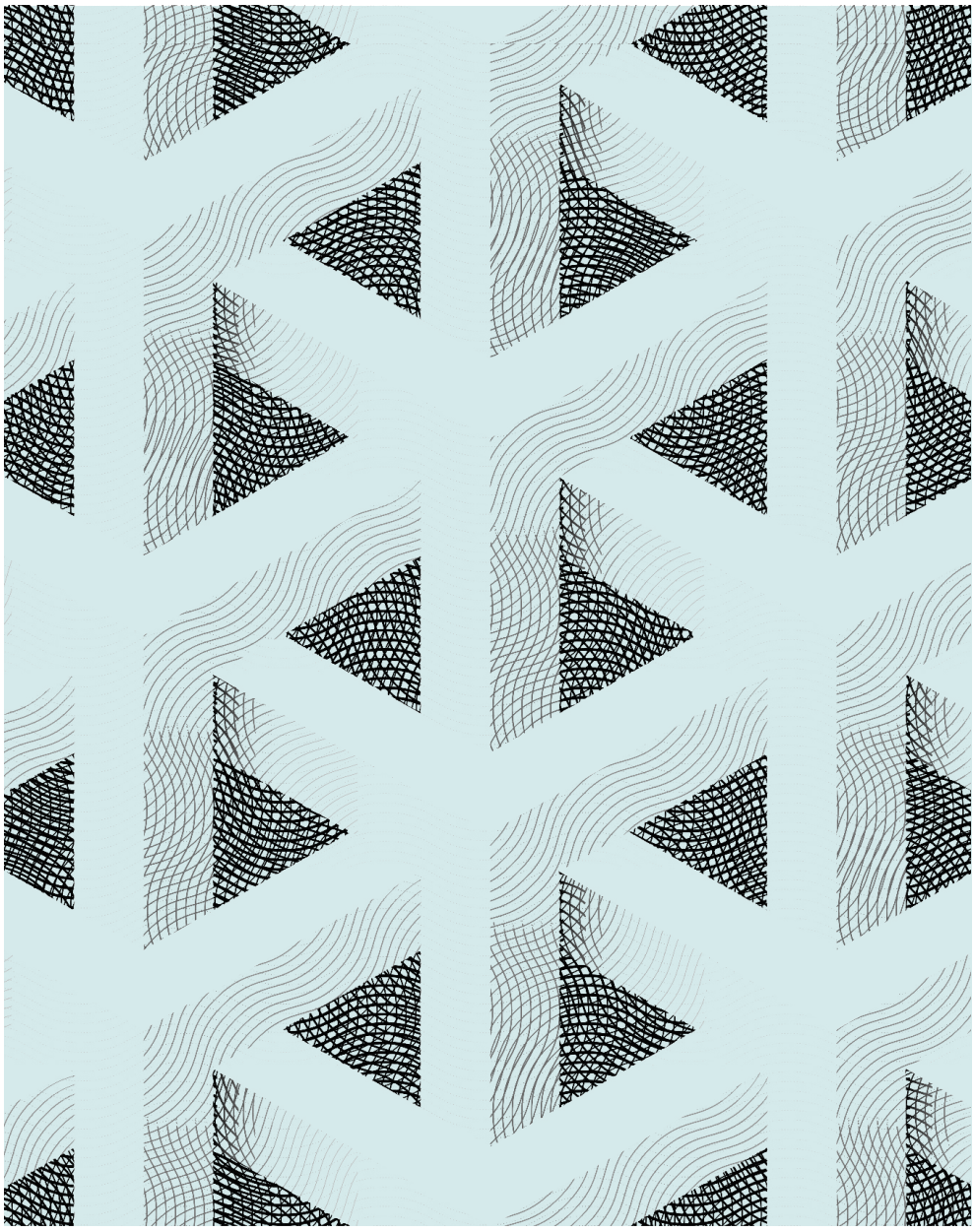
Whitepaper

November 2020

Get Your App Ready for the Global B2B Market

Understanding the power of enterprise identity integration

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

Contents

2 Integrating B2B Enterprise Identities

5 Aspects of Federated ID Implementations

9 Leveraging Okta for Enterprise Identity Integration

13 User Model Use Cases

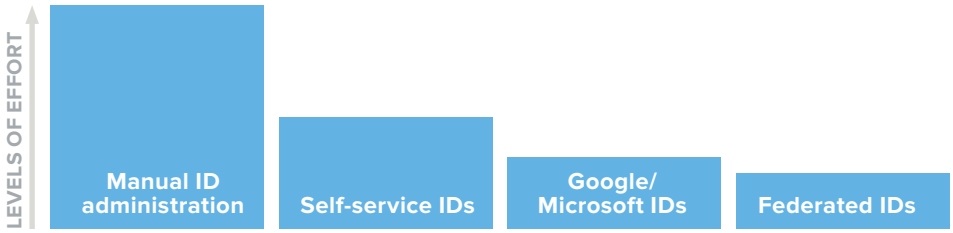
15 Facilitating Authentication and Identity Integration

