Okta Identity Management for SharePoint Server

Extend SharePoint to All Your Users

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Contents

Executive Summary

Okta is an enterprise grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. With Okta, IT can manage access across any application, person or device. Okta's service includes complete authentication and user management for Microsoft SharePoint Server 2010 and 2013. The integrated solution allows enterprises to more seamlessly and securely collaborate with their customers and partners using the on-premises version of SharePoint in combination with Okta's cloud-based identity management service.

The integration enables IT administrators to manage customer or partner access to SharePoint with Okta in much the same way they would use Active Directory to manage employee access to an internal SharePoint-based portal. This hybrid architecture allows IT to leverage existing investments in SharePoint, and to simply and securely extend access to users outside of the company. There are no more security risks associated with adding non-employees to a corporate directory, and Okta's cloud-native architecture means there is no need to install, configure or maintain an additional on-premises directory.

Okta allows enterprises to allow all their users to access SharePoint sites and portals, whether they are customers, partners or even employees across disparate organizations.

Okta: A Platform for Cloud Identity and Access Management

Okta is an on-demand identity and access management service that provides single sign-on (SSO), user management, and analytics across cloud applications and on premises web applications from any device and for any user. Okta also operates as a federation service provider, serving as the identity layer for web applications. Enterprises use Okta to manage access for multiple types of internal and external users as they use more cloud applications. ISVs and developers use Okta to handle all the identity needs of their websites or cloud services.

Websites and Portals on SharePoint Server: Overview and Challenges

Microsoft SharePoint Server is on-premises software that provides a flexible platform for content management and collaboration. SharePoint Server 2013 is the 6th major version of the product that was initially released in 2001. Enterprises can extend the generic concept of a "site" in SharePoint to build portals that provide users with a central place to access a variety of resources, or even to create entire websites. This flexibility gives enterprises a powerful toolkit, providing a quick way for organizations to give employees access to company resources, partners access to applications for collaboration or for building an external web presence for customers.

While the flexibility of SharePoint provides a useful toolkit, enterprises often find that managing identity and access for a SharePoint portal can present a number of challenges:

- Single Sign-On and Provisioning: SharePoint can be used to build a landing page that provides access into other cloud or on-premises applications. In this scenario, users still need to be authenticated into the "behind-the-scenes" applications, and likely provisioned into those applications as well. This can be difficult and costly integration work.
- Maintaining External User Credentials and Profiles: SharePoint by default can easily connect to Active Directory, which most enterprises use for authenticating employees and storing their profiles. However, if an organization wants to provide access to external users, it would need to either mix those in with their employee database or stand up an additional user database. Those options incur additional costs and management overhead.
- B2B Federation and Social Authentication: Many enterprises want to manage external users by organization, and allow their customers or partners to use their own organization's identity system to authenticate. In addition, some businesses may want to allow users to authenticate to their site using a popular social identity. These are advanced B2B and consumer federation features not easily supported in SharePoint.
- Access for Independent Business Groups: Enterprises that have gone through mergers and acquisitions or operate a franchise model, often have groups within the company that maintain autonomy, sometimes with their own directory infrastructure. This can be a challenge if the IT organization is trying to roll out enterprise-wide shared services, including a central SharePoint portal.

Increasing the ROI from SharePoint Server with Okta

Okta provides a broad set of functionality to address the user management, single sign-on, and reporting needs ideal for enterprises using SharePoint in a heterogeneous environment.

Single Sign-On and Provisioning

This business issue for external portals starts with an enterprise, for example, a printer company that wants to provide a mix of marketing, sales, and support functionality online within a single portal to its customers and partners. Customers can open support tickets, look up answers to commonly asked questions, and download manuals and software updates. Additionally, partners can use the portal to access partner marketing materials and register deals for special discounts. To both customers and partners, this portal should look like the printer company's own web application. But behind the scenes, administrators selected several different applications and platforms to manage these tasks. They chose SharePoint Server for content management; Jive for customer communities; a shipping company's proprietary application to handle all returns; and a set of custom built ASP.NET apps for specific business functions.

