Sun Role Manager 4.1 User's Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part Number : 820-5757

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la legislation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la legislation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement designés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Table of Contents

Preface

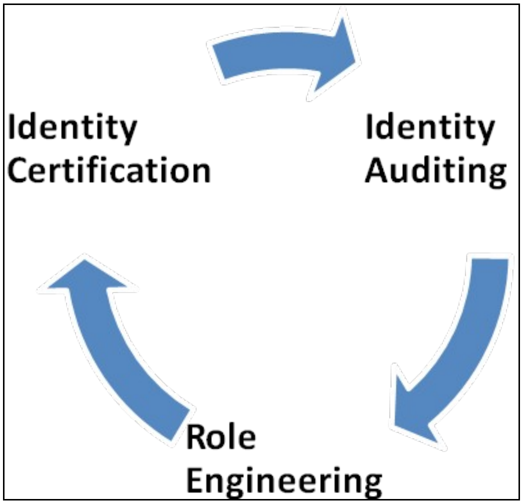
Who should read this guide

The guide is intended for business users, managers, role engineers and security administrators who serve as the end users of the Sun^{TM} Role Manager software (formerly Vaau's Sun Role Manager product). This guide will help you understand the functionality and operation from the point of the product's Role Manager and Identity Compliance Manager Solution areas. The next section serves as an overview of the product and describes what the solution provides. We suggest that you read this section first to familiarize yourself with Role Manager terms and concepts.

1

◆ ◆ ◆ CHAPTER 1

Role Manager – An Introduction



Sun Microsystems understands that organizations today need to be in complete control of their enterprise security. The Sun^{TM} Role Manager 4.1 software (formerly Vaau's RBACx) addresses all aspects of Role Based Access Control (RBAC), enabling an enterprise to quickly and effectively embrace new opportunities, improve operational efficiencies, reduce costs, and actively manage virtually all security threats and risks to the IT security of the organization. The Sun Role Manager software contains areas that are grouped as follows: Identity Warehouse, Role Engineering & Management, Identity Certification and Identity Auditing.

Identity Warehouse

The Role Manager Identity Warehouse captures and stores relevant entitlement data from systems containing simple to a complex entitlement structure. These entitlement feeds are imported on a scheduled basis and Role Manager accommodates an n-level entitlement structure which can be stored in the Role Manager data repository**.** Role Manager has an import engine which supports complex entitlement feeds from a text or xml file and also includes ETL (Extract, Transform, Load) processing capabilities. Role Manager also captures the *glossary* description of each entitlement and this can be inputted as a separate feed to Role Manager. Glossary information provides business descriptions that are associated with the raw entitlement data for improved usability and understandability. The complete entitlement data can be correlated during the certification phase and the entitlement hierarchy can be shown as part of the drill-down entitlements.

Role Engineering & Management

One of the most challenging problems in managing large networks is the complexity of security administration. Role based access control (also called role based security), has become the predominant model for advanced access control because it reduces the complexity and cost of security administration in large networked applications. Most information technology vendors have incorporated RBAC into their product line, and the technology is finding applications in areas ranging from health care to defense, in addition to the mainstream commerce systems for which it was designed.

RBAC is emerging as an alternative to traditional access control methodologies as it established a framework to facilitate management of users and information assets across an enterprise in a controlled and effective manner. The primary concept of RBAC is that access to information assets is assigned by using pre-defined and approved roles.

Role Manager provides a complete mechanism to define roles which are based on different access levels on different platforms. Roles can be defined based on the collected user entitlements or can be generated using the software's Role Mining Interface. The Role Mining component in Role Manager uses sophisticated algorithms to generate roles based on user entitlements and the cuts the role definition time to about 50 %.

Role Manager offers an enhanced workflow engine to manage the lifecycle of roles. This new workflow engine provides the ability to design various workflow processes and also allows users to call external functions from the workflow. It also provides a complete setup of security, workflow and auditing features to manage the lifecycle of rules. This functionality will help companies obtain greater efficiencies from a role-based access control model. You can define multiple rules to assign new and existing users specific role-based access. The rule management feature provides a robust rule creation engine with a vast combination of user attributes (such as job codes, department, location, etc.) and multiple conditions to assign and de-assign roles from users.

Identity Certification

Managing enterprise-wide attestation is a major challenge. Organizations must align a strategy to provide review of granular entitlements of a user's access within the organization to the user's manager(s). Today, there are various challenges involving this with a single user having access to a multitude of platforms, systems, and applications. Organizations must be able to manage increasing costs associated with gathering the user entitlements and distributing them across to the managers. They must also be able to manage increased security risks associated with the escalating volume of gathering and distributing these entitlements. Additionally, Federal requirements mandate the needs to address Time-Based Certifications, Granular Entitlements, certify Contractors on Unique Schedules, Set Baseline and Certify Incremental Changes and provide a Certification Dashboard of all the certifications issued.

To help solve these needs, Role Manager provides an Identity Certification module which enables easy handling of the collecting and distributing user entitlements and provides scheduled certifications on these entitlements. In addition, Role Manager provides unique features which allow users to certify **granular entitlements** and entitlements which are **outside of user roles**. Furthermore, business-friendly glossary names can be stored and displayed for each entitlement during certification and can be stored in Role Manager.

This powerful Identity Certification module is further extended in Role Manager to provide the ability to perform certifications at the instance or server level of a resource, providing advanced drill down capabilities for users, and advanced filtering and searching capabilities on the certification interface.

The Role Manager Identity Certification module also adds two important Certification types:

1) **User Access Certification –** Allows certifiers to certify roles and entitlements associated with a user

2) **Role Entitlement Certification -** Allows role owners to certify roles and role content

3) **Application Certification -** Allows application owners to certify entitlements pertaining to an application narrowed down by each instance of the application

Identity Auditing

Exception Monitoring is an integral piece of Identity Auditing and Management. In organizations today, there are numerous exceptions of user accounts on various target systems. A detective mechanism to monitor and acquire exceptions is needed in organizations where a centralized store for all the exceptions would be available. Organizations must be able to manage Continuous Exception Monitoring, Segregation of Duty (SoD) Violations, Detective Scanning, Inter & Intra-Application SoD Enforcement, Actual vs. Assigned Exceptions, Exception Lifecycle Management. These exceptions can be captured in Role Manager and produced in a central repository. Role

Manager provides the capability to define Audit policies and the ability to capture and report any exceptions from these policies.

Role Manager provides a Compliance Dashboard for Executives/Auditors which enable them to monitor these exceptions from a central point. Also, the various exceptions generated are stored in Role Manager and a security analyst can *accept* them or *mitigate* these risks and exceptions.

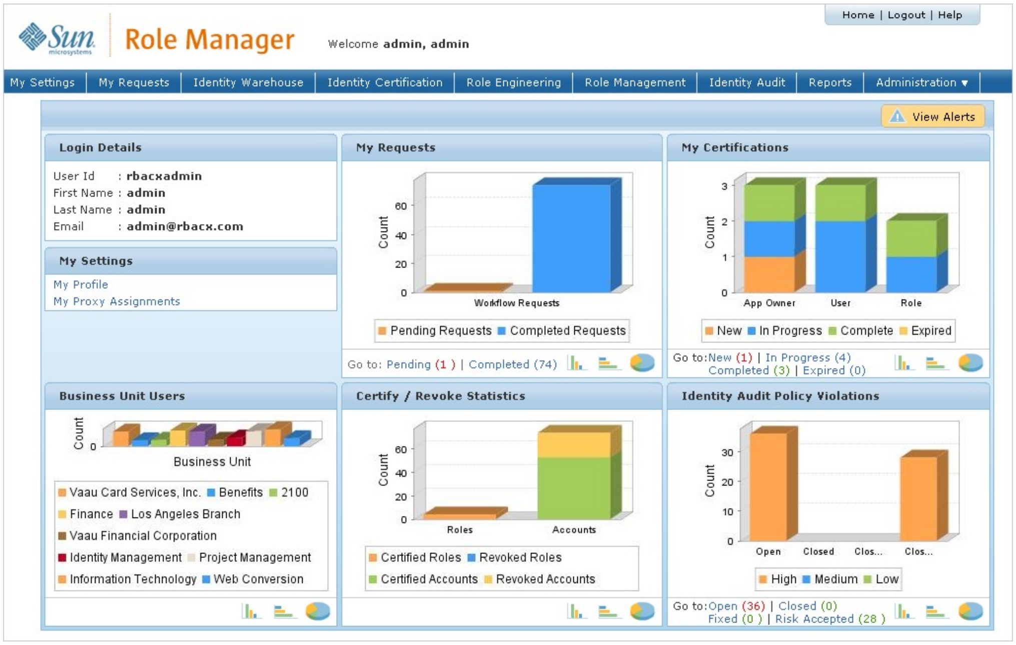
2

◆ ◆ ◆ CHAPTER 2

My Settings

Home

When a user logs into Role Manager, they are routed to the home screen. Role Manager contains a user interface that provides in-depth graphical views on whether users have any requests or Identity Certifications to approve, complete, or dismiss.



Welcome **admin, admin**

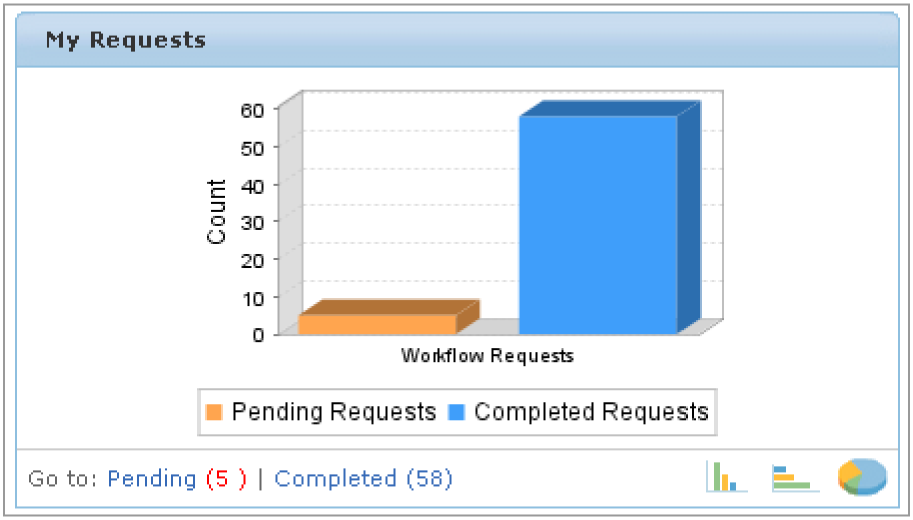
Login Details

User Id : **rbacxadmin**
First Name : **admin**
Last Name : **admin**
Email : **admin@rbacx.com**

Figure 2.1 – Role Manager Home Screen

Understanding the Graphical Representation of Data

1. My Requests



Go to: Pending (5) | Completed (58)

Figure 2.2 –My Requests

The My Requests graph shows Pending vs. Completed Requests. The Pending and Completed links guide the user to the Requests approval page. For more information on My Approval Requests, refer to chapter 5. Clicking the icons provides a different chart view of the data.

2. My Certifications

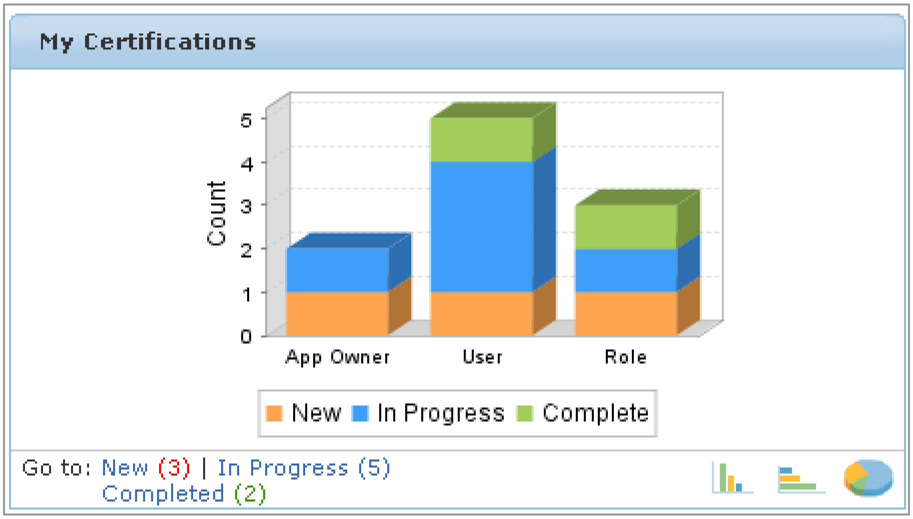


Figure 2.3 –My Certifications

The My Certifications graph displays New, In Progress and Completed certification statistics. Clicking the Pending, In Progress or Completed links takes you to the Certification inbox containing the appropriate certifications. For more information on Identity Certifications, refer to chapter 6. Clicking the 📊 ▤ ◕ icons provides a different chart view of the data.

3. Business Unit Users

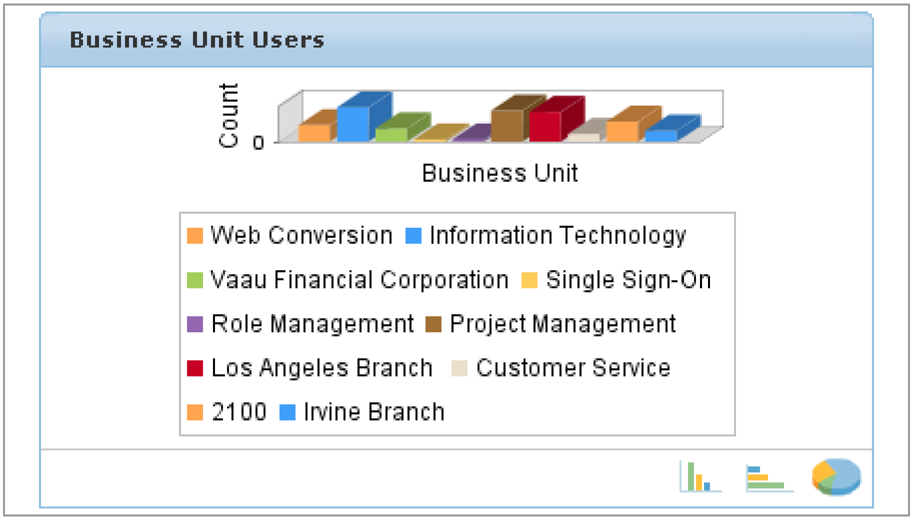


Figure 2.4 –Business Unit Users

The Business Unit Users graph displays statistics on the number of users per each business unit. For more information on Business Units, refer to chapter 3. Clicking the icons provides a different chart view of the data.

4. Certify/Revoke Statistics

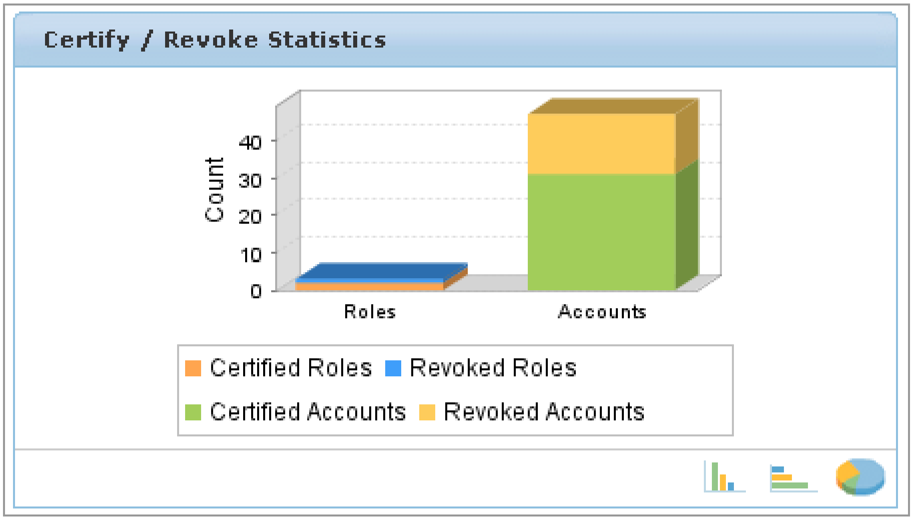


Figure 2.5 –Certify / Revoke Statistics

The Certify/Revoke Statistics graph displays the number of certified roles, revoked roles, certified accounts and revoked accounts by that user during an identity certification. For more information on different types of Identity Certifications, refer to Chapter 6. Clicking the icons provides a different chart view of the data.

5. Auditing Policy Violations

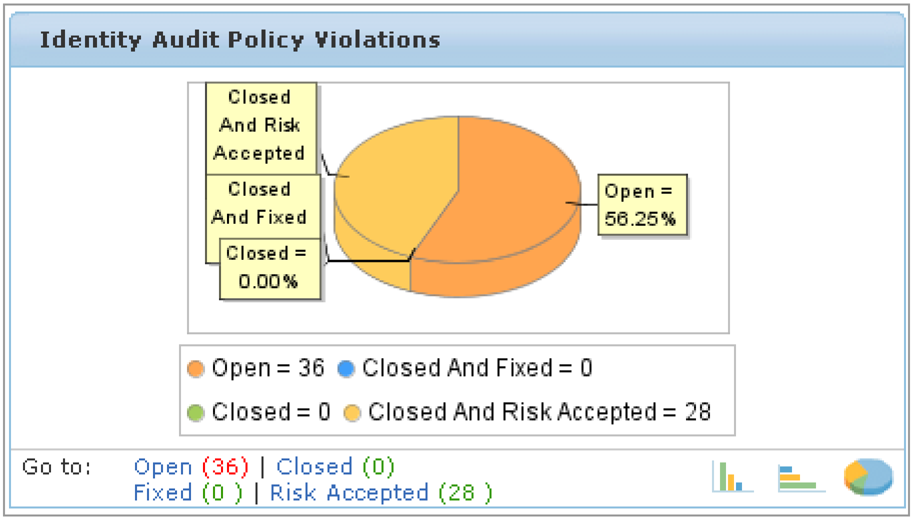
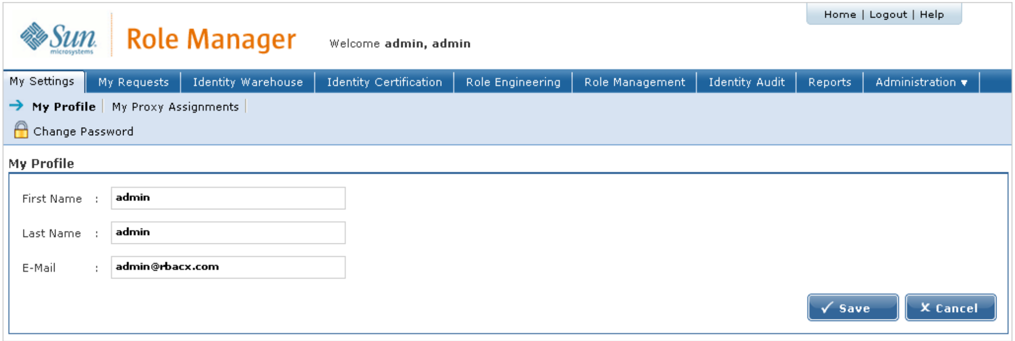


Figure 2.6 –Identity Audit Policy Violations

This graph displays the number of open, closed, fixed and risk accepted Identity Audit policy violations. Clicking the links takes the user to the appropriate violations. For more information on Identity Audit, refer to chapter 7. Clicking the icons provides a different chart view of the data.

My Profile

The My Profile tab displays the user's name and email information.



First Name : admin

Last Name : admin

E-Mail : admin@rbacx.com

Figure 2.7 – My Profile

▼ Steps to change My Profile Information

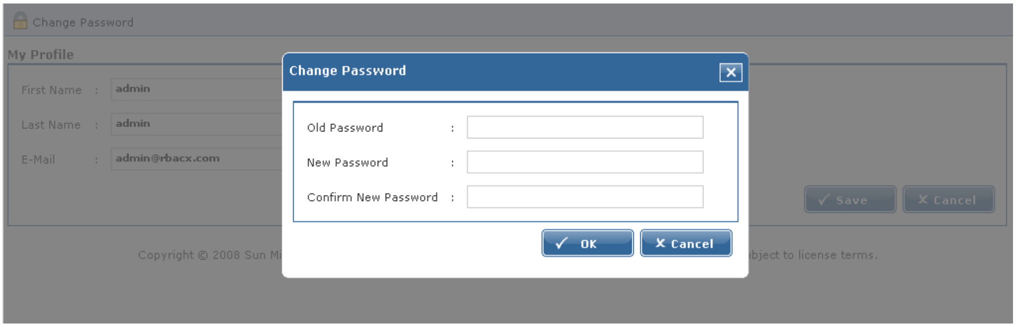
1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Go to My Settings G My Profile
4. To change the existing information, edit the required First Name, Last Name or E Mail field and click ✓ Save

Change My Password

This option is used to change the password of the current user.

▼ Steps to change password

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Go to My Settings -> My Profile -> Change Password tab



Change Password

My Profile

First Name : admin

Last Name : admin

E-Mail : admin@rbacx.com

Change Password

Old Password :

New Password :

Confirm New Password :

Copyright © 2008 Sun Mi … bject to license terms.

Figure 2.8 – Change Password

4. Enter the old password, new password and confirm it. Click ✓ Ok and then Click ✓ Save

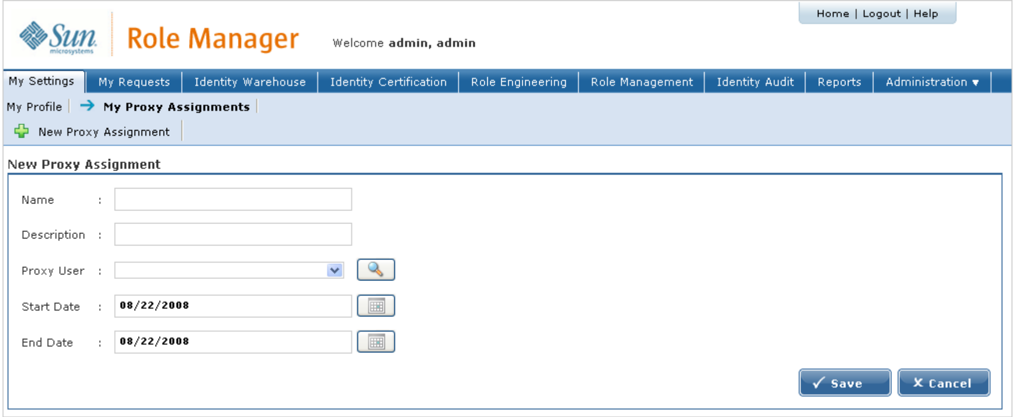
My Proxy Assignments

This option is used to delegate managers, role owners, application or data owners while on vacation or out of office. A Proxy allows a user to complete a certification when on leave by setting up another actor on the user's behalf. The delegate should be set from the day that manager leaves and cannot be set for more than 30 days.

New Proxy Assignment

▼ Steps to create a new Proxy Assignment

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Go to My Settings -> My Proxy Assignment -> New Proxy Assignment



Name :

Description :

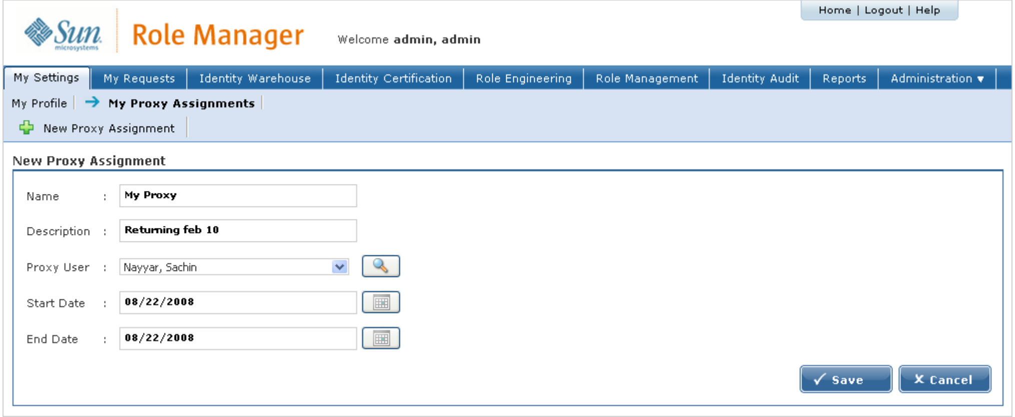
Proxy User :

Start Date : 08/22/2008

End Date : 08/22/2008

Figure 2.9 –New Proxy Assignment

4. A form as shown above is displayed. Enter the Name, Description, select the Delegate from the list of available Users and enter the Start Date and End Date.



New Proxy Assignment

Name	:	My Proxy
Description	:	Returning feb 10
Proxy User	:	Nayyar, Sachin
Start Date	:	08/22/2008
End Date	:	08/22/2008

Figure 2.10 –Enter Proxy Details

5. Click ✓ Save

6. A new Proxy Assignment will be created. The designated proxy can now log into Role Manager and perform all tasks designated to this user until the specified end date.

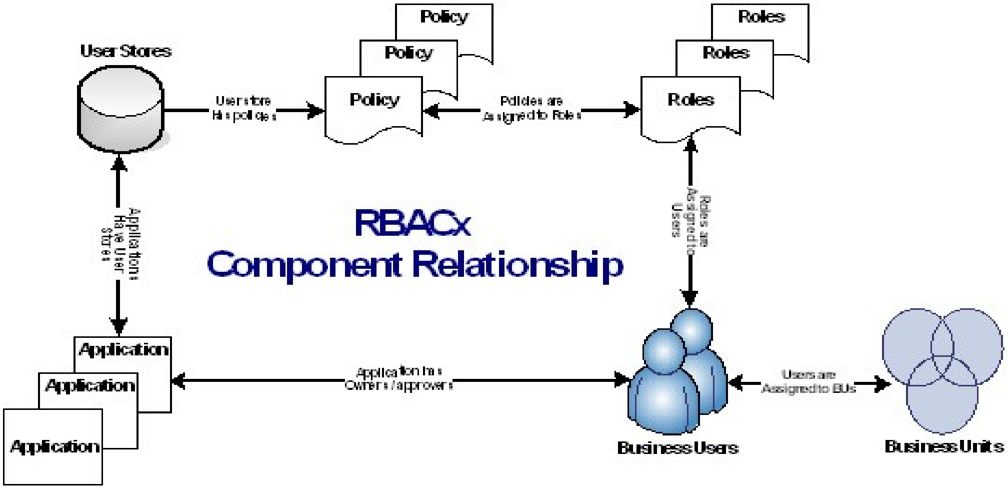
3

◆ ◆ ◆ CHAPTER 3

Role Manager Components

User Identities are stored on multiple systems within organizations. The complexity of managing and tracking user identities is compounded by various organizational lifecycle changes – mergers, acquisitions, outsourcing, job enrichment, employee transfers, contractors, terminations, business unit amalgamation and business unit break ups. Each transformation within the organization brings about a movement of user identities and change in user access on the systems.

The mandates by various privacy acts ask for more control over the access that users have to the various systems owned by the organization. The threat to data security is more from within the organization then from outside elements. These attacks can be mitigated and avoided by the advent of a framework – Role Based Access Control (RBAC). Role based access control in simplified terms implements a framework that allows for the access of systems based on the roles assigned to an individual. Administering users in this manner controls the access that users need across diverse systems.



The components illustrated above have a "many to many" relationship and are described in detail below.

Business Units/Business Structures

A *business unit* in Role Manager is defined as a department or sub-department within an organization. An organization can be segregated into as many business units as required to replicate the business structure, with as many levels of hierarchy as desired to represent teams and sub-teams within the organization. The maximum number of users that can be assigned to a business unit can be configured and does not have a ceiling. All operations in Role Manager such as Role Based Access Control, Identity Auditing and Identity Certification are performed on basis of a *Business Unit* or *Business Structure*.

Users/Business Users

A User is defined as a discrete, identifiable entity that has a business needs to access or modify enterprise information assets. Typically, a user is an individual user but can also be a program, a process or a piece of computer hardware.

Business Users or Users are associated to business units in various ways. A user can be assigned to several business units based on his access level and details in an organization. A Business user has a Manager or an Application Approver who handles the various operations of user and role management on a user.

User Store

A *user store* is the platform / database / directory where the users are stored. Examples of these are Active Directory, Exchange, ORACLE®, SAP, UNIX®, RDBMS Tables.

The entitlements from the various applications are stored in a centralized user store in Role Manager. The user store can be a relational database which handles the various user entitlements. Once the entitlements are in the user store, role engineering, identity certification and identity auditing pieces can be carried out on them.

Roles

A *role* represents a job function. Roles contain policies that describe the access that individuals have on a directory. They represent unique job function performed by users in the domain. For example, a person can function as a manager, developer, and trainer. In this case, you have three roles that represent each job function because each requires different privileges and access to different Endpoints.

Roles give you the flexibility and power to enforce enterprise standards by being able to:

- Manage users who perform the same tasks the same way no matter where they are located in the enterprise.
- Perform less work when managing users because you do not have to manually specify privileges every time a change is made to a person's job function.

A role can be embedded inside a role as a nested role. Role hierarchy can be defined to any level of subnets have role ordering in an organization.

Policy

Policies define account attributes and privileges that users have on different platforms or applications. A policy has a specific privilege on specific data resource. Policies are assigned to roles and roles are assigned to users. Policies provide consistent directory permissions and user rights across and within the organization for all of the users in a role.

Application

An *application* is a data resource that requires access by an entity. These applications may be individual assets or grouped under a common owner. Primarily applications are either platforms (Windows 2000, Win NT, UNIX, Mainframe) or Business Applications (such as, Billing, Accounts Payable). Each Application has an application owner who handles the various operations on the application like reviewing user entitlements. The user entitlements are collected from the different applications and stored in a centralized repository.

Endpoints

Endpoints are instances of a namespace. A Namespace can have multiple end-points assigned to it. For example an ORACLE namespace can have the various databases as End-Points.

User

A user is a global identity to which various accounts are associated. A user can have multiple accounts but all of the accounts are associated with a single global identity in Role Manager. This global identity is defined under the Users View. The 'Users View' shows the entire list of users that belong to the organization. In an organization the initial feed of the users is done by getting a feed from the HR system and create all the global identities in Role Manager. Alternatively the global identities can be created from a provisioning system such as Sun System Identity Manager.

A naming convention for all users should be established. A common naming convention is a combination of a user's name in lowercase letters and a set of numbers. For example, John Smith's user name might be josmit01. User names must be unique.

Create User

▼ Steps to create User

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Users View by selecting it from the Identity Warehouse Tab
4. To add a new user, click the ✚ New User New User button on the top panel
5. When the pop up window opens up, enter the User name, First name and last name for the user. Click ✓ Ok to create the user

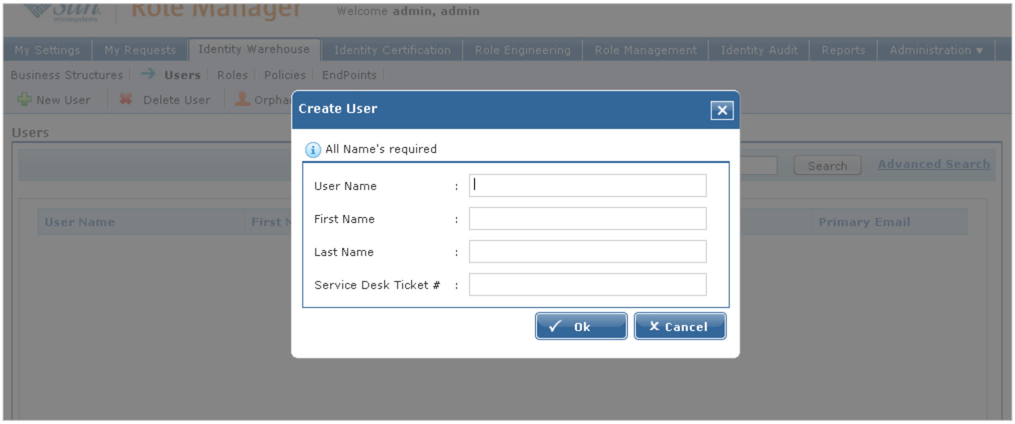


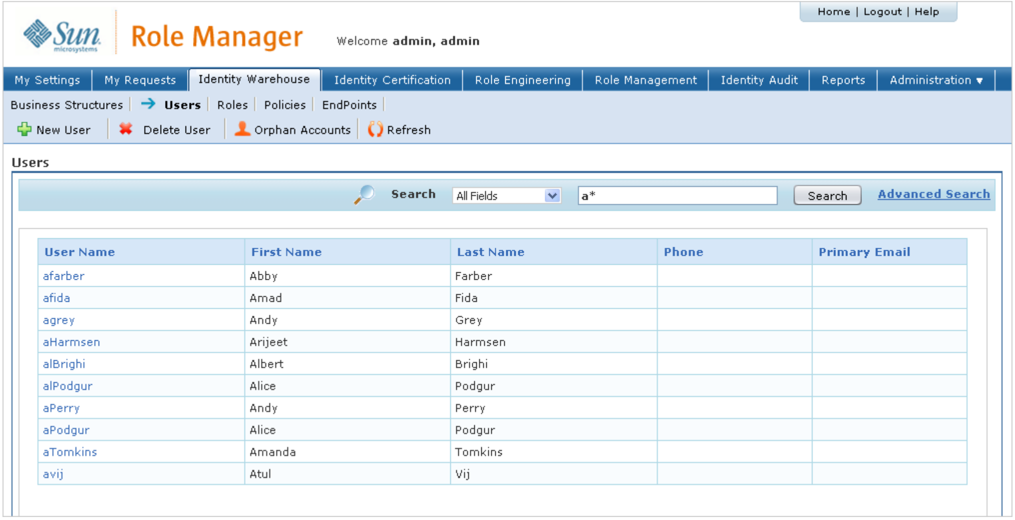
Figure3.1 –Create User

Search a User

Sun Role Manager provides quick search and advanced search options for User Search. Quick search enables search for Users on any of the commonly populated User fields (eg User Name, First Name, Last Name, Business Unit, Department, Manager etc.) Advanced Search should be used to search on a narrower search criterion. It provides the capability to create complex search conditions.

▼ Steps to Search a User(Quicksearch)

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the Users Tab
4. To use quick search select a field from the drop down box. All the commonly populated fields are available to search on
5. Enter a value to search for. Wildcards are accepted (e.g a* , *xyz*)
6. To search on the selected field for the entered value click “Search”
7. The results for the search are displayed in the panel below



Search: All Fields, a*

User Name	First Name	Last Name	Phone	Primary Email
afarber	Abby	Farber		
afida	Amad	Fida		
agrey	Andy	Grey		
aHarmsen	Arijeet	Harmsen		
alBrighi	Albert	Brighi		
alPodgur	Alice	Podgur		
aPerry	Andy	Perry		
aPodgur	Alice	Podgur		
aTomkins	Amanda	Tomkins		
avij	Atul	Vij		

Figure 3.2 – User quicksearch

▼ Steps to Search a User (Advanced Search):

1. Start Sun Role Manager by clicking the Sun Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Sun Role Manager
3. Select the Identity Warehouse Tab and then select the Users Tab

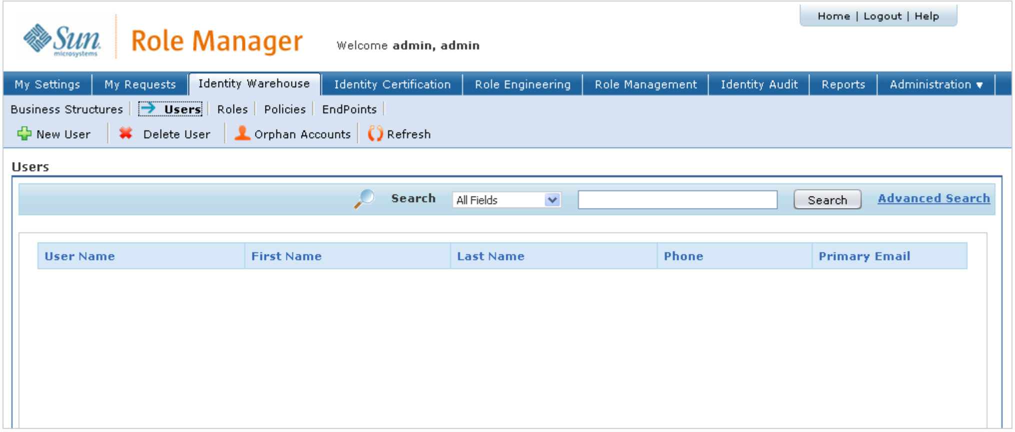
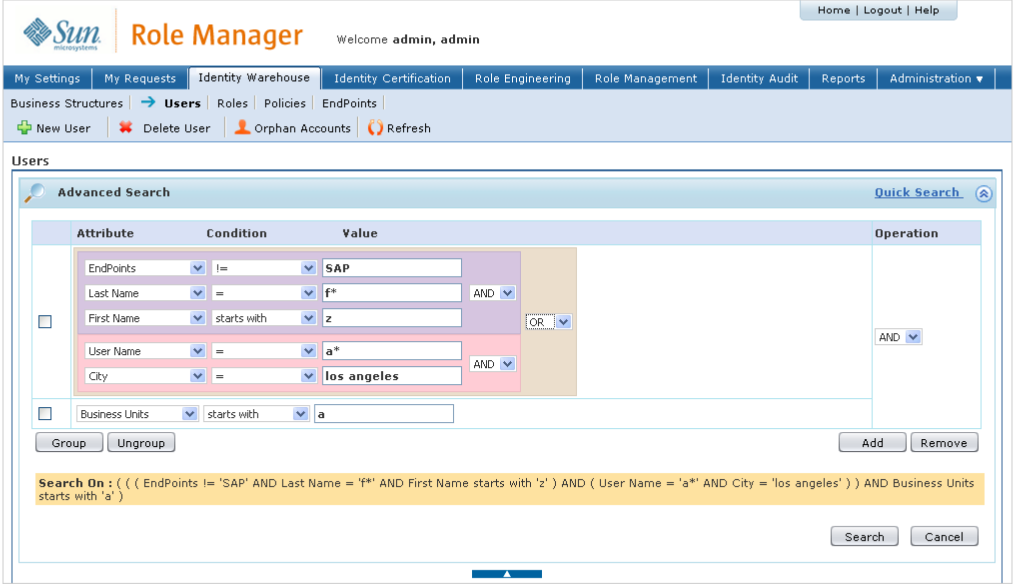


Figure 3.3 - User Advanced Search

4. Select the Advanced Search Tab
5. Create a condition by selecting values for “Attribute”, “Condition” and “Value”. Attribute can be selected over an extensive range including endpoints, business units and any other commonly populated user field. Value supports wildcards (eg. a* or *xyz*)
6. To create more conditions click “Add”
7. To remove any condition(s) select the condition(s) by selecting its corresponding checkbox and click “Remove”
8. n the case of multiple conditions set “Operation” to “AND” or “OR” to specify the logical operation between the conditions.
9. To group two conditions together select them and click “Group”
10. Groupings are displayed by a different color coding for each group. In the case of nested groups the outermost grouping will have one color code with each component group having its own color code.
11. To ungroup a grouped conditional select the grouped conditional by selecting its corresponding checkbox and click “Ungroup”

12. The created search condition is dynamically displayed in a high-lighted line under the “Group” and “Ungroup” tags as a single logical condition

13. To search on the created condition click “Search”



	Attribute	Condition	Value			Operation
□	EndPoints	!=	SAP		OR	AND
	Last Name	=	f*	AND		
	First Name	starts with	z			
	User Name	=	a*	AND		
	City	=	los angeles			
□	Business Units	starts with	a			

Search On : (((EndPoints != 'SAP' AND Last Name = 'f*' AND First Name starts with 'z') AND (User Name = 'a*' AND City = 'los angeles')) AND Business Units starts with 'a')

Figure 3.4 – User Advanced Search Conditions

Set User Status

User status allows the user to set the status as active or inactive. A User in Role Manager can be terminated and the end date of the user can be specified. Depending on the User status in an organization this field can be set.

▼ Steps to Set User Status

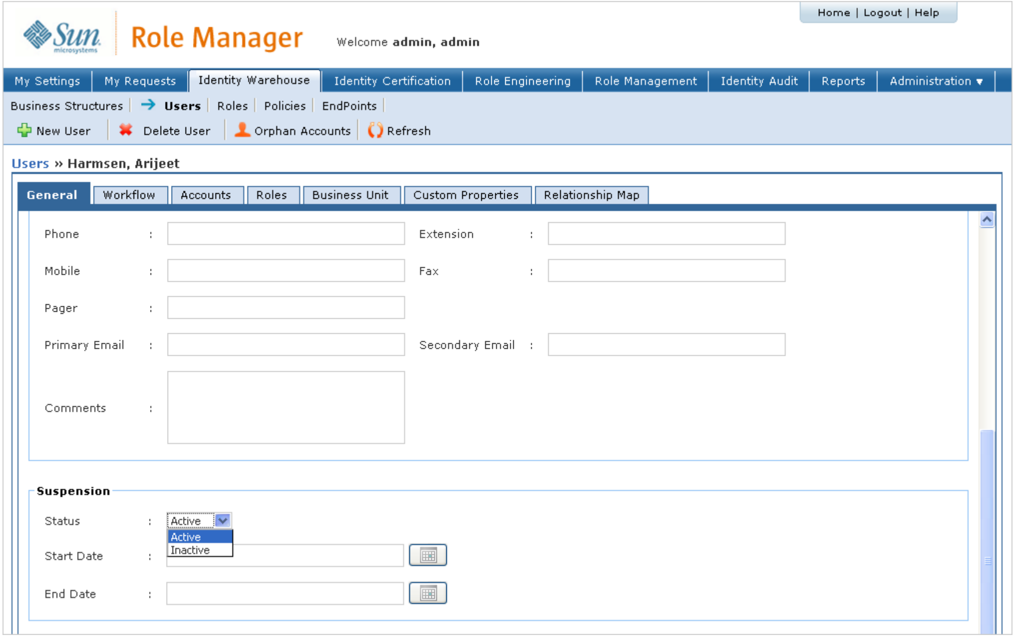
1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the User Tab

4. Select a User by double clicking it

5. Browse to the General tab of the User

6. Scroll down to the Status field

7. Select the Status as Active or Inactive from the drop down dialog box



Users » Harmsen, Arijeet

Status : Active

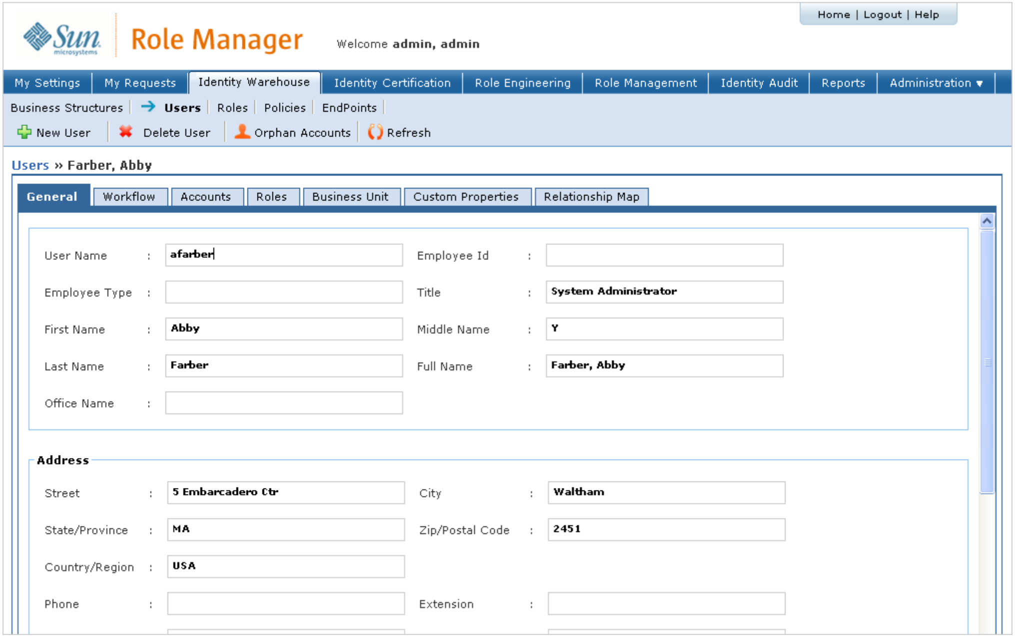
Figure 3.5 – Set Status of User

8. If the user is set as Inactive specify the End Date of the user.

Rename a User

▼ Steps to Rename a User

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the User Tab
4. Right click a User and select Rename



User Name :	afarber	Employee Id :	
Employee Type :		Title :	System Administrator
First Name :	Abby	Middle Name :	Y
Last Name :	Farber	Full Name :	Farber, Abby
Office Name :			

Address

Street :	5 Embarcadero Ctr	City :	Waltham
State/Province :	MA	Zip/Postal Code :	2451
Country/Region :	USA		
Phone :		Extension :	

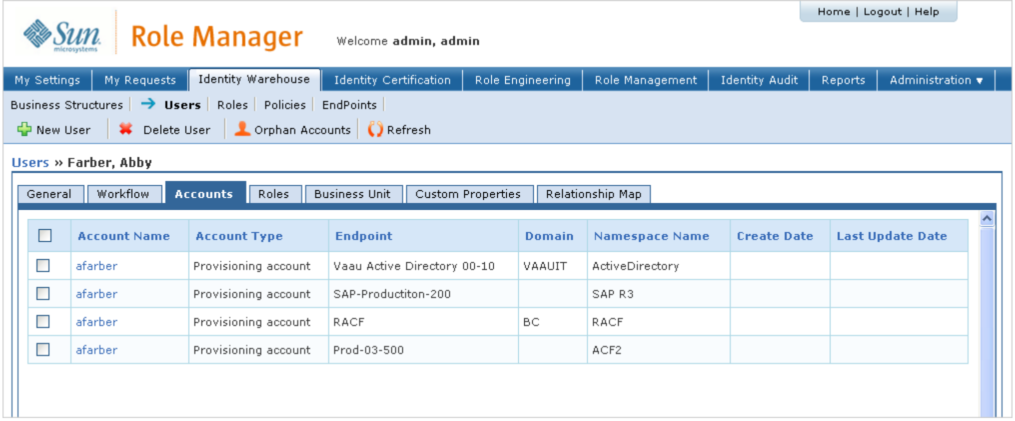
Figure 3.6 – Rename User

5. Enter the new User name for the User

View User Accounts (Entitlements)

▼ Steps to View User Accounts of a User

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the User Tab
4. Search for the required user
5. Click the User and navigate to the Accounts Tab
6. Click the required Account as shown below to view Account details



□	Account Name	Account Type	Endpoint	Domain	Namespace Name	Create Date	Last Update Date
□	afarber	Provisioning account	Vaau Active Directory 00-10	VAAUIT	ActiveDirectory		
□	afarber	Provisioning account	SAP-Productiton-200		SAP R3		
□	afarber	Provisioning account	RACF	BC	RACF		
□	afarber	Provisioning account	Prod-03-500		ACF2		

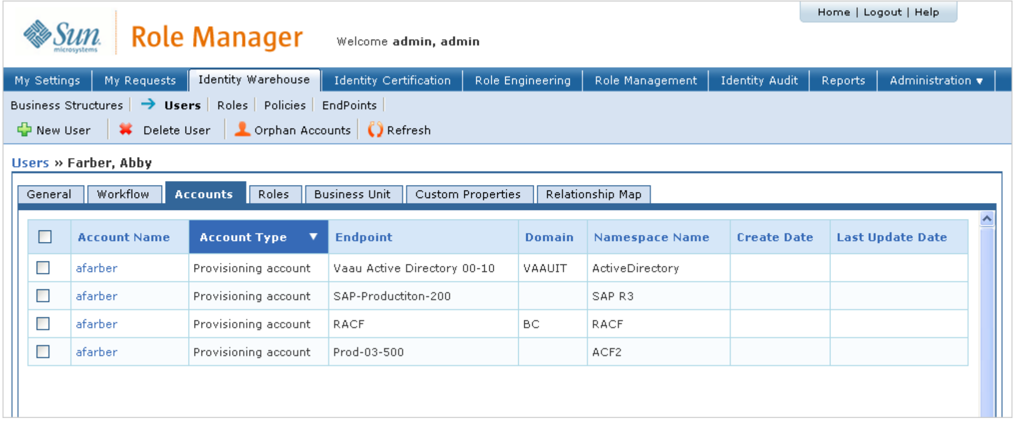
Figure 3.7 – Account Details

Account Type

Account Type facilitates an enhanced account definition. The ability to identify the "type" associated with an account promotes better decisions during tasks such as performing remediation, access certification and performing a role engineering wave. To designate an account type while importing accounts using the Role Manager automated import process a “type” attribute should be provided in the .rbx schema file. This predefined account “type” could then be leveraged while performing Identity Certifications, Role Engineering and remediation allowing the different Role Manager actors to make educated decisions.

▼ Steps to view Account Type:

1. Start Sun Role Manager by clicking the Sun Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Sun Role Manager
3. Select the Identity Warehouse Tab and then select the Users Tab
4. Search for a User using the quick search or Advanced Search feature
5. Select a user by clicking the User Name
6. Select the Accounts Tab
7. “Type” of the account is visible under the Account Type field



Users » Farber, Abby

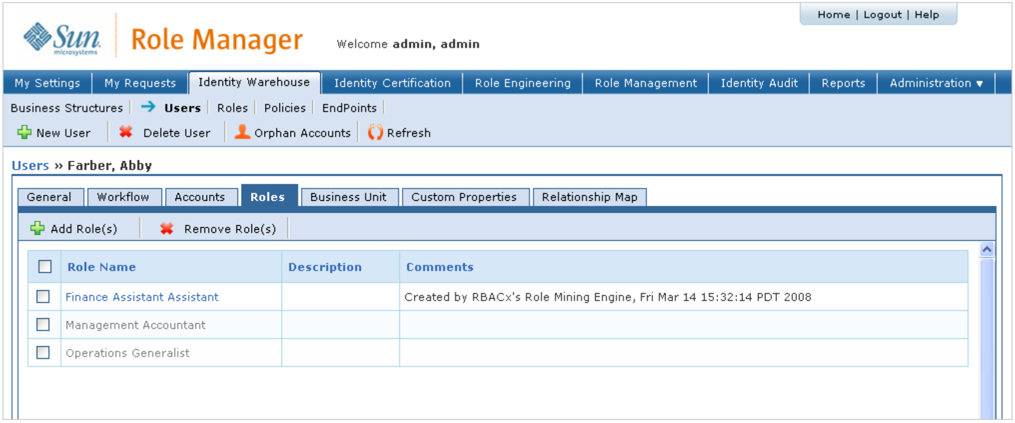
□	Account Name	Account Type ▼	Endpoint	Domain	Namespace Name	Create Date	Last Update Date
□	afarber	Provisioning account	Vaau Active Directory 00-10	VAAUIT	ActiveDirectory		
□	afarber	Provisioning account	SAP-Productiton-200		SAP R3		
□	afarber	Provisioning account	RACF	BC	RACF		
□	afarber	Provisioning account	Prod-03-500		ACF2		

Figure 3.8 – Account Type

Associate User to Role(s)

▼ Steps to associate user to role(s)

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the User Tab
4. Search for the required user
5. Click the User and navigate to the Roles Tab
6. Click the ✚ Add Role(s) icon and add the desired roles to the User. Click ✓ Save



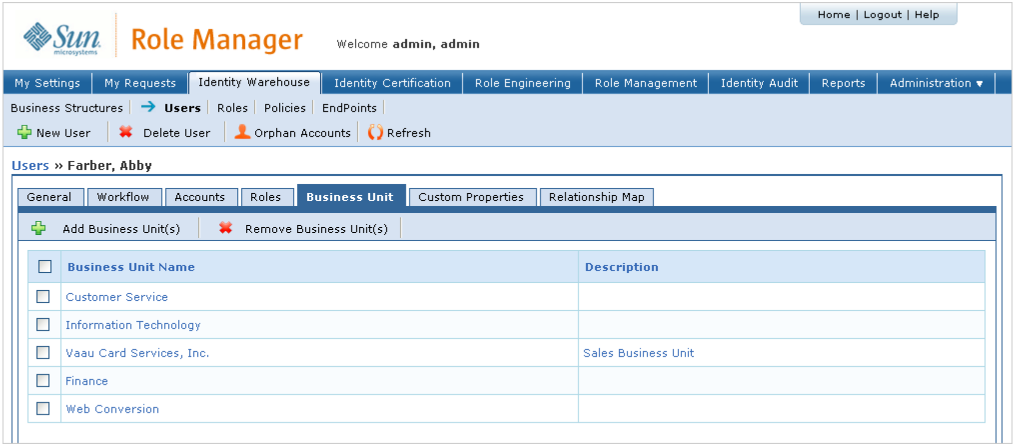
☐	Role Name	Description	Comments
☐	Finance Assistant Assistant		Created by RBACx's Role Mining Engine, Fri Mar 14 15:32:14 PDT 2008
☐	Management Accountant		
☐	Operations Generalist		

Figure 3.9 – Add Roles to User

Associate User to Business Unit

▼ Steps to associate user to Business Unit

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the User Tab
4. Search for the required user
5. Click the User and navigate to the Business Unit Tab
7. Click ✚ Add Business Unit(s) and add the desired Business Unit(s) to the User. Click ✓ Save



☐	Business Unit Name	Description
☐	Customer Service	
☐	Information Technology	
☐	Vaau Card Services, Inc.	Sales Business Unit
☐	Finance	
☐	Web Conversion	

Figure 3.10 – Add Business Unit(s) to User

Delete a User

▼ Steps to Delete a User

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the Users Tab
4. Search for a User using user quicksearch or advanced user search capability
5. To delete a user, select it by clicking on the username and click the ✖ Delete User (delete) button

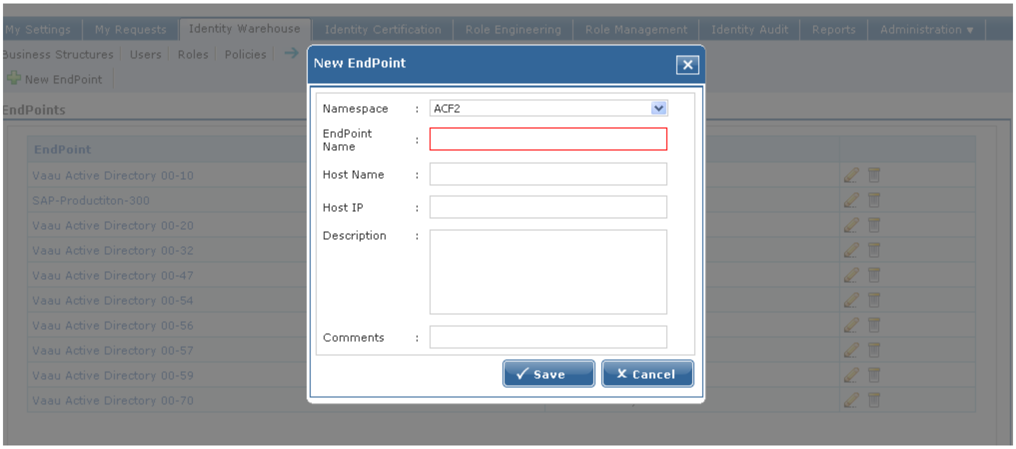
Endpoints

Endpoints are instances of a namespace. A Namespace can have multiple end-points assigned to it. For example an ORACLE namespace can have the various databases as End-Points.

