User's Guide (Printable)

Added by K-2, last edited by K-2 on Oct 01, 2009

Sun Role Manager 5.0 User's Guide

About This Guide

This guide describes how to use the Sun™ Role Manager 5.0.3 software. Some of the topics that are covered in this guide include granting employees and partners access to applications, checking for access violations, modifying access based on changes, and identifying, assessing, and prioritizing segregation of duties (SoD).

Who Should Read This Guide

This guide is written for business managers and other users in a supervisory role who need information about how to use the Sun Role Manager 5.0.3 software to grant employees and partners access to applications, check for access violations, and so on.

- Compliance officers and IT specialists who need to configure and maintain role management and compliance functionality should see the ***Sun Role Manager 5.0.3 Business Administrator's Guide***.
- System administrators, deployment engineers, and service providers who need information about how to administer the Sun Role Manager software at a systems level should see the ***Sun Role Manager 5.0.3 System Administrator's Guide***.
- Deployment engineers who are responsible for integrating Sun Role Manager with other IT systems should see the ***Sun Role Manager 5.0.3 System Integrator's Guide***.

Sun Role Manager Overview

This chapter covers the following topics:

- Introduces the role-based access control (RBAC) model
- Describes the many benefits that Sun Role Manager extends to organizations with large numbers of employees
- Introduces the software's major functional areas
- Introduces terminology that you need to know in order to be successful with Sun Role Manager

Introducing the Role-Based Access Control Model

With the enactment of strict compliance-related legislation, like the Sarbanes-Oxley (SOX) Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley (GLB) Act, it has become imperative for companies to secure their information and exercise control over access to mission-critical applications within the organization. Sun Microsystems understands that organizations today need a strong governance environment around access control. To establish strong governance, a robust framework around access control is necessary. This can be attained using the Role Based Access Control (RBAC) framework and an enterprise-wide role definition effort.

Role-based access control (RBAC) limits access to system applications to only authorized users within an organization. The model simplifies identity and access control compliance by managing access based on a user's roles within a company, not on an individual, user-by-user basis. Roles are created based on usage and enterprise policies. For example, new employees need access to certain system applications in order to perform their job responsibilities. Using the RBAC model, the new employees can be assigned to existing roles, which automatically give them access to the necessary set of system applications. Business managers are required to check and certify or revoke access to system applications on a regular basis.

Understanding Sun Role-Manager Benefits

Sun™ Role Manager 5.0.3 software (Role Manager) addresses all aspects of role-based access control. The software allows organizations to streamline the access-control process, simplify attestation, and enhance audit effectiveness, thereby resulting in secure and robust role management.

Role Manager enables you to accomplish the following tasks:

- Simplify the assignment and management of user access
- Create and manage roles rather than users
- Achieve compliance by way of access certifications and separation of duties (SoD)
- Align business and IT processes with a common terminology for IT access permissions
- Ensure an ongoing understanding of access: who has it, who approved it, and what access violations exist
- Reduce the risk of security violations and access control-related deficiencies
- Manage the role lifecycle through the use of workflows, versioning, consolidation, history, and ownership
- Provide complete rule lifecycle management to effectively manage the rapid on-boarding and off-boarding of users

Understanding the Sun Role Manager Model

Sun Role Manager is organized into the following modules: Identity Warehouse, Identity Certification, Role Engineering and Management, and Identity Auditing.

Identity Warehouse

The Identity Warehouse is a central repository that contains data on user entitlements. This data is imported from one or more databases within your organization on a scheduled basis. The Role Manager import engine supports complex entitlement feeds saved as either text or XML files. Extract, Transform, and Load (ETL) processing capabilities are also available. Imported data is then correlated or mapped to various roles during the certification phase. A glossary description of each entitlement is also captured during the import process.

top

Identity Certification

Managing and auditing enterprise-wide attestations is a major challenge to companies with a large number of employees. Because individual users may have access to a multitude of platforms, systems, and applications, organizations need an easy-to-use tool that managers can use to review user entitlements on a regular basis. Moreover, federal requirements require time-based certifications, granular entitlements, and so on.

Role Manager's identity certification module makes user entitlements easy to monitor and distribute. Managers can easily communicate with IT administrators to monitor, authorize, add, or revoke application access based on changes. The Sun Role Manager identity certification module allows managers to collect, manage, and distribute user entitlements. In addition, these certifications can be scheduled depending upon the compliance requirements of the entitlement certification.

The identity certification module can perform four types of certifications:

1. **User Entitlement Certification**. Allows managers to certify employee access to roles and other related entitlements.
2. **Role Entitlement Certification**. Allows role owners to certify roles and role content.
3. **Resource Entitlement Certification**. Allows resource owners to certify user access to resources.
4. **Data Owner Certification**. Allows data owners to certify users.

Each certification addresses different audience types and ensures stringency at every step of the access management process.

top

Role Engineering and Management

Role-based access control is one of the complex and challenging efforts carried out in security administration. RBAC restricts access of the systems to authorized users by using predefined and approved roles. Within an organization, roles are seldom stationary. With a dynamic business environment, role management is also in a constant state of flux. New roles need to be created while old ones need to upgraded or managed on a regular basis.

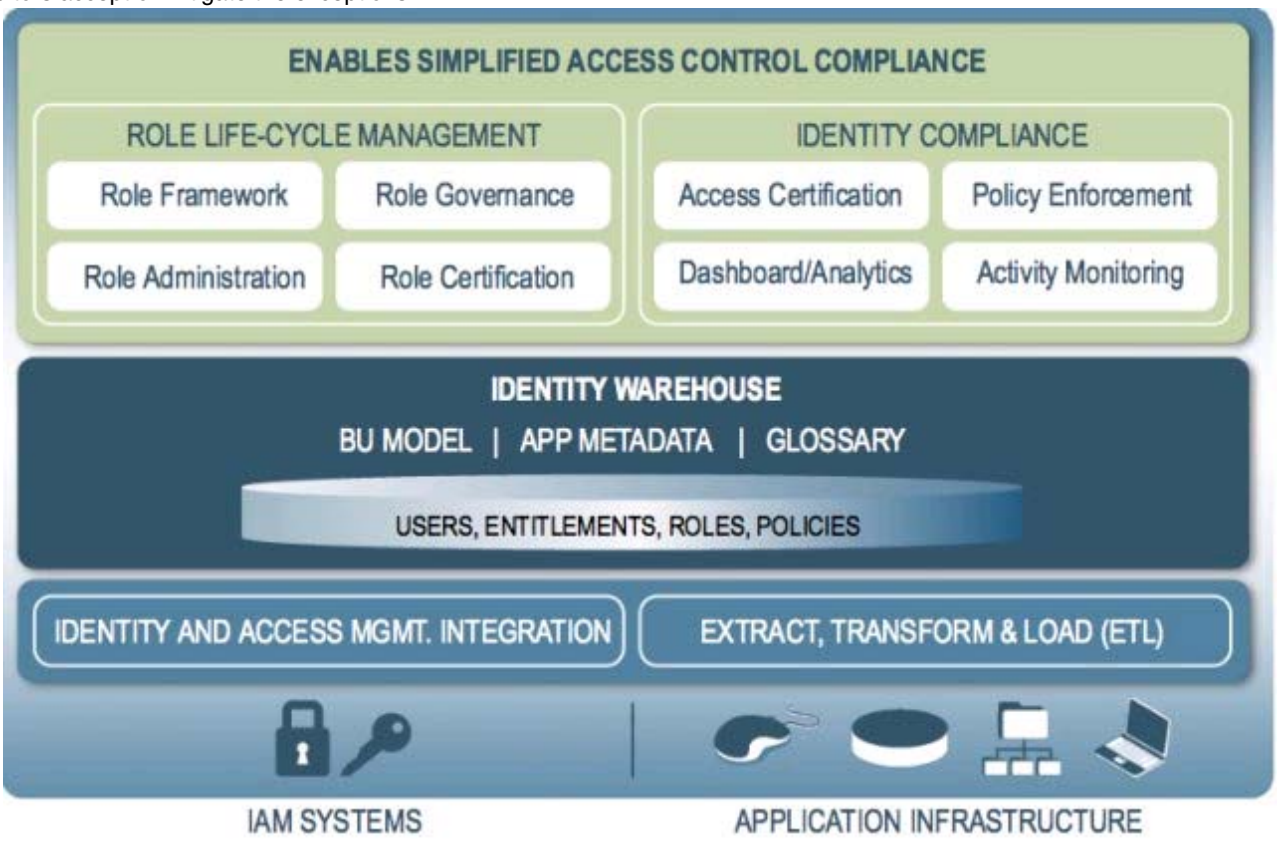
The Role Manager software is a good alternative to manual access control methodologies because its superior framework facilitates easy management of users and their access to roles in a controlled and effective manner. Sun Role Manager provides a complete setup of security, workflow, and auditing features to manage the lifecycle of roles. The built-in workflow engine provides the ability to configure the best suited workflow processes depending on the business requirements and allows stakeholders to call external functions from the workflows. This functionality enables greater efficiencies from a role-based access control model. Additionally, multiple rules and a combination of attributes (such as job codes, department, and location) can be used to assign role-based access to new and existing users.

top

Identity Auditing

Today, organizations need to manage Continuous Exception Monitoring, Segregation of Duty (SoD) Violations, Detective Scanning, Inter and Intra-Application SoD Enforcement, Actual vs. Assigned Exceptions, Exception Lifecycle Management, and so on. Organizations also tend to have numerous exceptions related to the access users have to target systems.

Close monitoring is an integral part of Sun Role Manager. The identity auditing module has a detective mechanism that monitors users' actual access to resources and captures any violations on a continuous basis. The software can also be programmed to conform to audit policies and to report exceptions. It provides a summary of all exceptions, which helps security analysts, executives, or auditors accept or mitigate the exceptions.



top

Understanding Sun Role Manager Components and Terminology

This section introduces Sun Role Manager components and defines terminology that you need to know in order to be successful with the software.

Understanding Users

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

Users are associated with business structures in various ways. A user can be assigned to several business structures based on access level and other details within an organization. A business user has a *manager* or an *application approver* who is tasked with carrying out various user- and role-management functions on the user.

top

Understanding Resources and Resource Types

Resources are the applications and enterprise information assets that users need to do their jobs. In Role Manager, a resource is an instance of a *resource type*, which is a grouping of like resources. For example, multiple Oracle® database instances may compose a resource type named Oracle. Each database instance is a resource.

Common resource types include platforms (Windows 2000, UNIX®, Mainframe) or business applications (such as, billing and accounts payable applications). Each resource has an owner who handles the various operations on the resource, such as reviewing user entitlements. The user entitlements are collected from different resources and stored in a central repository.

Note - In previous releases, the term *endpoint* was used to denote a resource, while the term *namespace* was used to denote a resource type.

---

top

Understanding Business Structures

A *business structure* in Role Manager is defined as a department or sub-department within an organization. An organization can be segregated into as many business structures, with as many levels of hierarchy as is required to represent teams and sub-teams within the organization. There is no limit to the number of users that can be assigned to a business structure. All operations in Role Manager such as identity auditing and identity certification are performed on the basis of a business structure.

top

Understanding the User Store

The *user store* is the central platform or database or directory where user records are stored. Commonly used user stores include Active Directory, Exchange, ORACLE, SAP, UNIX, and RDBMS Tables.