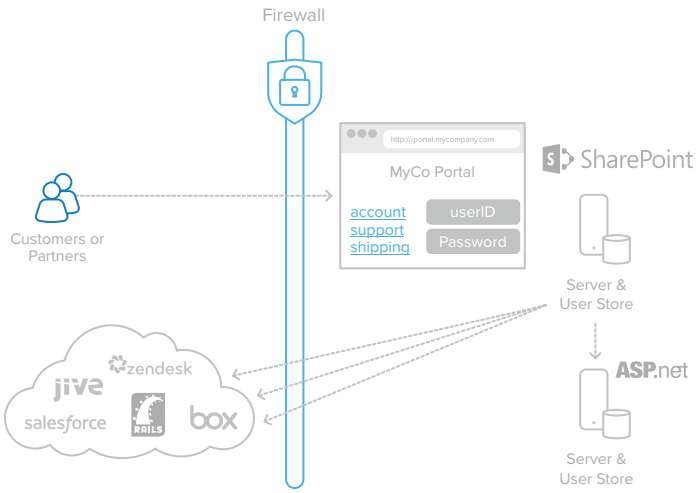

Figure 1: SharePoint site as a landing page for other behind-the-scenes web apps

While each of those components provide the best features and user experience for their specific function, there are several challenges associated with the disjointed approach represented in Figure 1:

- The user experience is not seamless—different logins are often needed for different sections of the portal.
- Users must register separately for each section, complicating the user experience.
- Separate user stores proliferate and become difficult for the IT team to manage.

Solving this problem with custom software development is difficult, time-consuming, and potentially very expensive. Okta's identity management service solves these problems by organizations to present a single, well-integrated web application to all customers and partners, who can navigate it with a single set of credentials (see Figure 2). Centralized registration can be automated, and users log in only once. Okta also allows users to be easily provisioned and de-provisioned in the target applications. Upon login, customers and partners can be routed to a single landing page, from which they can navigate to any allowed application with no additional hurdles.

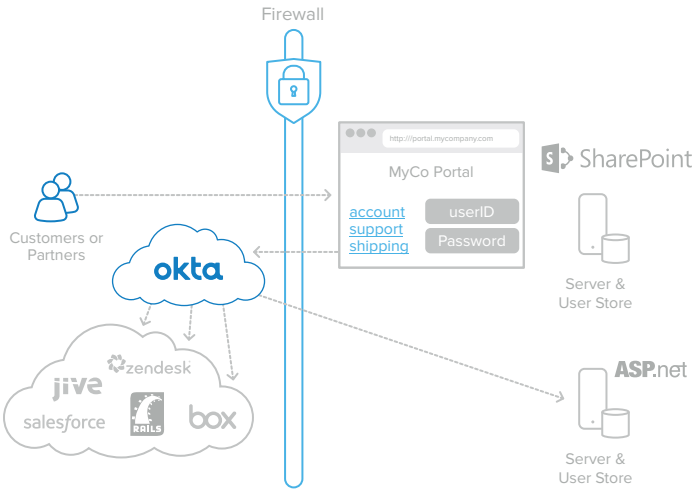

Figure 2: Customer portal simplified and improved with Okta

With Okta, organizations can quickly and easily automate all portal user management functionality and provide customers and partners with a seamless experience—all with a 100-percent on-demand, secure, highly available service.

Managing External Users, B2B Federation and Social Authentication

By leveraging Okta as the identity layer for your SharePoint portal, you also tap into Okta's broad functionality as a federation service provider and a cloud directory. With Okta, your options for authenticating users are greatly increased.

