LIMOSS
London Insurance Market Operations & Strategic Sourcing

LIMOSS SSO - Azure Integration Options and Costs

Market Guidance Document

Market firms are advised to make their own assessment of which Azure solution is best for their organisation. LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Information correct As At August 2018

Contents

Market firms are advised to make their own assessment of which Azure solution is best for their organisation. LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Introduction

This document provides guidance to technical leads on the options available for managing Microsoft Azure. Understanding an organisation's Azure presence can be helpful when adopting LIMOSS SSO.

Overview

- Approximately 85% of the market have an existing Azure presence. These organisations should be able to adopt LIMOSS SSO with no incremental costs for users who are within their Cloud licencing.

- Organisations with no Azure presence have 2 options:

  i) **Free User Created Accounts** - User Created Microsoft Accounts- The Zero Cost Option.

  ii) **Simple Cloud integration** at a licence cost of <£9 per user per annum (or free with no SLA). These also enable Cloud use beyond LIMOSS.

- Azure adoption options are shown from the perspective of an organisation with no current Azure capability (Approximately 15% of the market). Costs mentioned would be incurred directly by the Market Participant in provisioning their Azure capabilities, not including TMEL/LIMOSS charging for LIMOSS SSO.

- Each adoption option outlined delivers benefits to the organisation (in addition to LIMOSS SSO integration) which are not reflected in this deck. These benefits may include:
  - Enabling increased resilience for Cloud Authentication
  - Enabling Single Sign On (SSO) to many global cloud services outside of LIMOSS
  - Cloud SSO is often the first step in migrating Line of Business applications to Cloud
  - Updating / modernising & licencing of Office tools, enabling later Office 365 options

- For additional support, please contact servicedesk@limoss.london.

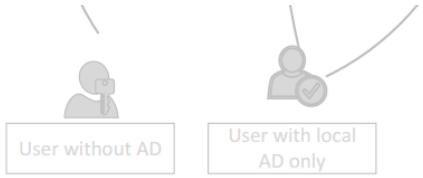
Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