Initially, an organization in Role Manager is populated with users using a feed from an HR system. The HR system is used to create all the global identities in Role Manager. Alternatively, the global identities can be created from a provisioning system such as Sun Identity Manager.

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

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, which shows the entire list of users that belong to the organization.

A naming convention for all users needs to 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.

top

Understanding Roles

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

Roles give you the flexibility and power to enforce enterprise standards, so that you can do the following:

- 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 required in an organization.
top

Understanding Policies

Policies define account attributes and privileges that users have on different platforms or applications. A policy has a specific privilege on a 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.
top

Understanding Orphan Accounts

An *orphan account* is an account that belongs to a user who is no longer with the organization or controlling business unit. (The user may have left the organization or shifted departments, but the account was not deactivated when the user left or moved.)

top

Using the Sun Role Manager User Interface

Logging In to Sun Role Manager

To open the Sun Role Manager user interface, you need a supported browser. For a list of supported browsers, see the Compatability Matrix chapter in the *Sun Role Manager Installation & Upgrade Guide*.

▼ To Log In to the User Interface

1. Open the Role Manager login page by typing the URL into your browser, or by clicking the Role Manager icon (if available).
   The login page opens.
2. Enter your user name and password.
   If your user name and password are accepted, the Role Manager home page opens.

Using the Sun Role Manager User Interface Menu

The Sun Role Manager user interface menu organizes the interface into multiple sections or modules. Most modules have a secondary row of tabs (or views) that further organize Role Manager functionality.

The following table provides a brief description of the top-level tabs that are available in the Sun Role Manager interface. Depending

on your role and entitlements, only some tabs may be visible to you.

Tab or Module	Description
Home	Click to view a dashboard that summarizes whether you have any requests or identity certifications to approve, complete, or dismiss. This screen is displayed upon logging in to Role Manager. For help, including information on how to open the Home page, see the Home Page .
My Settings	Click to view information about your Sun Role Manager account, including your name, password, and email address, as well as information about your proxy assignments. Proxy assignments enable you to delegate approvals and certifications to another user while you are away from the office.
My Requests	Click to view and either approve or reject pending requests, such as role change requests and membership change requests. You can also view completed requests on a separate subtab.
Identity Warehouse	Click to create, view, and manage business structures, users, roles, policies, and resources.
Identity Certification	Click to view the certification dashboard. Additional tabs allow you to create, view, search, manage, and complete certifications. Identity certifications are conducted periodically to verify that users have access only to the proper entitlements on the assigned systems.
Role Management	Click to perform role consolidation, entitlements discovery and Rules for Role Assignments. This module is primarily intended for use by administrators.
Identity Audit	Click to create audit rules and audit policies, and to scan for audit violations.
Reports	Click to access various reports, including business unit reports, system reports, audit reports, and custom reports.
Administration	Click to configure and maintain Sun Role Manager. This module is primarily intended for use by administrators.

top

The Home Page

Home Page

The home page contains a dashboard with five charts or graphs that represent important data related to workflow requests, certifications, approvals, and policy violations. You can select whether the dashboard displays vertical charts, horizontal charts, or pie charts.

Figure - Role Manager Home Page

▼ To Open the Home Page

1. Log in to Role Manager.
2. Click Home in the upper right corner of the screen.
   The Home page opens.

top

My Requests

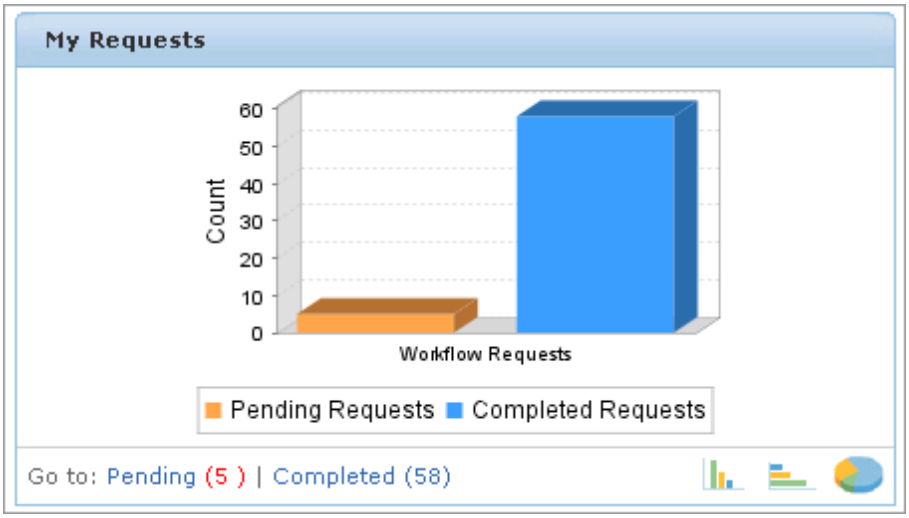


Figure - My Requests

The My Requests chart shows how many workflow requests are completed and how many are awaiting action from the user. Click the Pending and Completed links to open the requests approval page. Click the  icons to view a different chart type.

My Certifications

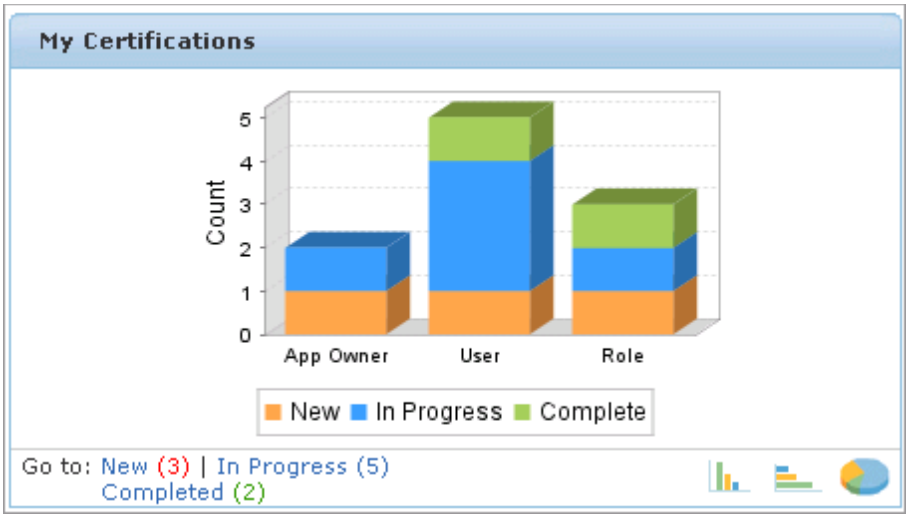


Figure - My Certifications

The My Certifications chart displays information about New, In Progress, and Completed certifications. Click the Pending, In Progress, or Completed links to open the Certification inbox that contains the appropriate certifications. Click the  icons to view a different chart type.

Business Structure Users

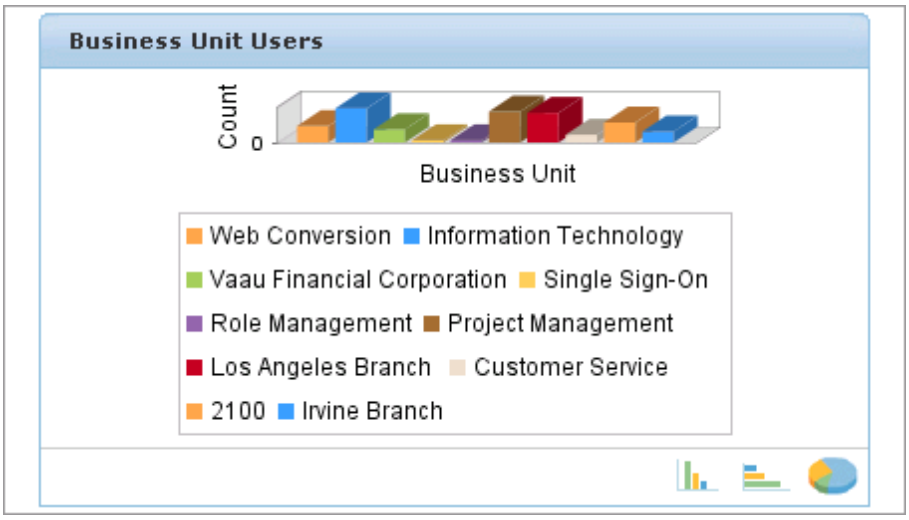


Figure - Business Structure Users

The Business Structure Users chart displays the number of users that belong to each business unit. Click the  icons to view a different chart type.

Certify/Revoke Statistics

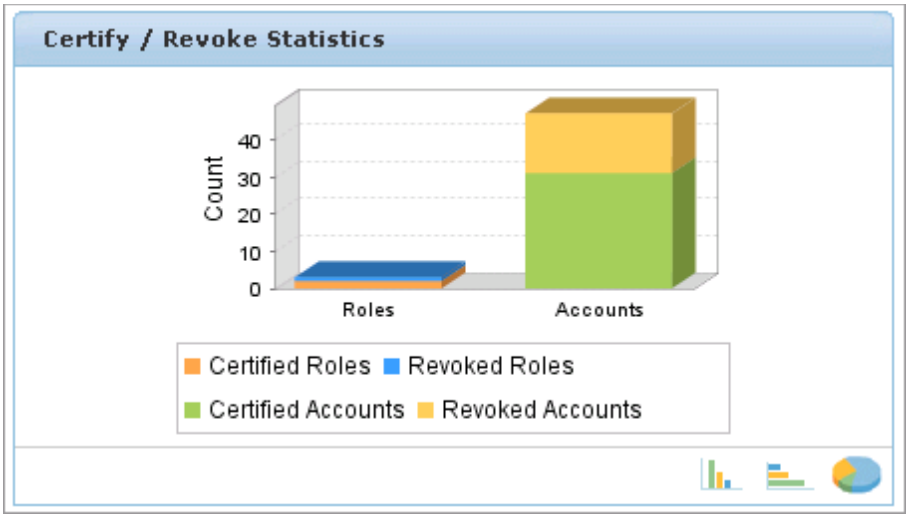


Figure - Certify / Revoke Statistics

The Certify/Revoke Statistics chart displays the number of roles and accounts that are certified and revoked during a certification process. Click the  icons to view a different chart type.

Identity Audit Policy Violations

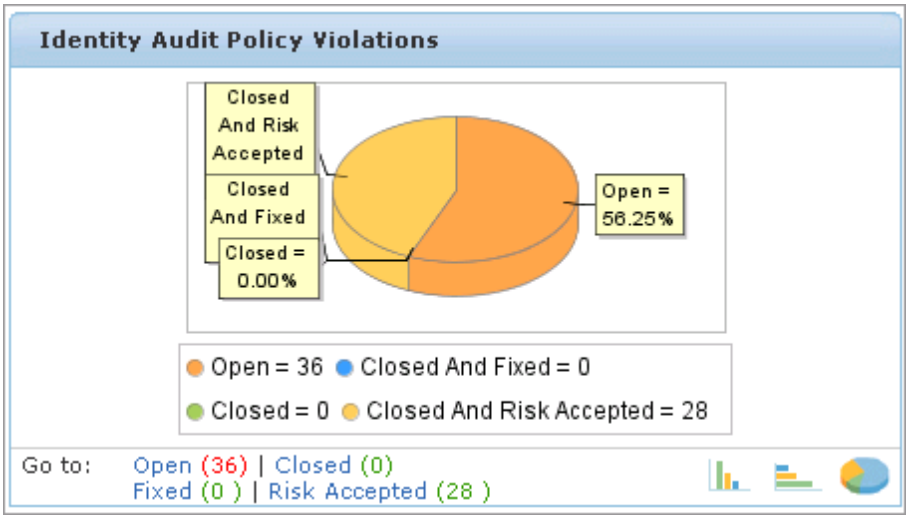


Figure - Identity Audit Policy Violations

This chart displays the number of open, closed, and risk-accepted identity audit policy violations. Click the links to view the corresponding violations. Click the  icons to view a different chart type.

top

My Settings

My Settings Tab

Use the My Settings Tab to manage your Sun Role Manager user account and to manage your delegations while you are out of the office.