Create / Modify Endpoints

▼ Steps to Manage an Endpoint view

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse Tab and then select the End Point.
4. To add a new Endpoint , click the ✚ New EndPoint (new) button on the top panel



Vaau Active Directory 00-10
SAP-Productiton-300
Vaau Active Directory 00-20
Vaau Active Directory 00-32
Vaau Active Directory 00-47
Vaau Active Directory 00-54
Vaau Active Directory 00-56
Vaau Active Directory 00-57
Vaau Active Directory 00-59
Vaau Active Directory 00-70

New EndPoint

Namespace : ACF2
EndPoint Name :
Host Name :
Host IP :
Description :
Comments :

✓ Save ✕ Cancel

Figure 3.11 – New Endpoint

5. This opens a new pop up window from where you select the namespace to which the new end point/directory would belong to, Endpoint Name, Host Name, etc. and click ✓ Save

Policies

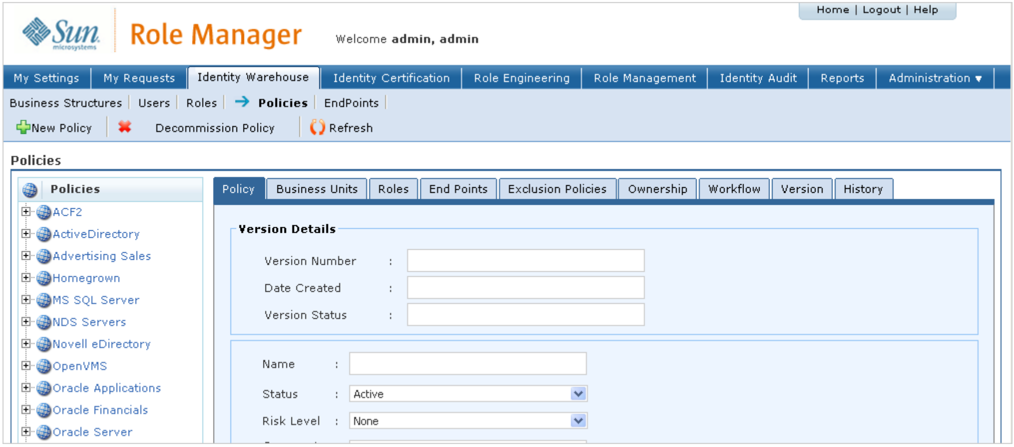
Policies are templates which define the various access levels a user has on the target systems. Policies are uniquely defined for the end-points and Roles consist of Policies. The Polices component displays all available policies that exist for the organization categorized according to namespaces. Namespaces are depicted as 🌐. Under each Namespace the available policies are shown.

Create / Modify Policies

▼ Steps to manage a policy

1. Start Role Manager by clicking the Role Manager Icon

2. The login dialog box appears. Enter your credentials and login to Role Manager



Version Number :

Date Created :

Version Status :

Name :

Status : Active

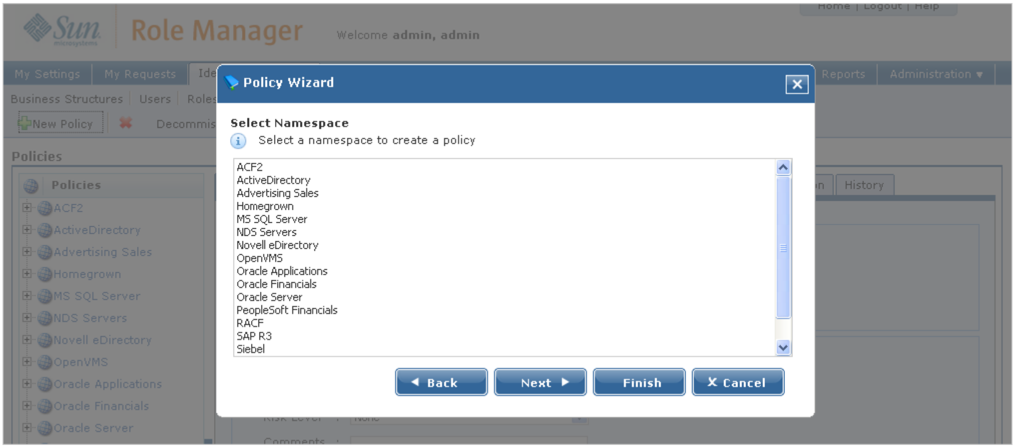
Risk Level : None

Figure 3.12 – Create Policy

3. Select the Identity Warehouse Tab and then select the Policy Tab

4. To add a new policy, click the New Policy (new) button on the top panel

5. This opens a new pop up window which prompts the selection of the namespace on which the policy is to be created



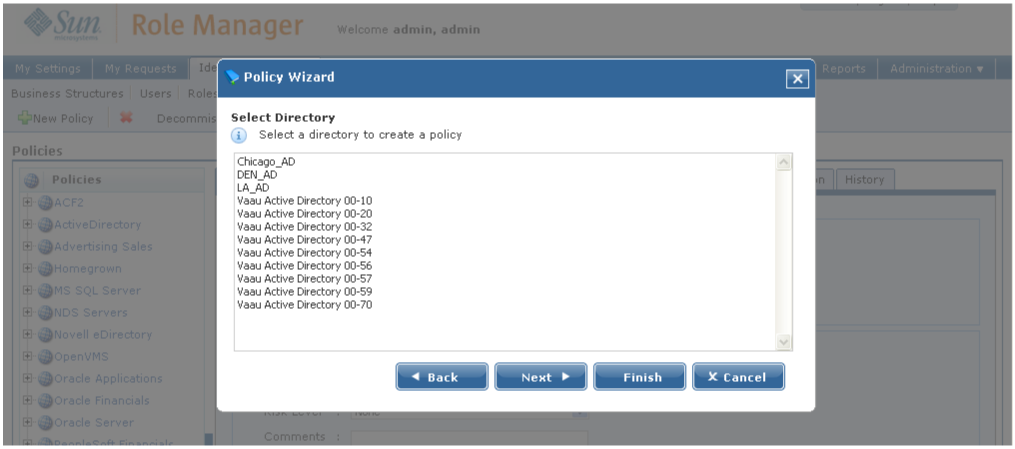
Select Namespace

Select a namespace to create a policy

ACF2
ActiveDirectory
Advertising Sales
Homegrown
MS SQL Server
NDS Servers
Novell eDirectory
OpenVMS
Oracle Applications
Oracle Financials
Oracle Server
PeopleSoft Financials
RACF
SAP R3
Siebel

Figure 3.13 – Policy Wizard –Select Namespace

6. After you select the above options click Next ▶



Policy Wizard

Select Directory

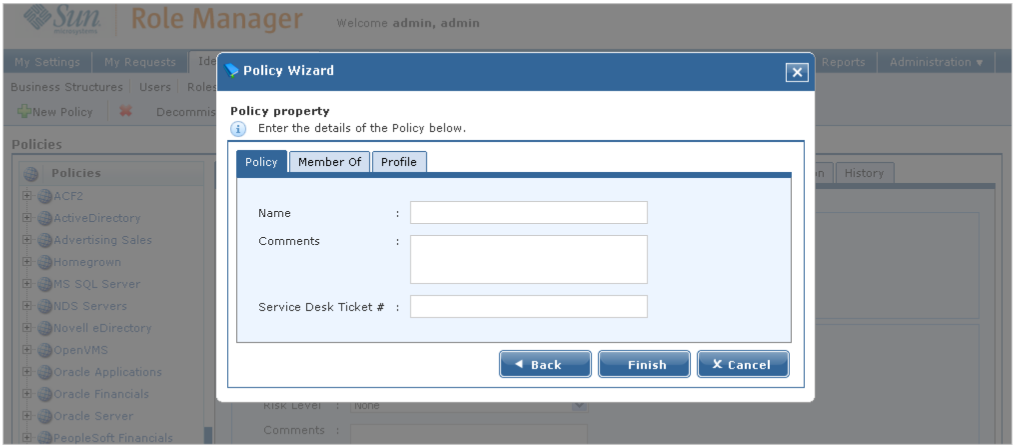
Select a directory to create a policy

Chicago_AD
DEN_AD
LA_AD
Vaau Active Directory 00-10
Vaau Active Directory 00-20
Vaau Active Directory 00-32
Vaau Active Directory 00-47
Vaau Active Directory 00-54
Vaau Active Directory 00-56
Vaau Active Directory 00-57
Vaau Active Directory 00-59
Vaau Active Directory 00-70

◀ Back | Next ▶ | Finish | ✕ Cancel

Figure 3.14 – Policy Wizard – Select Directory (Endpoint)

7. After the namespace is selected the Endpoints in the namespace will be displayed. Select the directory / end point on which the access level need to be defined



Policy Wizard

Policy property

Enter the details of the Policy below.

Policy | Member Of | Profile

Name :

Comments :

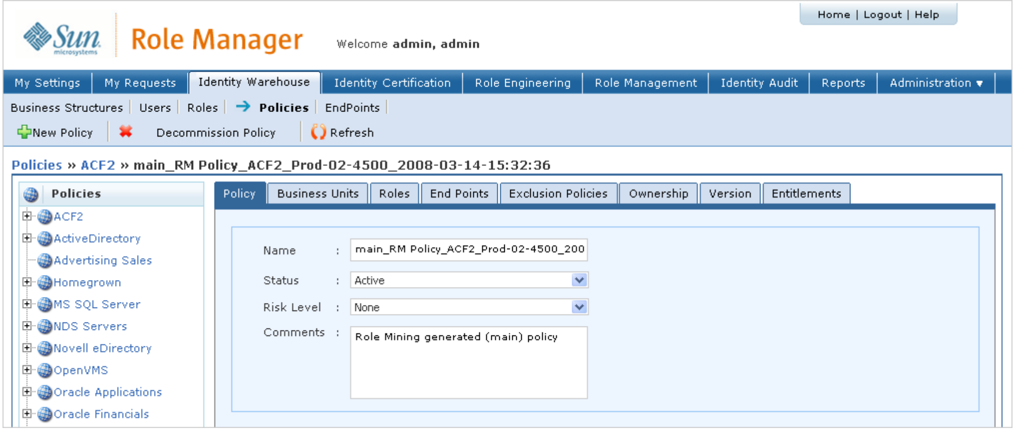
Service Desk Ticket # :

◀ Back | Finish | ✕ Cancel

Figure 3.15 – Policy Wizard – Policy Properties

8. Once the Directory is selected the Policy property sheet is displayed. The Property sheet is different for different namespaces. Enter the details of the policy and save the policy. Once it is saved it will be shown under its namespace.

9. To rename a policy select the policy by clicking on the policy name. Change the name of the policy under “Policy” Tab and click “Save”



Policies » ACF2 » main_RM Policy_ACF2_Prod-02-4500_2008-03-14-15:32:36

Name : main_RM Policy_ACF2_Prod-02-4500_200

Status : Active

Risk Level : None

Comments : Role Mining generated (main) policy

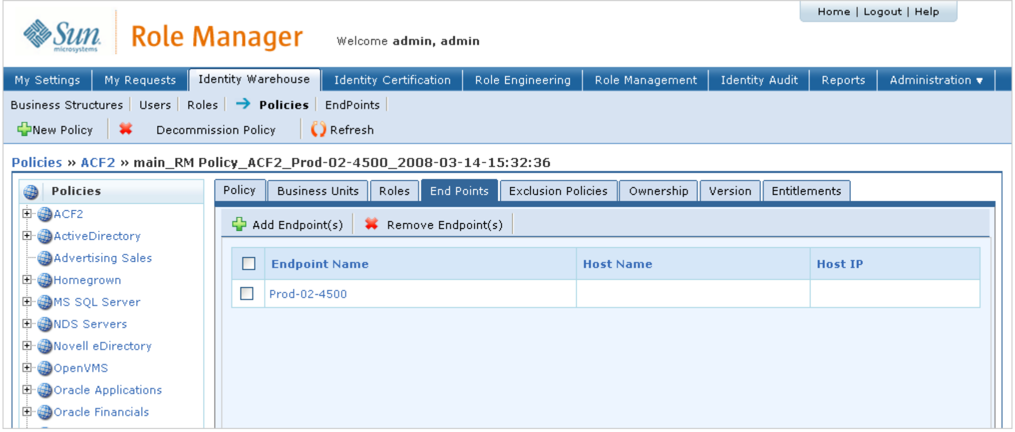
Figure 3.16 – Rename Policy

10. To delete a policy, select the policy to be deleted and click the ✖ Delete Policy button.

Associate Policy / Endpoints

▼ Steps to Associate Policy with Endpoints

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Identity Warehouse tab and then select the Policy Tab
4. A Directory is added when a Policy is created
5. The Association between a Policy and Directory is shown in the Directory tab



Policies » ACF2 » main_RM Policy_ACF2_Prod-02-4500_2008-03-14-15:32:36

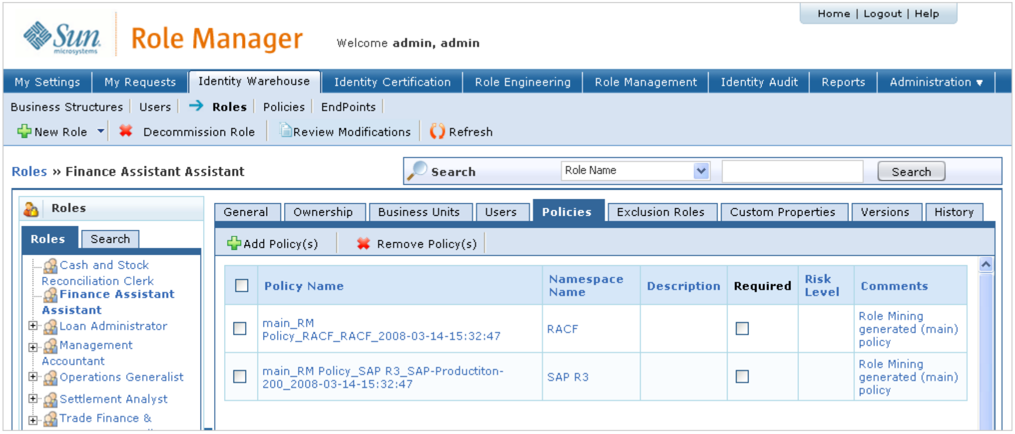
□	Endpoint Name	Host Name	Host IP
□	Prod-02-4500		

Figure 3.17 –Associate Policy Endpoint

Associate Policy / Role

▼ Steps to Associate Policy with Roles

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Role View by selecting it from the Identity Warehouse Tab.
4. Select a Role and add Policies to a Role from the Policy tab
5. Addition of any policy from the available list to the Selected Policies list is done by clicking the Add Policy(s) button
6. Similarly to remove any associated policy for that directory, click the Remove Policy(s) button. Once a change has been made, click the ✓ Save button.
7. The Policies associated with a Role will be shown under the Policies tab for the role



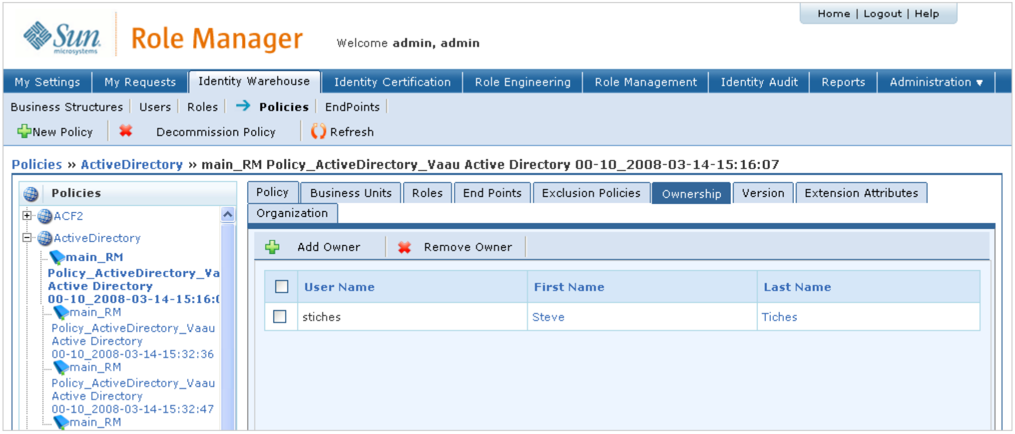
☐	Policy Name	Namespace Name	Description	Required	Risk Level	Comments
☐	main_RM Policy_RACF_RACF_2008-03-14-15:32:47	RACF		☐		Role Mining generated (main) policy
☐	main_RM Policy_SAP R3_SAP-Productiton-200_2008-03-14-15:32:47	SAP R3		☐		Role Mining generated (main) policy

Figure 3.18 – Associate Policy to Role

Associate Policy Owners to Policy

▼ Steps to associate policy owners to policy

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Policy View by selecting it from the Identity Warehouse Tab
4. Click a Role and browse to the Ownership Tab
5. Click Add Owners and select the desired User(s) . Click ✓ Save



Policies » ActiveDirectory » main_RM Policy_ActiveDirectory_Vaau Active Directory 00-10_2008-03-14-15:16:07

□	User Name	First Name	Last Name
□	stiches	Steve	Tiches

Figure 3.19 – Associate Policy Owner to Policy

Roles

Role Manager is used to administer Role Based Access Control. A primary component to administer Role Based Access is Roles. A Role is a collection of access level and a user is defined his access level based on the Role. Roles can be defined in a hierarchical format and Segregation of Duties (SOD) can be administered through a Role.

Role-based administration typically grows and expands as new situations occur. The main advantage to using this approach is ease of implementation. Role-based administration can be established in a centralized fashion, distributed throughout your network, or hybridized. Implementing Role Manager allows you to optimally match the unique structure and needs of your organization.

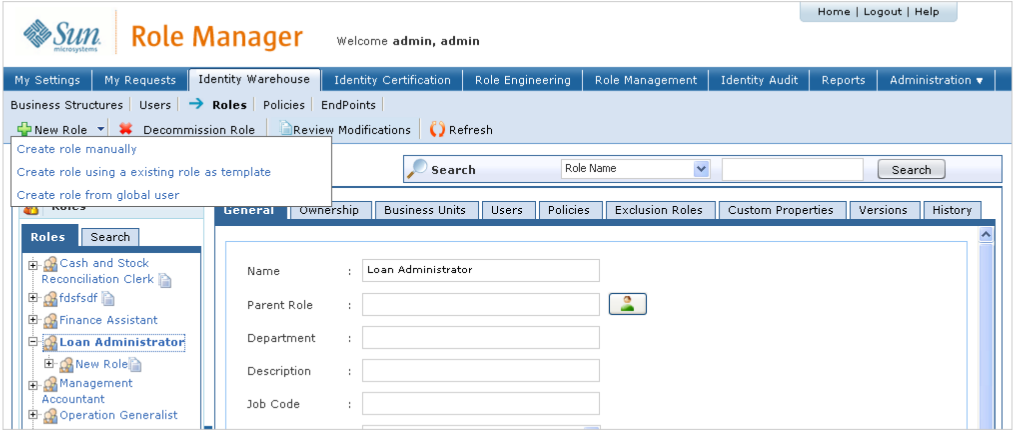
Create Roles

Sun Role Manager provides three options for Role creation. Roles may also be renamed or decommissioned

Create Role Manually

▼ Steps to create Role manually

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialog box appears. Enter your credentials and login to Sun Role Manager
3. Select the Role view by selecting it from the Identity Warehouse Tab
4. Take the cursor/pointer over the Tab “New Role”
5. A small menu appears with three options. Select “Create role manually”



Name : Loan Administrator

Parent Role :

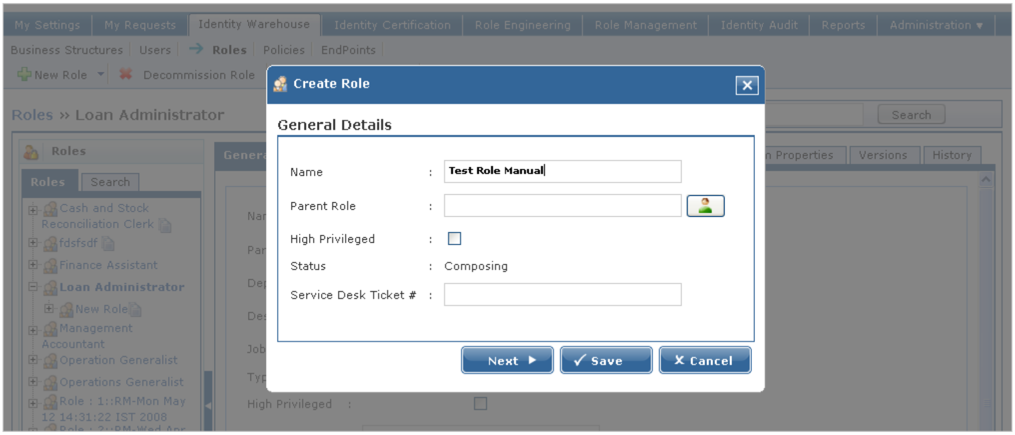
Department :

Description :

Job Code :

Figure 3.20 – Create Role Options

6. A Create Role window opens up. Fill in the values for Name. Select the check-box for High privileged to make this a high privileged role

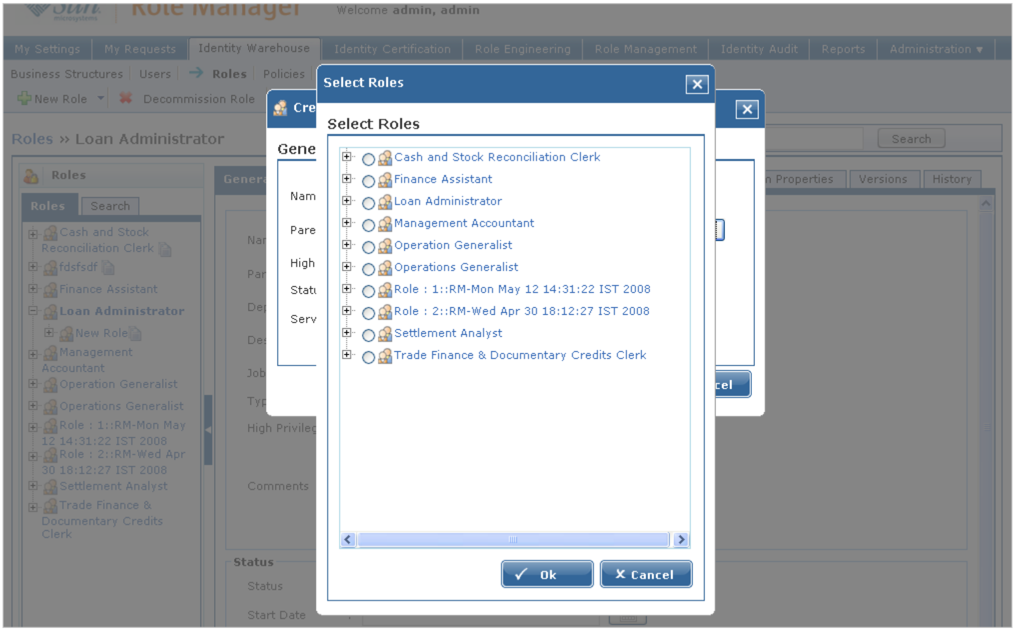


General Details

Name	:	Test Role Manual
Parent Role	:	
High Privileged	:	□
Status	:	Composing
Service Desk Ticket #	:	

Figure 3.21 – Create Role Manually – General Details

7. To select a parent for the Role click on the icon next to the Parent Role field. This opens a Select Role window. Select the Role to be made the parent Role and click “Ok”

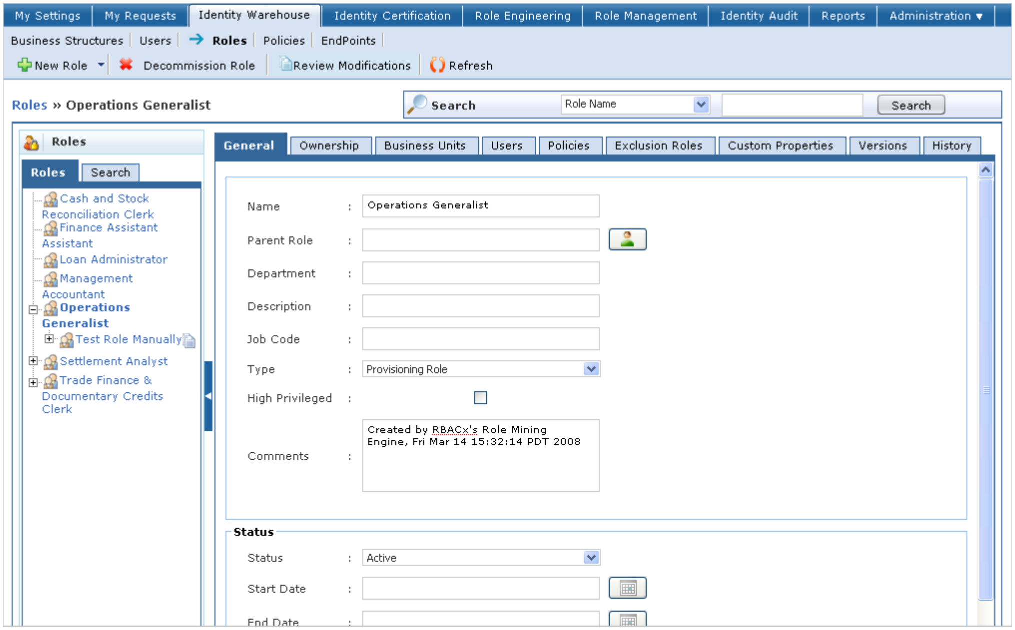


Select Roles

- ○ Cash and Stock Reconciliation Clerk
- ○ Finance Assistant
- ○ Loan Administrator
- ○ Management Accountant
- ○ Operation Generalist
- ○ Operations Generalist
- ○ Role : 1::RM-Mon May 12 14:31:22 IST 2008
- ○ Role : 2::RM-Wed Apr 30 18:12:27 IST 2008
- ○ Settlement Analyst
- ○ Trade Finance & Documentary Credits Clerk

Figure 3.22 – Create Role Manually – Select Parent Role

8. After filling in values in the Create Role window click “Save” to create the Role. The Role is now available in the Roles view under Identity Warehouse Tab



Roles » Operations Generalist

Name : Operations Generalist

Parent Role :

Department :

Description :

Job Code :

Type : Provisioning Role

High Privileged : □

Comments : Created by RBACx's Role Mining Engine, Fri Mar 14 15:32:14 PDT 2008

Status

Status : Active

Start Date :

End Date :

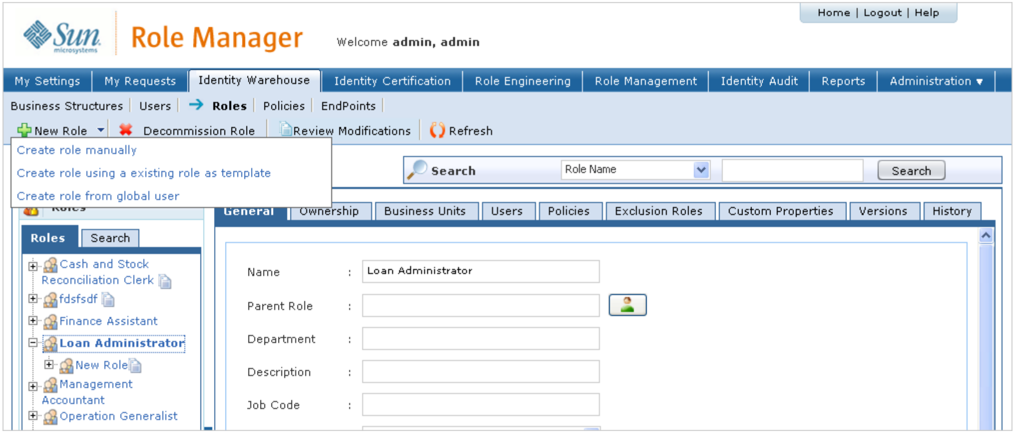
Figure 3.23 – Create Role Manually – Created Role

Create Role from Existing Role

Sun Role Manager allows the creation of a Role from an existing Role as template. The new Role created will be an exact copy of the template Role. It can then be modified as required.

▼ Steps to Create a Role from an Existing Role

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialogue box appears. Enter your credentials and login to Sun Role Manager
3. Select the Role view by selecting it from the Identity Warehouse Tab
4. Take the cursor/pointer over the Tab “New Role”
5. A small menu appears with three options. Select “Create role using an existing role as template”



Name : Loan Administrator

Figure 3.24 – Create Role Options

6. A “Create Role” window opens up

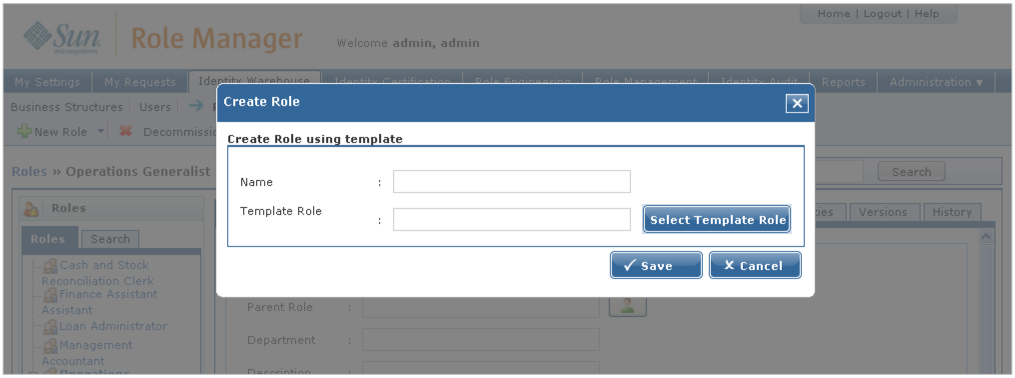
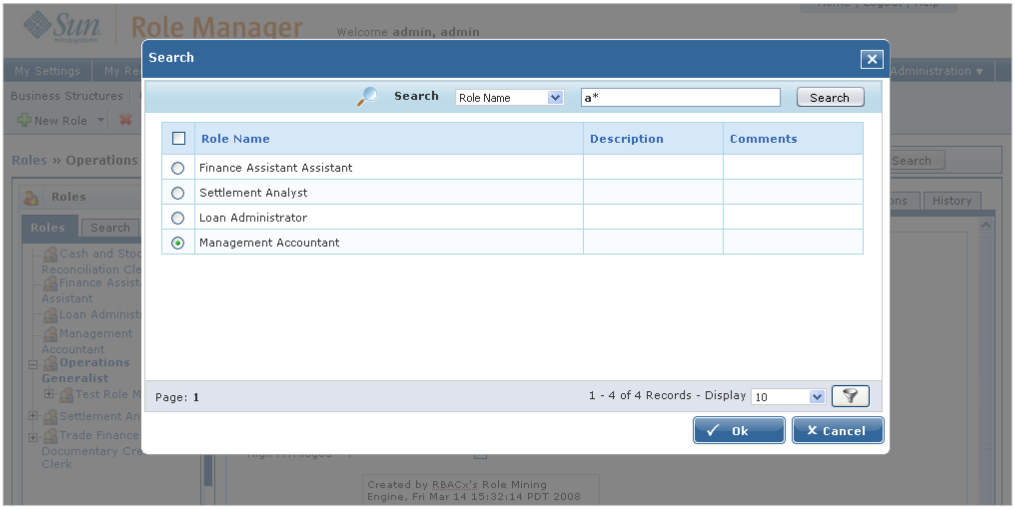


Figure 3.25 – Create Role from Existing Role

7. Enter the name for the new Role

8. Select “Select Template Role” to select the role to be used as a template

9. A search window opens. Use the Role quick search feature to search for a Role. Select a role from the result and click “Ok”



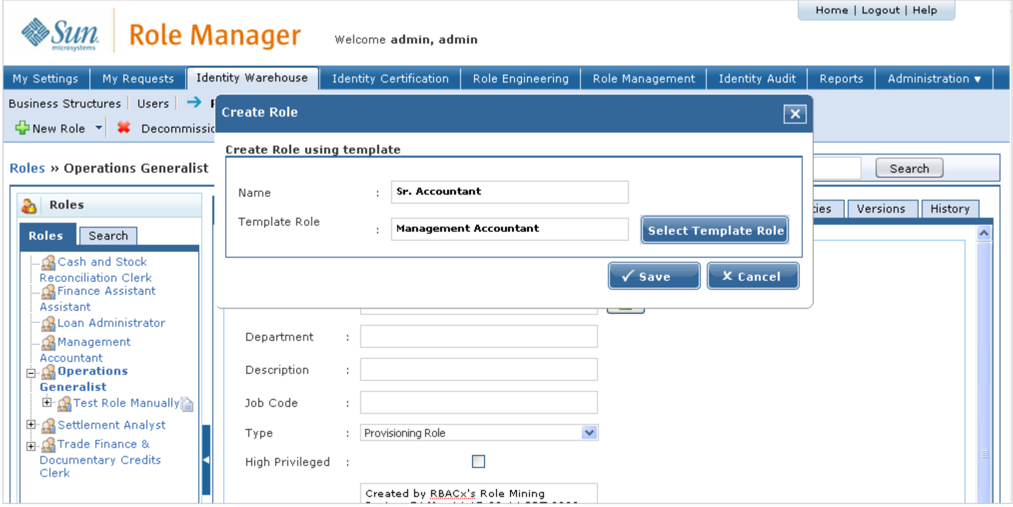
Search: Role Name — a*

☐	Role Name	Description	Comments
○	Finance Assistant Assistant		
○	Settlement Analyst		
○	Loan Administrator		
●	Management Accountant		

Page: 1   1 - 4 of 4 Records - Display 10

Figure 3.26 – Select Template Role from Role Search Results

10. Select “Save” on the “Create Role” window to create the Role



Create Role

Create Role using template

Name : Sr. Accountant

Template Role : Management Accountant

Department :

Description :

Job Code :

Type : Provisioning Role

High Privileged : ☐

Created by RBACx's Role Mining

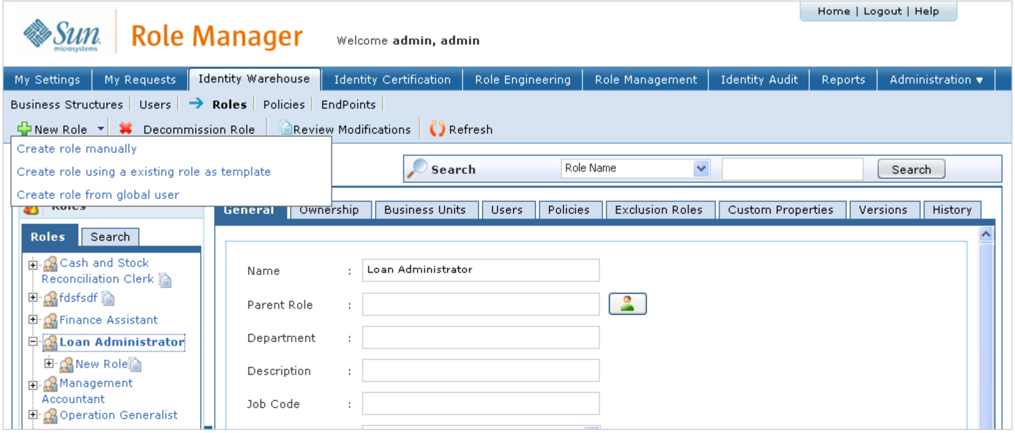
Figure 3.27 – Create Role using Template – click “Save”

Create Role from Global User

Sun Role Manager allows the creation of a new Role from a Global User. All the entitlements that the selected Global User has are used to create corresponding policies that are assigned to the new Role.

▼ Steps to Create a Role from a Global User

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialogue box appears. Enter your credentials and login to Sun Role Manager
3. Select the Role view by selecting it from the Identity Warehouse Tab
4. Take the cursor/pointer over the Tab “New Role”
5. A small menu appears with three options. Select “Create role from global user”



Name : Loan Administrator

Parent Role :

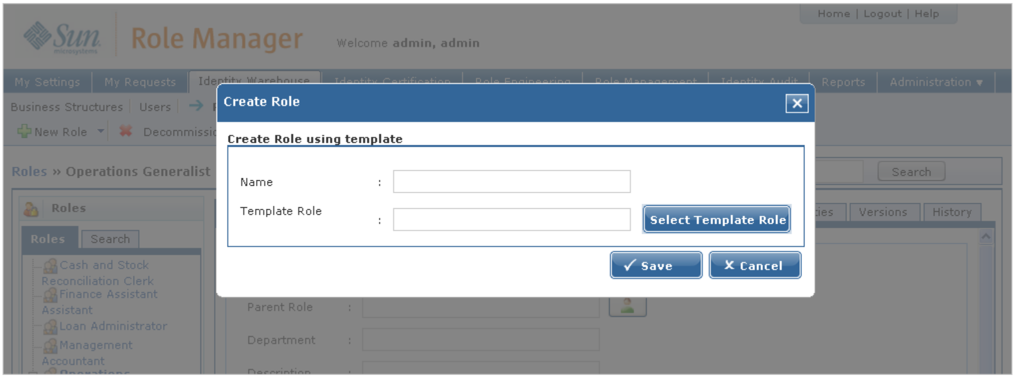
Department :

Description :

Job Code :

Figure 3.28 – Create Role Options

6. A “Create Role” window opens up



Create Role

Create Role using template

Name	:	
Template Role	:	Select Template Role

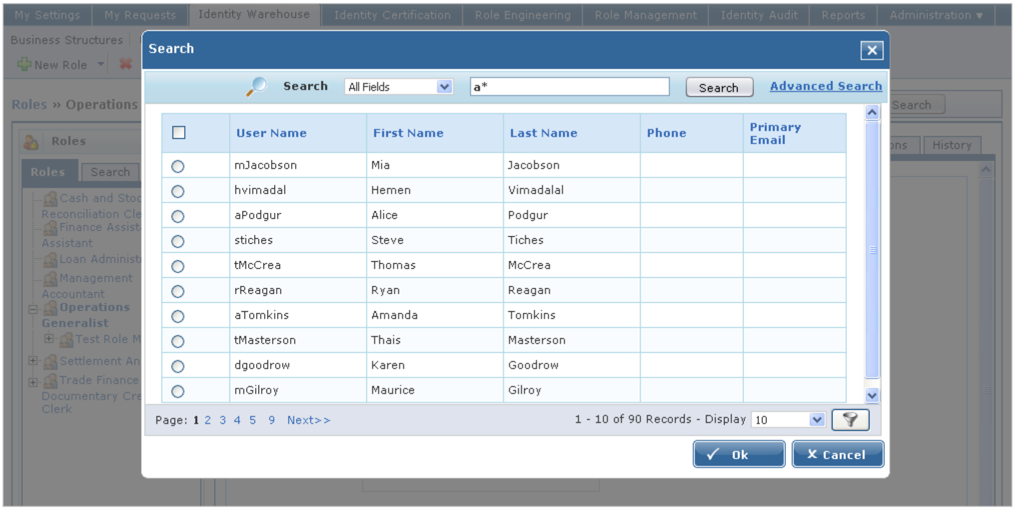
✓ Save ✕ Cancel

Figure 3.29 – Create Role from Global User

7. Enter the name for the new Role

8. Select “Select Global User” to select the Global User to be used

9. A search window opens. Use the User quick search or Advanced Search feature to search for a User. Select a User from the result and click “Ok”



Search

Search All Fields a* Search Advanced Search

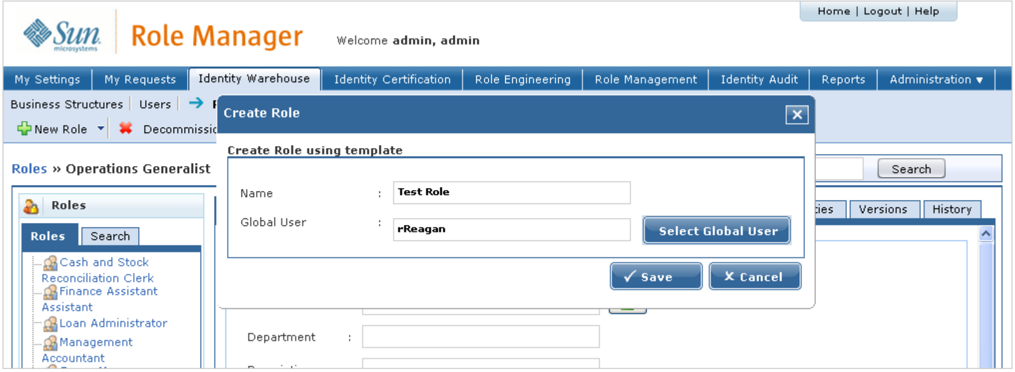
□	User Name	First Name	Last Name	Phone	Primary Email
○	mJacobson	Mia	Jacobson		
○	hvimadal	Hemen	Vimadalal		
○	aPodgur	Alice	Podgur		
○	stiches	Steve	Tiches		
○	tMcCrea	Thomas	McCrea		
○	rReagan	Ryan	Reagan		
○	aTomkins	Amanda	Tomkins		
○	tMasterson	Thais	Masterson		
○	dgoodrow	Karen	Goodrow		
○	mGilroy	Maurice	Gilroy		

Page: 1 2 3 4 5 9 Next>> 1 - 10 of 90 Records - Display 10

✓ Ok ✕ Cancel

Figure 3.30 – Select User from User Search Result

10. Select “Save” on the “Create Role” window to create the Role

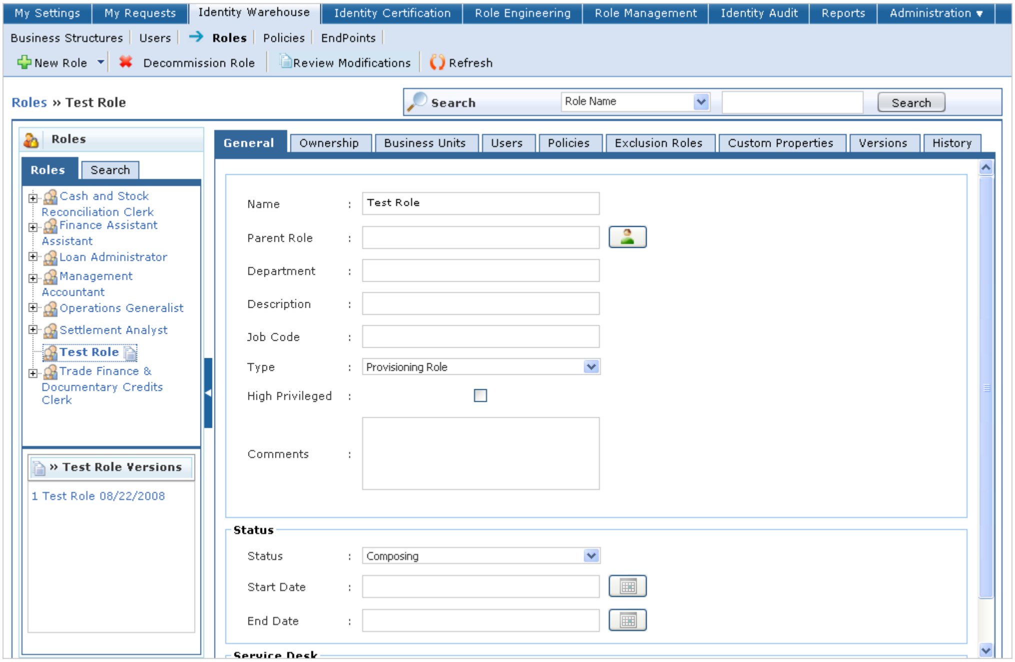


Name : Test Role

Global User : rReagan

Figure 3.31 – Create Role from Global User – Click “Save”

11. The Role will now be available in the Roles view under Identity Warehouse



1 Test Role 08/22/2008

Name : Test Role

Parent Role :

Department :

Description :

Job Code :

Type : Provisioning Role

High Privileged : ☐

Comments :

Status

Status : Composing

Start Date :

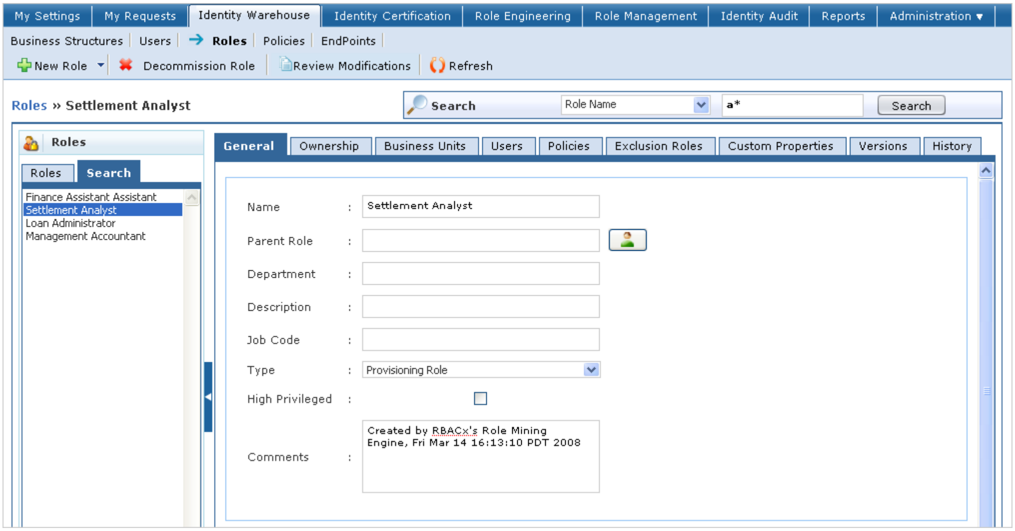
End Date :

Figure 3.32 – Create Role from Global User – Created Role

Role Search

▼ Steps to Search for a Role

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialogue box appears. Enter your credentials and login to Sun Role Manager
3. Select the Role view by selecting it from the Identity Warehouse Tab
4. To use quick search select a field from the drop down box. All the commonly populated fields are available to search on
5. Enter a value to search for. Wildcards are accepted (e.g a* , *xyz*)
6. To search on the selected field for the entered value click “Search”
7. Results are displayed on the “Roles” panel on the left under the Tab “Search”. Double click on a role to select it



Search: Role Name a* Search

Finance Assistant Assistant
Settlement Analyst
Loan Administrator
Management Accountant

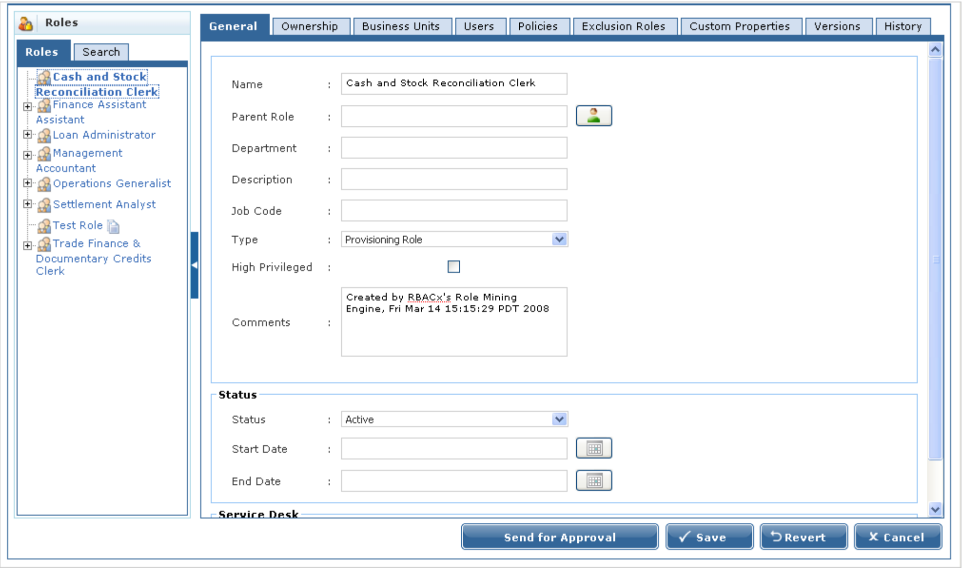
Name : Settlement Analyst
Parent Role :
Department :
Description :
Job Code :
Type : Provisioning Role
High Privileged : □
Comments : Created by RBACx's Role Mining Engine, Fri Mar 14 16:13:10 PDT 2008

Figure 3.33 – Role Search

Manage Roles (Rename/Modify/Decommission)

▼ Steps to manage roles

1. Start Role Manager by clicking on the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select Roles view under the Identity Warehouse Tab
4. Search for a Role using the Role Search or select a role from the Roles panel on the left
5. To rename a Role navigate to the General Tab. Fill the in the desired role name in the Name field and click “Save”
6. To modify a Role by changing properties like Description, Type etc modify these values and click “Save”



Name : Cash and Stock Reconciliation Clerk

Parent Role :

Department :

Description :

Job Code :

Type : Provisioning Role

High Privileged : □

Comments : Created by RBACx's Role Mining Engine, Fri Mar 14 15:15:29 PDT 2008

Status

Status : Active

Start Date :

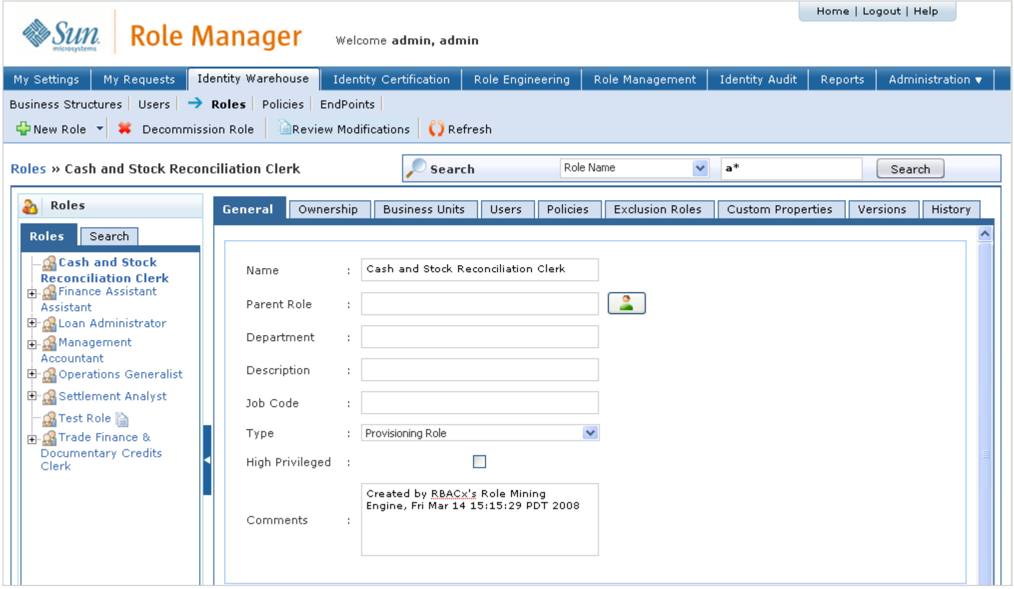
End Date :

Service Desk

Figure 3.34 – Role Details

7. To de-commission a Role use the “Decommission Role” button. Decommissioning a role leads to the removal of all role-user associations. The Role itself however is made inactive and stored in Role Manager. The role cannot be made active again. It

cannot be modified in any way or assigned to the user.


