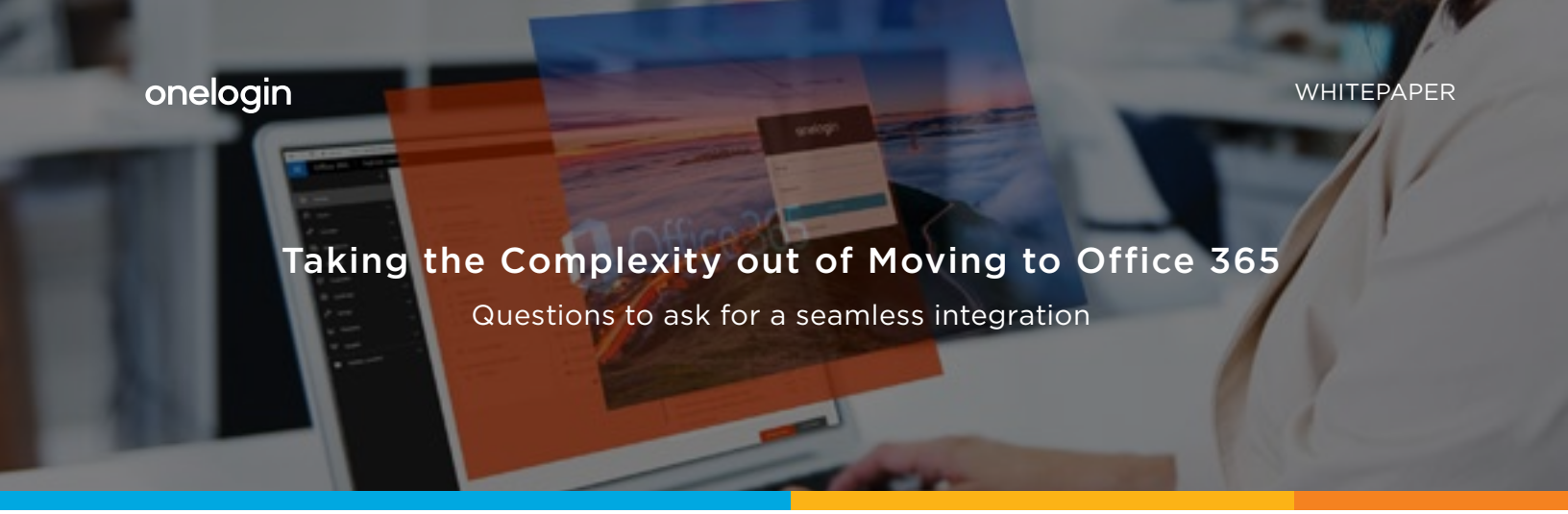

Taking the Complexity out of Moving to Office 365

Questions to ask for a seamless integration

Many organizations have begun their push to the cloud with a handful of applications. Microsoft's Office 365 offering is the driving force for many, but getting to the point where Office 365 is seamlessly integrated and ready for use is no small project.

Ask yourself and/or your vendors the questions below and understand the impact on your organization. By doing so, you'll be in a good position to choose the best way for your organization to integrate Office 365 with Active Directory and enable secure single sign-on across web, Outlook and mobile email clients.

PART 1

WHEN CONSIDERING THE MICROSOFT SOLUTION SET

Microsoft has a rapidly evolving platform for cloud identity management that centers on its Active Directory brand. Below are a few questions to ponder as well as some FAQs that pertain to implementing a 100 percent Microsoft-based solution.

1. WHICH COMPONENTS OF MICROSOFT'S CLOUD IDENTITY ARCHITECTURE WILL I NEED FOR MY ORGANIZATION?

At a minimum, Office 365 will require the deployment of Azure Active Directory, Azure AD Directory Synchronization appliance (aka DirSync) and Active Directory Federation Services (AD FS). The top two premium Azure AD editions include a license to Microsoft's MFA Server (for multi-factor authentication). The MFA Server can also enable VPN integration and RADIUS support.

Organizations with larger directories will need a full version of Microsoft SQL Server to handle the Azure AD Directory Synchronization database. Do you have more than one Active Directory forest? If so, then synchronizing multiple forests with Microsoft's native solution set requires a custom deployment of Forefront Identity Manager (FIM) or Microsoft Identity Manager (MIM). Designing and deploying FIM or MIM for this purpose generally requires the use of specialized consultants plus the added burden of ongoing maintenance. If you only have one AD forest but want to sync with an additional LDAP directory then you'll also need FIM or MIM.

