



SOLUTION BRIEF

Bring Fine-Grained Access Control to SAP

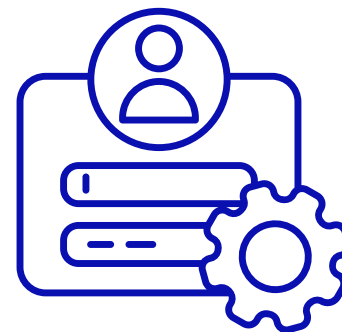
Streamlined sharing and compliance

Whether it be a large enterprise or a smaller business of less than 100 employees, tech stacks are exploding in size. In fact, on average companies (all sizes) use roughly 291 applications. That said, there are some applications that seem to pop up in almost every tech stack and one of those is SAP - the world's largest provider of enterprise application software. As of 2024, 99 out of 100 of the world's largest companies use SAP. SAP contains an abundance of sensitive data spread across a large surface. Consider just the sensitive data in the ERP and it has everything from personal data of employees, customers, financial data, trade secrets, etc.

This sensitive data needs to be protected as per many international compliance regulations but also for the continued success of the organization. Similarly, the same can be said for any sensitive data contained in many of the other 290 applications that the average company manages.

Permissions, permissions, so many permissions!

In order to control access and protect sensitive information, compliance and IT teams are tasked with applying a multitude of permissions across these various applications and keeping track of who has access and under what conditions. One of the more established and common methods is to employ [role-based access control \(RBAC\)](#). The principle is that every user is categorized with a role and their access entitlements are based on that role.



The challenge with this approach is that it's static in nature, so it's based on the decision of a role assignment that occurred when the user was provisioned and it doesn't take into account any current context that should be evaluated at the time of access.

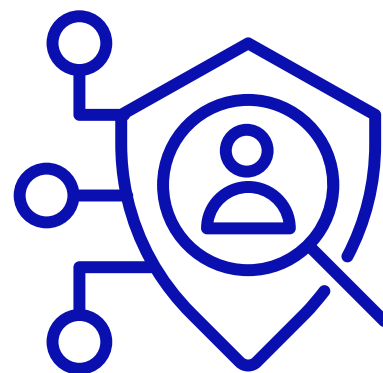
Additionally, since many people end up holding more than one role, role explosion occurs. This can be very confusing and can result in conflicts between roles assigned to the same user, making things very difficult to manage. The secondary but equally important challenge with this approach is that not every RBAC solution works with every application. The result is that a team may be forced to compromise on a less capable access control solution for some of their apps, and leverage another one for other apps. They may even need to apply some access controls manually for other applications. In some cases, they may be forced to enable more broader access than they would like, simply because there's not a way to apply fine-grained access controls that limit a user to viewing only certain information in the application. Managing access policies in all of these disparate systems is a recipe for a headache. When a policy change is required, it will need to be made across multiple systems, and many will require downtime for an update, adding further delays to productivity.

1. https://chiefmartec.com/wp-content/uploads/2023/04/saas-count-and-spend_1456px.png

2. <https://www.sap.com/about/company.html?pdf-asset=4666ecdd-b67c-0010-82c7-eda71af511fa&page=1>

What's the best approach?

When looking for a solution to implement fine-grained access controls, [attribute-based access control \(ABAC\)](#) is an approach that goes beyond the static decision of what role(s) a user has been assigned and instead leverages multiple attributes in real time to make a dynamic decision. With SAP being used at nearly every organization, it makes sense to choose [an ABAC solution that can work with SAP](#). On the flip side, you also want to ensure that the solution you select can be leveraged beyond SAP so that you aren't forced into a situation of managing multiple policies in multiple solutions. The goal is to have a limited portfolio of solutions that your team needs to manage.



Aside from simplicity, it means that when a change in policy needs to be made, it can be made in one solution and pushed out from there to take effect in all connected applications, both SAP and non-SAP. By leveraging an ABAC approach, it also enables the organization to account for multiple use cases beyond an approval or denial of access. Consider scenarios where you may want to approve access, but you need to apply specific transaction controls. An example of this could be when access can be approved, but with the caveat that any PII data is masked. This way, the user can still do their job, but thanks to the policy, security and compliance are maintained.