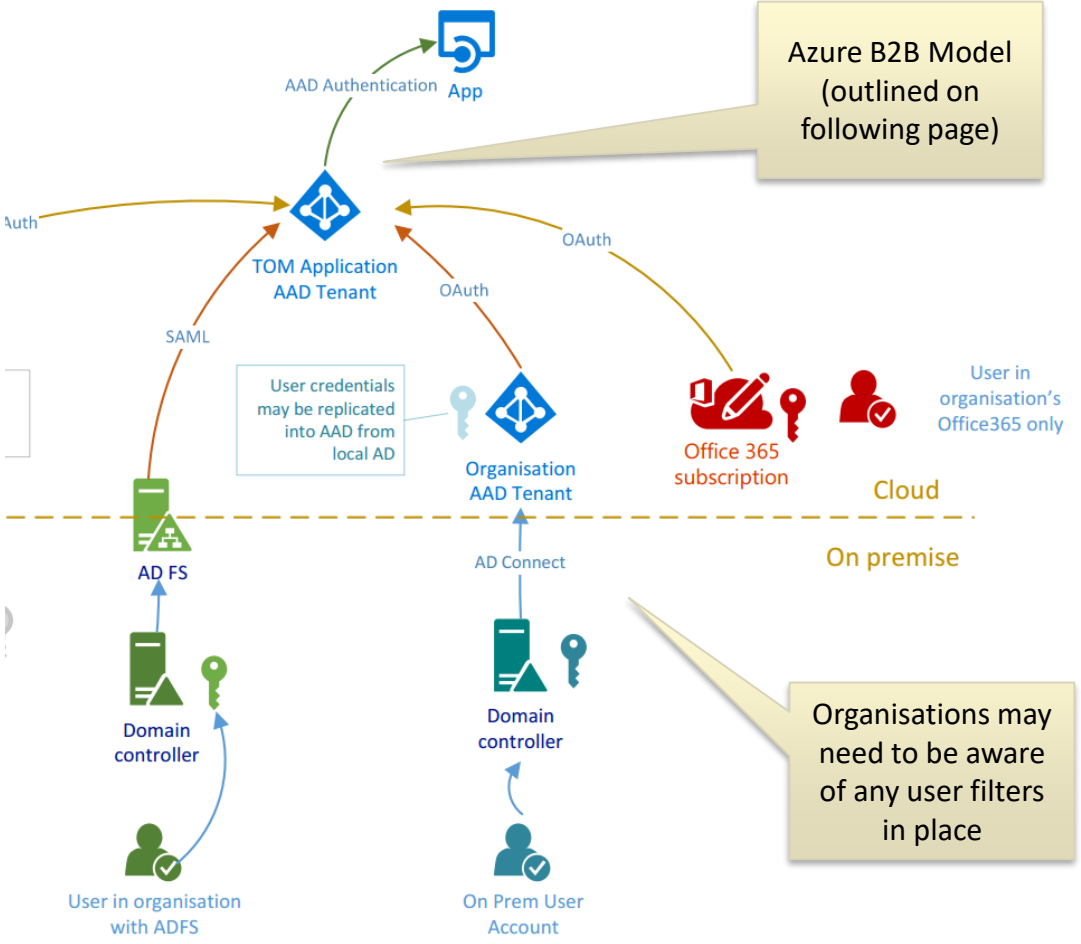
Existing Azure Presence

Scenarios for an Existing Azure Presence

Organisations that already have an Azure presence will follow one of the scenarios shown here. Typically, these solutions are chosen to allow hosting of applications in the Cloud, access Enterprise Apps (e.g. Salesforce), or utilise Office365.

Some users may not be aware they are using Azure services and may not have seen an Azure "login prompt" as part of their usage.





Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Existing Azure Presence – Guest Accounts

- If you already have an Azure presence, most of your users probably have “member accounts”. Members are fully fledged users of your directory (and other Azure services) and consume an Azure Active Directory (AAD) licence.

- Microsoft enables B2B collaboration in AAD using “guest” accounts. These are limited AAD users who are invited to join a host tenant in a partner organisation. In this case, LIMOSS SSO provides the host tenant.

- The “guest account” is a pointer to your own AAD tenant, where the actual authentication occurs. The user continues to use his/her own credentials and control of the AAD account remains with the partner organisation (e.g. password resets, disablement etc).

- Organisations who disable or remove guest accounts, will remove access to LIMOSS SSO services (after expiry of current login tokens).

- Guests are “invited” to join LIMOSS SSO by sharing their email and Full Name. For existing Azure users, we can add guests without sending email invitations. This requires IT to permission an Azure “Guest Inviter” account. Please email servicedesk@limoss.london and ask about “LIMOSS SSO Guest Inviter” to find out more.

- Your organisational Licence is valid for this guest account (no increased licence charges apply to any party).

- Account “Expiry” (of temporary accounts) is not reflected in Azure AD when using AD Connect. If you have significant and frequent use of temporary accounts, consider scripting automatic account disablement based on expiry (disabled status is synchronised).

Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

No Existing Azure Presence

Summary Table of Options for Organisations Adopting Azure

The table below shows the 5 key options discussed in this guide.

Option	Adoption Complexity	Existing User Credentials used ?	New Infrastructure Requirements	Incremental Cost
1: User created Azure Accounts	N/A (no actions required)	No	None	None
2: AD Federated Services[1]	High	Yes	6 + Servers Azure Subscription	6+ Servers, Network change, implementation + Ongoing Support
3: AD Connect – Hash Password Sync	Low	Yes	1 Virtual Server Azure Subscription	1 non-critical VM + £0.74/user/month[2]
4: AD Connect – Pass Through Authentication	Medium	Yes	2-3 Virtual Servers Azure Subscription	1 non-critical VM, 2+ "Cloud Critical" VMs + £0.74/user/month[2]
5: Office365[3]	Ensure all LIMOSS SSO users have an Office365 licence/account	Yes, (Office 365 Credentials) which may differ from those used on site depending on implementation	None	None

