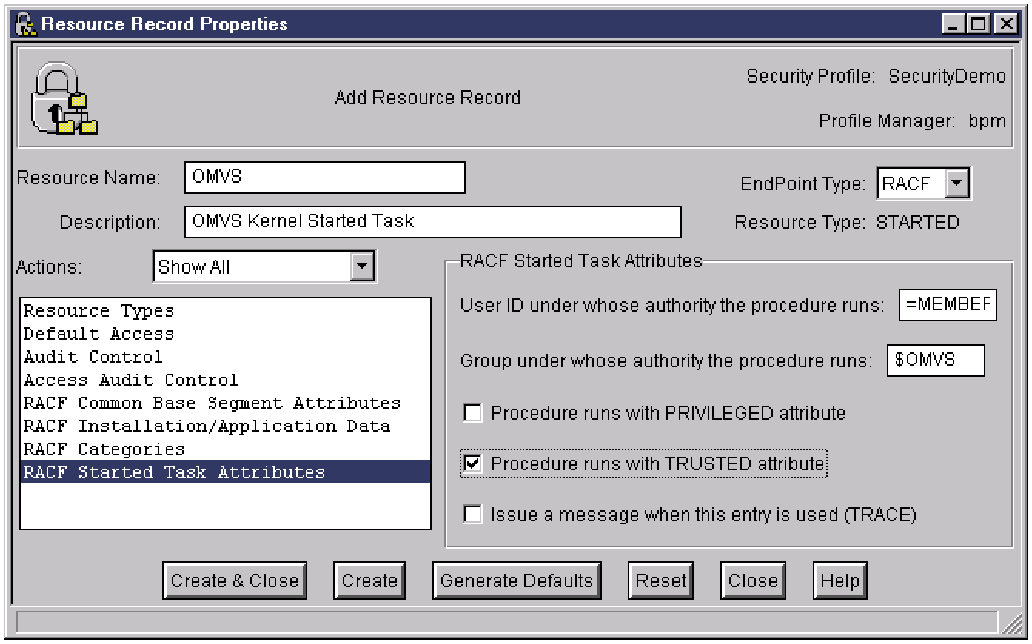
Level: 0

Security Label:

Security Level:

- Selecting the endpoint type will result in a list of applicable resource types (RACF class names) in the Resource Types dialog (not shown)
- Customer-defined RACF classes can be added with a command
- Note the RACF-specific dialogs
- Only those actions which apply to the resource type are displayed

Editing Started Task Properties



Resource Record Properties

Add Resource Record

Security Profile: SecurityDemo

Profile Manager: bpm

Resource Name: OMVS

EndPoint Type: RACF

Description: OMVS Kernel Started Task

Resource Type: STARTED

Actions: Show All

```
Resource Types
Default Access
Audit Control
Access Audit Control
RACF Common Base Segment Attributes
RACF Installation/Application Data
RACF Categories
RACF Started Task Attributes
```

RACF Started Task Attributes

User ID under whose authority the procedure runs: =MEMBEF

Group under whose authority the procedure runs: $OMVS

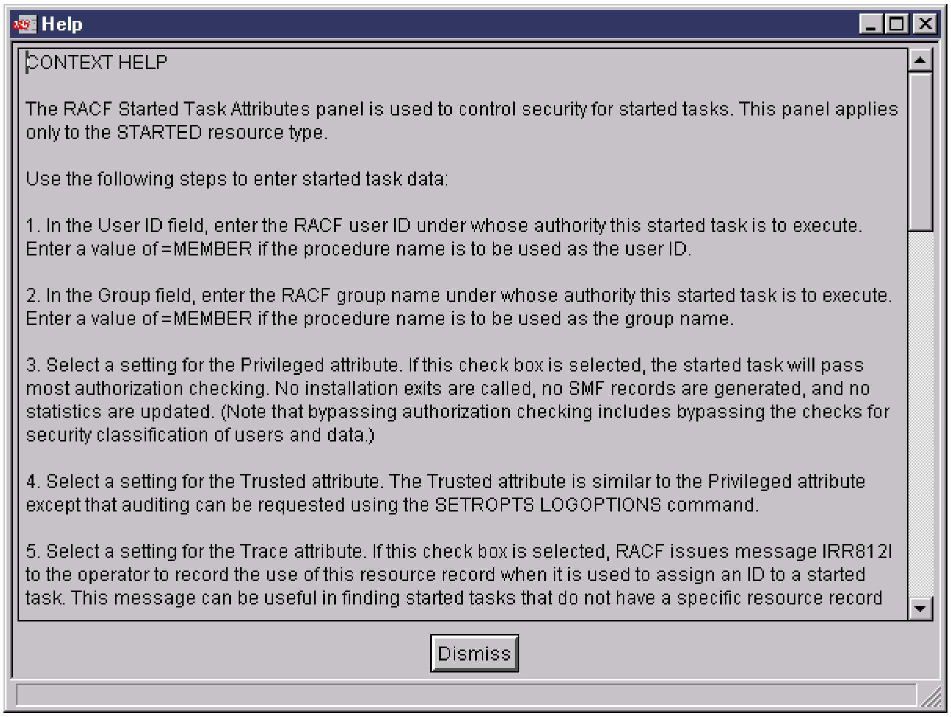
□ Procedure runs with PRIVILEGED attribute

☑ Procedure runs with TRUSTED attribute

□ Issue a message when this entry is used (TRACE)

- Note that for type STARTED, I no longer see the data set attributes selection.
- Specific dialogs (not shown) also exist for APPCLU (session segment), G/TERMINAL (access times and time zone), DLFCLASS (DLFDATA segment), and for grouping classes, the member list
- Online help text exists for each of the RACF dialogs.
- Click on "Help" for help text (next slide)

Displaying Context Help



CONTEXT HELP

The RACF Started Task Attributes panel is used to control security for started tasks. This panel applies only to the STARTED resource type.

