



SOLUTION BRIEF

Protect Critical Data and Enable Collaboration with ABAC

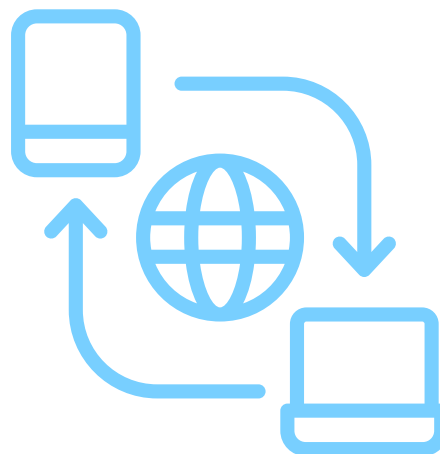
Access control has evolved to meet the changing security challenges organizations face in the digital age. Attribute-based access control, known in brief as ABAC, is quickly becoming the standard model for organizations confronted by the need for a robust and flexible solution to today's increasingly complex security demands.

Unlike earlier access control models, ABAC provides a multi-dimensional system that through its use of attributes and policies prevents role explosion, increases scalability, enables relationships, eliminates Segregation of Duty conflicts, and externalizes authorization for ease of management and control. Additionally, it allows organizations to comply with an ever- growing body of regulations in an increasingly demanding regulatory environment.

5 Key Features of ABAC

1. Externalized

Instead of delivering applications with authorization hard-coded, the software developer simply implements core business functionality and reuses common blocks for nonfunctional aspects such as authentication, logging, and data storage. For authorization requirements, this separates the management of access control policies from the application development lifecycle. In essence, it reduces the need to touch application code every time there is a business, regulatory or internal change. And developers stay focused on building great applications, not security processes.



2. Centralized

ABAC policies introduce a centralized mechanism to fine-tune and control who has access to what, and under what conditions. A change to a policy or new policy can be coded once, and implemented across the application and data ecosystem.



3. Attribute-based

Attributes are labels - or pieces of information - that describe anyone or anything. Role, department, and year are examples of attributes. An attribute is typically a key-value pair, meaning that attributes come in sets: an identifier (or key) and the value or values identified with it. The attribute identified as “role” could, for example, have values such as “art teacher,” “teaching assistant,” “nurse,” etc. The fact that we can use attributes that describe virtually anything makes ABAC multi-dimensional.



4. Policy-driven

Attributes alone, though, are not enough. Policies are statements that bring together attributes to express what can happen and is not allowed. Policies in ABAC can be granting or denying policies. Policies can also be local or global and can be written in a way that they override other policies.

Examples include:

- A user can view a document if the document is in the same department as the user
- A user can edit a document if they are the owner and if the document is in draft mode
- Deny access before 9am

With ABAC you can have as many policies as you like that cater to many different scenarios and technologies.



5. Standardized

In the past, authorization rules were embedded in the programming code of individual information systems. The definition of access control was therefore done not by business managers but by the technical staff responsible for software configurations or programming, often in siloed business units. XACML however, offers a standardized approach that is used consistently across all applications. The focus is on corporate policies rather than the technicalities of varying software environments.



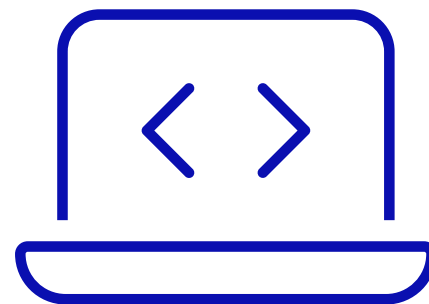
Key Benefits of ABAC

- Simplifies authorization requirements gathering and implementation
- Makes onboarding new APIs faster and more streamlined
- Provides agile, more loosely-coupled, flexible architecture
- Provides consistent and coherent authorization
- Enables policy-driven authorization
- Simplifies audits and access reviews
- Saves development time

Take the next steps

Learn how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

[Meet with our solution experts for a demo](#) of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



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](#)

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: <https://linkedin.com/company/axiomatics>

Join us on YouTube: <https://youtube.com/@axiomatics>

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