My Profile

Click My Profile to change your first and last name and email address.

Figure - My Profile Page

▼ To Change Your User Name and Email Address

1. Log in to Role Manager.
2. Choose My Settings > My Profile.
3. Edit the First Name, Last Name, and E-Mail fields and click Save.

top

▼ To Change Your Password

1. Log in to Role Manager.
2. Choose My Settings > My Profile.
3. Click Change Password.
   The Change Password pop-up window opens.
4. Complete the form and click OK.
5. Click Save.

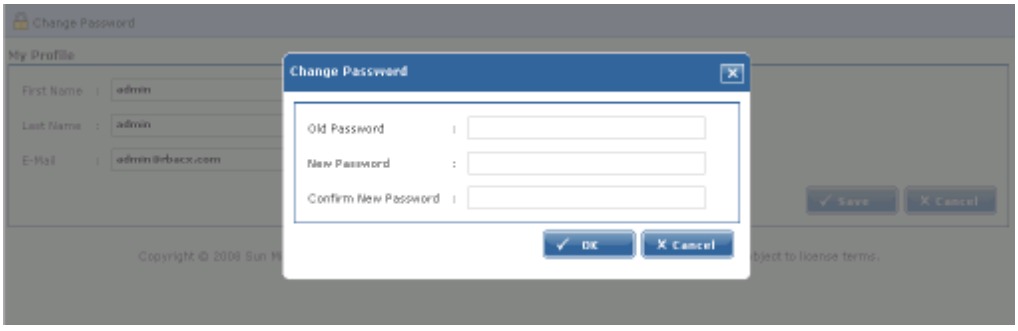


Figure - Change Password

top

My Proxy Assignments

Click My Proxy Assignments to delegate certification-related duties to another user while on vacation or out of the office. Delegations cannot be set for more than 30 days.

top

▼ To Delegate Certification-Related Duties to Another User

1. Log in to Role Manager.
2. Choose My Settings > My Proxy Assignments.
3. Click New Proxy Assignment.
   The New Proxy Assignment page opens.
4. Complete the form.
   - The start date should be set to the date that you will leave.
   - The end date should be set to the date that you will return. Proxy users will not be able to delegate on your behalf on the end date.
   - Delegations cannot be set for more than 30 days.
5. Click Save.
   A new Proxy Assignment will be created. As of the start date, the designated proxy can log in to Role Manager and perform the tasks that you designated up until the specified end date.

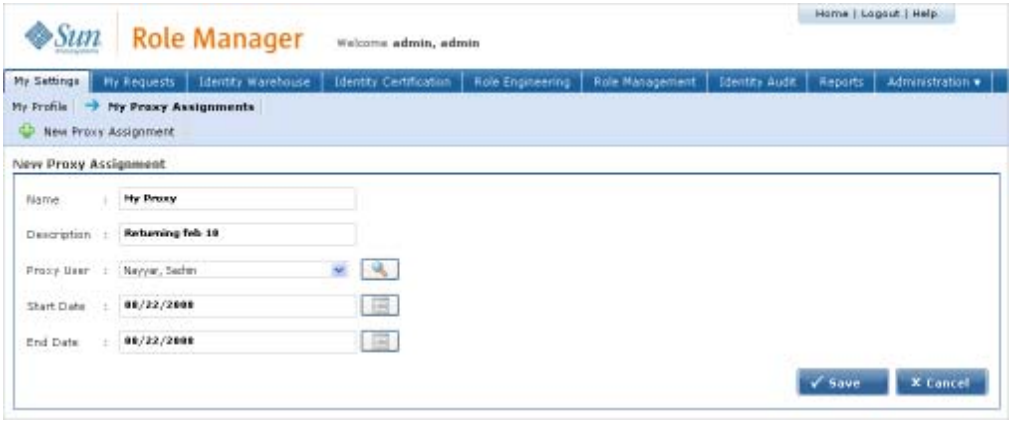


Figure - Enter Proxy Details

top

My Requests

My Requests Tab

Use the My Requests Tab to view and either approve or reject pending requests, such as role change requests and membership change requests. You can also view completed requests on a separate subtab.

▼ To Approve Pending Requests

1. Log in to Role Manager.
2. Choose My Requests > Pending Requests.
   The requests are listed.
3. Click View to view a request in detail.
4. Click either Approve or Reject, as desired.
   The object is listed in the Completed Requests tab.

▼ To View Completed Requests

1. Log in to Role Manager.
2. Choose My Requests > Completed Requests.
   The completed requests are listed.

3. Click View to review the details of a request.

Note - If a role or policy owner is not assigned, then Role Manager automatically approves any changes made.

Identity Warehouse

What Is the Identity Warehouse?

The Identity Warehouse is a central repository that contains all of the important entitlement data for your organization. This data is imported from your organization's databases on a regular, scheduled basis. The Sun Role Manager software has an import engine that supports complex entitlement feeds. The engine accepts either text or XML files, and includes Extract, Transform, and Load (ETL) processing capabilities. The engine also captures the glossary description of each entitlement.

top

Understanding the Identity Warehouse User Interface

This section provides help using the Identity Warehouse portion of the user interface.

Business Structures

To open the Identity Warehouse - Business Structures page, choose Identity Warehouse > Business Structures from the main menu.

The Business Structures page has the following subtabs:

Subtab	Description
General	Displays basic information including type, division, and owner. Also provides information about the status of the business structure. Actions can only be taken on a business structure if it is in the active state.
Users	Displays all users who are part of the selected business structure.
Roles	Displays all the roles associated with the selected business structure.
Policies	Displays all the policies associated with the selected business structure.
Relationship Map	Displays the relationship hierarchy with other business structures.

Users

To open the Identity Warehouse - Users page, choose Identity Warehouse > Users from the main menu.

This page displays user name, first name, last name, and primary email information. Quick search and advanced search are provided.

Roles

To open the Identity Warehouse - Roles page, choose Identity Warehouse > Roles from the main menu.

The Roles page is divided into the following sections:

- The right top section is where the search feature is located. Search results are displayed in the search tab on the left-hand side of the page.
- The left top section displays roles in the organization.
- The left bottom section displays roles that have been revised, but not approved.
- The right side displays the following subtabs:

Subtabs	Description
General	Displays basic information about the role, such as the role type. A role can be one of the following types: • Provisioning role: Entitlement roles used in Identity Manager or other provisioning solutions. • Access Control role: Roles which capture policies for products that are integrated with Role Manager like Siteminder and Open SSO. • Organizational role: Roles which are job functional roles, such as Consultant, Analyst, Contractor, etc. This tab also displays the role start date, end date, and status. A role can exist in one of the following states: • Active: Applies to roles that have been approved by the role owner. Only active roles can be acted upon. • Inactive: Applies to old roles. • Composing: Applies to roles that are in the process of being created. Roles in a composing state have not yet sent by an administrator for approval. • Pending Approval: Applies to roles that have been sent by an administrator for approval. • Decommissioned: Applies to roles that no longer exist. All information regarding the role, however, is retained in Role Manager.
Business Structures	Displays the business structures associated with the role.
Policies	Displays the policies that make up the role.
Users	Displays the users who have the role assigned.
Exclusion Roles	Displays conflicting roles. This information is what defines Segregation of Duties at the role level.
Ownership	Displays the owner of the role.
Workflow	Displays the steps that make up the role's workflow.
Custom Properties	Displays the custom properties associated with the role.
Versions	Displays all versions of the role. This section allows you compare two versions and revert to an older version of the role.
History	Displays the role's history. Role history is divided into four sections: role membership history, owner history, policy history, and attribute history.

Policies

To open the Identity Warehouse - Policies page, choose Identity Warehouse > Policies from the main menu.

The policies page is divided into the following sections:

- The left section displays resource types. Policies are displayed below each resource type.
- The left bottom section displays policies that have been revised, but not approved.
- Each policy has the following subtabs:

Subtabs	Description
General	Displays general information about the policy including status and risk level. A policy can exist in one of the following states: • Active: Applies to policies that have been approved by the policy owner. Only active policies can be acted upon. • Inactive: Applies to old policies . • Composing: Applies to policies that are in the process of being created. Policies in a composing state have not yet sent by an administrator for approval. • Pending Approval: Applies to policies that have been sent by an administrator for approval. • Decommissioned: Applies to policies that no longer exist. Role Manager retains all information about the policy, however.
Business Structures	Displays the business structures associated with the policy.
Roles	Displays the roles associated with the policy.
Resources	Displays the resources that are part of the policy.
Exclusion Policies	Displays conflicting policies. This information is what defines Segregation of Duties at the policy level.
Ownership	Displays the policy owner.
Workflow	Displays the steps that make up the policy's workflow.
Version	Displays all versions of the policy.
Entitlements	Displays the resource attributes and values that make up the policy.

Applications

To open the Identity Warehouse - Applications page, choose Identity Warehouse > Applications from the main menu.

The Applications page lists the applications in Role Manager. When you click an application's name, you can view the following information:

Subtab	Description
General	Displays basic information about the application.
Users	Lists all the users that are associated with the application.
Ownership	Lists the assigned owner of the application.
Conditions	Lists the resource type, resource, attribute name and attribute value associated with the application.

To learn more about working with applications, see the Working With Applications section in the *Sun Role Manager 5.0.3 Business Administrator's Guide*.

Resources

To open the Identity Warehouse - Resources page, choose Identity Warehouse > Resources from the main menu.

The Resources page lists all the resources in Role Manager. When you click a resource, you can view the following information:

Subtab	Description
General	Displays basic information about the resource.
Data Management	Displays all the attributes and their corresponding attribute values.
Remediation	Displays remediation settings and information for the resource.

To learn more about working with resources, refer to the Working With Resources section in the *Sun Role Manager 5.0.3 Business Administrator's Guide*.

top

Working With Users

This section contains instructions on how to perform common user tasks in Role Manager.

▼ To Create a User

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. To add a new user, click the New User button on the top panel.
   The Create User pop-up window opens.
4. Complete the form and click OK to create the user.

▼ To Rename a User

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. Search for the user.
   For help using Search, see Searching For a User.
4. Click the user's link in the User Name column.
5. Type a new name for the user and click Save.

▼ To Delete a User

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. Search for the user.
   For help using Search, see Searching For a User.
4. Select the user name for the user that you want to delete, and click the Delete User button.

top

Searching for a User

Role Manager provides quick search and advanced search options for user searches. Quick search enables searching for users on any of the commonly populated user fields (for example, User Name, First Name, Last Name, Business Unit, Department, Manager). Advanced Search should be used to conduct a narrower search and to create complex searches.

