okta

Removing the Identity Barrier for Office 365 Migrations

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

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

Introduction

How do you quickly connect Active Directory (AD) and all its user and group attributes to Office 365? This guide describes how Okta can help you avoid costly Active Directory consolidations and speed up your overall Office 365 migration without deploying costly on-premises servers.

Office 365's Identity Barrier

Migrating to Office 365 can present many challenges. One of the greatest is the problem of identity. How do you easily connect your existing users, groups and other Exchange/Lync information in Active Directory to Office 365, and keep it up to date? Active Directory environments can be complex and often contain incorrect or inconsistent data. If you are working with Microsoft or one of their partners to migrate to Office 365, you may be advised to go through a lengthy clean up or consolidation of Active Directory. Migrating to Office 365 requires you to understand and resolve issues with Active Directory—otherwise you can expect delays in decommissioning expensive on-premises systems. In the following pages, we will examine how Okta's cloud identity service can be used to accelerate and simplify your Office 365 deployment while increasing overall security.

Understanding the Challenges of Migration

Making the move to Office 365 presents two big hurdles: the first is data migration: of mailboxes in Exchange, and files in SharePoint. The second hurdle is identity management: dealing with the problems of authentication and keeping user and group information in sync with Active Directory.

Data migration

Moving the email and file data—often terabytes of information—over the Internet to Office 365 can be time-consuming and error-prone. Built-in migration features in Exchange, combined with free tools from Microsoft, do not always provide a speedy and trouble-free experience. Exchange infrastructure might need to be upgraded to current versions, further delaying the Office 365 migration. Because of these limitations, many third-party companies like BitTitan and SkyKick have evolved to simplify and speed up the process of migrating.

Identity management

The second challenge of identity has similar traits. Complexities in Active Directory are not always addressed with free tools offered by Microsoft, and they and require you clean up and fix data prior to migration. Just like the Microsoft built-in migration capabilities, the free identity tools also don't deliver a complete end to end IT admin or end user experience, making the long-term management of Office 365 difficult. Third party vendors like Okta have developed solutions that are more complete and easier to use. The identity problem can be broken down into four main areas:

- **Authentication.** Most IT admins wish to minimize the impact of moving to Office 365 on their users and let them authenticate to Office 365 using their existing Active Directory username and password.
- **User and group synchronization**. Active Directory has all the information about users, distribution and security groups. Copying and keeping this information up to date in Office 365 is critical, especially for Exchange migrations.
- **Automating creation of new users, and offboarding of existing/terminated users.** Once Office 365 migration is complete, there will be new people joining, leaving, and changing roles within the business environment. Changes to users' information and access to Office 365 must be immediately reflected in Active Directory.
- **Simplifying, yet securing access on mobile devices.** Many users want to configure tablets and phones for email and to access documents. This should be easy for users but also allow the IT administrator to increase the security, leveraging techniques like multi-factor authentication (MFA) and enforcing phone passcodes.

Okta provides a modern identity platform for modern email and collaboration platforms. Microsoft's tools, like ADFS and Azure AD Connect, do not deliver a true end to end experience for both the IT administrator and the end user. Worse, they were designed over 10 years ago based on old legacy architectures. These tools are not suited for the new cloud era and force compromises when it's time to deploy Office 365. This is why Okta developed a service to fill in the gaps and provide a more automated and complete solution.

While this document focuses heavily on using Okta for Office 365, Okta is a service that extends far beyond just this one application. Okta has the most mature cloud identity integrations for platforms such as Salesforce, Box, Workday, ServiceNow, Google Apps, Zendesk to name a few. There are more than 5,000 pre-integrated applications in the Okta Integration Network. To use Okta as an enterprise-wide Identity and Access Management (IAM) platform, large enterprise and public-sector customers require integration to a multitude of on-premises and custom applications. Okta provides several mechanisms across products to enable integration to these systems. Okta also has the most mature provisioning integrations, and a mature mobile access management platform that is integrated with identity. While this paper discusses Okta and Office 365 in detail, please keep in mind that Okta is a much larger identity platform that addresses a wide variety of use cases across many other services.