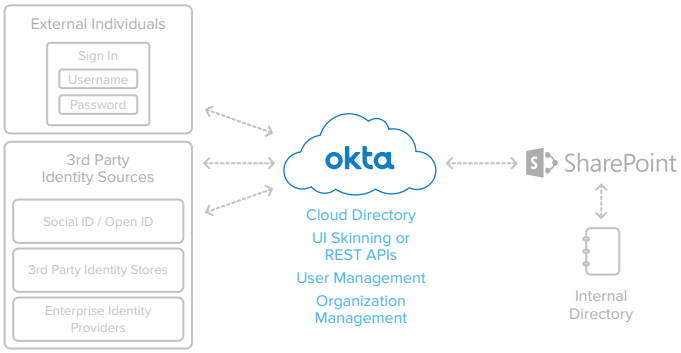

Figure 3: Okta as a Federation Service Provider for a SharePoint site or portal

Okta has a built-in cloud directory at the core of its architecture. This allows you to use Okta to manage users you do not want to store with all your employees in Active Directory. In addition, Okta can accept inbound federation from 3rd party identity sources, such as a partner's identity system or an application with outbound SAML functionality such as Salesforce.com.

Okta takes this one step further than most federation solutions, providing the option to integrate directly to a partner or customer user store, such as their AD or LDAP. Okta's directory integration is very lightweight, and only requires the installation of an agent on any windows server that has read access to the domain controller. It does not require any firewall changes. This makes it very easy and secure for you to provide single sign-on for your customers or partners using their own enterprise identities.

For consumer websites or in B2B cases where you want to make it easy for users to sign up for access, you can also use Okta to enable social authentication from popular social or consumer services.

Access for Independent Business Groups

Many larger enterprises that have gone through mergers and acquisitions have complex

identity architectures. They may have business units that maintain autonomy, and want to control their own employee directories. Or, there may be a desire to integrate all identity systems, but a directory consolidation project would be time consuming and costly.

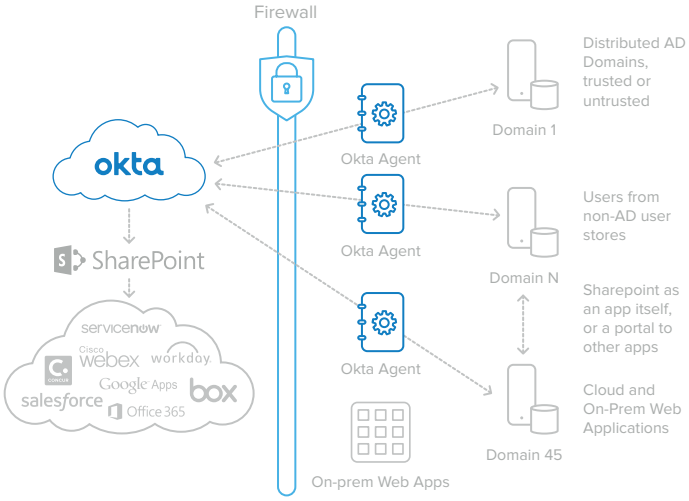

Figure 4: Using Okta to provide access to shared services for all user silos in an enterprise

Enterprises in this situation are held back from being able to offer shared IT services across their organization. Some may resort to having multiple subscriptions to cloud software, or multiple implementations of on-premises systems such as SharePoint, in order to serve all users. Other organizations may just choose to limit the scope of a SharePoint portal to only a subset of users within the organization.

Okta can solve this problem, allowing enterprises to roll out a portal on a platform such as SharePoint, and easily provide access to the entire organization, across multiple business units and silos.

Okta as the Identity Layer for your Website, Portal or Cloud Service

Okta can be used as the identity layer for a broad spectrum of external sites, such as consumer websites, B2B portals or SaaS applications. Okta is designed to provide a breadth of options for connecting people to applications; therefore it can be used as an identity provider and as a federation service provider for your applications.

As a cloud identity service that sits outside of your firewall and includes a cloud directory, Okta provides an elegant solution for situations where users and many of the applications they access are outside your corporate firewall. Okta can manage the identity of customers, partners, contractors or other non-employees connecting to a hybrid of cloud applications and custom applications that are external facing.

