A large, light blue abstract graphic dominates the background. It features several overlapping circular and semi-circular shapes. A prominent feature is a large circle on the right side, which is divided vertically into two halves by a white vertical line. The overall design is clean and modern, using a light blue color palette.

An Architectural Overview

Okta Inc.

301 Brannan Street, Suite 300
San Francisco CA, 94107

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

wp-portalarch-012913

Table of Contents

1. Okta: Enterprise Identity, Delivered
1. Customer and Partner Portals: Overview and Challenges
3. Automating Portal Identity Management with Okta
 3. A Flexible Cloud Identity Store
 3. Automated User Registration and Application User Management
 4. Single Sign-On to Any Cloud or Web Application
 6. Integration and Federated Authentication with 3rd Party Portals
 6. A Platform That Integrates with Existing Identity Management Solutions
7. Example: Acme Corp
8. Summary

Okta: Enterprise Identity, Delivered

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. Whether the people are employees, partners or customers or the applications are in the cloud, on premises or on a mobile device, Okta helps IT become more secure, make people more productive, and maintain compliance.

Customer and Partner Portals: Overview and Challenges

Enterprises use portals to manage access to web applications that serve customers and partners. Administrators often create these portals by assembling multiple behind-the-scenes web applications and services to form a complete solution.

For example, a printer company might offer a section of their website where customers can log in to process returns, track shipments, and recycle old printer cartridges. To customers, this portal should look like the printer company's own web application for all of these tasks. But behind the scenes administrators use several different applications to manage these tasks: a CRM application to manage customer account information, a customer support application for trouble tickets, and a shipping company's proprietary application to handle all returns (see Figure 1). Some of these applications can be cloud-based, and some are on-premises.

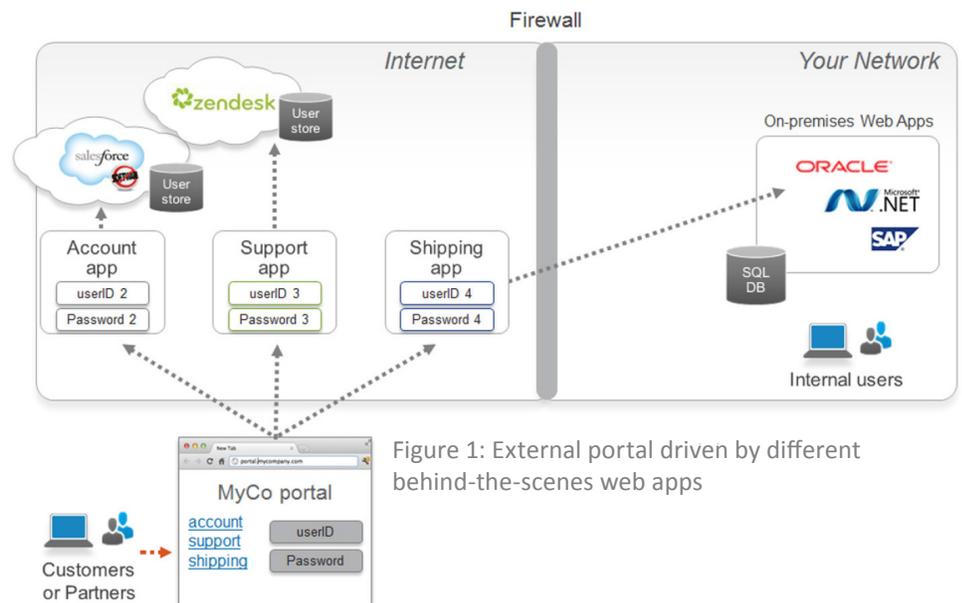


Figure 1: External portal driven by different behind-the-scenes web apps

There are several challenges associated with the disjoint approach 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 allowing 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 and navigate to any allowed application with no additional hurdles.