Okta was Born in the Cloud

Before we dive into the detail, we need to explain how Okta came to be the leading identity management service for Office 365. Okta was co-founded by Todd McKinnon, who was the vice president of engineering at Salesforce. Todd had intimate knowledge of how IT solutions were being developed in the new paradigm of the cloud. He knew that identity was going to be a big problem and decided to look at how to solve it from a new angle. Instead of basing his idea on existing on-premises identity management architecture, he wanted to build a cloud-first solution that could also be connected to on-premises systems without increasing the IT server footprint. People were moving to the cloud to get away from managing on-premises services, and Okta needed to provide a solution that fit in with that strategy.

Leveraging his experience at Salesforce, Todd built a team to design an identity solution where the majority of all the logic for enterprise identity would live in a massively scalable, always available, multi-tenant cloud service. He also wanted to ensure that everything was integrated, without multiple administrative portals, and delivered with a high-quality user interface—a consumer-grade experience for an enterprise technology. But, he knew that on-premises directories contained lots of information that is required to enable seamless access to a cloud application. Okta developed a completely new way of connecting the cloud back to the datacenter without having to deploy new servers with large-scale software to configure and maintain.

The result was Okta's identity and access management as a service—a clever approach to connect one cloud system to another, and also connect to on-premises identity resources. As we go through the rest of this guide, we'll highlight how this modern architecture benefits both Office 365 implementations and other cloud applications—and how to secure and connect them all together.

Authentication

The vast majority of Office 365 deployments are about migrating from the on-premises equivalent. The most common scenario is moving from Microsoft Exchange to Office 365. Exchange integrates heavily with Active Directory, and for many years IT administrators have invested massive time and effort in managing users and groups and other Exchange data in the directory. The main advantage for Exchange alongside Active Directory was a single username and password for authentication to Windows desktops and email. The Active Directory username and password were also used for many other business applications: file servers, finance systems, HR applications, and collaboration platforms. All these systems integrated with Active Directory, and with it, companies achieved a single sign-on (SSO) experience.

Office 365, however, is a SaaS application. After users are migrated to Office 365, each employee ends up with a brand-new user account in the cloud. You could just stop there, tell the user their new Office 365 login username and password—but lose the years of investment to achieve single sign-on in Active Directory. Users become frustrated because they now have to manage more than one password, and IT administrators become frustrated with disconnected environments.

Attempting to solve this problem of authentication using the Microsoft legacy technologies forces a choice among a few options:

- Implement Azure AD Connect and federate the authentication from Office 365 back to on-premises Active Directory using Active Directory Federation Services (ADFS)
- Sync the password hash from Active Directory into Office 365 using Azure AD Connect
- Implement Azure AD pass-through authentication (used with Azure AD Connect)

Active Directory Federation Services (ADFS)

ADFS is a powerful federation platform that authenticates Office 365 users to their Active Directory account by responding directly to the user authentication requests. You must configure and manage a network path from the internet to your ADFS servers, and from ADFS to your domain controllers. Network connectivity from the cloud, all the way into your Active Directory servers must be reliable. If anything fails, users cannot authenticate to Office 365.

ADFS Hardware Requirements

To deploy an ADFS solution, most companies end up with four new on-premises servers and network proxies and load balancers to configure. When there are multiple domains and forests, that number can climb dramatically and may require deployment of SQL server clusters. If you want to reduce costs by moving to the cloud, does it make sense to deploy more servers in your data center?