Use the following steps to enter started task data:

1. In the User ID field, enter the RACF user ID under whose authority this started task is to execute. Enter a value of =MEMBER if the procedure name is to be used as the user ID.

2. In the Group field, enter the RACF group name under whose authority this started task is to execute. Enter a value of =MEMBER if the procedure name is to be used as the group name.

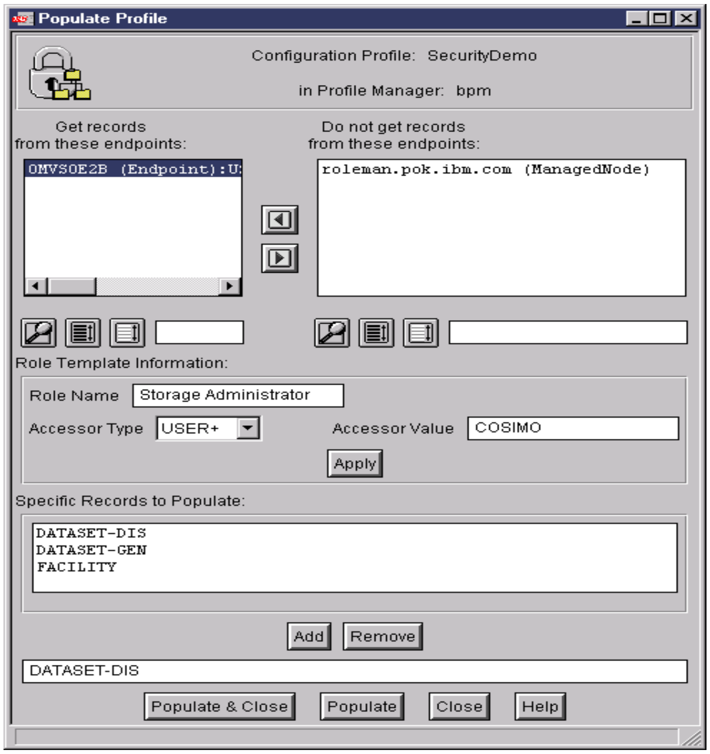
3. Select a setting for the Privileged attribute. If this check box is selected, the started task will pass most authorization checking. No installation exits are called, no SMF records are generated, and no statistics are updated. (Note that bypassing authorization checking includes bypassing the checks for security classification of users and data.)

4. Select a setting for the Trusted attribute. The Trusted attribute is similar to the Privileged attribute except that auditing can be requested using the SETROPTS LOGOPTIONS command.

5. Select a setting for the Trace attribute. If this check box is selected, RACF issues message IRR812I to the operator to record the use of this resource record when it is used to assign an ID to a started task. This message can be useful in finding started tasks that do not have a specific resource record

- For all the RACF-specific dialogs, you can click on the Help button for detailed help text
- Contains basic info similar to the Command Language Reference

Populating Resources



Configuration Profile: SecurityDemo

in Profile Manager: bpm

Get records from these endpoints:

OMVS0E2B (Endpoint):U:

Do not get records from these endpoints:

roleman.pok.ibm.com (ManagedNode)

Role Template Information:

Role Name: Storage Administrator

Accessor Type: USER+

Accessor Value: COSIMO

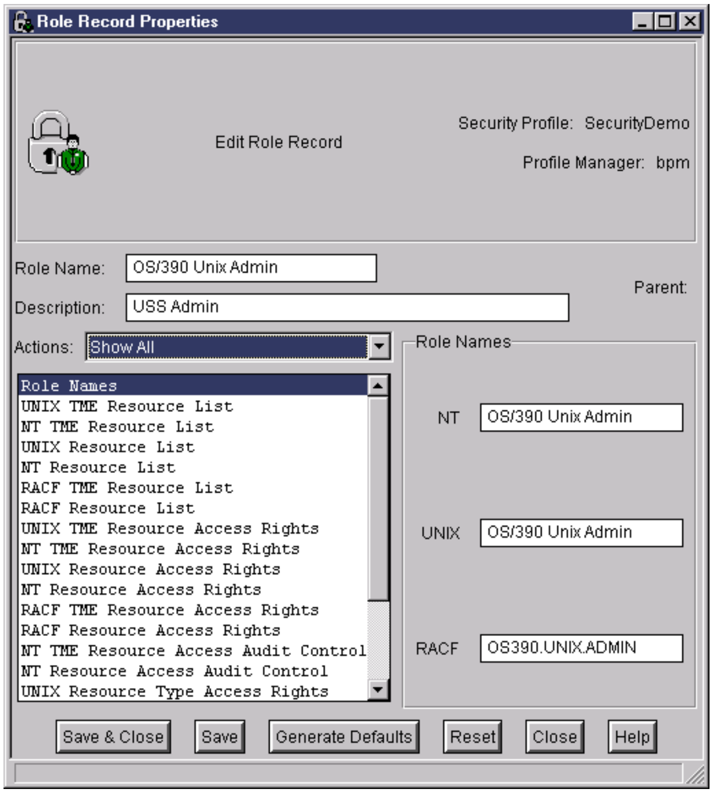
Specific Records to Populate:

