RSA® BUSINESS ROLE MANAGER

Automate Role Discovery and Creation

KEY BENEFITS

- Comprehensive Role Lifecycle Management – Enables organizations to implement a role-based approach to governing user access. Provides collaborative processes and automation for role discovery, modeling, modification, approval, certification and continuous lifecycle management, which streamlines access delivery and simplifies access compliance.
- Enterprise-Wide Visibility – Roles support a common language for access that can be easily understood by business users and IT. The correlation of "who has access to what" based on this access vocabulary provides the transparency to support simplified administration and compliance.
- Analytics & Decision Support – Sophisticated role modeling rules and analytics ensure that role management decisions are based on the value a role brings to an organization.
- Provisioning Integration – Role assignments and role entitlement structure changes are automatically synchronized with user provisioning systems, or directly fulfilled with RSA's Via Lifecycle module.

RSA® Business Role Manager helps organizations deploy effective role-based access control, which streamlines access delivery and simplifies access compliance.

With Business Role Manager Organizations Can:

- Automate the complete role lifecycle, including discovery, modeling, approval, modification, assignment, certification and on-going management.
- Create collaborative processes that engage key stakeholders in the design, modification, certification and management of roles.
- Design flexible processes for modeling roles top-down, mining roles bottom-up and creating organizational role hierarchies.
- Report and analyze the usage and effectiveness of roles over time.
- Detect and manage out-of-role entitlements to ensure that business policy and compliance objectives are being achieved.
- Integrate with user provisioning systems for role synchronization.

Capability Highlights

Enterprise-Wide Visibility – Business Role Manager automates the collection and correlation of entitlement and role information across all application and data resources to provide enterprise-wide visibility into common access across users.

Business Roles – Business context can be leveraged to define business roles, which provide a layer of abstraction above existing entitlements, technical roles and application roles. This establishes a common language for access that can be easily understood by business users. A collaborative process for role design, modification, approval and management ensures participation by key stakeholders from IT and the business in order to capture unique organizational processes, specific attributes and control requirements.

Flexible Role Model – Support for complex role hierarchies and inheritance models accommodates an organization's unique requirements for mapping access relationships between users and their roles. A powerful rules engine provides impact-scenario analysis when designing new roles or modifying existing roles, to ensure that entitlement combinations do not create business policy or compliance violations (e.g. segregation of duties).

Role Certification – When used in conjunction with the RSA Identity Governance module, provides an automated process for role certification, which ensures that roles are maintained appropriately and that role owners or other designated business managers are accountable for reviewing role entitlement structure and membership. Role structure changes that result from a role review are tracked for auditing purposes.

Change Management – User entitlement changes resulting from role assignments can be accomplished through notifications to application owners, IT change management systems or user provisioning systems. A closed-loop validation process ensures that changes are completed successfully, or escalated if not. A complete audit trail captures all approvals, escalations and changes.

Role Reporting and Analytics – A comprehensive set of metrics and reports provides the administrative insight and decision support to ensure that roles are effective for an organization, and minimizes role proliferation. Information security and business managers are able to set and monitor key performance indicators for roles, as well as identify and manage out-of-role entitlements. Role quality analysis provides the decision support for role owners to understand when a role needs to be changed or is no longer useful and should be combined with a similar role or retired.

Business, Technical and Application Roles – Existing technical or application roles defined within user provisioning, ERP systems and other applications can be imported for analysis, refinement or enhancement. Business context can be used to improve these roles or define new business roles that contain existing roles. User entitlement changes resulting from new or modified role assignments for users are orchestrated across applications, user provisioning systems, and other access change management systems.

Achieving Effective Role-Based Access Governance – Organizations can easily align access privileges to job responsibilities, and other business requirements, to ensure that user access is always compliant. Business Role Manager provides an automated, collaborative and continuous approach for discovering, designing, certifying and maintaining roles over their entire lifecycle

Part of a comprehensive Identity and Access Management Portfolio, RSA® SecurID® Suite:

RSA delivers a simple, secure, and efficient way to provide access to all of your users, no matter where they are, or what resources they are accessing. With a single, consistent approach, you can manage and control access for all of your users – internal and external, local and remote – across on-premise and SaaS applications and resources. With RSA® SecurID® Suite, you can easily ensure that users are properly authenticated, and have only appropriate levels of access throughout the identity lifecycle. You'll also be able to institute consistent governance and provisioning processes that help you efficiently deliver business user access, while maintaining continuous compliance with changing policies and regulatory controls.

RSA Identity Governance and Lifecycle Platform Automates the Complete Identity Lifecycle:

The RSA Identity Governance and Lifecycle platform provides robust capabilities to manage and automate the complete identity lifecycle. With this platform, organizations ensure that business users efficiently obtain access, while remaining compliant with security and regulatory policies. By streamlining access request and approval, simplifying access reviews, enforcing policies, and accelerating provisioning, organizations can reliably deliver business value from their IAM programs.

The RSA Identity Governance and Lifecycle platform comprises the following additional offerings:

RSA Identity Governance – Automates the monitoring, certification, reporting and remediation of user entitlements for on-premise and cloud-based applications.

RSA Identity Lifecycle – Delivers a streamlined request and fulfillment process with embedded policy controls to ensure that user access is appropriate, for on-premise systems, cloud-based applications, and data resources.

RSA Data Access Governance – Provides visibility, business ownership identification, and control over access to data resources, including file shares and Microsoft® SharePoint®.

RSA Identity Governance and Lifecycle can be deployed on-Premise or as a Service (SaaS). This flexible deployment model gives you the choice of managing and governing identities and applications with on-premise hardware or software, or from the cloud.

EMC², EMC, the EMC logo, RSA, the RSA logo, are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware is a registered trademark or trademark of VMware, Inc., in the United States and other jurisdictions. © Copyright 2015 EMC Corporation. All rights reserved. Published in the USA. 06/16 Data Sheet H12511

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.