Sun microsystems
Role Manager
Welcome admin, admin
Home | Logout | Help
My Settings | My Requests | Identity Warehouse | Identity Certification | Role Engineering | Role Management | Identity Audit | Reports | Administration ▾
Business Structures | Users | Roles | Policies | EndPoints
New Role | Decommission Role | Review Modifications | Refresh
Roles » Cash and Stock Reconciliation Clerk
Search | Role Name | a* | Search
Roles
Roles | Search
Cash and Stock Reconciliation Clerk
Finance Assistant Assistant
Loan Administrator
Management Accountant
Operations Generalist
Settlement Analyst
Test Role
Trade Finance & Documentary Credits Clerk
General | Ownership | Business Units | Users | Policies | Exclusion Roles | Custom Properties | Versions | History

Name : Cash and Stock Reconciliation Clerk

Parent Role :

Department :

Description :

Job Code :

Type : Provisioning Role

High Privileged : ☐

Comments : Created by RBACx's Role Mining Engine, Fri Mar 14 15:15:29 PDT 2008

Figure 3.35 – Role Decommission

Role Hierarchy

Similar to Business Unit hierarchy, an n-level Role Hierarchy can be defined in Role Manager. A role can have various roles under it as 'Child Roles'. The Role Hierarchy is defined when a new Role is added. When a child role is added to a user, the parent role automatically is assigned to the user. Role Hierarchy defines an organized structure of roles. Roles defined in an organization may have a hierarchy associated with them and also Enterprise Level Role and Application Level Role might be defined. Role Hierarchy will help address these points.

▼ Steps to Create Role Hierarchy

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Role View by selecting it from the Identity Warehouse Tab

4. The Role Hierarchy is defined when a new Role is created manually.

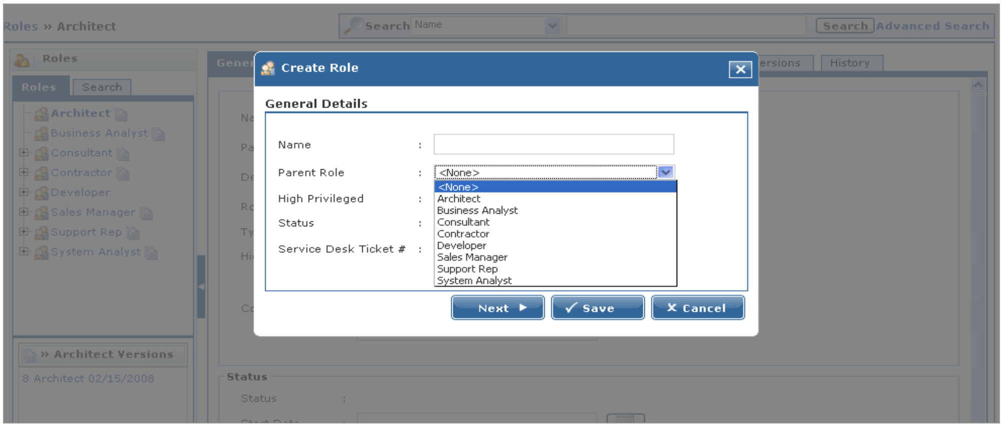


Figure 3.36 –Role Hierarchy

5. To change a role hierarchy, select the role and click the button located near the Parent Role label in the ‘General’ tab. From the list of roles that come up, select the parent for the role under consideration.

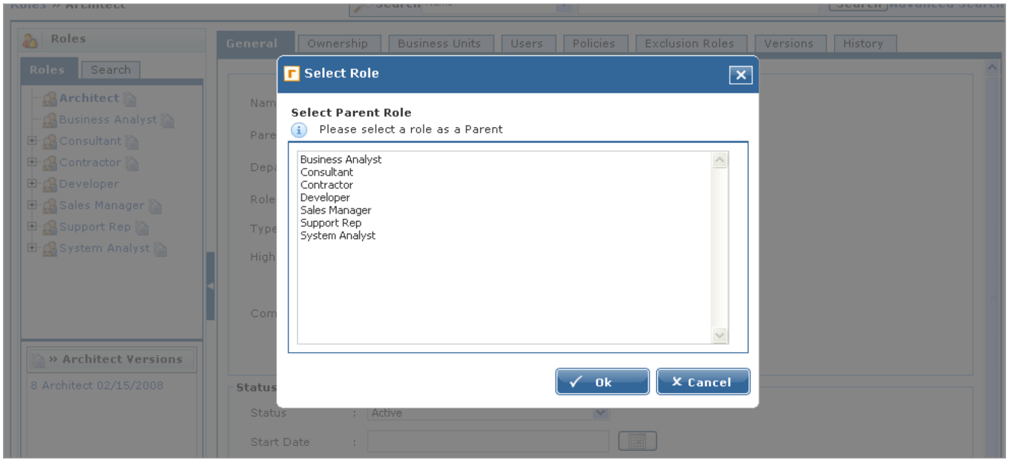

Please select a role as a Parent

Figure 3.37 – Select Parent Role

6. To Select the Child Role for a User. Go to the user view and select the user you need to assign role. Click Role Tab under user Tab and click Add Role(s) Button

7. The parent Role is automatically assigned to the user

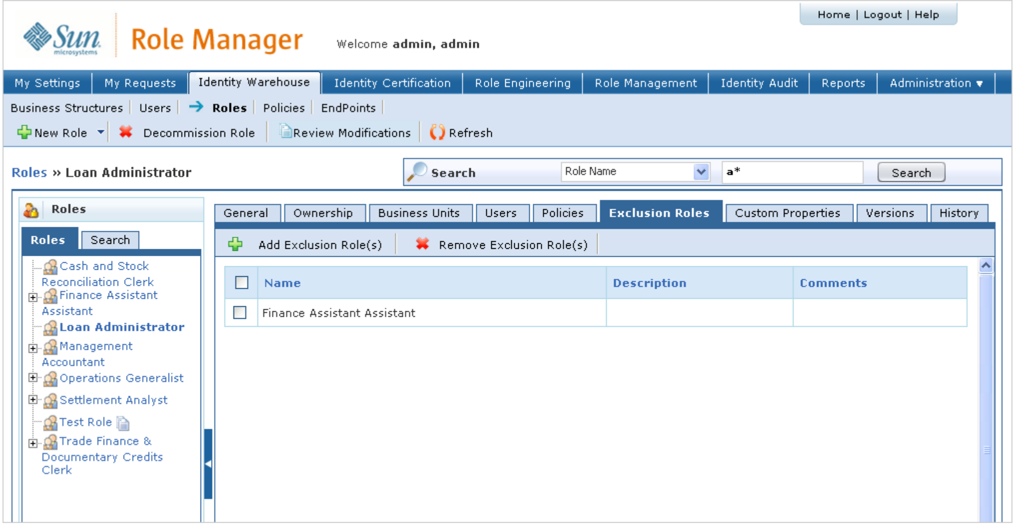
8. When the parent role is removed the child role is automatically removed from the user

Setting Segregation of Duties at Role and Policy Level

Segregation of Duties (SoD) are defined for separation of the management or execution of certain duties or of areas of responsibility is required in order to prevent and reduce opportunities for unauthorized modification or misuse of data or service. Segregation of duties is a primary internal control intended to prevent, or decrease the risk of, errors or irregularities; identify problems; and ensure that corrective action is taken. This is done by assuring that no single individual should have control over all phases of a transaction. Role Manager performs this SOD at the Role and Policy Level.

▼ Steps to Define Segregation of Duties

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Role View by selecting it from the Identity Warehouse Tab
4. Click a Role and browse to the Exclusion Roles tab
5. Add the Roles which need to be excluded from the one selected.



Roles » Loan Administrator

Search: Role Name ▾ a* [Search]

☐	Name	Description	Comments
☐	Finance Assistant Assistant		

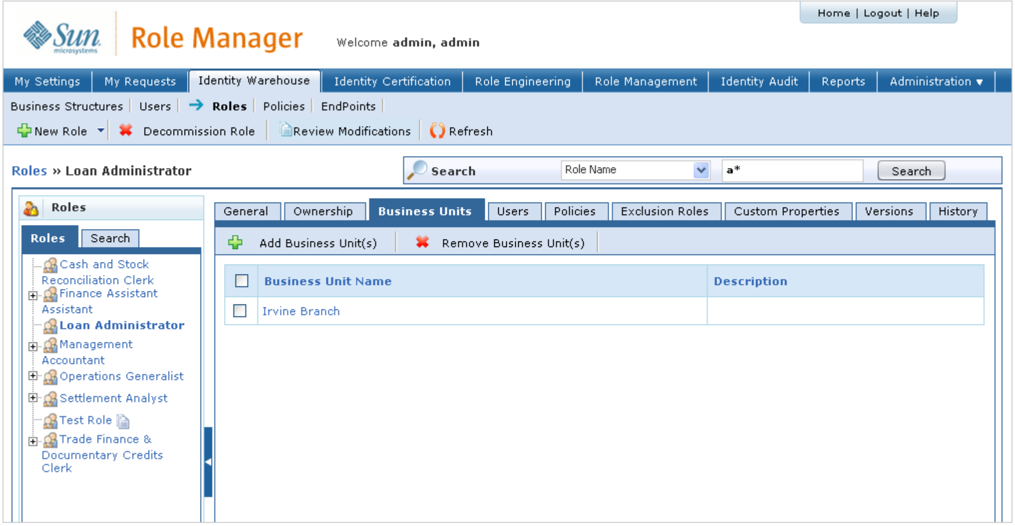
Figure 3.38- Business Unit Users

6. Similar to Roles, Segregation of Duties can be defined at the Policy level as well. Go to the Policy View from the View Menu.
7. Select a Policy by double clicking it and go to the Exclusion Policies tab
8. Add the policies which are to be excluded from the one selected
9. Similar to the Role, when a Policy is added to a Role, the excluded policies cannot be assigned to a Role

Associate Role to Business Unit

▼ Steps to associate role to business unit(s)

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Role View by selecting it from the Identity Warehouse Tab
4. Click a Role and browse to the Business Unit Tab
5. Click ✚ Add Business Unit(s) and select the desired Business Units. Click ✓ Save



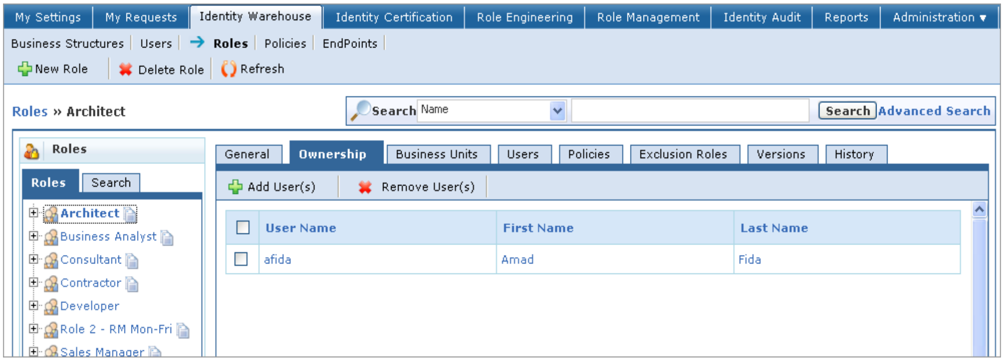
□	Business Unit Name	Description
□	Irvine Branch	

Figure 3.39 – Add Role to Business Unit

Associate Role Owners to Role

▼ Steps to associate role owners to roles

1. Start Role Manager by clicking the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Role View by selecting it from the Identity Warehouse Tab
4. Click a Role and browse to the Ownership Tab
5. Click Add Owners and select the desired User(s). Click ✓ Save



□	User Name	First Name	Last Name
□	afida	Amad	Fida

Figure 3.40 – Add Role Owner to Role

4

◆ ◆ ◆ CHAPTER 4

Role Engineering

The Role Engineering module in Role Manager delivers sophisticated role mining, identity correlation, and risk management functionalities. Robust 'identity correlation reengineering' capabilities offer an innovative approach towards traditional role engineering techniques. Role Manager defines Role Engineering in three process steps, which are as follows:

1. **Role Discovery** – describes the process of discovering relationships between users based on similar access permissions that can logically be grouped to form a role
2. **Role Entitlement Discovery** – describes the process of mining role content or discovering the content of these roles by analyzing and finding correlations in user access patterns in applications across the Enterprise
3. **Rules Discovery** – describes the process of discovering rules that can be used to govern assigning mined roles to new users, a powerful graphical feature that is embedded with the role mining process

Sun's Role Engineering methodology supports the top down, bottom up, and recommended hybrid approaches. A hybrid approach is one that accounts for a users job function and HR attributes such as manager or geographical location along with account permissions (entitlements) when mining for roles.

The Role Manager Role Mining feature uses Expectation Maximization and Cob Web Clustering algorithms for role discovery and J48 and C45 Decision Tree Classification Algorithms for Rule Discovery. Role Mining supports minable attributes which are can be set in the attributes configuration screen as described below. This gives the role engineer flexibility to include only relevant applications and relevant attributes for best data mining results. Irrelevant attributes can thus be discarded from the role mining exercise.

Role Discovery

Sun Role Manager performs role discovery by allowing users to create and run role mining tasks. All role mining tasks are stored by Sun Role Manager. This enables users to create tasks at one instant and then run or schedule tasks to be run at any later instant. Sun Role Manager provides a sophisticated scheduling mechanism which makes it easy to run periodic as well as one time tasks. Results of tasks that are completed are stored. This enables users to run a task at one instant and review results to configure and save roles at any later instant. A role mining task can be run any number of times. The results obtained by different instances of a task are stored and time-stamped. These capabilities allow flexibility in dealing with role mining tasks. Tasks can be executed on demand or scheduled for a future time. Users can view the list of role mining tasks and retrieve results for completed tasks. Tasks and results are permanently stored in Sun Role Manager unless they are explicitly deleted.

The Role Discovery process consists of 3 discrete steps

1. Set Minable Attributes
2. Create/Run a role mining task
3. Analyze role mining results and configure and save Roles

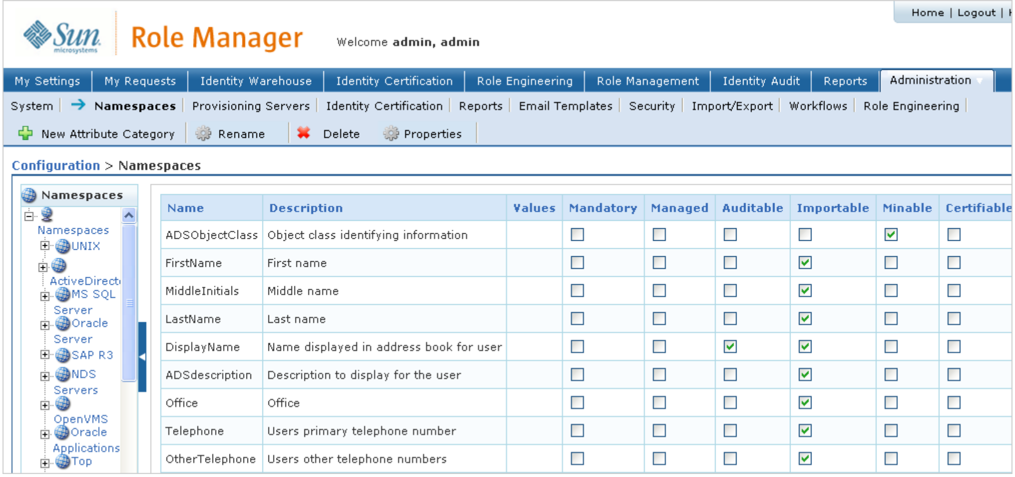
Set Minable Attributes

Minable attribute settings should be checked before a Role Mining effort is initiated to ensure that the appropriate applications and input data are accounted for while the algorithm is running. This can also be checked by previewing input data as shown in the next demonstration. Role mining run without any attributes set as minable will throw an error. It is also important to determine attributes that are critical in terms of defining access to a particular application/target system and set them as mineable as adding attributes that are not important will affect the accuracy of the role mining effort.

▼ Steps to set minable attributes before role mining

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialogue box appears. Enter your credentials and login to Sun Role Manager
3. Open attributes configuration screen under Administration->Configuration->Namespaces
4. Select the namespace whose attributes are to be selected or deselected for role mining by clicking on the namespace in the Namespaces panel on the left

5. Select (or deselect) attributes for mining by checking (or unchecking) the checkbox under Minable field for an attribute, keeping in mind that for best results only relevant attributes at the lowest level3 should be selected



Name	Description	Values	Mandatory	Managed	Auditable	Importable	Minable	Certifiable
ADSObjectClass	Object class identifying information		□	□	□	□	☑	□
FirstName	First name		□	□	□	☑	□	□
MiddleInitials	Middle name		□	□	□	☑	□	□
LastName	Last name		□	□	□	☑	□	□
DisplayName	Name displayed in address book for user		□	□	☑	☑	□	□
ADSdescription	Description to display for the user		□	□	□	☑	□	□
Office	Office		□	□	□	☑	□	□
Telephone	Users primary telephone number		□	□	□	☑	□	□
OtherTelephone	Users other telephone numbers		□	□	□	☑	□	□

Figure 4.1 – Set Minable Attributes

Create/Run a Role Mining Task

Sun Role Manager allows users to create role mining tasks and then run them on demand or schedule them for a later instant. During the Role Mining Task creation process attention must be paid to selecting users for role mining, setting role mining parameters and previewing mining data.

The key to good role engineering effort is selecting the best set of representative users for Role Mining. For most concrete roles results, Sun Role Manager's methodology suggests selecting a group of users whose job responsibilities lie closest together. Sun Role Manager Role Mining will then suggest roles based on their collective entitlements. For this purpose Sun Role Manager allows you to select a set of users based on a logical grouping by Business Unit, by Existing Role, by End Point or individually from a list of all Global Users.

Role mining parameters give the user more control over the Role Mining process. A number of parameters can be set to tune the role mining process. Refer to the table below for more information on Role Mining parameters.

Max. Number of Iterations to Run	Number of times the Role Mining algorithm will run. Keep this number between 100 and 200. Increase to a higher number only if the number of users

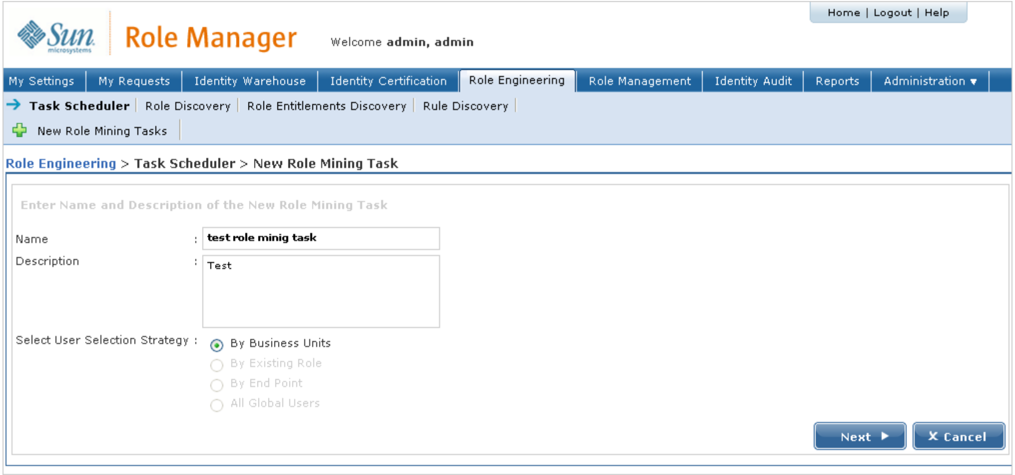
	selected exceeds 200
Stop when found this number of Roles	Criteria to Stop the Algorithm
Min. Standard Deviation	Number of Breath strokes for the Role Mining Algorithm to capture user detail. Use values between – (0, 1, 2) and + (0, 1, 2). A greater number will give more outliners in role.
Single instance per user	Keep this always checked to select a single instance per user
Resample data %	Best threshold value is 300%
User Properties	A list of attributes which include a user criteria's in the search algorithm. Using these parameters along with logical grouping of users by job responsibility can give best results for a hybrid role mining effort.
Rules Parameters	These values are for statistical purposes only and we recommend not changing them
Sub-tree Raising	Check this to cut off users that are in the lowest tree

A good practice before running a Role Mining task is to preview the input data selected for the Role Mining exercise. We do this to ensure that all and only correct attributes are accounted for and check for any visible inconsistencies in data.

▼ Steps to Create and Run/Schedule a Role Mining Task

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialogue box appears. Enter your credentials and login to Sun Role Manager
3. Select the Role Engineering Tab
4. Select the New Role Mining Tasks Tab
5. In the New Role Mining Task Window enter values for Name and Description Fields. Select the

User Selection Strategy from By Business Units, By Existing Role, By Endpoint or All Global Users. Select “Next”.



Enter Name and Description of the New Role Mining Task

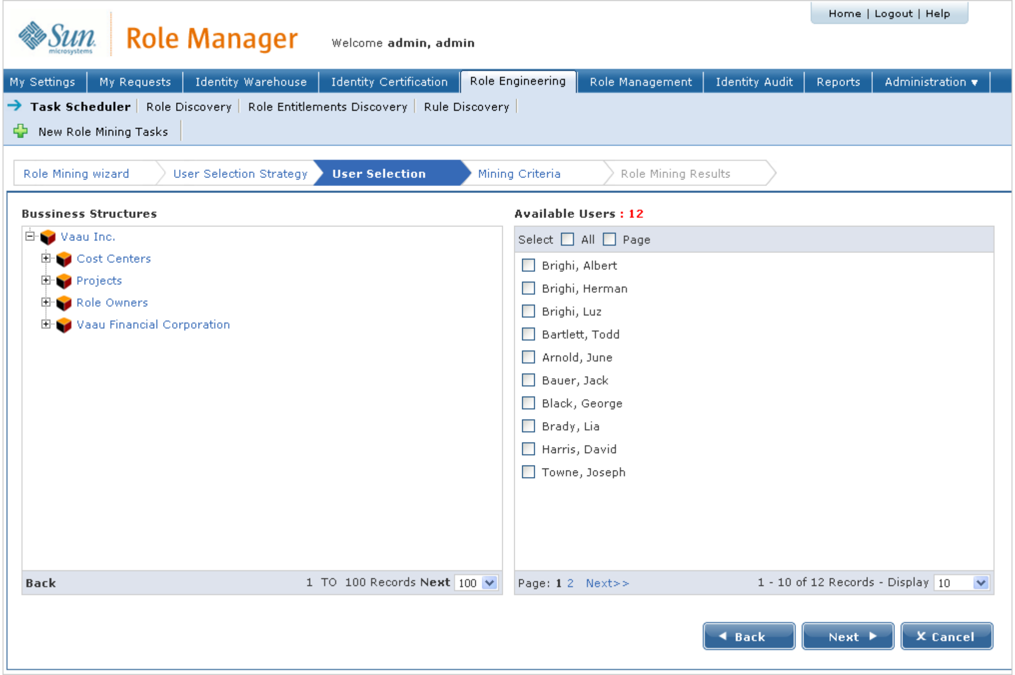
Name : test role minig task

Description : Test

Select User Selection Strategy :
● By Business Units
○ By Existing Role
○ By End Point
○ All Global Users

Figure 4.2 – New Role Mining Task

6. In this demonstration we select user selection strategy as “By Business Unit”. Follow corresponding steps for the other three options. Select the business unit from the “Available Business Units” panel on the left. All the Users corresponding to the Business Unit will be displayed on the “Available Users” panel on the right



Bussiness Structures

- Vaau Inc.
  - Cost Centers
  - Projects
  - Role Owners
  - Vaau Financial Corporation

Back 1 TO 100 Records Next 100

Available Users : 12

Select □ All □ Page

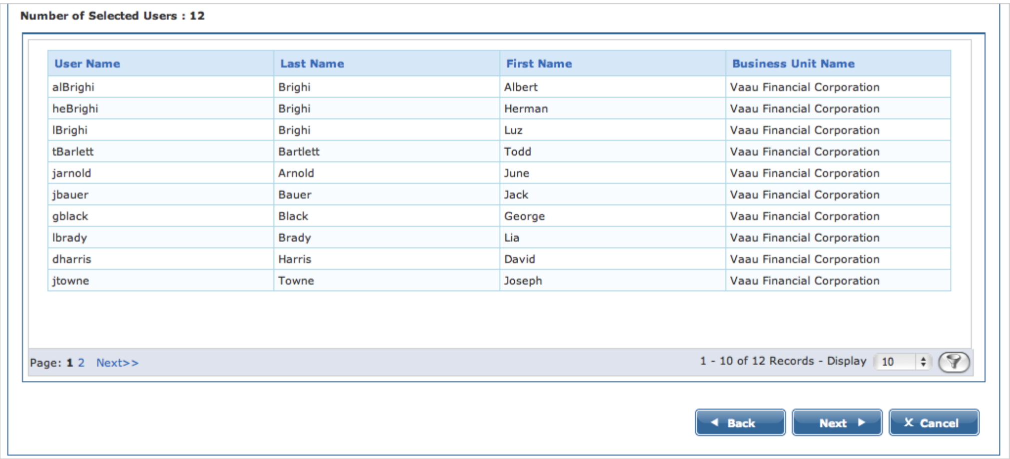
□ Brighi, Albert
□ Brighi, Herman
□ Brighi, Luz
□ Bartlett, Todd
□ Arnold, June
□ Bauer, Jack
□ Black, George
□ Brady, Lia
□ Harris, David
□ Towne, Joseph

Page: 1 2 Next>> 1 - 10 of 12 Records - Display 10

Figure 4.3 – Select Users by Business Units

7. Use the “All” and “Page” checkboxes to select users. All selects all the users in the “Available Users” panel. “Page” selects all the users being displayed on the current page. Use the drop down box next to “Display” to change the number of users displayed on one page. Use page numbers or “Next” button in the “Available Users” panel to scroll the pages. Individual checkboxes as well as the “All” and “Page” checkboxes can be used to select/deselect users to get the desired representative set of users for the role mining exercise.

8. As users are selected a new panel opens up at the bottom of the same page that dynamically displays the chosen set of users. This panel can be used to review the users selected.



Number of Selected Users : 12

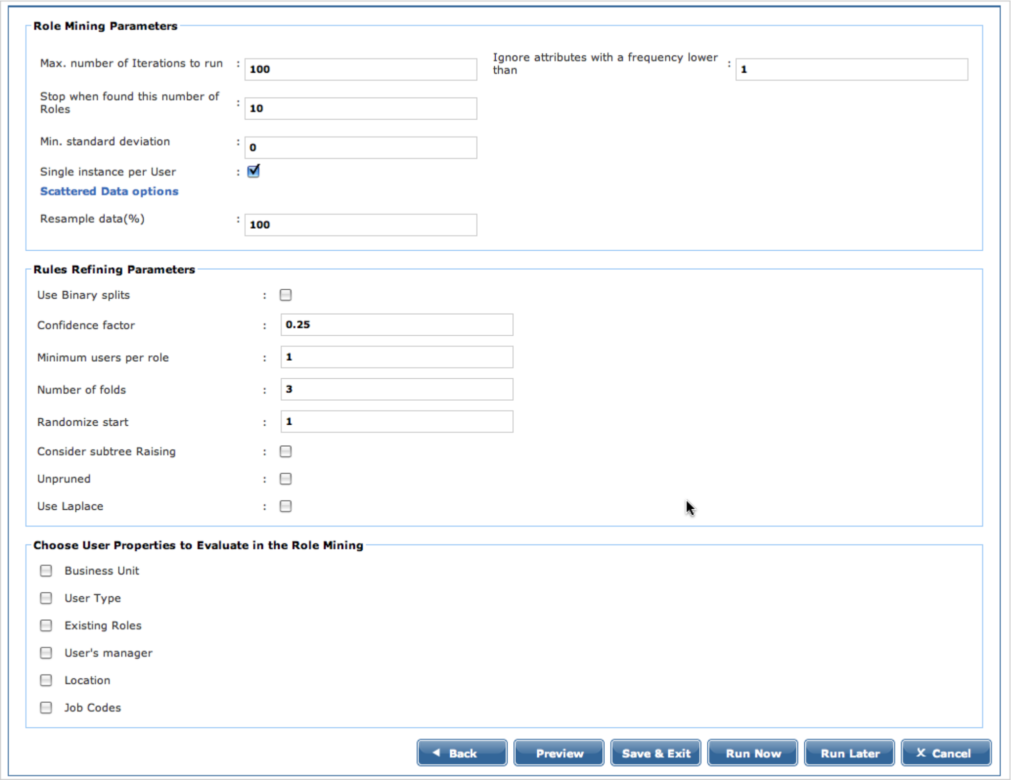
User Name	Last Name	First Name	Business Unit Name
alBrighi	Brighi	Albert	Vaau Financial Corporation
heBrighi	Brighi	Herman	Vaau Financial Corporation
lBrighi	Brighi	Luz	Vaau Financial Corporation
tBarlett	Bartlett	Todd	Vaau Financial Corporation
jarnold	Arnold	June	Vaau Financial Corporation
jbauer	Bauer	Jack	Vaau Financial Corporation
gblack	Black	George	Vaau Financial Corporation
lbrady	Brady	Lia	Vaau Financial Corporation
dharris	Harris	David	Vaau Financial Corporation
jtowne	Towne	Joseph	Vaau Financial Corporation

Page: 1 2 Next>>

1 - 10 of 12 Records - Display 10

Figure 4.4 – Selected Users View

9. Select “Next” when the user set desired for the role mining task have been selected



Role Mining Parameters

Max. number of Iterations to run : 100

Ignore attributes with a frequency lower than : 1

Stop when found this number of Roles : 10

Min. standard deviation : 0

Single instance per User : ☑

Scattered Data options

Resample data(%) : 100

Rules Refining Parameters

Use Binary splits : □

Confidence factor : 0.25

Minimum users per role : 1

Number of folds : 3

Randomize start : 1

Consider subtree Raising : □

Unpruned : □

Use Laplace : □

Choose User Properties to Evaluate in the Role Mining

□ Business Unit

□ User Type

□ Existing Roles

□ User's manager

□ Location

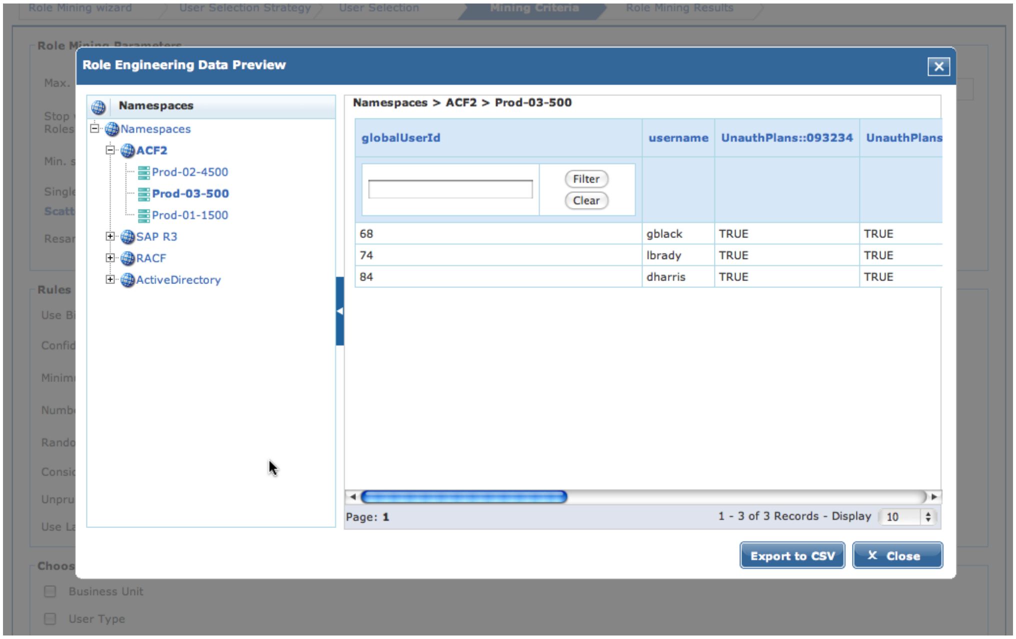
□ Job Codes

Figure 4.5 – Role Mining Parameters

10. Select parameters for the Role Mining task to better control the effort. Refer to the Role Mining Parameters table earlier in the section for more description of various parameters

11. To preview and analyze Role Mining Input Data select “Preview”

12. A Role Engineering Data Preview window opens up. Select individual Namespaces or Endpoints from the “Namespaces” panel on the left to view the data associated with them. To click the data associated with the entire user set selected select “Namespaces”. Use the “Filter” feature to filter users by GlobalUserId. Use “Clear” to clear the filtering. Select “Export to CSV” to get the Role Mining Input Data in the form of a CSV file



Namespaces > ACF2 > Prod-03-500

globalUserId	username	UnauthPlans::093234	UnauthPlans
68	gblack	TRUE	TRUE
74	lbrady	TRUE	TRUE
84	dharris	TRUE	TRUE

Page: 1 — 1 - 3 of 3 Records - Display 10

Figure 4.6 – Role Engineering Data Preview

13. By quick review of columns on this screen you can

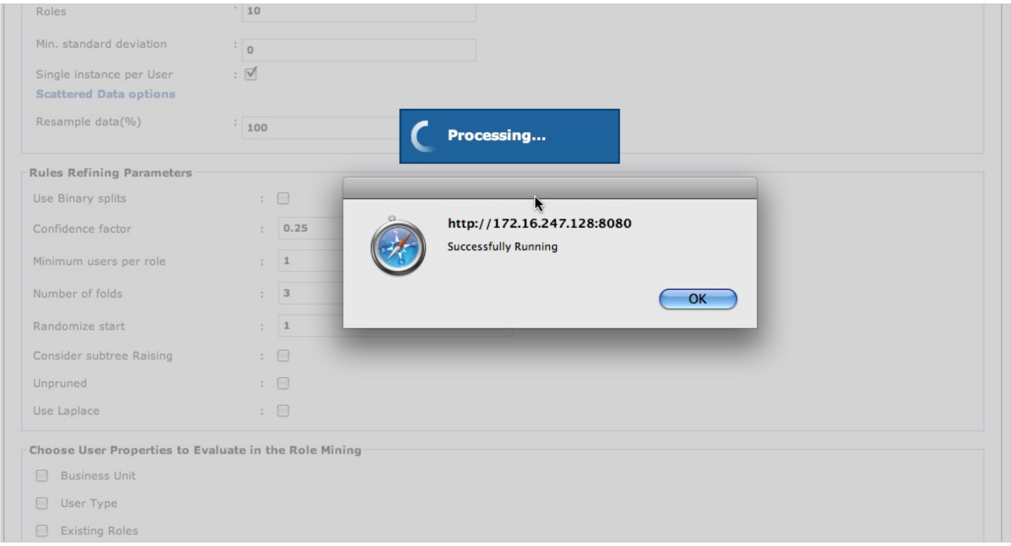
    a. Check the minable attributes that are accounted for in this run

    b. Reference minable attributes with respect to your set of representative users

    c. Check that multi-valued attributes show in separate columns. If not then check the attribute as multi-valued as defined in the attributes configuration screen

14. Click “Close” to return to the previous screen (Role Mining Configuration Screen)

15. Select “Run Now” to execute the Role Mining task now. A “Successfully Running” window pops up



Roles : 10

Min. standard deviation : 0

Single instance per User : ☑

Scattered Data options

Resample data(%) : 100

Processing...

Rules Refining Parameters

Use Binary splits : □

Confidence factor : 0.25

Minimum users per role : 1

Number of folds : 3

Randomize start : 1

Consider subtree Raising : □

Unpruned : □

Use Laplace : □

http://172.16.247.128:8080

Successfully Running

OK

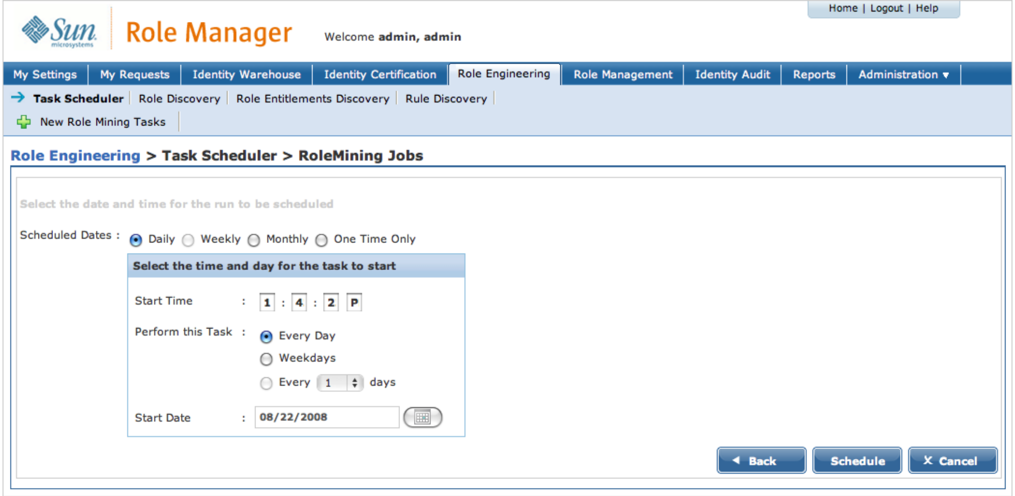
Choose User Properties to Evaluate in the Role Mining

□ Business Unit

□ User Type

□ Existing Roles

Figure 4.7 – Role Mining Task Successfully Running



Home | Logout | Help
Sun microsystems
Role Manager
Welcome admin, admin
My Settings | My Requests | Identity Warehouse | Identity Certification | Role Engineering | Role Management | Identity Audit | Reports | Administration ▾
Task Scheduler | Role Discovery | Role Entitlements Discovery | Rule Discovery
New Role Mining Tasks

Role Engineering > Task Scheduler > RoleMining Jobs

Select the date and time for the run to be scheduled

Scheduled Dates : ● Daily ○ Weekly ○ Monthly ○ One Time Only

Select the time and day for the task to start

Start Time : 1 : 4 : 2 P

Perform this Task : ● Every Day

○ Weekdays

○ Every 1 days

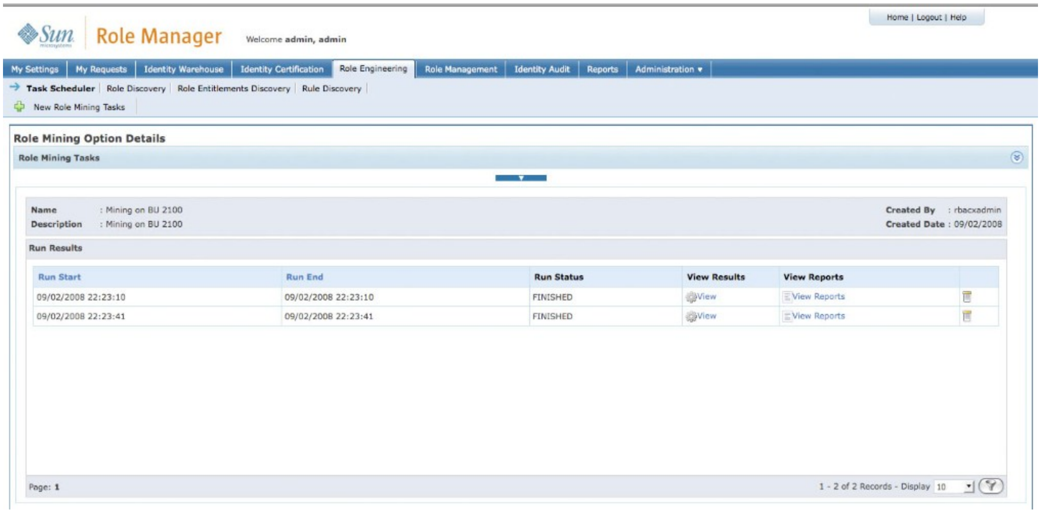
Start Date : 08/22/2008

Figure 4.8 – Role Mining Task Scheduler

16. Select “Run Later” to schedule the task. Scheduler window opens up. Select a daily, weekly, monthly or one-time only task by selecting the corresponding radio button. Depending on this selection further select values to setup the task. Select “Schedule” to schedule the task

17. To save the task and run/schedule the task at a later time select “Save and Exit”

18. To run/schedule a saved task go to the main Role Mining Task window by selecting Role Engineering =>Task Scheduler and use the “Run” or “Schedule” buttons for the saved task



Role Mining Option Details

Role Mining Tasks

Name : Mining on BU 2100
Description : Mining on BU 2100
Created By : rbacxadmin
Created Date : 09/02/2008

Run Results

Run Start	Run End	Run Status	View Results	View Reports
09/02/2008 22:23:10	09/02/2008 22:23:10	FINISHED	View	View Reports
09/02/2008 22:23:41	09/02/2008 22:23:41	FINISHED	View	View Reports

Page: 1

1 - 2 of 2 Records - Display 10

Figure 4.9 – Role Mining Tasks View

Analyze, Configure and Save Role Mining Results

Validate Role Mining Results

To better understand the role mining results and how well the Role Mining algorithm performed, the following Statistics and Rules Matrix can be examined.

The Result screen shows us the following statistics to interpret Role Mining results:

% of Users correctly/ incorrectly assigned	The Mining statistics tell us that the Algorithm delivered an acceptable result with 100% accuracy the Users have been

	assigned correctly and 0 % of the Users have been assigned incorrectly, which is very satisfactory.
Kappa Value	The Kappa value of 1.0 should be understood as “The higher the value of Kappa, the stronger the agreement”. Depending on the application, Kappa less than 0.7 indicates that your measurement system needs improvement. Kappa values greater than 0.9 are considered excellent.
Kononenko & Bratko Relative score	A score for the data mining algorithm, not to be used for interpretation of these results

Configure and Save Roles

Sun Role Manager Role Mining identifies users with nearly identical access entitlements and shows the role content (entitlements and associated endpoints) for analysis in the role configuration screen. Role engineers can decide to assign all or a partial list of these entitlements to the role based on a level of accepted risk.

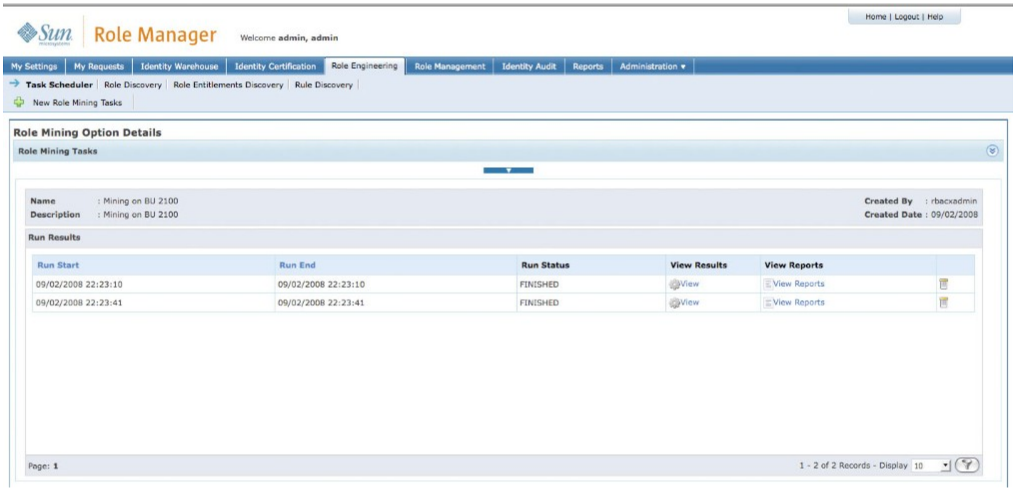
If the need is to match users with exact entitlements only, then a set cutoff percentage of 100% will save entitlements only where one hundred percent of users in that role have that access entitlement. An accepted risk of selecting any percentage below 100% allows Sun Role Manager to save all entitlements above the set cutoff to the role as a primary or parent role policy and those entitlements below the set cutoff as a secondary policy or child role. The end user can then later decide if they wish to maintain the child role policy for a transitional period of time or remove access altogether.

▼ Steps to Validate Role Mining Results and Configure Role(s) to be saved

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialogue box appears. Enter your credentials and login to Sun Role Manager

3. Select the Role Engineering Tab

4. Select the Task Scheduler Tab. This gives a list of all the saved and completed tasks



Role Mining Option Details

Role Mining Tasks

Name : Mining on BU 2100
Description : Mining on BU 2100

Created By : rbacxadmin
Created Date : 09/02/2008

Run Results

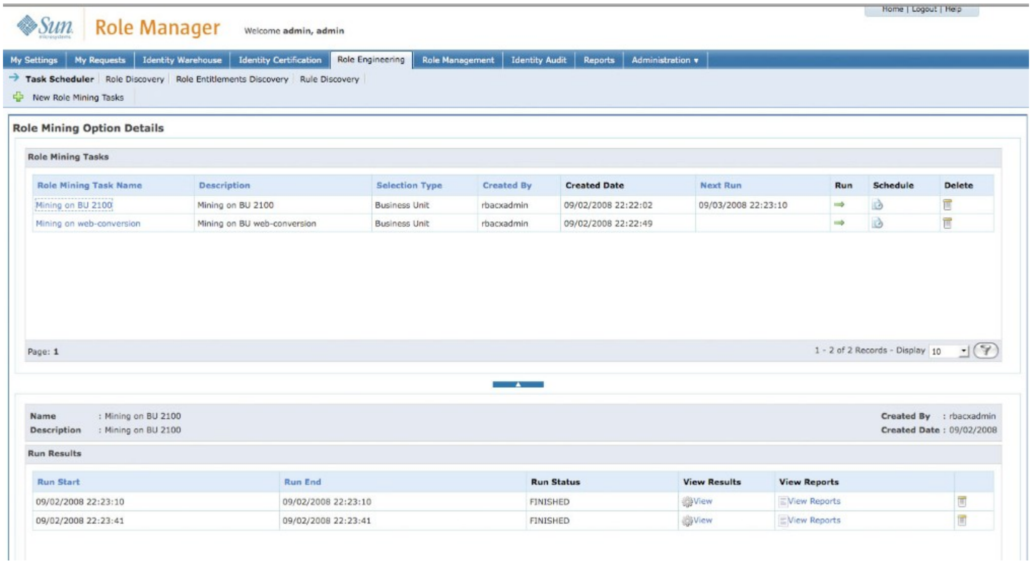
Run Start	Run End	Run Status	View Results	View Reports	
09/02/2008 22:23:10	09/02/2008 22:23:10	FINISHED	View	View Reports	
09/02/2008 22:23:41	09/02/2008 22:23:41	FINISHED	View	View Reports	

Page: 1

1 - 2 of 2 Records - Display 10

Figure 4.10 – Role Mining Tasks View

5. Select the task whose result is to be viewed by clicking on the task name. A new panel opens up at the bottom of the same page which contains results for all the instances that this task has been run



Welcome **admin, admin**

Role Mining Option Details

Role Mining Tasks

Role Mining Task Name	Description	Selection Type	Created By	Created Date	Next Run	Run	Schedule	Delete
Mining on BU 2100	Mining on BU 2100	Business Unit	rbacxadmin	09/02/2008 22:22:02	09/03/2008 22:23:10	➡		
Mining on web-conversion	Mining on BU web-conversion	Business Unit	rbacxadmin	09/02/2008 22:22:49		➡		

Page: **1**

1 - 2 of 2 Records - Display 10

Name : Mining on BU 2100
Description : Mining on BU 2100

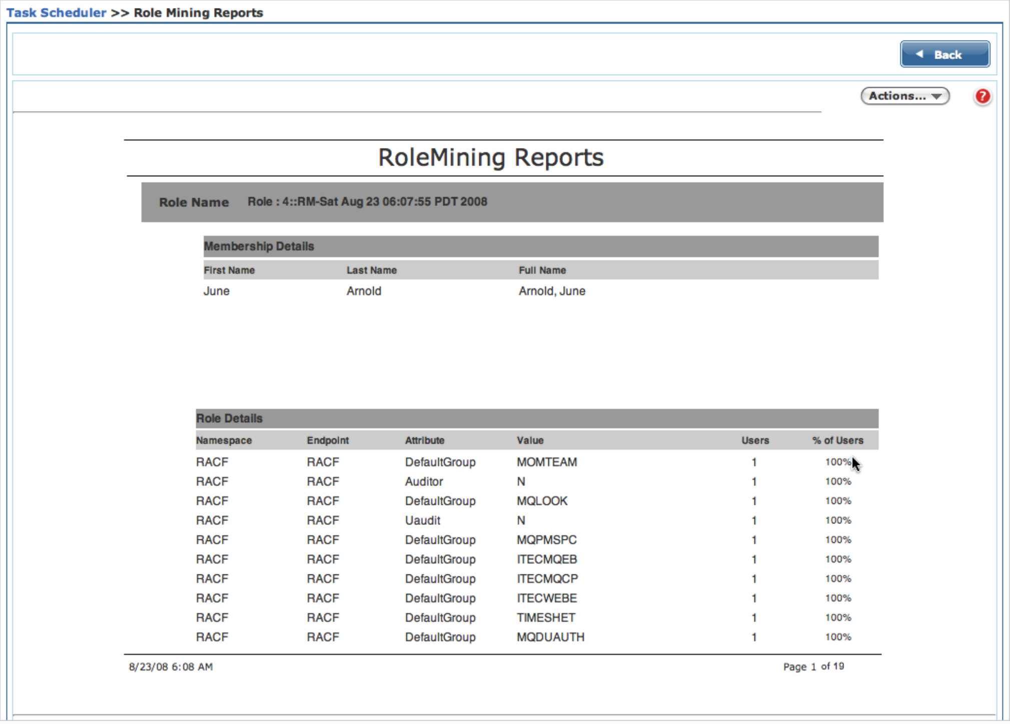
Created By : rbacxadmin
Created Date : 09/02/2008

Run Results

Run Start	Run End	Run Status	View Results	View Reports	
09/02/2008 22:23:10	09/02/2008 22:23:10	FINISHED	View	View Reports	
09/02/2008 22:23:41	09/02/2008 22:23:41	FINISHED	View	View Reports	

Figure 4.11 – Role Mining Task Results

6. Select “View Reports” under “View Reports” for the instance whose Role Mining Report is to be viewed



RoleMining Reports

Role Name Role : 4::RM-Sat Aug 23 06:07:55 PDT 2008

Membership Details

First Name	Last Name	Full Name
June	Arnold	Arnold, June

Role Details

Namespace	Endpoint	Attribute	Value	Users	% of Users
RACF	RACF	DefaultGroup	MOMTEAM	1	100%
RACF	RACF	Auditor	N	1	100%
RACF	RACF	DefaultGroup	MQLOOK	1	100%
RACF	RACF	Uaudit	N	1	100%
RACF	RACF	DefaultGroup	MQPMSPC	1	100%
RACF	RACF	DefaultGroup	ITECMQEB	1	100%
RACF	RACF	DefaultGroup	ITECMQCP	1	100%
RACF	RACF	DefaultGroup	ITECWEBE	1	100%
RACF	RACF	DefaultGroup	TIMESHET	1	100%
RACF	RACF	DefaultGroup	MQDUAUTH	1	100%