▼ To Search for a User (Quick Search)

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. To perform a quick search, choose a field from the drop-down menu.
   All the commonly populated fields are available to search on.
4. Enter a value to search for.
   Wildcards are accepted, for example, `a*` or `j*n*`.
5. To search on the selected field for the entered value, click Search.
   The results for the search are displayed.

▼ To Search for a User (Advanced Search)

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. Click the Advanced Search Tab.
4. Create a condition by selecting values for Attribute, Condition, and Value.
   Attributes can be selected over an extensive range including resources, business units, and any other commonly populated user field. Value supports wildcards, for example, `a*` or `j*n*`.
5. To create more conditions, click Add.
6. To remove conditions, select the condition by selecting its corresponding checkbox and click Remove.
   In the case of multiple conditions, set Operation to `AND` or `OR` to specify the logical operation between the conditions.
7. To group two conditions together, select them and click Group.
   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.
8. To ungroup a grouped conditional, select the grouped conditional by selecting its corresponding checkbox, and click Ungroup.
   The created search condition is dynamically displayed in a highlighted line under the Group and Ungroup tags as a single logical condition.
9. To search on the created condition, click Search.

top

Viewing User Details

▼ To View User Accounts (Entitlements)

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. Search for the required user.
   For help using Search, see Searching For a User.
4. Click to select the User, and click the Accounts tab.
5. Click the required Account to view Account details.

▼ To View a User's Account Type

Account Types help describe accounts. Knowing the *type* associated with an account can be helpful when making decisions during remediation and access certification, and when 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` can then be leveraged while performing identity certifications, role engineering, and remediations, allowing the different Role Manager actors to make educated decisions.

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. Search for a user.
   For help using Search, see Searching For a User.

4. Click to select the user.
5. Click the Accounts tab.
   The account type is listed in the Account Type column.

top

Working With Business Structures

▼ To Delete a Business Structure

1. Log in to Role Manager.
2. Choose Identity Warehouse > Business Structures.
3. Click to select the business structure that you want to delete.
4. Click Delete Business Structures.
   A Delete Business Structures confirmation window opens.
5. Click Yes to delete.
   The business structure is deleted.

▼ To Create a Business Structure Hierarchy

An *n*-level business structure hierarchy can be defined in Role Manager. A business structure can have various child business structures under it.

1. Log in to Role Manager.
2. Choose Identity Warehouse > Business Structures.
3. Click New Business Structure to create a business structure.
   The Create Business Structure window opens.
4. Complete the form as follows:
   - **Name** - Type the name of the business structure.
   - **Parent** - Select the parent business structure from the drop-down menu.
   - **Enter the Service Desk Tick #** - Each business structure can be associated with a unique service desk ticket number if an integration between Role Manager and a ticketing system is used in your organization.
5. Click OK.

top

Associating Users With Roles and Business Structures

▼ To Associate a User With a Role

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. Search for the user that you want to associate with a role.
   For help using Search, see Searching For a User.
4. Select the user and then click the Roles tab.
5. Click the Add Roles button and assign one or more roles to the User.
6. Click Save.

▼ To Associate a User With a Business Structure

1. Log in to Role Manager.

2. Choose Identity Warehouse > Users.
3. Search for the user that you want to associate with a business unit.
   For help using Search, see Searching For a User.
4. Select the user and then click the Business Unit tab.
5. Click the Add Business Unit(s) button, and assign one or more business unit(s) to the user.
6. Click Save.

top

Setting User Status

User status can be set to either *active* or *inactive*. If a user is scheduled to leave the company, the end date of the user can be specified in Role Manager.

▼ To Set User Status

1. Log in to Role Manager.
2. Choose Identity Warehouse > Users.
3. Search for the user.
   For help using Search, see Searching For a User.
4. Select the user.
5. On the General tab, scroll down to the Suspension section.
6. In the Status field, set the status to **Active** or **Inactive** in the drop-down menu.
7. If the user is set as Inactive, specify an End Date for the user.

top

Working With Policies

Policies are templates that define the various access levels that a user has on the target systems. Policies are individually defined for each resource. Roles are made up of policies.

The polices component displays all available policies that exist for the organization categorized according to resource type. Resources are depicted as  . The available policies are shown under each resource type.

▼ To Create a Policy

1. Log in to Role Manager
2. Choose Identity Warehouse > Policies.
3. Click New Policy.
   The Policy Wizard window opens.
4. Select the resource type for which you are creating the policy and click Next.
5. Select the resource for which access needs to be defined and click Next.
6. Click Select Owners to search for the owners for this policy and click Next.
   For help using Search, see Searching For a User.
7. When the Policy Property window opens up, complete the form:
   - **Name** - Type the name of the policy.
   - **Comments** - Type any additional comments about the policy.
   - **Service Desk Ticket #** - Add the helpdesk system reference number, if relevant to your organization.
8. Click the Entitlements tab and complete the form:
   - **Value** - Enter the value of the attribute defined for the resource.
   - **Required** - Selecting this means the value is mandatory and needs to be assigned to the role. This value cannot be

excluded.
- **Risk Level** - Signifies whether a given policy is low, medium, high, critical, or none. These risk levels are flagged during Identity Audit Exceptions or while performing Certifications.
- **+ / -** - Use these to add or delete an attribute value.

9. Click Finish.

The new policy is displayed under the resource type on the Policies page.

▼ To Delete or Rename Policies

1. Log in to Role Manager.
2. Choose Identity Warehouse > Policies.
   - To rename a policy, do the following:
     a. Select the policy by clicking on the policy name.
     b. Change the name of the policy and click Save.
   - To delete a policy, do the following:
     a. Select the policy by clicking on the policy name.
     b. Click the Delete Policy button.

▼ To Associate Policies With Resources

1. Log in to Role Manager.
2. Choose Identity Warehouse > Policies.
   Policies are listed by resource type on the left side of the page.
3. Click to select the desired policy.
4. Click the Resources tab in the panel on the right.
5. Click the Add Resources button.
6. Select one or more resources from the list and click OK.
   Hold down the Control key while clicking to select multiple items. Click an item again while holding down Control to clear that item.
7. Click Save.
   The resource will not be associated with the policy until it has been approved by the policy owner.
8. Click Send For Approval.

Once the policy owner approves it, the resource is associated with the policy.

▼ To Add Policies To Roles

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Select a role and click the Policies tab on the right side of the page to add policies to (or remove policies from) the role.
4. Choose one of the following tasks:
   - Click Add Policies to assign the selected policies to the role.
   - Click Remove Policies to remove the selected policies from the role.
5. Click Save.
   The policies associated with a role will display on the Policies tab for the role.

▼ To Associate Policy Owners With Policies

1. Log in to Role Manager.
2. Choose Identity Warehouse > Policies.
   Policies are listed by resource type on the left side of the page.
3. Click a policy and click the Ownership tab on the right side of the page.
4. Click Add Owner.
5. Select one or more user(s) and click OK.

For help using Search, see Searching For a User.
6. Click Save.

▼ To Approve Policy Change Requests

Modifications to a policy are activated only after the approval of the policy owner.

To approve a policy change request, see To Approve Pending Requests in the My Requests chapter.

▼ To Manage Lifecycle of Policies

The lifecycle of a policy is managed by out-of-the-box workflows. Workflows are step-by-step explanations (flowcharts) that Role Manager follows to complete a selected set of tasks. The workflows can be modified to suit the requirements of your organization.

Role Manager has the following policy workflows:

1. Policy creation workflow
2. Policy modification workflow

The default policy creation and policy modification workflows each have three steps:

- Start workflow: This steps kicks-off once a policy is created or modified.
- Policy Owner Approval: If a policy owner approves the request, the workflow proceeds to the next step. Otherwise, the policy is discarded.
- Finish: The policy is created.

To understand or change policy workflows, refer to the Role Manager Workflows chapter in the *Business Administrator's Guide*.

top

Working With Roles

Role Manager administers role-based access controls. Roles make it easier to assign access levels to users and to audit those assignments on an ongoing basis. Rather than assigning access levels to users directly, access levels are assigned to a role. Roles are assigned to users, and a user's access level is determined by the roles assigned to that user.

Role-based administration typically grows and expands as new situations occur. The main advantage of using this approach is ease of implementation. Role-based administration can be established in a centralized fashion, distributed throughout your network, or hybridized. Role Manager can be configured to match the unique structure and needs of your organization. Roles can be defined in a hierarchical format, and Segregation of Duties (SOD) can be administered through a role.

top

▼ To Search for a Role

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. To use quick search, use the Search panel at the top of the page and choose an option from the drop-down menu.
   Commonly populated fields are available to be searched on.
4. Enter a value to search for.
   Wildcards can be used (for example, `a*` or `j*n*`.
5. Click Search to search the selected field for the value specified.
   Search results are displayed in the Search panel on the left side of the screen.
6. Double-click a role to select it.

Creating Roles

There are three ways to create roles in Role Manager:

- Manually
- From existing roles
- From a global user

▼ To Create Roles Manually

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Choose New Role > Create Role Manually.
   The Create Role pop-up window opens.
4. Complete the form:
   - **Name** - Type a name for the role.
   - **Parent Role** - Click the button to open the Select Role window, select the role that you want to designate as the parent role for the role you are creating, and click OK.
   - **High Privileged** - Select the check box to make this a high privileged role.
   - **Start Date** - Enter the start date. The role will be active on this date.
   - **End Date** - Enter the end date. The role will be inactive after this date.
   - **Service Desk Ticket** - Add the helpdesk system reference number, if relevant to your organization.
5. Click Save to create the role.
   The role is available in the Roles view under the Identity Warehouse tab.

▼ To Create Roles From Existing Roles

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Choose New Role > Create Role Using an Existing Role as Template.
   The Create Role pop-up window opens.
4. Complete the form:
   - **Name** - Type a name for the role.
   - **Template Role** - Click Select Template Role, search for the role that you want to use as a template for the new role, select the role, and click OK.
5. Click Save to create the role.
   The role is available in the Roles view under the Identity Warehouse tab.

▼ To Create Roles Based On an Existing User

You can create a role based on an existing user. All of the entitlements that the selected user has are used to create corresponding policies that are assigned to the new role.

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Choose New Role > Create Role From Existing User.
   The Create Role pop-up window opens.
4. Type a name for the role and click Select User.
   The Search window opens.
5. Use either the user quick search or advanced search feature to search for the user whose entitlements will be used to create policies for the new role.
   For help using the search feature, see To Search For a Role.
6. Select the user and click OK.
7. Click Save to create the role.
   The role is available in the Roles view under the Identity Warehouse tab.

top

▼ To Rename, Modify, or Decommission (Delete) a Role

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Search for a role, or select a role from the Roles panel on the left side of the screen.
   For help using the search feature, see To Search For a Role.
4. Do one of the following tasks:
   - To rename a role, click the General tab, type the new role name in the Name field, and click Send for Approval or Save.
   - To modify a role, type or select the new role properties, and click Send for Approval or Save.
   - To delete a role, click the Decommission Role button.
     Decommissioning a role removes all role-user associations. The role itself, however, is not truly deleted. Instead, the role is made inactive and stored in Role Manager. The role cannot be made active again, and it cannot be modified in any way or assigned to users.

▼ To Associate Roles With Business Units

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Click a role and click the Business Structures tab.
4. Click the Add Business Structures button and select the desired business units.
5. Click Save or Send for Approval.

