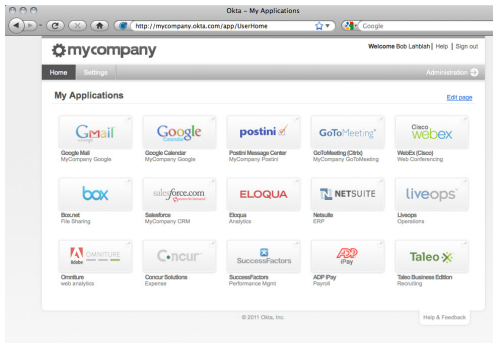


On-Demand Identity and Access Management for the Cloud

Single sign-on, user management, and reporting across all your web applications



End-User Single Sign-On Home Page

SaaS Adoption and the Cloud Services Network

Businesses everywhere are pursuing enterprise-wide deployments of business critical, Software-as-a-Service (SaaS) applications such as Salesforce.com, WebEx, or NetSuite. As a result, yesterday's Local Area Networks are giving way to today's Cloud Services Networks composed of a collection of on-demand services, from a variety of vendors, serving a set of highly distributed users who require access from any browser at any time.

Challenges of Running a Cloud Services Network

The on-demand applications that make up a Cloud Services Network enable companies to rapidly deploy powerful capabilities to users at very low costs, but also introduce a new set of challenges.

Controlling User Access

Controlling who has access to which applications becomes a real challenge when users can get access from any browser, at any time, from any place. This situation is exacerbated with SaaS as IT is often not involved in the purchasing process.

Password Fatigue

Every SaaS application has different password requirements. So, multiply the variety of requirements by the reset timing variations and the result is "password fatigue" from managing these constantly changing passwords across applications. This increases security risks as users resort to using obvious passwords, or writing them on Post-It notes or in spreadsheets.

Collaborative Administration

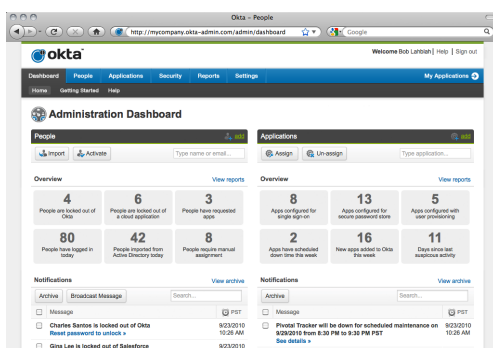
Each cloud application has a unique administration model and management of the application is typically shared between IT and the business. IT needs one way to perform user and access management across applications, while still giving the business the control of the application they need.

On-Premise Directory Integration

SaaS applications have independent user stores that are not integrated with on-premise directories. As a result, users have to remember more passwords, and IT has to manage multiple accounts and map users between their directories and cloud applications. IT needs a single integration with their on-premise directory that federates across all of their cloud applications.

Managing Compliance and ROI

To ensure the best ROI for the business, IT must understand actual SaaS usage and how it compares to what the business is currently paying for. In addition, with increasing regulatory pressure, IT must constantly monitor and control which users have access to which SaaS applications.



Centralized Administration and Reporting

Okta: Covering Your Cloud

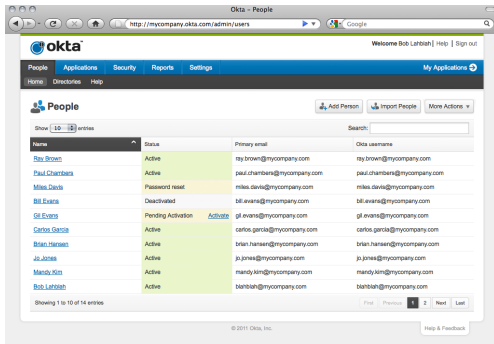
Okta is an on-demand identity and access management service that enables enterprises to accelerate the secure adoption of their web based applications, both in the cloud and behind the firewall. Okta delivers a complete solution addressing the needs of IT, end-users, and business leaders; no customization required.

End-Users: One Destination, All Applications

Once activated, each end-user receives a customized homepage providing single sign-on and self-services across applications, and credentials. The homepage can be accessed from any browser or device, and the entire homepage is easily integrated into a custom portal.

IT: Control Across People and Applications

Okta provides one service from which you can manage people, applications, and policies across all of your cloud and web applications. An administrative dashboard contains a summary of key usage and activity statistics, notifications of any problems or outstanding work to be completed, as well as shortcuts to the most commonly performed tasks.



Manage People and Applications

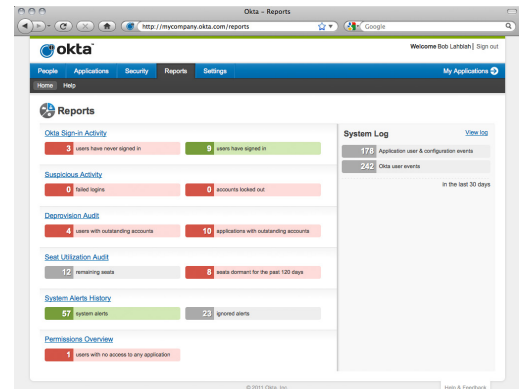
A central directory provides a view of both your people and the identities they are mapped to in all of their web applications. Adding applications is as simple as selecting a pre-integrated application from the Okta Application Network. Each application has its own administrative homepage, which provides a summary of the current integration settings across single sign-on and user management, as well as a view to recent log activity and the current people who have this application assigned to them.

Executives: Maximize ROI and Minimize Risk

Centralized logging captures a comprehensive set of events across Okta and the integrated applications. Okta also includes a full reporting experience, no separate BI solution needed.

The pre-canned reports include things such as User Activation, User Activity, User Access, Application Usage, User Provisioning, and De-Provisioning. Reports can be scheduled for distribution and data is easily exported.

Okta also offers an end-to-end de-provisioning workflow that informs an administrator when a user has been deactivated, indicates which applications they have automatically been deactivated from, and helps the administrator finalize any manual user account deactivation required. All of the deactivation activity is tracked in a central audit log for compliance purposes.



Robust Logging and Reporting

About Okta

Okta is the market leading on-demand identity and access management service that enables enterprises to accelerate the secure adoption of their web based applications, both in the cloud and behind the firewall. The Okta team has built, deployed, and supported market leading, on-demand and enterprise software solutions from companies including Salesforce.com, SuccessFactors, PeopleSoft, Microsoft, Sun, and HP. Okta is backed by premiere investors including Andreessen Horowitz, FLOODGATE, and Ron Conway.