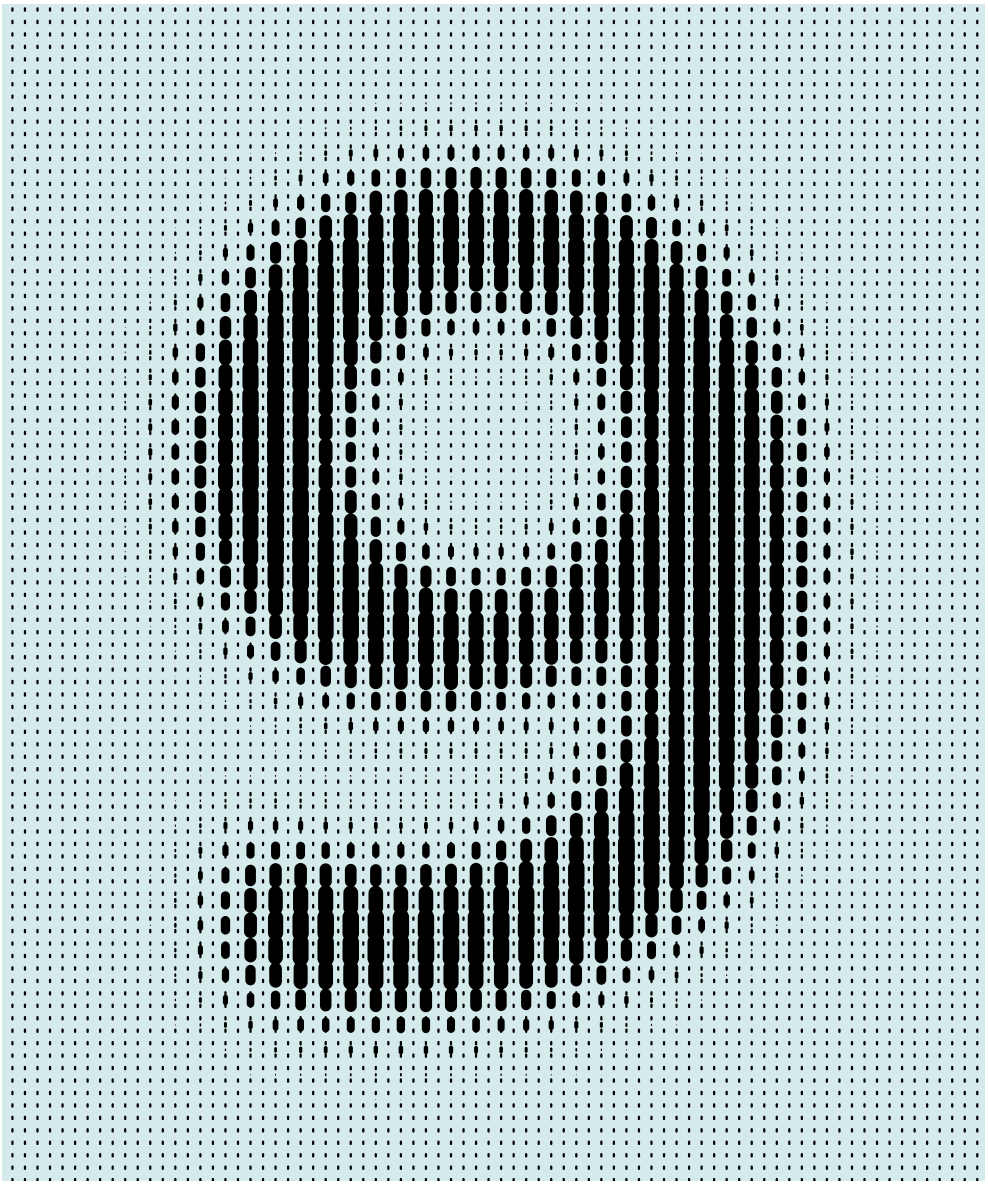
Whitepaper

January 2021

Top 9 Identity & Access Management Challenges with Your Hybrid IT Environment

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



Contents

The Importance of Identity for SaaS Applications

The enterprise cloud revolution is here. IT organizations everywhere, from small and mid-sized businesses to Fortune 500 companies, are moving from on-premises software to on-demand, cloud-based services. As enterprise IT adopts more cloud systems while keeping on-prem solutions, controlling who is granted access to which applications becomes increasingly important. This presents CIOs and their teams with a whole new set of identity management challenges. In addition, users must keep track of multiple URLs, user names, and passwords to get access to their applications from ground to cloud. IT's role is also fundamentally changing. As the steward of these new services, IT must provide insight and advice about Software-as-a-Service (SaaS) products to ensure the company is maximizing the business value of their investments, all while keeping on-prem systems secure and accessible from anywhere.

There are nine main identity and access management (IAM) challenges associated with adopting cloud and SaaS applications while keeping on-prem systems safe, as well as best practices for addressing each of them.

1. User Password Fatigue

Although the SaaS model initially makes it easier for users to access their applications, complexity quickly increases with the number of applications. Each application has their own identity store with their own login URLs and requirements for passwords. This proliferation of credentials results in diminished 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 users who react to this "password fatigue" by using obvious, insecure passwords or reusing the same passwords across multiple systems. Worse yet, these credentials are usually written down on Post-it notes or saved in an insecure text document on their laptop.

Cloud-based IAM services can alleviate these concerns by providing single sign-on (SSO) across all of these applications, giving users a central place to access all of their resources with a single username and password. A great SSO solution can connect equally well to both cloud applications and on-premises applications, which is critical as many organizations will need to enable access to both types of applications.

The majority of enterprises use Microsoft Active Directory (AD) as the authoritative user directory that governs access to basic IT services, such as email and file sharing. AD is often also used to control access to a broader set of business applications and IT systems. The right on-demand IAM solution should leverage Active Directory, and allow users to continue using their AD credentials to access SaaS applications—this increases the likelihood that users will find the newest and best SaaS applications their company provides them.

