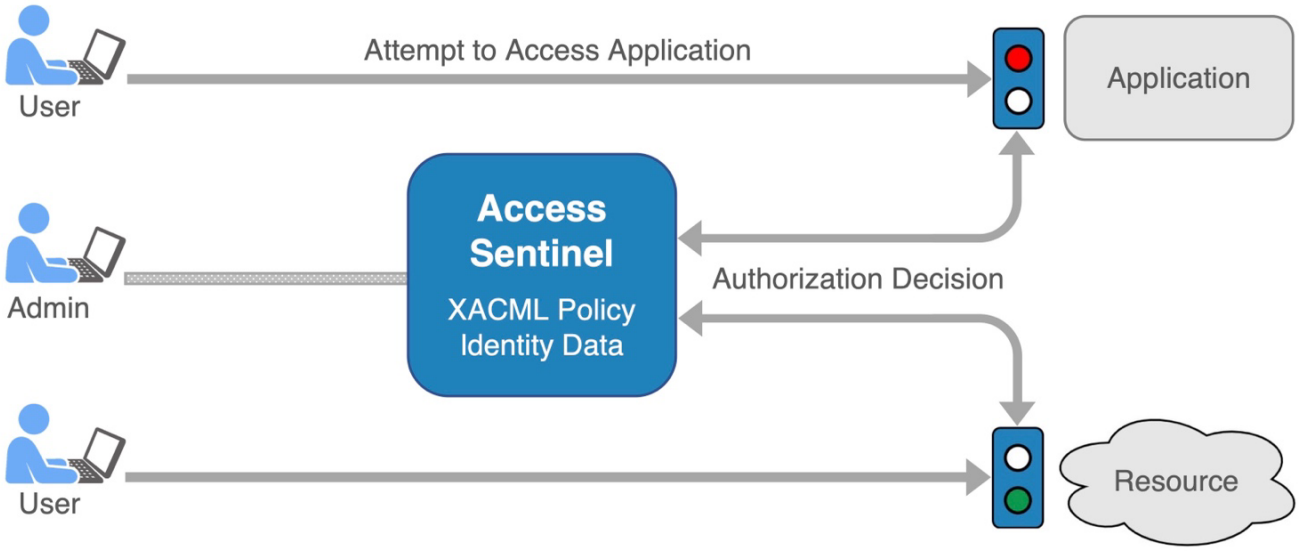
ViewDS Access Sentinel

Centralized, fine-grained access control across all on-premises and cloud applications increases efficiency and strengthens security.

The legacy approach to access control is to *embed* it within every application. This approach, however, is inefficient and costly. Even a simple change in policy requires an update to every application, and the complexity intensifies further when there's a range of technologies and interfaces in the mix.

ViewDS Access Sentinel is a highly efficient authorization server that centralizes policy management. It allows you to manage authorization for all applications, whether they're within your enterprise's infrastructure or part of your offering as a vendor.



The benefits of a unified view of authorization are realized when maintaining policy, when implementing new applications, and when auditing for compliance.

Additionally, Access Sentinel's fine-grained authorization, based on the XACML framework, provides greater levels of security and control. The framework goes beyond simply determining who has access to which resources by also considering the why, when and where of entitlement.

Centralized management across entire enterprise or vendor services

Attribute-based access control for greater levels of security and control

Intuitive UI for no-code policy definitions in the same format for all applications

Integrated architecture with native XML support is efficient, secure, and scalable

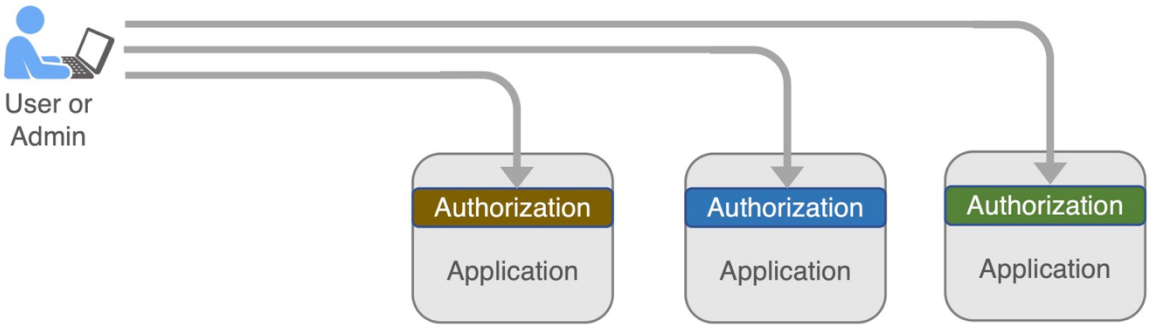
Rapid app integration with pre-built *Policy Enforcement Points* plus integration kits