▼ To Associate Role Owners With Roles

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Click a role and click the Ownership tab.
4. Click the Add Owners button and search for the user (or users) to add.
   For help searching for users, see Searching For a User.
5. Select one or more users.
6. Click Save or Send for Approval.

▼ To Create a Role Hierarchy

Similar to a business unit hierarchy, an *n*-level role hierarchy can be defined in Role Manager. A role can have various "child roles" under it. To define a role hierarchy, add a new child role to it. When a child role is added to a user, the parent role is also automatically assigned to the user. The role hierarchy defines an organized structure of roles. Roles defined in an organization may have a hierarchy associated with them. In addition, enterprise-level roles and application-level roles can be defined.

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
   The role hierarchy is defined when a new Role is created manually.
   - To change a role hierarchy, follow these steps:
     a. Select the role and click the button located next to the Parent Role field on the General tab.
     b. From the list of roles that appear, select the role that you want to designate as the parent role.
   - To select the child role for a user, follow these steps:
     a. Choose Identity Warehouse > Users and search for the user that you want to assign to a role.
     b. Select the user and click the Role tab.
     c. Click the Add Roles button.
        The parent Role is automatically assigned to the user. If the parent role is removed, the child role is automatically removed from the user.

▼ To Approve Role Change Requests

Modifications to a role are activated only after the approval of the role owner.

To approve a role change request, see To Approve Pending Requests in the My Requests chapter.

▼ To Manage the Lifecycle of Roles

The lifecycle of a role is managed by out-of-the-box workflows. Workflows are step-by-step explanations (flowcharts) that Role Manager follows to complete a selected set of tasks. The workflows can be modified to suit the requirements of your organization.

Role Manager has the following role workflows:

- Role creation workflow
- Role modification workflow
- Role membership workflow

The default role creation, role modification, and role membership workflows each have four steps:

1. Start workflow: This steps kicks-off once a role is created, modified, or a member is added or removed.
2. Policy Owner Approval: If a policy owner approves the request, the workflow proceeds to the next step. Otherwise, the role is rejected.
3. Role Owner Approval: If a role owner approves the request, the workflow proceeds to the next step. Otherwise, the role is rejected.
4. Finish: The role is created or modified.

To understand or change role workflows, refer to the Role Manager Workflows chapter in the *Business Administrator's Guide*.

top

Setting the Segregation of Duties at the Role and Policy Levels

Define Segregation of Duties (SoD) to separate certain duties or areas of responsibility so that they cannot be assigned to the same person. By defining Segregation of Duties, you reduce opportunities for unauthorized modification or misuse of data or services. 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 has control over all phases of a transaction. Role Manager performs SoD at the role and policy levels.

▼ To Define Segregation of Duties at the Role Level

1. Log in to Role Manager.
2. Choose Identity Warehouse > Roles.
3. Click a role, then click the Exclusion Roles tab.
4. Click Add Exclusion Roles.
5. Add the roles that need to be excluded.
6. Click Save or Send For Approval.

▼ To Define Segregation of Duties at the Policy Level

As with roles, segregation of duties can be defined at the policy level.

1. Log in to Role Manager.
2. Choose Identity Warehouse > Policies.
3. Click a policy to select it and go to the Exclusion Policies tab.
4. Click Add Exclusion Policies.
5. Add the policies to be excluded.
6. Click Save or Send For Approval.

As with roles, when a policy is added to a role, the excluded policies cannot be assigned to a role.

top

Identity Certification

This chapter describes the identity certification user interface pages and includes information about how to complete identity certifications. An overview of identity certification is presented first.

Identity Certification Overview

This section describes what, why, and how identity certifications are conducted. It also discusses who is typically involved in the identity certification process.

What Is Identity Certification?

Identity certification is the process of reviewing user entitlements to ensure that users have not acquired entitlements that they are not authorized to have. Certifications can be scheduled to run on a regular basis to meet compliance requirements. Managers use the Role Manager Identity Certification module to review their employees' entitlements to access applications and data. Based on changes reported by Role Manager, managers can authorize or revoke employee access, as needed.

The following table lists the four types of identity certification that are possible in Role Manager.

Identity Certification Type	Description
User Entitlement Certification	Allows managers to certify employee access to roles and other related entitlements.
Role Entitlement Certification	Allows role owners to certify roles and role content.
Resource Entitlement Certification	Allows resource owners to certify user access to resources.
Data Owner Certification	Allows data owners to certify users.

Business administrators are tasked with creating certifications for their organizations. For information about creating certifications, see the *Sun Role Manager 5.0.3 Business Administrator's Guide*.

Who Is Involved in Completing Identity Certifications?

The identity certification module in Role Manager allows personnel in an organization to review and certify user entitlement data, role content data, and application access data. Following are descriptions of the types of users that are typically involved in the identity certification process, as well as the certifications that each user type can authorize or revoke. In Sun Role Manager, personnel who participate in the identity certification process are called *actors*.

Actor Name	Description	Certification Types That Can Be Accessed
Certifier	A generic term that signifies a person who is responsible for reviewing and completing any kind of certification.	• User entitlement certification • Role entitlement certification • Resource entitlement certification • Data owner certification

top

Understanding the Identity Certification User Interface

This section provides help using the Identity Certification portion of the user interface, which you access by clicking Identity Certification on the main menu.

The Dashboard

To open the identity certification dashboard, choose Identity Certification > Dashboard from the main menu.

The identity certification dashboard summarizes status information for certifications in progress. The information presented is customized based on your user access. For example, if you are logged in as an administrator with global access, the dashboard presents certification data for the entire organization. If you are logged in as a manager, however, the dashboard only presents information relevant to your particular business units.

The identity certification dashboard presents the following information.

Dashboard Panel	Description
Certifications by Status	This bar graph compares certification statuses (new, in progress, complete, and expired) for each of the four certification types (user, role, resource, and data owner).
Summary	Provides the total number of users, accounts, resource types, and resources that are defined in Role Manager for your organization.
User Accounts Certification Status	This pie chart shows how many user accounts are marked as certified, revoked, and incomplete.
Notifications Issued in Last Week	This bar graph shows how many reminders have been sent in the last week to managers, senior managers, and the IT security department.
Statistics	Provides the average number of certifications per business structure, the average number of roles per user, the average number of accounts per user, and the average number of users in the average business structure.
User Roles Certification Status	This pie chart shows how many user roles are marked as certified, revoked, or incomplete.

My Certifications

To open the My Certifications page, choose Identity Certification > My Certifications on the main menu.

Use the My Certifications page to view and search for access certifications. If you are an administrator, you can create new access certifications from this page.

The first My Certifications page displays new and in-progress certifications. Filters are provided to view all certifications, or any combination of new, in-progress, complete, or expired certifications. Click any column header to sort the table by the column type. Click again to reverse-sort the table.

- Click Edit Certification to view progress and to conduct employee verification on the selected certification.
- Click Complete Certification to complete a certification process.
- Click View Reports to view a report of a completed certification.

Remediation Tracking

To open the Remediation Tracking page, choose Identity Certification > Remediation Tracking from the main menu.

Use the Remediation Tracking page to track the remediation status of revoked accounts, access within accounts, or roles.

This page is visible only to administrators. For details and instructions, see the Understanding Remediation Tracking section in the "Role Manager Identity Certifications" chapter in the *Sun Role Manager 5.0.3 Business Administrations Guide*.

Certification Jobs

To open the Certifications Jobs page, choose Identity Certification > Certification Jobs from the main menu.

Use the Certification Jobs page to view and delete certification jobs.

This page is visible only to administrators. For details and instructions, see Scheduling Certifications.

top

Finding and Reassigning Certifications

This section describes how to search for certifications and delegate certifications that are assigned to you to someone else.

▼ To Search for a Certification

1. Log in to Role Manager.
2. Choose Identity Certification > My Certifications.
3. Choose an option in the Show Me drop-down menu to display the desired certifications.
   The Show Me drop-down menu displays the following options: New & In Progress, All, New, In Progress, Complete, and Expired.
4. Click the expand icon on the left side of the page to display the Search panel.
   You can search a certification using the following fields: Certification Name, Business Structure, Created By, Updated By.
5. Complete the search form and click Search.

- Click Complete Certification to complete a certification process.
- Click View Reports to view reports for a complete, in progress, or expired certification.
- Click View Reminder Logs to see the certification notifications sent, receiver and date.

▼ To Delegate a Certification to Another User

If you will be unable to complete certifications for a period of time, you can delegate certifications to another user to complete. Refer to the Delegating Certification-Related Duties to Another User section to delegate a certification completion task to another manager.

If, however, you want to delegate a particular certification to someone else, follow these steps:

1. Log in to Role Manager.
2. Choose Identity Certifications > My Certifications.
3. Click the certification assigned to you.
   The certification page opens.
4. Click the Show Details button on the right side of the Certification Details section.
   Your name will be displayed as the certifier in the Certification Overview box.
5. Click the Search icon to search for a user to delegate the certification to.
   For help using Search, see Searching For a User in the Identity Warehouse chapter.
6. Click Close.

top

Completing Certifications

This section describes how to complete access certifications in Role Manager.

If closed-loop remediation is configured, you can directly de-provision the accounts you revoke. Closed-loop remediation is a feature that allows you to directly revoke roles and entitlements from the provisioning solution as a result of roles and entitlements revoked during the certification process. This feature is applicable only if the provisioning solution is Sun Identity Manager.

However, for non-managed applications, you can manually revoke roles and entitlements by using the information stored in the remediation configuration module.

To know how to de-provision accounts during a certification process, see To De-provision Accounts During The Certification

Process. When roles are revoked, Role Manager directly de-provisions them as it is the authoritative source for roles.

▼ To Complete a User Entitlement Certification

User Entitlement Certification enables managers to certify employee access to roles and related entitlements. User Entitlement Certification is a two-step process: Step one involves certifying or revoking access to an account, while step two involves certifying or revoking access to roles and the entitlements assigned outside of roles.

Note - During certification, to obtain additional information about users, roles, attributes, and policies, click the More Info link. See Getting More Information About User Accounts, Roles, Attributes, and Policies for help.

