okta

The Benefits of Migrating from ADFS to Okta

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

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

Challenges of Single Sign-On Deployments

The adoption rate of cloud applications has been dramatic in recent years. Cloud applications like Salesforce.com, Box, and Office 365 are being deployed across the enterprise. As a result, many organizations have either devised policies for cloud applications or are looking to do so in the near future.

Many enterprises today are looking to implement a single sign-on (SSO) so their users can easily access all of their cloud and web applications without authenticating to each application individually. They want to connect all of their cloud applications back to a single source of truth, which in many cases is Microsoft Active Directory. Many companies conclude that the solution for single sign-on from Active Directory is Active Directory Federation Services (ADFS)—simply because they are both Microsoft products.

But not all Active Directory integration solutions are created equal. IT departments considering ADFS should examine all aspects of implementing it for SSO. While the license for ADFS is free, there are several hidden costs associated with ADFS such as setup, ongoing support, and hardware. They should also consider what constitutes a complete identity management solution, including provisioning, contextual access management for mobile devices, centralized reporting and pre-integrated support for the thousands of applications that today's companies are using.

This white paper will discuss the hallmarks of a successful Active Directory integration and SSO deployment, and will highlight the benefits of migrating from on-premises ADFS to Okta's comprehensive, 100% cloud-based service.

Key Elements of a Successful SSO Solution

There are many things to consider when investigating how to implement single sign-on. It is helpful to focus on a few key elements to ensure success. Many of these elements may seem to be insignificant at first, but can become major frustrations later on as companies grow and adopt more applications.

- **Active Directory Integration**
  If your organization uses Active Directory, your SSO solution must let you leverage that investment, and keep cloud applications that support SSO synchronized with Active Directory.
- **Application Integrations and Support**
  The ability to support all of your applications, both today and in the future, should always be considered when looking at a company-wide solution. There may be one or two cloud applications to integrate today, but what is your company's longer-term strategy? As your applications scale, they may have different configuration requirements that change over time, requiring an IT admin to stay on top of individual apps. The labor and setup associated with each application can become a drain on both employees and IT budgets.
- **High Availability**
  Any downtime associated with your SSO deployment means downtime for your users. This downtime may be planned, but it may also be unexpected. An SSO service and associated support must be agile enough to remain up and running, even when the provider changes application configurations.

Any downtime—whether caused by your servers or changes to the application—lowers productivity for end users and the business as a whole.

- **Provisioning of Users and Cloud Apps**
  Provisioning entails creating, updating, and removing access to an application or other resources. On average, it takes an IT admin 30 minutes to process each provisioning or deprovisioning request. And that doesn't include all of the help desk calls for password resets and configuring employees on all their devices. By automating provisioning and user lifecycle management, management can save IT and other departments' valuable time and unnecessary frustration.
- **Contextual Access Management with Mobile Devices**
  Mobile might be the next thing to propel your team to new levels of productivity, but solving the security question is holding you back. Your SSO solution should integrate with whatever mobile device management (MDM) solution you already use. It should be configurable with policies to prevent unmanaged devices from accessing your applications and data. And it should also support multi-factor authentication using mobile devices and other factors, to increase security.
- **Efficient Domain Consolidation**
  When mergers and acquisitions bring different companies and their resources together, consolidating domains, tools, and approaches to security can be a challenge. A modern, cloud-based approach to SSO can speed up and simplify this process.
- **Logging and Reporting**
  Many regulatory agencies (e.g. SOX, HIPAA) require audit trails for users, including visibility into what applications and systems employees have (or had) access to. IT departments need to provide details around application deprovisioning for departing employees. The ideal SSO solution should be able to gather usage information for IT admins to quickly meet necessary company and industry reporting requirements.

Using Active Directory Federation Services as an SSO Solution

Customers look to Microsoft Active Directory Federation Services (ADFS) to extend identity from Active Directory to cloud applications outside of the firewall. ADFS is a "free" solution, but requires multiple hardware components, additional Microsoft software, and extensive configuration and maintenance. Organizations using ADFS for SSO face complex configuration requirements and dependency on other resources to meet the minimum requirements for an SSO solution.