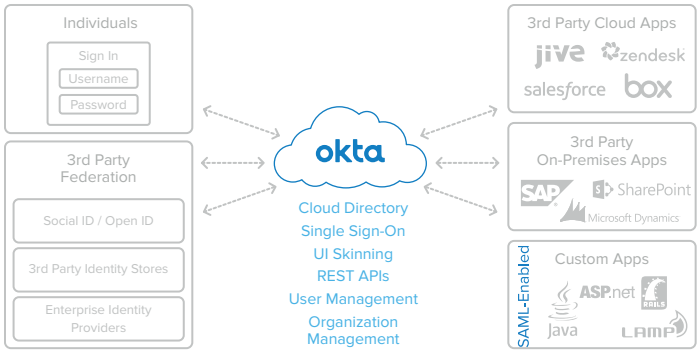

Figure 5: Okta provides a comprehensive identity layer for your external sites and applications

A Flexible Cloud Directory

Okta's service contains a native cloud user store, which allows customer, partner, and employee identities to be centralized in a single location. The native cloud user store can operate independently from, or in combination with, external directory services, including Active Directory. User profiles and their associated properties can originate in Okta and be managed from Okta, or they can be mastered from a variety of external sources.

For example, an organization may have a set of internal employees that needs access to its portal and whose identities are managed in Active Directory. Okta could leverage AD to authenticate internal employees who access the portal applications, but customer and partner user accounts could be managed natively in Okta, eliminating the need for yet another directory. Okta can also manage customer and partner accounts in an existing corporate directory.

Automated User Registration and Application User Management

If using SharePoint as an entry point for access to other applications, Okta can automate user registration and provisioning. SharePoint portal users only need to register once; accounts are then automatically created in each behind-the-scene web application using Okta's user management capabilities.

Application specific user properties such as group membership, role, or profile can be set based on rules associated with the Okta user profile and automatically pushed into the behind-the-scenes applications.

With Okta, portal users only need to register once; accounts are then automatically created in all of the underlying web applications that make up the overall portal, with Okta's user management capabilities.

When administrators add users to the system, Okta supports initial user registration with:

- The Okta administrative interface.
- Bulk import from a CSV file or from an external directory service.
- Programmatic use of Okta's RESTful user management APIs.

Okta's RESTful APIs (https://github.com/okta/api) an be used in conjunction with a custom user registration form built on SharePoint to support completely self-service user provisioning, or they can support required approval workflows.

As a part of the user creation process, Okta can also transform the username format to ensure there are no violations of various cloud applications' username format requirements. In addition, Okta supports application-specific user properties such permission groups, role, or profile can also be set based on rules associated with the Okta user profile.

Attributes of that profile are then pushed into the behind-the-scenes applications as part of the provisioning process.

In addition, you can enable SharePoint to query users in Okta dynamically from the SharePoint "People Picker", allowing SharePoint users or administrators to assign access rights for SharePoint resources to users in Okta's directory. To enable this functionality, all that is required is the installation and configuration on SharePoint Server of a small downloadable module from Okta.

