Whitepaper

# Okta for global, distributed organizations

The world's largest organizations can leverage a hub-and-spoke identity model to deliver a combination of agility and flexibility without sacrificing security and efficiency.

# Table of Contents

# Manage services across global organizations and diverse business units

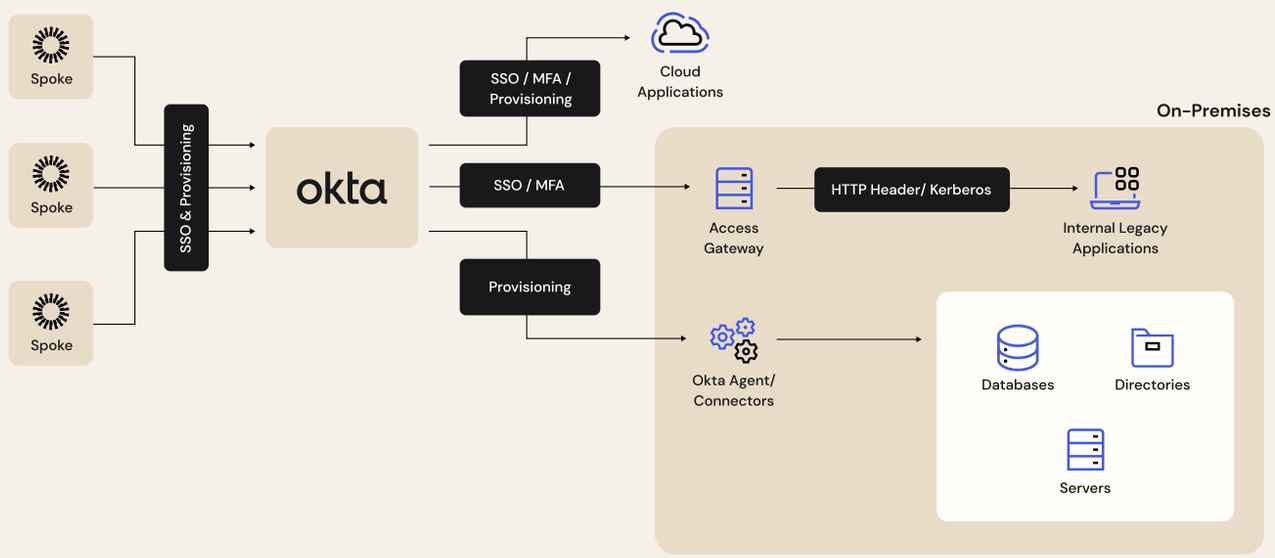
For large, complex organizations, centralizing aspects of identity can be extremely challenging. Business units, subsidiaries, and regional entities often operate independently, making their own decisions and managing their own technology and user bases. Multinational organizations must adhere to regulatory requirements related to data residency, and the ambitious goal of a centralized identity can seem impossible given the need to store personally identifiable information (PII) within each respective country. Finally, organizations looking to augment their capabilities for either the short term (i.e. seasonally) or for the long term (including M&A) have challenges centralizing identities originating from outside of their organization.

A 'hub-and-spoke' identity model can serve as the foundation for unified services and centralized visibility across an entire organization, while allowing for specific application and user management flexibility across distributed information technology (IT) organizations. Enter, Okta for Global 2000. There are a number of real world use cases for how this hub-and-spoke model can be leveraged to improve agility and flexibility without sacrificing security and efficiency, with deployment models for:

- Large organizations with multiple business units
- Multinational organizations with data residency
- Third-party (including contractor) outsourcing
- Integration for mergers and acquisitions

# Manage organizational complexity with Okta for Global 2000

Okta's hub-and-spoke model enables organizations to physically and logically separate a collection of identities from one another through the use of multiple Okta tenants (also referred to as Okta Orgs). The flexibility this model provides allows organizations to address complex use cases typically driven by business, technical, and/or compliance requirements. Through the use of the Okta Integration Network's (OIN) Org2Org connector, multiple Okta orgs can be integrated together to enable both single sign-on (SSO) and provisioning within a matter of minutes.