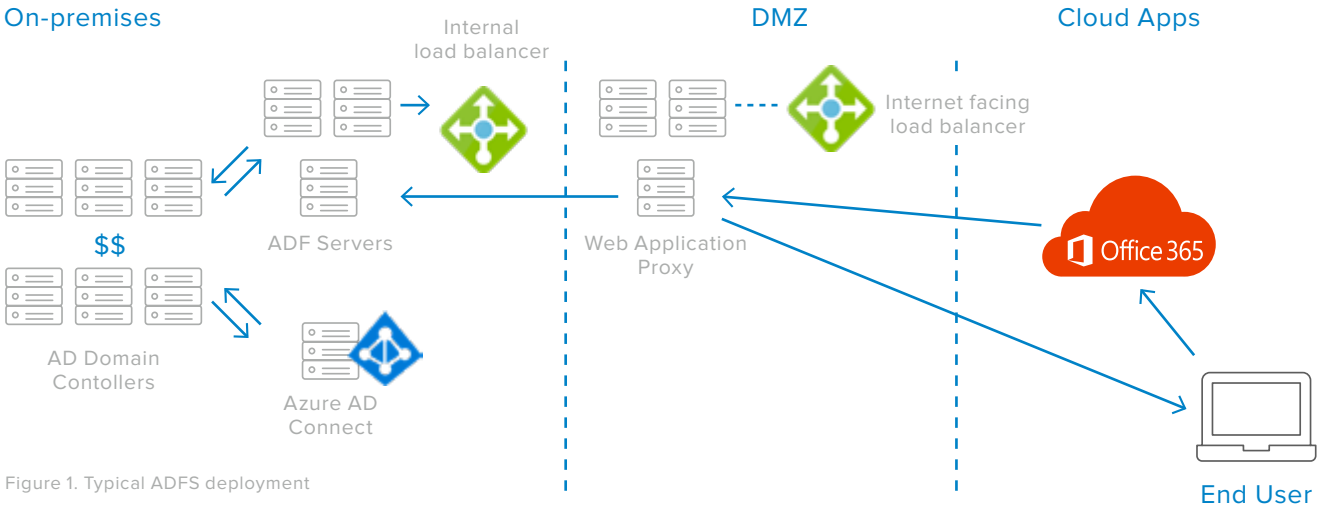

Figure 1. Typical ADFS deployment

Azure AD Connect

Microsoft offers an alternative to deploying ADFS, which is to use their directory synchronization solution, Azure AD Connect. Azure AD Connect also resides in your Active Directory domain, but it makes outbound internet connections to Office 365, copying your Active Directory data. There is no need to manage public internet traffic into your corporate network. However, your network must be configured to allow Azure AD Connect to communicate with all the forests and domains where user identities reside.

Azure AD Connect hardware requirements

Azure AD Connect requires you deploy a new dedicated server that connects to your Active Directory, copies the password hash, secures it again by hashing the hash, and then stores it in Azure Active Directory for Office 365. Azure AD then handles authentication requests directly, without federation. Often, this approach is called “Same Sign-On.” It may seem ideal for Azure AD Connect to store Active Directory password hashes in Azure AD, since it doesn’t require deployment of ADFS servers and infrastructure. But, using Azure AD Connect is a compromise.

ADFS, while complicated and expensive to deploy, brings the authentication immediately to the Active Directory environment. If you need to maintain multiple Active Directory environments, you can configure more ADFS servers. Azure AD Connect, on the other hand, is a single server with no automatic failover. Azure AD Connect's password synchronization option does not meet the security requirements for many organizations.

Pass-through Authentication

The newest option that Microsoft has introduced for synchronizing users to Azure AD and authenticating those users against Active Directory is Pass-through Authentication with Azure AD Connect. This is a much more lightweight SSO model than Active Directory Federation Services, as it does not require a large-scale server deployment. Although end users' credentials are validated against local Active Directory, Pass-through Authentication may not meet the criteria for larger customers, as it currently does not support deployments with untrusted Active Directory forests. Also, note that both ADFS and Pass-through Authentication depend on your Azure AD Connect server remaining up and running.

So, the choices here are not quite ideal. Do you invest in building out and maintaining a highly scalable federated identity service with ADFS? Do you lose the benefits of true single sign-on and deploy a single server to copy your password hash into Office 365? Or do you place your trust in a newer solution that has not been optimized for large-scale Active Directory environments?

Connecting Cloud to Active Directory with a Modern Lightweight Architecture

Okta bridges the gap between Active Directory and the cloud without requiring any of the extra servers or on-premises software. Like Azure AD Connect, Okta requires no network proxies or load balancers. There is no complicated certificate configuration, and there is no need to manage traffic from the public internet into the Active Directory environment. However, unlike Azure AD Connect, Okta does allow for automatic failover and real-time verification of user credentials to their Active Directory account—and can do so without requiring complex corporate network connectivity. How does Okta do this?

Okta looked at the functionality that resides in ADFS and Azure AD Connect and built a scalable version into our cloud service. Okta isn't running ADFS or Azure AD Connect. Rather, we've replicated the same features in our service on a modern cloud platform while using the same standard protocols and interfaces used by ADFS and Azure AD Connect. Office 365 users are not redirected to a login page hosted by your IT department, but instead to a cloud identity solution run by Okta. You get the same capabilities: ability to customize the login process, make access decisions about the authentication based on whether the user is in the office or out on the road, authorize users via multi-factor authentication, and authenticate to Active Directory. However, Okta manages the full deployment and service availability, and delivers reliability that outperforms anything you can deploy and manage yourself.

