okta

Automating User Management and Single Sign-on for Salesforce.com

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

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

Contents

The Growth of Salesforce.com in your Organization

Salesforce.com is one of the most successful, business critical on-demand applications. The company was started with a simple premise: "Why can't a sales system be as simple and easy to use as Amazon. com?" Over the years salesforce.com has expanded to provide services for other CRM categories, extended into collaboration (Chatter), and developed a platform (force.com) that spawned the creation of hundreds of partner applications.

In fact today, in many organizations, the entire sales and customer support team, external customers and partners (via salesforce.com Portals) and, with the services such as chatter, every employee in your company is a user. With this growth comes the need to ensure these users have seamless access via single sign-on and that their accounts within salesforce.com are created, updated and deactivated on an integrated cycle with the rest of the systems in IT.

Salesforce.com User Management Challenges

For both IT and end-users, managing access to salesforce.com presents challenges. Users don't want or need another password, in addition to the ones for their desktops, laptops, mobile devices, or other SaaS applications. Salesforce.com adds yet another password, one that typically expires on a regular cycle, making it more difficult for users to access the application when they need to. Users are forced to come up with elaborate schemes to create passwords they can actually remember, or worse they resort to writing passwords down on sticky notes or storing them in insecure spreadsheets. And if those schemes fail, IT spends countless cycles managing password resets just to keep the users productive.

Within IT you are likely already managing users and their access to core network resources with an internal directory such as Active Directory. Why spend time and effort duplicating a directory just for salesforce.com? And once you create users in salesforce.com, why spend time manually creating them in the other systems integrated to salesforce.com like your quoting tool and product configurator?

Manually adding, changing, and removing users from salesforce. com and other systems consume time and are prone to errors. Organizational productivity is impacted if a salesforce.com user isn't created in a timely manner and security and budget issues arise when an account that is no longer needed is not cleaned up. An additional concern for IT associated with managing these user accounts and passwords is that of compliance. Your auditors and compliance experts are asking your team to document and report on user account creation, user access and user de-provisioning. Automating user management and centralizing passwords using single sign-on makes it far simpler and less time consuming to ensure you meet your audit and compliance needs.

This paper provides insight into both the salesforce.com technology and 3rd party tools and solutions you can use to address these single sign-on (SSO) and user management challenges. Managing multiple stand-alone user directories that are not integrated with Active Directory can easily lead to a set of untenable security and access management challenges. Seamless integration with AD is a must for any solution used to manage access and authorization to your SaaS applications.

Collaborate with IT to Manage Users and Access

As you think through the best options for automating user management and single sign-on for salesforce.com, it's important to consider what IT is best at, and what the salesforce.com administrators know best. The right way to handle core IT functions like user and account management for salesforce.com is to let the experts in your IT organization manage this centrally and efficiently. This leaves salesforce.com administrators free to focus on application setup, administration, and optimization; ultimately driving better business results.

Using Salesforce.com User Management APIs

Salesforce.com provides industry leading capabilities to not only secure your data but also to integrate with other systems to achieve SSO and automate user management.

First, let's cover User Management or how user accounts are created, updated and removed from salesforce.com. Many companies do this manually through the salesforce.com web interface, but Salesforce.com also provides an API for these functions. The User API is fairly comprehensive and includes almost all fields on the User object. A developer can write a program or script to automate all common user management options and could even drive that creation and deactivation of users off of changes in your company network directory (like Microsoft Active Directory).

The User API can also access users across salesforce.com 's customer portal force.com, allowing you to develop software that could "register" a customer portal user before your customer logs in.

There are a few limitations to what you can do with this API. You can set the password, but you can't read the password value. There is also a specific command to reset the password to a value salesforce. com automatically generates and then emails to the user. You can't tell from the API if a user has been locked out of salesforce.com and you are also unable to unlock a locked user—this must be done from the salesforce.com web interface. You also can't delete users using the API or web interface. Instead you can control if a user is "Active" and able to log in using the "IsActive" field. When a user is deactivated, they are no longer able to log in, but the administrator can still change data record ownership and assignment rules to ensure a smooth transition to other users. Deactivated users also don't consume a user license so you can reuse those immediately.

Using Salesforce.com APIs for SSO

Salesforce.com supports an API called Delegated Authentication and the federated single sign-on standard, SAML (Security Assertion Markup Language). While both are associated with Single Sign-on and have some similarities, they also have significant differences.

Lets start with what they have in common. Both work independently of other salesforce. com security features like Security Token and Computer Activation / Activation link.

Your users will have to activate computers and use their Security Token as before. Both are just enabling technologies. You'll need to write or obtain additional systems or libraries to implement a complete solution–and of course maintain that solution over time.

Now lets look at the differences. For starters, SAML is an industry standard. Delegated Authentication is proprietary to salesforce. com. SAML is enabled by default on all salesforce.com orgs and just needs to be configured via the administrative interface. Delegated Authentication is only enabled after an administrator requests salesforce. com to activate this functionality.

SAML is enabled and configured for your entire organization. It is a supplement to the standard salesforce.com authentication process. When SAML is enabled, your users can log in either via SAML, or with their normal password. This means that you can't use SAML alone to enable a third party system to control who accesses salesforce.com.