Okta hub and spoke architecture model

In this architecture, the hub-and-spoke functions as the following:

**Hub**

A single Okta Org, acting as a hub, operates as an independent service provider (SP) to the spoke(s), and is responsible for providing directory services, authentication, and authorization services in a centralized manner. The hub then uses common identity standards to act as an identity provider (IdP) and integrate with downstream applications to provide seamless and secure access from an SSO (e.g. using SAML, WS-Federation, and OpenID Connect) and provisioning (e.g. using SCIM) perspective.

**Spoke**

One or more Okta Orgs, acting as individual spokes, operate as independent IdPs responsible for providing directory services, authentication, and authorization services. While these responsibilities are identical to the hub, the spokes provide these capabilities in a decentralized manner for users within each spoke. Spokes utilize their own instance of Okta's Universal Directory and store user profile and group information which can be created directly in Okta (i.e. Okta as the source of truth) or sourced from any other repository such as Active Directory, LDAP, or HR information systems.

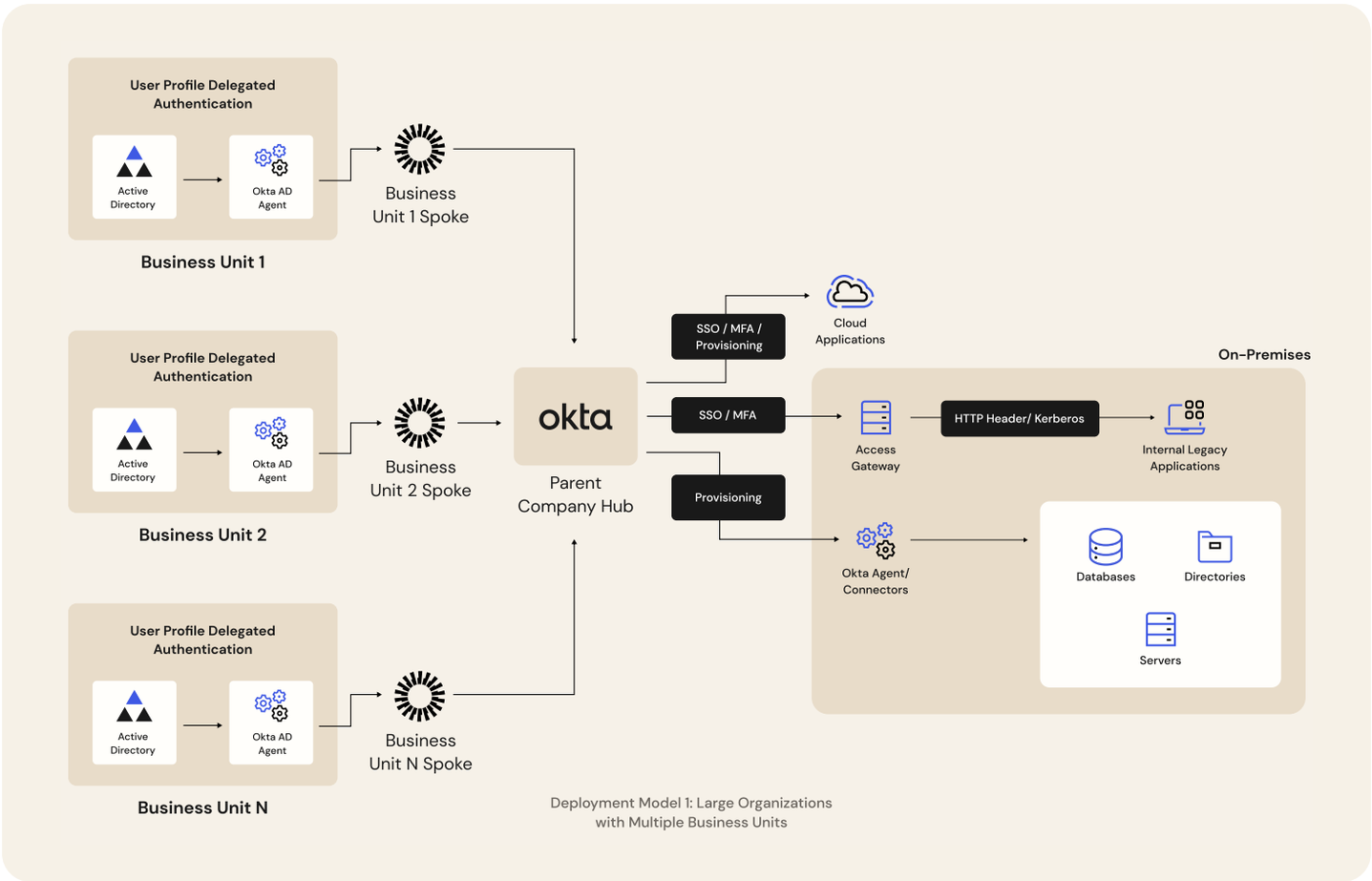
The spoke(s), leveraging the Okta Integration Network's (OIN) Org2Org connector, will provide seamless and secure access by provisioning user profiles into the hub as well as enabling SSO to any applications or services integrated with the hub. Using Okta Workflows, Okta for Global 2000 can solve complex identity management challenges with automation carried out across hub-and-spoke architectures. This model can be used in a variety of scenarios for organizations that manage both internal employees as well as external user identities.