16 Simplify ID Integration and Grow Your Business Faster

Integrating B2B Enterprise Identities

Seamless interactions with your enterprise partners and customers often require that you grant them access to enterprise applications or internal systems that you've developed or are developing. But in a world where each of your enterprise partners and customers' individual users might already be managing dozens of digital identities, you don't want to jeopardize their user experience by requiring them to create yet another identity to access your application or shared resources. To foster healthy relationships and increase the adoption rate of your technical innovations and applications, you need to create frictionless experiences that allow those users to use their existing enterprise identities.

There are a variety of ways to integrate your enterprise applications and internal systems with your partners and customers' identities. This paper discusses the most common methods, exploring their different advantages and disadvantages.



Manual ID administration

Manually adding partner users and their passwords into enterprise applications and internal systems is the oldest method currently in use in enterprises. Although sometimes referred to as the traditional method, the fact that it's old and is still a common way to connect partners to an enterprise system doesn't make it the best choice.

The manual nature of assigning credentials not only means administrators have knowledge of users' credentials, there's no guarantees that those credentials haven't been intentionally or unintentionally exposed to others. Neither enterprises nor their partners can afford this level of inherent risk. But if that's not enough reason to influence organizations to choose a newer, more secure enterprise identity integration option, then the lack of scalability in manual integration should be. The administrative overhead of adding all those different users and managing their account lifecycles from beginning to end is not sustainable as you and your partners grow.

Self-service IDs

Self-service allows individuals in your B2B and B2C relationships to self-register their own user accounts into your system. Since individual users are the only ones to see their own personal identifiable information (PII), it's a significant step up in security over the manual integration method. Additionally, most self-service methods also include built-in password recovery workflows. So, if users forget their passwords, they can recover or update them without administrative intervention and overhead.

While self-service IDs might be fine for B2C relationships, it creates a significant burden for your B2B partners since every user in the partner organization that needs to access your system needs to go through the registration process. These users also become responsible for remembering or securely storing their newly created credentials. Shifting these burdens to your business customers' and partners' users runs counter to your desire to nurture better B2B relationships through frictionless experiences.

An additional downside of self-service IDs is that if or when your partner relationship ends, you need to make sure to eliminate each one of those self-service accounts to ensure the security of your system and prevent unauthorized access. Often that requires a manual administrative effort that consumes significant time, especially when your dealing with large enterprises. There's also the added security risk that with such a daunting manual effort, it can be extremely difficult to verify that every account has been properly removed.

Google/Microsoft IDs

Sometimes known as bring your own identity solutions, these identity integration scenarios allow users to sign in with their Google or Microsoft credentials to access resources shared with customers or partners. This method has grown in popularity in recent history since it reduces friction in the overall experience. Neither your customers, partners, or administrative staff need to expend effort in creating and managing new user profiles.

Since a large user base exists for both the Google and Microsoft platforms, this method can greatly simplify enterprise identity integration. But the fact is that not everyone has Google or Microsoft identities. As a result, this method can leave out some of your customers' and partners' users, including identities created in homegrown systems or applications with unique user bases, such as Github or Fitbit. Due to these user exclusions this method might not meet your needs for enterprise identity integration on its own, but when combined with ID federation it can deliver some strong benefits.

Federated IDs

Since federation provides the most frictionless experience for users and administrators, an increasing number of enterprises continue to choose it for enterprise identity integration making it one of the most preferred methods. Under ID federation you and your partner or business customer mutually agree to allow their users to use their own enterprise identities to access authorized applications or services that you provide or share. It does this by pairing your different identity systems through a metadata exchange. This allows you to create a single sign-on (SSO) experience for their users while giving them a familiar user interface.