DATASET-DIS
DATASET-GEN
FACILITY

DATASET-DIS

- This is the populate screen.
- I show it in the context of resources because of the extra role-template feature you get (insensitive for other record types)
- Allows you to populate resources which a given user or group has access to, and populate their access levels into a role template.
- For example, Cosimo is a storage administrator. Define a role caled "Storage Administrator" and seed it with all resources which Cosimo has access to.
- For efficiency, resource types can be specified in order to limit the processing at the endpoint.
- For all record types, populate should be followed by distribute, in case data was added/altered by policy

Main Role Panel



Security Profile: SecurityDemo

Profile Manager: bpm

Role Name: OS/390 Unix Admin

Description: USS Admin

Parent:

Actions: Show All

Role Names
UNIX TME Resource List
NT TME Resource List
UNIX Resource List
NT Resource List
RACF TME Resource List
RACF Resource List
UNIX TME Resource Access Rights
NT TME Resource Access Rights
UNIX Resource Access Rights
NT Resource Access Rights
RACF TME Resource Access Rights
RACF Resource Access Rights
NT TME Resource Access Audit Control
NT Resource Access Audit Control
UNIX Resource Type Access Rights

Role Names

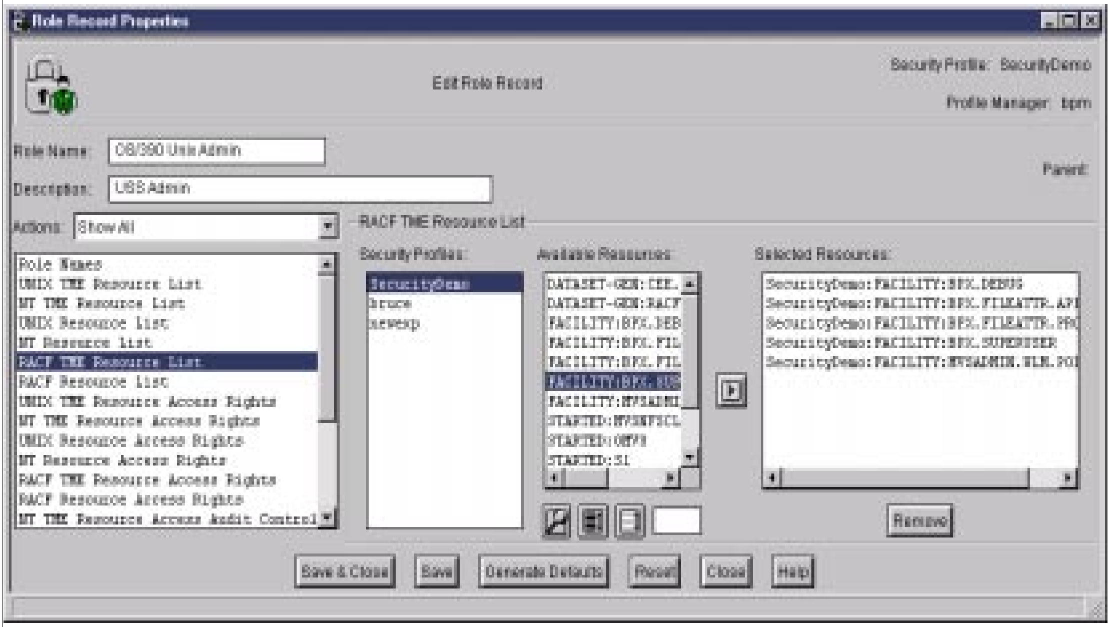
NT: OS/390 Unix Admin

UNIX: OS/390 Unix Admin

RACF: OS390.UNIX.ADMIN

- Here, we have double clicked on role record from the role table view. This is in fact the first panel you see.
- The RACF specific role name will be generated by default if not specified (same for groups)
- You can see the various subactions on the left which are used to define the resource names, their accesses, the groups, and the parent role

Adding Resources to a Role



Security Profile: SecurityDemo

Profile Manager: bpm

Role Name: OS/390 Unix Admin

Description: USS Admin

Parent:

Actions: Show All

Role Names
UNIX TME Resource List
NT TME Resource List
UNIX Resource List
NT Resource List
RACF TME Resource List
RACF Resource List
UNIX TME Resource Access Rights
NT TME Resource Access Rights
UNIX Resource Access Rights
NT Resource Access Rights
RACF TME Resource Access Rights
RACF Resource Access Rights
NT TME Resource Access Audit Control

RACF TME Resource List

Security Profiles:

SecurityDemo
bruce
newexp

Available Resources:

