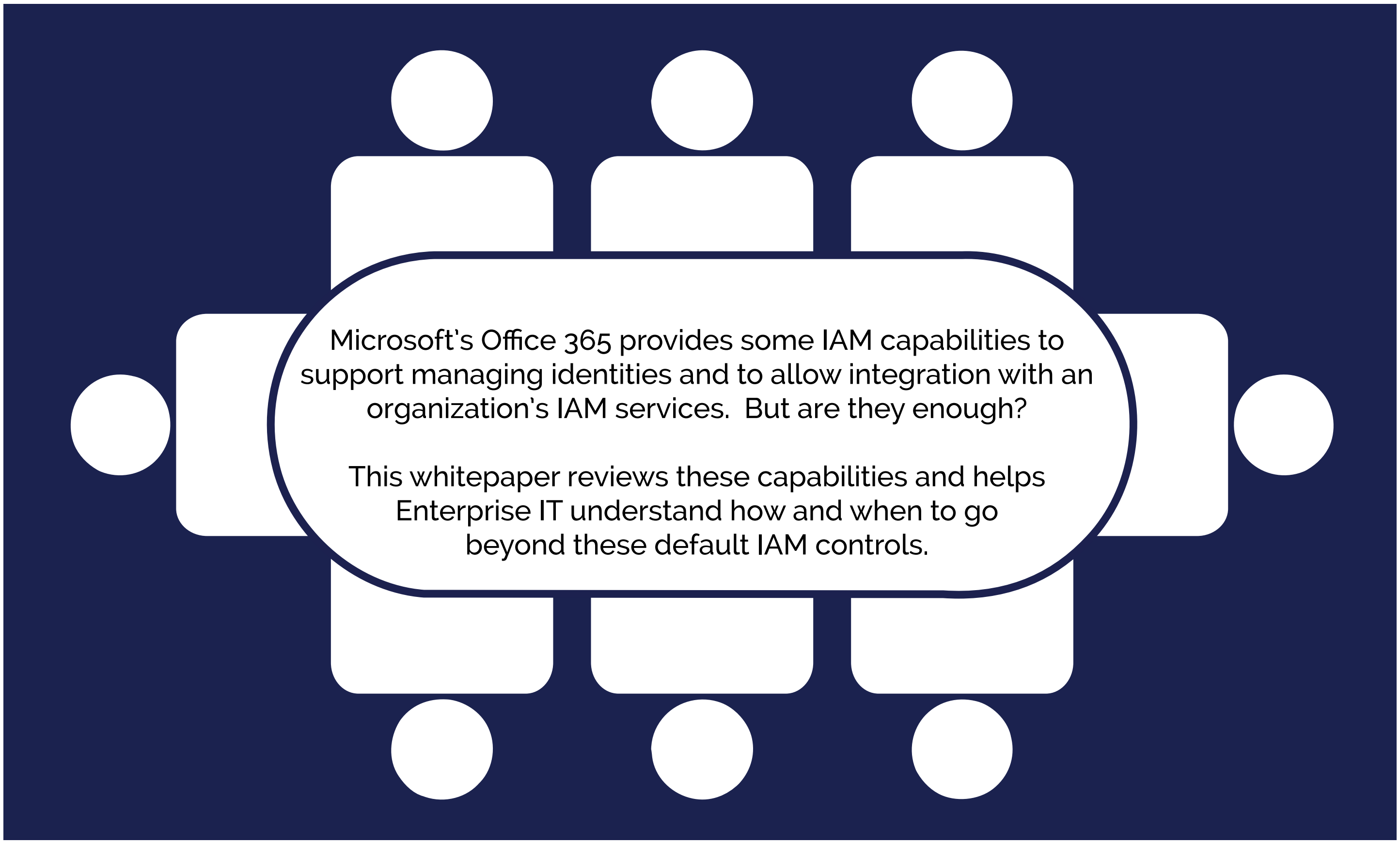
XMS SOLUTIONS

IAM for Office 365: When To Go Outside The Box

IAM Best Practices

version 1.0
August 2016



Microsoft's Office 365 provides some IAM capabilities to support managing identities and to allow integration with an organization's IAM services. But are they enough?

This whitepaper reviews these capabilities and helps Enterprise IT understand how and when to go beyond these default IAM controls.