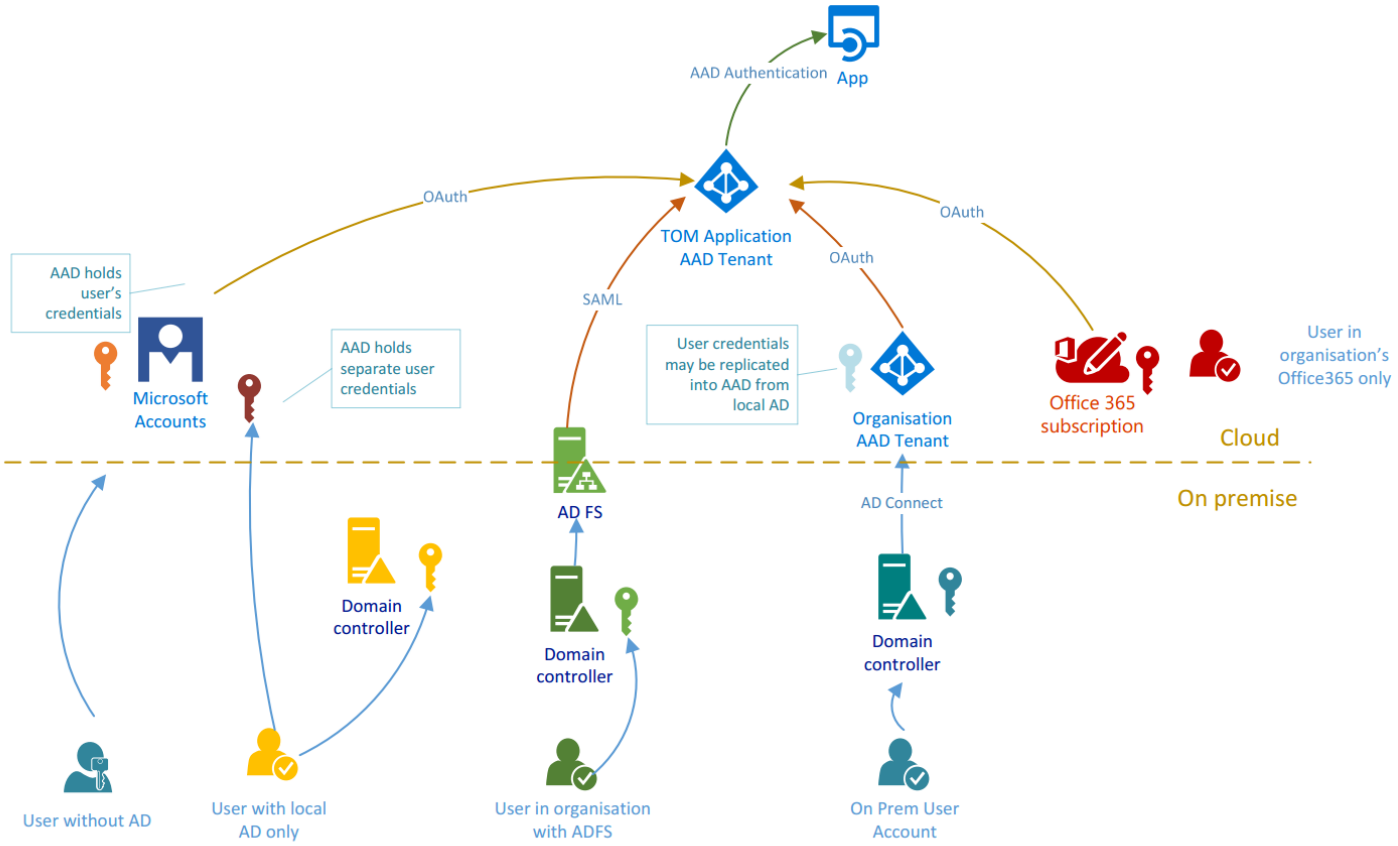
NOTES:

- [1] Organisations do NOT require the complexity of ADFS as a solution to LIMOSS SSO Integration. In the context of this deck in identifying options for organisations with NO existing Azure presence this scenario is very unlikely (as it would represent a move from "no cloud" to "highly sophisticated cloud-security integration")
- [2] FREE Azure user licences are available, but include no Service Level Agreement (cost options incl. 99.9% availability commitment). Organisations who choose to synchronise accounts to the Cloud will have positioned themselves well for Office365 adoption (the primary direction of the MS Office Roadmap).
- [3] AD licences are included in Office365 licencing.

Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Summary Graphic of Options for Organisations Adopting Azure

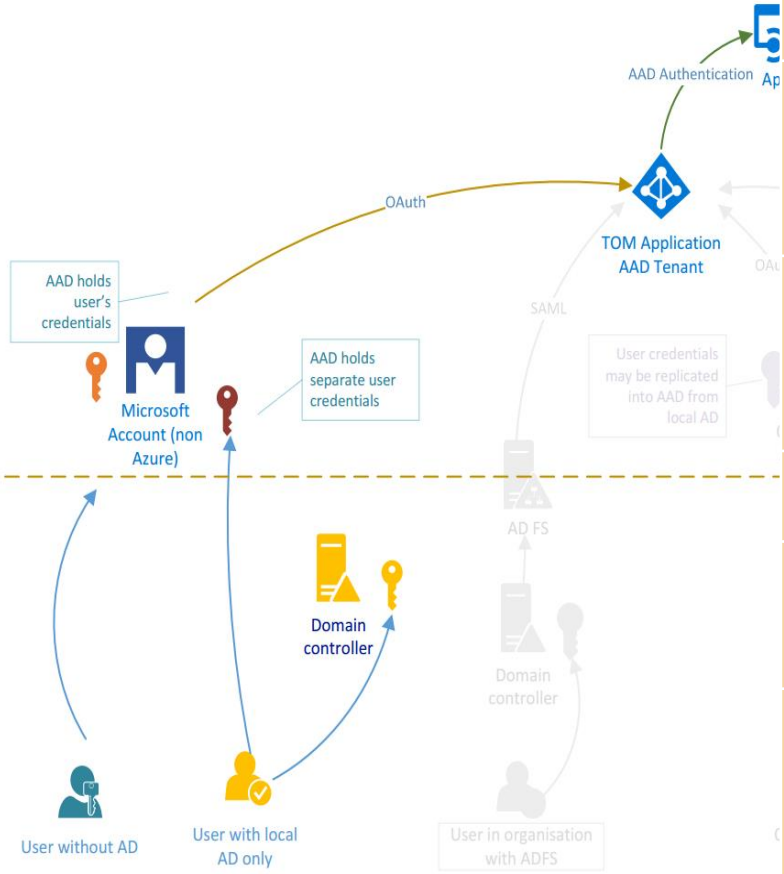
The 5 key mechanisms for creating a User's presence in Azure are shown in the graphic below:



Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Option 1: User Created Azure Accounts - The Zero Cost Option

- This option allows use of LIMOSS SSO with NO adoption cost or account synchronisation.