ADFS Components

When considering using ADFS for SSO needs, it's important to understand all the underlying components. Three things comprise ADFS itself: the ADFS Server, the Federation Service Proxy installed between the ADFS server farm and external applications, and the ADFS configuration database.[1]

ADFS was developed to be a toolkit—a feature of Windows Server—not an end-to-end solution for single sign-on needs. Toolkits can be flexible, but they require a significant amount of additional support to develop a complete solution. And that's work your IT team needs to perform.

[1] SQL or Windows Internal Database (WID)

Each ADFS component requires custom development and administrative time to understand, configure, and maintain the SSO connections to the target cloud applications—making it difficult to scale out to support a large number of applications.

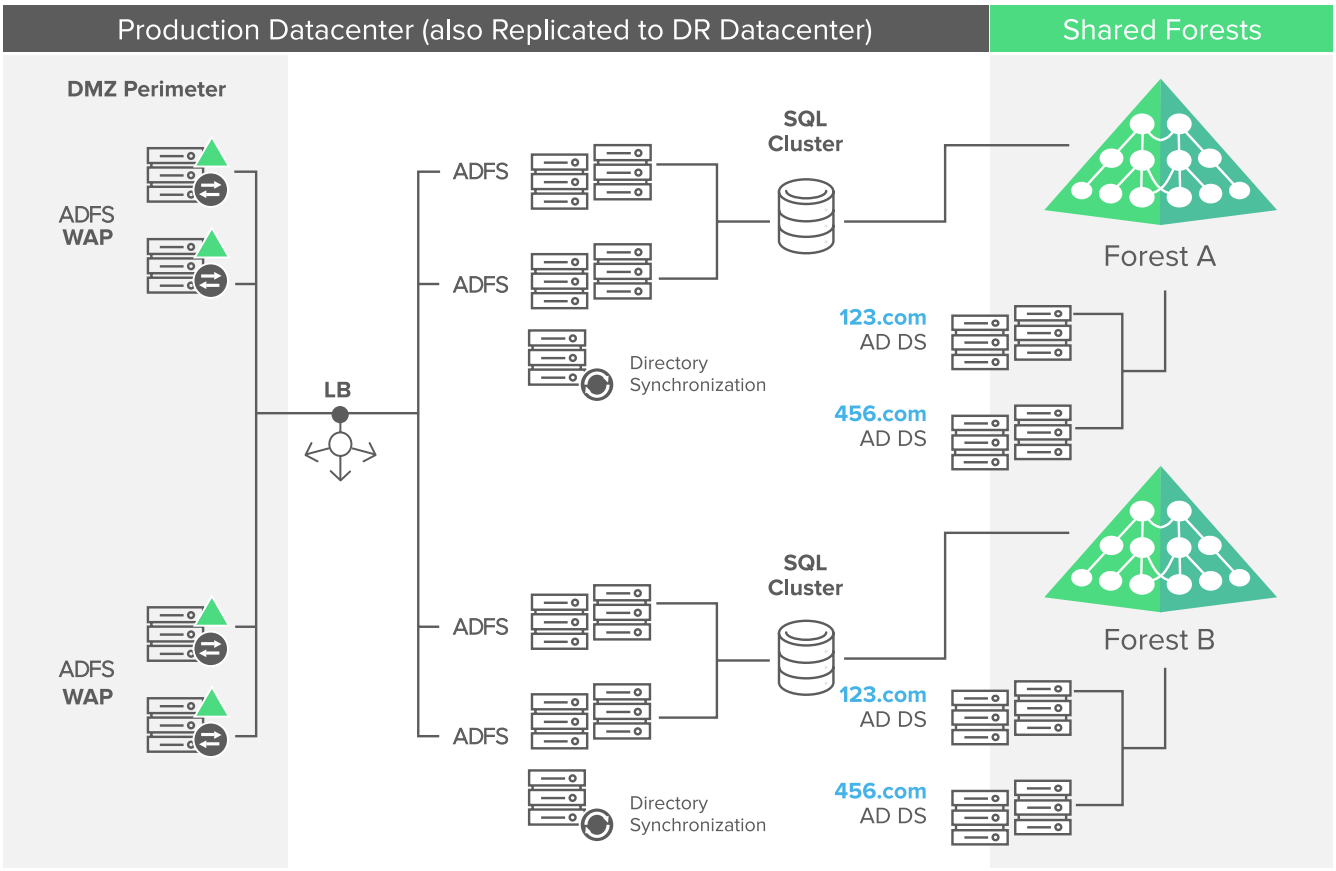

Figure 1: ADFS requires complex on-premises infrastructure to integrate with Active Directory