1. Log in to Role Manager.
2. Choose Identity Certifications > My Certifications.
3. To search for specific certifications, use the Show Me drop-down menu, or click the Search panel on the left side of the page. Certifications use the following naming convention: *Name-of-the-certification_Certifier's-last name_Certifier's-first-name*.
4. Click a certification to open it.
5. To view certification details, click Show Details on the right side of the page.
   See Certification Details Help to understand the information displayed.
6. Scroll down to the section titled Step 1: Employment Verification.
   In this step you verify that the listed employees work for you and also that you are responsible for verifying their assigned roles and entitlements.
7. Use the drop-down menu in the last column to assign a status update to each employee:
   - **Works for me** - The employee works for you and you are responsible for verifying his assigned roles and entitlements.
   - **Does not work for me** - The employee does not work for you and you are not responsible for verifying his assigned roles and entitlements.
   - **Reports to** - The employee reports to another manager. Select the manager who is responsible for verifying this employee's assigned roles and entitlements. You will not approve or revoke roles and entitlements for this employee in Step 2 of the certification process.
   - **Terminated** - The employee is no longer part of the organization. The employee is removed from the certification process and you will not approve or revoke roles and entitlements for this employee in Step 2.
     Note - To save time, use the global drop-down menu to make a selection for all of the employees listed.
8. Click Go To Step 2.
   In Step 2 you will approve or revoke roles and entitlements for the employees that work for you.
   The Approve or Revoke Roles and Entitlements page opens.
   Note - Use the Group Data By drop-down menu to select how you would like to see employees listed on the page. You can sort by the following variables: My Employees, Applications, Location, Job Code, Manager, Office Name, Department, Employee Type, Title, Country and State.
9. Click to expand each employee's role and entitlement information.
10. Information about the employee is listed. Information includes the name of the employee, designation, Employee Identification (EID) number, phone, and email ID.
11. Review each role and entitlement before completing the form.
    When completing the form, be aware of the following:
    - You can click the Certify All, Revoke All, Unknown All, or Exception Allowed All links. Clicking these links will change the status of all accounts and entitlements.
    - You can use the top-most drop-down menu to certify access to an employee account, while choosing Revoke, Unknown, or Exception Allowed to act on individual entitlements listed under that account.
    - When evaluating an employee's entitlement access, if you select Revoke, Unknown, or Exception Allowed from the top-most drop-down menu, you will lose the ability to enter line-item information for each entitlement. If you need to be able to evaluate individual entitlements, do not choose Revoke, Unknown, or Exception Allowed from this menu.
12. Use the top-most drop-down menu to select from the following list of actions:
    - **Certify** - The employee's access is valid.
    - **Revoke** - The employee's access is not valid and should be revoked. When selecting Revoke, you are prompted to annotate this record with a comment.
    - **Unknown** - You do not know if the employee's access is valid. The employee's access is neither certified nor revoked. The employee's access details appear in the certification report for post-certification action. When selecting Unknown, you are prompted to annotate this record with a comment.

- **Exception Allowed** - You temporarily certify access even though the access might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.

13. Do one of the following:
    - To complete the certification, click Yes and enter your password.
    - To edit the certification or return to the certifications page, click No.

top

▼ To Complete a Role Entitlement Certification

Role Entitlement Certification enables role owners to certify roles and role content. This certification is a two-step process: Step one involves verifying that you are responsible for the roles listed, while step two involves certifying or revoking access to the individual entitlements that define the role.

Note - During certification, to obtain additional information about users, roles, attributes, and policies, click the More Info link. See Getting More Information About User Accounts, Roles, Attributes, and Policies for help.

1. Log in to Role Manager.
2. Choose Identity Certifications > My Certifications.
3. To search for specific certifications, use the Show Me drop-down menu, or click the Search panel on the left side of the page. Certifications use the following naming convention: *Name-of-the-certification_Certifier's-last name_Certifier's-first-name*.
4. Click a certification to open it.
5. To view certification details, click Show Details on the right side of the page.
   See Certification Details Help to understand the information displayed.
6. Scroll down to the section titled Step 1: Role Verification.
   In this step you verify that you are responsible for the listed roles and the policies and entitlements that are linked to the role.
7. Use the drop-down menu in the right-most column to assign one of the following status updates to each role:
   - **Belongs to me** - You are responsible for the role and the policies and entitlements that are linked to the role. Selecting this option enables role review in Step 2 of the certification process.
   - **Does not belong to me** - You are not responsible for the role. You will not verify the role-associated policies and entitlements for roles that do not belong to you.
     Note - To view information about specific roles, accounts, and attributes, click More Info. See Understanding The Accounts Meta Information dialog box for more information.
8. Click Go to Step 2.
   In Step 2 you will certify or revoke the entitlements that are linked to the role.
9. Click to expand each role's policy and entitlement information.
   Roles contain policies, and policies contain entitlements.
10. Review the policy and entitlement information before completing the form.
    When completing the form, be aware of the following:
    - You can use the top-most drop-down menu to certify a role's entitlements, while choosing Revoke, Unknown, or Exception Allowed, to act on individual entitlements listed under that role.
    - When evaluating a role's entitlements, if you use the top-most drop-down menu to select Revoke, Unknown, or Exception Allowed, you will lose the ability to enter line-item information for each entitlement. If you need to be able to evaluate individual entitlements, do not choose Revoke, Unknown, or Exception Allowed from this menu.
11. Use the top-most drop-down menu to select from the following list of actions:
    - **Certify** - The entitlement is valid for this role.
    - **Revoke** - The entitlement is not valid for this role and should be revoked. When selecting Revoke, you are prompted to annotate this record with a comment.
    - **Unknown** - You do not know if the entitlement is valid. The employee's access is neither certified nor revoked. The employee's access details appear in the certification report for post-certification action. When selecting Unknown, you are prompted to annotate this record with a comment.
    - **Exception Allowed** - You temporarily certify access even though the access might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding

expired end dates.

12. When finished with the role certifications, click Complete Certification.
    The Complete Certification box opens.
13. Do one of the following:
    - To complete the certification, click Yes and enter your password.
    - To edit the certification or return to the certifications page, click No.

top

▼ To Complete a Resource Entitlement Certification

Resource Entitlement Certification involves certifying or revoking employee entitlements on one or more resources. Resource entitlements are entitlements that are assigned directly to an employee and are not assigned to an employee as part of a role.

Note - During certification, to obtain additional information about users, roles, attributes, and policies, click the More Info link. See Getting More Information About User Accounts, Roles, Attributes, and Policies for help.

1. Log in to Role Manager
2. Choose Identity Certifications > My Certifications.
3. To search for specific certifications, use the Show Me drop-down menu, or click the Search panel on the left side of the page.
   Certifications use the following naming convention: *Name-of-the-certification_Certifier's-last name_Certifier's-first-name*.
4. Click a certification to open it.
5. To view certification details, click Show Details on the right side of the page.
   See Certification Details Help to understand the information displayed.
6. Click each resource section to open it.
   One or more user accounts are listed for that resource. Information about the employee is listed. Information includes name of the employee, designation, Employee Identification (EID) number, phone, and email ID.
7. Review the entitlement information before completing the form.
   When completing the form, be aware of the following:
   - You can use the top-most drop-down menu to certify employee access to a resource, while choosing Revoke, Unknown, or Exception Allowed, to act on individual entitlements listed under that resource.
   - When evaluating an employee's entitlements, if you use the top-most drop-down menu to select Revoke, Unknown, or Exception Allowed, you will lose the ability to enter line-item information for each entitlement. If you need to be able to evaluate individual entitlements, do not choose Revoke, Unknown, or Exception Allowed from this menu.
8. Use the drop-down menu to select from the following list of actions:
   - **Certify** - The entitlement is valid for this employee.
   - **Revoke** - The entitlement is not valid for this employee and should be revoked. When selecting Revoke, you are prompted to annotate this record with a comment.
   - **Unknown** - You do not know if the entitlement is valid. The employee's access is neither certified nor revoked. The employee's access information is displayed in the certification report for post certification action. When selecting Unknown, you are prompted to annotate this record with a comment.
   - **Exception Allowed** - You temporarily certify access even though the access might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
9. When finished with the role certifications, click Complete Certification.
   The Complete Certification box opens.
10. Do one of the following:
    - To complete the certification, click Yes and enter your password.
    - To edit the certification or return to the certifications page, click No.

top

▼ To Complete a Data Owner Certification

Data Owner Certification enables data owners to certify whether employees should be able to access data. Data owner certification

is a two-step process: Step one involves verifying that you are the data owner, while step two involves certifying or revoking employee access to the data.

Note - During certification, to obtain additional information about users, roles, attributes, and policies, click the More Info link. See Getting More Information About User Accounts, Roles, Attributes, and Policies for help.

1. Log in to Role Manager
2. Choose Identity Certifications > My Certifications.
3. To search for specific certifications, use the Show Me drop-down menu, or click the Search panel on the left side of the page. Certifications use the following naming convention: *Name-of-the-certification_Certifier's-last name_Certifier's-first-name*.
4. Click a certification to open it.
5. To view certification details, click Show Details on the right side of the page.
   See Certification Details Help to understand the information displayed.
6. Scroll down to the section titled Step 1: Entitlement Verification.
   In this step you verify that you are responsible for the listed entitlements.
7. Use the drop-down menu in the right-most column to assign one of the following status updates to each role:
   - **Belongs to me** - You are responsible for the entitlement listed. Selecting this option enables data access certification in Step 2 of the certification.
   - **Does not belong to me** - You are not responsible for the entitlement listed. You will not verify entitlements that do not belong to you.
8. Click Go to Step 2.
   In Step 2 you will certify or revoke individual employees entitlements to access data that is under your control.
9. Review the entitlement information before completing the form.
   When completing the form, be aware of the following:
   - You can use the top-most drop-down menu to certify employee access, while choosing Revoke, Unknown, or Exception Allowed, to act on individual entitlements listed under that resource or role.
   - When evaluating entitlements, if you use the top-most drop-down menu to select Revoke, Unknown, or Exception Allowed, you will lose the ability to enter line-item information for each entitlement. If you need to be able to evaluate individual entitlements, do not choose Revoke, Unknown, or Exception Allowed from this menu.
10. Use the drop-down menu to select from the following list of actions:
    - **Certify** - The entitlement is valid for this employee.
    - **Revoke** - The entitlement is not valid for this employee and should be revoked. When selecting Revoke, you are prompted to annotate this record with a comment.
    - **Unknown** - You do not know if the entitlement is valid. The employee's access is neither certified not revoked. The employee's access information appears in the certification report for post certification action. When selecting Unknown, you are prompted to annotate this record with a comment.
    - **Exception Allowed** - You temporarily certify access even though the access might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
11. When finished with the certifications, click Complete Certification.
    The Complete Certification box opens.
12. Do one of the following:
    - To complete the certification, click Yes and enter your password.
    - To edit the certification or return to the certifications page, click No.

Certification Details Help

When you are completing a certification (see Completing Certifications), the certification details section displays three boxes:

- Certification Overview
- Certification History
- Export Options

Certification Overview

Details	Description
Certification	Displays the name of the certification. Certifications use the following naming convention : *Name-of-the-certification_Certifier's-last name_Certifier's-first-name*
Business structure	Displays the business structure selected for the certification.
Completed	Displays the progress (in percentage) of the certification completion.
Number of users	Displays the number of users that are part of the certification.
Number of roles	Displays the number of roles that are part of the certification.
Number of accounts	Displays the number of accounts that are part of the certification.
Number of resources	Displays the number of resources that are part of the certification.
Number of attribute values	Displays the number of attribute values that are part of the certification.
Certifier	Displays the name of the certifier.
Search button	Option to delegate the certification to another manager.

Note - You will be able to see the details in the Certification Overview section, depending on the type of certification.

Certification History

Details	Description
Start Date	The date from which the certification is valid.
End Date	The date when the certification expires. Managers cannot review certifications after the expiration date.
Incremental	If a certification is marked as incremental, then certifiers are required to certify only the changes made to a certification after the last time it was certified. Otherwise, certifiers are required to complete the entire certification again.
Created By	Displays the name of the creator of the certification.
Creation Date	Displays the date of creation.
Last Updated By	Displays the name of the user who updated the certification.
Last Update Date	Displays the date of the last update.

Export Options

Export options enable you to work on the certification offline. However, you have to return to the application to complete the certification. You can export the certification to PDF or `.xls` formats.

top

Getting More Information About User Accounts, Roles, Attributes, and Policies

During the certification process you can view additional details about roles, accounts, attributes, and policies by clicking a More Info link. When you click a More Info link, one of four Meta Information pages opens. The following sections provide details about the Meta Information pages.

