RAC/M
IDENTITY

At last: identity and access control

Optimization of Identity and Access Management to reduce risk and facilitate compliance

Once for all : Take control of identities and accesses

Just like trying to track thousands of fishes that all look the same but are unique entities, organizations are swimming in daunting complexity when faced with the challenge of determining and demonstrating who has access to what IT resources.

Based on its RAC/M Identity solution and top flight expertise, OKIOK's offer in the Identity and Access Governance space allows organizations to quickly regain control and obtain an accurate view of who has access to what.

While facilitating compliance and minimizing risk

As organizations grow, it becomes increasingly complex to track and demonstrate who has access to what and to maintain control over various issues, such as:

- the diversity and inconsistency of access data for users of various IT applications
- the multiple functions for a single user
- the perpetual changes in roles and responsibilities

Companies struggle to find the perfect balance between a protected environment and granting the necessary access rights and privileges to enable staff to work productively.

The RAC/M IdentityTM solution helps companies better understand the relationship between users and the information resources granted to them, thus enabling them to work toward more effective identity and access management, including management of any physical assets entrusted to users (access cards, telephones, tools, etc.).

In addition to facilitating and optimizing access management of various resources within the company, the RAC/M IdentityTM solution also allows an organization to effectively demonstrate control over access to critical information assets, as required by the various normative frameworks to which the company must comply (SOX, PCI, NERC, HIPAA, etc.).

A different approach, focusing on access governance

RAC/M IdentityTM differs from traditional Identity and Access Management (IAM) suites by prioritizing governance processes rather than proceeding directly to automated provisioning. In fact, organizations are often unable to validate which account belongs to which user and therefore cannot effectively automate user provisioning (creation, modification, removal of accounts).

The solution offers the establishment of a clear mechanism, customized to the organization's real needs, and provides processes enabling the company to:

1. Understand the organization's access right structure;
2. Gradually define access needs;
3. Automate requests and implement controls, while also establishing end-to-end traceability.

Flexible and non-intrusive

RAC/M IdentityTM centralizes and formalizes the access management process by easily adapting to each company's organizational context and by integrating with existing systems and business processes. Data collection is done in a unidirectional manner (read only), eliminating risk related to the reliability, availability and performance of the organization's systems.

Swift and compelling results

The initial cleaning of existing data and the creation of an access repository initiate a transformation that will enhance the organization's maturity level and make access management practices more effective. The initial process can be accomplished in a few days; therefore, the organization can quickly begin to benefit from the solution.

Risk reduction

By identifying and eliminating unnecessary accounts, identifying over-privileged accounts and conducting periodic reconciliations with HR and targeted systems, RAC/M IdentityTM enhances the security posture by better controlling access to critical information. Poor identity and access management exposes an organization to significant risk with regard to the protection of data, and loss of control may result in damages, which can be difficult and costly to address.

BROWSER-BASED USER INTERFACE

Features	Benefits
Works on any recent standards-compliant Web browser	No need to install proprietary client applications on everyone's computer. System is available from anywhere on the network, any time, and on any PC (Windows, Mac, Android, Linux)
Familiar Web browser navigation and controls	Familiar environment right from the start
Login Authentication using Active Directory domain or Web form credentials	Users and managers can sign in quickly using their domain user name and password or application specific credentials
Roaming user support	Any time, anywhere secure access from virtually any Web browser, even when traveling
Multi-language support	Web interface supports multiple languages
Web based administration menus	Administrators can easily configure and maintain the access models, identities, groups, and resources, directly from the browser interface

REDUCES RISK

Features	Benefits
Identification and elimination of unused and obsolete accounts	Better security due to less bait for hackers and reduced risk of rogue users
Identification of over-privileged accounts	Better control of sensitive data, locations, and resources
Periodic reconciliation with HR sources and target systems	Proactive enforcement of policies and formal access model, and tight management of exceptions

WORKFLOW

Features	Benefits
Self-serve capability for requesting changes to job, role, or access entitlements	Streamlined process means faster service, fewer mis-steps, and less nagging of approvers and IT staff
Both cascading and escalating request and approval path methods available; the right path for the right job	Requests always go to the right people at the right time; no lost approval requests
Automatic rules generation based on existing access information	Rapid setup and configuration of aggregation and normalization
Standards-based public-key cryptography using S/MIME	Your confidential files remain confidential until processed by a recipient
Task-based workflows for employees and supervisors	Easy to see and act on outstanding tasks; quicker responses, less waiting
Contextual approval model	Approval by appropriate person means better delegation, less wasted time, fewer frustrations
Dynamic management tasks	Manual or automated processing of imported files, simplified exception management, recertification and reports only when needed

REDUCES COSTS

Features	Benefits
Uses existing file collectors	No need to design, develop and test proprietary collectors
Rules-based design	No need for expensive role membership management activities
Integrates with existing business processes	Reduces or eliminates redundant data captures and manual operations
Flexible, workflow-driven approval model	Supports delegation, cascading approver lists, workload sharing, and escalation paths

RAC/M Identity

Reduce acquisition, deployment and operation costs

Support evolving business requirements without additional programming
Reduce security risks

Reduce costs, effort, and time to achieve compliance

SYSTEM REQUIREMENTS

Hardware Requirements

- Server must be at minimum a Dual-Core with 2 GB RAM
- 20 GB hard disk minimum

RAC/M IDENTITY SOFTWARE COMPATIBILITY

Operating Systems

- Linux
- Solaris
- Windows

Other Software

- Java based
- MS-SQL

Client Software Requirements

- Windows: Internet Explorer 8.0 or higher, Firefox 4.0 or higher, Chrome 9.0 or higher
- Mac OS X with any supported browser

Licensing

- Perpetual and annual site license

OKIOK is a leader in the field of computer security. Since 1973, the company has distin-guished itself through the excellence of its products and the high quality of its services. OKIOK offers a wide range of integrated solutions designed to meet the needs of organiza-tions of all sizes.