

WHITE PAPER

Reduce Role Explosion with Axiomatics

AXIOMATICS
a LEONARDO company

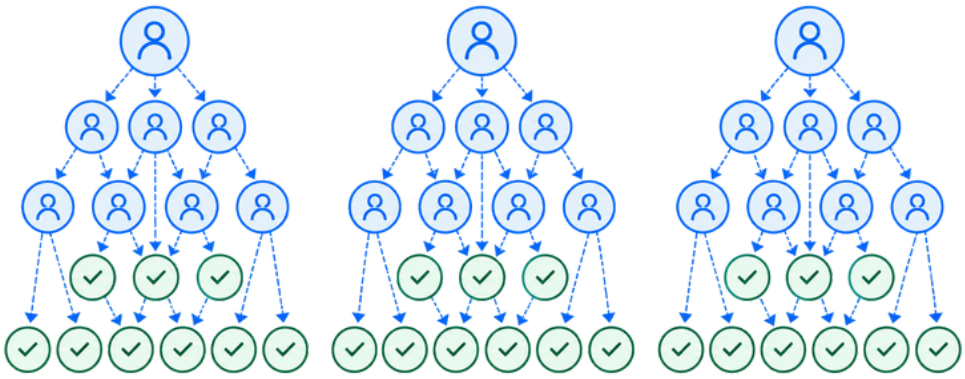
Role explosion occurs when organizations create an excessive number of user roles in order to manage access across applications, data, APIs, cloud services and business processes. New roles are continuously being added to accommodate different departments, regions, job functions, and compliance requirements.

What begins as a traditional role-based model quickly becomes difficult to scale.

For example, an organization may require department managers to approve employee corporate card transactions. Instead of defining access dynamically through policy, separate roles are often created for each department and country combination.

Examples include:
- → Finance Department Manager, UK
- → Finance Department Manager, Canada
- → Engineer, USA, Project Delta
- → Sales Manager, Sweden

If the organization operates across 20 departments in 20 countries, this results in: 20 departments × 20 countries = 400 roles



And this is only for a single business function. As additional requirements are introduced — such as temporary access, regional restrictions or data sensitivity levels — the number of roles expands rapidly. It becomes easy to see how the number of roles can quickly grow out of control, resulting in role explosion.

Is Role Explosion Becoming a Problem?

Many organizations don't realize they're experiencing role explosion. It often happens gradually as new applications, business units, regions, projects, and compliance requirements lead to the creation of increasingly specific roles.

Instead of broad business roles such as Sales Manager or Finance Analyst, organizations begin creating highly specialized role variations to accommodate different combinations of attributes. Over time, these role variations multiply, making access management increasingly difficult to scale.

If any of the following sound familiar, it may be time to rethink your authorization strategy:

- Your identity and access management (IAM) team manages hundreds or thousands of roles.
- New projects frequently require creating new roles.
- Users accumulate multiple overlapping roles.
- Temporary or project access requires creating permanent roles.
- Business units request role exceptions on a regular basis.

Challenges of Role Explosion

Administrative Overhead: Managing hundreds or thousands of roles becomes increasingly complex and time-consuming for IT and security teams.

Increased Security Risk: It becomes more difficult to maintain consistent least-privilege access. Excessive, overlapping, or outdated roles can lead to overprovisioned access and increase the risk of unauthorized access or compliance violations.

Reduced Agility: Making access changes often requires creating, modifying, testing, and deploying new roles across multiple systems. This slows down onboarding and the ability to adapt quickly to changes.

Poor User Experience: Users frequently accumulate unnecessary permissions or experience delays waiting for new roles to be created and approved.

High Operational Costs: Role engineering projects can take months or years and require continuous maintenance across applications and business units.

Business Impact of Role Explosion

Role explosion is more than an IAM challenge — it can become a significant business and security issue. As the number of roles grows, organizations spend more time creating, maintaining, reviewing, and auditing access than responding to new business needs. Security teams become burdened with operational overhead while users experience delays in obtaining the access they need.



At the same time, an increasingly complex role model makes it more difficult to consistently enforce least-privilege access. Overlapping, outdated, or overly specific roles can result in excessive permissions, increase compliance risk, and make it harder to understand why users have access to sensitive resources. As organizations expand through new applications, cloud services, mergers and acquisitions, or AI initiatives, these challenges only become more pronounced.