8/23/08 6:08 AM

Page 1 of 19

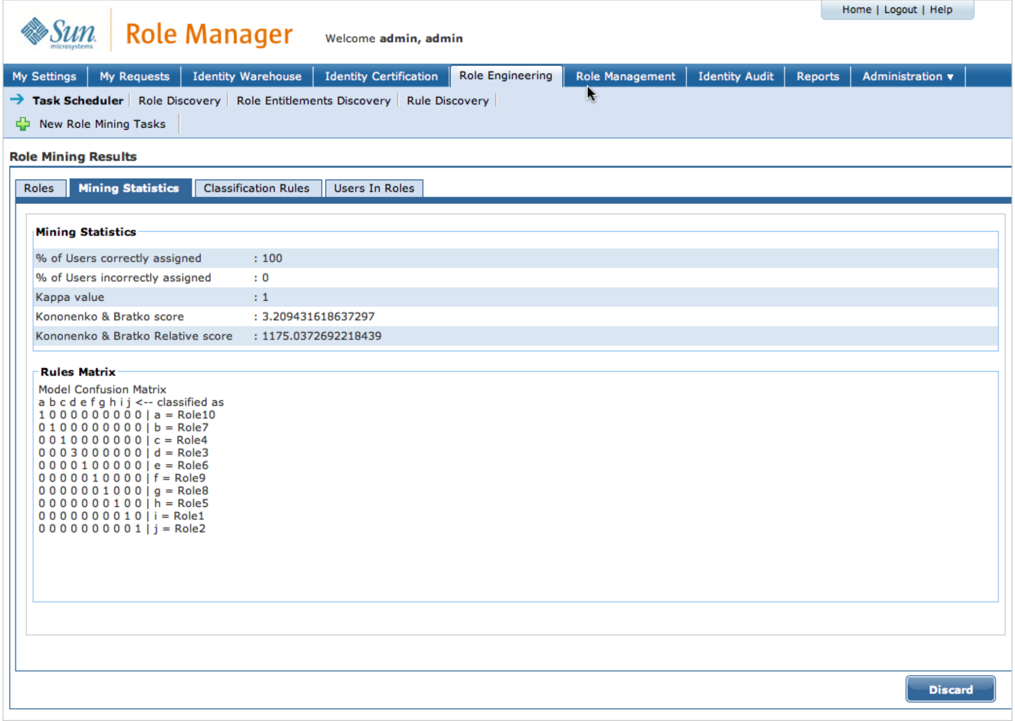
Figure 4.12 – Role Mining Reports

7. Role Mining Report for the role mining effort gives the membership details and details regarding all the attributes and values across all endpoints and namespaces for all the roles created in the Role Mining effort

8. The report can be exported to a format of choice by using the “Actions…” button. Use the “Back” button to go back to the task results page

9. Select “View” under “View Results” for the instance whose result is to be viewed. This opens the Role Mining Results page

10. Select Mining Statistics Tab to view the statistics used to validate the result of the Role Mining effort



Mining Statistics

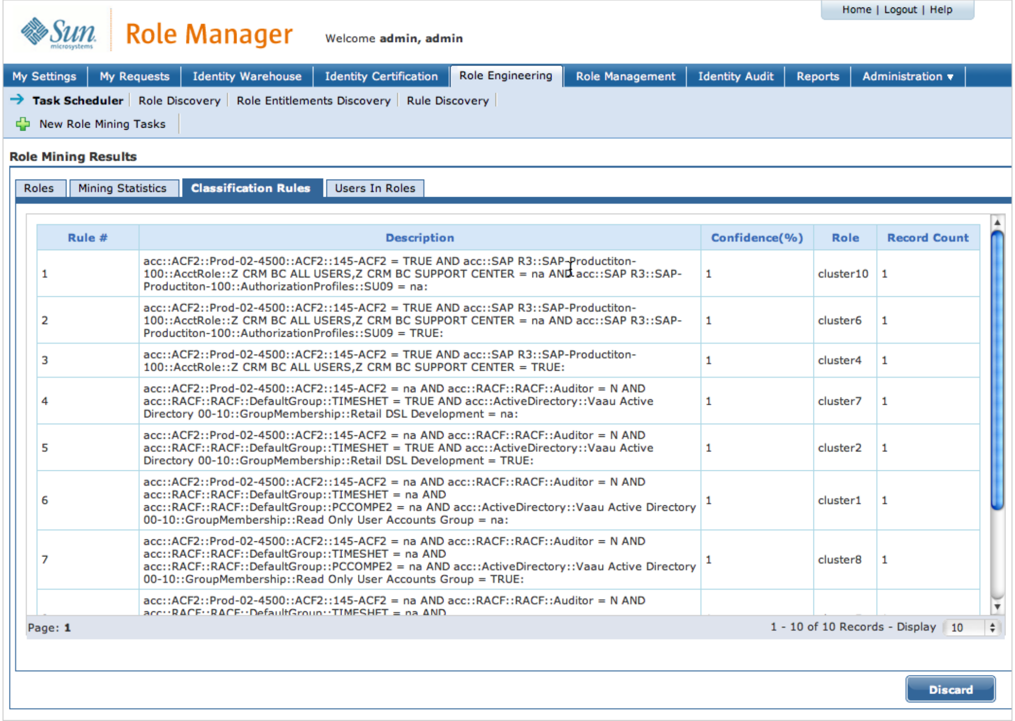
% of Users correctly assigned	: 100
% of Users incorrectly assigned	: 0
Kappa value	: 1
Kononenko & Bratko score	: 3.209431618637297
Kononenko & Bratko Relative score	: 1175.0372692218439

Rules Matrix

```
Model Confusion Matrix
a b c d e f g h i j <-- classified as
1 0 0 0 0 0 0 0 0 0 | a = Role10
0 1 0 0 0 0 0 0 0 0 | b = Role7
0 0 1 0 0 0 0 0 0 0 | c = Role4
0 0 0 3 0 0 0 0 0 0 | d = Role3
0 0 0 0 1 0 0 0 0 0 | e = Role6
0 0 0 0 0 1 0 0 0 0 | f = Role9
0 0 0 0 0 0 1 0 0 0 | g = Role8
0 0 0 0 0 0 0 1 0 0 | h = Role5
0 0 0 0 0 0 0 0 1 0 | i = Role1
0 0 0 0 0 0 0 0 0 1 | j = Role2
```

Figure 4.13 – Role Mining Results - Statistics

11. Select Classification Rules Tab to view the classification rules used in the creation of each role in the result



Role Mining Results

Rule #	Description	Confidence(%)	Role	Record Count
1	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = TRUE AND acc::SAP R3::SAP-Productiton-100::AcctRole::Z CRM BC ALL USERS,Z CRM BC SUPPORT CENTER = na AND acc::SAP R3::SAP-Productiton-100::AuthorizationProfiles::SU09 = na:	1	cluster10	1
2	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = TRUE AND acc::SAP R3::SAP-Productiton-100::AcctRole::Z CRM BC ALL USERS,Z CRM BC SUPPORT CENTER = na AND acc::SAP R3::SAP-Productiton-100::AuthorizationProfiles::SU09 = TRUE:	1	cluster6	1
3	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = TRUE AND acc::SAP R3::SAP-Productiton-100::AcctRole::Z CRM BC ALL USERS,Z CRM BC SUPPORT CENTER = TRUE:	1	cluster4	1
4	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = na AND acc::RACF::RACF::Auditor = N AND acc::RACF::RACF::DefaultGroup::TIMESHET = TRUE AND acc::ActiveDirectory::Vaau Active Directory 00-10::GroupMembership::Retail DSL Development = na:	1	cluster7	1
5	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = na AND acc::RACF::RACF::Auditor = N AND acc::RACF::RACF::DefaultGroup::TIMESHET = TRUE AND acc::ActiveDirectory::Vaau Active Directory 00-10::GroupMembership::Retail DSL Development = TRUE:	1	cluster2	1
6	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = na AND acc::RACF::RACF::Auditor = N AND acc::RACF::RACF::DefaultGroup::TIMESHET = na AND acc::RACF::RACF::DefaultGroup::PCCOMPE2 = na AND acc::ActiveDirectory::Vaau Active Directory 00-10::GroupMembership::Read Only User Accounts Group = na:	1	cluster1	1
7	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = na AND acc::RACF::RACF::Auditor = N AND acc::RACF::RACF::DefaultGroup::TIMESHET = na AND acc::RACF::RACF::DefaultGroup::PCCOMPE2 = na AND acc::ActiveDirectory::Vaau Active Directory 00-10::GroupMembership::Read Only User Accounts Group = TRUE:	1	cluster8	1
	acc::ACF2::Prod-02-4500::ACF2::145-ACF2 = na AND acc::RACF::RACF::Auditor = N AND acc::RACF::RACF::DefaultGroup::TIMESHET = na AND			

Page: **1**   1 - 10 of 10 Records - Display 10

Figure 4.14 – Role Mining Results – Classification Rules

12. Select Users in Roles Tab to view a pie chart depicting the participation percentages of the Role Mining User Set in the new roles created

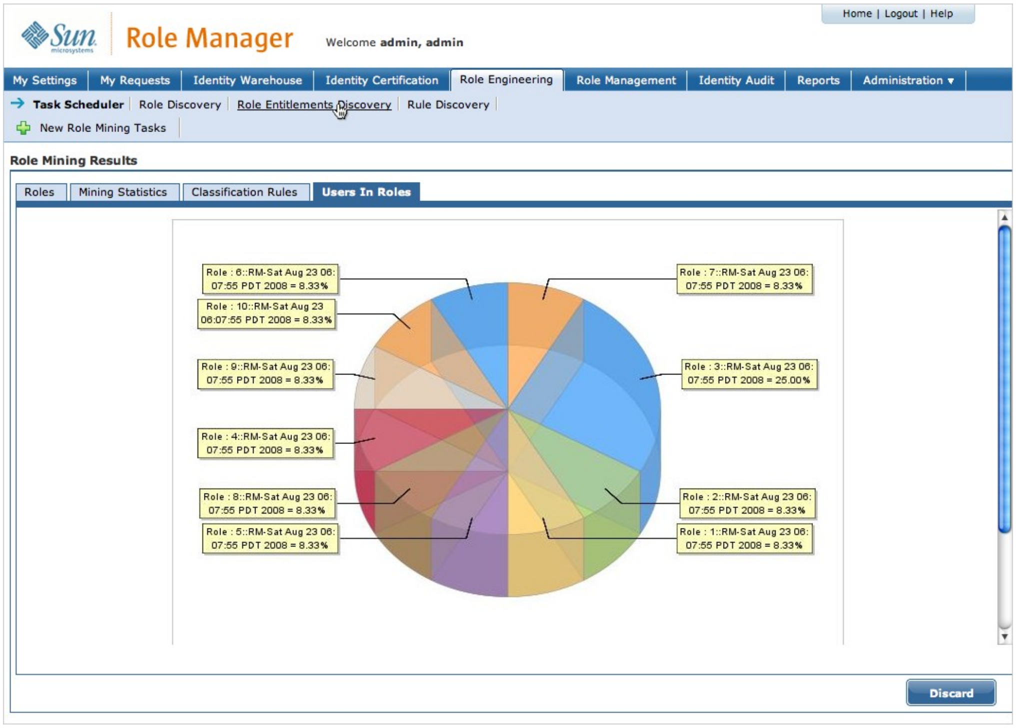
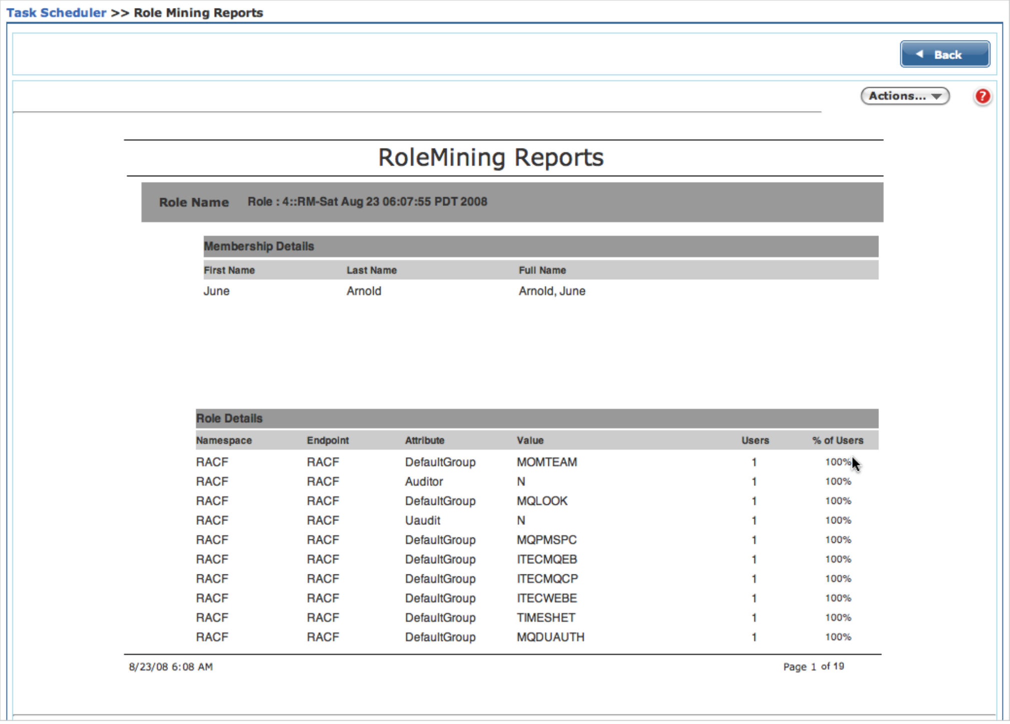

Home | Logout | Help
Sun microsystems
Role Manager
Welcome admin, admin
My Settings
My Requests
Identity Warehouse
Identity Certification
Role Engineering
Role Management
Identity Audit
Reports
Administration ▾
Task Scheduler
Role Discovery
Role Entitlements Discovery
Rule Discovery
New Role Mining Tasks
Role Mining Results
Roles
Mining Statistics
Classification Rules
Users In Roles
Role : 6::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 10::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 9::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 4::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 8::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 5::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 7::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 3::RM-Sat Aug 23 06:07:55 PDT 2008 = 25.00%
Role : 2::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Role : 1::RM-Sat Aug 23 06:07:55 PDT 2008 = 8.33%
Discard

Figure 4.15 – Role Mining Results – Users in Roles

13. To save roles from the list of roles created by the mining effort select the Roles Tab. This gives a list of all the roles created in the “Roles Found” panel on the left

14. To view Role Mining Reports of one or more roles, select the Roles by checking their corresponding checkboxes and select “View Reports”



RoleMining Reports

Role Name Role : 4::RM-Sat Aug 23 06:07:55 PDT 2008

Membership Details

First Name	Last Name	Full Name
June	Arnold	Arnold, June

Role Details

Namespace	Endpoint	Attribute	Value	Users	% of Users
RACF	RACF	DefaultGroup	MOMTEAM	1	100%
RACF	RACF	Auditor	N	1	100%
RACF	RACF	DefaultGroup	MQLOOK	1	100%
RACF	RACF	Uaudit	N	1	100%
RACF	RACF	DefaultGroup	MQPMSPC	1	100%
RACF	RACF	DefaultGroup	ITECMQEB	1	100%
RACF	RACF	DefaultGroup	ITECMQCP	1	100%
RACF	RACF	DefaultGroup	ITECWEBE	1	100%
RACF	RACF	DefaultGroup	TIMESHET	1	100%
RACF	RACF	DefaultGroup	MQDUAUTH	1	100%

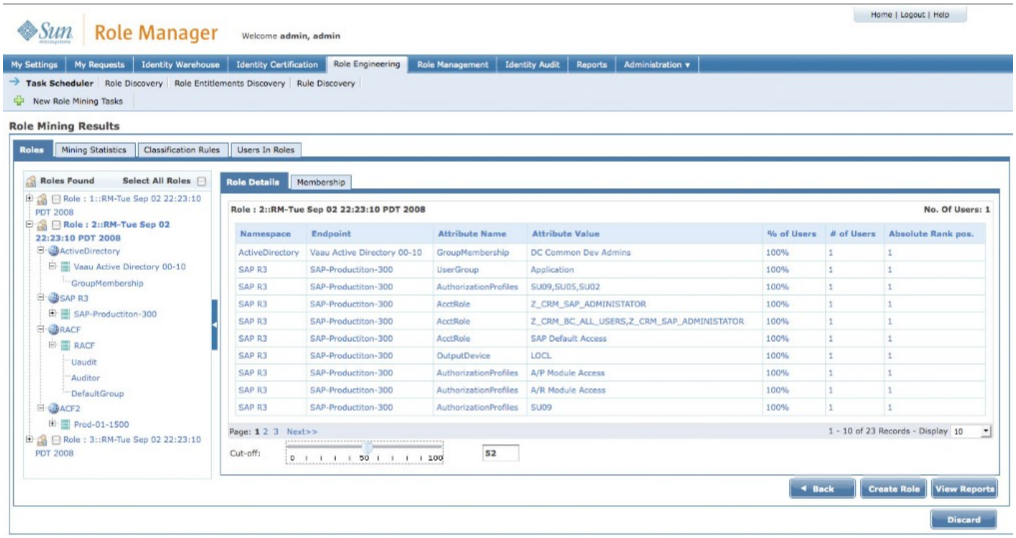
8/23/08 6:08 AM Page 1 of 19

Figure 4.16 – Role Mining Report

15. Role Mining Report for a role gives the membership details and details regarding all the attributes and values associated with the role across all endpoints and namespaces.

16. The report can be exported to a format of choice by using the “Actions…” button

17. Select a role from this list to view the details of the created role. Each Role on the Roles Found panel on the left has further drill down capability to view namespaces, endpoints and attributes associated with the role. Click on a namespace, endpoint or attribute within a Role to view role membership details.



Role : 2::RM-Tue Sep 02 22:23:10 PDT 2008

No. Of Users: 1

Namespace	Endpoint	Attribute Name	Attribute Value	% of Users	# of Users	Absolute Rank pos.
ActiveDirectory	Vaau Active Directory 00-10	GroupMembership	DC Common Dev Admins	100%	1	1
SAP R3	SAP-Productiton-300	UserGroup	Application	100%	1	1
SAP R3	SAP-Productiton-300	AuthorizationProfiles	SU09,SU05,SU02	100%	1	1
SAP R3	SAP-Productiton-300	AcctRole	Z_CRM_SAP_ADMINISTATOR	100%	1	1
SAP R3	SAP-Productiton-300	AcctRole	Z_CRM_BC_ALL_USERS,Z_CRM_SAP_ADMINISTATOR	100%	1	1
SAP R3	SAP-Productiton-300	AcctRole	SAP Default Access	100%	1	1
SAP R3	SAP-Productiton-300	OutputDevice	LOCL	100%	1	1
SAP R3	SAP-Productiton-300	AuthorizationProfiles	A/P Module Access	100%	1	1
SAP R3	SAP-Productiton-300	AuthorizationProfiles	A/R Module Access	100%	1	1
SAP R3	SAP-Productiton-300	AuthorizationProfiles	SU09	100%	1	1

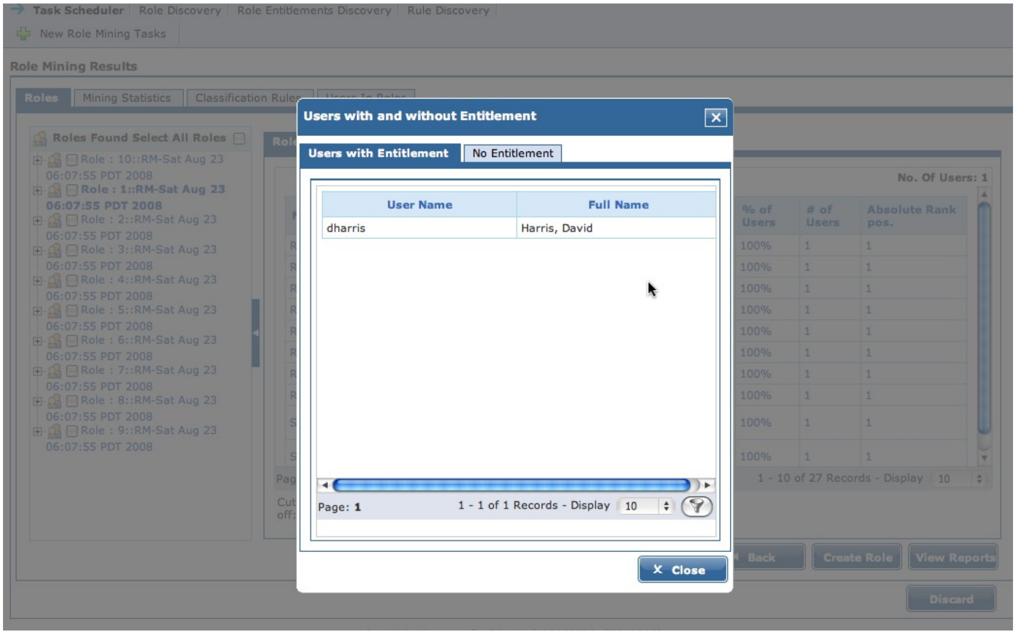
Page: 1 2 3 Next>>

1 - 10 of 23 Records - Display 10

Cut-off: 0 50 100 52

Figure 4.17 – Role Mining Result - Roles

18. Click on a namespace, endpoint, attribute or attribute value in the Role Details panel on the right to see the association details for the particular attribute. A new window opens up that shows the users with and without entitlement


Task Scheduler
Role Discovery
Role Entitlements Discovery
Rule Discovery
New Role Mining Tasks
Role Mining Results
Roles
Mining Statistics
Classification Rules
Roles Found Select All Roles
Role : 10::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 1::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 2::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 3::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 4::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 5::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 6::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 7::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 8::RM-Sat Aug 23 06:07:55 PDT 2008
Role : 9::RM-Sat Aug 23 06:07:55 PDT 2008
No. Of Users: 1
% of Users
# of Users
Absolute Rank pos.
1 - 10 of 27 Records - Display 10
Back
Create Role
View Reports
Discard
Users with and without Entitlement
Users with Entitlement
No Entitlement
Page: 1
1 - 1 of 1 Records - Display 10
Close

User Name	Full Name
dharris	Harris, David

Figure 4.18 – Role Mining Results – Users with and without Entitlement

19. The value “ No. of Users” indicates the number of users from those found in the role that have correlation to the attribute listed in that role

20. The “% of Users” indicates the number of users that have access to the selected attribute

21. Slide the cutoff ruler to the desired accepted risk percentage. All attributes above the cutoff percentage will be set to a primary or parent role policy and those below will be set to a secondary policy for child roles.

22. Select “Create Role” to save the role in the Sun Role Manager Identity Warehouse

23. The Role is displayed in the Identity Warehouse with the appropriate timestamp. Navigate to Identity Warehouse -> Roles menu to view the saved role

24. The Role can now be renamed and its corresponding policy viewed and modified as required. Generally, a feedback from the business or a role owner committee is recommended before changing the policies (associated access attributes) is done.

Role Entitlement Discovery

This module uses existing roles to define, re-evaluate or refine the content of these roles. This can also be used for role consolidation if the role engineer or owner needs to include more applications in the role entitlement mix.

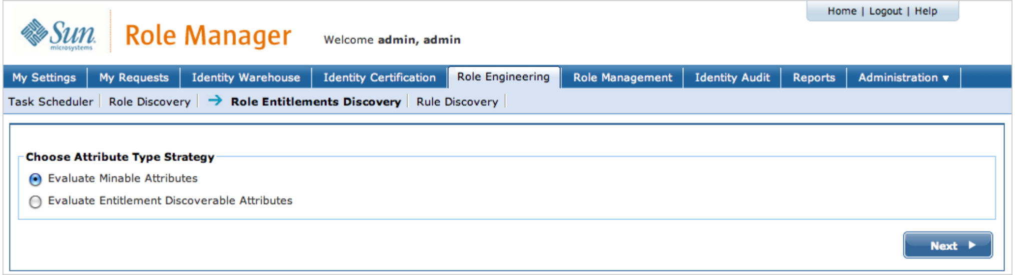
Once roles have been defined for critical applications then the role engineer or owner might not want to increase the number of roles defined for the business or change the makeup of a role, but would like to introduce a larger domain of application entitlements in those roles. In this case the role engineer or owner will select the relevant attributes of the new application only as mine-able and run Role Entitlement Discovery on the existing roles.

Role Entitlement Discovery can also be utilized for top-down roles if they are already defined in the organization for reduced time to arrive at a hybrid, best practice role definition process.

▼ Steps to perform Role Entitlement Discovery

1. Double click the Role Manager icon to launch the thin client.
2. When login screen is presented, enter your credentials and log in.
3. Under Role Engineering tab, select Role Entitlement Discovery. You are presented with the following screen
4. Select Evaluate Mineable attributes and click Next ▶

Figure 4.19 – Choose Role Entitlements Discovery Strategy

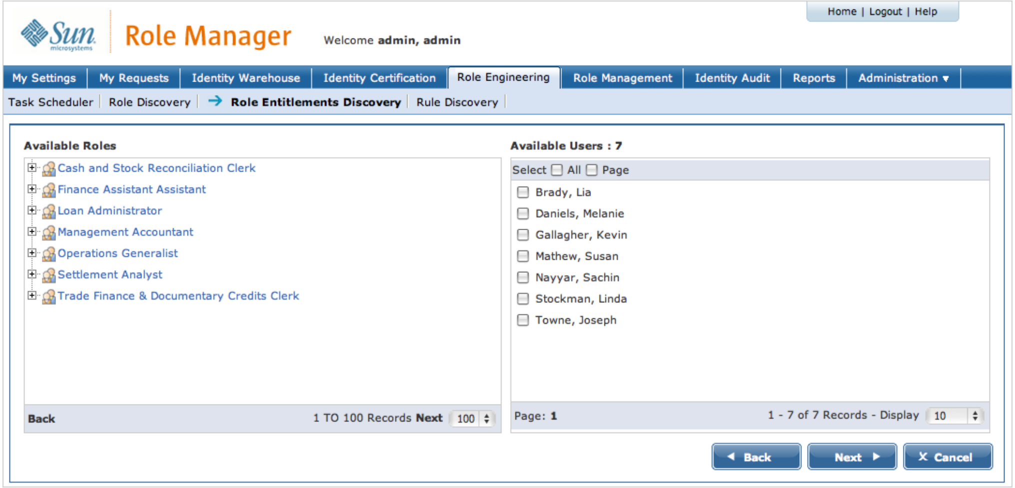


Choose Attribute Type Strategy

● Evaluate Minable Attributes

○ Evaluate Entitlement Discoverable Attributes

5. Select the desired role from the Available Roles on the left hand pane which displays the Users that belong to that role. Select all users or a subset of the users. Click Next ▶



Available Roles

- Cash and Stock Reconciliation Clerk
- Finance Assistant Assistant
- Loan Administrator
- Management Accountant
- Operations Generalist
- Settlement Analyst
- Trade Finance & Documentary Credits Clerk

Back 1 TO 100 Records Next 100

Available Users : 7

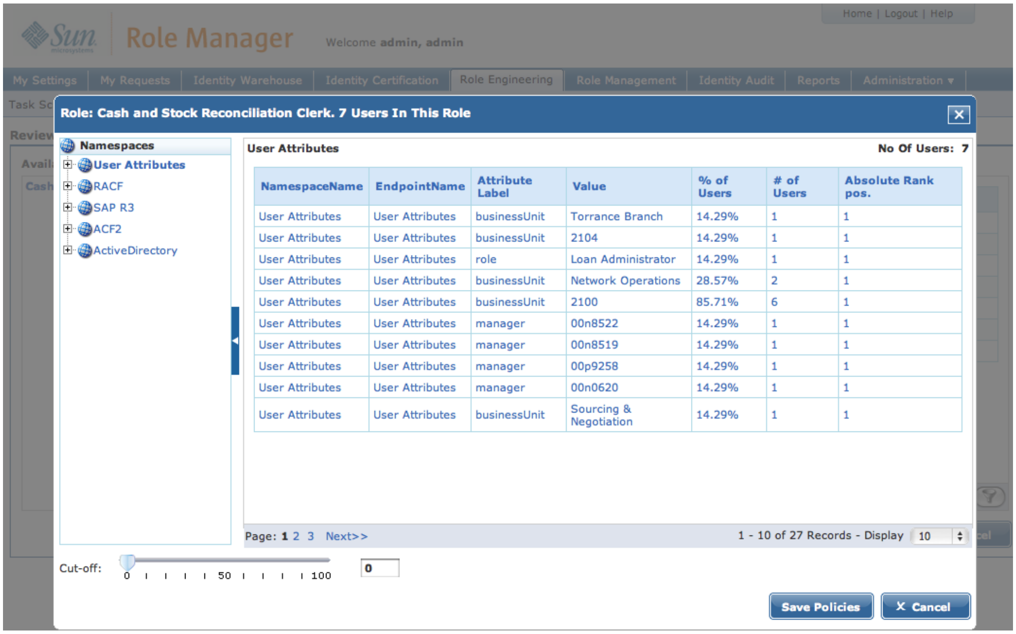
Select □ All □ Page

- □ Brady, Lia
- □ Daniels, Melanie
- □ Gallagher, Kevin
- □ Mathew, Susan
- □ Nayyar, Sachin
- □ Stockman, Linda
- □ Towne, Joseph

Page: 1 1 - 7 of 7 Records - Display 10

Figure 4.20 – Available Roles

6. On the left hand part of the screen, select the Role and click View Details.



Role: Cash and Stock Reconciliation Clerk. 7 Users In This Role

Namespaces

- User Attributes
- RACF
- SAP R3
- ACF2
- ActiveDirectory

User Attributes No Of Users: 7

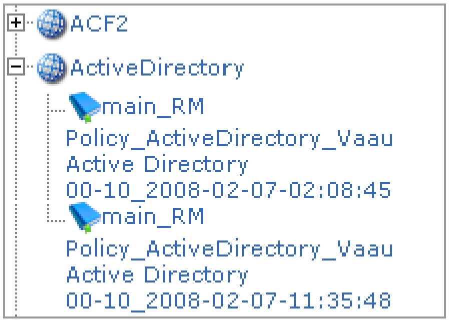
NamespaceName	EndpointName	Attribute Label	Value	% of Users	# of Users	Absolute Rank pos.
User Attributes	User Attributes	businessUnit	Torrance Branch	14.29%	1	1
User Attributes	User Attributes	businessUnit	2104	14.29%	1	1
User Attributes	User Attributes	role	Loan Administrator	14.29%	1	1
User Attributes	User Attributes	businessUnit	Network Operations	28.57%	2	1
User Attributes	User Attributes	businessUnit	2100	85.71%	6	1
User Attributes	User Attributes	manager	00n8522	14.29%	1	1
User Attributes	User Attributes	manager	00n8519	14.29%	1	1
User Attributes	User Attributes	manager	00p9258	14.29%	1	1
User Attributes	User Attributes	manager	00n0620	14.29%	1	1
User Attributes	User Attributes	businessUnit	Sourcing & Negotiation	14.29%	1	1

Page: 1 2 3 Next>> 1 - 10 of 27 Records - Display 10

Cut-off: 0 50 100 0

Figure 4.21 – Role Details

7. Select Cut-off percentage and click Save Policies. This will save the Policies in the Identity Warehouse. Click Identity Warehouse -> Policies to view the time stamped policies.



ACF2
ActiveDirectory
main_RM Policy_ActiveDirectory_Vaau Active Directory 00-10_2008-02-07-02:08:45
main_RM Policy_ActiveDirectory_Vaau Active Directory 00-10_2008-02-07-11:35:48

Figure 4.22 – New Policies Saved in Policies View

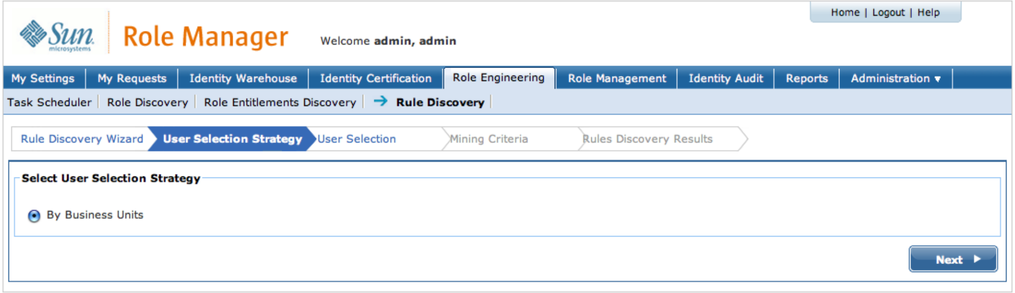
8. The access (attributes) related to these policies can be evaluated and added or removed as required. Generally, a feedback from the business or a role owner committee is recommended before changing the policies (associated access attributes) is done. These policies, once renamed and finalized, can be re-associated to the original role.

Rules Discovery

Role Manager can also be used to help find and design rules to assign Roles to users based on current HR attributes. The Rules Discovery wizard prompts for a selection of a subset of users to learn the classification model from them and their associated HR attributes. These HR attributes are assumed to be associated to the user when they are imported into the Role Manager Identity Warehouse.

▼ Steps to perform Rules Discovery

1. Double click the Role Manager icon to launch the thin client.
2. When login screen is presented, enter your credentials and log in.
3. Under Role Engineering tab, select Rule Discovery.
4. Users can be selected on the basis of Business Units, End Point or from a selection of all users. For this example, we will select By Business Units. Click Next ▶

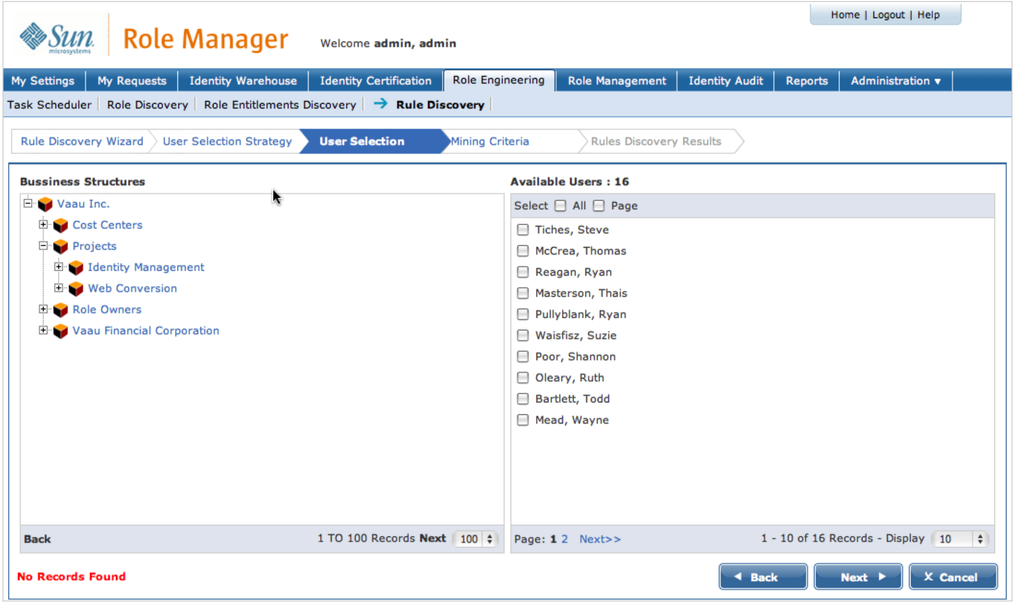


Select User Selection Strategy

● By Business Units

Figure 4.23 – Rule Discovery User Selection Strategy

5. Select the desired business unit on the left hand pane and select all users or a subset of users on the right hand pane. Click Next ▶



Bussiness Structures

- Vaau Inc.
  - Cost Centers
  - Projects
    - Identity Management
    - Web Conversion
  - Role Owners
  - Vaau Financial Corporation

Back 1 TO 100 Records Next 100

Available Users : 16

Select □ All □ Page

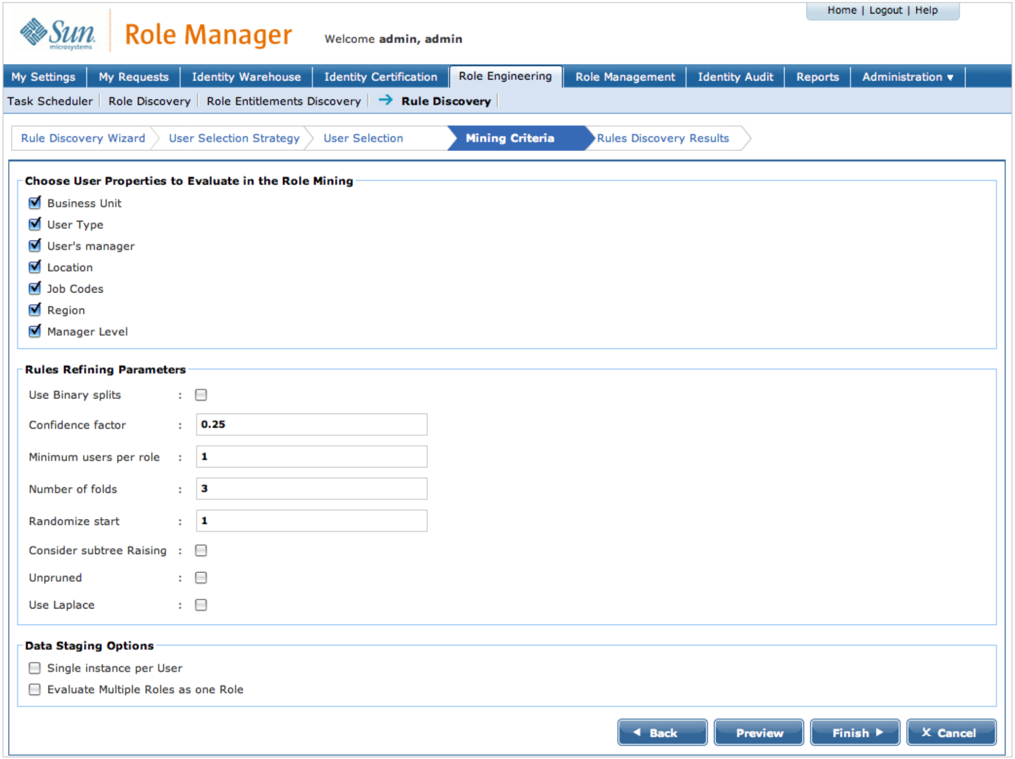
□ Tiches, Steve
□ McCrea, Thomas
□ Reagan, Ryan
□ Masterson, Thais
□ Pullyblank, Ryan
□ Waisfisz, Suzie
□ Poor, Shannon
□ Oleary, Ruth
□ Bartlett, Todd
□ Mead, Wayne

Page: 1 2 Next>> 1 - 10 of 16 Records - Display 10

No Records Found

Figure 4.24 – User Selection

6. Select the appropriate Role Mining properties, Rule Refining Parameters and Data Staging Options. Click **Preview** if you wish to preview the selected data or click **Finish ▶**



Choose User Properties to Evaluate in the Role Mining

☑ Business Unit
☑ User Type
☑ User's manager
☑ Location
☑ Job Codes
☑ Region
☑ Manager Level

Rules Refining Parameters

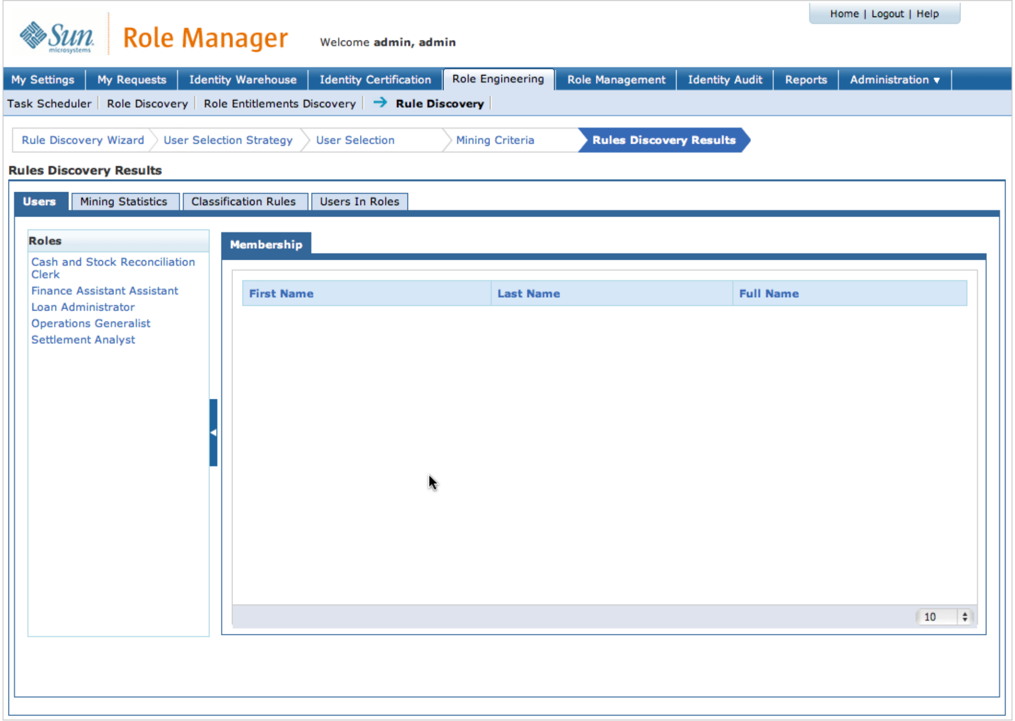
Use Binary splits : □
Confidence factor : 0.25
Minimum users per role : 1
Number of folds : 3
Randomize start : 1
Consider subtree Raising : □
Unpruned : □
Use Laplace : □

Data Staging Options

□ Single instance per User
□ Evaluate Multiple Roles as one Role

Figure 4.25 – Rule Mining Criteria

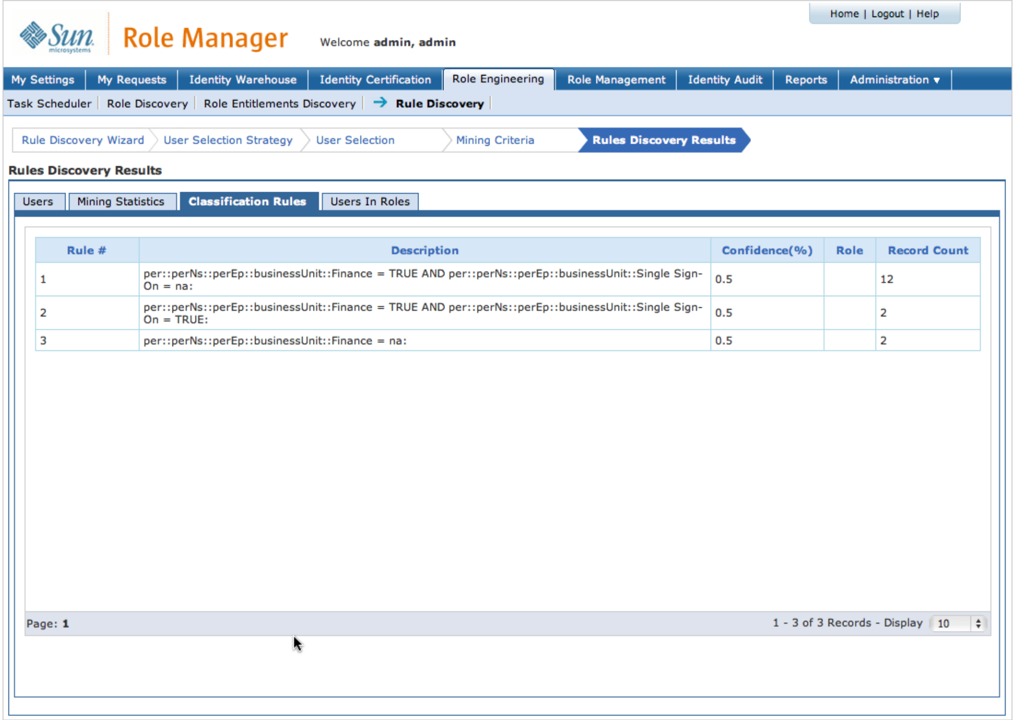
7. The first tab in the Rule Discovery screen displays the roles and users in the roles along with the Rules matrix and mining statistics.



Rules Discovery Results

Figure 4.26 – Rule Discovery Result

8. The second tab, Classification Rules, displays the rules on the basis of which a role can be assigned to a user.



Rules Discovery Results

Rule #	Description	Confidence(%)	Role	Record Count
1	per::perNs::perEp::businessUnit::Finance = TRUE AND per::perNs::perEp::businessUnit::Single Sign-On = na:	0.5		12
2	per::perNs::perEp::businessUnit::Finance = TRUE AND per::perNs::perEp::businessUnit::Single Sign-On = TRUE:	0.5		2
3	per::perNs::perEp::businessUnit::Finance = na:	0.5		2

Page: 1 1 - 3 of 3 Records - Display 10

Figure 4.27 – Classification Rules

9. The third tab, users In Roles, displays a graphical percentage of users to roles they belong to.

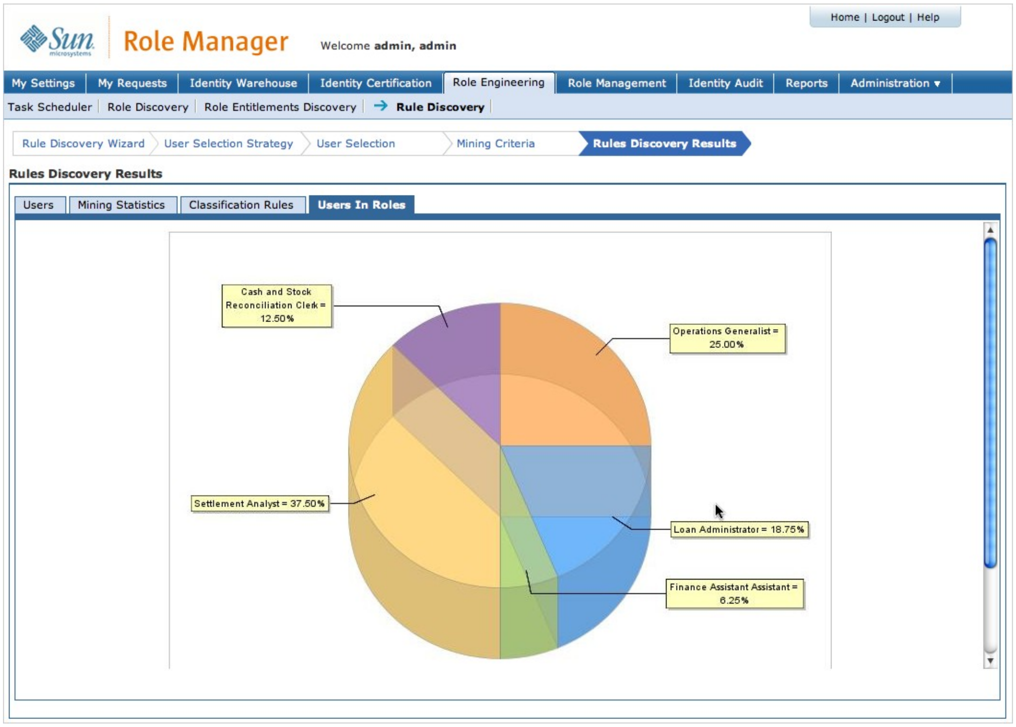
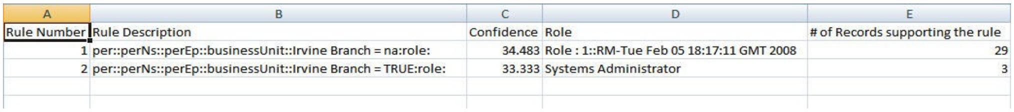


Figure 4.28 – Users in Roles

10. Click Export Classification Rules to export to a .csv file. The .csv file contains the description of the rule which can then be used for Rule Engineering (Refer to the Sun Role Manager 4.1 Administration Guide).



A	B	C	D	E
Rule Number	Rule Description	Confidence	Role	# of Records supporting the rule
1	per::perNs::perEp::businessUnit::Irvine Branch = na:role:	34.483	Role : 1::RM-Tue Feb 05 18:17:11 GMT 2008	29
2	per::perNs::perEp::businessUnit::Irvine Branch = TRUE:role:	33.333	Systems Administrator	3

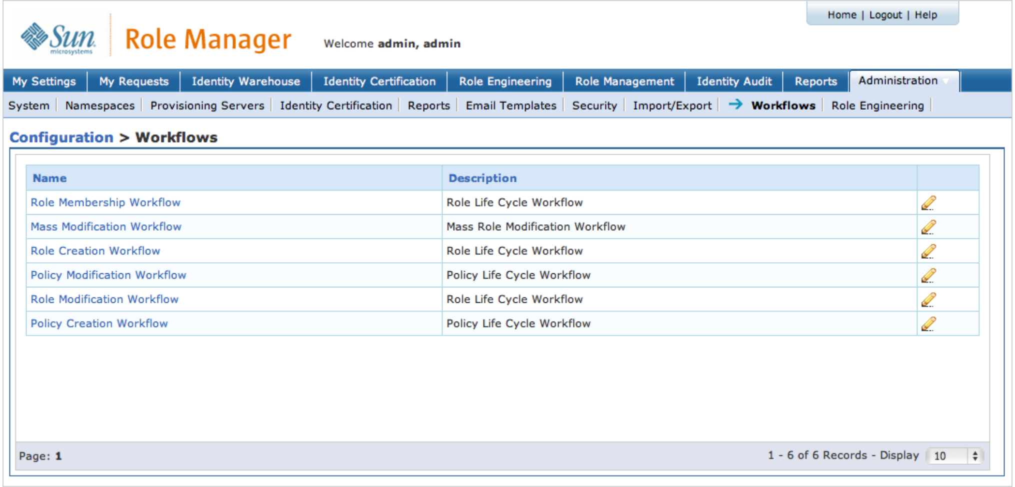
Figure 4.29 – Classification Rules in csv format

5

◆ ◆ ◆ CHAPTER 5

Role Management & My Requests

Role Manager offers an enhanced workflow engine to manage the lifecycle of roles. This new workflow engine provides the ability to design various workflow processes and also allows users to call external functions from within the workflow.



Name	Description	
Role Membership Workflow	Role Life Cycle Workflow	
Mass Modification Workflow	Mass Role Modification Workflow	
Role Creation Workflow	Role Life Cycle Workflow	
Policy Modification Workflow	Policy Life Cycle Workflow	
Role Modification Workflow	Role Life Cycle Workflow	
Policy Creation Workflow	Policy Life Cycle Workflow	

Figure 5.1 – Role Management Workflows

Role Manager provides a robust and easily configurable workflow engine to facilitate Role Management involving various actors and entities in an organization. It can be customized to cater to diverse requirements to support different actors, role approval paths, policy approval paths, email integration, and also exposes web services to communicate with third party applications.

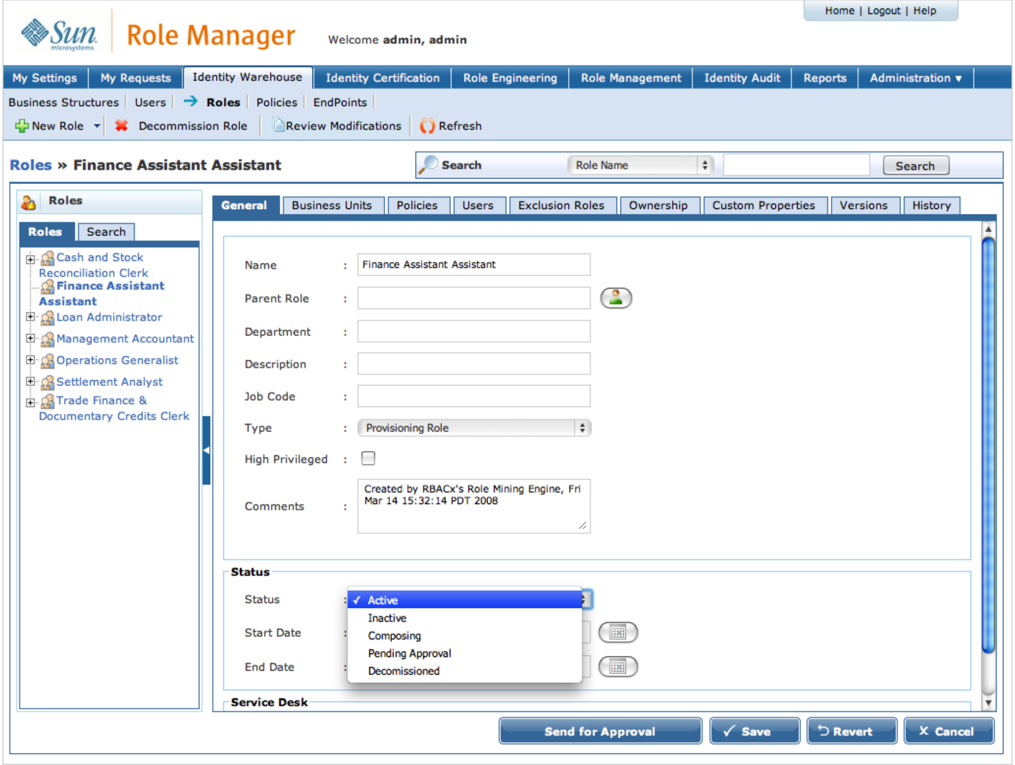
Role Manager allows for the creation of six types of workflow:

1. **Role Membership Workflow:** An 'n' level approval process to approve any Role-User Membership changes
2. **Role Creation Workflow:** An 'n' level approval process to approve the creation of a role and its underlying access
3. **Role Modification Workflow:** An 'n' level approval process to approve the modification of roles and its underlying access
4. **Policy Creation Workflow**: An 'n' level approval process to approve the creation of a policy and its underlying access
5. **Policy Modification Workflow:** An 'n' level approval process to approve the modification of a policy and its underlying access
6. **Mass Modification Workflow:**

Hence, these six workflow types can each generate individual request types depending on the action performed on any role or policy and its lifecycle in Role Manager.