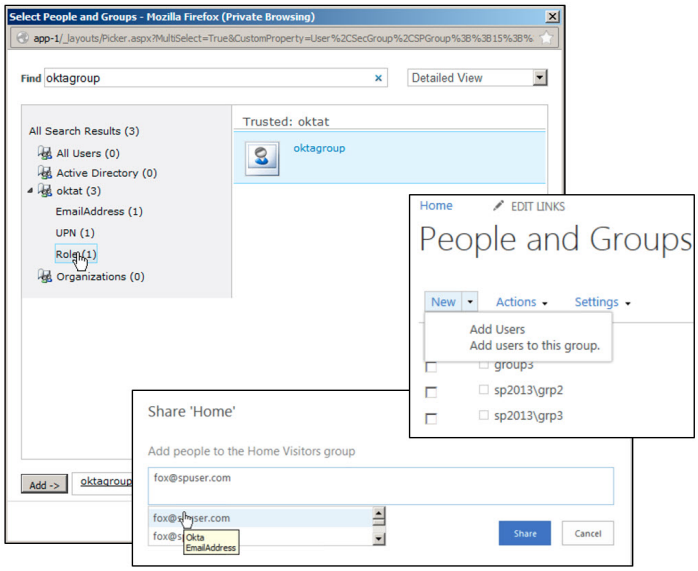

Figure 6: "People Picker" in SharePoint Server 2010 and 2013

Single Sign-On to Any Cloud or Web Application

Okta creates a seamless user experience by providing single sign-on to all of the web applications that make up an organization's portal. Users log in once, and then are passed on to each portion of the portal without having to re-enter credentials.

To provide SSO to all applications, Okta must first establish an authenticated session with the user's browser. Once this session has been established, Okta can authenticate the user to any connected application subject to the access control rules set within

Okta. For SharePoint, Okta uses Microsoft's claims-based identity model. There are multiple ways that the initial Okta session can be created:

- Using the Okta "My Applications" landing page.
- Using Okta's REST APIs within a custom application to authenticate users.
- Using Service Provider Initiated SAML (SP SAML) or WS-Fed with an existing portal.
- By POSTing credentials to the Okta service, then redirecting back to a custom portal page in SharePoint or elsewhere.

Okta's "My Applications" landing page provides a simple launch point to all assigned applications. This option is commonly used when no central portal exists and the requirements for customization are minimal.

Enterprises rolling out an external site to the general public or with high visibility often need complete control over the user experience. For these scenarios, companies can use Okta as a development platform. Okta can authenticate users through its REST APIs (https://github.com/okta/api)

In the SharePoint initiated WS-Fed method, users navigate to a central portal, for example, http://support.acme.com. If they are not already logged in, they are redirected to an Okta login page along with a WS-Fed request, then sent back to the portal with a WS-Fed response after entering their correct username and password. The WS-Fed response transparently logs the user into the portal. At this point, the user has both a portal session and an Okta session that can be used to transparently authenticate to any assigned application (see Figure 6).

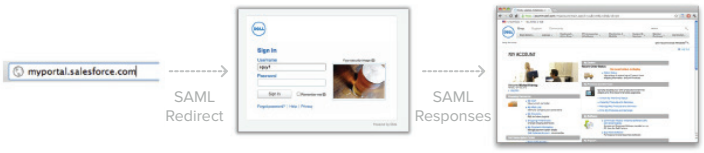

Figure 7: Service Provider Initiated SAML authentication

In the last option, POSTing credentials to Okta, then redirecting back to a custom portal page, users are first presented with an unauthenticated landing page built on the platform of your choice. Typically, the page includes a login widget showing username and password fields. When the user fills these in and clicks "log in", the form is POSTed to Okta where the credentials are validated against Okta's user store. An Okta session is then created and the user is then sent back into the base portal using SAML, WS-Fed or any other supported mechanism.

Figure 8: Form authentication to Okta

Once the Okta session has been established, users can transparently authenticate to any assigned application using a catalog-based or custom SSO integration. Those SSO integrations can either be federated (supporting a standard such as SAML, WS-Fed or another proprietary federated authentication protocol) or leverage Okta's Secure Web Authentication (SWA) to perform a secure, form-driven post to the application login page.

Applications in the Okta Application Network (generally, any commercial application) come pre-integrated for SSO using SAML, WS-Fed or SWA. These integrations are delivered as part of the service and are continually maintained and updated by Okta.

For custom applications that are not in the Okta Application Network, Okta provides integration toolkits to easily enable SAML or WS-Fed, as shown in Figure 5. The SAML integration toolkits are available for a variety of languages including Java and PHP. For ASP.NET apps, Okta provides an easy way to integrate them via WS-Fed. Alternatively, organizations can leverage Okta's SWA to achieve SSO to these applications.