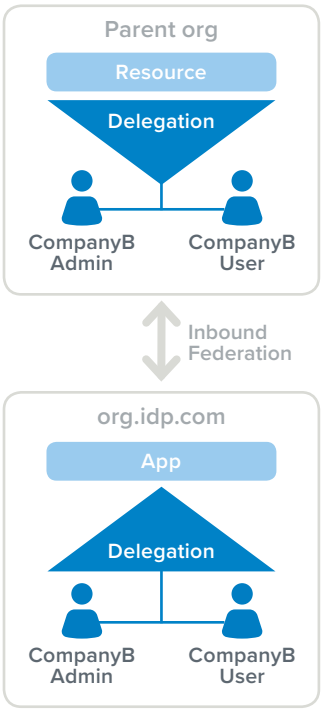
With the exponential growth of partner ecosystems, federation offers enterprises the best option for integrating identities in a way that enhances collaboration with partners. It simplifies integration in a manner that provides frictionless experiences, facilitating your ability to quickly get your applications to market and adopted so you can grow your business. That's why it's becoming a standard method of supporting enterprise relationships. There are different ways to implement ID federation and there are different aspects and use cases related to the technology that you should be familiar with as you plan your enterprise ID integration strategy.

Aspects of Federated ID Implementations

Delegated administration

Delegated administration allows another entity to manage or administer their own users who access the application, services, or resources you provide or share. This could include delegating some level of administration rights to your partners or business customers, such as the ability to grant and remove their own users' access rights to your applications. It could also extend to giving them the ability to define the login experience for their users.

Delegated administration could also be used to give your partners or customers complete access over policy and user management. This could be achieved by leveraging a cloud-based solution for user storage. Such solutions prove to be more cost effective than on-premises solutions based on client access license (CAL) scenarios. Regardless of how delegated administration is employed, it's an important part of the trust relationship that two business entities enter into when creating relationships.



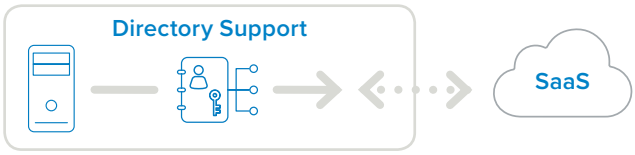
Security and lifecycle management

An ID federation solution that provides centralized management is vital to simplifying management of your integrated IDs and keeping your environments secure. Through a central management point you can more easily enforce policies across all the applications that you authorize your partners or customers to use. For example, you could heighten security on sensitive systems using multi-factor authentication (MFA) and by enforcing risk-based policies.

Centralized management also makes it easier to revoke access to users when a B2B relationship ends. This might include the ability through ID federation to tie into a customer's or partner's identity system to leverage their system's lifecycle management functions to terminate users' access to your application. Having a simple and effective means to grant and terminate authorized access is critical to your ability to prevent system abuses and breaches.

Legacy integration with migration

Some ID federation solutions can provide bridged access between cloud-based identity services and legacy on-premises identity systems. This can provide a standards-based way of integrating disparate identity systems, while providing a migration path from a legacy, proprietary system to a newer modern system. And it does it without requiring you to create a separate login experience for the old legacy system and the new cloud service.



Flexible and secure user models

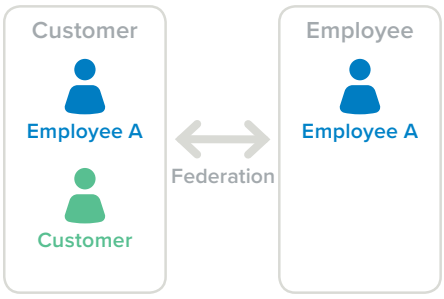
Whether it's a mix of customer, employee, or partner users, the types of users you need to account for when integrating enterprise identities vary from one relationship to another. The makeup of your relationship's user model will be a key influencer on how you address customer data access, data separation, and user experiences in your identity integration strategy. To handle these different scenarios, an ID federation solution that enables you to easily connect to different identity providers can give you much needed flexibility when it comes to architecting your user structure.