# Increase agility with flexible deployment models

Okta for Global 2000 allows large organizations to increase agility, efficiency, and security by enabling leaders to balance flexibility and autonomy with centralized resource management. Okta's flexible deployment models allow businesses to reduce complexity and increase agility across a number of use cases.

**Deployment model 1: large organizations with multiple business units**
Large organizations can consist of numerous independently managed business units, which can make their own decisions around the selection of various technology solutions and may also have their own personnel responsible for managing these IT investments and user lifecycles. While these business units operate independently, parent organizations looking to lower overall cost and improve efficiency across the entire organization may offer various technology services and platforms to all business units through a shared services model. Enabling these independent business units to participate in a shared services model for various applications and platforms while not requiring them to relinquish their independence can be a difficult challenge both organizationally and from a technology perspective.

As depicted in the following diagram, by leveraging the Okta for Global 2000 with a hub-and-spoke architecture, the Parent Company (i.e. hub) is able to centralize various applications and platform services, both on premises and cloud-based, without disrupting the individual business units or requiring them to relinquish any control of their existing user repositories and technology investments. Individual business units will utilize their existing Active Directory user repository, which they manage themselves, to not only provide access to their applications via the spoke, but to also enable access to applications provided by the hub in a shared services model. Business Unit users will access all applications, including applications provided by the hub, in a seamless and secure manner (i.e. SSO) and continue to authenticate using their existing Active Directory credentials. Finally, the hub can provision user access to downstream applications and user repositories where appropriate.




Deployment Model 1: Large Organizations with Multiple Business Units

NTT DATA

**NTT DATA automates provisioning while enhancing security**

A top priority for NTT has always been security. For large organizations like NTT, workforce turnover and role changes add to the pain of manual provisioning tasks that not only drain IT resources, but risk security vulnerabilities through orphaned accounts and credentials.

To address this, NTT DATA's hub-and-spoke model manages its 140K+ employees — some of whom with the same names — to keep each person's information, logins, and apps organized. NTT adopted the Okta Workforce Identity Cloud to automate provisioning tasks and allow each company to remain connected, yet operate autonomously. One of NTT's goals was for every employee to have the same NTT branded email. Behind the scenes, the central identity hub knows every identity ever created across the 900+ companies and has created a branding suffix to ensure that no one person can crash or collide with another identity across the different spokes.