2. WHAT'S INVOLVED IN DEPLOYING AD FS AS A HIGH AVAILABILITY SERVICE?

As you may know, the service level agreements (SLAs) that cloud hosted services like Office 365 offer are a moot point if the AD FS infrastructure that brokers logins to these applications and services isn't running at the same service level (or higher). Highly available AD FS is primarily predicated on load balancing multiple sets of servers. For organizations with advanced requirements, SQL Server or a SQL Server cluster may be required to take advantage of advanced AD FS features like token replay detection and SAML artifact resolution. When AD FS is deployed in geographically dispersed data centers, then a global traffic management solution will be needed to manage requests across data centers.

3. WHAT TYPE OF EXPERTISE WILL I NEED TO DEPLOY AD FS AS A HIGH AVAILABILITY SERVICE?

The dependencies above add several layers of complexity to AD FS, and require collaboration across multiple teams. For example, in many enterprises, load balancers and global traffic management solutions (i.e. F5 Global Traffic Managers or Cisco Global Site Selectors) are generally managed by dedicated networking teams. SQL Server may require support from a database administration team, and the addition of SQL Server clustering will add a dependency on a storage management team as well.

4. WHAT'S THE DIFFERENCE BETWEEN AZURE AD AND AZURE AD PREMIUM?

While many of the basic directory and federation features are available for free in the basic edition, the features that make Azure AD a competitive cloud identity management solution are licensed via premium editions. These are licensed on a per user basis (as of the time of this writing $6 to $9 per user per month) and include premium features for each user. The premium feature set of Azure Active Directory is focused around branding and customization, group-based access control, self-service password management, multi-factor authentication, and advanced reporting—with identity protection and PIM available in the Premium P2 edition.

5. WHAT IS AZURE'S RELIABILITY AND UPTIME?

Microsoft Azure has had its share of incidents resulting in significant downtime affecting large numbers of users. For example, in 2018 the "South Central US" incident affected large numbers of users, including those well beyond that particular region, and data. In April of 2018, users across Europe were affected by Azure and Office 365 login issues. If you don't want to be reliant on Azure availability, having a local AD instance or one separate from the Azure cloud is a good idea.

PART 2

WHEN CONSIDERING INDEPENDENT IDENTITY AND ACCESS MANAGEMENT (IAM) VENDORS

Due to the challenges with Microsoft's native solution set and the hybrid nature of organizations today, most enterprises are looking at independent identity and access management systems. These turnkey solutions deliver rapid cloud identity management and SSO to Office 365 without the overhead and setup complexity of maintaining an AD FS infrastructure and related components. The best of them provide unified access management, using a central cloud directory to integrate with Active Directory and other directories and provide a single tool for managing identity and access to both cloud and on-prem applications. Below are some questions you should consider or directly ask any third party vendor vying for your business.

1. IS AN ON-PREM OR CLOUD-BASED IDENTITY MANAGEMENT SOLUTION THE RIGHT OPTION FOR MY OFFICE 365 IMPLEMENTATION?

Independent vendor solutions come in two main deployment models: on-prem and cloud. The cloud model offers compelling cost and security efficiencies across multiple dimensions, including patterns in infrastructure, greater automation, and discipline in process. Cloud-based identity management solutions take full advantage of these efficiencies, but is that enough for you to go cloud rather than on-prem for your Office 365 deployment?

Clearly, the more that is happening beyond your corporate firewall, the more it makes sense to put identity in the cloud as it provides an innately more centralized control point for managing identities across all apps and devices, independent of access location (Office for Surface anyone?).

In addition to Office 365, consider your rate of adoption of additional cloud apps, how and where users will be accessing corporate applications and data, and your propensity to develop your own web apps accessible beyond your firewall.

2. WHAT OTHER PIECES OF INFRASTRUCTURE OR TOOLS WILL I NEED TO INSTALL, CONFIGURE, OR MAINTAIN OFFICE 365 WITH YOUR SOLUTION?

This is especially important to understand with a cloud-based IAM solution. After all, one of the key benefits of going with cloud IAM is to avoid the complexity of managing disparate pieces of software, hardware, and tools. Most cloud-based solutions will require an agent that sits behind your corporate firewall to securely sync back with the identity provider and out to cloud apps like Office 365. Beyond that, will you need to install a separate tool to enable Desktop SSO.

You should also ask whether you'll still need to use additional tools like DirSync to enable synchronization with Active Directory or whether the vendor provides a direct AD Azure integration. Similarly, will you need to install and run PowerShell or setup and configure any other services outside of the vendor's solution to make it work with Office 365.

3. DOES YOUR SOLUTION SUPPORT MULTI-FOREST TOPOLOGIES?

Smaller firms with less complicated directory infrastructures may never need to support more than one Active Directory forest with Office 365. However, if you do have multiple ADs and forests then make sure your vendor supports this requirement. If they do support it, be sure to ask if any additional infrastructure is required.