The following are some of the most common user models that organizations deal with when integrating enterprise identities:

- Customer and employee user models
- Customer, partner, and employee user models
- SaaS to multi-customer user models

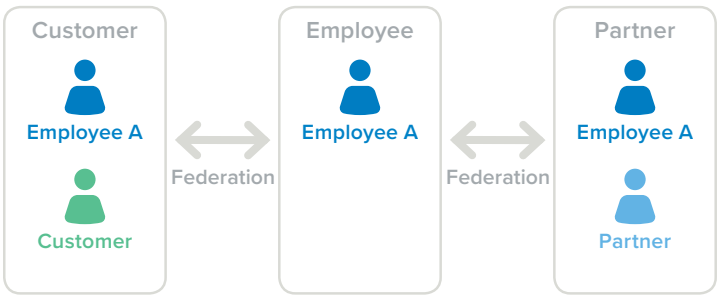
Customer and employee user models

When it comes to the customer identities you maintain for your B2B and B2C relationships, those customer identity profiles often need to be stored in a separate identity system than where your organization stores identity profiles for its internal employees. This separation of identity data helps you safeguard customers' personal identifiable information (PII) from unauthorized access and data breaches, while enabling authorized internal employees, such as certain marketing personnel and IT staff, to access customer information as needed for marketing and administration purposes.



Customer, partner, and employee user models

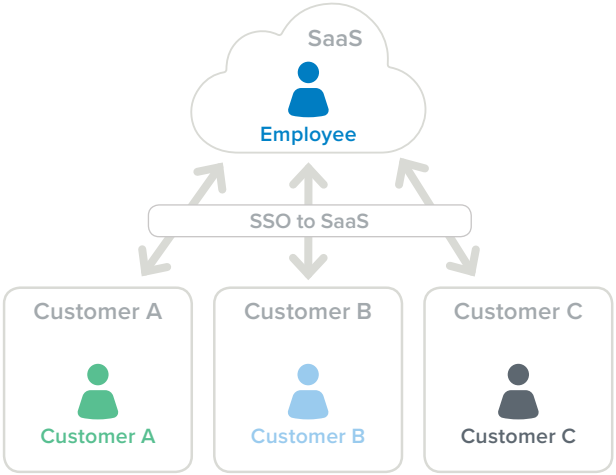
When you add partner users to a customer and employee user model, you need to also segregate the storage of the identities associated with the partner's users. This multi-tenancy requirement should allow you to maintain partners and partner portals in one tenant, customers and customer-specific apps in another tenant, and employees in yet another tenant. Your ID federation solution should give your administration team the ability to manage all three user types through federation.



SaaS to multi-customer user models

Many software companies moving to the cloud want to move away from on-premises solutions for storing user identities and profiles. To do this, some create an identity provider, add their customers' and partners' users to it, and then assign those users the appropriate resource accesses. But this can be a complex undertaking for many software as a service (SaaS) providers, especially those that have a delegation subscription model that allows their partners or customers to resell services or application licenses to other customers or partners.

In these complex kinds of scenarios, SaaS vendors have to create unique user stores for all the downstream customers and partners, and then connect those user stores to the parent identity provider that maintains the access information for their cloud-hosted software. To effectively implement this user model, the ID federation solution needs the ability to facilitate the granting of policy and user management to downstream customers and partners when appropriate. This requires the ability to programmatically create an identity provider and configure its connection back to the main parent resource.



Leveraging Okta for Enterprise Identity Integration

The applications you build and the web services you create are the things that bring real value to your business. That's your expertise. That's your focus. Anything that distracts you from that focus negatively impacts your ability to deliver expected business outcomes. Having to build your own authentication and identity integration functionality disrupts and distracts your ability to achieve those business outcomes. That's where Okta can help.

Through its identity cloud and Okta's Customer Identity solutions, Okta facilitates enterprise identity integration for all your B2B and B2C use cases. It frees you from the task of building your own authentication and identity connections for your different partners, customers, and even separate internal business units. As a result, you can get to market faster and foster better B2B and B2C relationships by giving your partners and customers the secure and frictionless access to your services they want and need.

Okta Inbound Federation

The inbound federation functionality in Okta allows your Okta tenant to act as a service provider, granting external identities access to your Okta protected application or website. While this is a role reversal of traditional SSO solutions, it gives you consumption endpoints for authentication, enables just in time (JIT) user creation, and makes it easy to terminate connections with other enterprise entities. It also provides identity provider discovery (IDP discovery) functionality, which adds a rules engine to your login flow that directs users to the appropriate IDP login page based on set criteria.

Okta allows you to implement inbound federation with either the Security Assertion Markup Language (SAML 2.0) protocol or the OpenID Connect (OIDC).