Okta enables NTT to have one single provisioning point where it can provision everything in its central hub and then connect to every office — keeping all of NTT's organizations aligned, while still allowing them to operate as individual entities. Additionally, NTT's IT teams now have a clean graphical user interface to seamlessly combine custom actions across applications and within specific time frames to enhance security and efficiency within the enterprise.

**Deployment model 2: multinational organizations with data residency**

Governments have become more involved in the protection of individuals' data privacy through the passage of various laws and regulations. These protections are afforded to citizens who may be employees, partners, and/or customers of an organization. In addition, many of these laws and regulations can vary by country and oftentimes require that the personally identifiable information (PII) of a citizen reside within their respective country (i.e. data residency requirements). Managing and governing identities and delivering applications and services to distributed and heterogeneous workforces in this highly complex regulatory environment poses significant challenges for multinational organizations, often leading to compliance challenges, lost productivity, and manual processes stretched across siloed environments.

By leveraging Okta for Global 2000, a hub is able to deliver various applications and platform services, while ensuring that PII remains persistently stored only within the users' appropriate region (i.e. spoke) and conforms to data residency requirements for employees, customers, and/or partners.

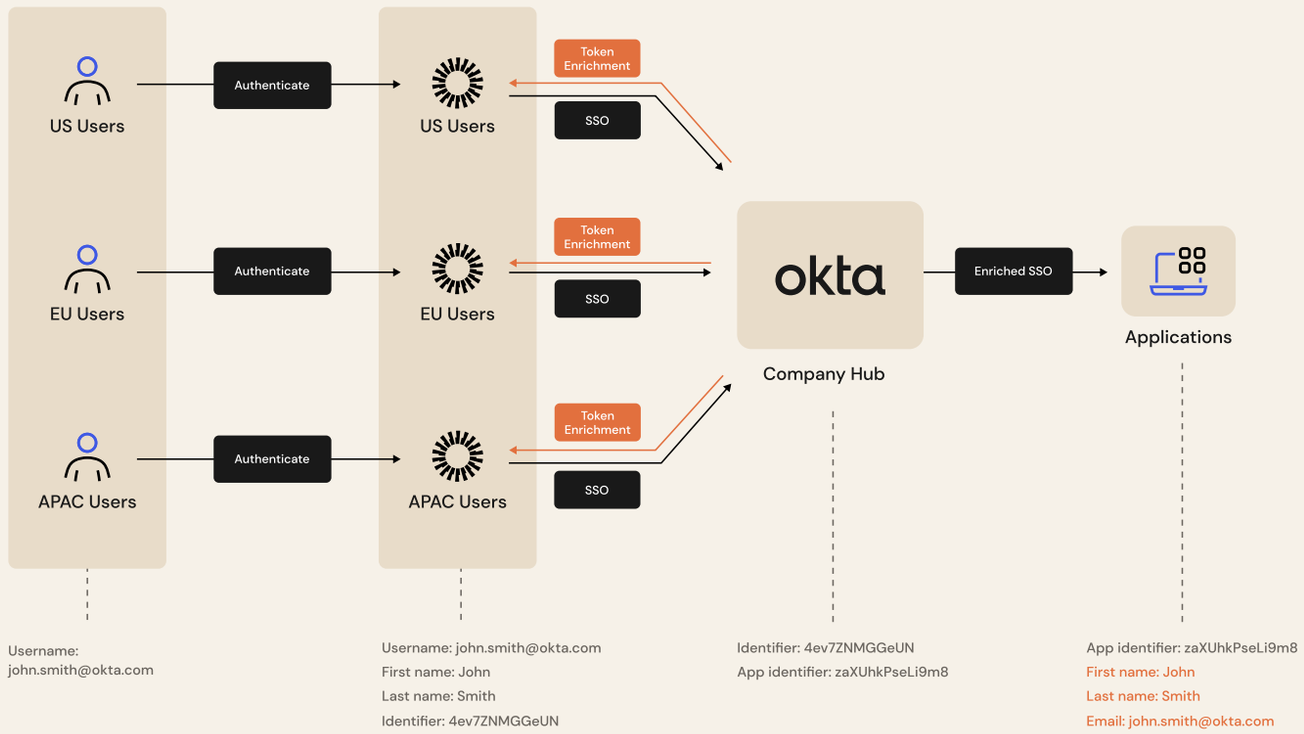
Each region (US, EU, and APAC) will employ its own spoke located in its respective region to persistently store user profile information including PII and adhere to data residency requirements. These regional spokes will store user profile information containing PII that was created either directly in their spoke (i.e. Okta Sourced) or sourced from other repositories such as Active Directory, LDAP, or HR applications (depending on the type of user).