Access Control for multiple decision outcome scenarios

In order to make this a reality, we need to break the challenge down into three elements:

1. Policy Decision Point (PDP) which is where the decision is made.
2. Policy Information Point (PIP) which refers to the points where information is collected, such as the classification of a file, location of the user, risk score, time of day, and so on.
3. Policy Enforcement Point (PEP) which is where the rubber hits the road and the user is either blocked from accessing, or is permitted access but with a condition such as data masking.

The difference in the RBAC and ABAC approach is that RBAC only looks at the role as the sole policy information point. Again, the role of the user may have been assigned months or even years ago and no other real time information is considered. Axiomatics has integrated with Pathlock Dynamic Access Control to apply ABAC to SAP and extend those same policies across the rest of the enterprise environment. This integration enables organizations to craft very specific policies that apply specific transaction controls in SAP that can also be pushed out to the rest of an organization's applications as well.

Walking the tightrope between security and efficiency

Looking at manufacturing as an example, if a business is supplying specific products to the government or military, they will almost always have to prove compliance with whatever export controls exist in their country. These can be quite complicated depending on the sensitivity of the information and context. These sorts of compliance requirements can put security teams in the very difficult position of walking a tightrope between locking things down while still enabling the business to function.

Export Controlled Information (ECI) example

In this simplified fictional scenario, a battery manufacturer is a supplier to the military and one of their batteries is used in a specific piece of military hardware. While they may not possess details or even know what piece of military hardware their batteries are used in, the details around the measurements and power specifications of the battery model could be very dangerous in the wrong hands. As such, almost all of the information related to the battery model is considered ECI under International Traffic in Arms Regulations (ITAR). The battery manufacturer is required to classify all related data and control access based on a number of attributes such as the country of control, classification of the data and so on.

Below explains how an access attempt of data within SAP would be handled using fine-grained access controls.