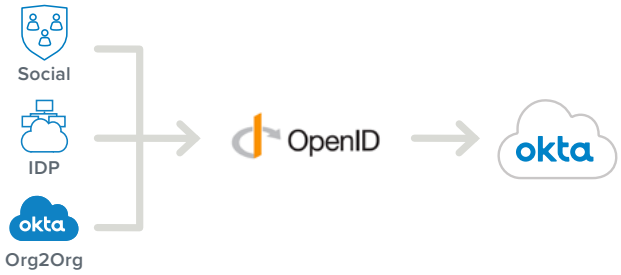
For more information, visit our Identity Providers API documentation page.

SAML

For years SAML has been the gold standard for federation in the enterprise space. It allows you to use a set of attributes to identify a user. It's secure and easy to setup. While it is still a great solution and will work for most enterprise ID integrations, SAML 2.0 was developed in 2005. Technology has changed a lot since then and it might not be the best choice in today's fast paced, highly mobile world.

OpenID Connect and OAuth 2.0

With the onset of the exponential growth of apps and the API economy, OpenID Connect and OAuth 2.0 are becoming the new federation standard. OAuth 2.0 is an open standard authorization framework designed to support a variety of use cases. OpenID Connect sits on top of the OAuth 2.0 framework to provide authentication. Together, OAuth and OpenID Connect take a different approach to federation than SAML. They work together to provide identity and access management using scopes and claims to support a wider variety of deployment models, user experiences, and devices. You can learn more about OpenID Connect at **www.okta.com/openid-connect**. To discover how to connect enterprise identities using OpenID Connect with Okta, visit the **Authentication Guide**.



Pre-built Identity providers

In a recent study, 77 percent of IT professionals surveyed indicated that the ability to create custom identity providers as well as the desire for pre-built identity providers was equally balanced. As such, in addition to facilitating the creation of custom identity providers, Okta provides pre-built identity providers for the most common enterprise business providers, making it fast and easy to integrate with Google and Microsoft out of the box.

For more information, visit our Social Login documentation page.

Directory integrations

Many organizations have made significant investments into on-premises identity solutions with deep integrations that pre-date many of today's cloud applications. These organizations don't have to abandon their investments or integrations to move to the cloud. Tying into either their Active Directory or LDAP on-premises identity stack, Okta provides directory integrations that enable organizations to take advantage of legacy solutions in a hybrid on-premises and cloud deployment model. So, as you look to integrate enterprise identities in your enterprise customer and partner relationships, these directory integrations from Okta allow your customers and partners to take advantage of your cloud offering even if they need to or want to continue using their on-premises identity systems.

For more information, visit our Supported Directory integrations documentation page.

Multi tenancy

As software companies and service providers move to the cloud, they are faced with the challenge of building SSO into their products and services, as well as building identity connections with their business partners and business customers. Building those connections and authentication capabilities take time and expertise, which delays their ability to deliver the core services and valueadded features with the immediacy that their customers demand. That's why many of these businesses turn to Okta. Using Okta and the Okta API's automated tenant creation functionality, software and service providers can use Okta as their identity layer and give their customers access to their own Okta tenant, while still retaining control via ID federation.

User Model Use Cases

As previously discussed, organizations deal with a variety of user models when trying to integrate enterprise IDs. In both B2B and B2C relationships, Okta has simplified this effort for a broad spectrum of organizations across all these different types of user scenarios.

Customer and employee use case

Bazaarvoice has 750 employees accessing a suite of internal and external applications, more than 590 million shoppers who use Bazaarvoice apps each month to speak to brands, and 10,000 client users in 80 countries who log into Bazaarvoice apps to capture consumergenerated content. Okta makes sure Bazaarvoice employees get access to the applications they need, while giving its application developers an identity and authentication platform they can leverage when building client applications.

Read the full story at **www.okta.com/customers/bazaarvoice**.

Customer, partner, and employee use case

As a global manufacturing firm, Flex has about 200,000 employees connected to cloud and on-premises apps, thousands of suppliers with fluctuating access to its supply chain, and more than 100 factories connected to its supply chain, customers, and company. Okta provides Flex a unified identity platform that secures its supply chain for its partner and business customers, while connecting its employees with the apps they need.

Read the full story at **www.okta.com/customers/flex**

> “Okta plays a role in all three of my initiatives: Cyber security, business productivity, and best of breed. It fits all three, so it’s a perfect match.
>
> Gus Shahin
> CIO, Flex

SaaS to multi-customer use case

Adobe uses Okta as its authentication layer for both internal employees and for its Adobe Creative Cloud suite of software. That translates into more than 20,000 Adobe employees using Okta for SSO into 300 enterprise apps, as well as thousands of Adobe's business customers using Okta to access the Adobe Creative Cloud suite of products.