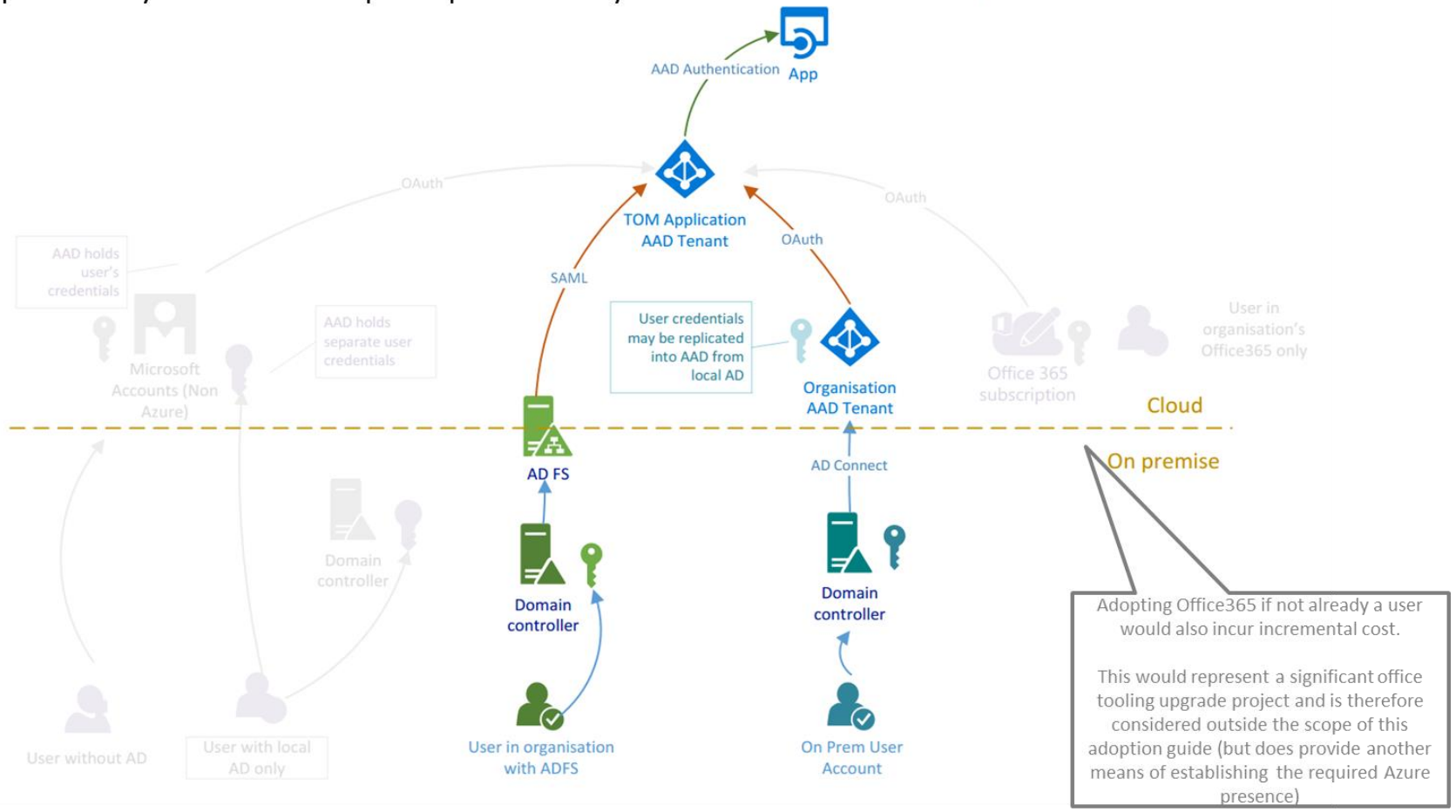


Individually Managed Azure Accounts	
Description	• Market participants can allow their users to create new Microsoft accounts following an invitation from LIMOSS SSO. • The end-users create their own passwords, and can use their existing name@organisation.com as the user name (if the organisation has not reserved their domain in Azure)
Suitability	• Organisation has no AD presence, and a "No cost" solution is required for LIMOSS SSO SSO • The organisation has AD on-prem, but is undecided on the best mode of Azure Integration (this is the easiest / least impactful model from which to change to the others)
Utilises User's Existing Account	• No. One new account is created per user to access all LIMOSS applications
New infrastructure	• NONE. No Synchronisation of this account or password takes place with any of the account details held "on-site" (Onboarding process requires user to have access to the account email)
Administration	• The Market participant will not be able to remove or disable the account directly, but it will be removed from the LIMOSS AAD tenant by Service Request. • Removing the account from LIMOSS's AD tenant removes access to ALL integrated Applications. • Password resets can be performed by the user within simple Azure-provided screens.
New Cost Items	NONE

Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Options 2, 3 and 4: Costed Options for Organisations with No Existing Azure Presence