4. DOES YOUR SOLUTION SUPPORT MIXED DIRECTORY TYPES?

Many enterprises have LDAP or cloud directories like Workday and Google Apps. Is your vendor's solution capable of creating a meta-directory from mixed directory types and presenting them as one unified cloud directory to Office 365 and other cloud apps?

5. IS YOUR ACTIVE DIRECTORY INTEGRATION WITH OFFICE 365 BATCH OR REAL-TIME?

Real-time directory integration means that all directories are updated whenever changes are made in one directory with the changes propagating through to connected services like Office 365 within seconds. This not only saves a tremendous amount of time and effort, but also acts as an effective "kill switch" for when employees leave the company. This is critical in order to eliminate backdoor access to Office 365 through protocols like IMAP.

Unless the user is immediately disabled, unwarranted access can occur. If the vendor's directory synchronization is batch and you are comfortable with that, then what is the default synchronization interval? Can this interval be shortened? If so, what are the implications on your infrastructure? Any scalability issues in synching at shorter intervals?

6. HOW EASY IS IT TO DEFINE A LOGICAL STRUCTURE FOR OFFICE 365 ACCESS THAT DOESN'T CORRELATE EXACTLY WITH ACTIVE DIRECTORY GROUPS?

Will you ever need to manage Office 365 access outside of your on-prem Active Directory model? Today, many businesses are hiring temporary workers and external consultants. For example, let's say you have an external graphic designer. If she was an internal employee, she would belong to the marketing group in Active Directory. However, you only want the contractor to have access to a subset of the internal marketing team's applications, including Office 365. Furthermore, you want to impose stricter security policies for outside consultants then you would for regular employees.

Rather than having to modify Active Directory and create a whole new permission structure that supports this requirement, you might find it helpful to be able to do this in the identity management solution—outside of AD. This is one of the key benefits of a unified access management (UAM) system.

7. WERE THERE ANY EXCEPTIONS WITH REGARD TO YOUR "WORKS WITH OFFICE 365" VALIDATION?

For each vendor, Microsoft does single sign-on interoperability tests across three sets of clients and then notes any exceptions. The three clients are:

- Web-based clients such as Exchange Web Access and SharePoint Online.
- Rich client applications such as Lync, Office Subscription, CRM.
- Email-rich clients such as Outlook and ActiveSync.

If the vendor has exceptions to their support for one or more types of clients, then how will these impact your Office 365 deployment? For example, if the vendor doesn't support Desktop SSO (Integrated Windows Authentication) with SharePoint Online and your employees often access SharePoint while on the corporate network then what friction will that cause in the way they work? Does the vendor require the setup of additional on-prem infrastructure that you'll have to maintain? If so, how will that affect the complexity of your network, maintenance overhead, etc.?

8. WHAT AUTOMATIC AND MANUAL OPTIONS FOR OFFICE 365 USER PROVISIONING DOES THE VENDOR OFFER?

Automatic user provisioning allows a large user base to be quickly paired up with Office 365 licenses without having to manually update each user individually. Does the vendor's automatic user provisioning capabilities allow you to create custom mappings based on Active Directory Groups as well as define role-based access to Office 365? Can you preview how users will be affected by your user provisioning mappings? Can you use the user management capabilities within the identity management solution or will you have to disable those capabilities when integrating with Office 365? Will you need to use any additional tools in order to automatically sync users?

In terms of manual Office 365 user provisioning, can you do this within the vendor's solution or are you limited to simply importing users from Active Directory? Do you have to sync your identity management solution with Office 365 and then carry out a separate sync with Active Directory?

9. DOES THE VENDOR SOLUTION HELP WITH LICENSE MANAGEMENT?

Currently, Microsoft does not offer easy user license management. One of the benefits of a third-party, centralized identity and access management system, such as UAM, is better license management. Does the vendor make it easy to report on active Office 365 users based on provisioning and deprovisioning? Does it enable you to implement delete versus disable policies, which is important because disabled users still incur licensing costs?

About OneLogin

OneLogin is the leader in Unified Access Management, Enabling Organizations to Access the World™. Businesses of all sizes use OneLogin to secure company data, while increasing IT administrator and end user efficiencies.

Implementation of our identity management solutions can be achieved in hours rather than days, delivering a fully featured administrative and self-service portal. Our ability to handle on-premises and cloud/SaaS applications makes us the identity-as-a-service vendor of choice for the hybrid enterprise. Multi-factor authentication, mobile identity management for one-click access on smartphones and tablets, and real-time directory synchronization all add an extra layer of protection. For more information, visit www.onelogin.com, Blog, Facebook, Twitter, or LinkedIn.

Contact us to learn more about OneLogin.

https://www.onelogin.com/company/contact