“Near Zero” On-Premises Footprint

How does Okta connect to Active Directory if all the directory synchronization functionality has been moved to the cloud? This is a critical difference in architecture. Okta installs lightweight agents onto existing servers in your Active Directory environment. The agents don’t have to be installed on your Active Directory Domain Controllers, although some customers decide to do so. They can be installed on any existing Windows server that is joined to your Active Directory domain.

Okta agents are installed in minutes, are less than 5MB in size, and run as system services. There is no need to create, set up, and configure new, dedicated on-premises servers or databases as with ADFS. The functionality in these agents is just enough to talk to Active Directory, validate user login information, and connect back to Okta. The local agents store only the connection-related configuration required to allow them to connect securely back to the cloud. The agent maintains an outbound connection to Okta over standard secure web protocols (SSL/HTTPS). A typical Okta customer has two, three or more agents installed in their Active Directory domain, but some customers have connected over 100 Active Directory domains to a single Okta tenant.

While not a focus for this document, it is important to also mention that Okta isn’t just about Active Directory. The same agent architecture that allows you to connect any V3 LDAP-compliant server to the cloud. Office 365 users can authenticate to LDAP and also use it as the source of information for Office 365 users and groups. Because Okta is a true identity management platform, you can mix both LDAP and Active Directory groups and/or users for Office 365. Okta also has a Java-based agent that our customers and partners have integrated with other on-premises systems like Oracle HR platforms and mainframes.

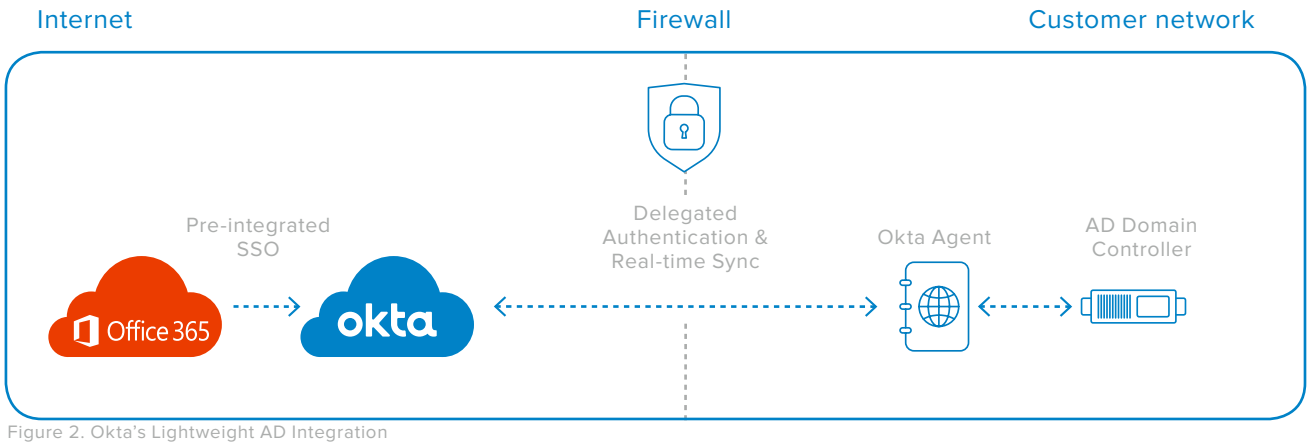

Figure 2. Okta’s Lightweight AD Integration

Preconfigured Office 365 Connectivity

Now that you understand how Okta connects to on-premises systems, let's discuss how the Okta cloud service connects to Office 365. Unlike ADFS, which requires you to set up certificates, review claims policies and expose the service to the internet, Okta has preconfigured the connectivity to Office 365 to help you easily set up a WS-Fed integration. Search the Okta Integration Network for the Office 365 app and add it to your Okta organization. By passing in only a few pieces of information—such as the Office 365 tenant name, domain you are going to federate, and an administrator username and password—Okta will automate the entire setup of federation for you. Okta's Universal Sync capability uses Azure AD Connect's SOAP API to synchronize Active Directory users, distribution groups and contacts to Office 365. The provisioning features in the Okta Office 365 application also allow you to assign licenses to any Microsoft Online service and assign roles directly from within the provisioning UI. Soon, Okta's enhanced offboarding capability will allow you to remove licenses for deactivated users.