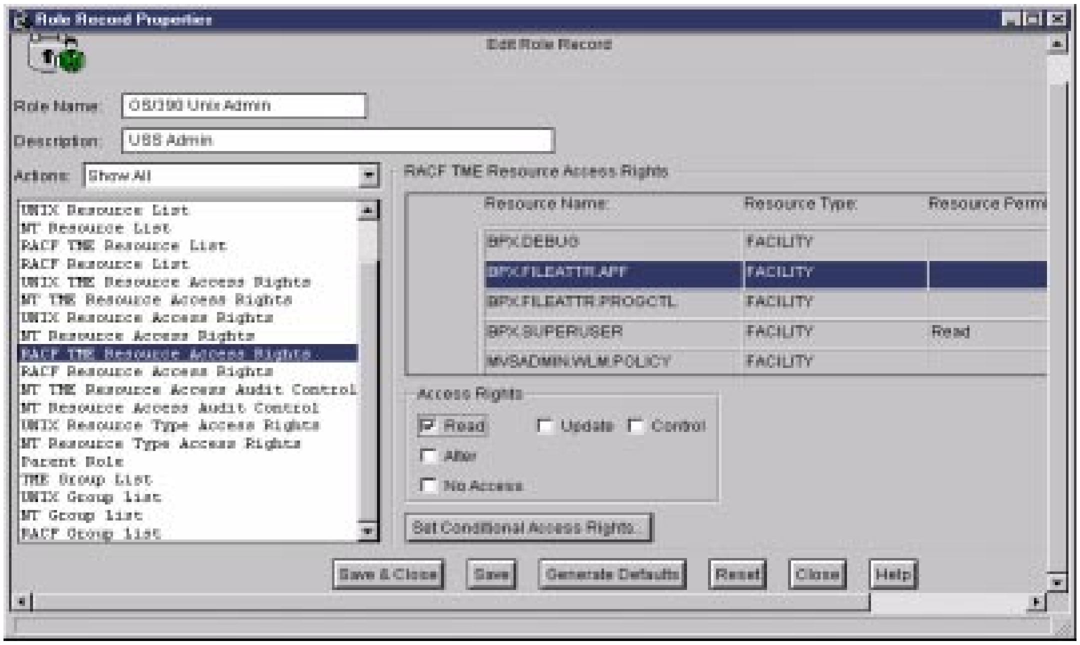
DATASET-GEN:CEE.
DATASET-GEN:RACF
FACILITY:BPX.DEB
FACILITY:BPX.FIL
FACILITY:BPX.FIL
FACILITY:BPX.SUS
FACILITY:MVSADMI
STARTED:MVSNFSCL
STARTED:OMVS
STARTED:SI

Selected Resources:

SecurityDemo:FACILITY:BPX.DEBUG
SecurityDemo:FACILITY:BPX.FILEATTR.API
SecurityDemo:FACILITY:BPX.FILEATTR.PRO
SecurityDemo:FACILITY:BPX.SUPERUSER
SecurityDemo:FACILITY:MVSADMIN.WLM.POL

- Similar to user membership in group records, resources can be added to roles by either selecting from existing TSM profiles, or keying in text for an endpoint resource which is not being managed by TSM.

Defining Resource Access



Role Name: OS/390 Unix Admin

Description: USS Admin

Actions: Show All

UNIX Resource List
NT Resource List
RACF TME Resource List
RACF Resource List
UNIX TME Resource Access Rights
NT TME Resource Access Rights
UNIX Resource Access Rights
NT Resource Access Rights
RACF TME Resource Access Rights
RACF Resource Access Rights
NT TME Resource Access Audit Control
NT Resource Access Audit Control
UNIX Resource Type Access Rights
NT Resource Type Access Rights
Parent Role
TME Group List
UNIX Group list
NT Group list
RACF Group list

RACF TME Resource Access Rights

Resource Name:	Resource Type:	Resource Perm
BPX.DEBUG	FACILITY	
BPX.FILEATTR.APF	FACILITY	
BPX.FILEATTR.PROGCTL	FACILITY	
BPX.SUPERUSER	FACILITY	Read
MVSADMIN.WLM.POLICY	FACILITY	

Access Rights

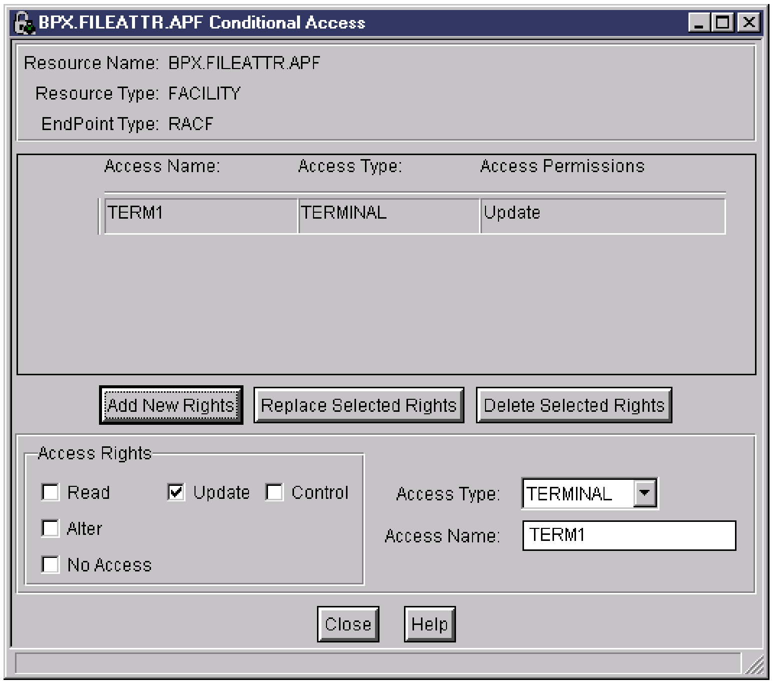
☑ Read ☐ Update ☐ Control

☐ Alter

☐ No Access

- Separate dialogs are used to define resource access
- The "Access Rights" box is set dynamically based on the resources type. E.G., if this were a PROGRAM resource, you would also see execute access. Also, mutual exclusivity is enforced with RACF access levels...this is not true on other endpoint types
- Click "Set Conditional Access Rights" to set conditional access (next slide)

