



## **Top Eight Identity & Access Management Challenges with SaaS Applications**

Okta White Paper

## Table of Contents

The Importance of Identity for SaaS Applications .....	2
1. End User Password Fatigue.....	2
2. Failure-Prone Manual Provisioning and De-Provisioning Process.....	2
3. Compliance Visibility: Who Has Access to What? .....	3
4. Siloed User Directories for Each Application .....	3
5. Managing Access across an Explosion of Browsers and Devices.....	4
6. Keeping Application Integrations Up to Date .....	4
7. Different Administration Models for Different Applications.....	4
8. Sub-Optimal Utilization, and Lack of Insight into Best Practices.....	5
Addressing these Challenges with Okta .....	6
Getting Started with Your Free Trial .....	6
About Okta.....	6

## The Importance of Identity for SaaS Applications

The enterprise cloud revolution is upon us. IT organizations everywhere, from small and mid-sized businesses to Fortune 500 companies, are moving from on-premise application software to on-demand, cloud-based services. As enterprise IT makes this transition to a new hybrid on-demand/on-premise paradigm, controlling who is granted access to which applications and data becomes increasingly important. This presents CIOs and their IT organizations with a whole new set of identity management challenges. In addition, end users face the challenge of keeping track of multiple URLs, usernames, and passwords to get access to their applications, and the role IT must play is also fundamentally changing. As the steward of these new services, IT must provide additional insight and advice about software-as-a-service (SaaS) applications to ensure the company is maximizing the business value of their investments.

This whitepaper presents the eight biggest identity and access management (IDM) challenges associated with adopting and deploying cloud and SaaS applications, and discusses best practices for addressing each of them.

### 1. End User Password Fatigue

The SaaS model makes it easier for users to initially access their applications, but complexity increases quickly with the number of applications they use. Each application has different password requirements and password expiration cycles also vary. So, multiply the variety of requirements by the variety of expiration cycles and the result is lost user productivity and increased user frustration as they spend time trying to reset, remember, and manage these constantly changing passwords and URLs across all of their applications.

Perhaps of even greater concern are the security risks caused by the same users who react to this “password fatigue” by resorting to the use of obvious or reused passwords written down on Post-It notes or saved in Excel files on laptop computers.

Cloud-based identity and access management (IAM) services can alleviate these concerns by providing single sign-on across all of these applications, giving end users a central place to access all of these systems with one username and password. Better yet, a cloud-based identity management system can also enable your IT department to manage identities across both on-demand and on-premise applications.

### 2. Failure-Prone Manual Provisioning and De-Provisioning Process

When a new employee starts at your company, IT often provisions the employee with access to the corporate network, file servers, email accounts, printers. Since many SaaS applications are managed at the department level (Sales Operations manages Salesforce.com, Accounting manages QuickBooks, Marketing manages Marketo), access to these applications is often granted one-at-a-time by the specific application’s administrator, not by someone in IT.

Why shouldn’t SaaS apps be as easy to provision centrally as your core network services? A robust cloud identity and access management service should be able to automate the provisioning of new SaaS applications – as a natural extension of your current on-boarding process. As a user is added to your core directory service (such as Active Directory), their

membership in particular security groups should ensure that they are automatically provisioned with the appropriate applications and given the role/set of access permissions necessary for them to do their job. It should be just that simple.

Arguably, an even bigger concern arises when an employee is terminated. IT can centrally revoke access to email and corporate networks, but they have to rely on external application administrators to revoke the terminated employee's access to SaaS applications. This leaves the company vulnerable, with critical business applications and data in the hands of sometimes disgruntled former employees and auditors quick to jump on holes in their de-provisioning audits.

A cloud-based IAM service should not only enable IT to automatically add new applications but also provide:

- Automated user de-provisioning across all on-premise and on-demand applications
- Deep integration with Active Directory
- Clear audit trails

The IAM service should help restore piece of mind that once an employee has left the building, the company's data hasn't left with her!

### **3. Compliance Visibility: Who Has Access to What?**

It's always important to understand who has access to applications and data, where they are accessing it, and what they are doing with it. This concern increases when it comes to cloud services. Unfortunately, only the most advanced offerings like Salesforce.com even offer any compliance-like reporting, and when they do it's siloed for just that one application.

When your auditors ask you who has access to applications and data, you need central visibility and control across all your systems. Your IAM service should enable you to set access rights across services and provide centralized compliance reports across access rights, provisioning/de-provisioning, and end-user and administrator activity.

### **4. Siloed User Directories for Each Application**

If you're like most enterprises, you've made a significant investment in a corporate directory (such as Microsoft Active Directory) to manage access to on-premise network resources. As you adopt cloud based services, you need to leverage that investment and extend it to the cloud, rather than create a parallel directory and access management infrastructure just for those new SaaS applications.

A best-of-breed cloud-based IAM solution should provide centralized "out-of-the-box" integration into your central Active Directory or LDAP directory so you can seamlessly leverage and extend that investment to these new applications – without on-premise appliances or modifications to your firewall required. As you add or remove users from that directory, access to cloud-based applications should be modified automatically, via industry standards like SSL, without any network or security configuration changes. Just set and forget.