2. Failure-Prone Manual Provisioning and Deprovisioning Process

When a new employee starts at a company, IT often provides the employee with access to the corporate network, file servers, email accounts, and printers. Since many SaaS applications are managed at department level (e.g. Sales Operations manages Salesforce.com), access to these applications is often granted separately by the specific application's administrator, rather than by a single person in IT.

Given their on-demand architecture, SaaS apps should be easy to centrally provision. A modern IAM solution should be able to automate the provisioning of new SaaS applications as a natural extension of the existing onboarding process. When a user is added to the 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 access permissions their role would be entitled to.

Almost certainly, an employee termination is a bigger concern. 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 each SaaS application. This leaves the company vulnerable—critical business applications and data are in the hands of potentially disgruntled former employees, while auditors look for holes in your deprovisioning processes.

A strong IAM solution should not only enable IT to automatically add new applications, but it should also provide:

- Automated user deprovisioning across all applications
- Deep integration with all user stores including Active Directory and LDAP
- Clear audit trails

The IAM service should provide organizations with the peace of mind that once an employee has left the company, the company's data hasn't left with them.

3. Compliance Visibility: Who Has Access to What?

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

To answer auditors who ask you which employees have access to your 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 and deprovisioning, and user and administrator activity.

4. Siloed User Directories for Each Application

Most enterprises have made a significant investment in a corporate directory (such as Microsoft Active Directory) to manage access to on-premises network resources. As organizations adopt cloud based services, they 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-premises appliances or firewall modifications 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 for Remote Work

One of the great benefits of cloud applications is that access is available from any internet-connected device. But more apps means more URLs and passwords, and the rise of mobile devices introduces yet another access point to manage and support.

IT departments must facilitate access across multiple devices and platforms without compromising security—a difficult feat with existing IAM systems.