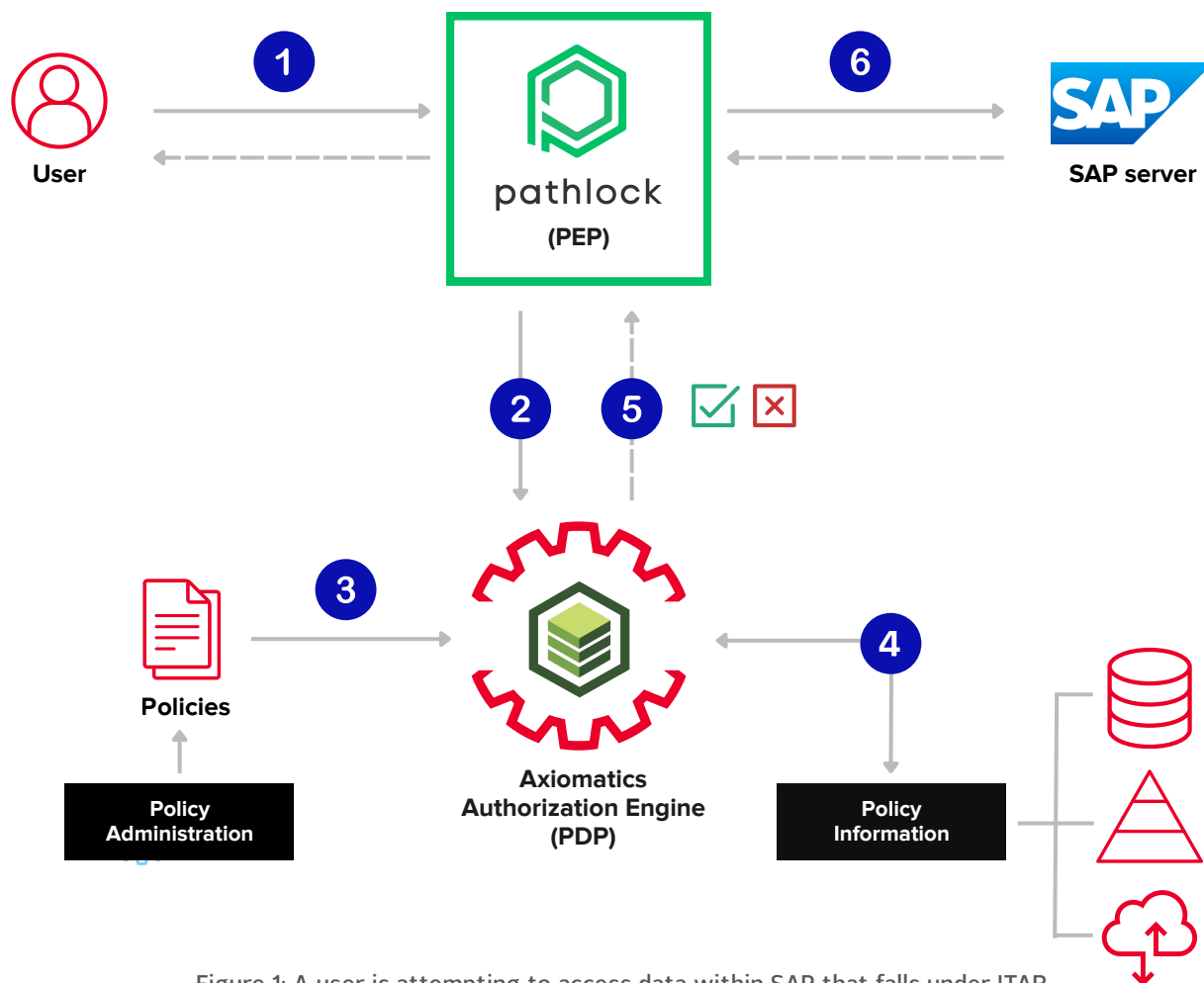


Figure 1: A user is attempting to access data within SAP that falls under ITAR

- | | |
|--|--|
| <p>1 User attempts to access the data in SAP</p> <p>2 Pathlock (PEP) sends the user's intent to Axiomatics (PDP)</p> <p>3 Axiomatics reviews policies in real time</p> <p>4 Axiomatics collects the necessary attributes from the appropriate information points (PIPs). Some of the attributes in this example could include:</p> <ul style="list-style-type: none"> a) data classification (i.e. is it considered export controlled?) b) Country of control pertaining to the data c) Country of residence of user d) Citizenship of the user, etc | <p>5 Axiomatics sends the decision and any necessary conditions (i.e. file can be viewed BUT some of the data must be masked) back to Pathlock to enforce (PEP)</p> <p>6 The user is able to access the data in SAP with any necessary conditions applied (or receives a denied message)</p> |
|--|--|

Create once, deploy everywhere...SAP and beyond

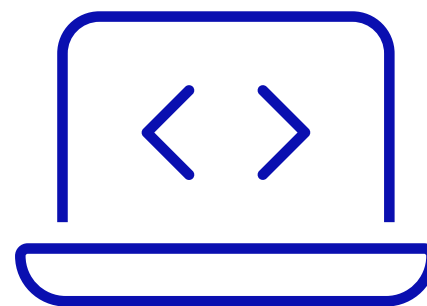
While ABAC has been around as a concept for years, the challenge that has kept many organizations from adopting it is that it was notoriously difficult to implement on complex applications like SAP. Administrators were forced to rely on whatever out of the box capabilities that applications came with or simply limit access to those applications as best they could. But with so much information contained in an ERP system like SAP, that becomes increasingly difficult as so many teams across the organization need to access their relevant data contained within, in order to do their jobs. Now with this integration between Axiomatics and Pathlock, organizations can create very detailed policies once in Axiomatics, and then push them out to all appropriate applications across the enterprise, starting with SAP via Pathlock. Even with multiple SAP servers, the policy can be managed and pushed out once and there is no longer a need to duplicate and manage the policy separately for each SAP server. If the policy pertains to certain data that is contained in SAP and other applications - no problem. That same policy can be applied to multiple applications via several deployment options. The result is one policy solution for a centralized policy library that is used with an approach that works for your organization based and your particular requirements.

To learn more about the Axiomatics integration with Pathlock, please visit axiomatics.com.

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