

IDENTITY CERTIFICATION

BEST PRACTICES

White Paper
October 2009

Abstract

As organizations deal with increasingly complex internal structures and an array of regulatory requirements, manual or piecemeal access control processes are no longer adequate. To ensure compliance, companies around the world are implementing automated certification processes that provide needed security and enable greater business agility. By deploying Sun Role Manager and leveraging best practices developed by Simeio Solutions, a Sun preferred partner, your organization can quickly and effectively implement automated certification that meets your specific requirements.

Table of Contents

Introduction.....	1
Prepare	2
Develop a Communications Plan	2
Build the Identity Warehouse	4
Choose the Right Certification	6
Determine the Certification Campaign Cycle	7
Test.....	7
Quick Checklist	7
Certify.....	8
Remediate.....	10
Remediation Activity	10
Measure ROI.....	10
Pitfalls to Avoid.....	11
For More Information	12

Introduction

Today, the explosive global growth within organizations across verticals has created an unprecedented security challenge. Even as companies are battling the security threat from the outside, complex organizational structures, an expanding geographical footprint, and multiple areas of business are paving the way for an ever-increasing threat from the inside. Compliance laws such as Sarbanes Oxley, HIPPA, or Model Audit Rule (MAR) are forcing companies to streamline their access-control review processes. Organizations need to strike a balance: tighten information security without jeopardizing the business agility of the enterprise and achieve the nirvana state of ‘least privilege’ for employees.

To accomplish this goal, companies are moving away from cumbersome, manual access control processes and embracing an automated mechanism that effectively monitors the fundamental security challenge: who has access to what, and who has approved the access.

The advantages of an automated certification process include:

- Accurate monitoring and management of access by relevant stakeholders in the organization
- Ability to filter and review access to only critical applications, thereby saving time
- End-to-end monitoring via review of access to applications, resources, attributes, and roles
- Availability of archived certification reports, providing a comprehensive audit trail
- Organized reminder and escalation workflow to ensure an organization meets compliance deadlines
- Ability to directly remediate accounts from the provisioning solution based on revocations made during the certification process
- Minimizing downtime and maximizing ROI

Sun Role Manager, Sun Microsystems’ flagship role administration and identity compliance solution, provides a robust identity certification module. This paper discusses the best practices for a seamless identity certification deployment in your organization and describes Sun Role Manager 5.0 features that can help companies realize the benefits of a successful automated identity certification program.

The deployment strategy is developed based on best practices created by Simeio Solutions, a Sun preferred partner that provides expertise in identity and access management, role-based access control (RBAC), and IT governance, risk, and compliance (GRC) solutions. The New Jersey-based company has more than 60 successful deployments to its credit, including some of the largest Sun Role Manager implementations across various verticals and geographies.

This paper includes four sections that represent the four phases of access certification deployment—prepare, test, certify, and remediate—and provides insight into how to avoid the most common pitfalls that companies encounter when implementing such a solution.

Prepare

Develop a Communications Plan

One of the first steps in an identity certification deployment is to communicate the intrinsic changes that are about to occur in your environment. Create a certification management or certification governance team, that is responsible for managing the certification process and communicating to key stakeholders and users affected by the changes. The team must:

- Know the certification management tool
- Manage the lifecycle of certifications
- Steer the communication strategy

The following are some considerations that may be relevant to your organizational structure or culture. Included are a list of possible recipients (audiences) for your communication efforts, objectives, types of communication, and desired outcome of the communication.

AUDIENCE	OBJECTIVE	COMMUNICATION CHANNEL	DESIRED OUTCOME
Corporate communications manager	Work with the corporate communications manager to communicate the change and benefits across the enterprise	Emails, posters, intranet	An ally in communicating the change
Users/managers, and data owners	Involve those responsible for the certification process; get their buy-in Communicate the benefits of changing from a manual to an automated process	Demonstrations, emails, guides	-Understand the goal of the change, the timeline, how it will impact them, what their responsibilities are within the process, how to use the system, and how to escalate problems

