



RoleCourier®

Enterprise Role Management

Benefits

- **Cost-effective:** Automates role creation and simplifies enterprise provisioning.
- **Business alignment:** Aligns business roles with IT accounts and access rights.
- **Comprehensive:** Delivers end-to-end role lifecycle management.
- **Dynamic:** Dynamic role attributes reduce role proliferation.
- **Flexible:** Combines “bottom-up” role mining and “top-down” role definition for creating optimal roles.
- **Analytical:** Enables role consolidation management and “what if” analysis.
- **Integrated:** Enhances and simplifies user provisioning and compliance functions.

RoleCourier® is Courion's role management solution for organizations seeking to simplify and optimize security and access policy enforcement by creating user roles that align IT accounts and access rights with business functions. RoleCourier automates the often complex, cumbersome, and inefficient process of role creation and ongoing management. Unlike third-party role creation tools with limited capabilities that lack true, real-time integration with the user provisioning process, RoleCourier creates a foundation for robust ongoing role lifecycle management that is fully integrated with AccountCourier®, Courion's industry-leading provisioning platform, and readily adapts to changes in today's business environment.

Access Assurance and Role Management

Access Assurance is Courion's unique approach to access and compliance management that ensures only the right people have the right access to the right resources and are doing the right things. Access Assurance unifies Access Governance, Access Provisioning and Access Compliance even in the most complex, heterogeneous environments. Role management is a core element of Access Governance and Access Provisioning by providing the foundation for aligning business roles and responsibilities with IT accounts, access rights and security policy.

Addressing Role Challenges

A role is a representation of a set of access rights to resources or data that corresponds to a business function. Examples include senior teller, business analyst, sales representative, marketing manager, etc. In order for an end user to be successful, their business role must be aligned with their IT-based accounts and access rights. Different roles require access to different systems and varying access rights, depending on the application functions and data the user must utilize to complete their daily tasks effectively and efficiently.

Role management is desirable to organizations wishing to deploy or leverage user provisioning because of its potential to simplify security policy administration and enforcement, particularly in environments with many applications. Roles reduce the complexity of user administration by mapping a potentially large number of users with related functions into a smaller number of well-defined IT accounts and entitlements. Those roles become the cornerstone of ongoing user security and access policy management.

Bottom-Up or Top-Down?

Organizations wishing to create an enterprise role infrastructure often find that initial role creation is a major undertaking. Even in small and medium-sized companies, the number of users, accounts, systems, locations, lines of business, and other attributes that map into roles is daunting.

Lacking a centralized view, many organizations start from the “bottom up” by dumping user access data from multiple systems into databases and manually correlating access rights on a user-by-user basis. This role mining process is useful because it is based on existing IT accounts, however it lacks strong connections with the business view of roles. Simply because a group of individuals have a set of accounts and access rights in common doesn’t necessarily mean that they represent a good role candidate. Poor data quality can also lead to role recommendations that may not be aligned with business goals, security policies or best practices.

Other organizations adopt a “top down” approach to create roles based on organizational hierarchies and require creation of complex management frameworks. This role discovery perspective is typically very business-centric, but lacks tight integration with the IT roles, accounts and entitlements that users require to perform their daily tasks.

What is needed is a hybrid methodology that blends both the role mining (bottom-up) and role discovery (top-down) approaches to deliver the best of both. The difficulty is finding tools that can automate and simplify the data collection and analysis aspects of role creation, create a capability for ongoing role management, and integrate it into an automated provisioning process.

Automating Role Creation

Courion’s automated role creation function enables organizations to take a “hybrid” approach to role creation. A “bottom up” role mining capability starts with data from existing accounts. Candidate users are dynamically checked for common access patterns and thresholds are applied to determine attributes for inclusion or exclusion. Candidate roles are checked against the user security policy for exceptions, policy conflicts (such as segregation of duties), and least privilege violations.

Then, by correlating those results with a “top down” business organization model, RoleCourier produces a role template that can then be applied across the enterprise. The role creation function is optimized to minimize the number of required roles, easing the role management and governance burden on customers. It also accommodates all types of roles, including enterprise, IT, business, or application-specific roles.

Dynamic Role Definition

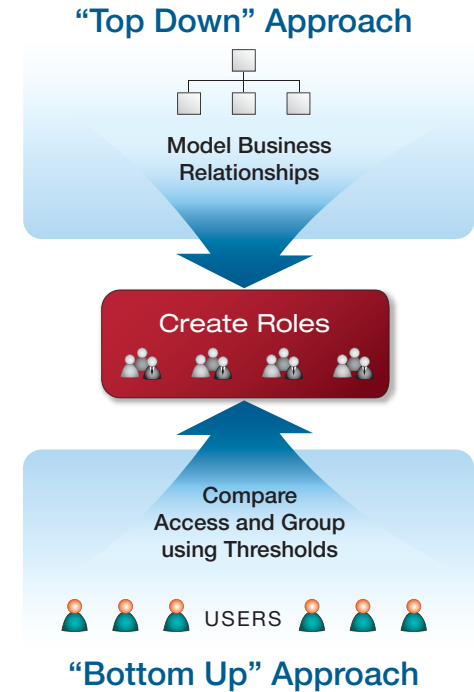
Some vendors use hard-coded rules to create roles that combine static and dynamic attributes. This often results in role proliferation, where an organization may wind up with more IT roles and accounts defined than it has users.