Role Meta Information Page Help

The Role Meta Information Page consists of four sections:

- **General** - This section includes information about the role.
  - **General tab** - Displays basic information about the role.
  - **Business Structures tab** - Displays business structures associated with the role.
  - **Users tab** - Displays users assigned to the role.
  - **Exclusion Roles tab** - Displays conflicting roles. This helps define Segregation of Duties at the role level.
  - **Ownership tab** - Displays the role owner.
  - **Custom Properties tab** - Displays the custom properties associated with the role.
- **Rules** - This section displays rules associated with the role.
- **Certification History** - This section shows the certification history of the role. Information includes last date of action, the nature of the action, and comments, if any.
- **Policy Entitlements** - This section displays all the policies that are part of the role. All policy-related information, such as business structures, roles, resources, exclusion policies, ownership information, and entitlements, are displayed.

Accounts Meta Information Page Help

The Accounts Meta Information Page consists of four sections:

- **General** - This provides information about the account and its entitlements.
  - **Account** - This lists account information such as name, resource, and domain.
  - **Entitlement** - This lists information about the account's entitlements.
- **Open Audit Exception** - This section shows if the account is part of an open-audit exception. An open-audit exception is a violation that has not been fixed.
- **Certification History** - This section shows the certification history of the account. The information provided here includes a description of the action taken, the date that the action was taken, and comments, if any.
- **User Activity** - This section displays the user's recent account activity. The section is divided into two subtabs:
  - **Alerts -** Displays the alerts raised by the Intellitactics Security Information and Event Monitoring (SIEM) solution when it detects event violations based on the SIEM solution's internally defined rule set. The tab displays the alert title, description, time range, score, and status. These fields display the value captured by the SIEM solution.
  - **All Events -** Displays user activity events, which are collected by monitored endpoints by the Intellitactics SIEM system and reported in Role Manager as daily summarized data. The tab displays the event ID, event type, time range, count, and user ID. These fields display the value captured by the SIEM solution.

Note - The User Activity section will be displayed if Role Manager is integrated with Intellitactics Security Manager, a security information and event monitoring solution. To learn more about Intellitactics Security Manager, see Integrating with Intellitactics Security Manager in the *Sun Role Manager 5.0.3 System Integrator's Guide*.

Attribute Meta Information Page Help

The Attribute Meta Information Page consists of two sections:

- **General** - This section lists the attribute name, value, and glossary information. It also lists the attribute hierarchy, if any.
- **Certification History** - This section shows the certification history of the attribute. The information provided includes a description of the action taken, the date the action was taken, and comments, if any.

Policy Meta Information Page Help

The Policy Meta Information Page consists of three sections:

- **General** - This section includes information about the policy.
  - **General tab** - Displays basic information about the policy.
  - **Business Structures tab** - Displays the business structures associated with the policy.
  - **Ownership tab** - Displays the policy owner.
  - **Resources tab** - Displays all the resources associated with the policy.
  - **Exclusion Policies tab** - Displays conflicting policies. This helps define Segregation of Duties at the policy level.
  - **Roles tab** - Displays the roles associated with the policy.
  - **Entitlements tab** - Displays the attribute and the corresponding attributes values.
- **Open Audit Exception** - This section shows if the account is part of an open audit exception. An open audit exception is a violation, which is not fixed.
- **Certification History** - This section shows the certification history of the account. Information includes a description of the action taken, the date the action was taken, and comments, if any.

top

▼ To De-provision Accounts During The Certification Process

As a certifier, you can directly de-provision the accounts or roles you revoke during the certification process. Please check with your Role Manager administrator if this feature is configured.

To check and de-provision accounts, do the following:

1. Go to Step 2 in the certification process.
2. Here, you will review and certify or revoke access to accounts, attributes, roles, policies and entitlements.
3. Select 'revoke' from the drop-down menu against an account, attribute, role or policy.
4. Click the hyperlinked resource name under the resource column.
5. Follow the steps.

Note - If Role Manager is integrated with Sun Identity Manager, then revoked accounts will be de-provisioned automatically.

top

Viewing Certification Reports

Managers can view or export reports of completed certifications. Various reports are available for each certification type.

▼ To View a Certification Report

1. Log in to Role Manager
2. Choose Identity Certifications > My Certifications.
3. Choose Complete from the Show Me drop-down menu.
   A list of completed certifications is displayed.
4. Click the certification that you want to view.
5. Select the type of report you want to view and click OK.
   The report is displayed.
6. Click Actions to either print or export the report.

Certification Reports Available in Role Manager

This section details the various certification reports that are available in Role Manager.

User Entitlement Certification Reports

Reports Available	Description
Revoked access report	Lists access marked as revoked.
Certified access report	Lists access marked as certified.
Terminated users report	Lists employees that were marked as terminated.
Completed certification report	Comprehensive report of a user entitlement certification. This report includes a list of all employees and their access.

Role Entitlement Certification Reports

Reports Available	Description
Revoked entitlement report	Lists entitlements marked as revoked.
Certified entitlement report	Lists entitlements marked as certified.
Complete certification report	Comprehensive report of a role entitlement certification.

Resource Entitlement Certification Reports

Reports Available	Description
Revoked entitlement report	Lists entitlements marked as revoked.
Certified entitlement report	Lists entitlements marked as certified.
Complete certification report	Comprehensive report of a resource entitlement certification.

Data Owner Certification Reports

Reports Available	Description
Data belongs to me report	Lists attributes marked as Belongs To Me during certification.
Data does not belong to me report	Lists attributes marked as Does Not Belong To Me during certification.
Complete data ownership report	Comprehensive report of a data owner certification including revoked and certified access.

top

Identity Audit

This chapter describes the identity audit user interface pages and includes information about how to complete an identity audit.

Identity Audit Overview

The Identity Audit module is designed to detect segregation of duties (SoD) violations. A *segregation of duties violation* is a violation whereby a user account, a user attribute, or a role has been assigned two entitlements that should not be held in combination.

While the identity certification module enables managers to certify or revoke access of users, the identity audit module has a detection mechanism that monitors users' actual access to resources and captures any violations on a continuous basis. The

software can also be programmed to conform to audit policies and report exceptions. It provides a summary of all exceptions, which helps security analysts, executives, or auditors accept or mitigate the exceptions.

In Role Manager, audit rules define violations. Audit rules are collected together to create an audit policy. User accounts and business structures are then scanned for audit policy violations. User accounts, user attributes, and roles that violate an identity audit policy are flagged and tracked until the violation is resolved.

Use the Identity Audit module to create and track audit rules, audit policies, and audit policy violations throughout the audit lifecycle. The module maintains a history of audit scans.

top

Understanding the Identity Audit User Interface

This section provides help using the Identity Audit portion of the user interface.

The Dashboard

To open the identity audit dashboard, choose Identity Audit > Dashboard from the main menu.

The identity audit dashboard summarizes identity audit policy violation status information. It displays graphs that enumerate the number of violations, and lists violations by state, priority, and date-of-last-update. The following four graphs are displayed:

1. Identity Audit Policy Violations
2. Identity Audit Policy Violations By State
3. Identity Audit Violation By Priority
4. Identity Audit Policy Violations By Updated Date

Figure - The Identity Audit Dashboard

To change the view of the graphs, click  .

To change the time period that the Dashboard reports on, click the Period drop-down menu at the bottom-right of the screen.

Policies

To open the identity audit Policies page, choose Identity Audit > Policies from the main menu.

Use the identity audit Policies page to edit and run audit policies, as well as to preview audit policies and view the results of completed audit policy scans. Click the New Policy button to create a new audit policy.

Rules

To open the identity audit Rules page, choose Identity Audit > Rules from the main menu.

Use the identity audit Rules page to create and edit audit rules.

Policy Violations

To open the identity audit Policy Violations page, choose Identity Audit > Policy Violations from the main menu.

The audit Policy Violations page has the following subtabs.

Subtab	Description
Open violations	Displays all the violations that are not yet fixed by the remediator. You can view the open violations by clicking them.
Closed Violations	Displays all violations that have been addressed by a remediator and closed.

top

Understanding Audit Policy Violations

An audit policy violation occurs if one or more rules associated with a policy is broken by a user account, a user attribute, or a user role. Role Manager tracks the violation until it is resolved.

Audit policies have designated remediators who are responsible for taking action when violations are discovered. The following three actors can be remediators:

- Rbacxadmin
- Policy Owner
- Remediator (designated person assigned during policy creation)

A remediator can reassign violations to another user so that action can be taken to resolve the violation. The remediator is mentioned in the audit trail of every violation, thereby making the remediator accountable for the action.

Each broken rule, and the user, account, role, and membership details that caused the violation are recorded. Each Identity Audit Violation contains at least one cause. When more than one rule in the policy matches, then the violation will have multiple causes. Violation causes are displayed on the Violation Details page under three different categories:

1. Account Causes
2. Role Causes
3. HR Attribute Causes

For more information about the Audit Violation Details page, see Audit Violation Details Help.

Acting on Audit Policy Violations

The following procedures describe how to take action on audit policy violations.

▼ To Assign an Audit Policy Violation to Another User

1. Log in to Role Manager.
2. Choose Identity Audit > Policy Violations.
   A list of open violations is displayed.
3. Click a violation in the Exception column.
   The Policy Violation Details page opens.
4. To reassign the violation to another user, click Reassign To in the Violation Details section.
   A page asking you to select another remediator opens.
5. Use search to choose another user.
   For help using search, see the Searching For a User section in the Identity Warehouse chapter.
6. Click OK.

▼ To View and Take Action on Audit Policy Violations

1. Log in to Role Manager.
2. Choose Identity Audit > Policy Violations.
   A list of open violations is displayed.
   Audit policy violations can be sorted by four different states:
   - **Open** - The remediator has not yet taken any action on the violation.
   - **Closed** - The remediator has closed the violation.
   - **Closed and Fixed** - The remediator has fixed the violation and therefore it should not appear in the next policy scan.
   - **Closed as Risk Accepted** - The remediator has acknowledged the violation and opted to allow the access for a certain time period.
3. Click a violation in the Exception column.
   The Policy Violations Details page opens.
4. To take action on the violation, review the user's access.
   To understand the Audit Violations page, see Audit Violation Details Help.
   - If you click Close Violation or Close as Fixed, a comment box opens.
     Enter a comment for future reference and click OK.
   - If you click Close as Risk Accepted, enter a comment and an end date, after which time the exemption will expire, then click OK.

Audit Violation Details Help

When taking action on an open violation (see To View and Take Action on Audit Policy Violations), the Policy Violation Details page displays the following information.

Violation Details Section

Field	Description
Policy	Displays the name of the policy.
Assigned To	Displays the remediator's name.
Reassign To	Allows you to reassign the violation to another user.
Assigned Date	The date when the policy was assigned to the remediator.
State	Displays the state of the violation.
Detection Count	The number of scans in which the violation was detected.
Last Detected	Last time the violation was found in an identity audit scan.
Expiration Date	Displays the expiration date of a "Close as Risk Accepted" violation.

Close Date	The date a remediation action was taken and the violation was moved to one of the "Closed" states.
Comments	Displays any comments added by the remediator.

User Details Section

Field	Description
Name	Displays the name of the user.
Department	Displays the user's department.
E-mail	Displays the user's email ID.
User Name	Displays the user name.
Manager	Displays the name of the manager.
Job Title	Displays the user's job title.