ADFS Customization

To configure ADFS for SSO, you have to set up policies to authenticate users, authorize access, and generate claims rules to enable authentication with each cloud application. This requires establishing trust between ADFS and the target applications, using a valid SSL certificate that binds to the ADFS service. A self-signed certificate is sufficient for testing, but a third-party signed certificate is required for production. Once trust is established, claims rules need to be generated for authenticating with the target cloud application. Finding the claims rules for each application used to be a manual process for ADFS administrators, but has improved somewhat with the new access control policy templates in ADFS 2016.

The rules for each application may change over time and invalidate your SSO integration. You have to keep track of these application changes and update access control policies accordingly.

Once you've established the ADFS infrastructure and developed the appropriate claims rules for each target cloud application, it's still necessary to determine how users will actually use SSO to access these applications. Most commonly this is through Azure Active Directory.

Single Sign-On and Provisioning

If your company plans to use ADFS scale from one application today to five or six in the next three years, each new application needs manual configuration. Be prepared to perform regular maintenance to ensure each application remains connected with corporate networks and infrastructure. While this may not seem like a large upfront cost, the number of person-hours required for each new application won't decrease with economies of scale.

To integrate applications for SSO from Active Directory using ADFS, a replica of every user needs to be populated into Azure Active Directory. This requires licenses for the Microsoft Enterprise Mobility + Security (EMS)—Microsoft's cloud-based identity and access management solution on Azure Active Directory.

Provisioning and lifecycle management with ADFS require purchasing and configuring yet another tool—Microsoft Identity Manager (MIM), previously named Forefront Identity Manager.

Benefits of Migrating from ADFS to Okta

If your organization has already deployed ADFS but is looking to expand coverage to support more cloud applications and more functionality, adding Okta offers several benefits:

Simplicity

Okta's founders looked at the functionality of ADFS and built the best aspects of it into a scalable cloud platform. Okta manages the full deployment and service availability, and delivers reliability that outperforms large and complex on-premises identity federation infrastructure.

Okta is an integrated identity management service that's designed to securely connect people to their applications from any device, anywhere, at any time.