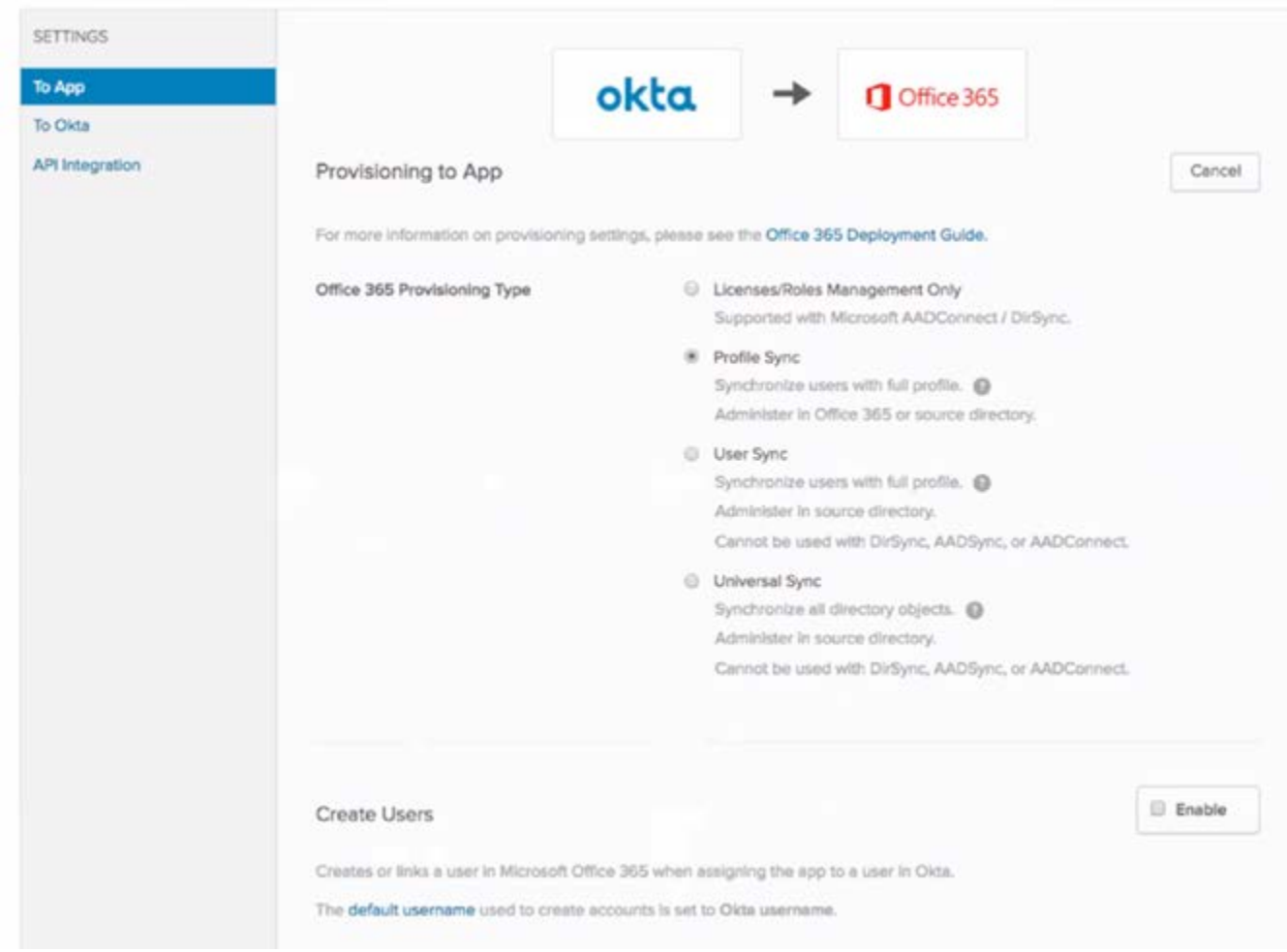

Figure 3. Office 365 Provisioning

Delegated Authentication

When a user attempts to access Microsoft Office 365, they are redirected to Okta for authentication. Okta's cloud service now has a pool of agents, all connected to Active Directory, that are ready and waiting. One agent connection is chosen automatically (and in turn connectivity to your Active Directory is load balanced by Okta), and user credentials are securely communicated down to the domain controllers where the agent validates it. This method is called "delegated authentication." Okta is the federation service for Office 365. For users who have an Active Directory account, we delegate that authentication back to Active Directory via our network of agents. If one of the servers on which an agent is installed is unavailable, Okta will automatically and transparently fail over to the next agent as long as there is at least one more agent installed. This automatic failover is transparent to both the end user and the IT administrator.