Defining Conditional Access



BPX.FILEATTR.APF Conditional Access

Resource Name: BPX.FILEATTR.APF
Resource Type: FACILITY
EndPoint Type: RACF

Access Name:	Access Type:	Access Permissions
TERM1	TERMINAL	Update

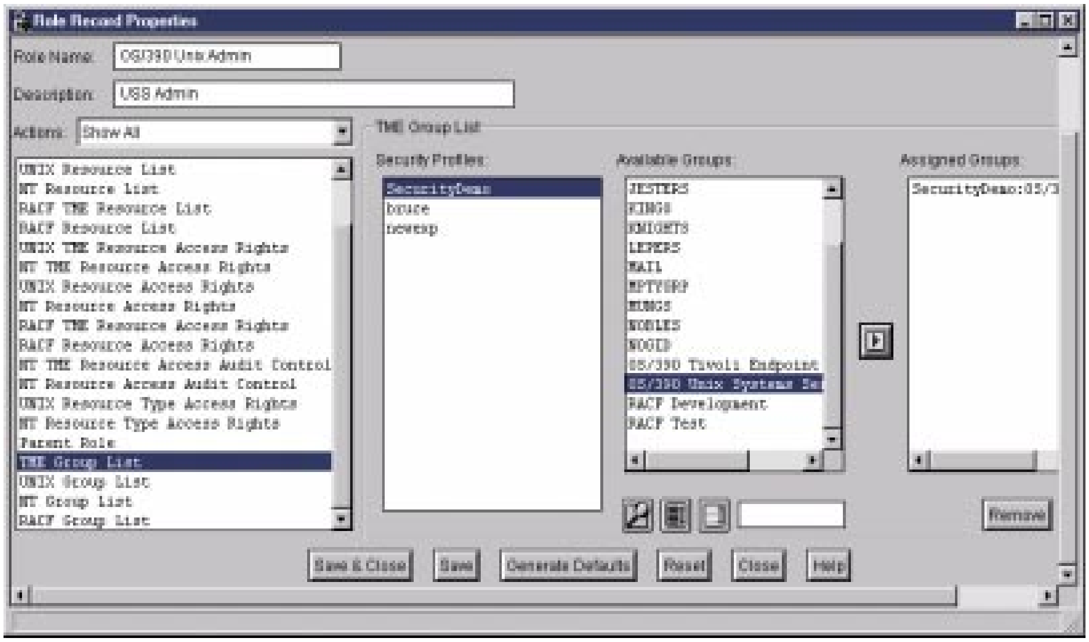
Access Rights

☐ Read ☑ Update ☐ Control
☐ Alter
☐ No Access

Access Type: TERMINAL
Access Name: TERM1

- The "Access Type" choices will vary depending on the resource type

Adding Groups to a Role



Role Name: OS/390 Unix Admin

Description: USS Admin

Actions: Show All

UNIX Resource List
NT Resource List
RACF TME Resource List
RACF Resource List
UNIX TME Resource Access Rights
NT TME Resource Access Rights
UNIX Resource Access Rights
NT Resource Access Rights
RACF TME Resource Access Rights
RACF Resource Access Rights
NT TME Resource Access Audit Control
NT Resource Access Audit Control
UNIX Resource Type Access Rights
NT Resource Type Access Rights
Parent Role
TME Group List
UNIX Group List
NT Group List
RACF Group List

TME Group List

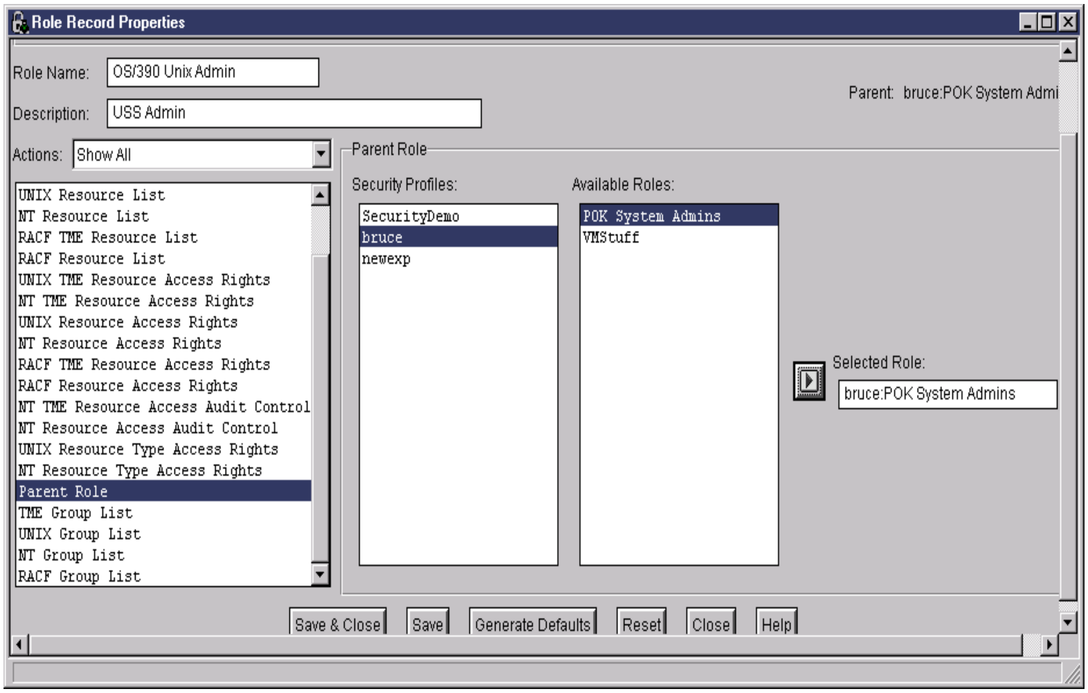
Security Profiles:
SecurityDemo
bruce
newexp