## 5. Managing Access across an Explosion of Browsers and Devices

One of the great benefits of cloud applications is that access is available with any device that is connected to the Internet. As discussed previously, more apps mean more URLs and passwords, and the rise of mobile devices that have real computing capability introduces yet another access point.

Your department needs to facilitate browser and mobile device access across multiple devices and platforms without compromising security, a tough feat with existing IAM systems.

A cloud-based IAM solution should help both end-users and IT administrators with the “anywhere, anytime, from any device” access challenge. A good solution should provide not only browser-based single sign-on for end-users to all of their applications but also enable simple access to those same services from the users’ mobile device of choice.

## 6. Keeping Application Integrations Up to Date

Truly centralizing single sign-on and user management requires building integrations with numerous applications and keeping track of the maintenance requirements for new versions of each application. For the vast majority of organizations, having their IT department maintain its own collection of connectors across that constantly changing landscape is unrealistic and inefficient.

Today’s enterprise cloud applications are being built with cutting-edge, Internet-optimized architectures. The modern web technologies underlying these applications provide excellent choices for vendors to develop their service and its associated interfaces. Unfortunately for the IT professionals, that also means that every new vendor may require a new approach when it comes to integration, particularly concerning user authentication and management.

In addition, like on premise applications, SaaS apps also change over time. A good cloud-based IAM solution should keep up with the wide variety of changes and make sure that the application integration, and thus your access, is always up to date and functional. Your IAM service should mediate all of these different integration technologies and approaches, making these challenges transparent for IT. And as the various services’ APIs change and multiply, the cloud IAM provider should manage these programmatic interfaces, abstracting the technological heavy-lifting away from your IT department. No more tracking dependencies between connectors and application versions.

This should also translate to making the addition of a new application into your network as easy as adding a new app to your iPhone. With only minimal, company-specific configuration, you should be able to integrate new SaaS applications with single sign-on and user management capability within minutes.

## 7. Different Administration Models for Different Applications

As cloud applications become easier and less expensive to get up and running, companies adopt more point SaaS solutions every day. These solutions are often managed by the corresponding functional area in a company, such as the Sales Operations group in the case of Salesforce.com. While this is beneficial to IT, leaving application administration to others and freeing up more

time for other tasks, it also creates a new problem with no centralized user and application administration and reporting.

A cloud IAM service should provide IT with central administration, reporting, and user and access management across cloud applications. In addition, the service should provide a built-in security model to provide the right level of access to your individual application administrators, so that they can manage their specific users and applications within the same IAM system.

## **8. Sub-Optimal Utilization, and Lack of Insight into Best Practices**

One of the reasons for the rise of cloud applications is that low upfront costs and monthly subscription models have replaced the upfront lump sum of the old, on-premise license purchase. CFOs clearly prefer to pay for the services that employees use as they go. With no centralized insight into usage, however, information technology and financial managers have no data to manage these subscription purchases and little idea whether they are paying for more than they actually use..

A cloud-based IAM service should provide greater visibility into seat utilization and help IT optimize SaaS subscription spend. Managers should have real-time access to service utilization reports with data on how many users log into the different services, and how often. In addition, by superimposing access trends to various applications across top employee performers, corporate executives should be able to use a centralized user management service to memorialize employee best practices and spread the lessons learned across the organization.

## Addressing these Challenges with Okta

Okta is an on-demand identity management service designed to help companies address these challenges and accelerate the adoption of SaaS applications across their enterprise.

With Okta you can bring all of your SaaS applications together to help build what we refer to as a Cloud Area Network. With Okta at the center of your Cloud Area Network, you can easily address the challenges of securing and controlling users and access, simplify the adoption and scaling of these applications, and get insight on usage and utilization to ensure that your business is optimizing its cloud investments.

Okta's offering is designed from the ground up combining enterprise class, on-demand functionality with a consumer web ease of use to provide value to every level of your organization, giving:

- **Executives** the ability to maximize business potential while minimizing business risk
- **IT** the insight and control necessary to lead, not impede, the move to the cloud
- **End Users** one place to access the applications they need, whenever and wherever they need them.

## Getting Started with Your Free Trial

We encourage you to not just take our word for it, but to discover on your own how easy it can be to get started with Okta and begin addressing these key challenges that you are facing with your cloud applications.

Just go to [www.okta.com/freetrial](http://www.okta.com/freetrial) and you can get started today!

## About Okta

Okta is an on-demand identity management service designed to help companies accelerate the adoption of SaaS applications across their enterprise. Okta integrates with existing directory solutions and provides businesses with secure, integrated control of users, applications, and data in the cloud and behind the firewall. The Okta team has built, marketed, and sold market-leading, on-demand solutions including Salesforce.com, SuccessFactors, and Rearden Commerce, and is backed by premiere silicon valley angel and venture investors.