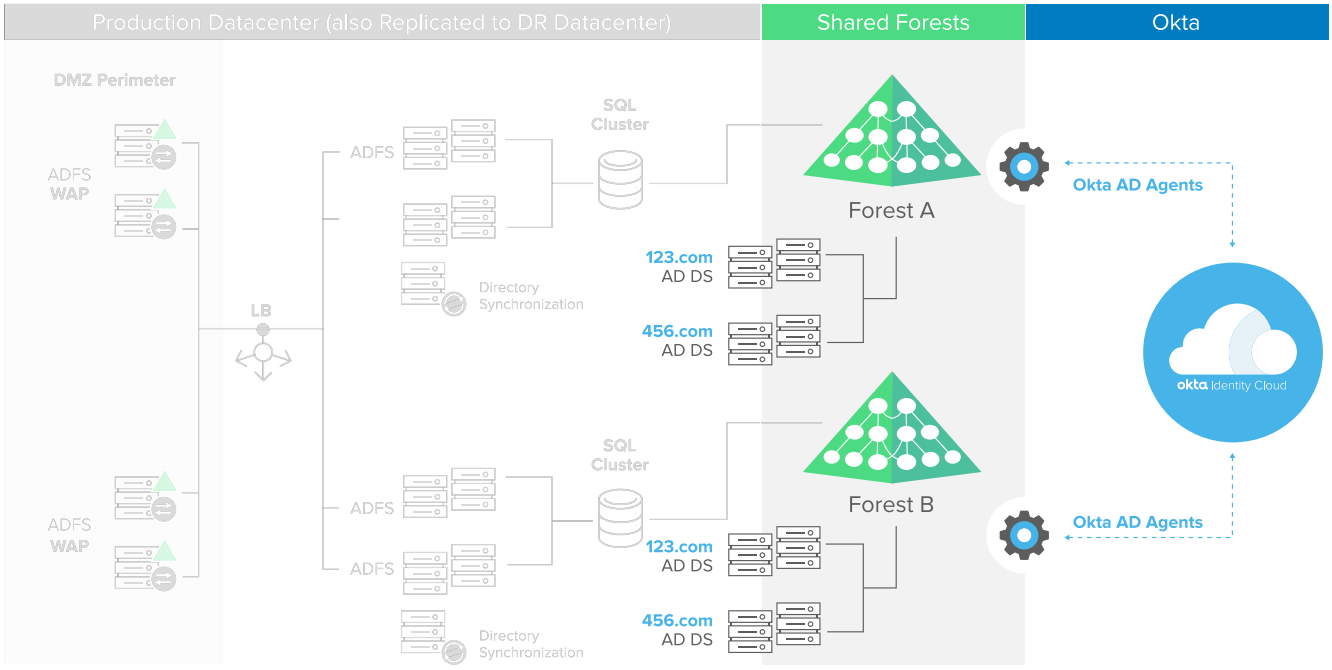

Figure 2. Okta's lightweight AD agents and Cloud platform provide secure integration with your existing Active Directory infrastructure.

Active Directory Integration

Okta's cloud platform is a 100 percent on-demand offering that provides secure integration with your existing Active Directory infrastructure.

Okta's core service is a multi-tenant solution with an Active Directory agent that installs locally but without any appliances or servers to buy or maintain. Okta's lightweight agent makes a secure, outbound-only connection over HTTPS—no firewall configuration changes are required. Once Okta authenticates a user with the cloud application, it then gets out of the way. All ongoing traffic is between the user and the application.

Okta supports delegated authentication, provisioning and deprovisioning, directory sync, and AD password management. Whenever a change occurs in either direction between Active Directory or Okta, those changes are synchronized incrementally. An administrator can deactivate a user in Okta Universal Directory, and the user's record in Active Directory will also be deactivated instantly.

Single Sign-On with Easy Application Integrations

The Okta Integration Network is a large catalog of pre-integrated business and personal applications, infrastructure, and devices. End users see a central portal of applications that lets them easily access the applications that have been provisioned to them. As shown in Figure 3, single sign-on from Active Directory, Federated SSO and deep application integrations can be deployed using Okta in much less time because of its integrated cloud platform.