Role Status

Role Manager provides a **Role Status** feature, with pre-defined statuses, to further enhance the lifecycle of roles. These statuses provide important information on the state of a role at any given point in time.



Roles » Finance Assistant Assistant

Name : Finance Assistant Assistant

Parent Role :

Department :

Description :

Job Code :

Type : Provisioning Role

High Privileged : □

Comments : Created by RBACx's Role Mining Engine, Fri Mar 14 15:32:14 PDT 2008

Status

Status : ✓ Active

Start Date :

End Date :

Figure 5.2 – Role Status

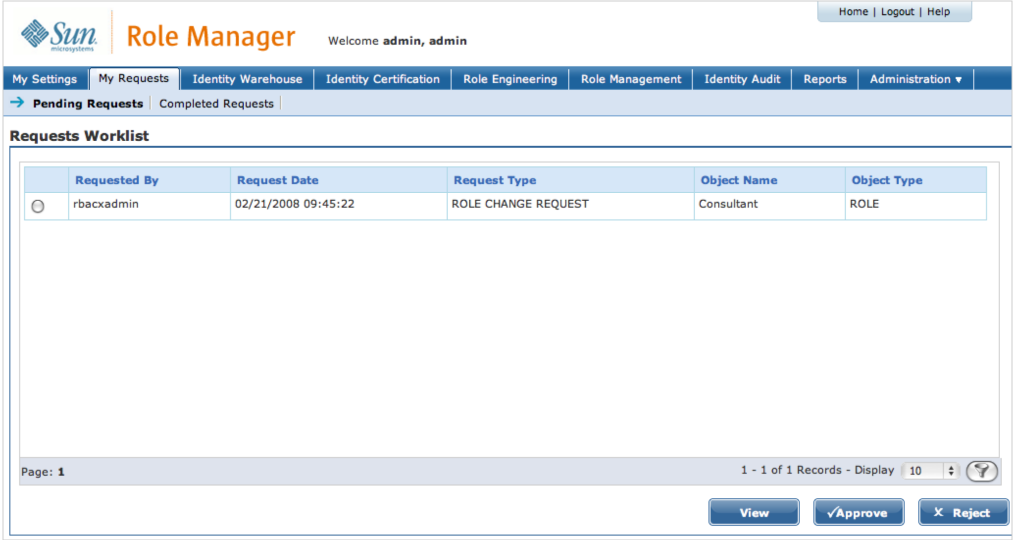
Every time a new role is created, it enlists a status of "Composing". This role, along with its members (users) and its underlying access (associated policies) is sent for Approval by a Role Owner or Role Manager administrator. It is then up to the Role Approver to approve the Role Creation, Role Modification or Role Membership request so that the status of the role can be changed to "Active" and it can then be officially used for role based access control purposes.

Pending Requests

Role content approval or role membership requests can now be approved in Role Manager by various actors (such as a manager, role owner, policy owner, etc.) by simply logging into Role Manager and approving a detailed request waiting in their queue.

▼ Steps to Approve a Pending Request

1. Log into the Role Manager Web-Interface using a Java enabled web browser
2. Log in with credentials of administrator or business unit manager or Role Approver
3. Click My Requests -> Pending Requests to view your pending requests
4. Click View to view the request details.



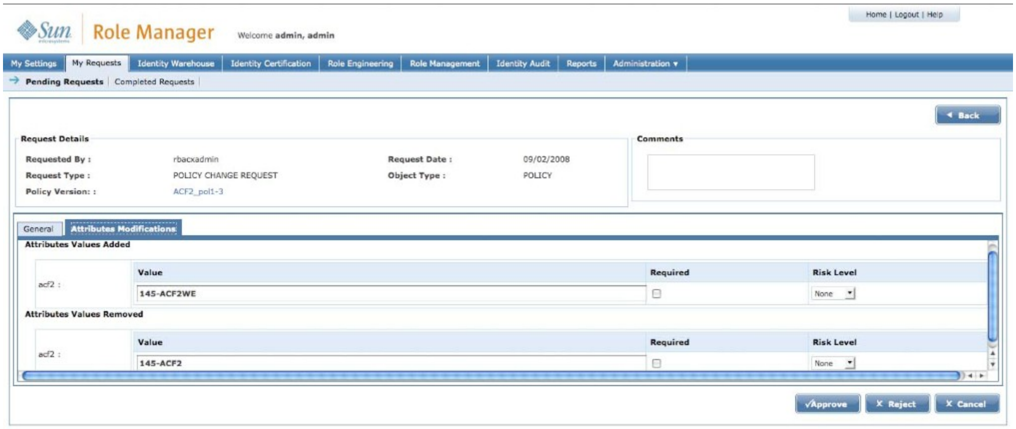
Requests Worklist

	Requested By	Request Date	Request Type	Object Name	Object Type
○	rbacxadmin	02/21/2008 09:45:22	ROLE CHANGE REQUEST	Consultant	ROLE

Page: 1 1 - 1 of 1 Records - Display 10

Figure 5.3 – My Requests Work list

Analyzing a Request



Request Details

Requested By : rbacxadmin

Request Type : POLICY CHANGE REQUEST

Policy Version: : ACF2_pol1-3

Request Date : 09/02/2008

Object Type : POLICY

Comments

Attributes Values Added

	Value	Required	Risk Level
acf2 :	145-ACF2WE	□	None

Attributes Values Removed

	Value	Required	Risk Level
acf2 :	145-ACF2	□	None

Figure 5.4 – Request Details

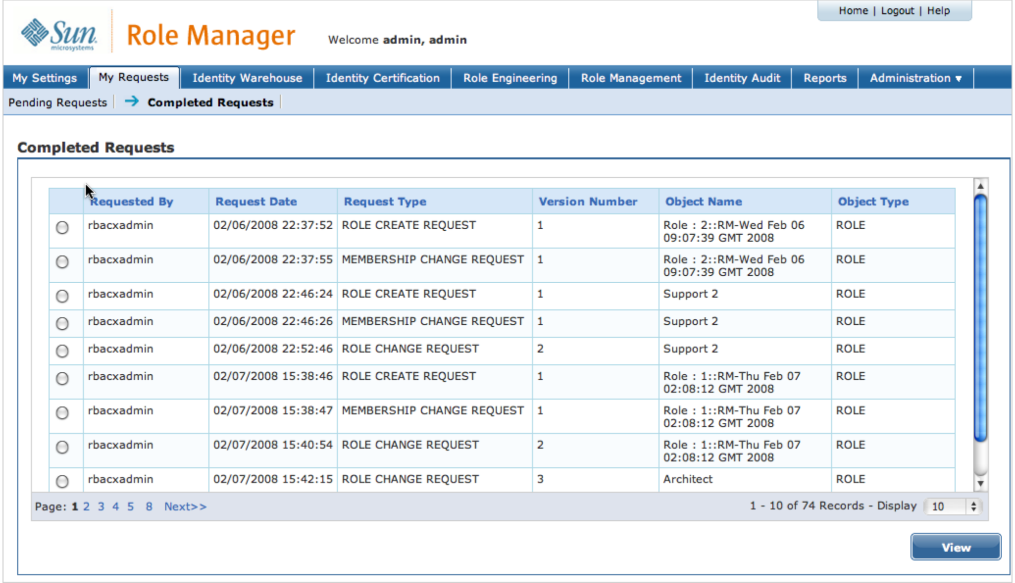
5. The Request Details provide the following information:

- The Name of the Requestor
- Type of Request (Role Creation, Role Modification, Role Membership)
- Request Date
- Role Version
- Approval History (Who already approved the request)
- Any Role attribute modifications requested
- Any Policy modifications requested (new access added or existing access removed)
- Role Consolidation (Provides information specifying the role to be approved has a similarity percentage in terms of Role Membership or not and whether the role to be approved has a similarity percentage with other existing roles and their underlying access or not)

6. To approve or reject the request after analysis, the role approver can click √Approve or X Reject

Completed Requests

In order to view completed requests history, the user can click My Requests -> Completed Requests.



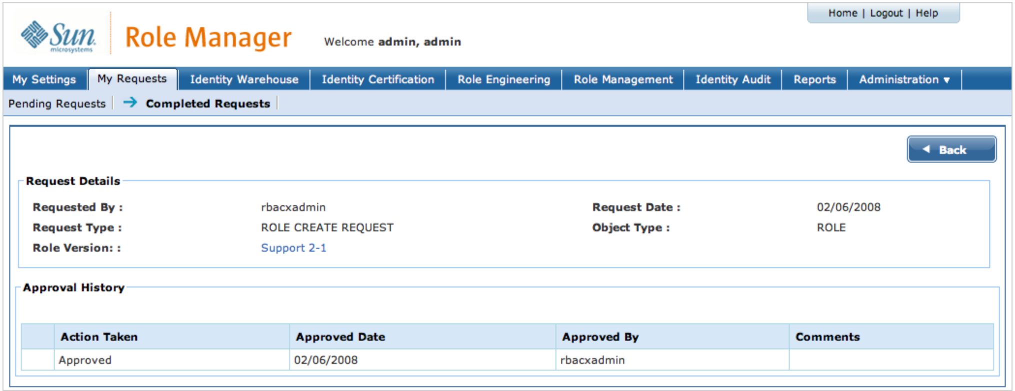
Completed Requests

	Requested By	Request Date	Request Type	Version Number	Object Name	Object Type
○	rbacxadmin	02/06/2008 22:37:52	ROLE CREATE REQUEST	1	Role : 2::RM-Wed Feb 06 09:07:39 GMT 2008	ROLE
○	rbacxadmin	02/06/2008 22:37:55	MEMBERSHIP CHANGE REQUEST	1	Role : 2::RM-Wed Feb 06 09:07:39 GMT 2008	ROLE
○	rbacxadmin	02/06/2008 22:46:24	ROLE CREATE REQUEST	1	Support 2	ROLE
○	rbacxadmin	02/06/2008 22:46:26	MEMBERSHIP CHANGE REQUEST	1	Support 2	ROLE
○	rbacxadmin	02/06/2008 22:52:46	ROLE CHANGE REQUEST	2	Support 2	ROLE
○	rbacxadmin	02/07/2008 15:38:46	ROLE CREATE REQUEST	1	Role : 1::RM-Thu Feb 07 02:08:12 GMT 2008	ROLE
○	rbacxadmin	02/07/2008 15:38:47	MEMBERSHIP CHANGE REQUEST	1	Role : 1::RM-Thu Feb 07 02:08:12 GMT 2008	ROLE
○	rbacxadmin	02/07/2008 15:40:54	ROLE CHANGE REQUEST	2	Role : 1::RM-Thu Feb 07 02:08:12 GMT 2008	ROLE
○	rbacxadmin	02/07/2008 15:42:15	ROLE CHANGE REQUEST	3	Architect	ROLE

Page: 1 2 3 4 5 8 Next>> 1 - 10 of 74 Records - Display 10

Figure 5.5 –Completed Requests

Click View to view the request details.



Request Details

Requested By :	rbacxadmin	Request Date :	02/06/2008
Request Type :	ROLE CREATE REQUEST	Object Type :	ROLE
Role Version: :	Support 2-1		

Approval History

Action Taken	Approved Date	Approved By	Comments
Approved	02/06/2008	rbacxadmin	

Figure 5.6 – Request History Details

Role Versioning

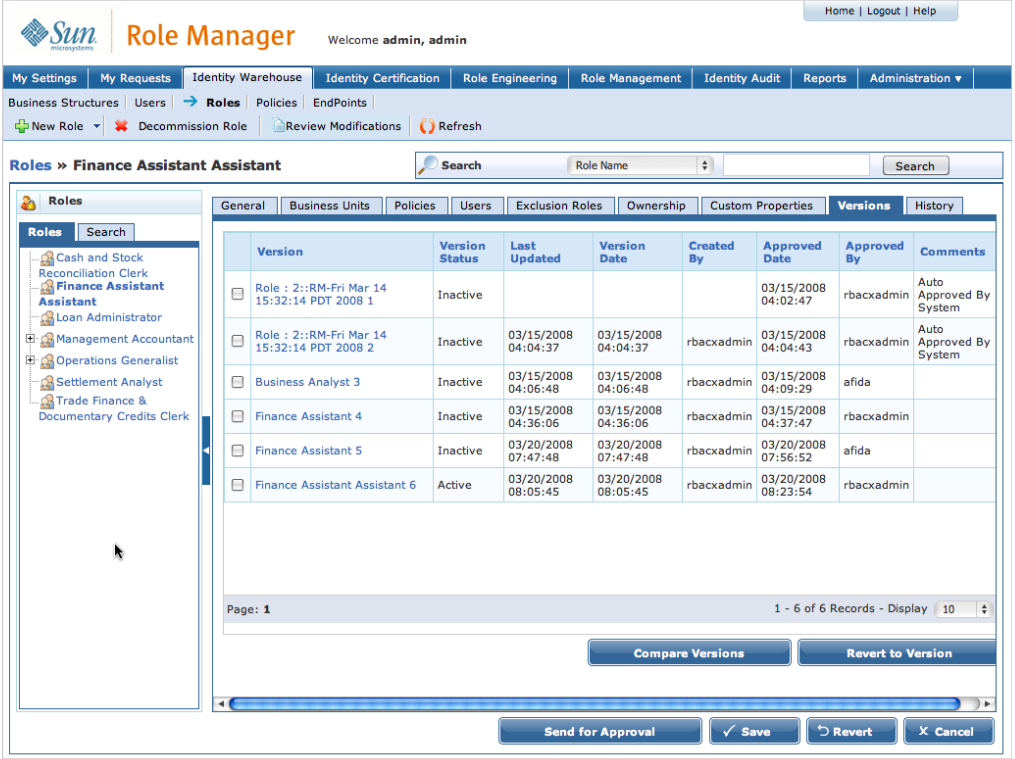
Sun Role Manager provides sophisticated role versioning capabilities, allowing role engineers and administrators to create different versions of roles so that modifications made to a role do not affect the original role. Sun Role Manager allows ‘n’ number of versions to be created for any particular role, requiring a version to be approved before it is made active. This feature assists in managing the lifecycle of roles ensuring no role modifications are made without approval and that there is always a previous version of the role to fall back on. Sun Role Manager provides sophisticated role version management with the ability to compare versions and revert to any version. All versions have an audit trail of when and by whom they were created and approved. Comparing two versions gives an individual comparison all the attributes, owners, business units, policies and exclusion roles of a role in a tabular fashion. Different color codes are used to indicate values that are unmodified, modified, added or deleted.

The key Role Versioning features in Sun Role Manager are:

- Version Creation: Sun Role Manager automatically creates a new version for a Role when the definition of a Role is changed. Role definition changes due to number of actions on role properties such as policy addition/removal, change in an associated policy, addition/removal of owners, change in name, manual change in status etc
- Version Comparison: Sun Role Manager allows the comparison of two versions of role. Role properties are divided into General, Ownership, Business Units, Policies or Exclusion Roles modules for comparison. All properties for the compared versions are displayed side by side and the changes are highlighted with color codes for modification, addition and deletion
- Reverting to a Version: Sun Role Manager stores all created versions of a role. Only one version of a role can be active at an instant. A Role can easily be reverted to any of the inactive versions using the Revert to Version capability

▼ Steps to Manage Role Versions (View, Compare, Revert)

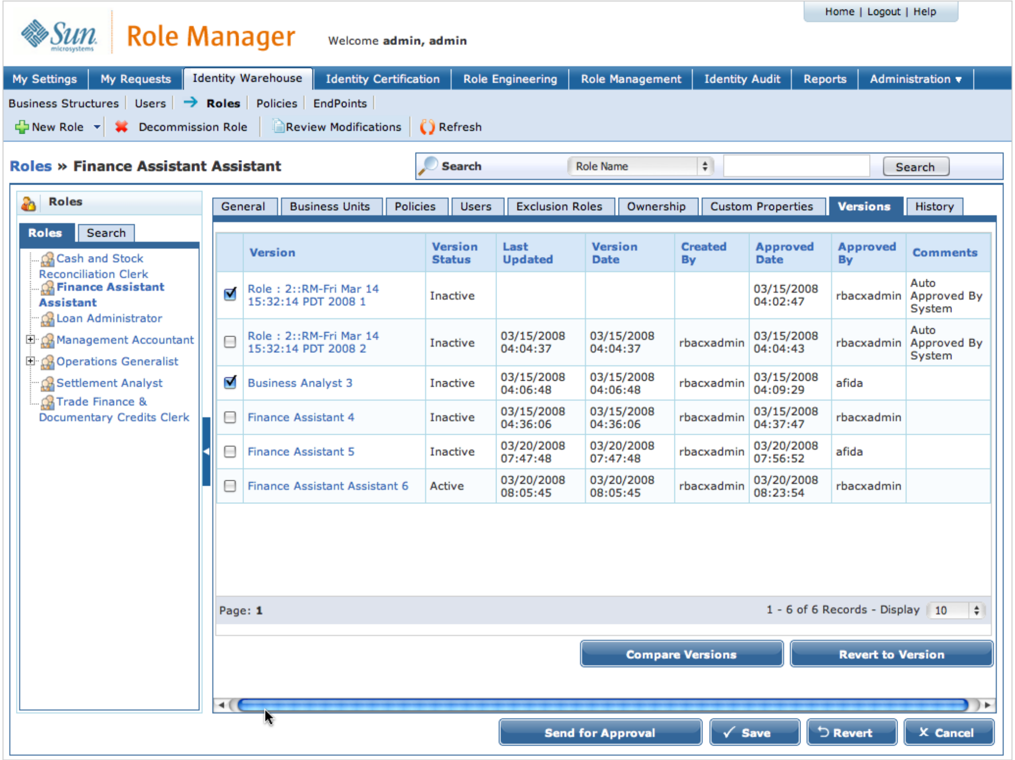
1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialogue box appears. Enter your credentials and login to Sun Role Manager
3. Select the Role view by selecting it from the Identity Warehouse Tab
4. Select a Role from the Roles panel on the left
5. Select the Versions Tab



	Version	Version Status	Last Updated	Version Date	Created By	Approved Date	Approved By	Comments
□	Role : 2::RM-Fri Mar 14 15:32:14 PDT 2008 1	Inactive				03/15/2008 04:02:47	rbacxadmin	Auto Approved By System
□	Role : 2::RM-Fri Mar 14 15:32:14 PDT 2008 2	Inactive	03/15/2008 04:04:37	03/15/2008 04:04:37	rbacxadmin	03/15/2008 04:04:43	rbacxadmin	Auto Approved By System
□	Business Analyst 3	Inactive	03/15/2008 04:06:48	03/15/2008 04:06:48	rbacxadmin	03/15/2008 04:09:29	afida	
□	Finance Assistant 4	Inactive	03/15/2008 04:36:06	03/15/2008 04:36:06	rbacxadmin	03/15/2008 04:37:47	rbacxadmin	
□	Finance Assistant 5	Inactive	03/20/2008 07:47:48	03/20/2008 07:47:48	rbacxadmin	03/20/2008 07:56:52	afida	
□	Finance Assistant Assistant 6	Active	03/20/2008 08:05:45	03/20/2008 08:05:45	rbacxadmin	03/20/2008 08:23:54	rbacxadmin	

Figure 5.7 – Role Versions

6. To compare two versions select them by selecting their corresponding checkboxes and select “Compare Versions”



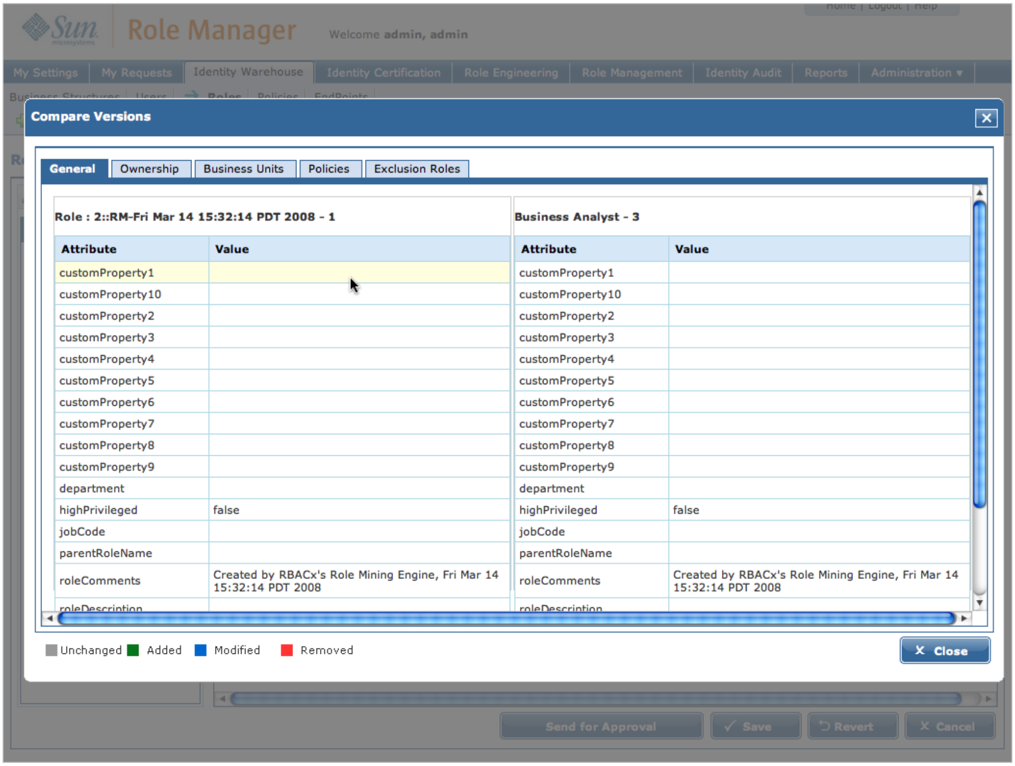
Roles » Finance Assistant Assistant

	Version	Version Status	Last Updated	Version Date	Created By	Approved Date	Approved By	Comments
☑	Role : 2::RM-Fri Mar 14 15:32:14 PDT 2008 1	Inactive				03/15/2008 04:02:47	rbacxadmin	Auto Approved By System
☐	Role : 2::RM-Fri Mar 14 15:32:14 PDT 2008 2	Inactive	03/15/2008 04:04:37	03/15/2008 04:04:37	rbacxadmin	03/15/2008 04:04:43	rbacxadmin	Auto Approved By System
☑	Business Analyst 3	Inactive	03/15/2008 04:06:48	03/15/2008 04:06:48	rbacxadmin	03/15/2008 04:09:29	afida	
☐	Finance Assistant 4	Inactive	03/15/2008 04:36:06	03/15/2008 04:36:06	rbacxadmin	03/15/2008 04:37:47	rbacxadmin	
☐	Finance Assistant 5	Inactive	03/20/2008 07:47:48	03/20/2008 07:47:48	rbacxadmin	03/20/2008 07:56:52	afida	
☐	Finance Assistant Assistant 6	Active	03/20/2008 08:05:45	03/20/2008 08:05:45	rbacxadmin	03/20/2008 08:23:54	rbacxadmin	

Page: 1 1 - 6 of 6 Records - Display 10

Figure 5.8 – Select Versions for Comparison

7. Select the General, Ownership, Business Units, Policies or Exclusion Roles Tab to compare these aspects of the versions



Role : 2::RM-Fri Mar 14 15:32:14 PDT 2008 - 1

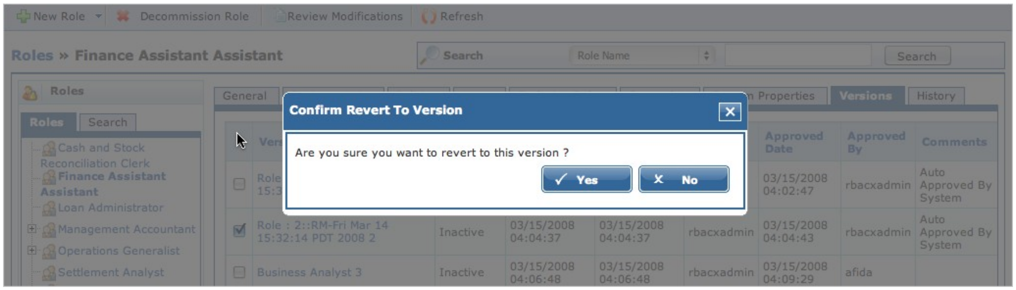
Attribute	Value
customProperty1	
customProperty10	
customProperty2	
customProperty3	
customProperty4	
customProperty5	
customProperty6	
customProperty7	
customProperty8	
customProperty9	
department	
highPrivileged	false
jobCode	
parentRoleName	
roleComments	Created by RBACx's Role Mining Engine, Fri Mar 14 15:32:14 PDT 2008
roleDescription	

Business Analyst - 3

Attribute	Value
customProperty1	
customProperty10	
customProperty2	
customProperty3	
customProperty4	
customProperty5	
customProperty6	
customProperty7	
customProperty8	
customProperty9	
department	
highPrivileged	false
jobCode	
parentRoleName	
roleComments	Created by RBACx's Role Mining Engine, Fri Mar 14 15:32:14 PDT 2008
roleDescription	

Figure 5.9 – Compare Versions

8. To revert to an inactive version of the Role select a version by selecting its checkbox and select “Revert to Version”.



Are you sure you want to revert to this version ?

	Ver					Approved Date	Approved By	Comments
□	Role 15:3					03/15/2008 04:02:47	rbacxadmin	Auto Approved By System
☑	Role : 2::RM-Fri Mar 14 15:32:14 PDT 2008 2	Inactive	03/15/2008 04:04:37	03/15/2008 04:04:37	rbacxadmin	03/15/2008 04:04:43	rbacxadmin	Auto Approved By System
□	Business Analyst 3	Inactive	03/15/2008 04:06:48	03/15/2008 04:06:48	rbacxadmin	03/15/2008 04:09:29	afida	

Figure 5.10 – Revert to Version

9. A “Confirm Revert to Version” Window opens. Select “Yes”. The version status of the version reverted to will change from “Inactive” to “Pending Approval”

Role History

Role History creates a complete snapshot of the Role. Role History provides at a glance all instances of addition/removal of members, policies and owners as well as modification to attribute values of the Role. An audit trail is created by recording and displaying when and by whom a change is made.

The aspects covered by Sun Role Manager Role History are:

- Role Membership History: provides a view of all members added to or removed from the Role along with the Sun Role Manager User responsible for the action and the date of member addition/removal
- Policy History: provides a view of all policies added to or removed from the Role along with the Sun Role Manager User responsible for the action and the date of policy removal
- Owner History: provides a view of all owners added to or removed from the Role along with the Sun Role Manager User responsible for the action and the date of owner addition/removal
- Attribute History: provides a view of all modifications made to attributes associated with a role. The Attribute name, old value of the attribute and the new value after modification are displayed. Also displayed are the Sun Role Manager User responsible for the modification and the date of the change.
- Certification History: provides a view of all certifications done on a Role. Details of Certification creator, creation date, Certification period, Certifier, Certification Status and Certification date are displayed.

▼ Steps to view Role History

1. Start Sun Role Manager by clicking the Sun Role Manager icon
2. The login dialog box appears. Enter your credentials and login to Sun Role Manager
3. Select the Role view by selecting it from the Identity Warehouse Tab
4. Select a Role from the Roles panel on the left
5. Select the History Tab

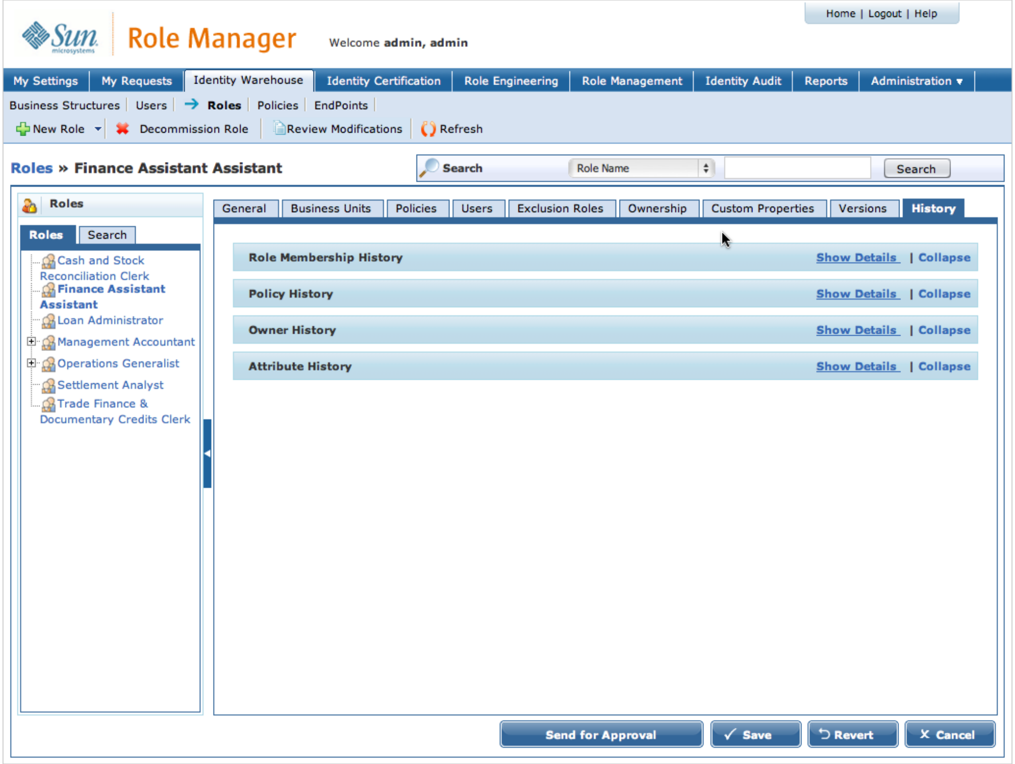
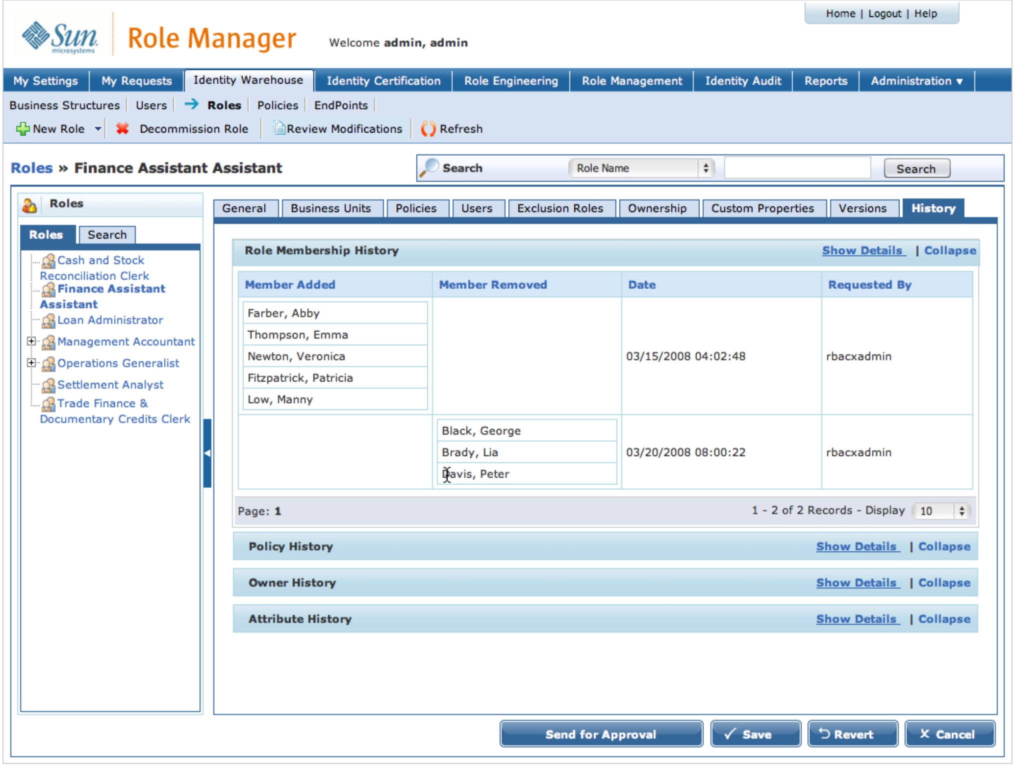


Figure 5.11 – Role History

6. To view member addition/deletion history select “Show Details” corresponding to “Role Member History”



Roles » Finance Assistant Assistant

Role Membership History

Member Added	Member Removed	Date	Requested By
Farber, Abby Thompson, Emma Newton, Veronica Fitzpatrick, Patricia Low, Manny		03/15/2008 04:02:48	rbacxadmin
	Black, George Brady, Lia Davis, Peter	03/20/2008 08:00:22	rbacxadmin

Page: 1 1 - 2 of 2 Records - Display 10

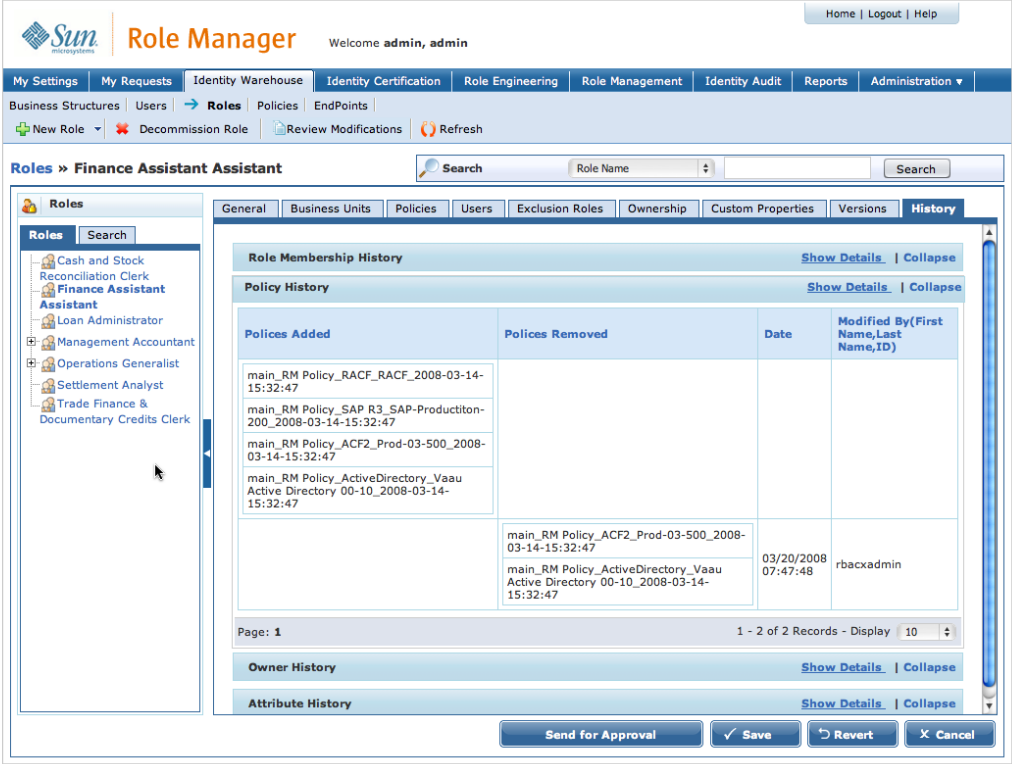
Policy History

Owner History

Attribute History

Figure 5.12 – Role History - Role Membership History

7. To view Policy addition/deletion history select “Show Details” corresponding to “Policy History”



Roles » Finance Assistant Assistant

Role Membership History

Policy History

Polices Added	Polices Removed	Date	Modified By(First Name,Last Name,ID)
main_RM Policy_RACF_RACF_2008-03-14-15:32:47 main_RM Policy_SAP R3_SAP-Productiton-200_2008-03-14-15:32:47 main_RM Policy_ACF2_Prod-03-500_2008-03-14-15:32:47 main_RM Policy_ActiveDirectory_Vaau Active Directory 00-10_2008-03-14-15:32:47			
	main_RM Policy_ACF2_Prod-03-500_2008-03-14-15:32:47 main_RM Policy_ActiveDirectory_Vaau Active Directory 00-10_2008-03-14-15:32:47	03/20/2008 07:47:48	rbacxadmin

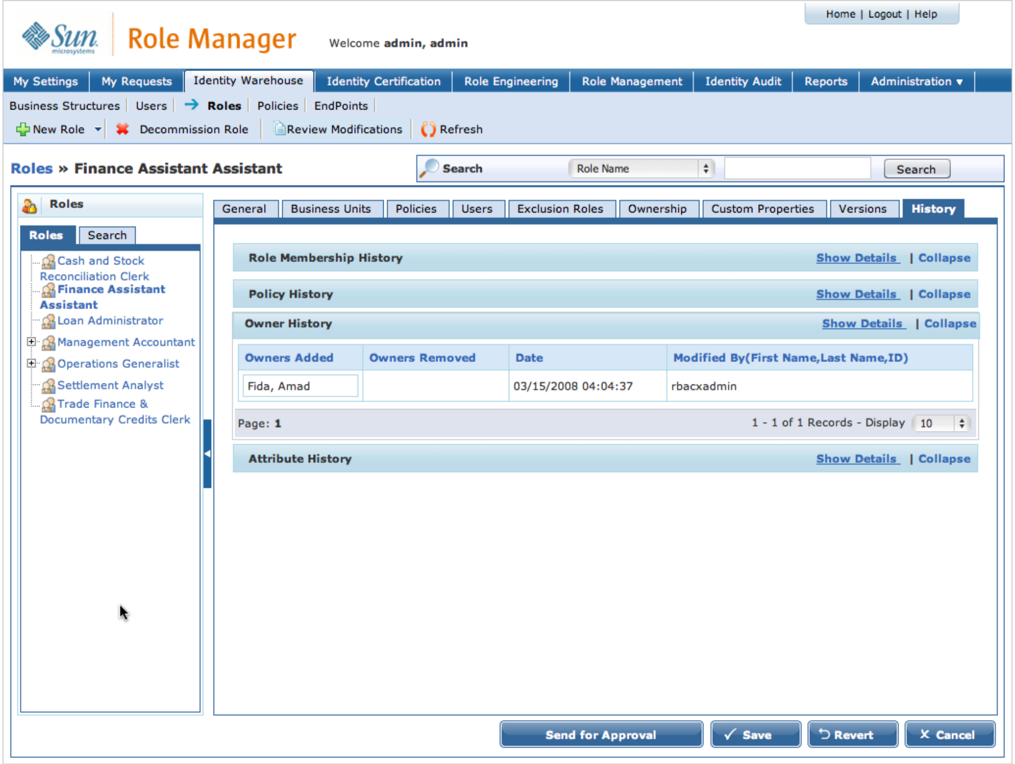
Page: 1 1 - 2 of 2 Records - Display 10

Owner History

Attribute History

Figure 5.13 – Role History – Policy History

8. To view Owner addition/deletion history select “Show Details” corresponding to “Owner History”



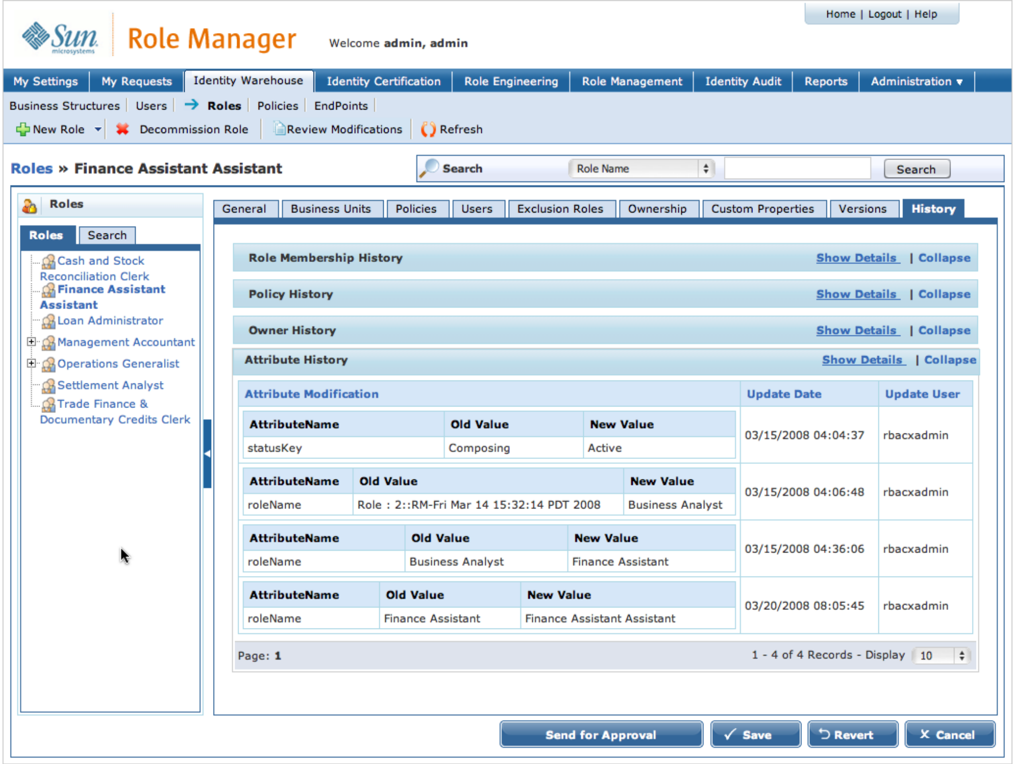
Owner History

Owners Added	Owners Removed	Date	Modified By(First Name,Last Name,ID)
Fida, Amad		03/15/2008 04:04:37	rbacxadmin

Page: 1 — 1 - 1 of 1 Records - Display 10

Figure 5.14 – Role History – Owner History

9. To view Attribute modification history, select “Show Details” corresponding to “Attribute History”. This displays the Attribute Name, Old Value and New Value along with timestamp and User.

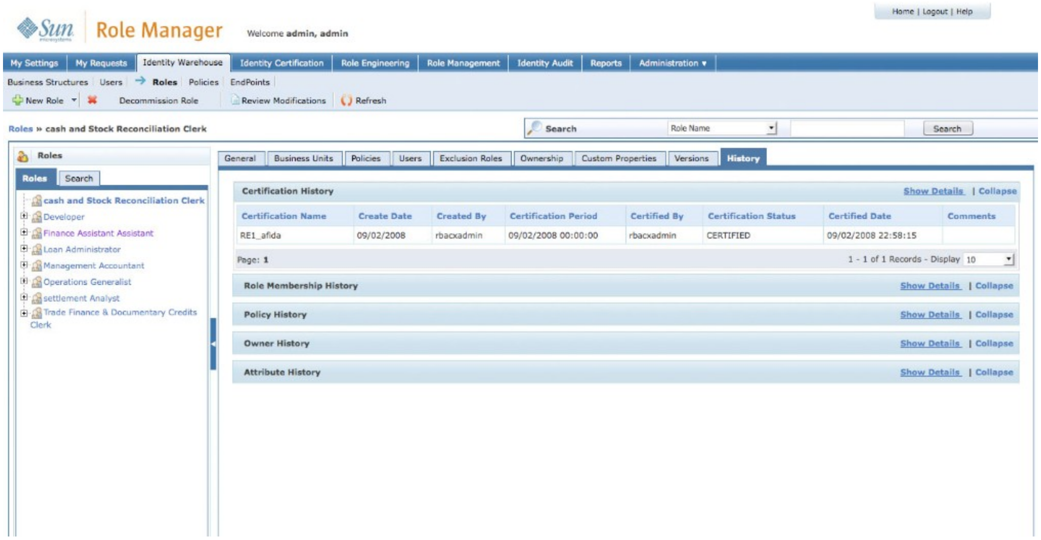


Attribute Modification	Update Date	Update User
AttributeName: statusKey Old Value: Composing New Value: Active	03/15/2008 04:04:37	rbacxadmin
AttributeName: roleName Old Value: Role : 2::RM-Fri Mar 14 15:32:14 PDT 2008 New Value: Business Analyst	03/15/2008 04:06:48	rbacxadmin
AttributeName: roleName Old Value: Business Analyst New Value: Finance Assistant	03/15/2008 04:36:06	rbacxadmin
AttributeName: roleName Old Value: Finance Assistant New Value: Finance Assistant Assistant	03/20/2008 08:05:45	rbacxadmin

Page: 1 1 - 4 of 4 Records - Display 10

Figure 5.15 – Role History – Attribute History

10. To view Certification history, select “Show Details” corresponding to “Certification History”.



Certification Name	Create Date	Created By	Certification Period	Certified By	Certification Status	Certified Date	Comments
RE1_afida	09/02/2008	rbacxadmin	09/02/2008 00:00:00	rbacxadmin	CERTIFIED	09/02/2008 22:58:15	

Page: 1 1 - 1 of 1 Records - Display 10

Figure 5.16 – Role History – Certification History

6

◆ ◆ ◆ CHAPTER 6

Chapter 6: Identity Certification

Sun Role Manager is the Industry leading solution that provides enterprise level certifications of user entitlements, role content and application access. It supports periodic certification of user entitlements (access) by business managers, role owners and application owners. Sun Role Manager also supports granular certifications – to support systems that have complex security models for authorization.

Sun Role Manager includes a robust and fully customizable glossary feature, which helps translate cryptic access permissions into business friendly terms. Certifications in progress and completed certifications can be viewed under the Compliance dashboard, enabling auditing analysts to view reports of certified certifications.

The Identity Certification module includes a configurable workflow functionality which has the ability to send reminder notices and escalations to various actors designated to be a part of the certification process. This is more of an administrator level function and has been explained in detail in the *Sun Role Manager 4.1 Administrators Guide.*

This powerful Identity Certification module is extended in Sun Role Manager 4.1 to provide the ability to perform certifications at the instance or server level of a resource, provides advanced drill down capabilities for users, and advanced filtering and searching capabilities on the certification interface.

The Identity Certification module has three Certification types:

1) User Access Certification: Allows certifier to certify Role Membership and User Entitlements

2) Role Entitlement Certification: Allows certifier to certify roles and role content

3) Application Owner Certification: Allows certifier to certify entitlements pertaining to an application narrowed down by each instance of the application

Understanding the Actors

The Identity Certification module in Sun Role Manager assists various personnel in an organization to review and certify user entitlement data, role content data and application access data, which further assists in cleaning up entitlement access and ensures that users have access to the correct entitlements across various target systems. It is important to understand the various actors that are a part of the Identity Certification process, as described in the table below:

Actor Name	Description	Identity Certification Type
Certifier	Generic term representing personnel responsible for reviewing and completing any kind of certification	User Access Certification, Role Entitlement Certification, Application Certification
User Manager	An employee's direct "reports to" manager	User Access Certification
Access Reviewer	Designated personnel responsible for reviewing user access	User Access Certification, Application Certification
Application Owner	Designated personnel (usually) responsible for reviewing a users access in a particular target system by endpoint or domain	Application Certification
Role Owner	Designated personnel (usually) responsible for reviewing role and its content	Role Entitlement
Sun Role Manager Administrator	Administrator with full access to the Sun Role Manager application; has the ability to create and view progress of all certifications	User Access Certification, Role Entitlement Certification, Application Certification
Certification Administrator	Limited access to the Sun Role Manager application; has the ability to create and view progress of all certifications only	User Access Certification, Role Entitlement Certification, Application Certification
Audit Analyst/Auditor	Accesses the Identity Certification Dashboards to view progress of each certification and view reports of completed certifications	Identity Certification Dashboard

Identity Certification Dashboard

The Identity Certification Dashboard provides a single view for statistical information regarding certifications. The dashboard provides panels for:

1. Bar graph representation of the number of new, in progress, complete and expired certifications for each of the three types of certification (user access, role entitlement and application owner)

2. A summary of the total number of users, accounts, namespaces and endpoints involved in the certification process

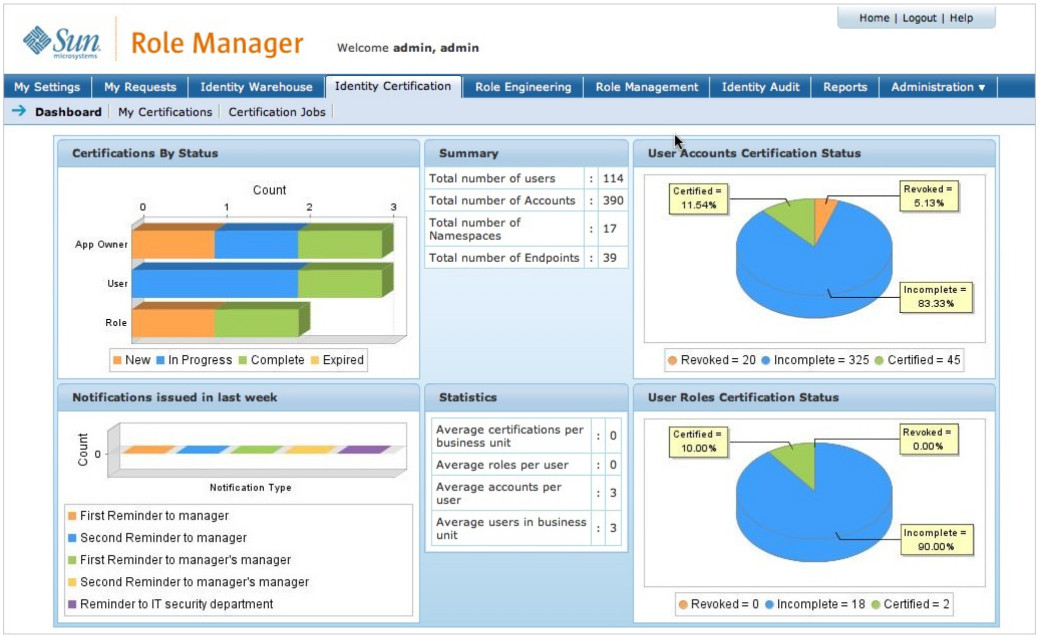
3. A pie chart representation of the certified, revoked and incomplete certification of accounts in User Account Certifications

4. A pie chart representation of the certified, revoked and incomplete certification of roles in the Role Entitlement certifications

5. A listing of the average number of certifications per business unit, roles per user, accounts per user and users in business units

6. A graph representing the notifications issued in the last week

The dashboard can be great tool for monitoring the certification progress.