AUDIENCE	OBJECTIVE	COMMUNICATION CHANNEL	DESIRED OUTCOME
Executive leadership	Provide high-level overview of the implementation, its objectives, and timeline	Emails, presentations, spread word of mouth	Advocate the move to an automated certification process
Risk/compliance officer or team	Determine certification schedule and define project plan	Regular meetings, emails to determine certification schedules	Understand the goals of implementation Develop a definite plan and schedule of certifications. Review and modify the plan annually as some applications change compliance status with external auditors (i.e., SOX critical versus just SOX testable)
Support center/help desk	Provide information to enable them to guide users from a functional point of view	Emails	Ability to handle end user calls
Application support (Tier II)	Provide training and materials to enable them to effectively support the application	Sessions, demonstrations, and administrator's guide	Ability to support application and associated architecture Understands escalation workflow

AUDIENCE	OBJECTIVE	COMMUNICATION CHANNEL	DESIRED OUTCOME
Human resources	<p>Communicate how the new process will address incorrect manager notices</p> <p>Help them understand the certification process</p>	Meetings and demonstrations	Act as a catalyst in the certification completion process
Application owners	Communicate their involvement and responsibilities within the certification process and remediation process	Guides, knowledge transfer sessions with implementation partners	Understand the impact of the change, responsibilities within the process, timeline, how to use the tool, and how to decipher the reports generated
User administration team	Communicate their involvement in handling all remediation reports	Demonstration targeted to user administration team	Equipped to handle remediation

Build the Identity Warehouse

The building block of a successful identity certification launch is building the identity warehouse. The identity warehouse is a central repository within Sun Role Manager that is the unified source of all HR- and access-related data. The identity warehouse provides a single view of all users and all applications where access is granted. The recommended way to build the warehouse includes the following steps:

- **Critical applications first.** Choosing the important applications is critical to maximizing your ROI. Analyze your business risks, limit your scope, and finalize the access information of applications you want to include in the certification process. Analyze the criticality of applications based on two criteria:
 - Does the application contain sensitive data from an audit standpoint?
 - Is the application critical from a provisioning standpoint? Is it an application with a huge user base, which requires regular updating?

Sun Role Manager gives you the flexibility to create an application view across various endpoints. This translates into reviewing user access to only ‘high-level’ applications during the certification process, thereby saving time.

You can now...

Create an application view across multiple resource types and resources. Certifiers can review only 'high-level' applications during the certification process.

- **Define certifiable attributes.** Within accounts, select only key attributes and include only these attributes in your certifications. This reduces the certifier's time and effort.
- **Import glossary information.** To user managers, entitlements are mere cryptic codes that are difficult to understand. To ensure that the right entitlements are certified or revoked, import glossary information into Role Manager. The goal of glossary descriptions is to provide capability detail. For example, an entitlement in PeopleSoft such as 'P_xyz_500' means 'an account payable clerk with the authority to approve checks from \$500 and above.' Assign an administrator to review and update entitlements on a regular basis.
- **Review orphan accounts and users.** As you create the warehouse, orphan accounts become critical. Orphan accounts may be important process or system accounts, for which owners should be assigned. This ensures that all accounts are certified and have the required access.
- **Assign data owners/stewards to high-privileged entitlements.** It is critical to identify as high-privileged those entitlements that are highly sensitive in nature. These would include high-risk entitlements, system accounts, accounts with administrator level privileges, and so on. Because of the sensitive nature of these entitlements, they should be included as part of two certifications: user entitlement and data owner.
- **Validate your processes.** Ensure that the identity warehouse is current and accurate. Important steps to achieve this include:
 - Integrate with a provisioning solution to update user and account information in the identity warehouse
 - Schedule a regular import process for user and account information on a nightly basis

Sun Role Manager can be tuned to reflect the organizational changes that are a part of your everyday business. The Identity Warehouse and the import process supported by Sun Role Manager ensures that the warehouse stores the most updated version of user entitlements in addition to updated user records, which reflect organizational changes on a day-to-day basis. This captures any users being on-boarded into the organization, transferring from one department to another, or being terminated—which in turn allows Sun Role Manager to take appropriate actions such as triggering audit scans or creating access certifications or rule-based assignments and de-assignments of roles to new, transferring, or terminated users. The Identity Warehouse also records the most up-to-date user entitlements across an enterprise, allowing for a more streamlined reporting and auditing process.

Choose the Right Certification

Sun Role Manager offers four out-of-the-box certifications to review user access. Use the table below to choose the best certification type for your organization.