Delegated Authentication is enabled at the user profile level (i.e., users in one profile can log in via delegated authentication, while others use the normal authentication process). It applies to all user access and can be used to enable a third party system to control who can access salesforce.com.

SAML single sign-on is done entirely via web requests from a user's browser and thus does not impact salesforce.com client applications like Salesforce for Outlook or Force.com Connect Offline. Users still use their salesforce.com password to connect with those applications.

Delegated Authentication requires salesforce.com's servers to call out to another web server. Also, it applies to the web interface and to client applications.

To either automate user management or achieve single sign-on into salesforce.com with your internal directory, these APIs enable you to create a custom solution. There is a significant amount of custom development required to actually achieve a fully functioning solution, and a non trivial amount of effort required to maintain that custom solution over time.

Managing Beyond Salesforce.com

While salesforce.com is a critical component of your corporate IT environment, it is not the only system users need to access, and likely not your only SaaS solution. Truly enhancing end user and administrator productivity means looking at all the applications and systems users need access to, within and outside of your firewall. You need a turn-key solution that seamlessly integrates with all of these regardless of if these systems support standard APIs like SAML, or proprietary APIs like Delegated Authentication. The solution must support cloud applications like salesforce.com, and on premise systems like Active Directory or internally hosted web applications.

Vendor Solutions to the Problem

With the acceleration of SaaS app deployments, several vendors have emerged to help enterprises address their single sign-on and user management needs. Unlike pursuing an application specific integration strategy that leverages similar APIs to those discussed earlier in this paper for salesforce.com, these solutions offer a single way to automate SSO and user management across all your applications.

When evaluating these solutions, several aspects should be considered:

- A Solution or a Tookit?: The right option should not require you to purchase additional products, spend money for services, or require custom development. It should provide:
- Seamless Single sign-on that is integrated with Active Directory.
- A robust catalog of pre-integrated business and personal applications including salesforce.com
- Integration with AD that addresses user management and single sign-on needs.
- An SSO home page for every user, across their applications including salesforce.com
- An integrated administrative experience that allows you to manage users, applications, and your AD integration from one console, anywhere, at anytime.
- Do I need to purchase and maintain hardware?: A modern solution, like salesforce.com itself, should be 100% on-demand, and require no hardware.
- Are the integrations maintained over time?: A true solution should also insulate your business from changes in the underlying SaaS applications and ensure that you can continue to manage users and sso to your applications even as they change over time.
- Is the integration secure and configuration free?: Any integration with AD should be outbound, and should take place over standard HTTPS to ensure security and avoid the need to make any changes to your existing firewall configuration.
- Will the solution degrade user experience?: To maximize performance and user experience, a sso solution should authenticate a user and get out of the way. Routing all traffic through a proxy creates bottlenecks, degrades performance, and does not scale as usage increases.

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. The Okta service provides directory services, single sign-on, strong authentication, provisioning, workflow, and built in reporting.

If you just want to get started with salesforce.com, Okta provides a complete solution to integrate this one cloud application back to Active Directory. Okta for salesforce offers a complete end-to-end solution that requires no services to install and includes:

- Self-configurable, secure integration with your existing Active Directory infrastructure.
- A large catalog of pre-integrated applications, including salesforce.com.
- A single sign-on home page for every user and all of their applications, including salesforce.com.
- An integrated administrative experience that allows you to manage users, applications, and your AD integration from one console, anywhere, at anytime.
- A 100 percent on-demand offering. The core service is a multi-tenant solution with a very light footprint AD agent that installs locally but is managed centrally. No appliances.
- A single AD integration that enables you to integrate once and federate Active Directory across all of your SaaS applications, including salesforce.com.
- Application integrations that are maintained over time. Okta modifies the integrations as underlying applications change and you never know it.
- Outbound AD connection over HTTPS. Our lightweight agent makes a secure, outbound-only connection over HTTPS—no firewall configuration changes are required.
- Out of band authentication. Okta authenticates a user with the SaaS application and then gets out of the way. All ongoing traffic is between the user and the application.

About the Author

Todd McKinnon is a seasoned entrepreneur and executive with deep experience focused on software development and design of web-scale services. In early 2009, Todd started Okta with a powerful vision: Leverage the power of the cloud to make IT more secure and people more productive.

From 2003 to 2009, Todd worked at salesforce.com where he served as overall head of the engineering, user interface design, documentation and localization teams. Under Todd's leadership, the team grew from 15 to over 250 people while the salesforce.com service grew from 3 million to over 150 million transactions per day with industry leading performance and reliability.

Prior to salesforce.com, Todd worked at PeopleSoft in the PeopleTools group building the underlying platform for the PeopleSoft applications. He worked as an engineer, technical lead and engineering manager for various areas of the product.

Todd earned a BS in Business from Brigham Young University and an MS in Computer Science from Cal Poly San Luis Obispo.

Getting Started with Your Free Trial

To discover how easy it is to get started with Okta, establish a comprehensive integration with Active Directory, and begin securely managing access across all of your cloud, on premises and mobile apps, visit www.okta.com/freetrial.

And if you want to use Okta with just salesforce and Active Directory, that product is free. Visit http://www.okta.com/salesforce.

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.