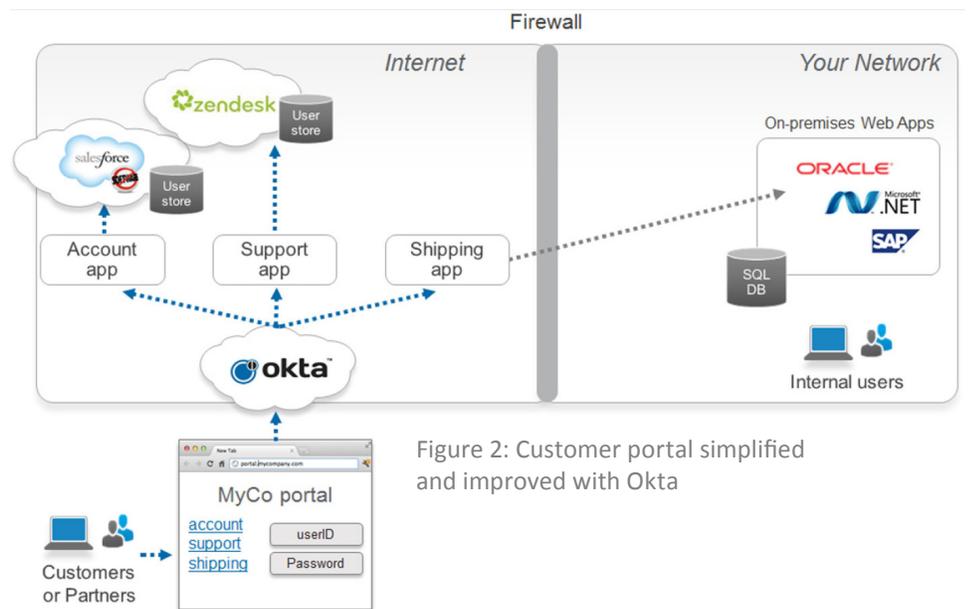


Figure 2: Customer portal simplified and improved with Okta

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.

Automating Portal Identity Management with Okta

Okta provides a broad set of functionality to address the user management, single sign-on, and reporting needs for customer and partner portals.

A Flexible Cloud Identity Store

Okta's service contains a native cloud user store, which allows customer, partner, and employee identities to be centralized into a single location. The native cloud user store can operate independently from, or in combination with, external directory services. 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 or LDAP. Okta could leverage AD or LDAP for the authentication of 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. However, Okta can also manage customer and partner accounts in an existing corporate directory as well.

Automated User Registration and Application User Management

With Okta, portal users only need to register once; accounts are then automatically created in each behind-the-scenes web application with Okta's user management capabilities.

To 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 can be used in conjunction with a custom user registration form 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 user name format to ensure there are no violations of various cloud applications' user name format requirements. For example, if a portion of an organization's portal is based on the Salesforce.com platform, it's possible that a customer or partner that tries to register with that portal already has an existing Salesforce.com account (for example, sally@customer.com). In this case, she would normally be prevented from creating an additional account or registering. Okta solves this problem by applying a transformation for that user and would instead provision her as sally@okta.customer.com to ensure there are no user namespace conflicts with Salesforce.com.

Okta goes even further: application-specific user properties such as group membership, 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.

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. There are two primary ways that the initial Okta session can be created:

- Using the Okta "My Applications" landing page.
- Using Service Provider Initiated SAML (SP SAML) with an existing portal.

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. When the SP SAML method is used:

1. Users navigate to a central portal, for example, <http://support.acme.com>.
2. If they are not already logged in, they are redirected to an Okta login page along with a SAML request, then sent back to the portal with a SAML response after entering their correct user name and password.
3. The SAML response transparently logs the user into the portal.
4. Now the user has both a portal session and an Okta session that can be used to transparently authenticate to any assigned application. See Figure 3 for details.

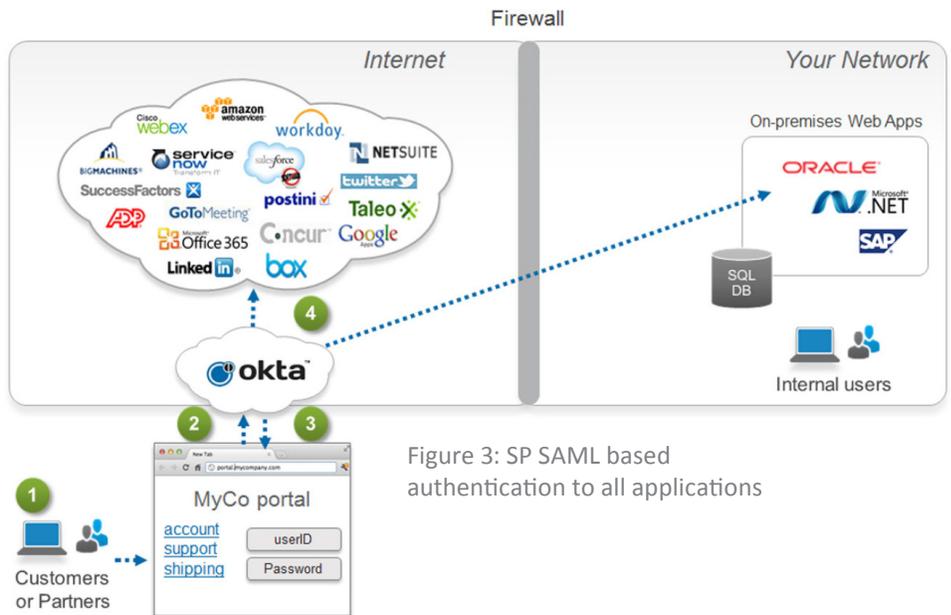


Figure 3: SP SAML based authentication to all applications

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 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 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, as shown in Figure 4. The SAML integration toolkits are available for .NET apps running on IIS, and they support forms authentication and a variety of other languages including Java, and PHP. Alternatively, organizations can leverage Okta's Secure Web Authentication (SWA) to achieve SSO to these applications.