Okta + Office 365

Real time authentication to Active Directory	✓
Highly scalable	✓
Dedicated on-premises servers	✗
Deploys quickly with minimal identity skills	✓
Requires ADFS or Azure AD Connect for sync to Office 365	✗
Real-time reporting and monitoring	✓
Automated license management	✓
Auto-provisioning with HR systems	✓

Okta is truly a modern approach to identity, with an architecture that was built from the ground up with the cloud in mind. Unlike Microsoft's approach, Okta's agent architecture avoids the hassle of opening internet ports, proxying and load balancing user authentication traffic, and having to host the federation service. Okta's approach also means you don't have to copy your Active Directory password hash into the Office 365 service, because authentication takes place in Okta, delegated to your Active Directory. Okta is the best of ADFS, Pass-through Authentication, and Azure AD Connect.

Support for Office 365 modern authentication (ADAL)

For many years, Office 365 only supported WS-Federation authentication to Office 365. While the WS-Federation protocols worked fine when Office 365 was accessed via a browser, they presented a problem with software clients such as Microsoft Outlook or the native email clients on iOS or Android devices. These "thick" clients use WS-Trust, a less flexible method of authentication which required the software client to have specific knowledge about the login process. With the significant increase in the use of multi-factor authentication, these clients don't know how to work with the variety of MFA methods. They either ignored the MFA step, required complex, long, application-specific passwords, or they broke and were unable to authenticate a valid user.

Microsoft, therefore, updated its own Office clients to use the new Azure Active Directory Authentication Library (ADAL, or sometimes known as “Modern Authentication”). ADAL is a proprietary set of Microsoft software libraries that allow a thick client to embed a browser into the authentication phase. By doing this, the identity provider being used for authentication can present any type of authentication flow and therefore implement MFA. As an identity provider on the Azure AD federation compatibility list, Okta partners with Microsoft to ensure the Okta service fully supports this new method of authenticating to Office 365.

Directory synchronization

Solving the authentication challenge is only half of the problem. In most migration scenarios from your on-premises Exchange environment to Office 365, part of the data you are migrating are email contacts, distribution lists, and all the identity information about users which is stored in Azure Active Directory (Azure AD). IT administrators want to make use of existing security groups in Active Directory to control permissions to different areas of Office 365. Therefore, you need to copy this data from Active Directory into Azure AD. This is not a one-time copy when you migrate, but a constant sync of identity information between Active Directory, Okta, Office 365, and Azure Active Directory. Depending on the deployment model chosen for Office 365, you may be required to manage security groups and users in your Active Directory environment, and any changes you make need to be quickly reflected in Azure AD.

Turning once again to the Microsoft tools, Azure AD Connect is the common choice for directory synchronization. Azure AD Connect is the lightweight version of a much larger identity management platform, Microsoft Identity Manager (MIM). Both Azure AD Connect and MIM are based on a 10-year-old on-premises meta-directory called Microsoft Identity Integration Server (MIIS). A meta-directory is essentially a database with connections to different data sources like Active Directory or Office 365.

On top of this database is identity management software that maintains information about users, groups, and so on. This server regularly communicates to all the connected systems, gets updates and transfers changes to Office 365 and Azure AD. Vendors like Microsoft, IBM, Oracle, and CA have been using this approach to identity for over a decade. It’s an old architecture that requires maintaining lots of software in your on-premises IT environment.

Timeline of Microsoft sync tools

Azure AD Connect is the evolution of an on-premises product designed back in 1999. While the name of the software has changed, and improvements been made, the underlying architecture is exactly the same.

1999 Microsoft Metadirectory Server
2003 Microsoft Identity Integration Server
2007 Microsoft Identity Lifecycle Manager Server
2009 DirSync
2010 Microsoft Forefront Identity Manager
2012 Windows Azure Active Directory Synchronization
2014 Microsoft Azure AD Sync Services tool
2015 Azure AD Connect
2016 Microsoft Identity Manager

Handling the complexity of Active Directory

If you have a more complex Active Directory environment, Azure AD Connect struggles, and you must upgrade to the bigger Microsoft Identity Manager (MIM). This upgrade isn't free and requires you to purchase both software and consulting services to deploy. MIM deployments require a minimum of 1-2 months and result in 2-4 new servers you need to maintain.