TABLE OF CONTENTS

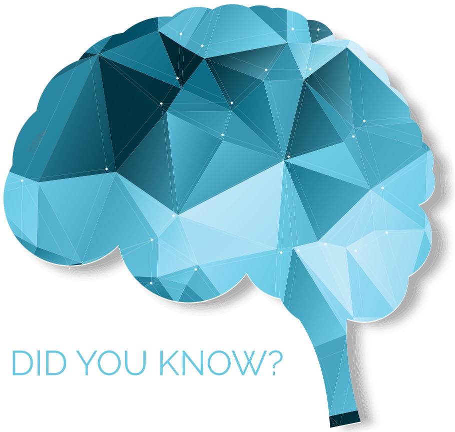
IAM For Office 365: When To Go Outside The Box

INTRODUCTION

In a Gartner survey conducted in early 2016, 78% of the enterprises surveyed indicated that they are using or planning to use Office 365, up from 64% in mid-2014.

Office 365 includes a subset of functionality that is part of Microsoft's broader IDaaS offering, Azure Active Directory (Azure AD) Premium.

Given what data is moving to Office 365, IAM should be the first line of defense. Consider the risk of employees downloading data from the cloud. Microsoft supports device registration with adaptive access with ADFS. If a device is not on the list, can you can enforce multifactor authentication to verify the user's identity?

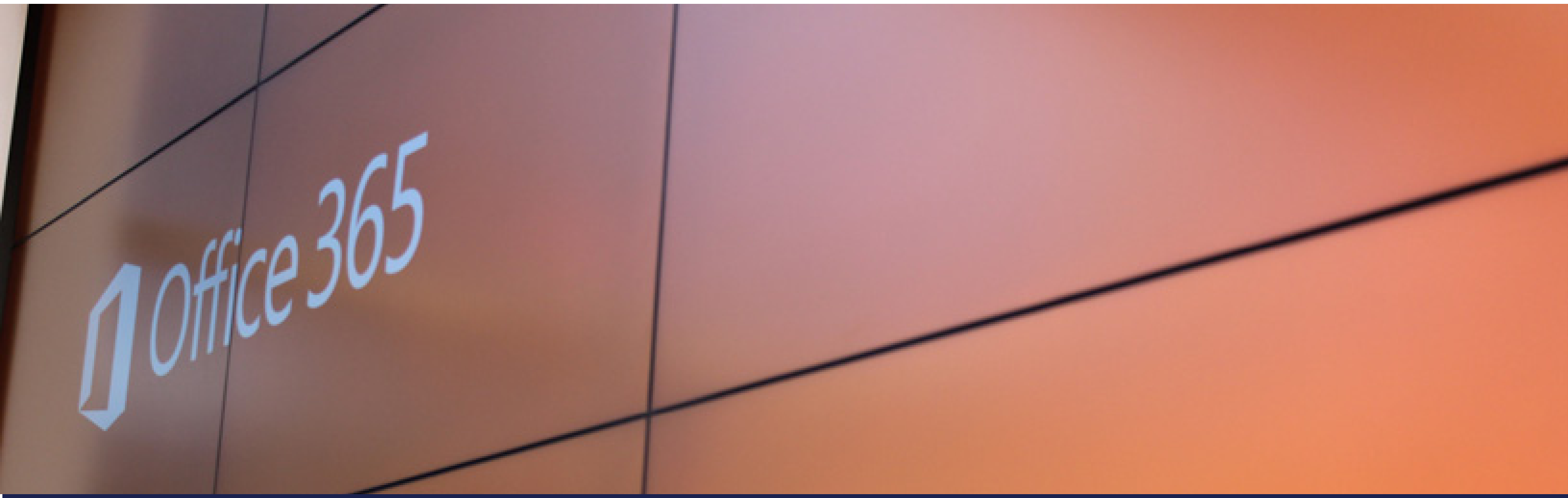


Through 2018, less than 25% of organizations using Office 365 will use the basic IAM features included with the licenses to manage IAM for other applications.

Like any other SaaS application, Enterprise IT will manage identities within Office 365 independently from on-premises applications. Leveraging the out-of-the-box Office 365 IAM capabilities will be a satisfactory solution for certain types of companies.