Summary

Total number of users	:	114
Total number of Accounts	:	390
Total number of Namespaces	:	17
Total number of Endpoints	:	39

Statistics

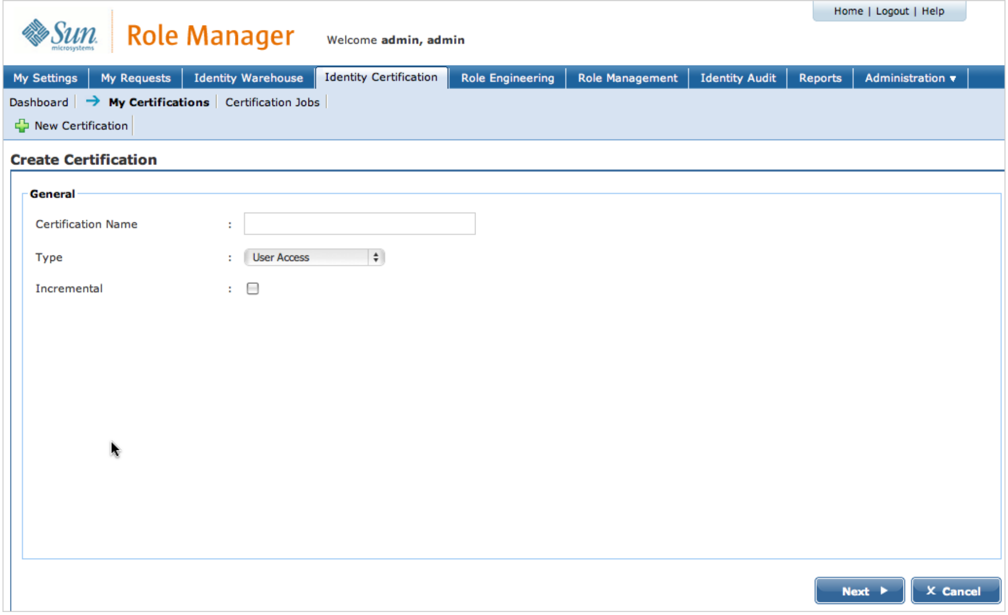
Average certifications per business unit	:	0
Average roles per user	:	0
Average accounts per user	:	3
Average users in business unit	:	3

Figure 6.1 – Identity Certification Dashboard

New Identity Certification

▼ Steps to Create a New Identity Certification Job

1. Log into the Sun Role Manager Web-Interface using a Java-enabled web browser
2. Log in with credentials of administrator or business units manager
3. Select the My Certifications Tab under Identity Certification Tab
4. Click New Certification
5. The Create Certification window opens. Fill in the Certification Name. Select the type of certification to be created from User Access, Role Entitlement and Application Owner. To create an incremental Certification select the Checkbox for Incremental. Select Next



Create Certification

General

Certification Name :

Type : User Access

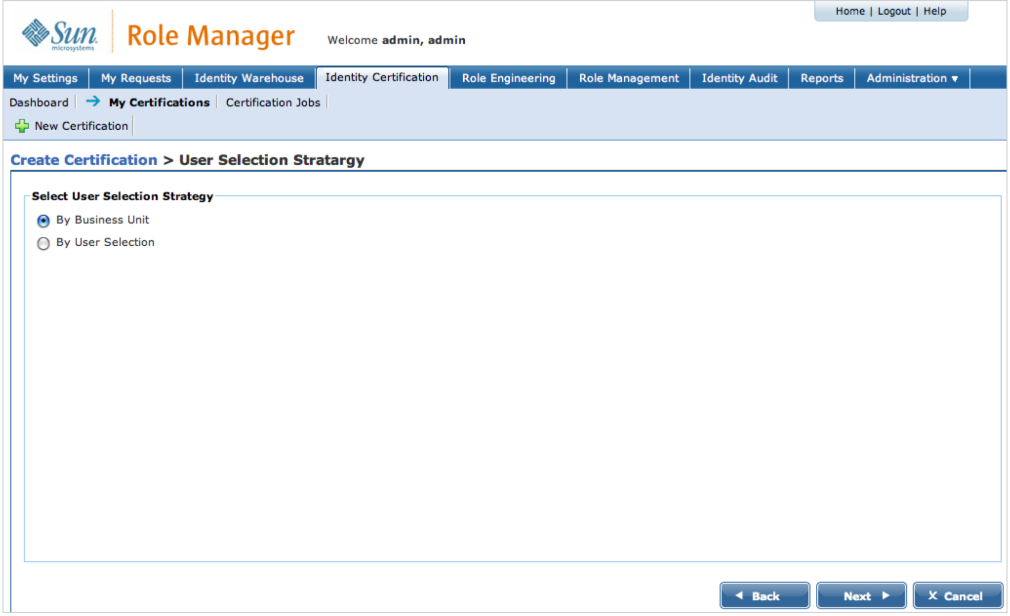
Incremental : □

Figure 6.2 – New Certification

6. Select the User Selection Strategy. This step is applicable only if the type of certification is

selected as “User Access”. For Role Entitlement and Application Owner Certification type User selection is done on the basis of Business units. For User Access certifications there is the option of doing a custom user selection

7. For Role Entitlement Certifications, Application Owner Certifications and User Access certifications where User Selection Strategy is selected as “By Business Unit” the Business Unit Selection window opens. Click Add Business Unit(s) button to add business units for user selection



Create Certification > User Selection Stratargy

Select User Selection Strategy

● By Business Unit

○ By User Selection

Figure 6.3 – New Certification – User Selection Strategy

8. The Select Business Unit(s) window opens up. Drill down into business units to select the business unit for selecting users. To select a business unit select the corresponding checkbox(s) and click “Ok”

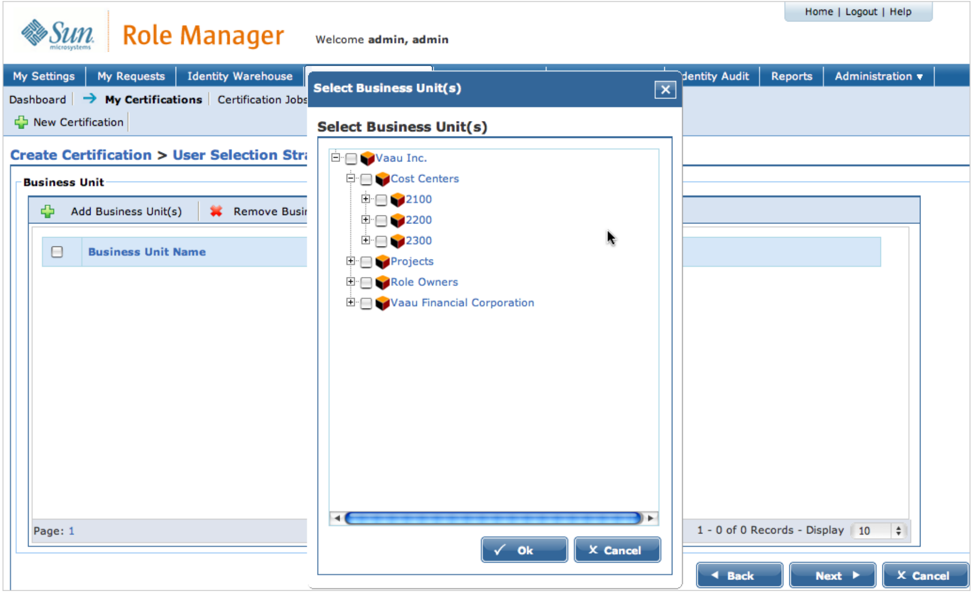
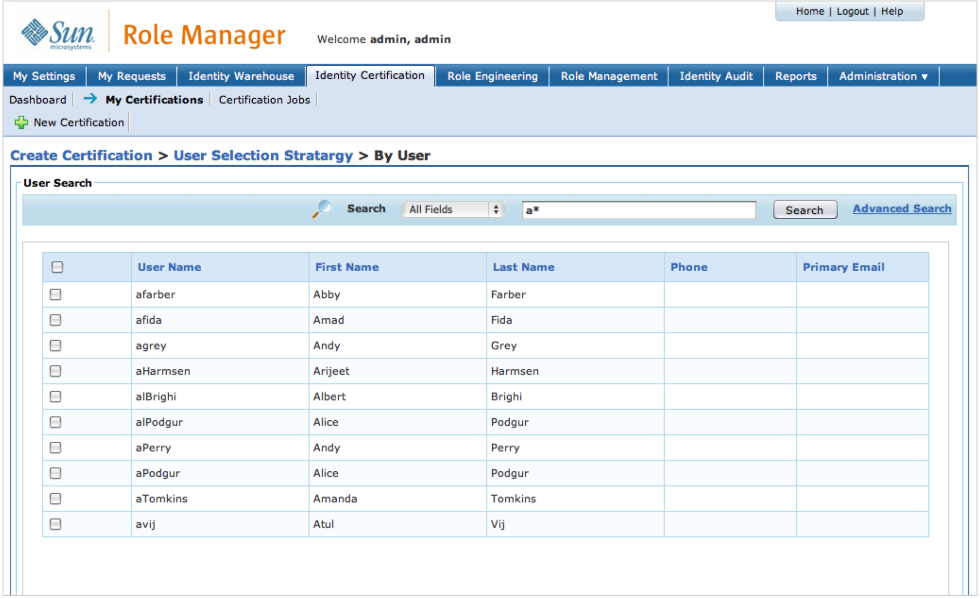


Figure 6.4 – New Certification – User Selection by Business Unit

9. Use the corresponding checkboxes and “Remove Business Units” button to remove business units. Select “Next”

10. If the certification type is “User Access” and the user selection strategy is “By User Selection” a user selection window opens up that allows users to be selected using the advanced user search or quicksearch capabilities. Select users for certification from the search result by using corresponding checkboxes. No users are included by default. Select “Next”



Create Certification > User Selection Stratargy > By User

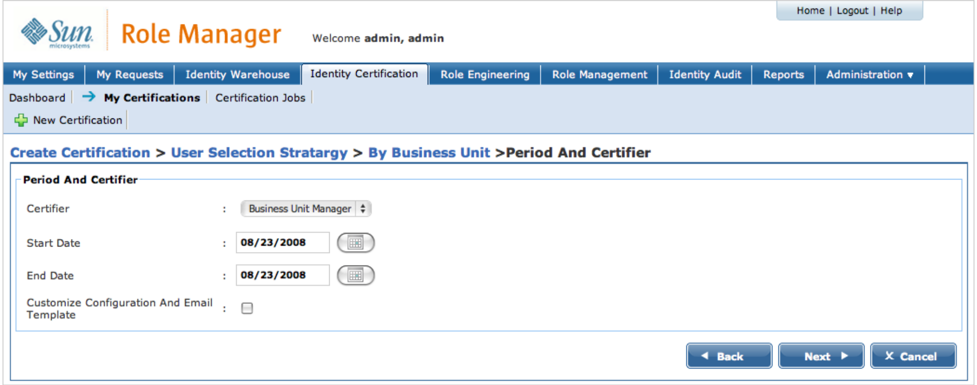
User Search

Search: All Fields; a*

□	User Name	First Name	Last Name	Phone	Primary Email
□	afarber	Abby	Farber		
□	afida	Amad	Fida		
□	agrey	Andy	Grey		
□	aHarmsen	Arijeet	Harmsen		
□	alBrighi	Albert	Brighi		
□	alPodgur	Alice	Podgur		
□	aPerry	Andy	Perry		
□	aPodgur	Alice	Podgur		
□	aTomkins	Amanda	Tomkins		
□	avij	Atul	Vij		

Figure 6.5 – New Certification – User Selection by User Search

11. The Period and Certifier window opens up. This window allows selecting the certifier, start and end dates, and customized configuration and email templates for the certification



Create Certification > User Selection Stratargy > By Business Unit >Period And Certifier

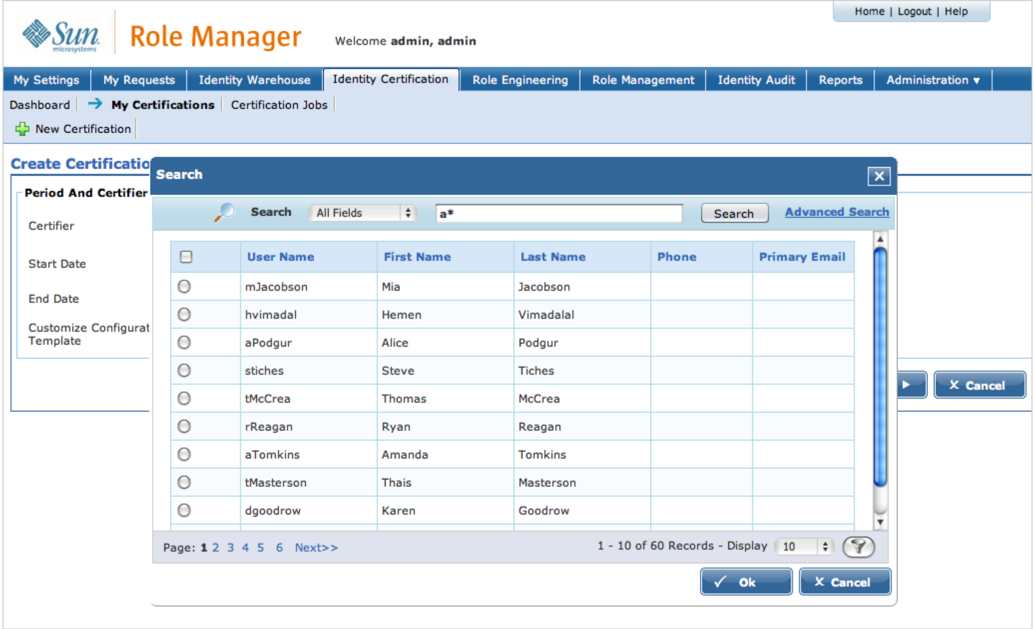
Period And Certifier

Certifier	:	Business Unit Manager
Start Date	:	08/23/2008
End Date	:	08/23/2008
Customize Configuration And Email Template	:	□

Figure 6.6 – New Certification – Period and Certifier

12. Certifier can be selected as the Business Unit Manager in which case a separate certification will be created for each distinct business unit in the user set selected for the certification

13. The “Select” option for certifier allows the use of the advanced user search and quicksearch capability to search for the global user that is to be selected as the certifier. Click the search button that appears when “Select” option is set for certifier



Search: All Fields a*

□	User Name	First Name	Last Name	Phone	Primary Email
○	mJacobson	Mia	Jacobson		
○	hvimadal	Hemen	Vimadalal		
○	aPodgur	Alice	Podgur		
○	stiches	Steve	Tiches		
○	tMcCrea	Thomas	McCrea		
○	rReagan	Ryan	Reagan		
○	aTomkins	Amanda	Tomkins		
○	tMasterson	Thais	Masterson		
○	dgoodrow	Karen	Goodrow		

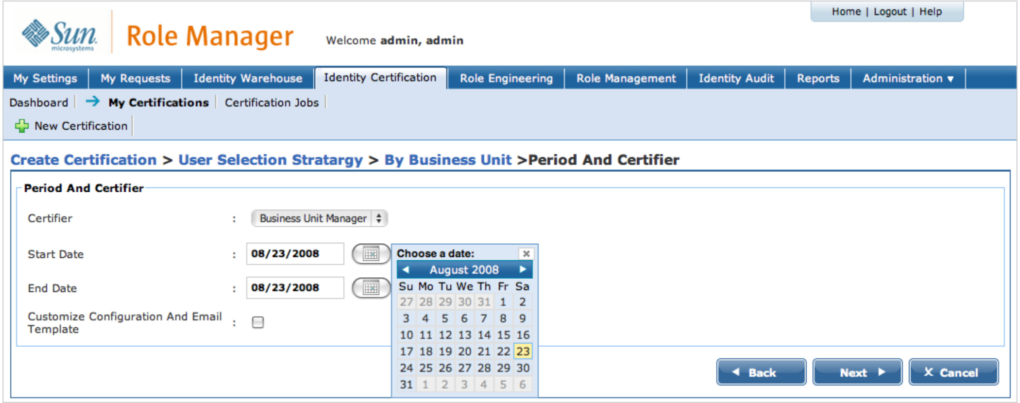
Page: 1 2 3 4 5 6 Next>>

1 - 10 of 60 Records - Display 10

Figure 6.7 – New Certification - Select Certifier by User Search

14. Select the User from the Search result that is to be selected as Certifier and click “Ok”

15. Sun Role Manager uses a customizable notification mechanism to send reminders and notifications to the various parties involved. The notifications are sent relative to the Start Date and End Date. End date should be set to give sufficient time to the certifier to complete the certification. Once the End date is passed the Certification is marked as “Expired” and cannot be edited or completed



Create Certification > User Selection Stratargy > By Business Unit >Period And Certifier

Period And Certifier

Certifier : Business Unit Manager

Start Date : 08/23/2008

End Date : 08/23/2008

Customize Configuration And Email Template : □

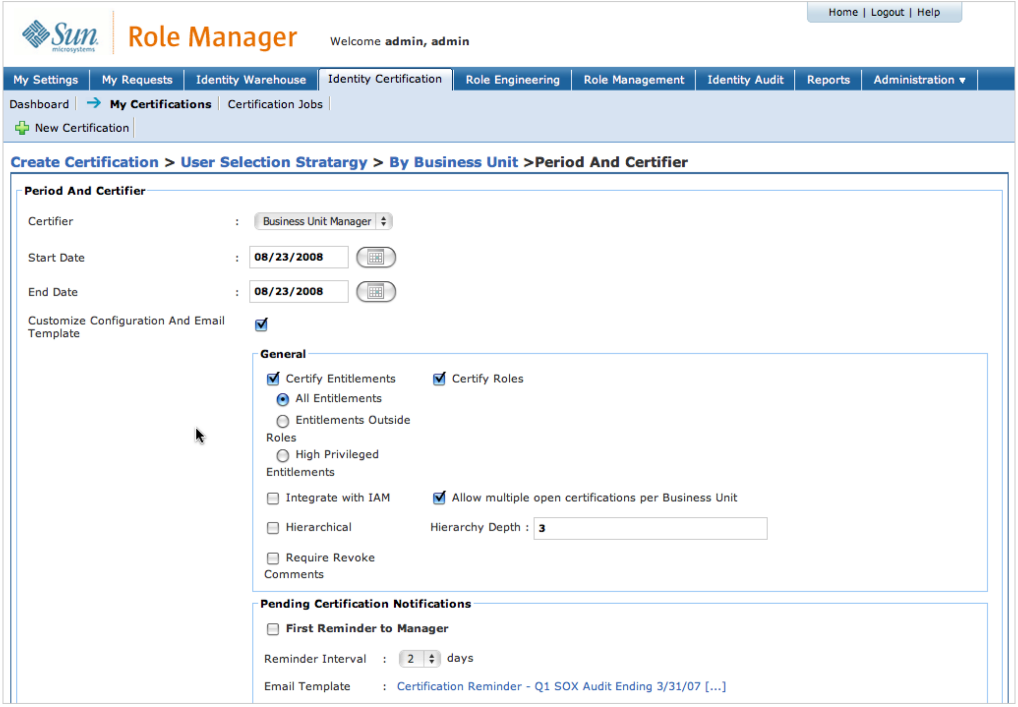
Choose a date:

August 2008

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Figure 6.8 – New Certification – Start and End Date

16. The general Identity Certification workflow is set by navigating to Configuration=>Identity Certification Tab. However each certification can be customized by setting these values. Select the checkbox for Customize Configuration and Email Template. For more information on these fields refer to the Identity Certification section in the chapter on Sun Role Manager – Configuration. Click “Next”



Create Certification > User Selection Stratargy > By Business Unit >Period And Certifier

Period And Certifier

Certifier : Business Unit Manager

Start Date : 08/23/2008

End Date : 08/23/2008

Customize Configuration And Email Template ☑

General

☑ Certify Entitlements ☑ Certify Roles

● All Entitlements

○ Entitlements Outside Roles

○ High Privileged Entitlements

☐ Integrate with IAM ☑ Allow multiple open certifications per Business Unit

☐ Hierarchical Hierarchy Depth : 3

☐ Require Revoke Comments

Pending Certification Notifications

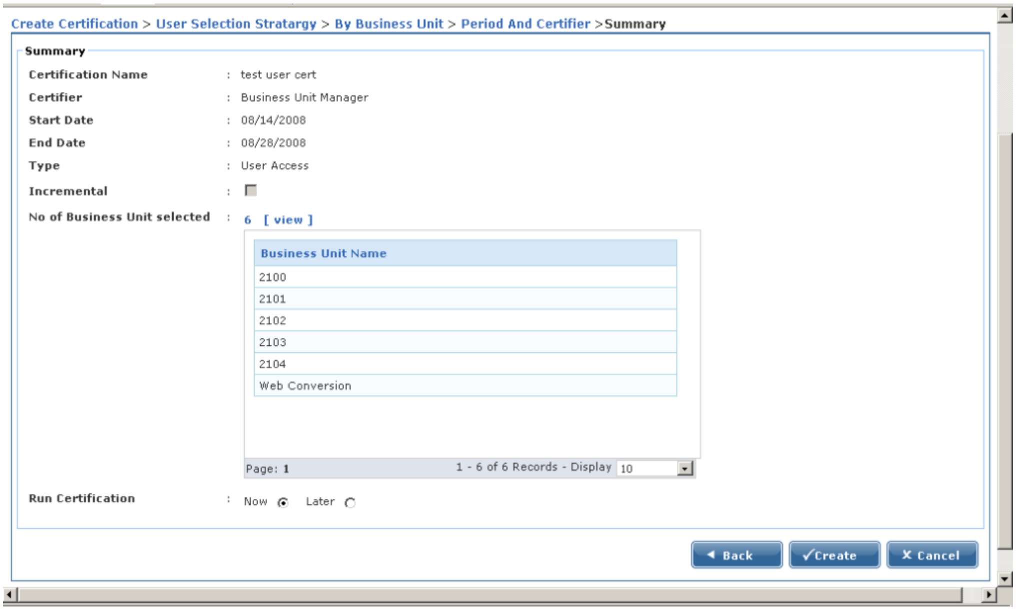
☐ **First Reminder to Manager**

Reminder Interval : 2 days

Email Template : Certification Reminder - Q1 SOX Audit Ending 3/31/07 [...]

Figure 6.9 – New Certification – Customized Configuration

17. The final configuration summary page opens. The certifier field will display the name of the user selected if the “Select” option was used and “Business Unit Manager” if business unit manager option was chosen. If user selection strategy used was “By Business Unit”, number of business units selected will be displayed. If user selection strategy used was “By User Selection”, the number of users selected will be displayed. Click the “view” button to view the names of business units or users



Create Certification > User Selection Stratargy > By Business Unit > Period And Certifier >Summary

Summary

Certification Name	:	test user cert
Certifier	:	Business Unit Manager
Start Date	:	08/14/2008
End Date	:	08/28/2008
Type	:	User Access
Incremental	:	□
No of Business Unit selected	:	6 [view]

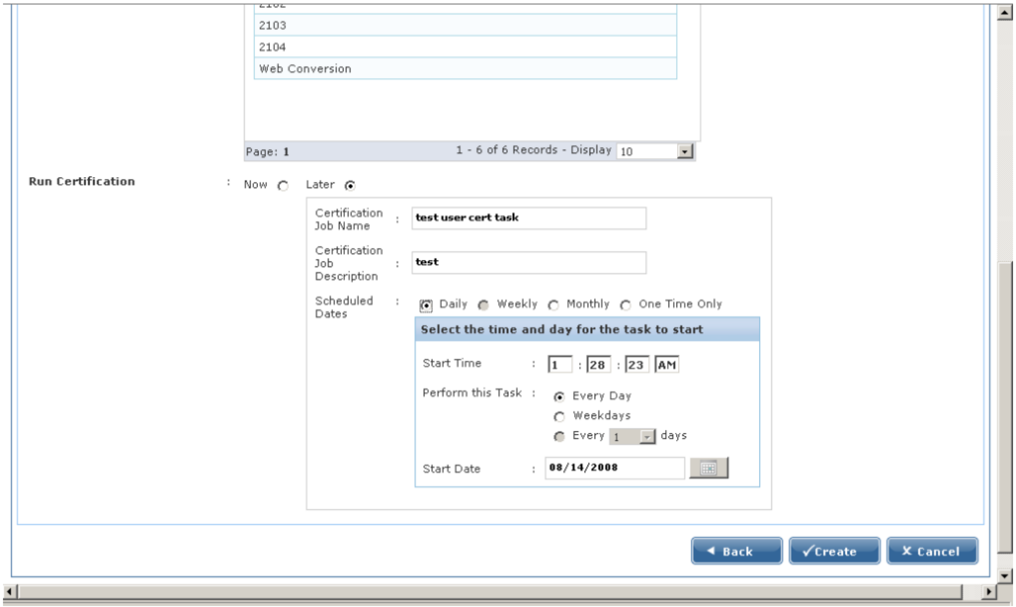
Business Unit Name
2100
2101
2102
2103
2104
Web Conversion

Page: 1 1 - 6 of 6 Records - Display 10

Run Certification : Now ● Later ○

Figure 6.10 – New Certification - Summary

18. There are two options for running the certification. It can be run at the current instant by selecting “Now” for Run Certification field, or it can be scheduled as a daily, weekly, monthly or one time task to be run at any particular data/time. Select “Later” to schedule a task. A new panel opens up for the scheduler. Select a name and description for the scheduled task. Select the type of the task and the corresponding fields



2103

2104

Web Conversion

Page: 1 1 - 6 of 6 Records - Display 10

Run Certification : Now ○ Later ●

Certification Job Name : test user cert task

Certification Job Description : test

Scheduled Dates : ● Daily ○ Weekly ○ Monthly ○ One Time Only

Select the time and day for the task to start

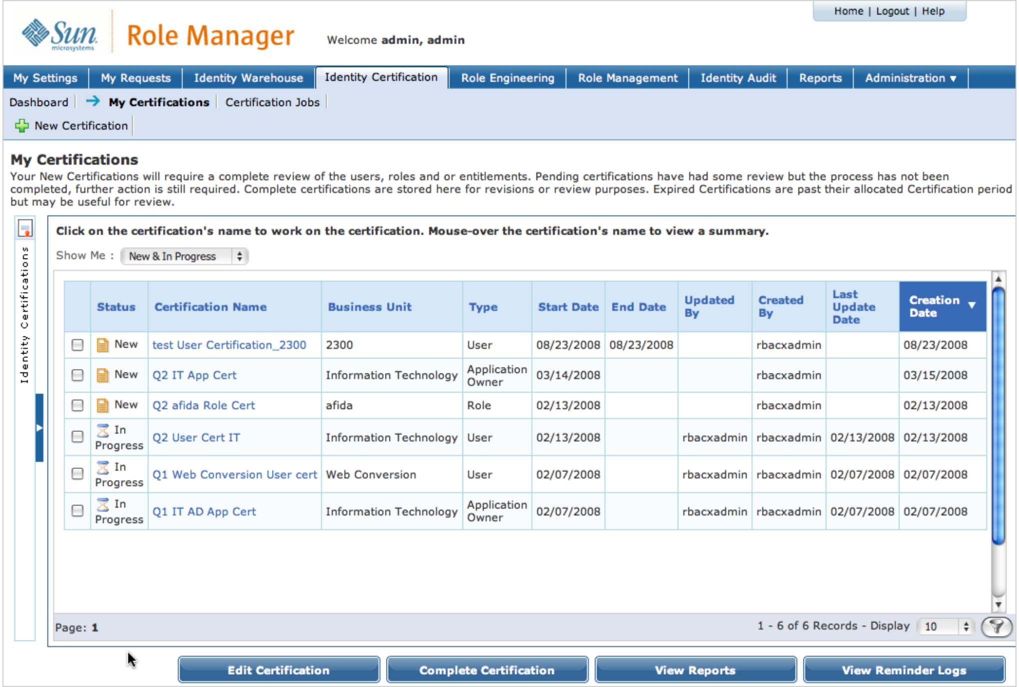
Start Time : 1 : 28 : 23 AM

Perform this Task : ● Every Day ○ Weekdays ○ Every 1 days

Start Date : 08/14/2008

Figure 6.11 – New Certification – Run Later

19. Select “Create” to create the certification



My Certifications

Your New Certifications will require a complete review of the users, roles and or entitlements. Pending certifications have had some review but the process has not been completed, further action is still required. Complete certifications are stored here for revisions or review purposes. Expired Certifications are past their allocated Certification period but may be useful for review.

Click on the certification's name to work on the certification. Mouse-over the certification's name to view a summary.

	Status	Certification Name	Business Unit	Type	Start Date	End Date	Updated By	Created By	Last Update Date	Creation Date ▾
□	New	test User Certification_2300	2300	User	08/23/2008	08/23/2008		rbacxadmin		08/23/2008
□	New	Q2 IT App Cert	Information Technology	Application Owner	03/14/2008			rbacxadmin		03/15/2008
□	New	Q2 afida Role Cert	afida	Role	02/13/2008			rbacxadmin		02/13/2008
□	In Progress	Q2 User Cert IT	Information Technology	User	02/13/2008		rbacxadmin	rbacxadmin	02/13/2008	02/13/2008
□	In Progress	Q1 Web Conversion User cert	Web Conversion	User	02/07/2008		rbacxadmin	rbacxadmin	02/07/2008	02/07/2008
□	In Progress	Q1 IT AD App Cert	Information Technology	Application Owner	02/07/2008		rbacxadmin	rbacxadmin	02/07/2008	02/07/2008

Figure 6.12 – New Certification – Created Certification

20. The Certification Jobs window opens and displays the new task created

21. The created certification Jobs can be viewed from the “Certification Jobs” view. When a job is run using the “Run now” or schedule features it will be available in the certifier’s “My Certifications” view

View and Search Certifications

The “My Certifications” view under the “Identity Certifications” Tab provides the main interface in Sun Role Manager to view and access certifications. By default the view shows New and In Progress certifications. Filters are provided to view All or any combination of New, In Progress, Complete and Expired certifications. For further precision a certification search capability is provided that can be used in conjunction with the filters to quickly search for a certification

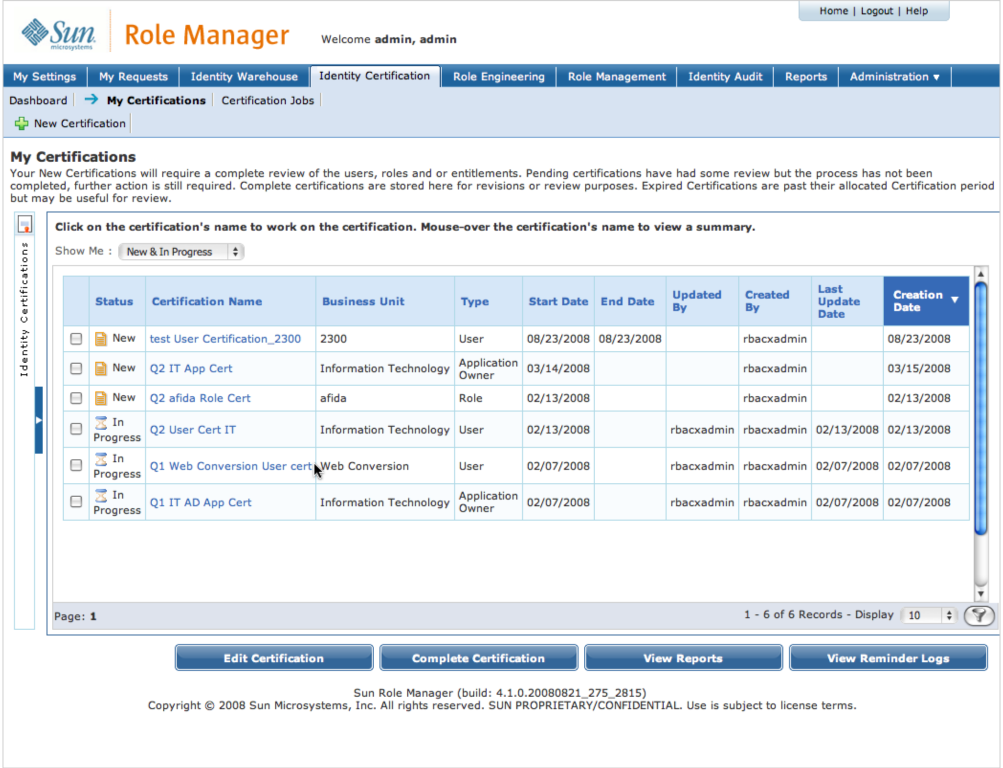
▼ Steps to Search and View Certifications

1. Log into the Sun Role Manager Web-Interface using a Java-enabled web browser

2. Log in with credentials of administrator or certifier

3. Select the My Certifications Tab under Identity Certification Tab

4. New and In Progress Certifications are available for view by default. This is also indicated by the selected value in the drop down option “Show Me”



My Certifications

Your New Certifications will require a complete review of the users, roles and or entitlements. Pending certifications have had some review but the process has not been completed, further action is still required. Complete certifications are stored here for revisions or review purposes. Expired Certifications are past their allocated Certification period but may be useful for review.

Click on the certification's name to work on the certification. Mouse-over the certification's name to view a summary.

Show Me : New & In Progress

	Status	Certification Name	Business Unit	Type	Start Date	End Date	Updated By	Created By	Last Update Date	Creation Date ▾
□	New	test User Certification_2300	2300	User	08/23/2008	08/23/2008		rbacxadmin		08/23/2008
□	New	Q2 IT App Cert	Information Technology	Application Owner	03/14/2008			rbacxadmin		03/15/2008
□	New	Q2 afida Role Cert	afida	Role	02/13/2008			rbacxadmin		02/13/2008
□	In Progress	Q2 User Cert IT	Information Technology	User	02/13/2008		rbacxadmin	rbacxadmin	02/13/2008	02/13/2008
□	In Progress	Q1 Web Conversion User cert	Web Conversion	User	02/07/2008		rbacxadmin	rbacxadmin	02/07/2008	02/07/2008
□	In Progress	Q1 IT AD App Cert	Information Technology	Application Owner	02/07/2008		rbacxadmin	rbacxadmin	02/07/2008	02/07/2008

Page: 1

1 - 6 of 6 Records - Display 10

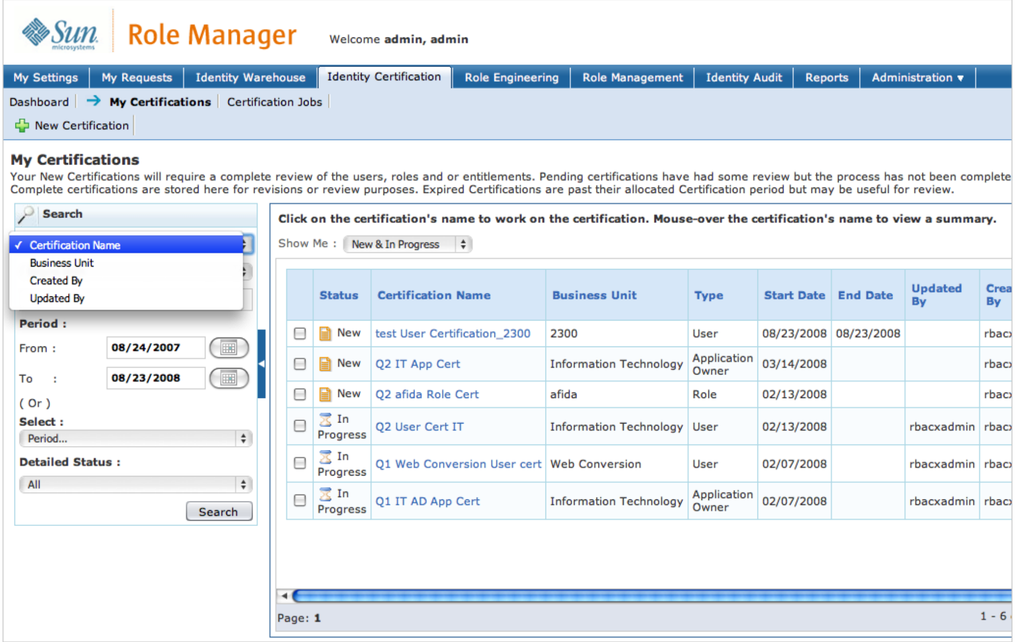
Sun Role Manager (build: 4.1.0.20080821_275_2815)

Copyright © 2008 Sun Microsystems, Inc. All rights reserved. SUN PROPRIETARY/CONFIDENTIAL. Use is subject to license terms.

Figure 6.13 – Certifications View

5. Select the appropriate value in the drop down option “Show Me” to get the desired certifications view

6. The Search panel can accessed by clicking the expand icon. Use the Search panel to search within the current certification view. Search can be done on Certification Name, Business Unit, Created By and Updated By fields. Search conditions can be created using Begins With, Ends With, Contains, Equals To, Does Not Contain. More restrictions can be imposed on the search criterion by selecting a period in which to search for the certification



My Certifications

Your New Certifications will require a complete review of the users, roles and or entitlements. Pending certifications have had some review but the process has not been complete Complete certifications are stored here for revisions or review purposes. Expired Certifications are past their allocated Certification period but may be useful for review.

Period :

From : 08/24/2007

To : 08/23/2008

(Or)

Select : Period...

Detailed Status : All

Click on the certification's name to work on the certification. Mouse-over the certification's name to view a summary.

Show Me : New & In Progress

	Status	Certification Name	Business Unit	Type	Start Date	End Date	Updated By	Crea By
☐	New	test User Certification_2300	2300	User	08/23/2008	08/23/2008		rbac
☐	New	Q2 IT App Cert	Information Technology	Application Owner	03/14/2008			rbac
☐	New	Q2 afida Role Cert	afida	Role	02/13/2008			rbac
☐	In Progress	Q2 User Cert IT	Information Technology	User	02/13/2008		rbacxadmin	rbac
☐	In Progress	Q1 Web Conversion User cert	Web Conversion	User	02/07/2008		rbacxadmin	rbac
☐	In Progress	Q1 IT AD App Cert	Information Technology	Application Owner	02/07/2008		rbacxadmin	rbac

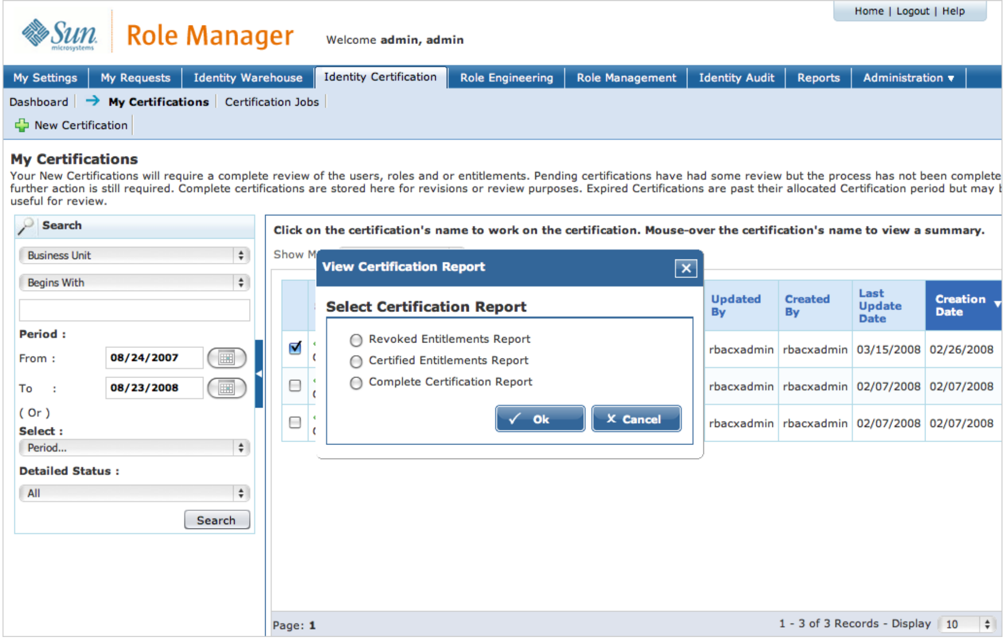
Page: 1 1 - 6

Figure 6.14 – Certification Search

7. To select a certification for viewing progress or performing verification actions click the Certification Name or use the checkbox to select the certification and click “Edit Certification”

8. To complete a certification whose attestation actions have been done select the certification using its corresponding checkbox and click “Complete Certification”

9. To view reports for a complete, in progress or expired certification select the corresponding checkbox and click “View Reports”. Sun Role Manager allows reports to be viewed for in progress certifications. This gives the flexibility of not having to wait till a potentially lengthy certification completes before reports can be viewed or exported. A “View Certification Report” box opens up which lists the reports available for the particular certification



My Certifications

Your New Certifications will require a complete review of the users, roles and or entitlements. Pending certifications have had some review but the process has not been complete further action is still required. Complete certifications are stored here for revisions or review purposes. Expired Certifications are past their allocated Certification period but may b useful for review.

Business Unit

Begins With

Period :

From : 08/24/2007

To : 08/23/2008

(Or)

Select : Period...

Detailed Status : All

Click on the certification's name to work on the certification. Mouse-over the certification's name to view a summary.

Select Certification Report

○ Revoked Entitlements Report
○ Certified Entitlements Report
○ Complete Certification Report

	Updated By	Created By	Last Update Date	Creation Date
☑	rbacxadmin	rbacxadmin	03/15/2008	02/26/2008
□	rbacxadmin	rbacxadmin	02/07/2008	02/07/2008
□	rbacxadmin	rbacxadmin	02/07/2008	02/07/2008

Page: 1

1 - 3 of 3 Records - Display 10

Figure 6.15 – Certification Reports

10. Select the type of report that is to be viewed and click “Ok”

11. To view the reminder logs for a certification select the corresponding checkbox and click “View Reminder Logs”

The following modules provide instructions for certifiers (User Managers, Role Owners and Application Owners) to sign off the different types of Certifications.

Completing a User Access Certification

This sub-section describes how to sign off a user access certification for attestation and reporting purposes. User Access Certification in Role Manager is a two step process.

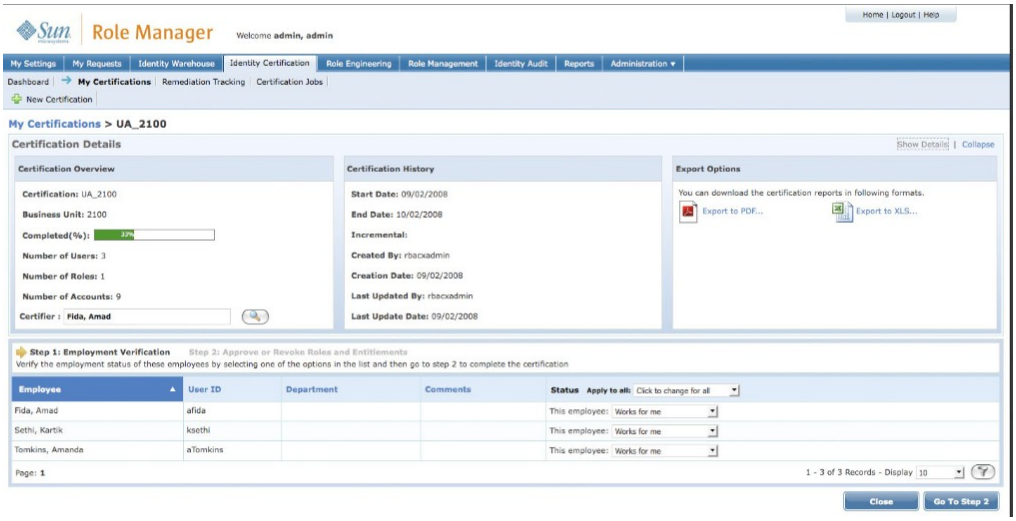
- Step 1: Employment Verification. This step entails confirming or denying whether the certifier is responsible for the accesses of the user being certified. Various options such as 'Terminated', 'Does not work for me' and 'Works for someone else' can be used for reporting an incorrect access. Indicating an incorrect access at step1 completes the certification process for the user. If 'Works for me' option is selected then step two of the certification process must be completed

- Step2: Approve or Revoke Roles and Entitlements. This step must be undertaken for each user who is verified as “Works for me” by the certifier. Step2 entails certifying or revoking all the accesses granted to a user. This includes Roles as well as entitlements outside roles.

Sun Role Manager provides flexibility for the certifier in completing the certification process. Step1 can be can be completed for as many users as desired before going to Step2. The certifier may opt to complete Step1 for all users and then complete Step2 for all users verified as “Works for me” or the certifier may verify a user in Step1 and then go to Step2 to complete the certification for the user. Irrespective of the approach taken Step2 displays all the users that have been verified by the certifier as “Works for me”

▼ Steps to Complete a User Access Certification

1. Log into the Sun Role Manager Web-Interface using a Java-enabled web browser
2. Log in with credentials of administrator or certifier
3. Click Identity Certification tab
4. Click My Certifications
5. Click the New or In-Progress Certification or search for the required certification using the “Show Me” option and certification search feature
6. Select the Certification to complete by clicking on the Certification Name or selecting the corresponding checkbox and clicking “Edit Certification”
7. The page for the selected Certification opens. Select “Show Details” to view a brief summary of Certification Overview and Certification History, as well as options for exporting certification reports



Welcome **admin, admin**

My Certifications > UA_2100

Certification Details

Certification Overview

Certification: UA_2100

Business Unit: 2100

Completed(%): 33%

Number of Users: 3

Number of Roles: 1

Number of Accounts: 9

Certifier : Fida, Amad

Certification History

Start Date: 09/02/2008

End Date: 10/02/2008

Incremental:

Created By: rbacxadmin

Creation Date: 09/02/2008

Last Updated By: rbacxadmin

Last Update Date: 09/02/2008

Export Options

You can download the certification reports in following formats.

Step 1: Employment Verification Step 2: Approve or Revoke Roles and Entitlements

Verify the employment status of these employees by selecting one of the options in the list and then go to step 2 to complete the certification

Employee ▲	User ID	Department	Comments	Status Apply to all: Click to change for all
Fida, Amad	afida			This employee: Works for me
Sethi, Kartik	ksethi			This employee: Works for me
Tomkins, Amanda	aTomkins			This employee: Works for me

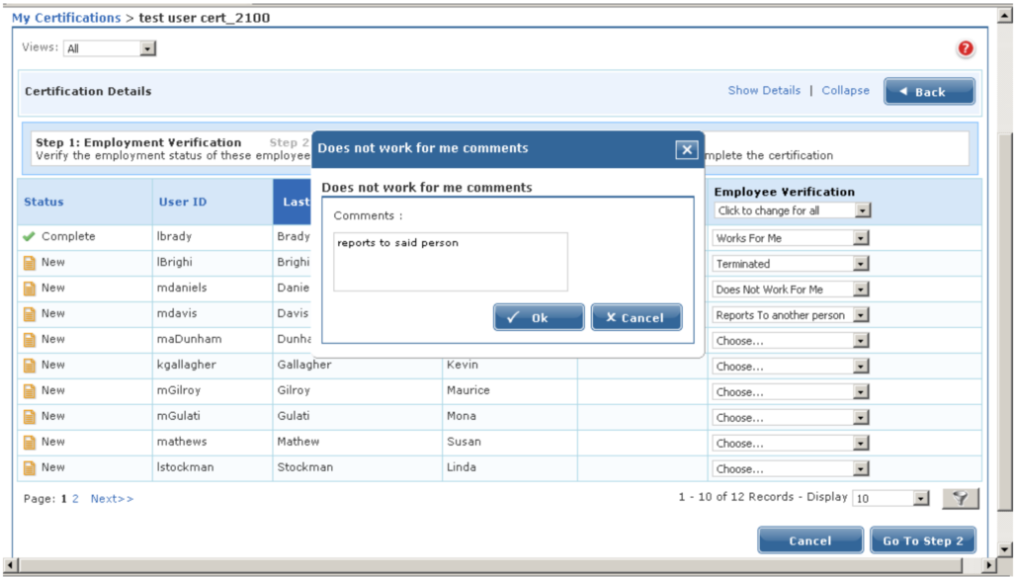
Page: 1 1 - 3 of 3 Records - Display 10

Figure 6.16 – Certification Details

Step 1

8. Complete Employee Verification . Select “Works for Me’, ‘Does Not Work for Me’, ‘Terminated’ or ‘Reports to Another Person’. “Click to change for all” can be used to change all the users to the same status. The ‘Does Not Work for Me’, ‘Terminated’ and ‘Reports to Another Person’ options prompt a corresponding comments box where further information can be provided.

9. The ‘Reports to Another Person’ option allows the selection of another Global User as the correct certifier for the user. This causes a new workflow where a new certification is created for the newly selected “Correct Certifier” to certify the particular user’s accesses. This new process will take place only if in the general Identity Certification configurations or in the custom configurations for the certification under consideration “Reporting Changes” and “Create New Certification per Reporting Manager” have been enabled. Refer to Sun Role Manager- Configuration => Identity Certification portion of Sun Role Manager 4.1 Admin Guide for more information on these settings. After filling in appropriate comment and clicking “Ok” a new window opens that allows use of the Advanced User Search or quicksearch feature to select a Global User as the appropriate certifying authority



My Certifications > test user cert_2100

Views: All

Certification Details — Show Details | Collapse — Back

Step 1: Employment Verification — Verify the employment status of these employee … Step 2 … mplete the certification

Does not work for me comments

Does not work for me comments

Comments :

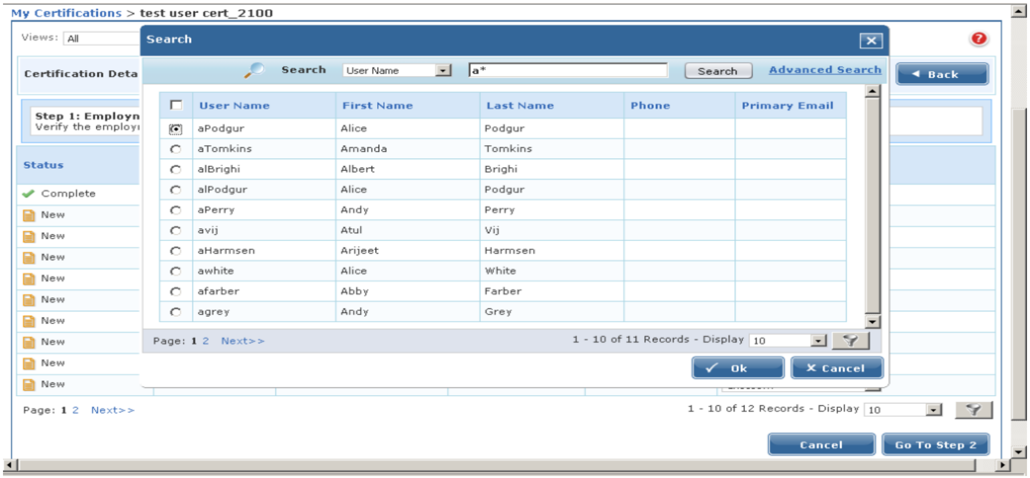
reports to said person

✓ Ok — ✗ Cancel

Status	User ID	Last			Employee Verification Click to change for all
✓ Complete	lbrady	Brady			Works For Me
New	lBrighi	Brighi			Terminated
New	mdaniels	Danie			Does Not Work For Me
New	mdavis	Davis			Reports To another person
New	maDunham	Dunha			Choose...
New	kgallagher	Gallagher	Kevin		Choose...
New	mGilroy	Gilroy	Maurice		Choose...
New	mGulati	Gulati	Mona		Choose...
New	mathews	Mathew	Susan		Choose...
New	lstockman	Stockman	Linda		Choose...

Page: 1 2 Next>> — 1 - 10 of 12 Records - Display 10

Cancel — Go To Step 2



My Certifications > test user cert_2100

Views: All

Search

Search: User Name — a* — Search — Advanced Search

☐	User Name	First Name	Last Name	Phone	Primary Email
●	aPodgur	Alice	Podgur		
○	aTomkins	Amanda	Tomkins		
○	alBrighi	Albert	Brighi		
○	alPodgur	Alice	Podgur		
○	aPerry	Andy	Perry		
○	avij	Atul	Vij		
○	aHarmsen	Arijeet	Harmsen		
○	awhite	Alice	White		
○	afarber	Abby	Farber		
○	agrey	Andy	Grey		

Page: 1 2 Next>> — 1 - 10 of 11 Records - Display 10

✓ Ok — ✗ Cancel

Certification Deta… — Back

Step 1: Employn… Verify the employ…

Status
✓ Complete
New
New
New
New
New
New
New
New
New

Page: 1 2 Next>> — 1 - 10 of 12 Records - Display 10

Cancel — Go To Step 2

Figure 6.17 – Employee Verification – Reports to Another Person

10. Selecting “Works For Me” makes the user eligible for review in Step2.

11. When one or more users have been verified by selecting “Works for me” and their roles and entitlements are to be certified select “Go To Step2”

Step 2

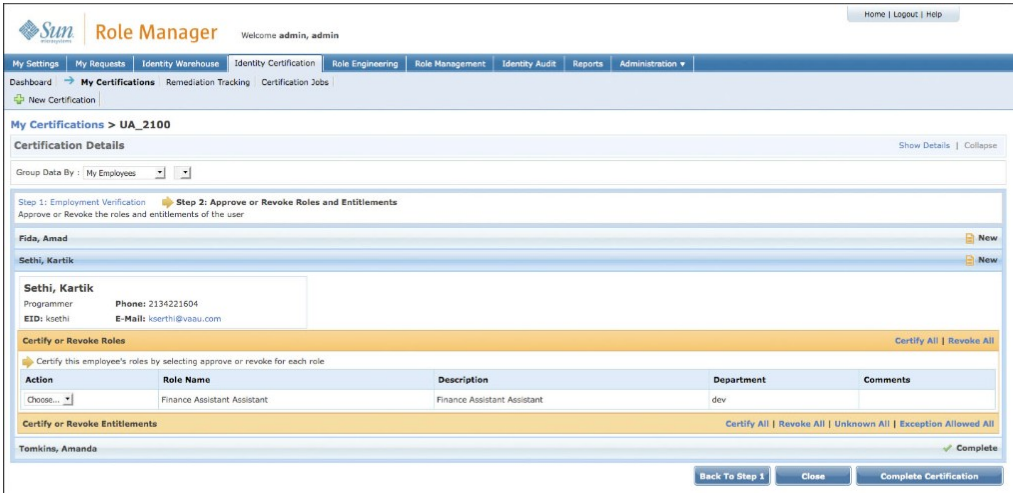
12. Complete the certification process for a user by certifying the roles and entitlements associated with the user. The “Group Data By” option can be used to filter the users to be certified based on various attributes such as 'location', 'Job Code', 'manager' etc.

Certify Roles

Once Roles have been defined for the Business Unit, Sun Role Manager can help your organization move to an attestation based on Roles. Business Unit managers would be responsible for certifying membership of Roles and Role Owners are responsible for role content.