Available Groups:
JESTERS
KINGS
KNIGHTS
LEPERS
MAIL
MPTYGRP
MUNGS
NOBLES
NOGID
OS/390 Tivoli Endpoint
OS/390 Unix Systems Se
RACF Development
RACF Test

Assigned Groups:
SecurityDemo:OS/3

- Again, groups can be selected from existing TSM profiles, or keyed in for an endpoint-specific group name
- When the role is distributed, each endpoint receiving the data will permit the defined goups to the defined resources with the defined permissions using endpoint-specific interfaces and semantics.
- On RACF, Tivoli role information is contained in the TME segment of ROLE, GROUP, and resource (data set and general resource) profiles. It should not be modified directly on RACF...let TSM manage it
- The endpoints will manage inheritance and role intersections such that each group obtains the privilege required for all of its roles.

Defining Role Inheritance



Role Name: OS/390 Unix Admin

Description: USS Admin

Parent: bruce:POK System Admi

Actions: Show All

UNIX Resource List
NT Resource List
RACF TME Resource List
RACF Resource List
UNIX TME Resource Access Rights
NT TME Resource Access Rights
UNIX Resource Access Rights
NT Resource Access Rights
RACF TME Resource Access Rights
RACF Resource Access Rights
NT TME Resource Access Audit Control
NT Resource Access Audit Control
UNIX Resource Type Access Rights
NT Resource Type Access Rights
Parent Role
TME Group List
UNIX Group List
NT Group List
RACF Group List

Parent Role

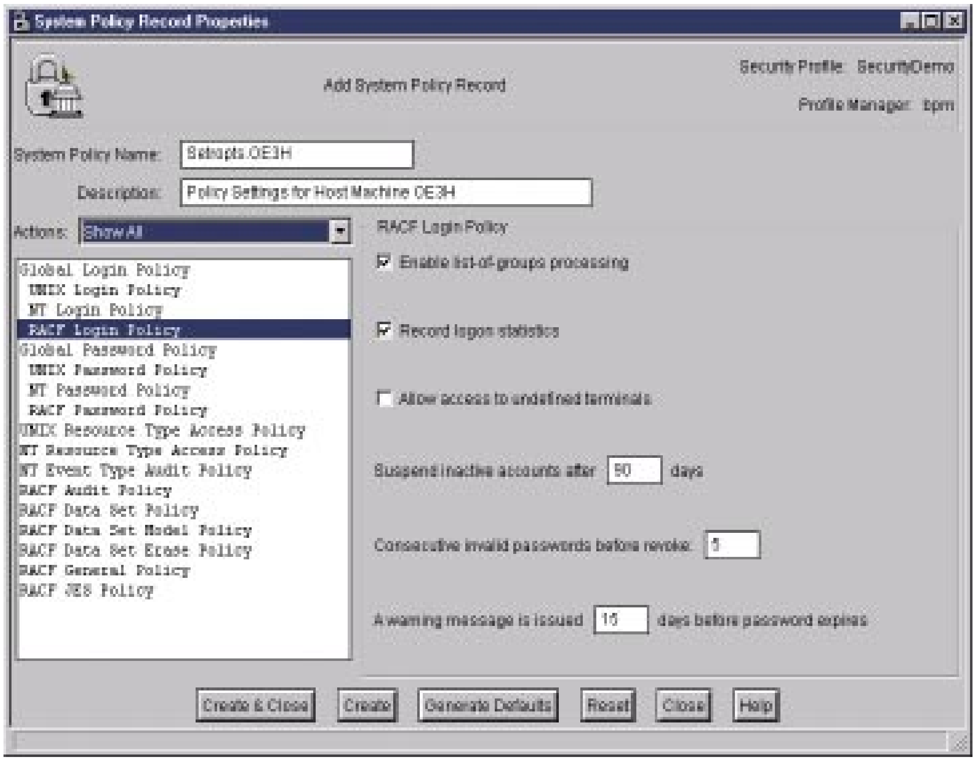
Security Profiles:
SecurityDemo
bruce
newexp

