okta + plainID THE AUTHORIZATION COMPANY

Combine Authentication and Authorization to Better Control Your Most Valuable Assets

Permissions and authorizations are often managed in siloed IT platforms and applications that might provision and even enforce access control, but the siloed nature makes this approach cumbersome, error prone and inefficient. As a result, often IT teams allow broad brush strokes of access to employees, which creates unprecedented security risk. Okta + PlainID work together to solve this problem by offering a policy-based access control solution that simplifies authorization to one point of decision on a dynamic, real-time basis.

Implement secure, end-to-end IAM services

Okta + PlainID combine authentication and authorization, so organizations can better control their most valuable assets. Okta centralizes authentication and PlainID centralizes access control and authorization to create a secure, end-to-end identity access management (IAM) process. Using Okta as its identity source, PlainID gives organizations the ability to better define and control the connection between identities and what identities can do and access, so they can plug security gaps and make better decisions more quickly.

Together, Okta and PlainID let you:

- Combine single sign-on (SSO) authentication and authorization for a more complete, more secure IAM process
- Add policy-based access control to identity management to better define and control the connection between identities and what they can do and access
- Centralize authentication and authorization across platforms and applications to make it easier for security teams to manage and refine access policies
- Make it easier to crate plain language, business-friendly dynamic access control policies and reduce the number of policies needed to reduce the burden on IT

How Okta + PlainID work together

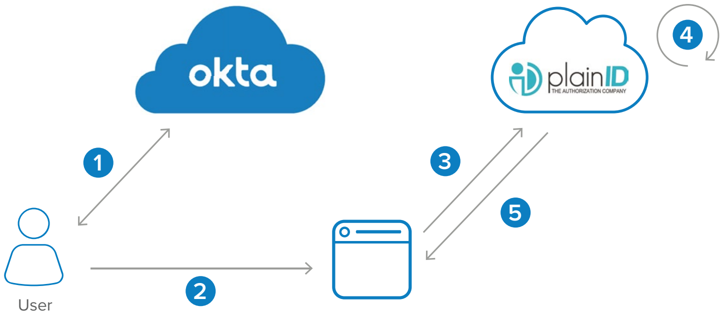
The Okta + PlainID integration focuses on three key areas:

- **Continuing the Authentication-Authorization process**—PlainID continues the authentication process carried out by Okta, to provide the full adaptive access to which the user is entitled. Application owners get combined authentication and authorization for complete end-to-end Identity and Access Management (IAM) services. What users can do is based on who the user is, creating secure IAM.
- **Adding Policy-Based Access control**—PlainID adds a policy layer on top of Okta's identities and roles, to better define and control the connection between identities and what identities can do and access.

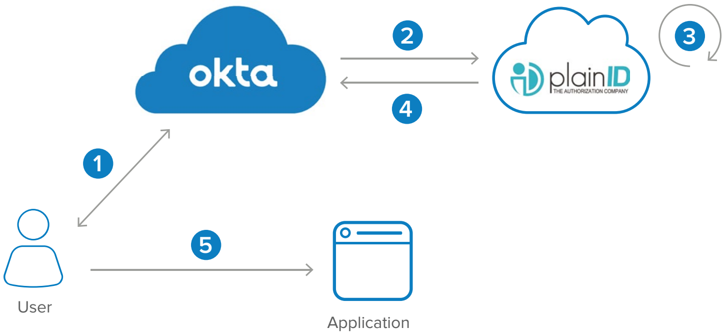
  For example, a bank might use Okta for SSO with the PlainID integration for Policy-Based Access Control. A policy example might say "Branch managers and branch clerks (once authenticated) can access the Client Basic Profile, Bank Accounts and Card Data of clients that belong to the same Line of Business and the Same Branch they belong to."

  This approach allows organizations to better control their access decisions and reduces the number of

Pattern 1



Pattern 2



overall access control policies IT needs to create and administer. It also enables organizations to create delegated admins, so partners can control their customers' level of access to upstream applications.

- **Providing Run-Time authorizations**—PlainID adds contextual and fine-grained support to enhance Okta-managed identities. This extends the identity context, to be used at run time, to enable real time access decisions and dynamic entitlements.

Users initiate an authentication request to Okta vis Okta SSO, and receive an Okta Authentication token. This token is used by PlainID as the main source for identity data. PlainID calculates the authorization for the user, based on information from the token, additional information points, and environmental attributes. PlainID sends the authorization decision back to the app to enforce user access accordingly.

PlainID supports SAML, OIDC, and JWT as a source for identity data, in addition to the authentication source of the user requesting the authorization decision. This option requires minimum integration efforts between the products; however, it requires the authentication token to include the relevant identity data.

With Okta + PlainID, organizations can use a GUI to create plain language, business-friendly, dynamic access control policies at coarse- and fine-grained levels. They can more easily manage access control across applications and get detailed access control analytics, including role mining, compliance, and audit capabilities.

With Okta + PlainID, enterprises can...

- Centralize management for authorizations across all platforms and applications to reduce the burden on IT
- Get a central authorization view for all identities, across all platforms and applications, to make it easier to manage identities
- Enable real-time authorizations determined according to the situation at the time of access, location, events, and other attributes to minimize risk.
- Make better, more informed access decisions to gain competitive advantage

For more information on this integration, go to okta.com/partners/plainid
If you have questions, please contact our sales team at okta.com/contact-sales

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 7,400 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to okta.com.