CERTIFICATION TYPE	DESCRIPTION	BEST SUITED SCENARIOS
User entitlement	Allows business managers to review their employees' access and certify or revoke access to applications	Enterprises that are automating their attestation process and making the managers responsible for the access of their direct reports
Resource entitlement	Allows application owners to review and certify or revoke access to applications they own	<p>Applications with a small user population where the application owner is responsible for all the access that the users have to the application</p> <p>Enterprises where the application owner attestation is considered as a step within the entire certification campaign. This is combined with user entitlement certification</p>
Data owner	Allows attribute owners to review and certify or revoke access to granular data they own	Used as an additional step in the certification of highly privileged access by data owners/stewards who are also responsible for the users who have access to highly privileged information
Role entitlement	Allows role owners to review role content	Organizations that have adopted an enterprise-wide role-based access control solution are best suited to use this certification type

You can now...

Get a complete view of accounts, roles and policies and user activity during the certification process. Certifiers can now make informed decisions.

Determine the Certification Campaign Cycle

Before you kick off your certification process, determine the frequency of your certification campaign. Use the 'incremental certification' feature—a setting that allows the user managers to certify only the changes that have taken place since the last-created certification. Enable this setting to avoid repetition of access evaluation for previously certified users.

An ideal certification campaign cycle is:

- **First year:** Schedule the certification job on a quarter-to-quarter basis. This will filter the orphan accounts and streamline user access. The first certification should be a complete certification followed by three incremental certifications.
- **Second year:** Schedule certification jobs on a half-yearly basis again with one annual baseline followed by an incremental.
- **Third year and onwards:** Schedule certification jobs on a half-yearly basis.

It is important that you consult your internal and external audit teams to verify the frequency suited for your organization.

Test

Testing the configuration setting is a critical step. A pre-launch run is an opportunity to detect all issues and address them to ensure a smooth launch.

- **Create Pilot Certifications.** Launch a pilot certification for a predetermined set of users. Include a good mix of system-savvy and non-IT users in the pilot to ensure a complete system run. Monitor the pilot certification process and progress. Refine your certification configuration based on the results of the pilot run.
- **Form a User Acceptance Testing Team and include team members in the process.** This team should participate in two different roles: testing the administrative functions and participating as an end user/requestor. They will gain greater understanding of how to manage their own access and support end users who need assistance.
- **Make Remediation Settings.** Include managed and non-managed applications. Sun Role Manager 5.0 allows you to automatically remediate accounts that have been revoked during the certification process. Ensure this setting is functional, as this will expedite the post-revocation activity.

Quick Checklist

Before you launch your certification, ensure the following:

- All the identity certification configurations are in line with your organization's requirements.
- Issues encountered during the pilot process have been addressed.
- Email templates have been created and contain relevant content. The escalation workflow has been developed and dates are set for reminders to managers.
- A list of high-profile users (senior vice presidents and above) has been created. This

group's daily administrative activities are performed by their respective executive assistants or designated proxies. Turn off the escalation emails for this set of users.

- Administrators have been blind copied (bcc) on all certification notifications.
- Configuration changes on the server have been made to accommodate increased traffic to the tool.

Certify

The organization is now set for the certification launch. Note that the success of this step depends on the pre-certification and pre-launch phases.

- **Launch in batches.** Launch the certification in batches of 50. A certification campaign—that is, an enterprise-wide certification exercise involving various business units and a broad range of actors including business line managers, application owners, and data owners—should last for four weeks. Managers must be instructed to complete their certifications in two weeks.
- **Handling certification for high-profile users.** Treat this set of users with care. After the escalation reminders are removed, make appropriate configuration settings that are suited to their job titles. Now, launch this certification.

After the certification is launched, two sets of audiences become part of the cycle—the certifiers and the Role Manager administrators.

ACTOR	TASKS DURING CERTIFICATION	TASKS POST-CERTIFICATION
Certifier	<p>Complete certifications on time</p> <p>Ensure all employees who report to them are listed. Contact the administrator regarding any omissions</p> <p>Ensure all application information is listed. Contact administrator regarding any omissions</p> <p>Sun Role Manager 5.0 gives you the ability to view granular information about a user's access to help you make informed</p>	<p>Print out certifications report for reference and distribution</p> <p>Set up a meeting with the administrator to discuss any omissions (users or accounts)</p>

ACTOR	TASKS DURING CERTIFICATION	TASKS POST-CERTIFICATION
<i>(Continued)</i>	<p>decisions. Review the access information, HR data, SoD violations, open-audit exceptions, etc. before you certify or revoke a user's access</p>	
<p>Role Manager administrators/ certification administrators</p>	<p>Ensure certification deadlines are met and facilitate the certification completion cycle in four weeks</p> <p>Monitor certification progress. Check for the number of certifications sent, number of completed certifications, and percentage of certifications completed</p> <p>Monitor all notifications</p> <p>Create reports on obsolete users and revoked accounts on a regular basis. Present this to management to assess the scale of the accounts clean-up task</p>	<p>Generate important reports</p> <p>Follow up with managers/application owners for incomplete certifications</p>

You can now...