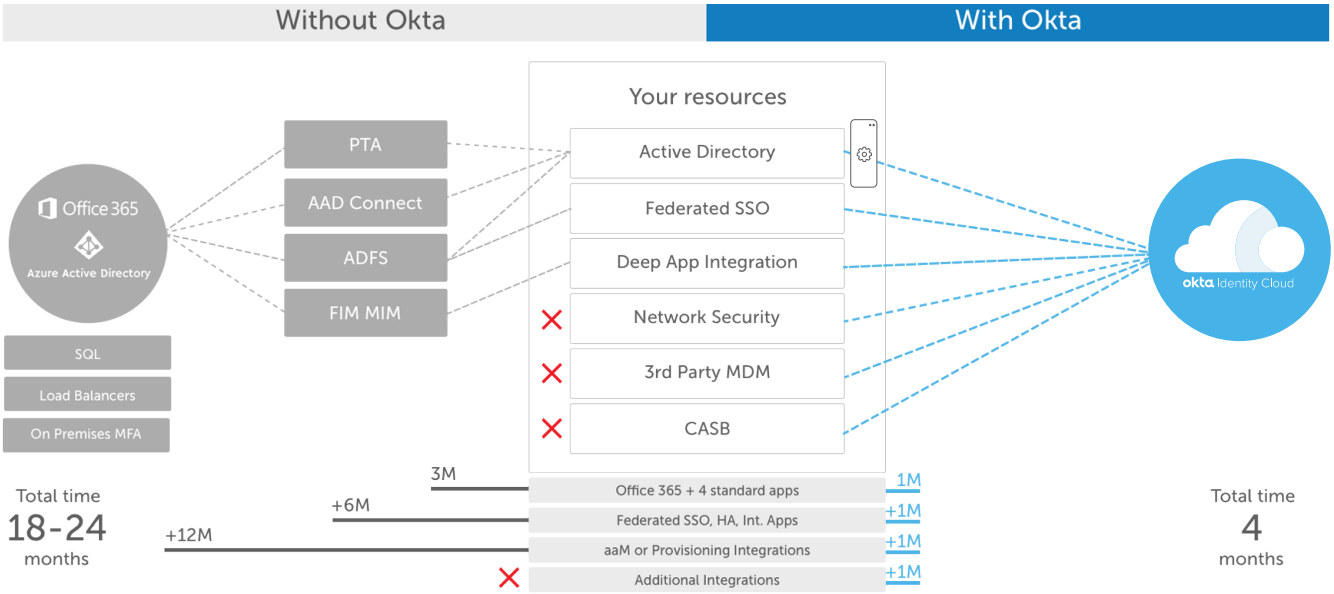

Figure 3: Okta simplifies and accelerates SSO, provisioning and integrations with other applications and services

High Availability

There's never a good time for your SSO solution to go down, even for planned maintenance. Okta's cloud platform is built for 99.99% availability and zero planned downtime.[2] Okta's cloud architecture is 100% multi-tenant, stateless, and extremely redundant across multiple availability zones and regions. You never have to worry about changes to underlying applications because Okta continuously manages and

[2] https://www.okta.com/a-secure-reliable-service-you-can-trust/

monitors cloud application integrations. Employees, partners, and customers get uninterrupted access to business critical applications.

Provisioning Users and Applications

Okta supports a group-based management system that can provision users to a set of applications based on job role as defined in Active Directory. If an employee were to switch roles within an organization, Okta will automatically update what applications the user has access to, based on changes to the employee record in Active Directory. As users depart, Okta detects the change to their status in Active Directory and automatically removes all access.

Okta offers pre-integrated provisioning to over 80 of the top SaaS apps, and enables identity mastering and provisioning of users using identity attributes from HR systems like Workday, SuccessFactors, and more.

Device-Aware Contextual Access Management

Okta Contextual Access Management reduces risk by managing how users and devices gain access to corporate resources. Through a combination of Adaptive Multi-Factor Authentication and Device Trust enrollment policies, Okta ensures only approved users and devices can access corporate-owned applications and data. With Okta, organizations can enforce granular access control to thousands of applications, and for the most commonly used devices. Okta Adaptive Multi-Factor Authentication lets an administrator choose whether to allow access, require step-up authentication, deny access, or restrict the scope of a user's access to certain applications. These decisions are based not just on passwords, security questions, and tokens, but on who the user is, what network or country they are connecting from, and what devices they are using.

Multi-Factor Authentication for ADFS

For customers who wish to continue using ADFS as their Identity Provider (IdP) to certain applications, they can still use Okta Multi-Factor Authentication to provide a strong method of authentication without having to build out additional on-premises MFA infrastructure.

Efficient Domain Consolidation

Okta's Universal Directory enables companies to connect an unlimited number of directories and bring legacy data to the web, with no need for AD forest trusts or opening firewall ports. For example, you may have an environment with multiple AD domains—some trusted, some untrusted. With Okta, you install an AD agent behind the firewall (two for built-in high availability) and Okta will manage these directories from a central admin console.

Logging and Reporting

Okta's unified dashboard makes it easy for IT to view status of users, access, and applications, and generate reports for compliance.

Always On, Always Up-to-Date

Okta was developed with our customers in mind and provides new updates to the product regularly with zero downtime. End users can access the applications that have been provisioned to them through a

[3] https://help.okta.com/en/prod/Content/Topics/integrations/adfs-okta-int.htm

central application portal. A similar solution via ADFS would either need to be manually created in-house or outsourced to another company—further increasing company costs.

Okta is a software as a service (SaaS) platform that provides all the benefits of ADFS—and the other Microsoft tools needed for a complete SSO solution—in a single cloud-based platform.