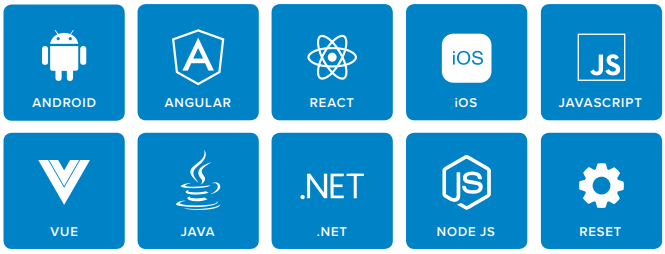
Read the full story at **www.okta.com/customers/adobe-systems**

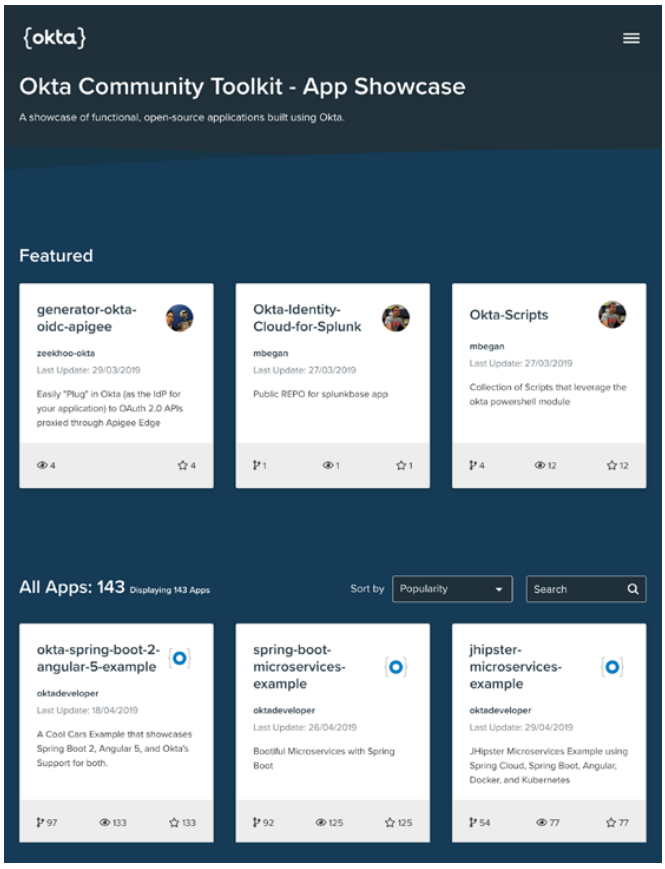
> I don't want to reinvent the wheel in our identity stack. I want to use what's best in class in the market and then apply the Adobe specific requirements to that stack to get something out to our customers really quickly.
>
> Scott Castle
> Adobe Creative Cloud, Product Manager, Adobe

Facilitating Authentication and Identity Integration

Okta provides a wide variety of SDK's to help organizations quickly take advantage of the power of the Okta Identity Cloud platform to securely connect businesses and people to the technologies they need. Okta provides a wide range of SDKs to help you get started in your preferred language, while the Okta Toolkit provides community generated code and solutions that have helped thousands of enterprises take advantage of Okta and its highly secure, global redundant infrastructure. The Okta SDKs and Okta Toolkit can be accessed at **toolkit.okta.com**.

In addition to its SDKs, organizations can take advantage of Okta services directly through its API and the new API endpoint enhancements that Okta continues to provide. Using the API, organizations can script the entire authentication process behind their normal login pages. This includes being able to custom build admin pages or self-service portals that organizations can use to allow partners to connect with the organization without manual intervention from a support team.