Directly de-provision accounts, roles, and policies based on revocations made during the certification process.

Remediate

The post-certification phase involves analyzing certification reports and taking action on the results.

Here are a few important reports and suggested actions:

REPORT	DESCRIPTION	ACTION
Consolidated certified access report	Compiles evidence of certifier's responses	Should be stored in a non-editable format
Consolidated revoked access certification report	Includes all revoked accounts, roles and entitlements across the organization	Must be shared with application owners and the user administration team for remediation action
Obsolete users report	Includes users with incorrect information about managers and terminated users	Share with the HR department to update their records

Consolidated certified access report: This is evidence of a certifier's responses.

Remediation Activity

Remediation is the last step for completing the certification cycle. Your organization is now armed with valuable information for this phase.

For managed resources, if Sun Role Manager 5.0 is integrated with Sun Identity Manager, the software directly revokes the account in the provisioning solution and updates information in the warehouse.

For non-managed resources, the certification administrator and application owners must ensure that the revoked accounts are de-provisioned. Continuous monitoring can be achieved by generating remediation reports on a regular basis.

Measure ROI

Communicating the change to drive acceptance during the implementation process is critical. Equally important is continuing to communicate after implementation.

Quantify the successes achieved by implementing Sun Role Manager and changing your identity management processes.

The following metrics will interest your management as well as internal and external auditors:

- Reduction in number of dormant or terminated user accounts
- Reduction in number of sensitive or high privilege accounts/entitlements

- Number of accounts/entitlements remediated
- Remediation count of incorrect user-to-manager reporting relationships

You can calculate ROI on the following four criteria:

- Reduction in time: Reduction in turn-around time vs. manual certification and in comparing a complete certification vs. incremental certifications
- Minimization of errors: With monitoring ease, an automated certification module eliminates manual errors
- Reduction in manpower costs: Fewer people are involved in the process
- Enhanced user experience: Certifiers now don't loathe the process

Pitfalls to Avoid

When deploying an access certification solution, there are some common pitfalls that can be avoided with careful planning and a solid methodology:

- **Rushing through the pre-certification and pre-launch periods.** Plan to communicate, pilot, remediate changes from the pilot, communicate again, and then launch your first batch of certifications. Overlooking this process creates risk that governance, training, and communication have not occurred to the proper degree to ensure sustainable success.
- **Choosing too many applications that may not be critical to your business risks.** The secret to saving time and minimizing business risk lies in the choice of applications. Organizations often make the mistake of either selecting too many applications, which do not pose a potential security threat, or to not include all the data-sensitive applications in the review process. Therefore, a team comprised of a business analyst and a technical expert must be consulted before short listing the target applications. Also, include your internal audit team in this discussion as they are most privy to the determination of compliance-critical and compliance-testable.
- **Choosing very long or short certification cycles.** Four weeks is the optimum time to launch and complete a certification cycle. Too short a cycle will rush user managers and administrators and too long a cycle will elongate the process, delaying your compliance deadline.
- **Ineffective communication processes.** The automated certification process involves many new actors. The concerted effort of all the actors is key to the success of an identity certification cycle. It's vital to create a seamless communication channel where all personnel involved are aware of their new roles and are prepared to fulfill the associated responsibility.
- **Lack of valid training to certifiers.** Certifiers can perceive the process as a daunting task if they are not adequately trained. Organize demonstrations and training sessions for certifiers to make them comfortable with the tool and the process.
- **Lack of action on revocation reports.** The certification cycle is only as good as the action the organization takes on the reports generated. Addressing all HR issues

and remediation actions will result in a compliant organization.

For More Information

For more information on Sun Role Manager, visit www.sun.com/rolemanager.

For more information on the services provided by Simeio Solutions, visit www.simeiosolutions.com.



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN (9786) Web sun.com

© 2009 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Information subject to change without notice. Printed in USA 09/09 SunWin # 570925