# PlainID Policy Manager

**Boost productivity with a runtime decision engine that creates cohesive and consistent policies across your organization and a direct connection between users and the resources they are authorized to access**

PlainID's Policy Manager revolutionizes everything you think about Identity Governance and Administration. The Policy Manager leverages Policy-Based Access Control to manage countless access rules distributed across endless repositories and directories, reducing the administrative burden that most IGA implementations bear, giving your organization the ability to grow at an unprecedented pace, feeling confident that access is kept under tight control.

## Why Policy Manager?

### ✓ Business-oriented approach

Policy Manager presents the business owner with a graphical view of the authorization decision, rules and the connection between them to identities, rather than the traditional technical language. In addition, a broad set of APIs offers the flexibility the technology experts require.

### ✓ Policy lifecycle management

Using Policy Manager, you can build your policy on a graph based editor, and then have it approved and certified. That, with the policy simulator function, provides a tighter control of access to data and resources.

### ✓ In-depth Analytics and Insights

Policy Manager offers the opportunity to fully explore the effects of each policy in relation to any/all of the Policy's building blocks. For example: Who are the Identities included in the policy? What applications are affected by the policy? What assets can the user access?

### ✓ Compliance and SOD

Policy Manager provides unobstructed visibility with a full audit trail. Compliance, regulation and audit requirements are set in a policy and managed on our graphical UI. Segregation of Duties is also managed through policies and the same easy-to-use UI, ensuring that the right people have the right access given whatever constraints you add to the policy.

### ✓ Universal Authorization Support

Policy Manager separates the business logic from the technical implementation, enabling usage or distribution of the same policy to various consumers. Policy Manager also answers different Authorization requests/ different access patterns with the same policies, keeping a consistency of answers across the various apps. Policy Manager supports all industry leading standards (REST, JWT, XACML, OAuth, etc.) in addition to adaptive integration with leading vendors such as AWS.

### ✓ Contextual access

Access is determined dynamically and in real time based on user attributes, environmental attributes (time, location, etc.) as well as event based authorizations. Policy Manager combines PBAC & attributes to form a united policy.

### ✓ Fine-Grained Authorization

Policy Manager amplifies Attribute-based Access Control (ABAC) by providing a flexible policy that enables attribute based decisions all the way from the user to the resource/action, based on a pattern or on resource attributes.

### ✓ Virtual identities

Policy Manager provides the ability to "see" all identities that require authorizations, within their management platforms. People, Devices, Things and Services, all require and are granted authorizations to enable access to resources and data.


## Features & Benefits

- Policy Lifecycle Management
- Runtime Access Decisions
- Advanced Analytics
- Contextual & Fine-grained access
- Rapid and Controlled Deployment
- Policy Mining
- Graphical UI & REST API
- Visibility and Investigation
- Version Control
- Virtual Identities
- Compliance and SOD control
- Approval Workflows
- Universal Authorization
- Built in support for leading standards (LDAP, SQL, REST, SCIM)

*"Policy-based access control technology offers a fundamental ability to develop one central facility or control point for managing data access across multiple infrastructures and applications using a "top-down" approach."*
*- Jay Bretzmann, Program Director, Security Products, IDC*

## PBAC Platform

**The PBAC Platform provides a focused approach to Authorization Management and control. Among the platform benefits are:**

**Enterprise grade solution**: Our platform provides the set of capabilities required to efficiently manage your access decisions including a full life-cycle management of application entitlements (fine and coarse grained), delegated admin rights to improve collaboration, audit logs and versions control, business workflows and more.

**Built for the business and IT**: Our platform unifies the access control efforts of IT professionals applying control such as basic 'Yes/No' access of entitlements with business owners adding business policy elements like 'read-only access if title is above manager-level, and if located in HQ office.' Our visualization UI endows entitlements with their business meaning, therefore bringing awareness into both worlds.

**Unified experience**: Browsing through entitlements from any business application, or mining for access policies, is done under a unified web interface with different access levels based on the person's role in the organization.

**Modularity of deployment:** Offers flexibility; start your project by mining for access policies, or begin by bringing context and visibility into access entitlement at any level from any business application.

**Integration with external tools** such as IGA/IDM systems and access enforcement tools is done through industry-standard APIs to further connect between disparate IAM systems, thus modernize your overall IAM program today.