SailPoint + plainID THE AUTHORIZATION COMPANY

SailPoint + PlainID Policy Manager Combined Identity and Authorization

Enterprises are constantly growing due to the continuous need to evolve and adapt. Digital transformation is now a necessity or organizations and with that comes and influx of applications in an enterprise. In order to stay secure and compliant, organizations are looking for a consistent way to control access across numerous applications, and to gain a centralized way of managing permissions. Companies also need a centralized way to manage permissions.

PlainID Policy Manager and SailPoint have come together to offer enterprises a unified and complete approach to control access across all applications. PlainID's Policy Manager offers run-time dynamic decisions while SailPoint provides identity security delivering complete control of access to your applications, whether course or fine-grained, admin-time or run-time.

Coarse-grained to Dynamic, Fine-grained Access: Policy Manager leverages SailPoint to make real time access decisions to applications

Policy Manager connects to SailPoint's identity information store using its built-in SCIM interface. Policy Manager uses SailPoint's identity context which includes identity attributes, roles and entitlements to make intelligent, real-time access decisions. These intelligent real-time decisions are used by applications to control the access to data, resources and actions, making the real-time access consistent with SailPoint.

Policy Manager's virtual directory capability has the ability to enrich the information it gets from SailPoint and can include real-time conditions, such as time of access, IP address, risk score and more. This makes sophisticated and intelligent real time access decisions to applications.

Policies for Coarse-Grained Access: PlainID provides the provisioning/deprovisioning decision to SailPoint based on central policies

SailPoint uses Policy Manager to make dynamic decisions on what to provision/de-provision based on the PlainID REST API. PlainID Policies support SailPoint decisions as part of the provisioning process. The policy layer will support the on-boarding, role changing and request processes, enabling adaptive control of what should and shouldn't be provided to users.

How SailPoint and PlainID work together

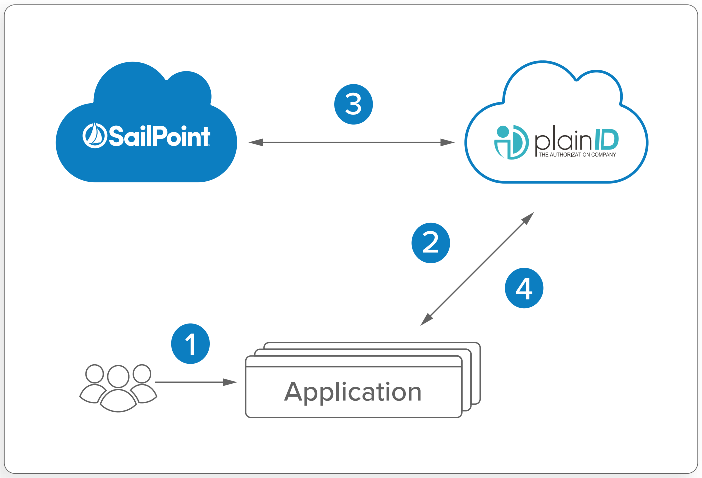
The Sailpoint + Policy Manager integration focuses on 2 key areas:

- **Intelligent Provisioning -** Policy Manager makes dynamic decisions based on current information about the user and the resources. For example, SailPoint gets a decision from Policy Manager to de-provision PII access from a user at the moment they are moved to a different position. At thesame time, applications get real time decisions from Policy Manager to deny the user access to PII information. This approach ensures the consistency of access across all applications in the organization.

- **Providing Run-Time authorizations -** Policy Manager addscontextual and fine-grained support to enhance SailPoint managed identities. This extends the identity context, to be used at run time, to enable real time access decisions and dynamic entitlements.

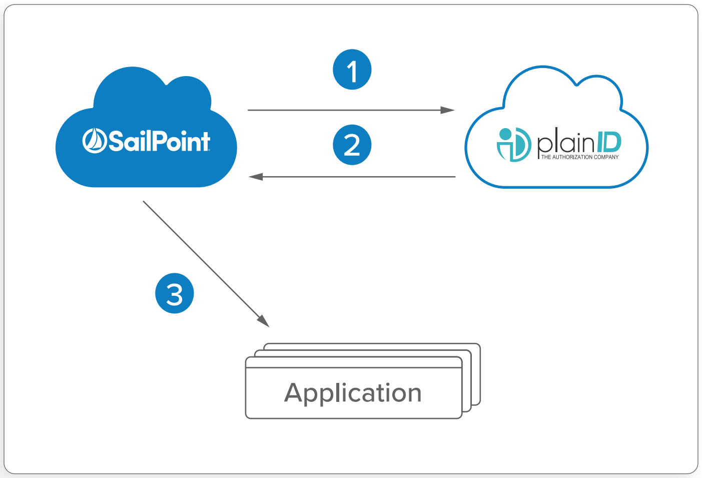
Architecture Pattern #1
Supporting Run-Time Access

1. A user accesses the application.
2. After authenticating the user, the application makes an access request to the Policy Manager.
3. Policy Manager fetches the user attributes and entitlements from SailPoint to make the access decision.
4. The response of what the user can access is sent back to the application.



Architecture Pattern #2
Suppotring Intelligent Provisioning

1. Provisioning Request is initiated in SailPoint.
2. SailPoint sends content of request to Policy Manager.
3. Policy Manager determines whether the request should be approved or denied based on information from SailPoint and additional sources.
4. Policy Manager passes the approval decision back to SailPoint for provisioning.



SailPoint + PlainID together streamline Identity Management with Identity Access Control. Enterprises will achieve:

- Consistent and unified access managment, for both admin-time and real-time access.
- Reinforce risk managment strategy by proactively securing access and supporting “Zero Trust” initiatives.
- Tighten compliance controls with a proactive approach to data and privacy regulations.
- Intelligent dynamic decisions what to provision or de-provision.
- Increase audits and certification process efficiency by maintaining the logic behind identities.
- Access to company data and business functions in PlainID policies.

For more information on this integration, contact us at plainid.com/contact