Simplify ID Integration and Grow Your Business Faster

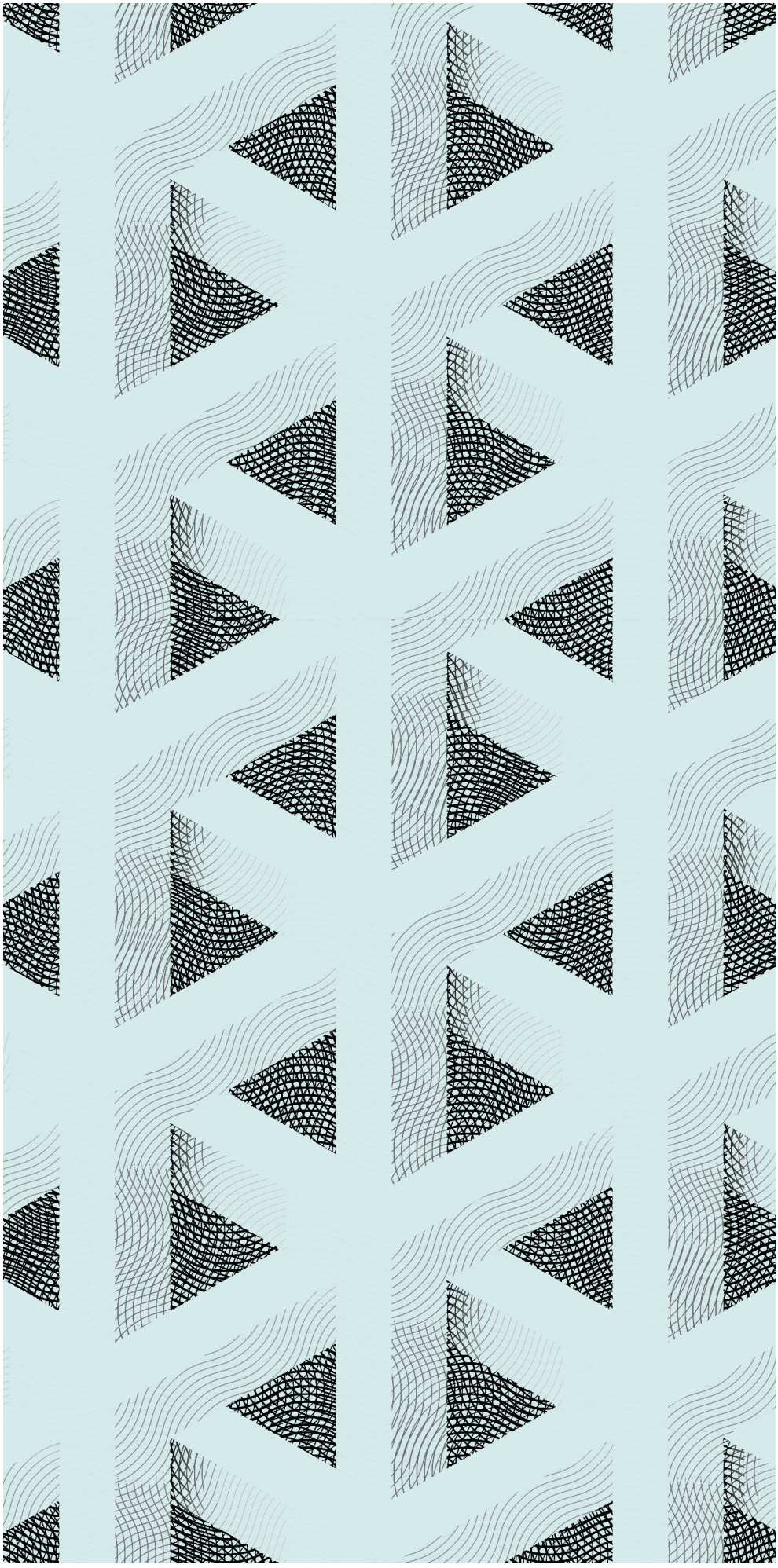
Today's expanding partner economy requires the ability to integrate with other identity providers, while meeting customer expectations for secure and easy to use applications. But building identity integrations to connect with enterprise partners and customers is a complicated and difficult endeavor that shouldn't distract your valuable development resources from focusing on the development of services and features that grow your business and meet customer demand. Okta lets you leverage its identity expertise and services, so you can focus on what matters most to your business.

With Okta serving as the identity layer for your infrastructure stack, you can free up your resources to focus your development efforts and resources on your business initiatives, while fully addressing the needs of your partners and customers. Okta's Customer Identity solutions give you the tools and services you need to not only simplify enterprise identity integration, but its futureproof approach and ongoing innovations will give you the agility to evolve your product security and customer experience as world and market forces evolve.

To take advantage of Okta or learn more about how it simplifies enterprise ID integration, visit **our B2B Integration page**. To get started with a free trial, visit **developer.okta.com**.

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 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit **okta.com**.



okta