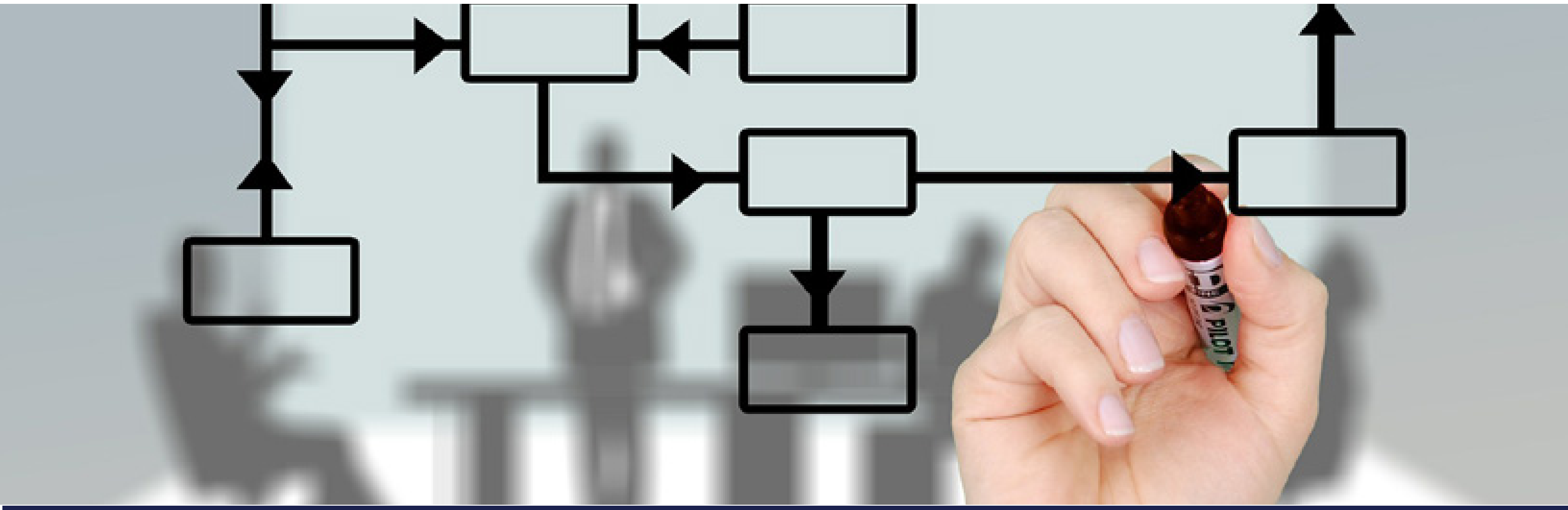
Others may extend on-premises IAM deployments to support identity administration, access enforcement and single sign-on (SSO) for cloud office implementations. Further, several companies are now embracing IDaaS (think SailPoint, BeyondTrust, etc) as an IAM broker, fully integrated with Office 365.

This whitepaper will define base Office 365 IAM features, helping you define your requirements and identify the appropriate level of IAM for your organization.



Office 365 Native IAM Capabilities Overview

IAM FUNCTION	CAPABILITY DETAIL
Password Management	Azure AD Connect synchronizes passwords between Azure AD and onpremises AD. Administrators can also reset passwords, but will need to upgrade to Azure AD Premium for writeback of passwords changed on Azure AD to on-premise AD.
Identity synchronization from on-premises directories to Office365	Windows PowerShell and Azure AD Connect Licenses must be enabled in a separate step following synchronization. No ability to sync updates in real time based on a change of identity in AD.
Cloud directory for identity administration of Office 365	Capability Present with API exposed. Allows administrators to administer identities directly in the service, and the APIs are for developers and IAM vendors to access the directories for query and provisioning operations.
Identity provisioning to on-premises applications, databases and directories	Supports provisioning to systems that support the System for Cross-Domain Identity Management (SCIM) v2 standard.
Authentication	Multi-Factor Authentication (MFA) for Office 365 does not include advanced features that come with Azure AD Premium and EMS, such as customization of voice and SMS prompts, fraud alerts or granular administrative control over MFA.
SSO to service based on authentication to enterprise directory or on-premises access management	SAML for browser-based SSO, and Web Services Federation Language (WSFederation) and Web Services Trust Language (WS-Trust) support to provide SSO for Microsoft rich clients from enterprise owned or third-party federation capabilities.
SSO to third-party cloud apps	SAML, OIDC and password-vaulting-based SSO for up to 10 apps per employee. Azure AD Premium is required to get the application proxy for access to on-premises Web apps.
Identity Governance	Not Provided
SSO to On-Premise Apps	Not Provided



STAYING IN THE BOX

Making the decision to leverage default IAM controls in Office 365 is a relatively straightforward one. Basic requirements include:

- Accounts are created for each user, users are authenticated to the service before use
- Add users to service quickly, remove access when no longer needed
- Basic authorization enforcement functions to appropriately limit what users can do within the apps, as well as provide basic reports or data to review administration and access events

If you have Active Directory (AD) as the authoritative identity store, have no third-party IAM tools, and wish to extend AD for user provisioning and SSO functions, Microsoft AD FS for authentication and SSO may be sufficient. However, if your requirements include access to applications beyond Office 365, or access to on-premise applications, you may need more than these default capabilities.

KNOW WHEN TO EXTEND

Securing Office 365 can be complicated, and the right level of planning is necessary to avoid time-consuming pitfalls and the introduction of security risks. For companies with mature or pre-existing IAM tools and teams, extending those solutions to Office 365 is a common tactic.

However, every organization must complete a series of common high-level tasks to ensure a successful deployment. If you using this tactic, leverage these best practices.