How AI Can Accelerate Role Explosion

AI agents are introducing a new category of identities that need access to enterprise applications, APIs, and data. Like human users, these agents may require different levels of access depending on what they are doing, what data they are accessing, and on whose behalf they are acting.

Trying to manage these variations through traditional roles can accelerate role explosion. Organizations may find themselves creating increasingly specific roles for different AI agents, applications, data types, tasks, or levels of privilege — adding another layer of complexity to an already difficult role model.

Policy-driven authorization provides a more scalable approach. Instead of creating a new role for every AI use case, organizations can evaluate attributes and context at runtime to determine what an AI agent is allowed to do. For example, policies can consider:

- Which AI agent is making the request
- The user or service the agent is acting on behalf of
- The resource or data being accessed
- The action the agent is attempting to perform
- The sensitivity of the data
- Current risk or environmental conditions

Moving Beyond Static Roles

To reduce role explosion, organizations are increasingly adopting dynamic, policy-based authorization models. These approaches support more fine-grained and context-aware access decisions that role-based models alone can't effectively manage.

By combining roles with policy-driven authorization, organizations can maintain simple business roles while using policies and attributes to make fine-grained access control decisions in real time.

Instead of creating new roles for every possible access scenario, access decisions are evaluated dynamically using centralized policies and contextual attributes.

This allows organizations to account for:

- Segregation of duties (SoD)
- Geographic restrictions
- Data sensitivity
- Time-based access
- Relationships
- Risk signals and user context

Rather than asking: "Does this user have Role X?"
The system evaluates: "Should this user have access to this resource under these conditions right now?"

How Dynamic Authorization Reduces Role Explosion



Scales with growth: Organizations can define policies instead of creating separate roles for every department, region, contractor type or exception.



Context-aware: Authorization decisions evaluate attributes such as user location, device type, data classification and risk level in real time.



Centralized authorization: Policies are managed centrally rather than hard-coded across individual applications, improving consistency and governance.



Easier to manage: Project-based, time-limited, or conditional access can be handled through policies instead of creating permanent roles.



Supports least-privilege access: Users receive only the access they need based on current context, reducing unnecessary permissions and standing access.

Why Organizations are Moving Beyond RBAC Alone

Modern enterprises need authorization that can adapt to changing users, resources, and risk. Policy-driven authorization complements a role-based approach by making access decisions based on real-time context rather than an ever-growing number of roles.

TRADITIONAL RBAC	POLICY-DRIVEN AUTHORIZATION
New role for every variation	Policies evaluate attributes dynamically
Static permissions	Context-aware decisions
Thousand of roles	Smaller set of business roles
Manual updates	Policies adapt automatically
Slow to change	Faster response to business changes
New roles for different AI agents and use cases	Policies govern AI access dynamically

Enterprise Use Case Example

An example would be a global manufacturing enterprise operating in 40 countries relying heavily on traditional role-based models to control access across ERP, supply chain, and manufacturing systems.

Over time, the organization accumulated more than 8,000 roles as new requirements were introduced for:

- Different plants and regions
- Contractors and suppliers
- Temporary project access
- Regulatory restrictions
- Sensitive production data

This made access reviews and audits more difficult to complete. Users were often over-permissioned and security teams struggled to maintain least-privileged access across systems.

To solve the problem, the enterprise implemented a centralized, policy-driven authorization solution. This reduced the amount of roles being created by enabling real-time access decisions based on attributes such as:

- Location
- Relationship
- Device
- Data sensitivity
- Operational risk level

As a result, the company significantly reduced the number of roles it needed to manage, while strengthening consistency, scalability, and security across its global operations.

Role explosion can make managing access across enterprise environments increasingly complex, creating administrative overhead and making it difficult to maintain consistent, secure access controls. Implementing a policy-driven authorization strategy helps organizations move beyond traditional role-based approaches and simplify access management.



Reach out to us for a consultation on how Axiomatics' Authorization Management Platform can help your organization reduce role complexity, introduce fine-grained authorization, and build a more scalable access control strategy.

Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel



About Axiomatics

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, APIs, data, and AI systems. The world's largest enterprises and government agencies rely on the Axiomatics Authorization Management Platform to centrally define and enforce dynamic access control.

Learn more or request a demo of our solution:

axiomatics.com
info@axiomatics.com
US Office: +1 (312) 374-3443
Europe Office: +46 8 51 510 240