13. Select the user to certify by clicking the name of the user

14. Select “Certify or Revoke Roles”. This will show all Roles associated to user



My Certifications > UA_2100

Certification Details

Group Data By : My Employees

Step 1: Employment Verification → Step 2: Approve or Revoke Roles and Entitlements
Approve or Revoke the roles and entitlements of the user

Fida, Amad — New

Sethi, Kartik — New

Sethi, Kartik
Programmer — Phone: 2134221604
EID: ksethi — E-Mail: kserthi@vaau.com

Certify or Revoke Roles

Certify this employee's roles by selecting approve or revoke for each role

Action	Role Name	Description	Department	Comments
Choose...	Finance Assistant Assistant	Finance Assistant Assistant	dev	

Certify or Revoke Entitlements

Tomkins, Amanda — ✓ Complete

Figure 6.18 – Certify or Revoke Roles

15. Click Certify/ Revoke on Role membership for the user.

Certify Access Outside Roles

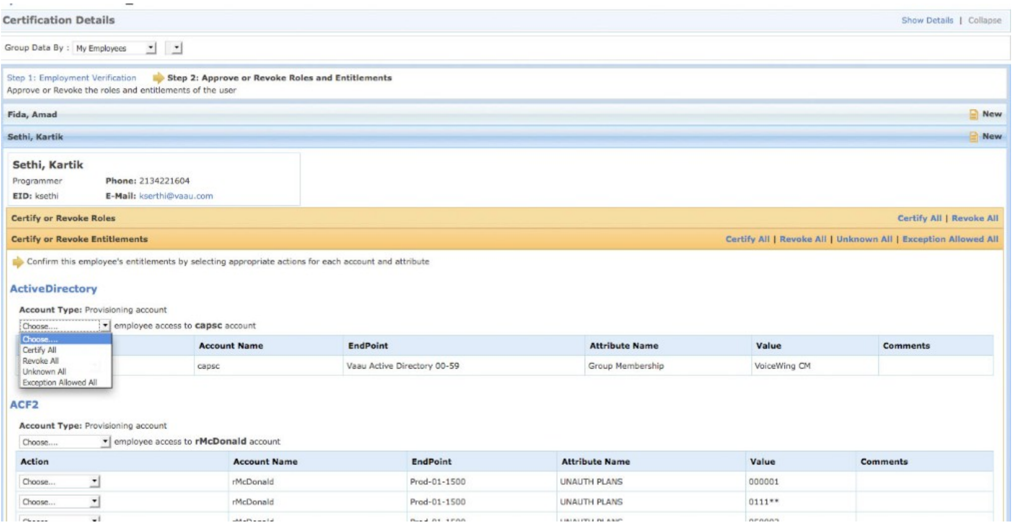
Sun Role Manager Identity Certification allows configuration of certifications that will show entitlements for each user that only lie outside a Role. This combined with the above **Certify by Role** completes a Role Based Access Attestation procedure. This allows an organization to identify and treat Actual versus Assigned access as an exception with high priority.

16. Select a User for certification. Select certify or revoke entitlements

17. This will list all the user's accounts in the various namespaces with detailed access permissions on each endpoint

18. The certification options at this stage are Certify, Revoke, Unknown and Exception allowed. Use Certify option to confirm valid access for the user. Use Revoke to revoke access for the user. Use Unknown when the accurate nature of the User's access is not known. Use Exception allowed to certify access to the user while acknowledging the undesirable or irregular nature of the access. These options can be used at 4 levels:

    a. Use the "All" option in the first 4 columns on this page to apply 'Certify', 'Revoke', 'Unknown' or 'Exception Allowed' across all attributes of all accounts of the user
    b. Use the checkboxes in the first 4 columns for individual accounts to apply 'Certify', 'Revoke', 'Unknown' or 'Exception Allowed' across all attributes of an individual account of the user
    c. Use the "All" option in the 4 columns under the "Attributes" field to apply 'Certify', 'Revoke', 'Unknown' or 'Exception Allowed' across all attribute values for an individual attribute of an single account of the user
    d. Use the individual checkboxes in the 4 columns to apply 'Certify', 'Revoke', 'Unknown' or 'Exception Allowed' for individual attribute values of a single attribute of an account of the user



Certification Details

Group Data By : My Employees

Step 1: Employment Verification

Step 2: Approve or Revoke Roles and Entitlements

Approve or Revoke the roles and entitlements of the user

Fida, Amad

Sethi, Kartik

Sethi, Kartik

Programmer

Phone: 2134221604

EID: ksethi

E-Mail: kserthi@vaau.com

Certify or Revoke Roles

Certify or Revoke Entitlements

Certify All | Revoke All | Unknown All | Exception Allowed All

Confirm this employee's entitlements by selecting appropriate actions for each account and attribute

ActiveDirectory

Account Type: Provisioning account

Choose.... employee access to **capsc** account

	Account Name	EndPoint	Attribute Name	Value	Comments
	capsc	Vaau Active Directory 00-59	Group Membership	VoiceWing CM	

ACF2

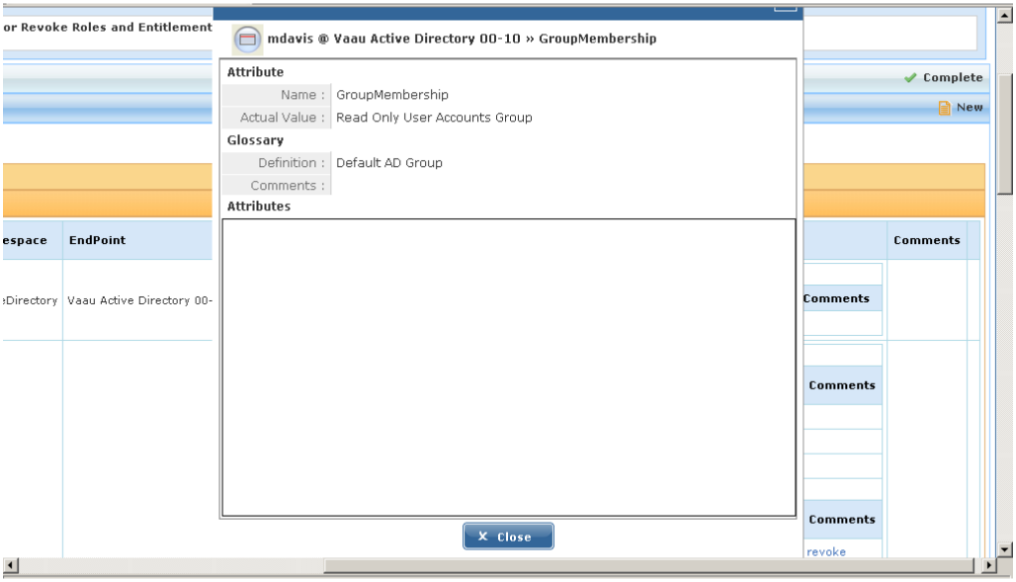
Account Type: Provisioning account

Choose.... employee access to **rMcDonald** account

Action	Account Name	EndPoint	Attribute Name	Value	Comments
Choose...	rMcDonald	Prod-01-1500	UNAUTH PLANS	000001	
Choose...	rMcDonald	Prod-01-1500	UNAUTH PLANS	0111**	

Figure 6.19 – Certify or Revoke Entitlements

19. Sun Role Manager provides a Glossary feature which translates the cryptic access entitlements into business friendly terms. Click the highlighted access entitlement (with hyperlink) to display the actual attribute value and its corresponding definition and comments



mdavis @ Vaau Active Directory 00-10 » GroupMembership

Attribute

Name : GroupMembership

Actual Value : Read Only User Accounts Group

Glossary

Definition : Default AD Group

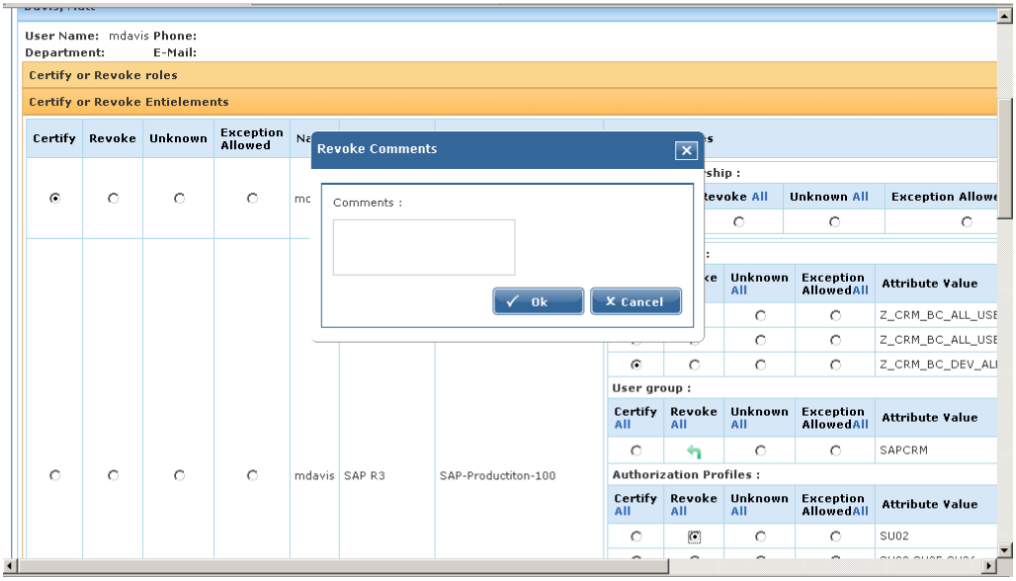
Comments :

Attributes

Figure 6.20 – Glossary Display in Certification

Revoking a Role or Access outside Role

20. To revoke any access whether it lies in a Role or Entitlement, select the Revoke radio button. This will bring up a comments field which must be filled for post certification (remediation) activities



User Name: mdavis Phone:
Department: E-Mail:

Certify or Revoke roles

Certify or Revoke Entielements

Certify	Revoke	Unknown	Exception Allowed	Na		
●	○	○	○	mc		
○	○	○	○	mdavis	SAP R3	SAP-Productiton-100

Revoke Comments

Comments :

ship :

Revoke All	Unknown All	Exception Allowe
○	○	○

ke	Unknown All	Exception AllowedAll	Attribute Value
	○	○	Z_CRM_BC_ALL_USE
	○	○	Z_CRM_BC_ALL_USE
○	○	○	Z_CRM_BC_DEV_ALI

User group :

Certify All	Revoke All	Unknown All	Exception AllowedAll	Attribute Value
○	↰	○	○	SAPCRM

Authorization Profiles :

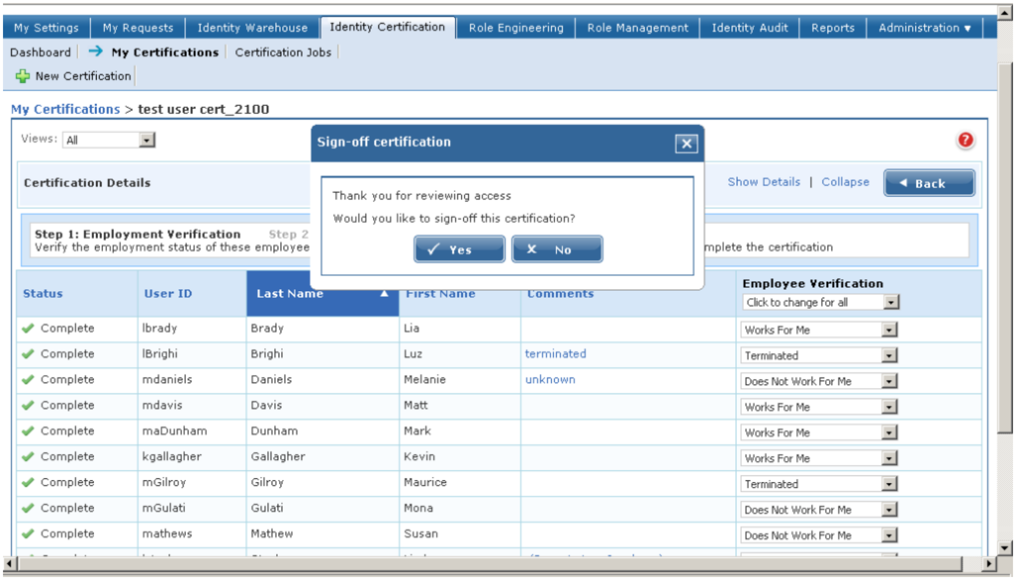
Certify All	Revoke All	Unknown All	Exception AllowedAll	Attribute Value
○	●	○	○	SU02

Figure 6.21 – Revoke Comments

Sign-off on Certification

Identity Certification supports a series of post certification activities which include reports, revoke emails and kicking off a workflow process if integrated with an IAM solution. To complete and sign off on a certification, complete the above steps to certify or revoke access for each user.

21. Complete attesting access of all users. Role Manager detects when a certification is completed and prompts for sign-off on the certification. Select “Yes” on the sign-off certification screen to sign-off certification



My Certifications > test user cert_2100

Views: All

Certification Details

Step 1: Employment Verification Step 2
Verify the employment status of these employee ... mplete the certification

Sign-off certification

Thank you for reviewing access

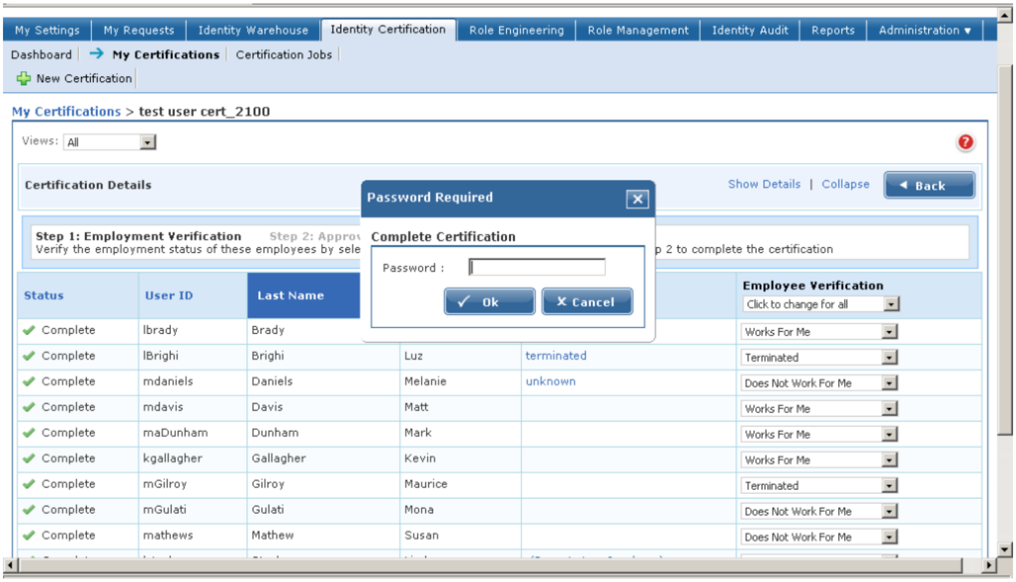
Would you like to sign-off this certification?

Status	User ID	Last Name ▲	First Name	Comments	Employee Verification Click to change for all
✓ Complete	lbrady	Brady	Lia		Works For Me
✓ Complete	lBrighi	Brighi	Luz	terminated	Terminated
✓ Complete	mdaniels	Daniels	Melanie	unknown	Does Not Work For Me
✓ Complete	mdavis	Davis	Matt		Works For Me
✓ Complete	maDunham	Dunham	Mark		Works For Me
✓ Complete	kgallagher	Gallagher	Kevin		Works For Me
✓ Complete	mGilroy	Gilroy	Maurice		Terminated
✓ Complete	mGulati	Gulati	Mona		Does Not Work For Me
✓ Complete	mathews	Mathew	Susan		Does Not Work For Me

Figure 6.22 – Sign-off Certification

22. To sign-off at a later instant use “Complete Certification” button

23. Enter your login password to secure your sign-off on this certification



My Certifications > test user cert_2100

Views: All

Certification Details

Step 1: Employment Verification Step 2: Approv
Verify the employment status of these employees by sele

p 2 to complete the certification

Complete Certification

Password :

Status	User ID	Last Name			Employee Verification Click to change for all
✓ Complete	lbrady	Brady			Works For Me
✓ Complete	lBrighi	Brighi	Luz	terminated	Terminated
✓ Complete	mdaniels	Daniels	Melanie	unknown	Does Not Work For Me
✓ Complete	mdavis	Davis	Matt		Works For Me
✓ Complete	maDunham	Dunham	Mark		Works For Me
✓ Complete	kgallagher	Gallagher	Kevin		Works For Me
✓ Complete	mGilroy	Gilroy	Maurice		Terminated
✓ Complete	mGulati	Gulati	Mona		Does Not Work For Me
✓ Complete	mathews	Mathew	Susan		Does Not Work For Me

Figure 6.23 – Sign-off Authorization

Completing a Role Entitlement Certification

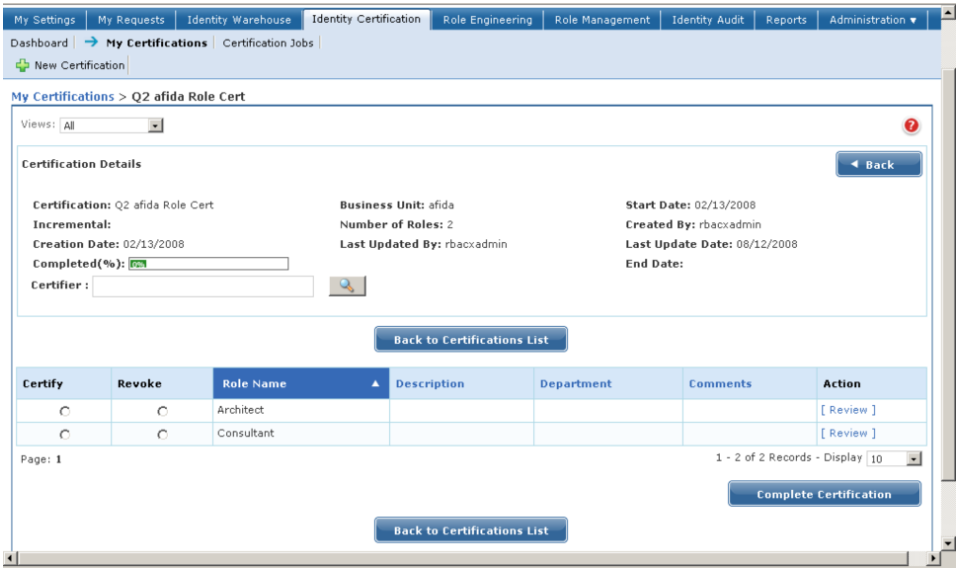
This sub-section describes how to sign off a role entitlement certification for attestation and reporting purposes.

▼ Steps to Complete a Role Entitlement Certification

1. Log into the Sun Role Manager Web-Interface using a Java-enabled web browser
2. Log in with credentials of administrator or certifier
3. Click Identity Certification tab
4. Click My Certifications
5. Click the New or In-Progress Certification or search for the required certification using

the “Show Me” drop down option

6. Select the Certification to complete by clicking on the Certification Name or using the corresponding checkbox and clicking “Edit Certification”



My Certifications > Q2 afida Role Cert

Views: All

Certification Details

Certification: Q2 afida Role Cert
Incremental:
Creation Date: 02/13/2008
Completed(%): 0%
Certifier :

Business Unit: afida
Number of Roles: 2
Last Updated By: rbacxadmin

Start Date: 02/13/2008
Created By: rbacxadmin
Last Update Date: 08/12/2008
End Date:

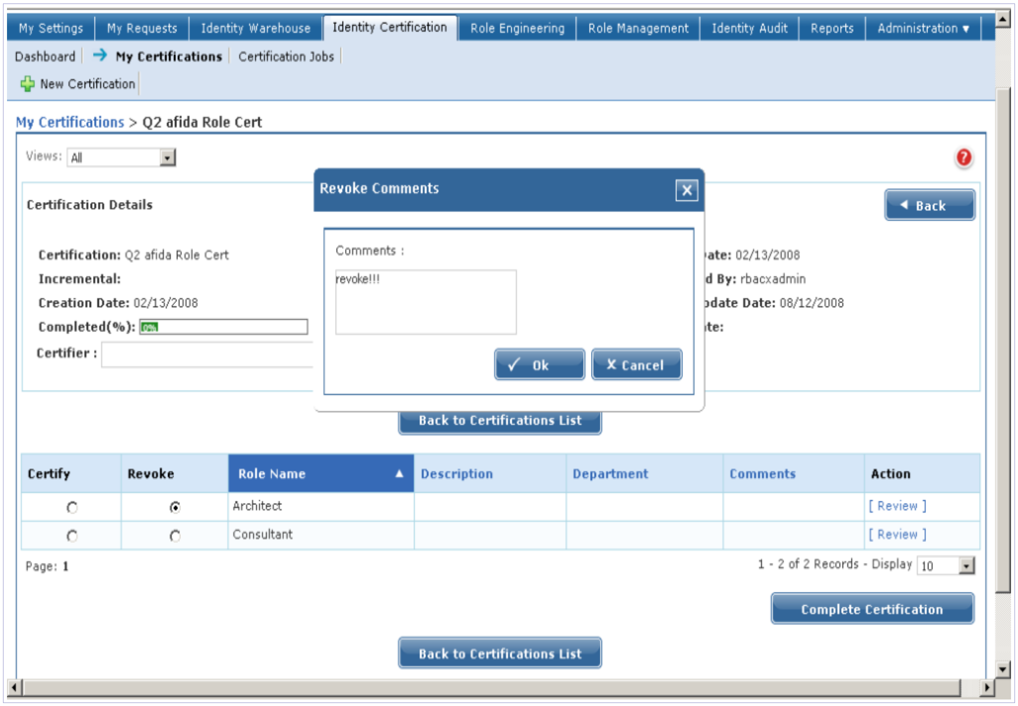
Certify	Revoke	Role Name ▲	Description	Department	Comments	Action
○	○	Architect				[Review]
○	○	Consultant				[Review]

Page: 1

1 - 2 of 2 Records - Display 10

Figure 6.24 – Select Certification

7. Click ‘Certify’ or ‘Revoke’ for each Role that the certifier is an owner for. Applying ‘Revoke’, ‘Unknown’ or ‘Exception Allowed’ to a role requires entering a comment to signify as to why the role should no longer belong under the certifier's ownership or if all its underlying entitlements are incorrect in case of “Revoke”



My Certifications > Q2 afida Role Cert

Views: All

Certification Details

Revoke Comments

Comments : revoke!!!

Certification: Q2 afida Role Cert
Incremental:
Creation Date: 02/13/2008
Completed(%): 0%
Certifier :

ate: 02/13/2008
d By: rbacxadmin
pdate Date: 08/12/2008
te:

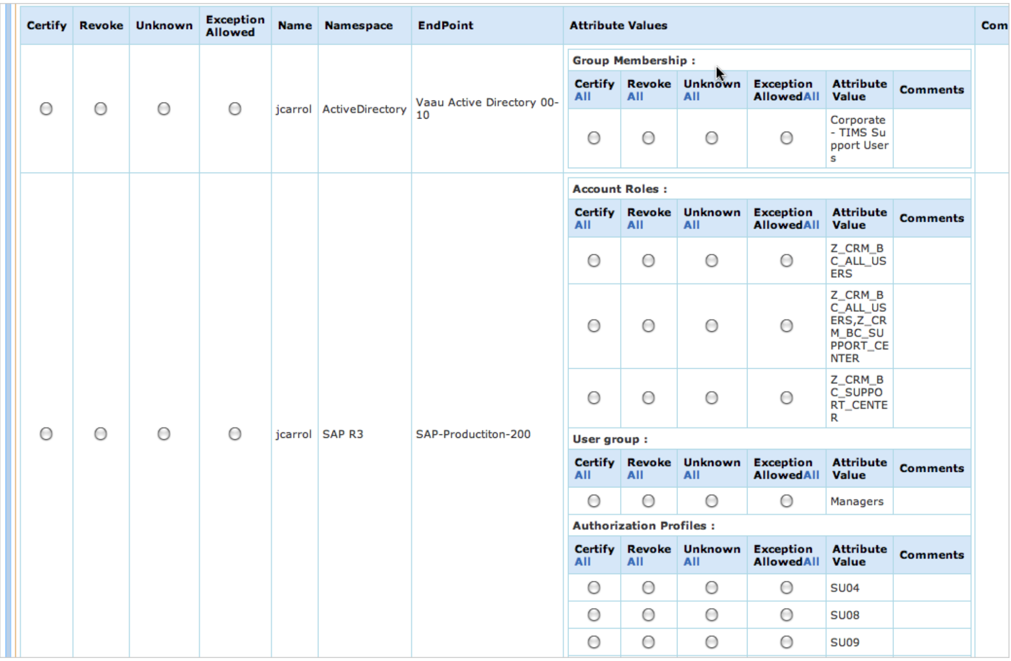
Certify	Revoke	Role Name ▲	Description	Department	Comments	Action
○	●	Architect				[Review]
○	○	Consultant				[Review]

Page: 1

1 - 2 of 2 Records - Display 10

Figure 6.25 – Revoke Comments

8. Click [Review] to review the Role Entitlements



Certify	Revoke	Unknown	Exception Allowed	Name	Namespace	EndPoint	Attribute Values	Com
○	○	○	○	jcarrol	ActiveDirectory	Vaau Active Directory 00-10	Group Membership :	
○	○	○	○	jcarrol	SAP R3	SAP-Productiton-200	Account Roles : User group : Authorization Profiles :	

Group Membership :

Certify All	Revoke All	Unknown All	Exception AllowedAll	Attribute Value	Comments
○	○	○	○	Corporate - TIMS Support Users	

Account Roles :

Certify All	Revoke All	Unknown All	Exception AllowedAll	Attribute Value	Comments
○	○	○	○	Z_CRM_BC_ALL_USERS	
○	○	○	○	Z_CRM_BC_ALL_USERS,Z_CRM_BC_SUPPORT_CENTER	
○	○	○	○	Z_CRM_BC_SUPPORT_CENTER	

User group :

Certify All	Revoke All	Unknown All	Exception AllowedAll	Attribute Value	Comments
○	○	○	○	Managers	

Authorization Profiles :

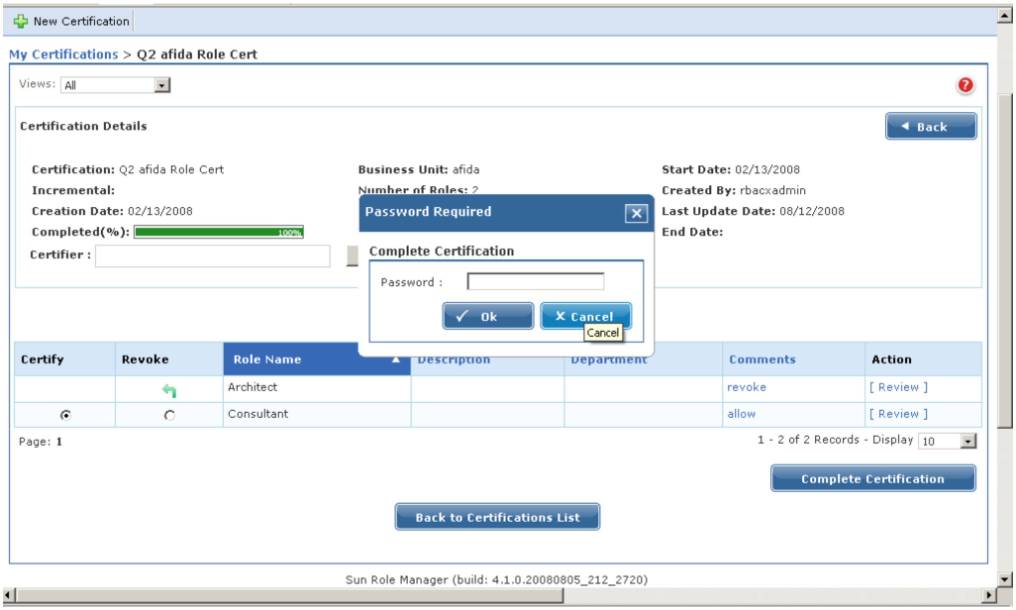
Certify All	Revoke All	Unknown All	Exception AllowedAll	Attribute Value	Comments
○	○	○	○	SU04	
○	○	○	○	SU08	
○	○	○	○	SU09	

Figure 6.26 – Review Role Entitlements

9. Assign ‘Certify’, ‘Revoke’, ‘Unknown’ or ‘Exception Allowed’ to sign off each attribute value within each policy that belongs to a particular role. Each policy can also be certified as a whole. Applying ‘Revoke’, ‘Unknown’ or ‘Exception Allowed’ to an attribute requires entering a comment to signify as to why the attribute/policy should no longer be associated with the role in case of “Revoke”, why the nature of the association of the attribute/policy is unknown in the case of “Unknown” and what is the exception and why is it being allowed in the case of “Exception Allowed”

10. If Sun Role Manager detects that all attestations have been completed a “Sign Off Certification” box appears. To complete certification at this point click “Ok”. Otherwise Complete attesting entitlements of all roles and then click Complete Certification

11. Enter your login password to secure your signoff on this certification



My Certifications > Q2 afida Role Cert

Views: All

Certification Details

Certification: Q2 afida Role Cert
Incremental:
Creation Date: 02/13/2008
Completed(%): 100%
Certifier :

Business Unit: afida
Number of Roles: 2

Start Date: 02/13/2008
Created By: rbacxadmin
Last Update Date: 08/12/2008
End Date:

Complete Certification

Password :

Certify	Revoke	Role Name	Description	Department	Comments	Action
	↰	Architect			revoke	[Review]
●	○	Consultant			allow	[Review]

Page: 1

1 - 2 of 2 Records - Display 10

Sun Role Manager (build: 4.1.0.20080805_212_2720)

Figure 6.27 – Sign-off Authorization

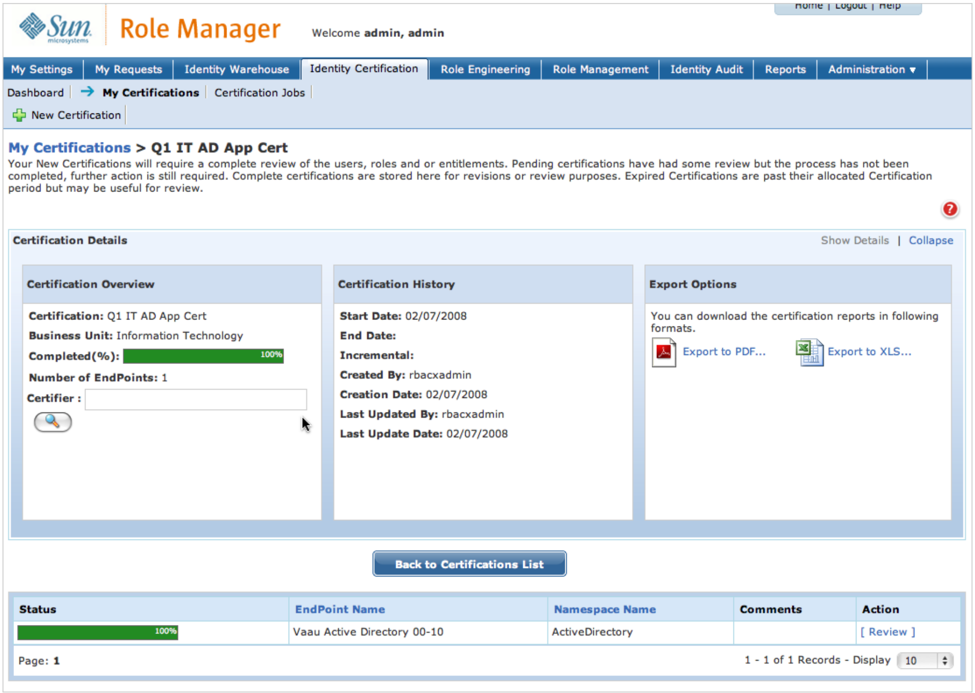
Completing an Application Owner Certification

This sub-section describes how to sign off an application owner certification for attestation and reporting purposes.

▼ Steps to Complete an Application Owner Certification

1. Log into the Sun Role Manager Web-Interface using a Java-enabled web browser
2. Log in with credentials of administrator or certifier
3. Click Identity Certification tab
4. Click My Certifications

5. Click the New or In-Progress Certification or search for the required certification using the available search filters



My Certifications > Q1 IT AD App Cert

Your New Certifications will require a complete review of the users, roles and or entitlements. Pending certifications have had some review but the process has not been completed, further action is still required. Complete certifications are stored here for revisions or review purposes. Expired Certifications are past their allocated Certification period but may be useful for review.

Certification Details

Certification Overview

Certification: Q1 IT AD App Cert
Business Unit: Information Technology
Completed(%): 100%
Number of EndPoints: 1
Certifier :

Certification History

Start Date: 02/07/2008
End Date:
Incremental:
Created By: rbacxadmin
Creation Date: 02/07/2008
Last Updated By: rbacxadmin
Last Update Date: 02/07/2008

Export Options

You can download the certification reports in following formats.

Export to PDF... Export to XLS...

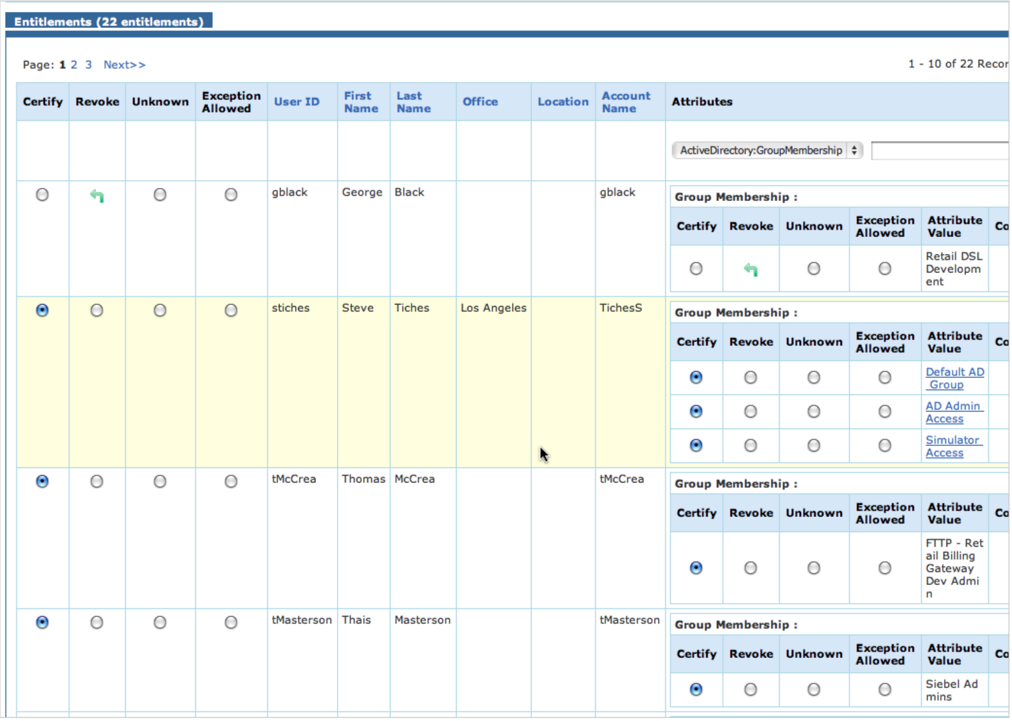
Status	EndPoint Name	Namespace Name	Comments	Action
100%	Vaau Active Directory 00-10	ActiveDirectory		[Review]

Page: **1** 1 - 1 of 1 Records - Display 10

Figure 6.28 – Certification Details

6. Select the Certification to complete by clicking on the Certification Name or using the corresponding checkbox and clicking “Edit Certification”

7. Click [Review] to view application entitlements. It is important to note that these application entitlements are filtered on the basis of their application endpoints.



Entitlements (22 entitlements)

Page: **1** 2 3 Next>>

1 - 10 of 22 Recor

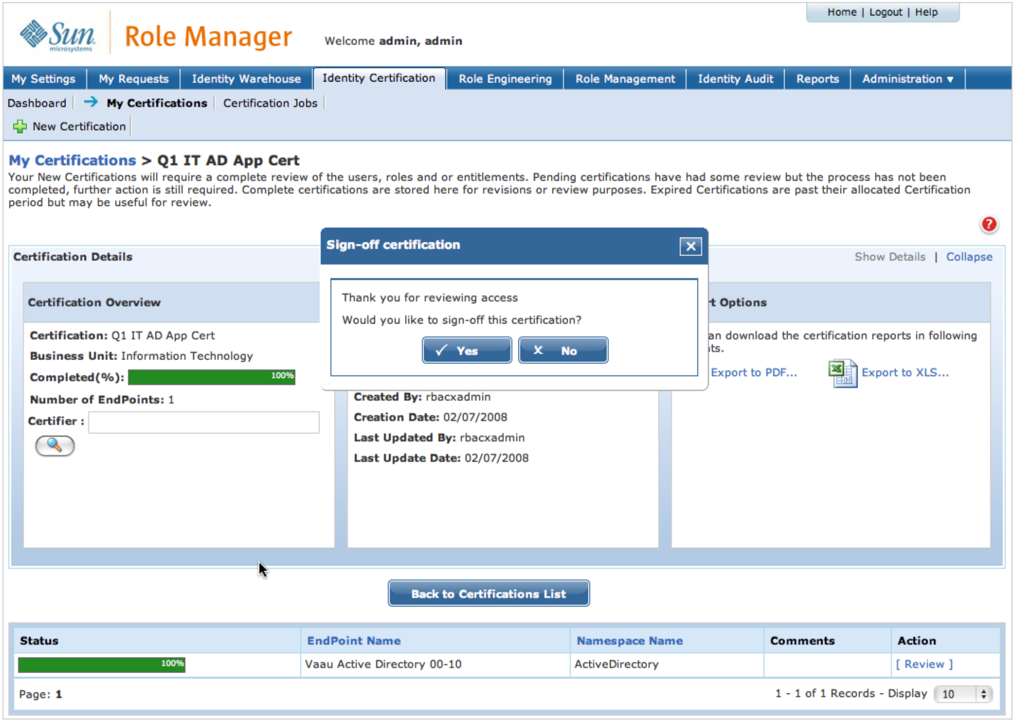
<table>
<tr><th>Certify</th><th>Revoke</th><th>Unknown</th><th>Exception Allowed</th><th>User ID</th><th>First Name</th><th>Last Name</th><th>Office</th><th>Location</th><th>Account Name</th><th>Attributes</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>ActiveDirectory:GroupMembership ⇕</td></tr>
<tr><td>○</td><td>↰</td><td>○</td><td>○</td><td>gblack</td><td>George</td><td>Black</td><td></td><td></td><td>gblack</td><td>Group Membership :
<table>
<tr><th>Certify</th><th>Revoke</th><th>Unknown</th><th>Exception Allowed</th><th>Attribute Value</th><th>Co</th></tr>
<tr><td>○</td><td>↰</td><td>○</td><td>○</td><td>Retail DSL Development</td><td></td></tr>
</table></td></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>stiches</td><td>Steve</td><td>Tiches</td><td>Los Angeles</td><td></td><td>TichesS</td><td>Group Membership :
<table>
<tr><th>Certify</th><th>Revoke</th><th>Unknown</th><th>Exception Allowed</th><th>Attribute Value</th><th>Co</th></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>Default AD Group</td><td></td></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>AD Admin Access</td><td></td></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>Simulator Access</td><td></td></tr>
</table></td></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>tMcCrea</td><td>Thomas</td><td>McCrea</td><td></td><td></td><td>tMcCrea</td><td>Group Membership :
<table>
<tr><th>Certify</th><th>Revoke</th><th>Unknown</th><th>Exception Allowed</th><th>Attribute Value</th><th>Co</th></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>FTTP - Retail Billing Gateway Dev Admin</td><td></td></tr>
</table></td></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>tMasterson</td><td>Thais</td><td>Masterson</td><td></td><td></td><td>tMasterson</td><td>Group Membership :
<table>
<tr><th>Certify</th><th>Revoke</th><th>Unknown</th><th>Exception Allowed</th><th>Attribute Value</th><th>Co</th></tr>
<tr><td>●</td><td>○</td><td>○</td><td>○</td><td>Siebel Admins</td><td></td></tr>
</table></td></tr>
</table>

Figure 6.29 – Review Entitlements

8. Click ‘Certify’, ‘Revoke’, ‘Unknown’ or ‘Exception Allowed’ for each User’s access account. Glossary definitions are useful in determining the true meaning of a cryptic or system level attribute value

9. Click Certify or Revoke to sign off each attribute value within each user’s account that belongs to a particular endpoint. Each account can also be certified as a whole.

10. If Sun Role Manager detects that all attestations have been completed a “Sign Off Certification” box appears. To complete certification at this point click “Ok”. Otherwise Complete attesting entitlements of all accounts and then click Complete Certification



Welcome **admin, admin**

My Certifications > Q1 IT AD App Cert

Your New Certifications will require a complete review of the users, roles and or entitlements. Pending certifications have had some review but the process has not been completed, further action is still required. Complete certifications are stored here for revisions or review purposes. Expired Certifications are past their allocated Certification period but may be useful for review.

Certification Details

Certification Overview

Certification: Q1 IT AD App Cert
Business Unit: Information Technology
Completed(%): 100%
Number of EndPoints: 1
Certifier :

Sign-off certification

Thank you for reviewing access

Would you like to sign-off this certification?

Created By: rbacxadmin
Creation Date: 02/07/2008
Last Updated By: rbacxadmin
Last Update Date: 02/07/2008

t Options

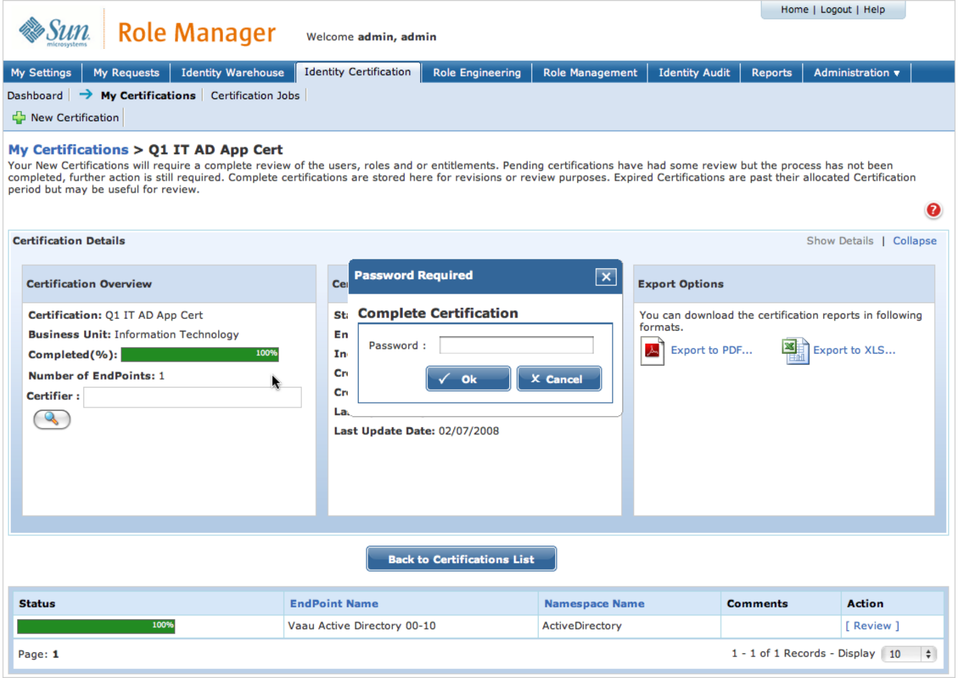
an download the certification reports in following ts.

Status	EndPoint Name	Namespace Name	Comments	Action
100%	Vaau Active Directory 00-10	ActiveDirectory		[Review]

Page: **1** 1 - 1 of 1 Records - Display 10

Figure 6.30 – Sign-off Certification

11. Enter your login password to secure your signoff on this certification



My Certifications > Q1 IT AD App Cert

Your New Certifications will require a complete review of the users, roles and or entitlements. Pending certifications have had some review but the process has not been completed, further action is still required. Complete certifications are stored here for revisions or review purposes. Expired Certifications are past their allocated Certification period but may be useful for review.

Certification Details

Certification Overview

Certification: Q1 IT AD App Cert
Business Unit: Information Technology
Completed(%): 100%
Number of EndPoints: 1
Certifier :

Complete Certification

Password :

Last Update Date: 02/07/2008

Export Options

You can download the certification reports in following formats.

Export to PDF...   Export to XLS...

Status	EndPoint Name	Namespace Name	Comments	Action
100%	Vaau Active Directory 00-10	ActiveDirectory		[Review]

Page: **1**   1 - 1 of 1 Records - Display 10

Figure 6.31 – Sign-off Authorization

7

◆ ◆ ◆ CHAPTER 7

Identity Auditing

Exception Monitoring is an integral piece of Identity Auditing and Management. In organizations today, there are various exceptions of user accounts on the various target systems. A detective mechanism to monitor and get exceptions is needed in organizations where a centralized store for all the exceptions is available. Organizations must be able to manage Continuous Exception Monitoring,Segregation of Duty (SoD) Violations, Detective Scanning, Inter & Intra-Application SoD Enforcement, Actual vs. Assigned Exceptions, and Exception Lifecycle Management. All of these exceptions can be captured in Role Manager and produced in a central repository. Role Manager provides the capability to define Audit policies and the ability to capture/report any exceptions from these policies.

Role Manager provides a Compliance Dashboard for Executives/Auditors which enable them to monitor these exceptions from a central point. Also, the various exceptions generated are stored in Role Manager and a security analyst can accept them or mitigate these risks/exceptions.

The Role Manager Audit Module ensures that users only have the access that they should for their job responsibility. Following are some of the key features of the Identity Auditing module:

- **Actual Account Scanning** - Role Manager scans actual accounts for Identity Audit exceptions. Irrespective of how an account is provisioned or modified (directly or through a provisioning solution), Role Manager will be able to detect any audit exceptions, since the scanning is done at the actual account details level.
- **Compliance Dashboard -** Role Manager provides a detailed dashboard for auditors, security administrators and compliance teams to review the status, history and trend of identity audit exceptions in the enterprise.
- **Exception Lifecycle Management -** Role Manager stores every action that is conducted on an audit exception and creates a history of the exception. This allows administrators to get a complete step-by-step history and lifecycle of the exception if required.

By closely monitoring user access privileges, who approved these access privileges, and what access privileges shouldn't be there, Role Manager provides organizations with the data required to take informed corrective actions in order to remediate policy violations. Role Manager provides a platform to enforce policies and generate audit trails that can be used to certify compliance with various laws and regulations.

The following types of exceptions are monitored by the system on a scheduled basis:

- **Actual vs. Assigned**: The system will monitor all instances where a user's actual access in the target system does not match the access assigned to the user based on the roles assigned to the user
- **Terminated User with Accounts**: The system will monitor all instances where a terminated user has active accounts

This section describes the concept of Audit Policies and Audit Rules and how to scan the Role Manager Identity Warehouse for exceptions. Thereafter, this module will cover how Role Manager helps manage a life-cycle of an exception or Audit Violation from assigning a remediator to opening and closing the exception tickets.

Audit Rules and Policies

Create Audit Rules and Audit Policies

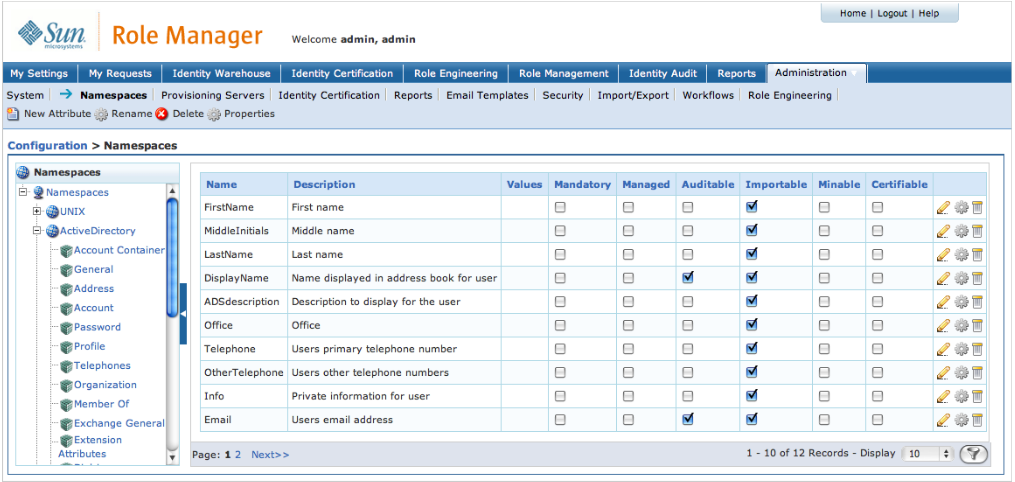
Set Auditable Attributes

The strength of Role Manager lies in its granular metadata definition. Here you can define properties for attributes, the lowest level of metadata, and set them as auditable to allow the system to scan for violations across applications. This gives flexibility in defining audit rules and audit policies that span the breadth of the enterprise considering user attributes along with access entitlements across all applications for the most flexible and comprehensive audit policy definition.

Note – Auditable attribute settings should be checked before Identity Audit effort is initiated to ensure that appropriate applications are accounted for while the system is being scanned. This may be an administrator level functionality and you may not have the rights to perform this action. If you do not see this option when you log into Role Manager, please talk to your administrator or refer to the *Sun Role Manager 4.1 Administration Guide*.

▼ Steps to set Auditable Attributes before Identity Audit

1. Log into the Role Manager Web-Interface from your Java enabled web browser.
2. The login dialog box appears. Enter the relevant credentials and login to Role Manager
3. Click the Configuration tab and then Namespaces link
4. Select desired namespace and check or uncheck ‘Auditable’ dialog box for each attribute



Name	Description	Values	Mandatory	Managed	Auditable	Importable	Minable	Certifiable
FirstName	First name		□	□	□	☑	□	□
MiddleInitials	Middle name		□	□	□	☑	□	□
LastName	Last name		□	□	□	☑	□	□
DisplayName	Name displayed in address book for user		□	□	☑	☑	□	□
ADSdescription	Description to display for the user		□	□	□	☑	□	□
Office	Office		□	□	□	☑	□	□
Telephone	Users primary telephone number		□	□	□	☑	□	□
OtherTelephone	Users other telephone numbers		□	□	□	☑	□	□
Info	Private information for user		□	□	□	☑	□	□
Email	Users email address		□	□	☑	☑	□	□

Page: 1 2 Next>>   1 - 10 of 12 Records - Display 10

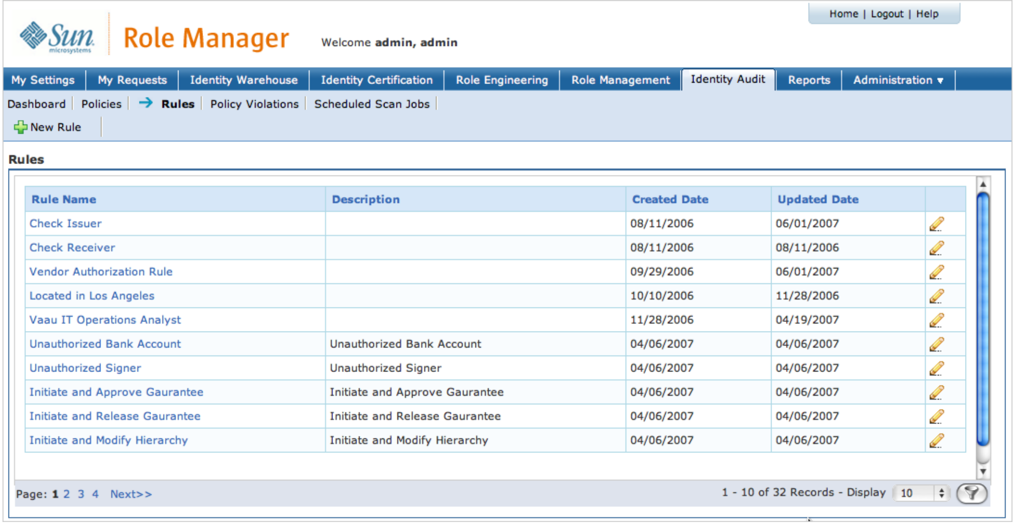
Figure 7.1 – Set Auditable Attributes

Create Audit Rules

An Audit Rule is a predefined condition for a set of Role Manager objects which can be user attributes or account attributes. Various types of audit rules with a combination of user and account attributes can be defined. A collection of Audit Rules defines an Audit Policy.