A cloud-based IAM solution should help both users and administrators solve the "anywhere, anytime, from any device" access challenge. It should not only provide browser-based SSO to all user applications, but it should know the user's context, such as location, device, and behavior. This ensures a high level of confidence the user is who they say they are. The perimeter is no longer at the network level, but now at the identity level.

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 built with cutting-edge, internet-optimized architectures. The modern web technologies underlying these applications provide excellent choices for vendors to develop their services and 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, whether on-prem or in the cloud, apps change over time. A good cloud-based IAM solution should keep up with these changes and ensure that the application integration, and thus your access, is always up to date and functional. Your IAM service should mediate all the 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, offloading the technological heavy-lifting away from your IT department, so they no longer have to track dependencies between connectors and application versions.

Adding a new application into your network should be as easy as adding a new app to your iPhone. With only minimal, company-specific configuration, you should be able to integrate new applications with SSO 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 are adopting 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. This can benefit IT because it leaves application administration to others and frees up time, but it can also create a new problem because there is no central place to manage users and applications, or provide reports and analytics.

A cloud IAM service should provide IT with central administration, reporting, and user and access management across cloud and on-prem applications. In addition, the service should include a built-in security model to provide the right level of access to your individual application administrators, so 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 reason for the rise of cloud applications is that monthly subscription models have replaced the upfront lump sum of the old, on-premises software license purchase. CFOs clearly prefer to pay for the services that employees use as they go. With no centralized insight into usage, however, IT and financial managers cannot manage these subscription purchases and have little idea whether they are paying for more than they actually use.

A cloud-based IAM service should provide accurate visibility into seat utilization and help IT optimize SaaS subscription spend. Managers should have real-time access to service utilization reports. 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 record and evangelize employee best practices.

9. Provide Consistent Access to On-Prem and Cloud Applications

Most organizations operate in a hybrid IT model, where users need to access a mix of SaaS apps and on-premises web applications—such as ERPs, financial, or enterprise solutions—with the same level of security and ease. The explosion of browsers and mobile devices alongside the need to provide secure access from anywhere adds an extra challenge for IT leaders with siloed IAM solutions: one for on-prem and another for cloud apps. Modern cloud-based IAM services can manage both. They provide access gateways for on-premises applications, extending the security and productivity benefits for all apps, regardless of where they are hosted. End users can access cloud and on-prem apps from a single dashboard without jumping through hoops, while IT administrators can control and audit access from the same place.

Addressing These Challenges with Okta

Okta is the leading independent provider of identity for the enterprise, built from the ground up in the cloud and delivered with an unwavering focus on customer success. The Okta Identity Cloud provides directory services, single sign-on, strong multi-factor authentication, automated provisioning, automated workflows, 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.

Okta can be used to manage access across all of your applications, and the service provides critical benefits for users, administrators, and executives.

Users: One Destination for All of Their Applications

As a service, adding new users to Okta is as easy as adding a user to any other SaaS application. Once activated, each user receives a customized home page, providing single sign-on across applications, and self-service provisioning and password reset. The home page can be accessed across browsers and devices, and the entire home page or individual applications are easily integrated into a custom portal.

Administrators: Secure, Integrated Control Across People and Applications

For IT, Okta helps administrators manage people, applications, and policies across all cloud and web applications, all from one place. A central directory provides a view of both 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 and performing any additional configuration specific to your organization.

Executives: Insight to Maximize ROI and Minimize Risk

Okta also offers a centralized system log that captures a comprehensive set of events across Okta and integrated applications. A full reporting experience spans all integrated applications, so no separate BI solution is needed. Out-of-the-box reports help executives track activity, ensure compliance, and monitor application usage and ROI Getting Started with Your Free Trial

Getting Started with Your Free Trial

To discover how easy it is to overcome identity and access management challenges in the cloud, visit **www.okta.com/free-trial** to get started with Okta.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit **okta.com**.