EXTENDING EXISTING IAM TO OFFICE 365

Synchronize on-premises directories with the Office 365. Leveraging existing IGA tools or a virtual directory server (VDS) with connectors for Office 365 offers a better level of integration. VDSs are good for complex on-premises environments where attributes are spread across heterogeneous repositories.

Enable licenses for users with O365. Extend on-premises access management federation capabilities (such as AD FS, PingFederate, or SecureAuth IdP using SAML) and other standards as needed to get users SSO that will support the primary use cases.

Ensure that third-party authentication methods previously implemented or planned as alternatives to passwords will work with the cloud office application through your access management/federation capabilities. For example, third-party authentication methods may not work properly in conjunction with pre-2016 versions of Microsoft rich clients, such as Lync or Outlook, and when the user's device is not domain-joined to the corporate AD.

Incorporate administrative and access event report data from Office 365 into on-premise security and event reporting used for other applications.

Ensure that the exit process for deprovisioning users includes cloud office license management.

WHEN IN ROME: CLOUD-BASED OPTIONS

The proliferation of SaaS applications for the workforce, combined with ongoing lack of IAM functionality on-premises or lack of staff to manage IAM functions, have been strong drivers for organizations to adopt IDaaS rather than extend existing IAM implementations.

IDaaS represents the quickest route to provide IAM functions for SaaS and, even on-premises, Web apps. Also, some companies with existing IAM implementations and the staff to manage them are choosing IDaaS as an extension strategy to support SaaS.

IDaaS vendors develop and maintain provisioning, authentication and SSO integrations for SaaS applications so customers don't have to. This provides faster time to value for application integration than most organizations can provide for themselves.

XMS SOLUTIONS: PROFESSIONAL RECOMMENDATION

Manage Privileged And Non-Privileged Accounts With BeyondTrust/ SailPoint IdentityIQ Integration

IT teams need to address three critical questions around user access. Identity and access management (IAM) solutions help IT teams answer 'Who has access to what?'

But, in order to achieve complete user visibility, privileged access management solutions address the remaining questions: 'Is that access appropriate?' and 'Is that access being used appropriately?'

XMS Solutions partners with two leading IAM vendors to answer these questions: SailPoint and BeyondTrust. SailPoint is a recognized industry leader in IGA, perenially appearing in Gartner's Magic Quadrant. BeyondTrust was recognized by Forrester as a global leader in privileged access management, serving over 4,000 customers worldwide.

Leveraging BeyondTrust Password Safe version 6.0 with SailPoint IdentityIQ, customers can leverage a dynamic, bi-directional certified integration allowing them to effectively manage user access for both privileged and non-privileged accounts.

This integration gives organization a single solution for the management and security of asset data, privileged and non-privileged users, and associated functions by role including assessments, auditing, rule creation, and reporting.

CONCLUSION

Organizations with more than very basic IAM needs should look beyond the default controls that come with Office 365.

If Office 365 apps are the only ones in scope for your IAM needs, then congratulations- your path is relatively clear and you should use the native features and functionality.

If IAM is viewed as a core function for your organization, current products are meeting your needs, and staffing and cost considerations are in line, extend your current deployment.

However, if you are focused on time and cost savings, or if you desire a solution that reduces workloads for internal IT, consider IDaaS to bridge existing IAM implementations or support new applications.

ABOUT XMS SOLUTIONS

For nearly 10 years, XMS Solutions has served Enterprise IT departments worldwide.

As a leader in collaboration, messaging and directory services, we saw how the distributed workforce, BYOD trends and growing demands for the cloud and data impacted our clients.

The scale of IAM will massively increase.

Gartner projects that, by 2020, across all organizations globally, IAM will span billions of people, tens of billions of things, and tens to hundreds of trillions of relationships.

The rush of new people and things accessing collaboration systems enhanced employee productivity and customer integration- but also created new kinds of risk around scale and security. Our architects and delivery teams continued to design and deploy high-performance Microsoft collaboration platforms for Active Directory, Exchange, SharePoint and Skype for Business, scaling through the cloud, on-premise or a mix of both.

However, as more users, devices and machines required access, directory and governance policies were no longer enough. As the need for system access and user privileges scaled, compliance and security couldn't keep up.
Our services have evolved with customer requirements around access, collaboration and security, focusing on identity-driven solutions that help the enterprise scale in a manageable and compliant fashion.

Our heritage in collaboration gives us a unique perspective on how systems are accessed, used and managed. Our partnerships give us the leading edge in designing, deploying and managing the best Enterprise IAM and Collaboration solutions on the market today.

Contact Us Today To Achieve Your Collaboration and IAM Goals

info@xmssolutions.com
702.940.6545