**Maintaining privacy**

In addition to storing user profile information which contains PII, regional spokes will also store a unique identifier for each user profile. This unique identifier will be constructed without containing any PII and be used as a referenceable key when creating persistent identities outside of the region as well as during runtime when users access applications (i.e. SSO). Leveraging this unique identifier will ensure that both user privacy and adherence to data residency requirements are maintained. Additionally, if downstream applications integrated with the hub require PII at runtime (i.e. during user access via SSO), Okta's powerful Hooks capability can be utilized at the hub to enrich identity tokens with PII stored at the spoke. These enriched tokens are then passed to the downstream applications.

It is important to note that use of the Okta Hooks functionality will not result in the persistent storage of PII at the hub and that the PII is purely transient in nature. That being said, applications that utilize the enriched token, which contains PII, must only utilize the information during the user's session at runtime.

Applications must not persistently store the PII (e.g. database storage) as this would not conform to privacy and data residency requirements.




Deployment Model 2: Multinational Organizations with Data Residency

**Deployment model 3: third-party (including contractor) outsourcing**

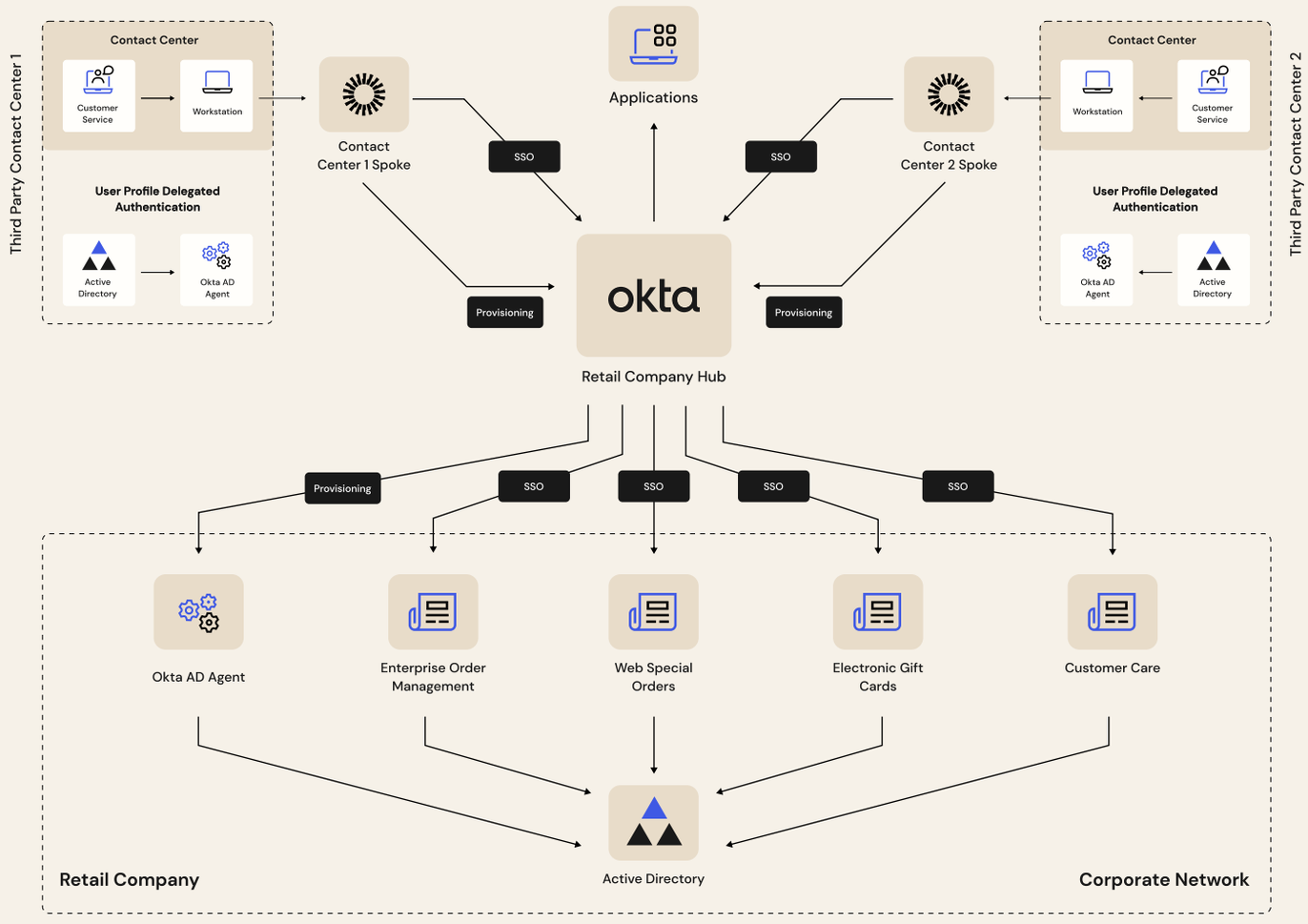
Many organizations outsource business functions (e.g. call center outsourcing) for various reasons such as increased efficiency, lower cost, or to elastically scale their business during high demand (seasonal) peaks. Organizations looking to provide outsourced personnel with seamless and secure access to applications and services that have been traditionally architected for employee use only can pose unique technology and security challenges.