As mentioned previously, having to deploy new servers in your IT environment when you are migrating to Office 365 doesn't make sense. The advantages of Office 365 are about moving away from hosting your own services, not deploying more servers. If you combine the requirements of directory synchronization with the footprint of ADFS, at a minimum there will be 5-6 new servers to run and maintain, and in most cases, the number is higher.

> "The advantages of Office 365 are about moving away from hosting your own services, not deploying more servers."

For very complex Office 365 environments, Okta is significantly simpler to deploy and maintain

A very common problem in an Office 365 migration is how to handle the synchronization of username—more specifically, the User Principal Name (UPN) to be created in Office 365. The UPN requires a domain that is public on the internet, for example, simon@okta.com. However, many Active Directory environments are built with private, non-public DNS domains that cannot be used on the internet, resulting in usernames like simon@okta.local. Therefore, the integration from Office 365 to Active Directory must figure out how to map the AD user with an invalid username to a valid Office 365 format. This mapping can be done in Azure AD Connect, but it's limited. MIM allows for total control, but is costly to configure, deploy and manage. Once again, Microsoft is forcing you to make a compromise.

Domain consolidation

If you have many complex environments, Microsoft will recommend you consolidate your different Active Directory domains into a single forest. But, this isn't always possible. It can be very costly for such projects and some companies outsource the IT management of their Active Directory environment, which means many change requests and statements of work. To avoid consolidation, customers could use MIM and replicate all the data from the different Active Directory environments into a single, new Active Directory forest. Azure AD Connect would then be used to sync this data to Office 365. This can take months and result in yet more new servers deployed in your IT environment.

Deploy Office 365 6x faster using Okta

We have seen customers spend 18-24 months attempting to get ADFS, Azure AD Connect, and Microsoft Identity Manager (MIM) to work for identity federation, domain consolidation, high availability, automated onboarding and offboarding, and licensing for Office 365. They turned to Okta when they realized they could support all of these requirements out-of-box and get it all done six times faster.

With Okta, an admin can import existing users and groups from AD and LDAP into Okta Universal Directory. From there, they can control both inbound and outbound profile attributes, and transform, manipulate, and apply logic to ensure that data is clean and reconciled during the process.

Organizations can use Okta to connect an unlimited number of directories, consolidate users and groups from untrusted forests, and synchronize them all to a central Active Directory. Okta will manage these directories from a central admin console. Once the user is authenticated to the AD domain, Okta will authenticate them into the cloud and to the applications they need.

Provisioning from HR Systems

The challenges of synchronizing user and group information into Office 365 is not confined to on-premises systems. Active Directory has traditionally been the place where the enterprise stored all information about users, but that is becoming obsolete. Companies are migrating other on-premises services to newer cloud solutions, like HR systems (Workday, BambooHR). They want to source the Office 365 usernames from these cloud applications, get the user's phone number from solutions such as RingCentral, and device information from Samanage. How do you connect all this information together into a single, up to date profile, and provision to Office 365?

You can't use Azure AD Connect because it doesn't connect to any cloud service other than Office 365. MIM requires the expensive and time-consuming development of that connectivity. This is a great example of how these older architectures struggle with the new concepts of cloud computing, and how Okta can ease the pain of investing in on-premises resources.

Okta for Office 365 is more than just authentication and synchronization

Okta isn't just about authentication and provisioning—it's about the full identity lifecycle for Office 365. Azure AD Connect will create users in Office 365 from Active Directory, but those users cannot use Office 365 services until they are licensed. Typically, you either use the Office 365 portal to assign licenses to users, or you create PowerShell scripts that you run or schedule.

Okta hosts all services for you, you can quickly take advantage of other features with only a few clicks. For example, if you need to add multi-factor authentication (MFA) to your Office 365 login process, it is simple to enable an MFA policy once for your Okta org. All subsequent logins will be secured with a second factor—there is no extra work required.