Available Roles:
POK System Admins
VMStuff

Selected Role: bruce:POK System Admins

- The parent role is optional, and can be selected from existing TSM profiles

Defining RACF Login Policy



System Policy Record Properties

Add System Policy Record

Security Profile: SecurityDemo

Profile Manager: bpm

System Policy Name: Setropts.OE3H

Description: Policy Settings for Host Machine OE3H

Actions: Show All

RACF Login Policy

☑ Enable list-of-groups processing

☑ Record logon statistics

☐ Allow access to undefined terminals

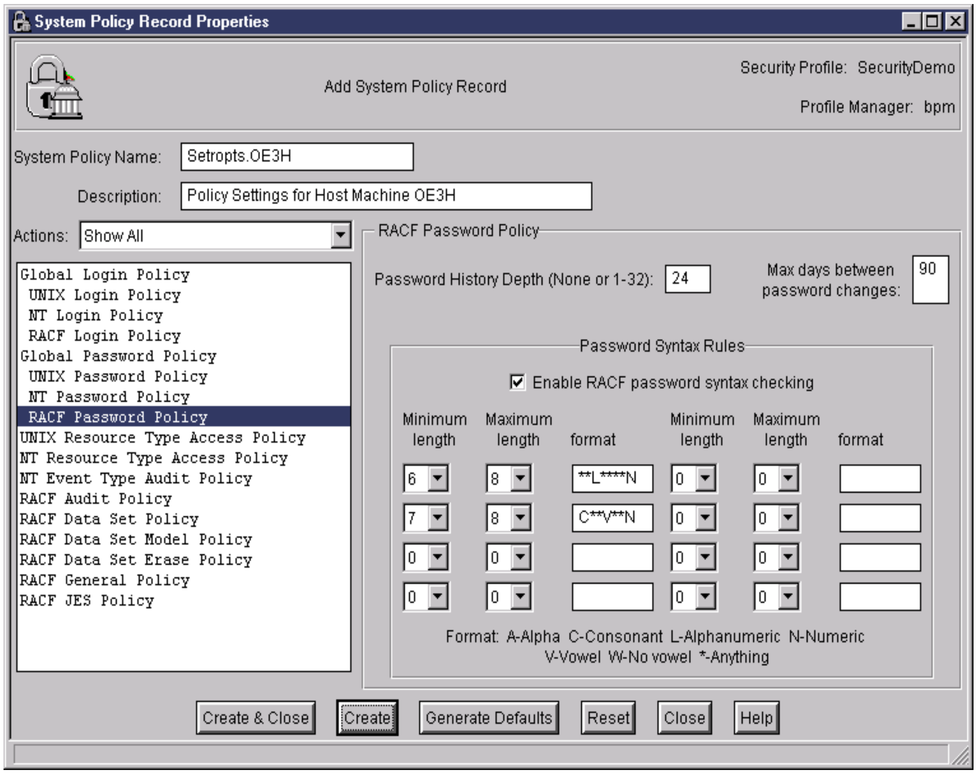
Suspend inactive accounts after 90 days

Consecutive invalid passwords before revoke: 5

A warning message is issued 15 days before password expires

- Now’ we’re in the System Policy dialogs. On RACF, system policy records control SETROPTS settings
- You **REALLY SHOULD** populate the System Policy record from RACF before altering/managing it from TSM
- If you don’t, you will have some manual steps to do...we really don’t want you shooting yourself in the foot.
- To apply the same policy to other RACF systems, add their host names to the RFEPList property using the command line interface (wmodsec)
- This property in effect implements record-level subscription for SystemPolicy records
- The dialogs group logically-related functions together

Defining RACF Password Policy



Add System Policy Record

Security Profile: SecurityDemo

Profile Manager: bpm

System Policy Name: Setropts.OE3H

Description: Policy Settings for Host Machine OE3H

Actions: Show All

```
Global Login Policy
 UNIX Login Policy
 NT Login Policy
 RACF Login Policy
Global Password Policy
 UNIX Password Policy
 NT Password Policy
 RACF Password Policy
UNIX Resource Type Access Policy
NT Resource Type Access Policy
NT Event Type Audit Policy
RACF Audit Policy
RACF Data Set Policy
RACF Data Set Model Policy
RACF Data Set Erase Policy
RACF General Policy
RACF JES Policy
```