By leveraging Okta for Global 2000, a Company (i.e. hub) is able to deliver various applications and platform services, both on premises and cloud-based, to outsourced personnel.

Each third-party outsourcing organization will leverage their existing Active Directory user repository and Okta spoke, which they could either manage themselves or use their own IdP to federate into the spoke. Third-party outsourcing organizations will access applications and platform services provided by the hub, in a seamless and secure manner, from both an SSO and provisioning perspective. In addition, outsourced personnel will continue to authenticate using their existing Active Directory credentials. Finally, the hub can provision user access to downstream applications and user repositories where appropriate.

It is important to note that while the company is relying on the third-party outsourcing organization to properly manage their personnel in Active Directory to ensure appropriate access, the company can still enforce its own security policies within the hub related to access through the use of Okta groups and group membership rules. The use of multi-factor authentication via Okta sign-on policies can also be implemented via the hub to add an additional level of security if required. In the event of an emergency situation where immediate termination of an individual's access is required, the company can suspend or deactivate the user access immediately within the hub without requiring any assistance from the third-party outsourcing organization, their Active Directory, or their spoke.

Finally, if the outsourcing partnership is terminated, the company (i.e. hub) can disconnect a spoke and immediately terminate all access for users of that spoke.




Deployment Model 3: Third-Party (Including Contractor) Outsourcing


**Dick's Sporting Goods seamlessly ramps up its seasonal workforce**

Dick's Sporting Goods — the largest omni-channel sporting goods retailer in the US — has a seasonal workforce that relies on outside contractors. During the winter holiday months, the organization grows from four customer call centers to nine.

As a result, its IT team needs to onboard all new agents in less than a month, and deprovision them in half that time after the holidays. This manual onboarding required an additional 1.5 full-time employees, prompting the organization to look for a more efficient and affordable way to grant new teammates the tools they needed to succeed.