Streamlines managing policy, auditing for compliance, and integrating applications

viewds identity solutions

Use case: Enterprise-wide authorization

With the *embedded* approach to authorization, each application contains an entitlement layer. When a user attempts to access an application, the application interrogates its local copy of the access-control policy to determine the user's access rights.



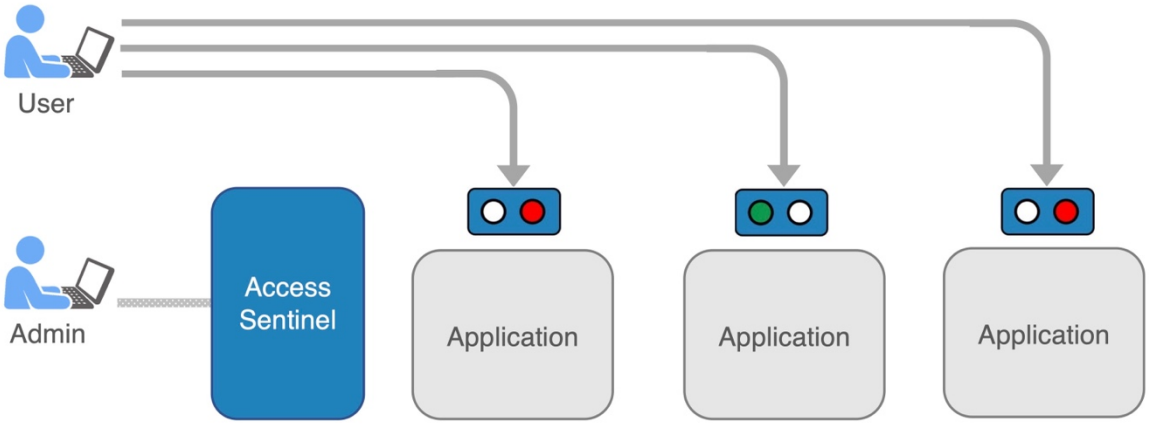
This approach is highly inefficient.

An enterprise-wide change of policy requires updates to every individual application. An audit for compliance requires examination of every individual application. And as there's no guarantee of consistency between entitlement layers, support staff may need to tackle the same tasks in many different ways, through different interfaces on different platforms.

Access Sentinel solution

Access Sentinel overcomes these inefficiencies, and mitigates their risks, by removing the entitlement layer from within each application and centralizing policy management and processing.

As well as providing a more efficient approach to maintaining and auditing policy, Access Sentinel allows access controls to be applied globally and consistently. Life becomes easier for support staff as they can define policy for all applications in one hit through a single, intuitive user interface.