RACF Password Policy

Password History Depth (None or 1-32): 24

Max days between password changes: 90

Password Syntax Rules

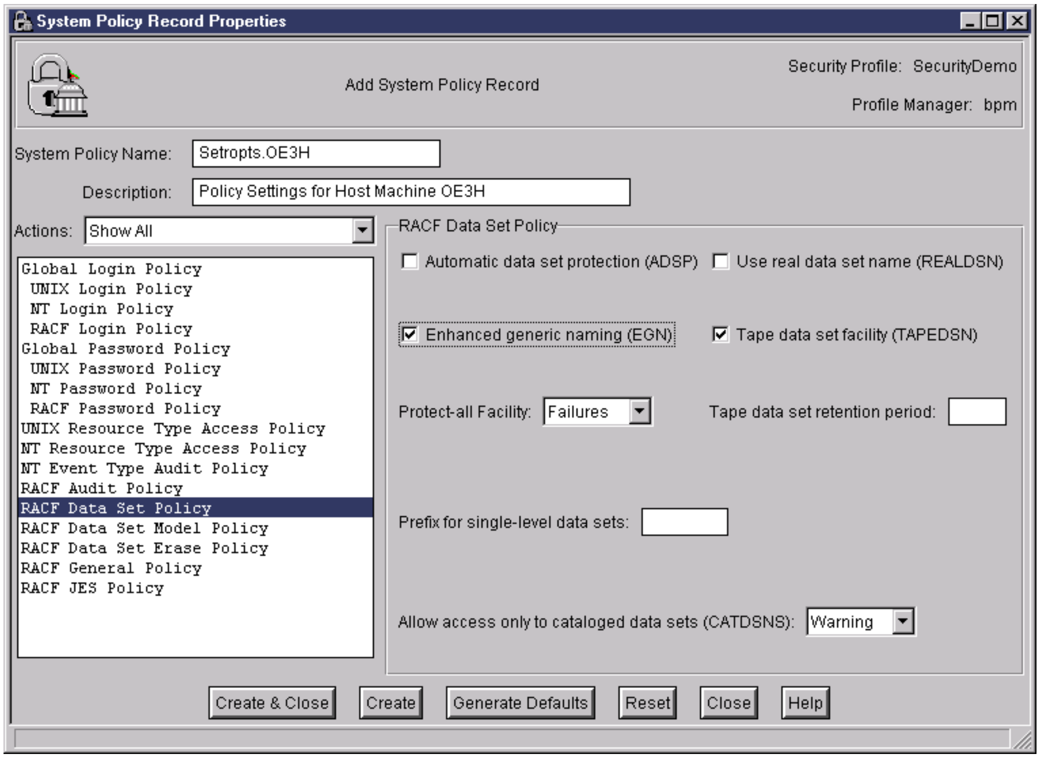
☑ Enable RACF password syntax checking

Minimum length	Maximum length	format	Minimum length	Maximum length	format
6	8	**L****N	0	0	
7	8	C**V**N	0	0	
0	0		0	0	
0	0		0	0	

Format: A-Alpha C-Consonant L-Alphanumeric N-Numeric
V-Vowel W-No vowel *-Anything

- Validation policy can be used to enforce common attributes (password change interval, invalid logon attempts etc) across all system types (default policy not shipped by default for RACF)
- Note all the RACF specific dialogs.
- Most, but not all, SETROPTS settings are supported

Defining RACF Data Set Policy



System Policy Record Properties

Add System Policy Record

Security Profile: SecurityDemo

Profile Manager: bpm

System Policy Name: Setropts.OE3H

Description: Policy Settings for Host Machine OE3H

Actions: Show All

RACF Data Set Policy

□ Automatic data set protection (ADSP) □ Use real data set name (REALDSN)

☑ Enhanced generic naming (EGN) ☑ Tape data set facility (TAPEDSN)

Protect-all Facility: Failures

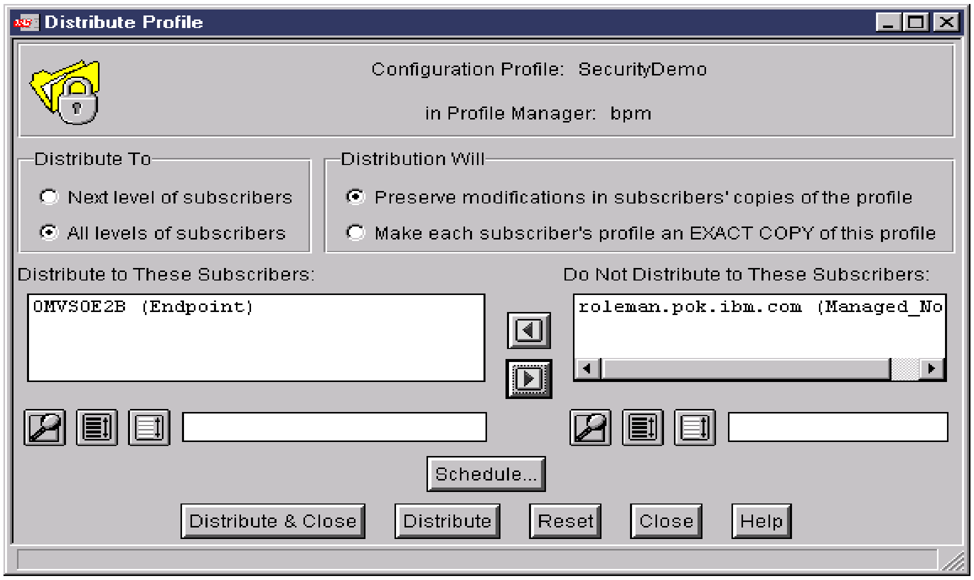
Tape data set retention period:

Prefix for single-level data sets:

Allow access only to cataloged data sets (CATDSNS): Warning

- Another example showing data set related settings

Distributing Profile Data



Distribute Profile

Configuration Profile: SecurityDemo

in Profile Manager: bpm

Distribute To

○ Next level of subscribers

● All levels of subscribers

Distribution Will

● Preserve modifications in subscribers' copies of the profile

○ Make each subscriber's profile an EXACT COPY of this profile

Distribute to These Subscribers:

```
OMVSOE2B (Endpoint)
```

Do Not Distribute to These Subscribers:

```
roleman.pok.ibm.com (Managed_No
```

- Data can be distributed to selected endpoints
- A distribution hierarchy can exist where profile managers subscribe to other profile managers
- Make exact copy is ignored on OS/390 endpoint
- The RACF endpoint will not alter RACF profile data which is not managable using TSM
- The RACF endpoint will limit its updates to only that data which has actually changed (concise SMF audit trail)
- Newer resource types, segments, and fields will not cause failures when distributed to lower level systems

To find out more

- Tivoli OS/390 and Enterprise Management Information
  - http://www.tivoli.com/products/solutions/390/
  - http://www.tivoli.com/products/solutions/security/

- 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