For example, a distributed financial services organization may create a teller role. While all tellers need teller system, network and email server accounts, the actual systems the teller needs to access may vary depending on the teller’s location. A teller based in New York requires access to different systems and servers than a teller based in San Francisco. A static, hard-coded role management system will create separate teller roles for New York and San Francisco, despite the fact that the business functions executed by the tellers are the same.

Courion’s dynamic role definition process creates a single role with attributes (teller system, email server, network server, etc.) that are dynamically assigned at run-time, when the account is actually provisioned. RoleCourier’s dynamic approach delivers a higher level of abstraction for role attributes and provides a pragmatic role definition and management model, which reduces role proliferation.

“What-if” Modeling

An important aspect of role management for compliance purposes is to perform checks for policy violations, such as segregation of duties. This is particularly critical in environments where users perform multiple roles, or where assignments of users to roles change on a frequent basis.



To address this need, RoleCourier provides the ability to perform “what-if” role modeling. This process examines a set of specified roles against the security policy to see if the superset of access rights across all the roles would create a policy violation. A similar process is used to detect attribute-level conflicts across multiple roles.

Managing Role Lifecycles

In addition to role creation and policy violation checking, enterprises need role lifecycle management capabilities to keep up with changes that occur over time. This includes the ability to modify or delete role attributes, enable or disable roles, manage role hierarchies and track the history of changes associated with roles. Role history analysis is a particularly important capability for compliance analysis and reporting.

Another key role management capability is role comparison and consolidation. This enables organizations to iteratively examine their role definitions and identify opportunities to simplify security policy management and administration by reorganizing roles, creating nested roles or merging similar roles.

Role Management

Hybrid Approach	Optimize the role definition process by combining existing account entitlements with the businesses organizational perspective.
Simplifies Provisioning	Provides a template that can be used to provision new employees much more quickly and easily, allowing managers to focus more attention on exception handling.
Enforce Policy	Ensure that access rights and entitlements are consistent with the user’s business function and help the organization meet access-related regulatory requirements, such as PCI-DSS or HIPAA.
“What-If” Analysis	Compare existing role definitions with candidate roles and uncover potential policy violations.
Dynamic Attributes	Changeable role attributes, such as location dependencies, are handled at provision time, reducing the potential for role proliferation.
Lifecycle Management	Comprehensive lifecycle management tools simplify the creation, management, and retirement of roles over time.

Compliance and Attestation

Companies are under increasing pressure to be able to validate and verify to auditors and regulators that their employee access rights and entitlements are consistent with corporate security policies, industry requirements (e.g., PCI-DSS) and government regulations (e.g., Sarbanes-Oxley, HIPAA, UK Data Privacy Act). Implementing and managing a comprehensive role management lifecycle provides a strong foundation for organizations to be able to repeatedly and accurately verify the access rights and entitlements that users are holding and ensure that these rights are consistent with corporate requirements. RoleCourier’s role definitions are fully integrated with, and supported by, Courion’s ComplianceCourier™ product, which quickly and cost-effectively enables managers to attest to the access rights and profiles of end-users within their business unit.

Backed by Industry-Proven Services

Courion’s Enterprise Suite is backed by world-class, expert services delivered directly by Courion or by our Certified Solution Partners. Courion’s discovery and implementation methodology allows customers to efficiently achieve the desired level of policy automation for their targeted business processes. Courion’s unrivaled access and compliance management expertise delivers the strategic services and support required to achieve timely deployments, a process for capturing and tracking measurable results, substantial cost savings, and notable improvements in your company’s security and service quality.

Courion Access Assurance Suite Solution

RoleCourier is part of the Courion Access Assurance Suite, which includes:

ComplianceCourier	Access certification and remediation – ensure that end user access rights comply with corporate policy, industry standards or government regulations.
RoleCourier	Enterprise role management – define and manage end user roles to automate role creation, provide role lifecycle management, and assign users to one or more roles as part of the provisioning process.
AccountCourier	End user provisioning – define and implement accounts and access rights to enterprise systems, including operating systems, networks, databases, servers and applications.
PasswordCourier	Client-based password management, including end user self-service password and profile management.
Sensitive Data Manager	Review sensitive data identified by data loss prevention products and approve or remediate user access rights to reduce risk and ensure compliance.
User Activity Manager	Monitor and manage access rights for users who may be engaged in risky or unauthorized activity.

Technical Specifications

Windows Server	Microsoft Windows Server® 2003 (Service Pack 1 or higher) OR Microsoft Windows Server® 2008	Minimum 3 GB of memory (single server installation)
	Microsoft XML 6.0 and Microsoft XML 3.0	Minimum of 2.0 GHz processing speed (multiple CPUs or multicore CPUs recommended)
	Microsoft Message Queuing	NTFS formatted disk drive, 80 GB minimum
Web Server	Microsoft IIS 6.0 or higher on Windows Server 2003, Microsoft IIS 7.0 on Windows Server 2008	

Other requirements may apply, contact Courion for further information.

About Courion

Courion, the leader in access risk management, helps companies identify, quantify and manage the risks associated with information access. Used by nearly 500 organizations and over 14 million users worldwide to quickly and easily solve their most complex identity and access management (password management, provisioning, and role management), risk and compliance challenges, Courion can help your company win in today's mobile, always-on, cloud-based business environment.

For more information, please visit our website at www.courion.com, our blog at blog.courion.com, or on Twitter at twitter.com/Courion.