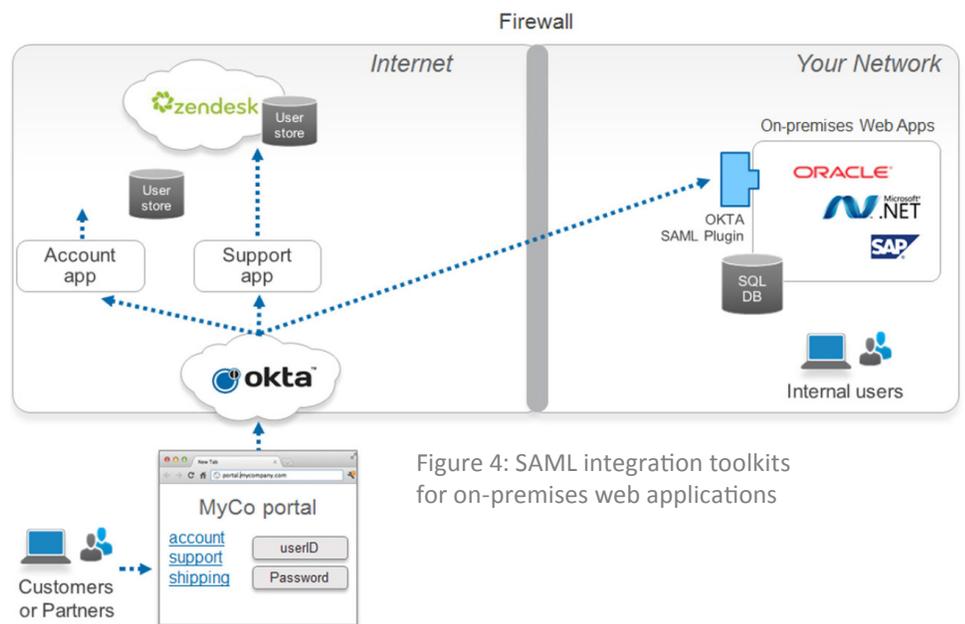


Figure 4: SAML integration toolkits for on-premises web applications

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.

Integration and Federated Authentication with 3rd Party Portals

A common configuration is an “embedded portal”, where your portal is embedded within another application operated by a third party. For example, let’s say you maintain a product configuration portal for your partners. One of your distributors could embed your product configuration portal within their own order processing application, and could then provide a more complete solution. With Okta, that solution is made seamless for the distributor’s employees because they only need to log in once.

A frequent additional requirement for these embedded portals is to allow users who access an embedded portal to do so seamlessly from their own company network, without requiring additional login credentials. Continuing with this example, the employees of the distributor would authenticate once by logging on to their corporate network in the morning; whenever they subsequently access the product configuration tool, they would do so without any additional logins. This seamless access would also require accounts to be automatically provisioned for employees of the distributor.

Okta enables all of this by supporting inbound SAML assertions from another identity provider; these are then used to both provision new accounts and to grant access to the relevant applications that power the portal.

In the example above, employees of the distributor authenticate to their corporate networks as normal, and when they first attempt to access the portal they are sent to Okta via SAML assertions from their Identity Provider (IDP) for authentication. If no account exists, a new user account can optionally be automatically provisioned. User permissions are then processed and accounts provisioned in all necessary applications that power the portal (in this example the product configuration tool). The result is a seamless user experience for the distributor’s employees when they navigate between their corporate apps and the portal.

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.

With this solution, existing infrastructure investments are leveraged 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 PHP.
- A partner site with deal registration built on Force.com.
- A support site built on Jive and Zendesk.

Acme needs to allow access to all of these using a single user name 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 called from the user registration form in the support and partner portals. 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 Zendesk and Force.com, this is enabled through the Okta Application Network and requires no custom code or configuration by the administrator.

For the custom PHP application, Okta can 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 Force.com, Jive, and Zendesk, administrators can achieve this by selecting the applications from the Okta Application Network following a simple 2-4 step wizard. SAML is the preferred SSO mechanism in each of 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 PHP application, Acme.com can use simple template and sample PHP code provided by Okta that can be integrated by Acme.com developers into the login page of the application. Once this code has been embedded, Okta can provide SSO into the app transparently in the same way that it does for Force.com and other cloud apps. Alternatively, Acme.com can also leverage Okta's SWA protocol to enable SSO.

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 or SAML libraries from Okta, and the user registration has been wired in using Okta's REST management API, 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's identity and access management service greatly simplifies the creation of web portals for both customers and partners. Okta allows organizations to:

- 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 an enterprise grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. The Okta service provides directory services, single sign-on, strong authentication, provisioning, workflow, and built in reporting.

Enterprises everywhere are using Okta to manage access across any application, person or device to increase security, make people more productive, and maintain compliance. The hundreds of enterprises, thousands of cloud application vendors and millions of people using Okta today also form the foundation for the industry's fastest growing, vendor neutral Enterprise Identity Network.

The Okta team has built and deployed many of the world's leading on-demand and enterprise software solutions from companies including Salesforce.com, PeopleSoft, Microsoft, BMC, Arcsight, Sun, and HP. Okta is backed by premiere venture investors Andreessen Horowitz, Greylock Partners, Khosla Ventures and Sequoia Capital.

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