Cost Benefits

As shown in Figure 4, ADFS incurs several costs: hardware and software installation, maintenance, custom integrations, licensing for virtual machines, Enterprise Mobility + Security (EMS) and Microsoft Identity Manager (MIM) software. There's also the opportunity cost of losing months of productivity due to the time required to get it all up and running.

Installation, maintenance, and custom integrations still add cost, even when EMS is bundled in for free. For organizations with existing ADFS, they may still have to pay for installation and license costs for MIM and EMS to support advanced features.

Okta's minimal customization requirements and license management capabilities can save organizations up to 60 percent in total cost of ownership. The cost for Okta never increases with new applications; therefore corporations will see larger savings as they continue to add cloud applications to their infrastructure.

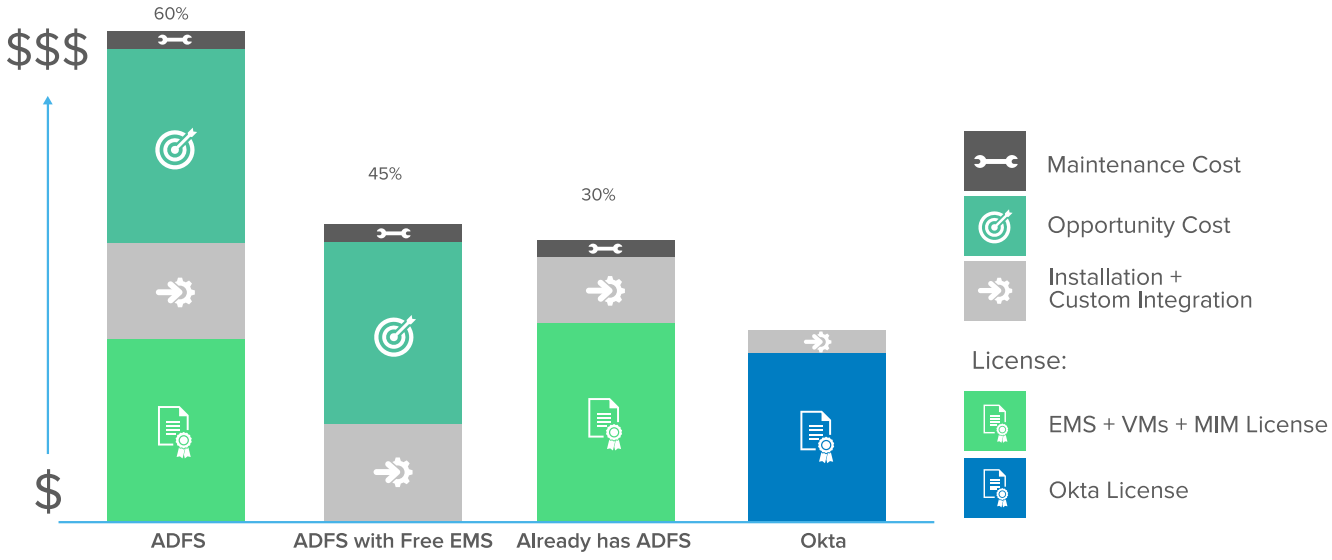

Figure 4: Relative ADFS costs for one application integration

Okta versus ADFS Quick Comparison

Metric	Okta Approach	ADFS Approach
Application Integrations	• Thousands of pre-integrated applications • No need to configure and maintain application integrations	• IT Admins build and maintain each integration
Availability	• 100% multi-tenant solution • Always-on with zero downtime • No changes required to AD infrastructure	• Must configure, install and manage • Required maintenance as applications evolve • Availability redundancy • Requires multiple servers (installation and failover)
Access and User Management	• Control access to all your applications • Easily map different username formats • Easily add, change or remove users and access • Import directly from AD, security groups • Automatically configured for all integrated applications	• Must create and manage custom AD attributes • Every application may require changes • No concept of user importing, matching
Reporting	• Dashboard of metrics to see overall health of users and applications • Easy access to user reports for compliance purposes	N/A

Getting Started with Your Free Trial

To discover how easy it is to deploy Okta and to begin securely scaling your cloud-based applications, visit www.okta.com/freetrial to get started today.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: www.okta.com


okta