▼ Steps to Create an Audit Rule

1. Log into the Role Manager Web-Interface
2. Click Identity Audit tab and click Rules link



Rules

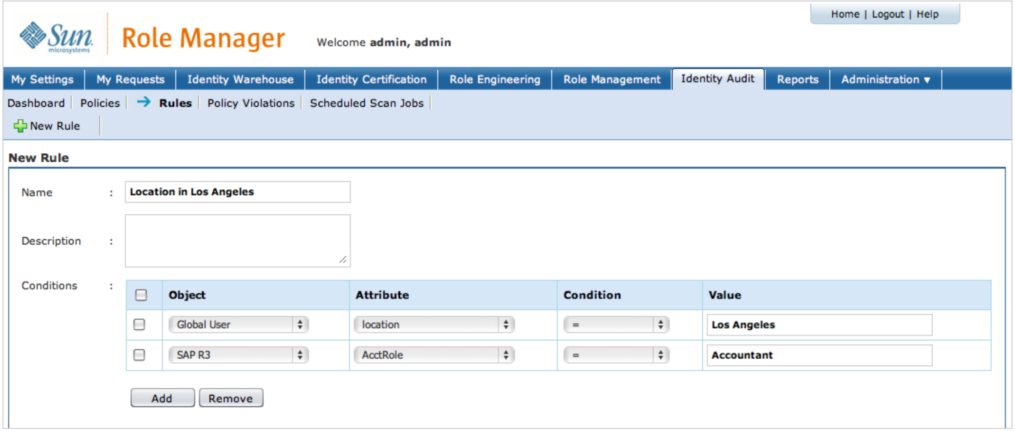
Rule Name	Description	Created Date	Updated Date
Check Issuer		08/11/2006	06/01/2007
Check Receiver		08/11/2006	08/11/2006
Vendor Authorization Rule		09/29/2006	06/01/2007
Located in Los Angeles		10/10/2006	11/28/2006
Vaau IT Operations Analyst		11/28/2006	04/19/2007
Unauthorized Bank Account	Unauthorized Bank Account	04/06/2007	04/06/2007
Unauthorized Signer	Unauthorized Signer	04/06/2007	04/06/2007
Initiate and Approve Gaurantee	Initiate and Approve Gaurantee	04/06/2007	04/06/2007
Initiate and Release Gaurantee	Initiate and Release Gaurantee	04/06/2007	04/06/2007
Initiate and Modify Hierarchy	Initiate and Modify Hierarchy	04/06/2007	04/06/2007

Page: 1 2 3 4 Next>>

1 - 10 of 32 Records - Display 10

Figure 7.2 – Audit Rules

3. Click New Rule
4. Enter a relevant Rule name and description
5. Select an Role Manager object from the drop down list – options will include User and each defined Namespace.
6. Selecting the Object will bring up a pull down list of Object’s attributes.
7. Select desired attributes, condition and value
8. To add another object to the Audit Rule, click *[Add]*



New Rule

Name : Location in Los Angeles

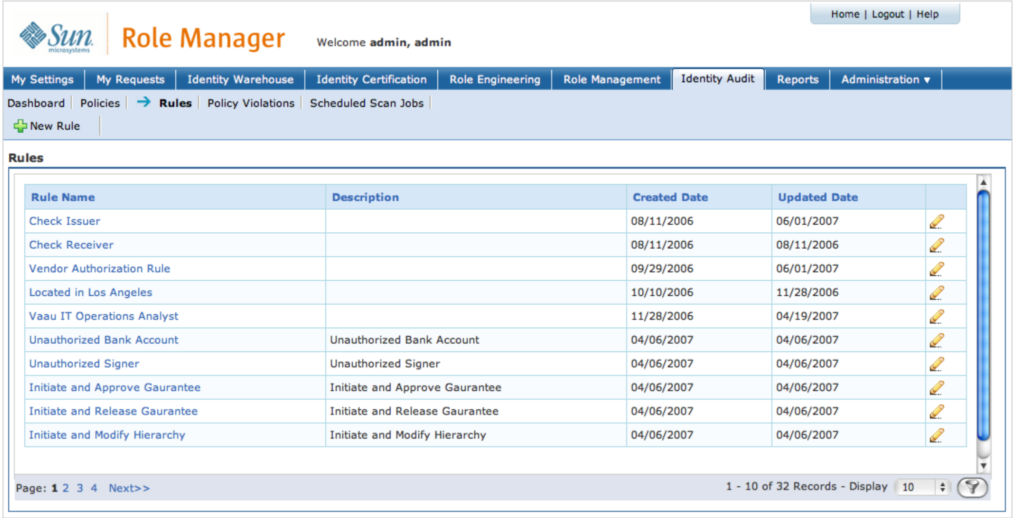
Description :

Conditions :

□	Object	Attribute	Condition	Value
□	Global User	location	=	Los Angeles
□	SAP R3	AcctRole	=	Accountant

Figure 7.3 – Add Audit Rules

9. Click ✓ Save when rule creation is complete.



Rules

Rule Name	Description	Created Date	Updated Date	
Check Issuer		08/11/2006	06/01/2007	✎
Check Receiver		08/11/2006	08/11/2006	✎
Vendor Authorization Rule		09/29/2006	06/01/2007	✎
Located in Los Angeles		10/10/2006	11/28/2006	✎
Vaau IT Operations Analyst		11/28/2006	04/19/2007	✎
Unauthorized Bank Account	Unauthorized Bank Account	04/06/2007	04/06/2007	✎
Unauthorized Signer	Unauthorized Signer	04/06/2007	04/06/2007	✎
Initiate and Approve Gaurantee	Initiate and Approve Gaurantee	04/06/2007	04/06/2007	✎
Initiate and Release Gaurantee	Initiate and Release Gaurantee	04/06/2007	04/06/2007	✎
Initiate and Modify Hierarchy	Initiate and Modify Hierarchy	04/06/2007	04/06/2007	✎

Page: **1** 2 3 4 Next>> 1 - 10 of 32 Records - Display 10

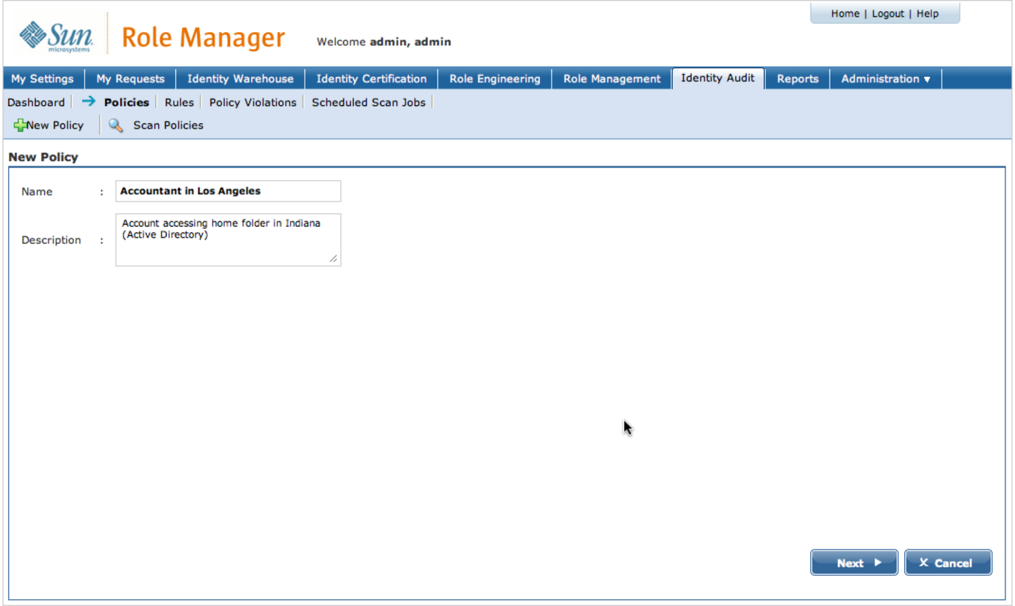
Figure 7.4 - Completed Rule Creation

Create Audit Policy

An Audit Policy definition includes predefined Audit Rules with a logical condition operator, and a Remediator who is an actor later assigned to each policy violation. The Remediator is responsible for assigning a status to the violation.

▼ Steps to Create Audit Policy

1. In the Identity Audit tab, click Policies.
2. Select New Policy and assign Policy name and description



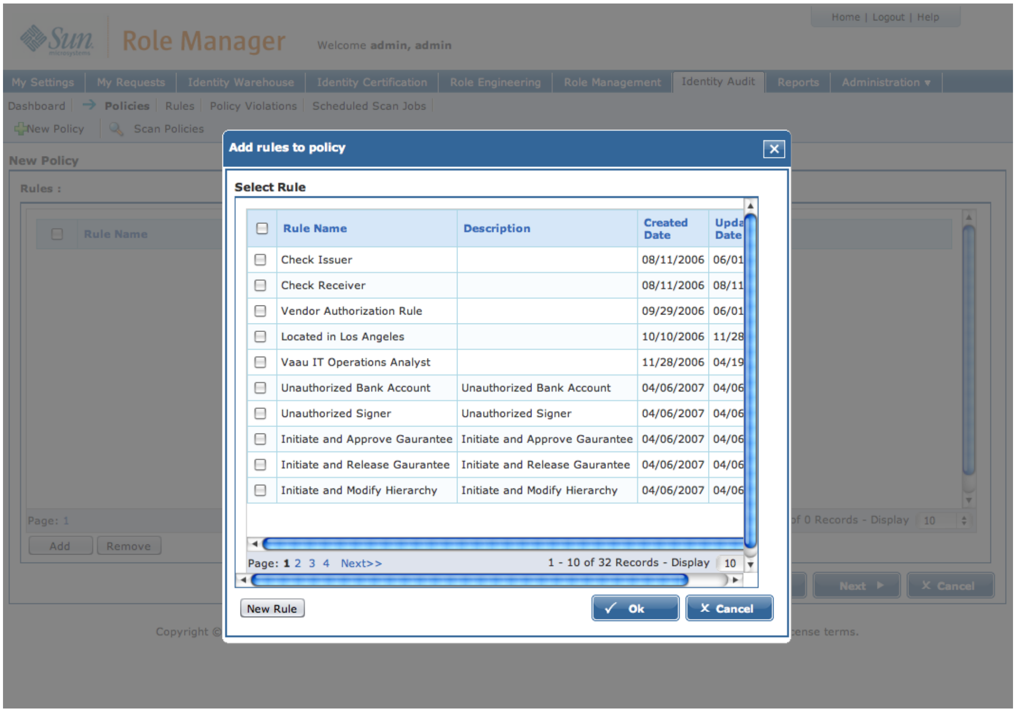
New Policy

Name : Accountant in Los Angeles

Description : Account accessing home folder in Indiana (Active Directory)

Figure 7.5 – Create Audit Policy

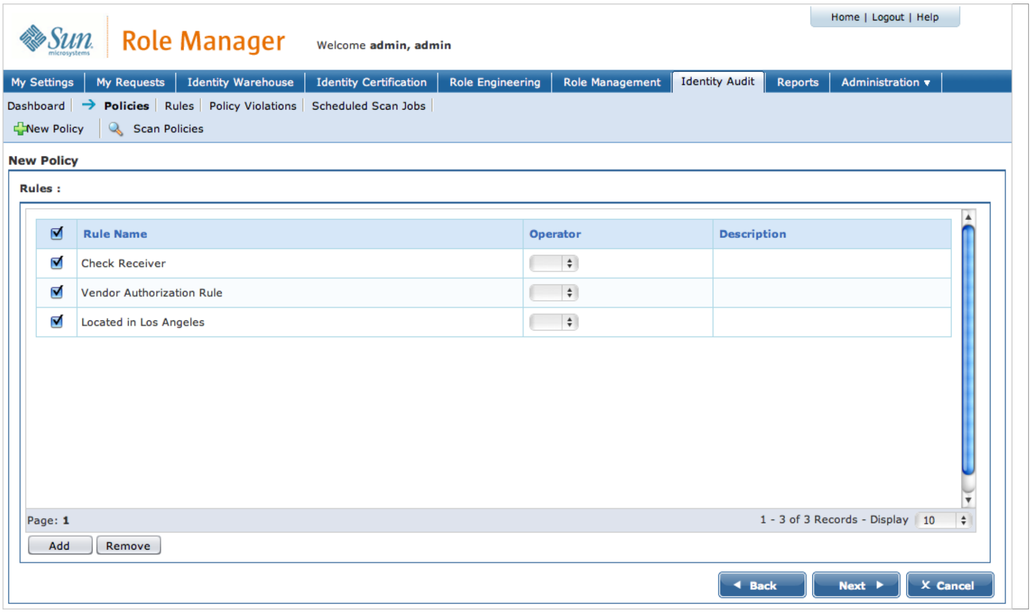
3. To add an Audit Rule, select *[Add]*. This will bring up a pop up window with all listed Audit Rules and dates of creation.



☐	Rule Name	Description	Created Date	Upda Date
☐	Check Issuer		08/11/2006	06/01
☐	Check Receiver		08/11/2006	08/11
☐	Vendor Authorization Rule		09/29/2006	06/01
☐	Located in Los Angeles		10/10/2006	11/28
☐	Vaau IT Operations Analyst		11/28/2006	04/19
☐	Unauthorized Bank Account	Unauthorized Bank Account	04/06/2007	04/06
☐	Unauthorized Signer	Unauthorized Signer	04/06/2007	04/06
☐	Initiate and Approve Gaurantee	Initiate and Approve Gaurantee	04/06/2007	04/06
☐	Initiate and Release Gaurantee	Initiate and Release Gaurantee	04/06/2007	04/06
☐	Initiate and Modify Hierarchy	Initiate and Modify Hierarchy	04/06/2007	04/06

Figure 7.6 – Add Rules to Policy

4. Check all desired Rules and click ✓ Ok



New Policy

Rules :

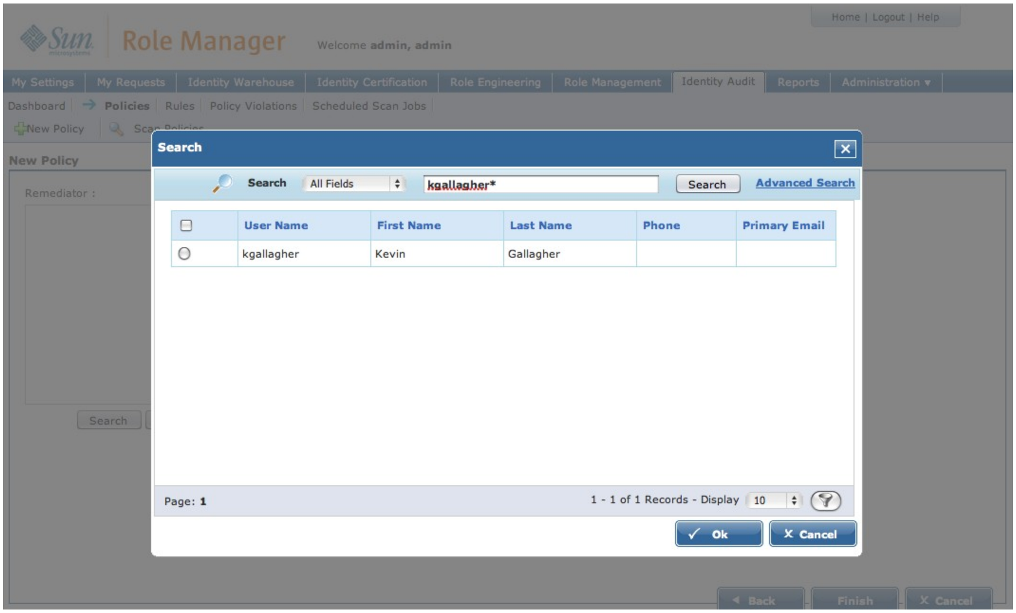
☑	Rule Name	Operator	Description
☑	Check Receiver		
☑	Vendor Authorization Rule		
☑	Located in Los Angeles		

Figure 7.7 - Check Rules

5. Set the logical condition operator between Rules. Options are AND, OR and add more rules if required.

6. Click Next ▸ to go to the remediators tab.

7. All violations of said policy will be assigned to this remediator and appropriate email notifications will be sent. Click *[Search]* to display a search box for users. Select one user and click ✓ Ok and then Finish ▸ to save the policy.



Search: kgallagher*

□	User Name	First Name	Last Name	Phone	Primary Email
○	kgallagher	Kevin	Gallagher		

Page: 1

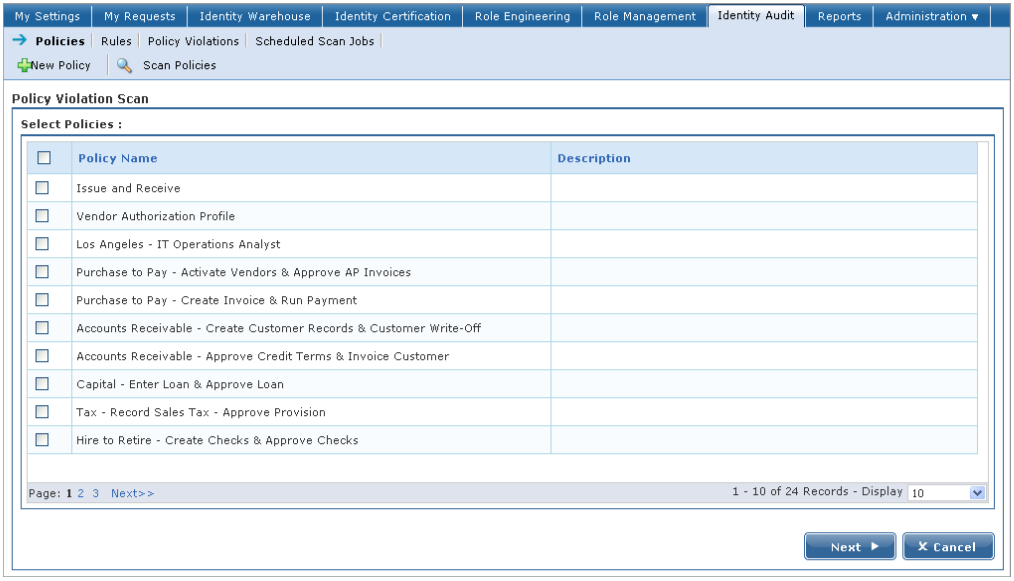
1 - 1 of 1 Records - Display 10

Figure 7.8 – Search Remediator

Scan Audit Policy Violations

▼ Steps to Scan System for Audit Violations

1. Click the Identity Audit -> Policies -> Scan Policies tabs.



Policy Violation Scan

Select Policies :

□	Policy Name	Description
□	Issue and Receive	
□	Vendor Authorization Profile	
□	Los Angeles - IT Operations Analyst	
□	Purchase to Pay - Activate Vendors & Approve AP Invoices	
□	Purchase to Pay - Create Invoice & Run Payment	
□	Accounts Receivable - Create Customer Records & Customer Write-Off	
□	Accounts Receivable - Approve Credit Terms & Invoice Customer	
□	Capital - Enter Loan & Approve Loan	
□	Tax - Record Sales Tax - Approve Provision	
□	Hire to Retire - Create Checks & Approve Checks	

Figure 7.9 – Scan Policy

2. Click ✚ Add Business Unit(s) to add certain business units from the selection or check *All Business Units* to scan against the entire warehouse.

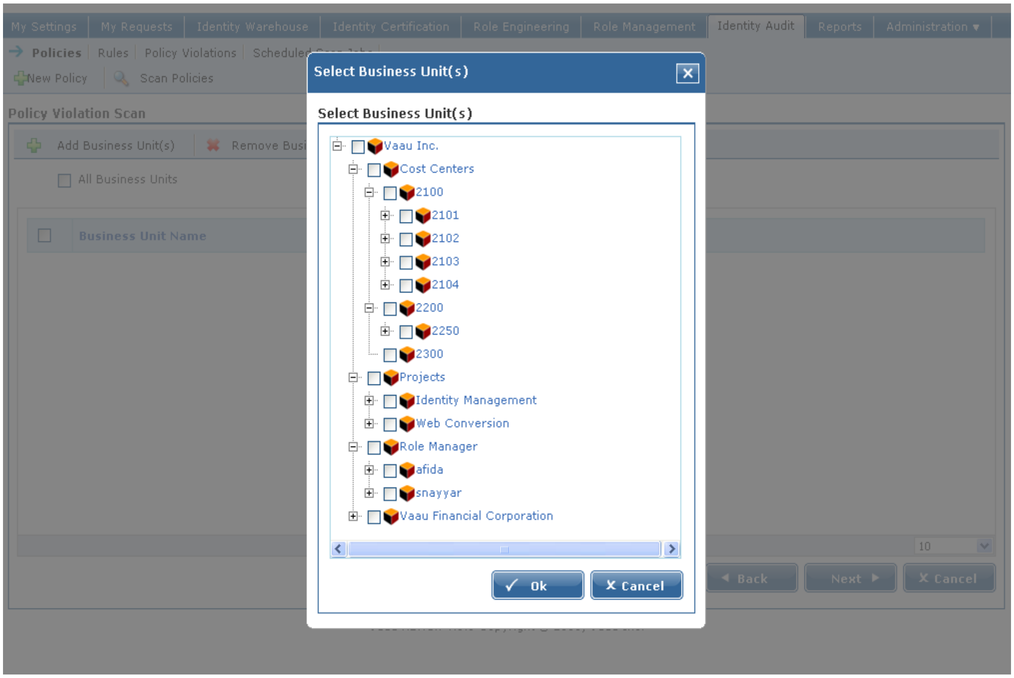
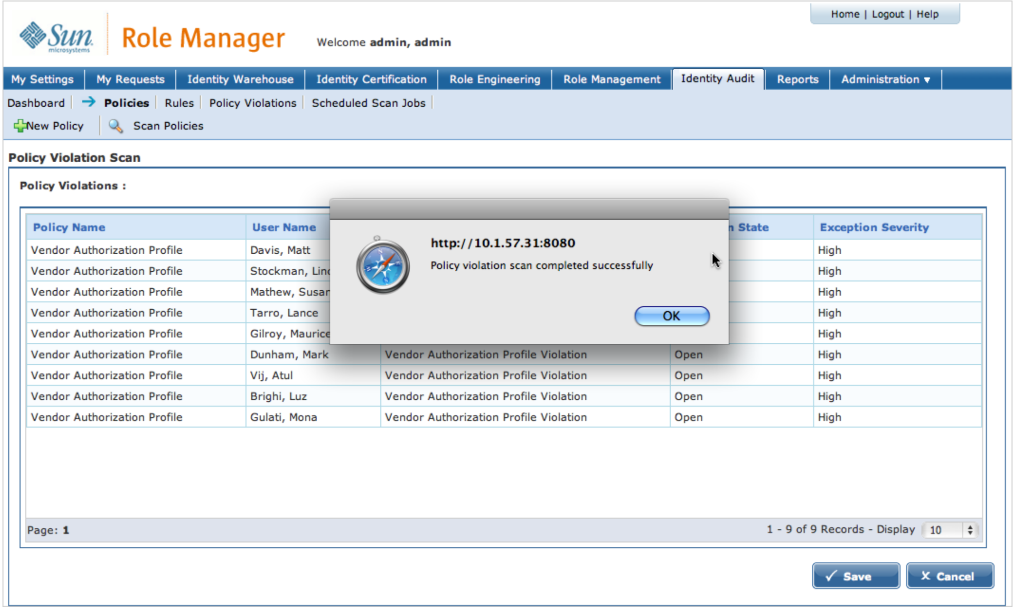


Figure 7.10 – Select Business Unit

3. Click ✓ Ok to select the required Business Units. Click Next ▶. This will guide the user to the Policy Violation Scan page where listed on top is the number of users being scanned and the progress of the audit scan. The following message appears once the scan is completed:



Policy Violation Scan

Policy Violations :

http://10.1.57.31:8080

Policy violation scan completed successfully

Policy Name	User Name		n State	Exception Severity
Vendor Authorization Profile	Davis, Matt			High
Vendor Authorization Profile	Stockman, Lin			High
Vendor Authorization Profile	Mathew, Susar			High
Vendor Authorization Profile	Tarro, Lance			High
Vendor Authorization Profile	Gilroy, Maurice			High
Vendor Authorization Profile	Dunham, Mark	Vendor Authorization Profile Violation	Open	High
Vendor Authorization Profile	Vij, Atul	Vendor Authorization Profile Violation	Open	High
Vendor Authorization Profile	Brighi, Luz	Vendor Authorization Profile Violation	Open	High
Vendor Authorization Profile	Gulati, Mona	Vendor Authorization Profile Violation	Open	High

Page: 1 1 - 9 of 9 Records - Display 10

Figure 7.11 – Policy Violation Scan

4. And violations found will be listed. Users violating the policy along with Audit Rule exception are also listed.

5. Click ✓ Save to start managing the life-cycle of this exception.

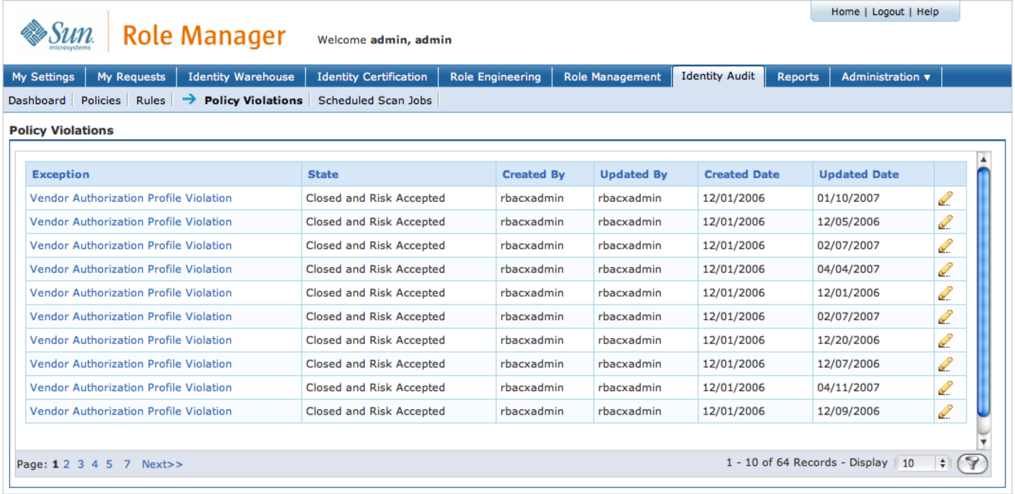
Exception Life-Cycle Management

Role Manager provides the capability of managing the entire life-cycle of an audit exception from opening a violation to assigning a remediator and, finally, closing it. It keeps a dated log or violation trail of all events related to every violation in the Role Manager data warehouse. When an audit policy violation is encountered, the remediator assigned to the policy receives an email requesting them to log into Role Manager and take an appropriate action. These possible actions are explained in further detail below.

▼ Steps to View Policy Lifecycle

1. Log into Role Manager Web Interface and click the Identity Audit tab.
2. Click Policy Violations to list all saved violations from your Audit scans.

Figure 7.12 – Policy Violations



Policy Violations

Exception	State	Created By	Updated By	Created Date	Updated Date	
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	01/10/2007	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	12/05/2006	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	02/07/2007	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	04/04/2007	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	12/01/2006	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	02/07/2007	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	12/20/2006	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	12/07/2006	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	04/11/2007	✎
Vendor Authorization Profile Violation	Closed and Risk Accepted	rbacxadmin	rbacxadmin	12/01/2006	12/09/2006	✎

Page: 1 2 3 4 5 7 Next>>   1 - 10 of 64 Records - Display 10

3. Click an Open exception.
4. The Audit Violation lists the Policy that was violated, current state of Exception, Date of Detection, Remediator assigned to this Violation, and details of the User in violation.
5. Scroll down the screen to list Account being violated including account name and target machine.
6. Further below note the violation trail.

Manage Life-Cycle of Audit Violation

▼ Steps to Manage life-cycle of an Audit Violation

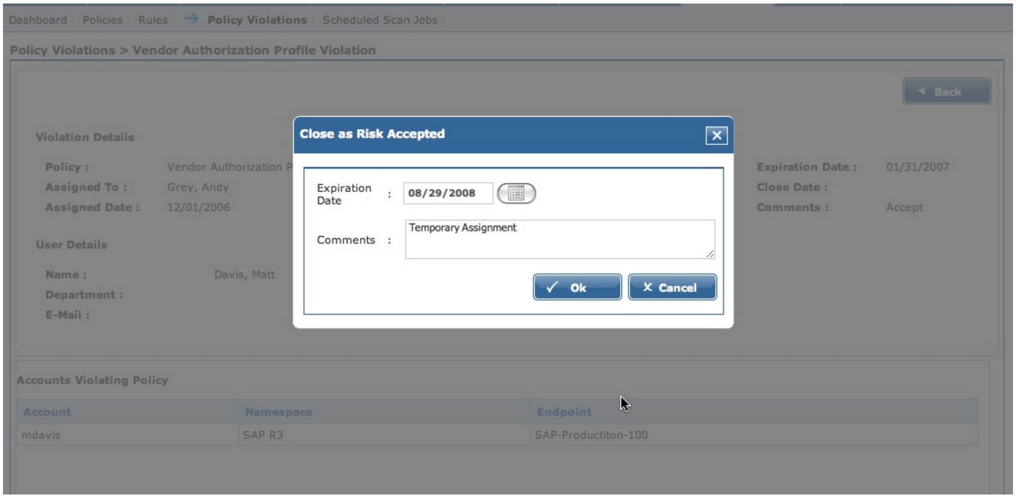
1. The options for a remediator are to assign the violation to another person, immediately close the violation or close with an accepted risk with an end date for this risk.

2. Click Close as Risk Accepted.

3. This will bring up a screen where you need to assign a future date until when this risk is acceptable.

4. Assign a mitigating control in the comments for this accepted risk.

5. Click ✓ Ok. Your action will show up in the violation trail for auditors and management/auditors to keep track of.



Policy Violations > Vendor Authorization Profile Violation

Violation Details

Policy : Vendor Authorization P

Assigned To : Grey, Andy

Assigned Date : 12/01/2006

Expiration Date : 01/31/2007

Close Date :

Comments : Accept

User Details

Name : Davis, Matt

Department :

E-Mail :

Close as Risk Accepted

Expiration Date : 08/29/2008

Comments : Temporary Assignment

Accounts Violating Policy

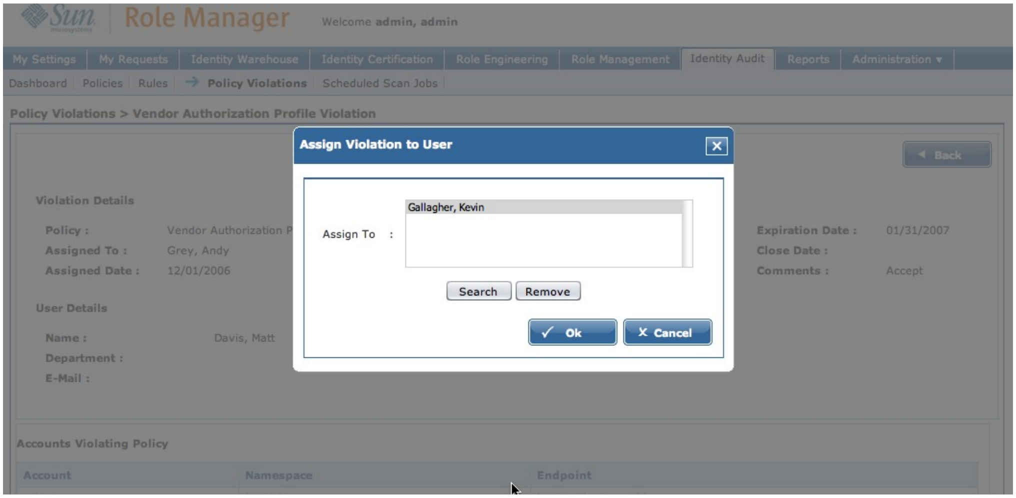
Account	Namespace	Endpoint
mdavis	SAP R3	SAP-Productiton-100

Figure 7.13 – Close as Risk Accepted

6. To assign another Remediator to this violation, click Assign.

7. This will bring up a User Search dialog box. Find relevant user and click ✓ Ok

Figure 7.14 – Assign Violation to User



Policy Violations > Vendor Authorization Profile Violation

Assign Violation to User

Assign To : Gallagher, Kevin

Violation Details

Policy : Vendor Authorization P

Assigned To : Grey, Andy

Assigned Date : 12/01/2006

Expiration Date : 01/31/2007

Close Date :

Comments : Accept

User Details

Name : Davis, Matt

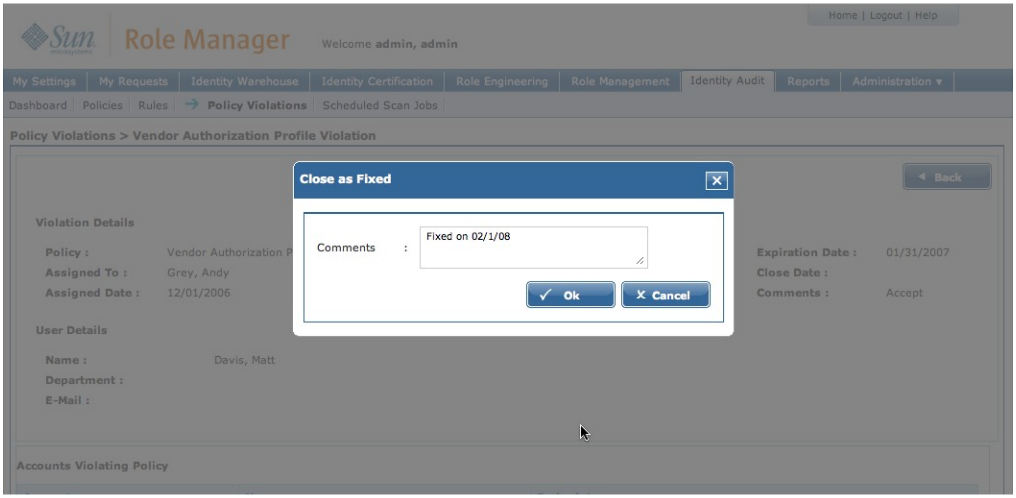
Department :

E-Mail :

Accounts Violating Policy

Account	Namespace	Endpoint

8. To close this Exception with no further action, click Close. You will need to enter your comments in the pop up box.



Policy Violations > Vendor Authorization Profile Violation

Close as Fixed

Comments : Fixed on 02/1/08

Violation Details

Policy : Vendor Authorization P

Assigned To : Grey, Andy

Assigned Date : 12/01/2006

Expiration Date : 01/31/2007

Close Date :

Comments : Accept

User Details

Name : Davis, Matt

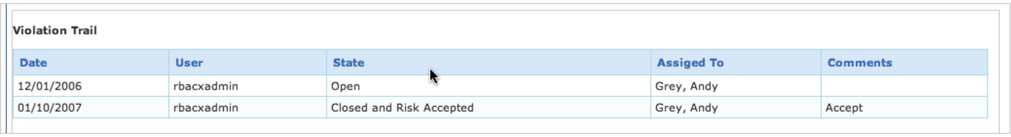
Department :

E-Mail :

Accounts Violating Policy

Figure 7.15 – Close as Fixed

9. All actions are recorded and logged with date stamps for a complete audit violation life-cycle trail.



Violation Trail

Date	User	State	Assiged To	Comments
12/01/2006	rbacxadmin	Open	Grey, Andy	
01/10/2007	rbacxadmin	Closed and Risk Accepted	Grey, Andy	Accept

Figure 7.16 – Violation Trail

8

◆ ◆ ◆ CHAPTER 8

Chapter – 8: Reports

Role Manager provides detailed reporting capabilities to the end user for Management and Audit Reviews. These reports are customizable and new reports can be easily generated. The different kinds of reports that can be generated are as follows:

- Business Unit Reports
- System Reports
- Audit Reports
- Custom Reports

A list of the reports listed under each section is listed below.

Business Unit Reports

The different kinds of Business Unit Reports are as follows:

REPORTS	DESCRIPTION
User Report	Provides list of all the users for each Business Unit
Roles Report	Provides list of all the roles for each Business Unit
User Role Report	Provides list of all the users and the roles they have for each Business Unit

Role User Report	Provides list of all the roles and the users they are assigned to for each Business Unit
Role Policy Report	Provides a list of all roles and the policies they contain for each Business Unit
Entitlement Report by User	Provides what access each user has in the organization by each user
Entitlement Report by Namespace	Provides what access each user has in the organization by each namespace
User Certification Report	Provides what roles each user has and associated rights with that role

System Reports

The different kinds of System Reports are as follows:

REPORTS	**DESCRIPTION**
Role Policies Report	Provides a list of roles and associated policies of different applications within those roles
Roles Users Report	Provide a list of roles and associated users within those roles
Policy Namespace Report	Provide a list of policies by namespace
Policy Role Report	Provide a list of roles in a policy
Policies Attribute Report	Provides a list of attributes in a policy.
User Business Unit Report	Provides a list of business units under a user.
User Role Report	Provides a list of roles under a user.
User Role Business Unit Report	Provides a list of business units under a role which is under a user.
User Application Report	Provides a list of applications under a user.

User Account Report	Provides a list of accounts under a user.
User Role based access Report	Provides a list of attributes under a policy in a namespace under a user.
Operational Exception Report	Reports on missing data required for correlations in Role Manager
Import Validation Report	A set of reports, displaying the data which has not been imported into Role Manager from the daily scheduled dumps.
Expiration Forecast Report	It contains three sub-reports. User expiration, Role expiration and User- Role association expiration. It provides a list of all the above mentioned expirations occurring within the current week.

Audit Reports

The different kinds of Audit Reports are as follows:

REPORTS	**DESCRIPTION**
Audit Exception Report a) ALL Open Identity Audit Exceptions b) Latest Open Identity Audit Exceptions	Provides a list of audit related exceptions which are: Segregation of Duties, Assigned Vs Actual Rights Violation and Terminated User. Report a) lists out all the Open Exceptions Report b) Lists out all exceptions for the current day.

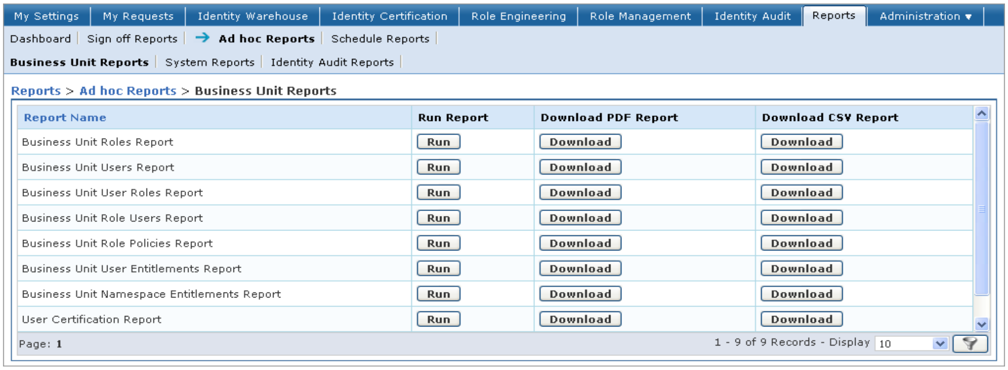
Custom Reports

Role Manager provides the capability to generate custom reports. Custom reports can be generated by importing .jrxml files for the reports and generating reports through Role Manager

Generating Reports

▼ Steps to generate reports

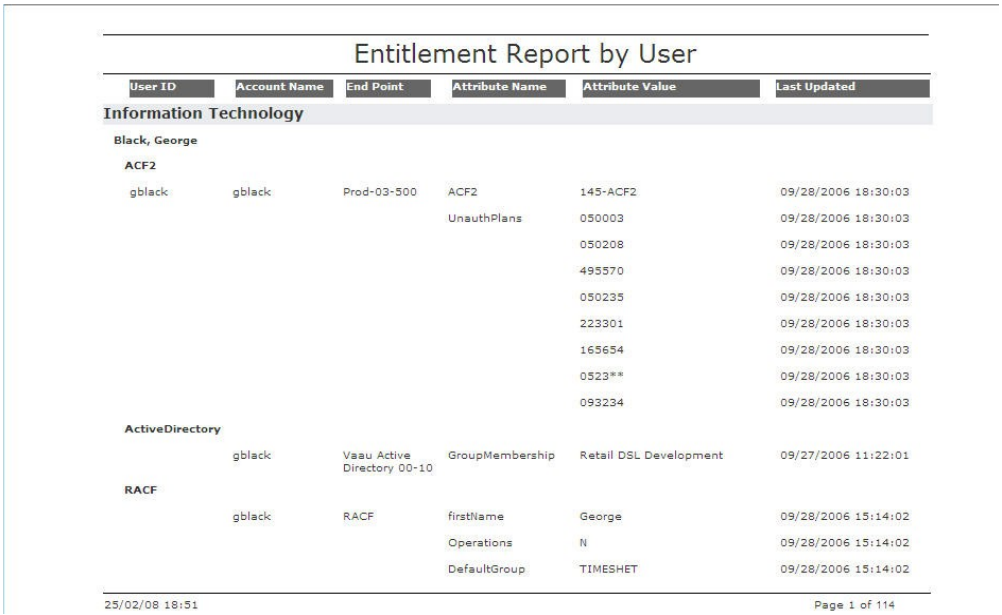
1. Start Role Manager by clicking on the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select a Report Type from the Reports Menu
4. Browse and Select for example, the ‘Entitlement Report by User’ report and click Run
5. Select the Business Unit on which the Report is to be generated
6. Click ✓ Ok to generate the report



Report Name	Run Report	Download PDF Report	Download CSV Report
Business Unit Roles Report	Run	Download	Download
Business Unit Users Report	Run	Download	Download
Business Unit User Roles Report	Run	Download	Download
Business Unit Role Users Report	Run	Download	Download
Business Unit Role Policies Report	Run	Download	Download
Business Unit User Entitlements Report	Run	Download	Download
Business Unit Namespace Entitlements Report	Run	Download	Download
User Certification Report	Run	Download	Download

Page: 1 1 - 9 of 9 Records - Display 10

Figure 8.1 – Generating Reports



Entitlement Report by User

User ID	Account Name	End Point	Attribute Name	Attribute Value	Last Updated
Information Technology					
Black, George					
ACF2					
gblack	gblack	Prod-03-500	ACF2	145-ACF2	09/28/2006 18:30:03
			UnauthPlans	050003	09/28/2006 18:30:03
				050208	09/28/2006 18:30:03
				495570	09/28/2006 18:30:03
				050235	09/28/2006 18:30:03
				223301	09/28/2006 18:30:03
				165654	09/28/2006 18:30:03
				0523**	09/28/2006 18:30:03
				093234	09/28/2006 18:30:03
ActiveDirectory					
	gblack	Vaau Active Directory 00-10	GroupMembership	Retail DSL Development	09/27/2006 11:22:01
RACF					
	gblack	RACF	firstName	George	09/28/2006 15:14:02
			Operations	N	09/28/2006 15:14:02
			DefaultGroup	TIMESHET	09/28/2006 15:14:02

25/02/08 18:51

Page 1 of 114

Figure 8.2 – Entitlement Report by User

The Report generated can be saved in different formats by clicking on the Actions button. The report can also be downloaded in .csv or .pdf format by clicking the "Download" button.

Generating Custom Reports

▼ Steps to create custom reports

1. Start Role Manager by clicking on the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Reports Tab
4. Select the Add Custom Reports Tab
5. The Custom Reports Details page opens. Select New Custom Report Tab

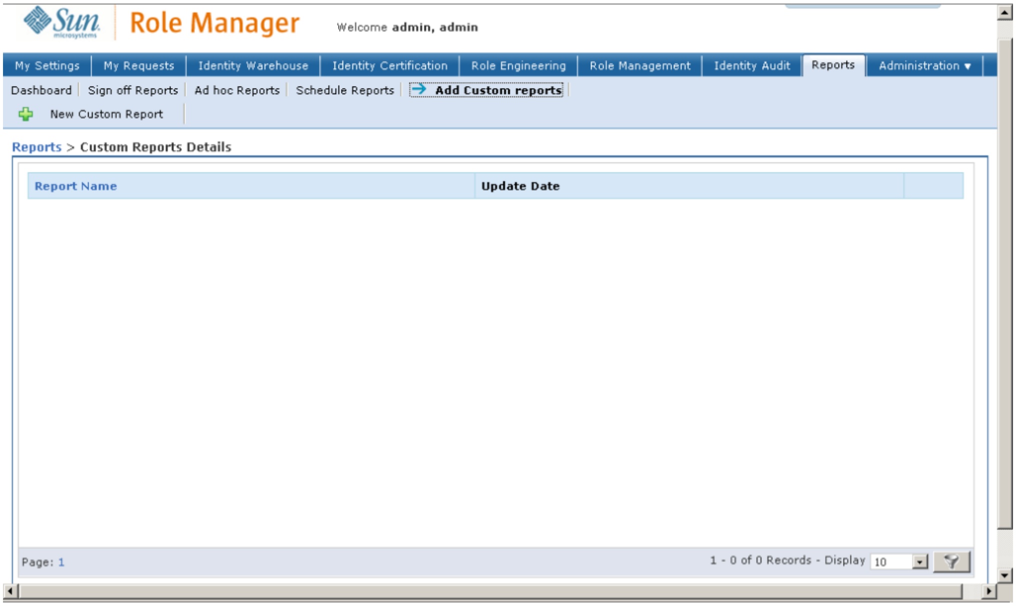
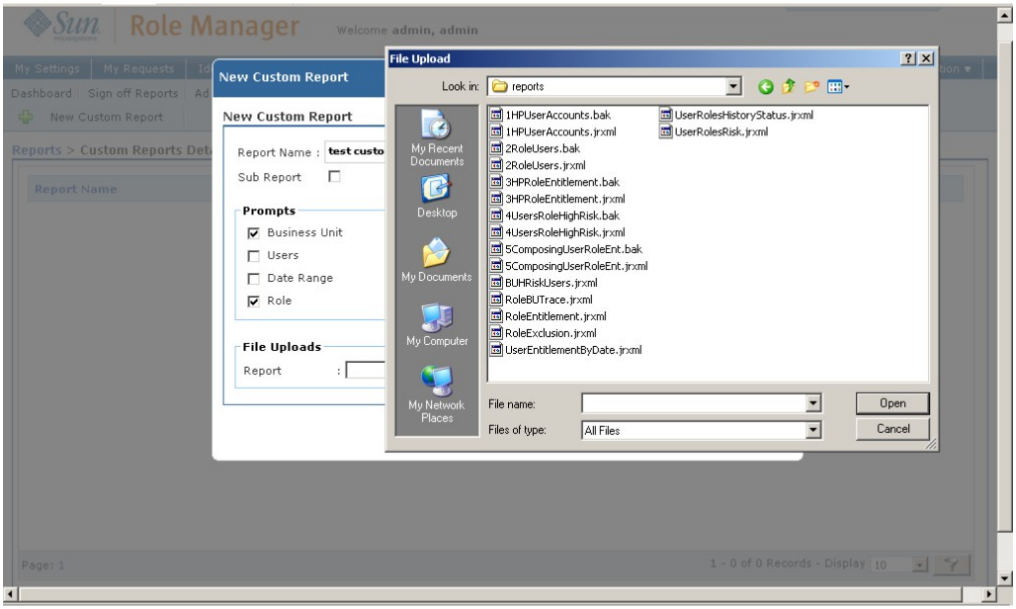


Figure 8.3 – New Custom Report

6. The New Custom Report window opens up. Fill in the value for Report Name. Select Sub Report checkbox if sub reports are required. Select appropriate checkboxes for prompts that the report should require. Click browse to upload the file from which the custom report is to be generated. A file upload box opens up that allows selecting the file to generate the custom report from



New Custom Report

Report Name : test custo

Sub Report □

Prompts

☑ Business Unit

□ Users

□ Date Range

☑ Role

File Uploads

Report :

Look in: reports

1HPUserAccounts.bak
1HPUserAccounts.jrxml
2RoleUsers.bak
2RoleUsers.jrxml
3HPRoleEntitlement.bak
3HPRoleEntitlement.jrxml
4UsersRoleHighRisk.bak
4UsersRoleHighRisk.jrxml
5ComposingUserRoleEnt.bak
5ComposingUserRoleEnt.jrxml
BUHRiskUsers.jrxml
RoleBUTrace.jrxml
RoleEntitlement.jrxml
RoleExclusion.jrxml
UserEntitlementByDate.jrxml
UserRolesHistoryStatus.jrxml
UserRolesRisk.jrxml

File name:

Files of type: All Files

Figure 8.4 – Select File for Custom Report

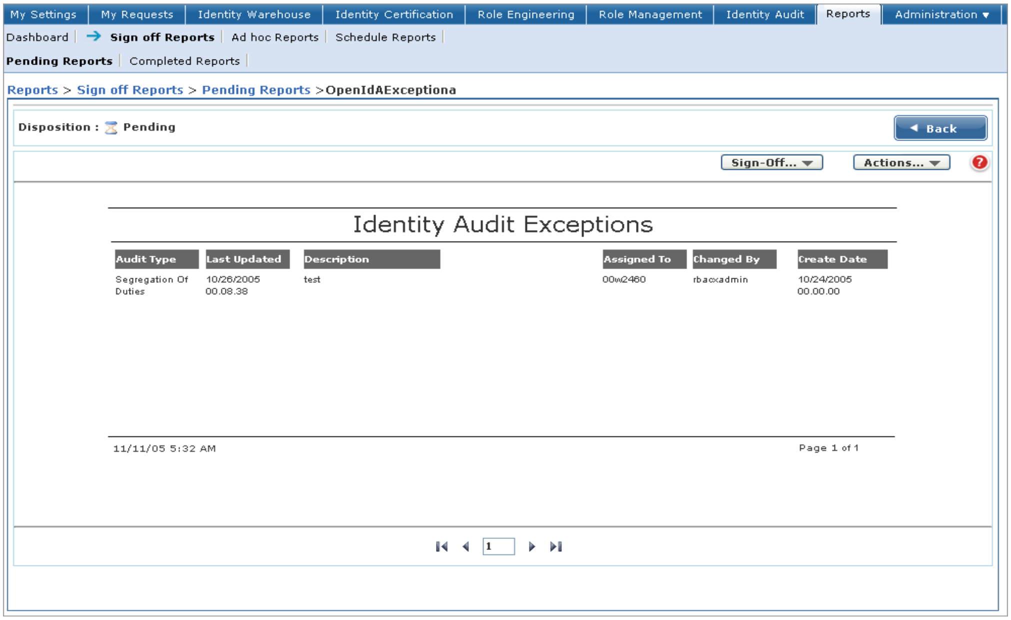
7. Select the file to be used to generate the report and click Open
8. Once all the values on the New Custom Report page have been selected click “Save”
9. The new custom report will be created available for view and editing configuration under the custom reports detail panel

▼ Steps to run custom reports

1. Start Role Manager by clicking on the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Select the Reports Tab
4. Select the Ad hoc reports Tab
5. Select the report type “Custom Reports”
6. This gives a list of all the custom reports available to be generated
7. Select “Run” to run the report and “Download” to get the report in pdf or csv form

▼ Steps to Sign off a Report

1. Start Role Manager by clicking on the Role Manager Icon
2. The login dialog box appears. Enter your credentials and login to Role Manager
3. Click Reports -> Sign Off Reports to display the list of Pending/Completed reports
4. Generate a Report by clicking [View Report]
5. Select the Sign Off to Sign – off on a Report By Accepting or Rejecting the Report



Disposition : Pending

Identity Audit Exceptions

Audit Type	Last Updated	Description	Assigned To	Changed By	Create Date
Segregation Of Duties	10/26/2005 00.08.38	test	00w2460	rbacxadmin	10/24/2005 00.00.00

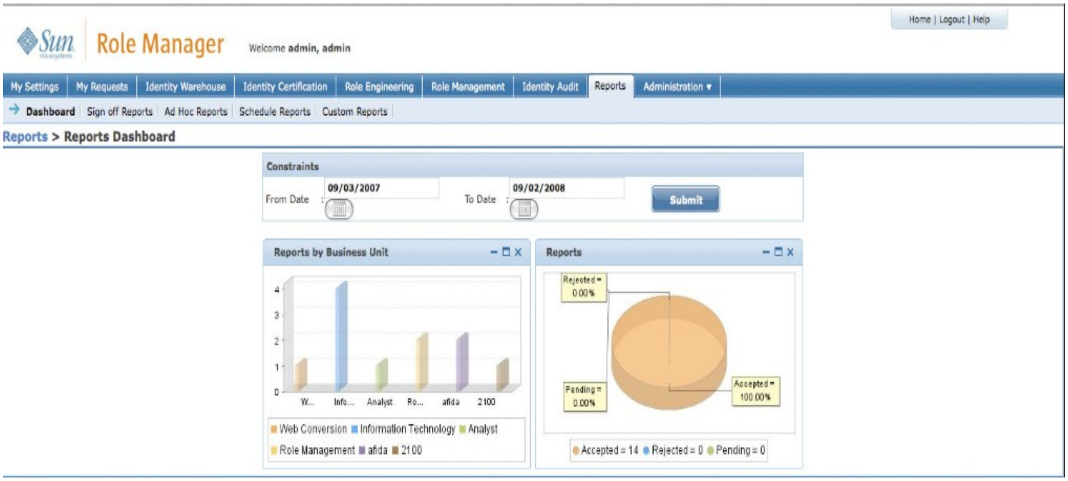
11/11/05 5:32 AM

Page 1 of 1

Figure 8.5 – Report Details

Reporting Dashboard

The reporting dashboard allows administrators to validate the number of reports that are pending, approved or rejected by data owners or managers and the number of reports that have been generated per business unit as shown below.



From Date : 09/03/2007

To Date : 09/02/2008

Figure 8.6 – Reports Dashboard

Appendix A

TABLE OF FIGURES