Group-based license assignment

It is easy to allow access to Office 365 for only a certain subset of your users. The Active Directory groups have already been imported via the Okta agents. Simply assign the relevant groups to the Office 365 app in Okta to control who has access to login to Office 365. You can now control who has access to Office 365 by simply managing group membership in Active Directory. Okta even has rules-based groups, so you can manage Office 365 access based on attributes. For example, everyone with the employeeType set to "Full Time" is automatically provisioned to Office 365.

Automated and granular license management

Okta presents you with all licensing and role management options directly in the application assignment UI. This removes yet another manual and disconnected task from your Office 365 deployment. When Okta licenses users, you can also specify specific services in each Microsoft Online license a user gets. This can be done based on groups, or for more granularity, you can also make assignments directly to a user. Those groups can be sourced from Active Directory, native to Okta or imported from other systems like an LDAP server, Workday or Box. For example, you could assign Microsoft E3 licenses with only Exchange and Lync enabled for your Sales team, while your Support team gets an E3 license with SharePoint Online enabled.

Automation for end users

Automation isn't just for the IT admin. Okta can also make the life of the end user much easier. When joining a company for the first time, users in the modern workplace want to access email on their own personal devices. Okta simplifies their Office 365 account setup. Users simply download Office 365 app onto your mobile device and authenticate to Okta. Combined with the automated provisioning and license management, your company needs to do only a few initial tasks, such as create a user in Active Directory and assign them to a group, and Okta will automate everything else. The final result is that the new employee can easily gain access to Office 365 within a matter of seconds of your IT group initiating the process.

MFA done differently

Now that you've moved your on-premises Exchange, SharePoint and Skype for Business workloads into the cloud, you want to increase the security of users accessing this data. The most effective and immediate way to do this is by implementing a second factor of authentication, more commonly known as adding Multi-factor Authentication (MFA). MFA introduces something other than your username and password into the authentication phase, by actions such as sending you a code via SMS to your mobile device, or by asking you to confirm or deny an authentication attempt via an app on your smartphone.

Office 365 bundles in a subset of Azure MFA features as part of the Office 365 subscription, so what does Okta do with MFA that is better?

Okta has powerful groups membership rules. This means you can derive group membership in Okta based on things like user attributes from Active Directory and other sources. MFA is enabled via group membership and is enforced by policy. You don't need to go and specify each user that should be prompted for MFA. Instead, you create a policy that defines when MFA should be applied and assign groups to that policy. If you create a new user in Active Directory and you use the "Domain Users" group in your Okta MFA policy, they are automatically going to require MFA for login. No extra IT admin intervention required. And MFA policies can be applied at either an application level, or at the Okta org level, depending on when you want your users to be prompted for MFA.

Okta's policy engine allows your increased flexibility and granularity in setting MFA policies and integrates with a large variety of third-party MFA vendors. If your employee is accessing Outlook via a browser and they do so from your company headquarters, they've usually passed some physical security measures, such as key cards to open doors. Therefore, you can relax the MFA enforcement for these circumstances. Unlike Okta, Office 365 doesn't give you these controls in their free version of MFA.

Okta access policies go beyond just the enforcement of MFA. You can ensure that certain groups of users can only access Office 365 resources only from specific networks. Okta's MFA policies can be fine-tuned on a per-application basis. So, you might want to enforce MFA for Office 365, but not for Zendesk.

Some customers have long recognized the value of MFA and have already deployed a solution from another vendor. Okta has no preference of the MFA solution you want to use with Office 365, therefore you can integrate our cloud service with RSA SecurID, Symantec VIP, YubiKey, and other cloud MFA vendors like Duo Security.

A Modern Cloud Identity for your Modern Cloud Applications

In summary, Okta was built from scratch with the cloud in mind, creating the concept of identity and access management as a service. We focus on automating many of the IT administrator's tasks, while simplifying end users access to Office 365. All of this is delivered with an architecture that doesn't impose old, legacy technology in your data center. Okta customers comment that we deploy Office 365 six times faster than estimates that included the use of ADFS and Azure AD Connect.

Not only do we care about the IT administrator and end user, but we care about the data and its security. We handle Office 365 authentication for companies like Adobe, Bose, Clorox, Post Foods and many more. We are very focused on security and have specialized teams analyzing and monitoring the security of our system on a daily basis. In the same way you chose Office 365 because it's more feature rich, less hassle to run, cheaper and more secure than the on-premises equivalent, Okta is the same logical choice for identity.


okta