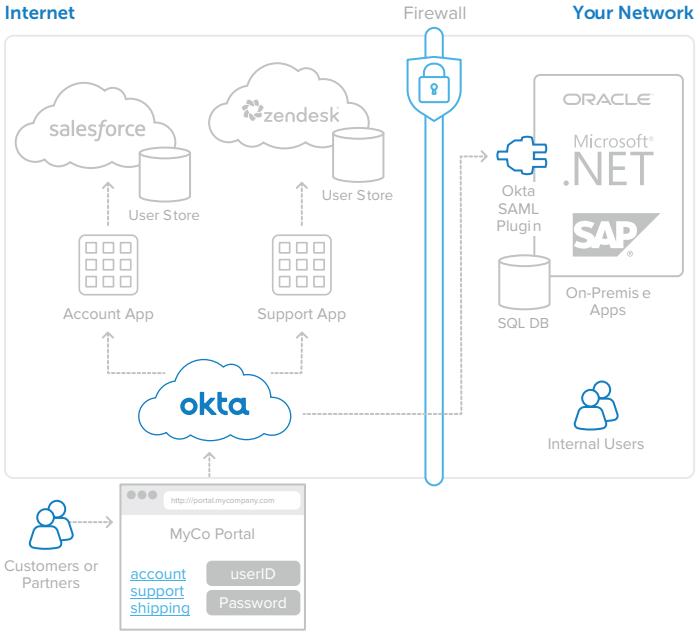

Figure 9: SAML or WS-Fed Integration toolkits for on-premises web applications

With SWA, no programmatic interface or protocols are required. Instead, users are authenticated transparently to the application by its automating the login process SWA only requires that the user account in the target application be provisioned with a known password that can then be stored securely in the Okta service.

Expose On-prem Business Intelligence or SQL Data to Federated Users

Okta's unique integration to SharePoint Server integrates with Microsoft's C2WTS module and is pre-built to translate a WS-Fed claim in SharePoint coming from Okta to a Kerberos token.

This gives you the power to expose on-prem data coming from a source that uses Kerberos to federated users of your SharePoint portal. Many enterprises face this issue as they expose SharePoint to external users that are not behind the firewall and authenticating to an AD domain. With Okta, you can give these federated users access to data on a SharePoint site that comes from sources such as a business intelligence system or a SQL database.

A Platform That Integrates with Existing Identity Management Solutions

Okta can easily integrate with custom-built applications, business processes, and even existing identity management solutions.

Web applications can be SSO-enabled using simple code templates provided by Okta in a variety of languages including Java, ASP.NET, and PHP. In addition, Okta can integrate with an existing on-premises identity management solution.

For example, a single integration between Okta and an existing identity management solution can allow Okta to provide both SSO and user management to all applications already integrated with that identity management solution. Additional cloud and on-premises applications can then be integrated directly with Okta, and the whole collection managed within a single consistent framework.

This solution leverages existing infrastructure investments for fast implementation while providing a consistent user experience across older and newer applications, whether on-premises or in the cloud.

Example: Acme Corp

Acme Corp has developed a set of applications for partners and customers. These apps include:

- A download site built using custom ASP.NET code.
- A partner site with deal registration built on SharePoint.
- A support site built on Jive and Salesforce CRM Customer Portal.

Acme needs to allow access to all of these using a single username and password. Users should register once and be granted access to the appropriate sites based on their profile. User profiles include customers with support contracts, customers without valid support contracts, and resell partners.

Customers with support get access to the download and support sites; unsupported customers get access to the download site only; and partners get access to all three sites. Supported and unsupported customers self-register by filling out a form hosted on an unauthenticated section of the support site. Partners are registered by partner managers via a form hosted on the partner portal.