Accounts Section

The accounts section displays the user account that resulted in an identity audit violation.

Field	Description
Name	Displays the name of the account under violation.
Resource Type	Displays the resource type under violation.
Resource	Displays the resource under violation.
Rule	Displays the identity audit rule.
Condition	Displays the identity audit rule condition.
Status	Displays the state of the rule.

Roles Section

The Roles section displays the name of the user role that resulted in the identity audit violation.

Field	Description
Name	Displays the role under violation.
Rule	Displays the identity audit rule.
Condition	Displays the identity audit rule condition.
Status	Displays the state of the rule.

HR Attributes Section

The HR Attributes section displays the user attributes and values that resulted in the violation. If the violation occurred due to a business structure membership, the name of the business structure is displayed.

Field	Description
Attributes	Displays the HR attribute under violation.
Rule	Displays the identity audit rule.
Condition	Displays the identity audit rule condition.
Status	Displays the state of the rule.

top

▼ To View Audit Trails

An audit trail is a permanent history of every audit violation identified by Role Manager as well as all subsequent actions taken to resolve the violation.

The audit trail is updated whenever a violation is updated or modified. The audit trail tracks date information (when actions were taken), as well as any changes that affect the user, state, remediator, and comments fields.

1. Log in to Role Manager.
2. Choose Identity Audit > Policy Violations.
   - To view the audit trail of an open violation, click Open Violations in the submenu bar.
     a. Select the violation.
        The Violations Details page opens.
     b. Click the Audit Trail page option.
        The audit trail for the violation is displayed.
   - To view the audit trail of a closed violation, click Closed Violations in the submenu bar.
     a. Select the violation.
        The violations details page opens.
     b. Click the Audit Trail page option.
        The audit trail for the violation is displayed.

top

▼ To Export A Violation

1. Log in to Role Manager.
2. Choose Identity Audit > Policies.
   All the identity audit polices are listed.
3. Select the desired policy whose violations you want to export.
4. Click Export Violations.
5. Select the options to generate your report:
   - Report Format: Select the report format. Formats include PDF, CSV, XML, HTML, or XLS.
   - Violations to be exported: Select from the options listed.
6. Click Ok.

top

Reports

This chapter describes the various reports that can be generated in Role Manager. Reports are valuable tools that auditors and end-user managers can use to evaluate, analyze, and review access controls in the organization.

Reports are broadly classified as follows:

- *Business structure reports*: Out-of-the-box reports that run on selected business structures.
- *System reports*: Out-of-the-box reports that are run on all users, roles, or policies in Role Manager.
- *Identity Audit reports*: Open-audit exception reports based on audit policy scans.
- *Custom reports*: Reports customized according to the requirements of your organization.

Understanding the Reports User Interface

This section provides help using the Reports portion of the user interface.

The Dashboard

To open the reports dashboard, choose Reports > Dashboard from the main menu.

The reports dashboard summarizes status information for reports. The two graphs are the following:

- Reports by Business Strcuture.
- Reports which are pending, accepted or rejected by the managers.

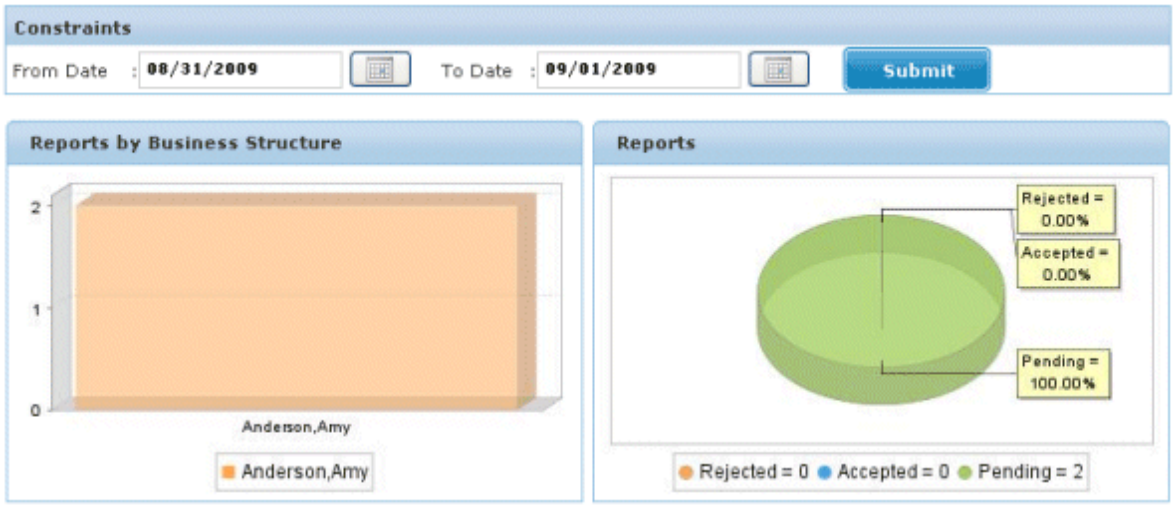


Figure - The Reports Dashboard

Sign Off Reports

To open the Sign Off Reports page, choose Reports > Sign Off Reports from the main menu.

Use the Sign Off Reports page to sign off on pending reports and to view completed reports.

Ad Hoc Reports

To open the Ad Hoc Reports page, choose Reports > Ad Hoc Reports from the main menu.

The Ad Hoc Reports page has four subtabs: Business Stucture Reports, System Reports, Identity Audit Reports, and Custom Reports. These reports can be run at any given time.

Use this page to run these reports and to download them.

Schedule Reports

To open the Schedule Reports page, choose Reports > Schedule Reports from the main menu.

Use the Schedule Reports page to generate specific reports at regular intervals.

Custom Reports

To open the Custom Reports page, choose Reports > Custom Reports from the main menu.

The Custom Reports page helps you to create customized reports based on the needs of your organization. Creating custom reports is an administrative function. See the Role Manager Reports chapter in the *Sun Role Manager 5.0.3 Business Administrator's Guide* to create a custom report.

top

Working With Reports

▼ To Schedule Reports

1. Log in to Role Manager.
2. Choose Reports > Schedule Reports.
3. Click New Report Job.
4. Complete the form:
   - Name: Enter the name of the report.
   - Description: Enter a description for the report.
   - Report Name: Choose a report from the drop-down menu.
     All out-of-the-box reports and custom reports are listed.
   - Set the date and time to schedule the report.
5. Click Create.

▼ To Sign Off on Reports

1. Log in to Role Manager.
2. Choose Reports > Sign Off Reports.
3. Select the report that you want to sign off on from the Pending Reports section.
4. Review the contents of the report. Select one of the following:
   a. Accept
   b. Reject
5. After signing off, the report is displayed in the Completed Reports section.

top

Defining Business Structure Reports

The following table describes the different business structure reports that Role Manager can generate.

Reports	Description
Business structure roles report	Lists all the roles under each business structure.
Business structure role users report	Lists all the roles and the assigned users under each business structure.
Business structure user roles report	Lists all the users and their assigned roles under each business structure.
Business structure users report	Lists all the users under each business structure.
Business structure user entitlements report	Lists all the users, under each business structure, with their entitlements.

User certification report	Lists all the users, under selected business structure, their roles and associated entitlements.
Business structure role policies report	Lists all the roles and associated policies under each business structure.
Data owner report	Lists all the entitlements and its owner.
Business structure resource type entitlement report	Lists all the users, under selected business structure, their associated resource types and entitlements.

▼ To Generate Business Structure Reports

1. Log in to Role Manager.
2. Choose Reports > Ad Hoc Reports.
3. Select Business Structure Reports to view a report under this section.
4. Select the report that you want to view and click Run.
   A window opens.
5. Select the Business Structure and click OK.
   The report is displayed.
6. Click the Actions drop-down menu for options to export the report in other formats.
   Formats include PDF, XLS, CSV, HTML, XML, and print.
7. (Optional) To download the report, click Download in either the Download PDF Report column or the Download CSV Report column.

top

Defining System Reports

System reports are further classified as follows:

1. Roles reports
2. Policy reports
3. User reports
4. Exception reports
5. Forecast reports

The different system reports that can be generated are described in the following tables.

System Reports > Roles Reports	Description
Role Policies Report	Lists the roles and associated policies of different applications within those roles.
Roles Users Report	Lists all roles and assigned users.

System Reports > Policy Reports	Description
Policy Roles Report	Lists the roles in a policy.
Policy Resource Types Report	Lists policies by resource type.
Policy Attributes Report	Lists the attributes in a policy.

System Reports > User Reports	Description
Policies Attribute Report	Lists the attributes in a policy.

User Business Unit Report	Lists the business units under a user.
User Role Report	Lists the roles under a user.
User Role Business Structure Report	Lists the business structures under a role, which is under a user.
User Application Report	Lists the applications under a user.
User Account Report	Lists the accounts under a user.
User Role-Based Access Report	Lists the attributes under a policy in a resource type under a user.

System Reports > Exception Reports	**Description**
Operational Exception Report	Reports the missing data required for correlations in Role Manager.
Import Validation Report	A set of reports displaying the data that has not been imported into Role Manager from the daily scheduled dumps.

System Reports > Forecast Reports	**Description**
Expiration Forecast Report	The report contains three subreports: User expiration, Role expiration, and User-Role Association expiration. It provides a list of all the expirations occurring in the current week.

▼ To Generate System Reports

1. Log in to Role Manager.
2. Choose Reports > Ad Hoc Reports.
3. Click System Reports and refer to the previous tables to determine the section.
4. Click the section and click Run against the Report Name that you want to view.
   The report is displayed.
5. Click the Actions drop-down menu for options to export the file in other formats.
   Formats include PDF, XLS, CSV, HTML, XML, and print.
6. (Optional) To download the report, click Download in either the Download PDF Report column or the Download CSV Report column.

top

Defining Identity Audit Reports

The different identity audit reports that can be generated are described here.

Reports	**Description**
All Open Audit Exceptions Report	Provides a list of audit-related exceptions, including Segregation of Duties, Assigned vs. Actual Rights Violation, and Terminated User reports.
Latest Open Audit Exceptions Report	Provides a list of audit-related exceptions, including Segregation of Duties, Assigned vs. Actual Rights Violation, and Terminated User reports. This report lists all exceptions for the current day.

▼ To Generate Identity Audit Reports

1. Log in to Role Manager.
2. Choose Reports > Ad Hoc Reports.
3. Click Identity Audit Reports.
4. Select the report name and click Run.
   The report is displayed.
5. Click the Actions drop-down menu for options to export the file in other formats.
   Formats include PDF, XLS, CSV, HTML, XML, and print.
6. (Optional) To download the report, click Download in either the Download PDF Report column or the Download CSV Report column.

top

Defining Custom Reports

You can create and run custom reports in Role Manager. To create a custom report, see Working With Custom Reports in the *Sun Role Manager 5.0.3 Business Administrator's Guide*.

▼ To Run Custom Reports

1. Log in to Role Manager.
2. Choose Reports > Ad Hoc Reports.
3. Click Custom Reports.
4. Click the report that you want to view and click Run.
5. Click the Actions drop-down menu for options to export the file in other formats.
   Formats include PDF, XLS, CSV, HTML, XML, and print.
6. (Optional) To download the report, click Download in either the Download PDF Report column or the Download CSV Report column.

top