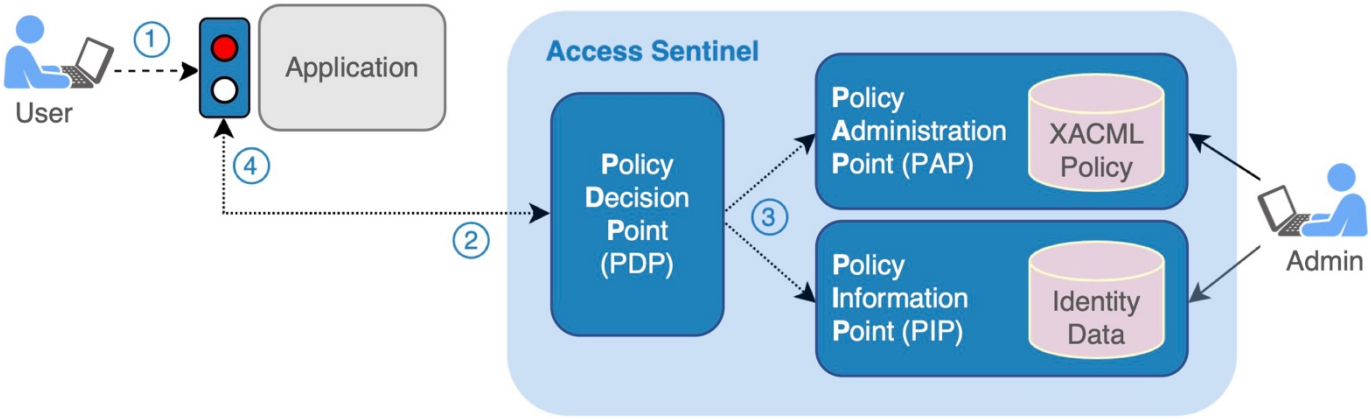


The world also becomes a little brighter for software developers as they no longer need to write an entitlement layer for each new application. Instead, Access Sentinel provides a lightweight *Policy Enforcement Point* (PEP) at the application to enforce the access-control decisions made centrally.

XACML framework

Access Sentinel uses a standardized framework – *eXtensible Access Control Markup Language*, or simply XACML – to deliver fine-grained access control. The framework provides an architecture, plus processing model and markup language, which extends access control to include attributes and resource metadata, such as a user's identity data, their environment, and actions.

Before going into more benefits, consider how Access Sentinel implements XACML.



The illustration shows what happens when a user tries to access an application:

1. The user's attempt to access the application is intercepted by the *Policy Enforcement Point* (PEP).
2. The PEP asks the *Policy Decision Point* (PDP) to make an authorization decision.
3. The PDP assesses the XACML policy (in the PAP), which may also involve considering identity data (in the PIP) such as the user's security level, job title, or location. Other factors in a policy might include the user's attempted action or device, or the time of day, or day of the week, etc.
4. The PDP makes its decision and tells the PEP to grant or deny access to the application.

A unique feature of Access Sentinel is that the PDP, PAP and PIP constitute a single component. Consequently, as the XACML policy and identity data reside in a single repository, an admin user (see above illustration) can manage policy and identity data from a single user interface.

The ability to store and manipulate XACML policy (an XML document) is possible because Access Sentinel supports *native XML*. It therefore has the rich indexing and search capabilities required by the PAP.

Benefits of integrated architecture

Access Sentinel's integrated architecture has major benefits. From the start, deployment and then administration are simplified because the PDP, PIP, and PAP are combined in a single component.

Performance and security are optimized because the PDP has direct access to the policy and identity data. There is no need for any external network traffic, additional authentication and authorization, or additional integrity and confidentiality protection.

Efficiency is also improved by unified access control. Just one set of XACML policies is required to control access to the external applications, the policies in the PAP, and the identity data in the PIP.

Application integration

Access Sentinel provides a range of pre-built *Policy Enforcement Points* (PEP) to integrate applications, networks, and services.

Also supplied are *Application Integration Kits* for Java and C#, which provide the libraries required to develop a new PEP. The kits abstract the complexities of building and wrapping XACML authorization decision requests and unwrapping responses, simplifying integration significantly.

Access Sentinel also supports SAML, REST + XML, REST + JSON. An application that supports any of these standards can interact with Access Sentinel and exchange authorization requests and responses.

Access control and zero trust

Access Sentinel provides role-based and attribute-based access control (RBAC and ABAC). While the RBAC model authorizes users based on their role, ABAC considers multiple factors such as the characteristics of the user, resource, and environment. Generally, the RBAC model is simpler and provides broad protection while ABAC offers fine-grained, dynamic control.

The ABAC model in Access Sentinel supports a zero-trust approach to security. It provides the ability to easily express least-privilege access controls at any level of granularity.

Summary

In summary, Access Sentinel delivers a highly secure solution that increases efficiency and flexibility and reduces risk and costs.

Efficiency…

- Fewer transactions and less network traffic when processing policy
- Standardized policy definitions maintained from a central location
- Single UI to manage identity data and XACML policy

Flexibility…

- Suite of pre-built PEPs to integrate applications, plus Application Development Kits to streamline development of new PEPs
- Option to mix and match RBAC and ABAC offers greater control, and Access Sentinel's implementation of ABAC provides the ability to apply a zero-trust approach
- Policy change is applied globally and instantly, requiring no application updates

Risk mitigation…

- Single component (PDP, PIP, PAP) simplifies deployment and administration, and improves security
- Designed and developed by a proven software innovator
- Responsive ongoing development to fulfil changing requirements