Architecting the Solution with Okta

Registering and Managing Users

To manage user registration and create user accounts in each of these applications, Okta provides rich user management capabilities. A user can be created via Okta APIs (https://github.com/okta/api) called from the user registration form in the SharePoint customer portal. The API supports setting basic user properties, including contact info and group memberships. For example, Joe Partner is created and added to a group called "partners". The Okta group membership determines which downstream accounts need to be created in the relevant applications. In Joe's case, accounts that can be automated using Okta's user provisioning capabilities need to be created in all four apps. For apps and platforms like Jive and SharePoint, this is enabled through the Okta Application Network and requires no custom code or configuration by the administrator. For SharePoint in particular, Okta's integration with the SharePoint People Picker allows Acme's administrators to easily manage access to different sites.

For the custom ASP.NET application, there are two alternatives. Okta supports WS-Fed as a protocol for federation, which is often easy to configure for applications built on a Microsoft stack. Okta can also call out via a simple REST-based interface to notify the application that a new user needs to be created. The application developer can then process that REST call and add the user to the app's user directory.

Enabling Single Sign-On

To enable SSO between these applications, Okta must be connected to each. For SharePoint, Jive, and Salesforce Customer Portal, administrators can achieve this by selecting the applications from the Okta Application Network following a simple two- to four-step wizard. WS-Fed and SAML are the preferred SSO mechanisms for these cases, but the details and heavy lifting required to establish a trust relationship and assertion bindings are hidden from the Acme.com administrator and delivered as a part of the Okta service.

For SSO to the custom ASP.NET application, Acme.com can use simple WS-Fed template and sample ASP.NET code provided by Okta and designed to be easily inserted into the app using Visual Studio. Once this code has been embedded, Okta can provide SSO into the app transparently in the same way that it does for SharePoint and cloud apps.

Automated Portal SSO and User Management

Once the applications have been enabled for SSO and user management, either with integrations from the Okta Application Network, SAML or WS-Fed templates from Okta, and the user registration has been wired in using Okta's REST APIs, the system is ready to go.

Users can register once and their accounts will be created in all relevant apps. They can seamlessly authenticate to any application and navigate via embedded links to any other app without being prompted for additional credentials. Moreover, if user properties such as email address or group memberships are updated, those properties will be propagated automatically to all relevant applications. The solution is simple to enable, easy to manage, and provides an excellent user experience.

Summary

Okta can help you apply the benefits of your investment in SharePoint Server to all your users. When you integrate Okta to SharePoint, you can enable access to SharePoint from multiple, autonomous business lines, or various groups of external users, with broad flexibility in how those users authenticate.

In addition, Okta can provide a complete identity layer for websites or portals that are built on SharePoint, or use SharePoint as one of many applications. Okta can unify the user experience and provide single sign-on across all external-facing applications. This provides users of your website or portal with an integrated experience, while still allowing you to choose best of breed components for each part of your external site.

Okta's identity and access management service greatly simplifies the creation of external sites and portals for both customers and partners. Okta allows organizations to:

- Provide access to an external site or portal to any type of external user with a variety of options for authentication.
- Choose whether to get their site up and running quickly, using components of Okta's consumer-grade UI, or have complete control of the user experience by using Okta as a development platform.
- Present a single, well-integrated web application to all customers and partners.
- Automate user registration and subsequent provisioning and de-provisioning for the target applications behind a portal.
- Provide customers and partners with a single landing page for login, and with navigation to allowed applications with no additional hurdles.
- Eliminate separate, unsynchronized user stores.

With Okta, organizations can quickly and easily automate all portal user management needs with a 100-percent on-demand, secure, and highly available service.

About Okta

Okta is the foundation for secure connections between people and technology. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security policies. It integrates directly with an organization's existing directories and identity systems, as well as 4,000+ applications. Because Okta runs on an integrated platform, organizations can implement the service quickly at large scale and low total cost. More than 2,500 customers, including Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International and Western Union, trust Okta to help their organizations work faster, boost revenue and stay secure.

For more information, visit us at www.okta.com or follow us on www.okta.com/blog.