Okta's hub-and-spoke approach provided the solution they were looking for. Each of their Business Process Outsourcing (BPO) partners each manage their own Okta spoke, which then connects into the Dick's Sporting Goods hub. From there, the Dick's Sporting Goods team has the ability to provision the call center, internal applications, order management, web special orders, gift cards, etc. The Dick's Sporting Goods team also gives BPO partners access to external applications that require authentication, such as carriers, fulfillment partners, etc. — and all via a repeatable process that can be used with multiple BPOs.

Since implementing Okta, the company has significantly reduced its licensing costs and sped up its holiday ramp-up time.

"Our Okta integrations have driven value into our customer service operations. With our existing and any new BPO partners, the ownership of identity becomes our partner's responsibility. This is a game changer for our IT support, and business operations teams. Our agent teammates have simplified access to our tools, as well as self-service password resets,"

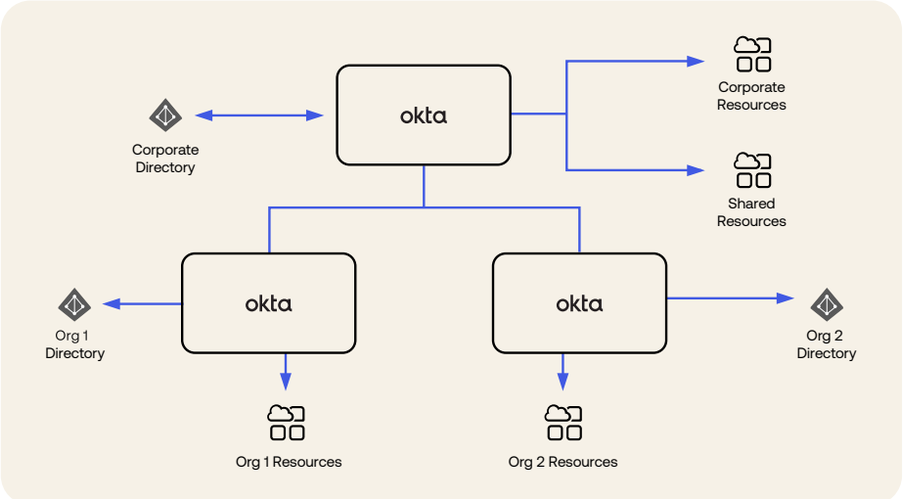
**Eva Sciulli**
IT Product Manager for Customer Interaction
Dick's Sporting Goods

**Deployment model 4: integration for mergers and acquisitions**

Mergers and acquisitions (M&A) are a key growth lever for businesses, and smooth technology integration is integral to accelerating value. As the common layer between the technology and human change associated with M&A, identity can help improve the success and velocity of M&A integrations by creating a single source of truth for identities, providing users with access to critical apps on Day 1, and standardizing security policies.

As depicted in the architecture diagram below, Okta enables user and group syncing from any source, making it easy to provide new employees with the right level of access to applications in the parent company's Okta Org on day one, whether the acquired company uses Active Directory, LDAP, Okta, or a different IdP. With a hub-and-spoke architecture, these users can subsequently be managed in the parent company's Okta Org or in the acquired company's directory, then synced to the parent Okta Org to access shared resources.

To boost productivity and security among new employees, authentication can be delegated to the acquired company to give users a seamless login experience that doesn't require them to reset usernames or passwords, but enforces the parent company's security policies for apps in the hub org. Finally, attribute-level sourcing allows the parent company to specify different sources for individual user attributes, to control attributes that are required for shared app provisioning without overriding the attributes in the acquired company's directory.



Okta for Global 2000 and its unique hub-and-spoke model enables organizations to provide centralized identity services across the organization while offering the flexibility and distributed autonomy required for large organizations. In doing so, organizations can simplify and automate complex lifecycle management processes while delivering seamless, secure access to technologies for their entire extended workforce.

For more information on Okta for Global 2000 and how architecting a hub-and-spoke model for your use case can improve your organizational agility, visit: https://www.okta.com/products/global-2000/