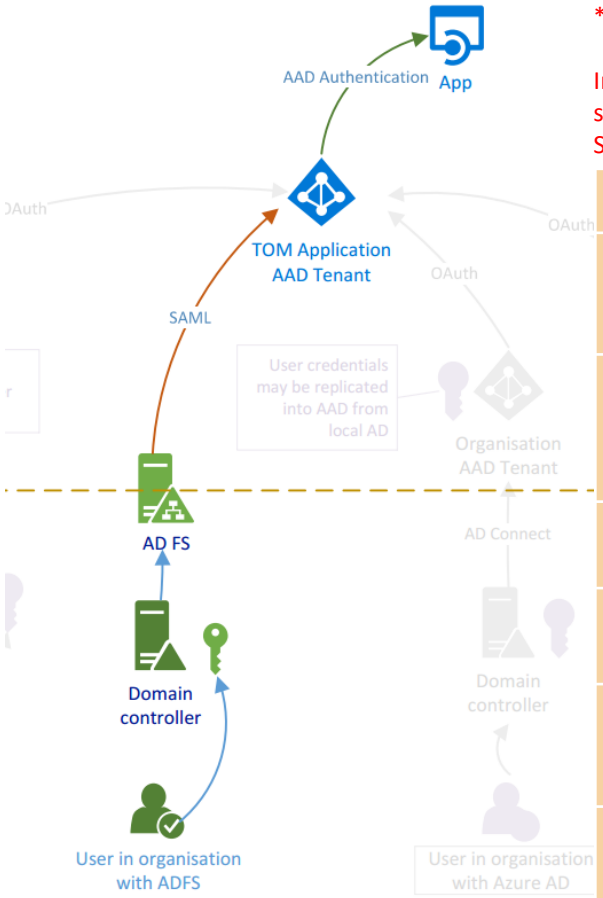
- For an organisation with NO existing Azure usage, options 2, 3 and 4 will incur incremental cost.
- Each option brings additional benefits to the organisation
- Some organisations may choose one of these options rather than the 'Zero cost' solution of Option 1.
- Approximately 85% of market participants already use one of these solutions.



Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Options 2 : Active Directory Federated Services (ADFS)

- ADFS is mainly used by organisations with complex requirements for Cloud-based authentication.
- This solution is unlikely to be suitable for organisations that do not have any Azure presence.



*NOTE: Organisations do NOT require the complexity of ADFS to access LIMOSS SSO.

In the context of this deck (identifying options for organisations with NO existing Azure presence) this scenario is very unlikely as it would represent a move directly from "no Azure" to "most sophisticated Azure Security integration"

Active Directory Federated Services (ADFS)	
Description	• ADFS "federates" an organisation's existing Active Directory (on prem or in any hosting centre) and usually results in part of the company AD running in the Cloud • Authentication requests are "handed off" from the Cloud to another authentication service (e.g. on Premises AD, or third party IAM tools)
Suitability	• Organisations have complex or unusual security requirements (e.g. requiring use of smart-card identity for login, or mandating on prem Multi-factor login for cloud apps) • ADFS will probably only be the preferred option where an organisation already has carefully planned it having identified complex requirement for it on their existing roadmap • **NOT recommended where the requirement is solely the adoption of LIMOSS SSO**
Utilises Users Existing Account	• Yes
New infrastructure	• COMPLEX. ADFS requires significant, infrastructure which must be resilient • New components are critical to cloud login, so are deployed with redundancy and high availability
Administration	• Account administration remains in organisation's own control • Significant increase in administrative burden to manage federation to Azure AD • Removing the account from LIMOSS's AD tenant removes access to ALL integrated Applications. • Password resets continue to be performed in Organisation's own solutions
New Cost Items	• 6+ Servers, Network Zones and Firewalls required (min. 2 of which in Azure Tenant) • Licencing for Windows Servers (likely to be with Enterprise Agreements) - No licence required for ADFS itself • Significant Incremental operational overhead managing *critical* ADFS infrastructure • Azure AD licence (Basic = £0.74 / user /month); Free account available with no SLA

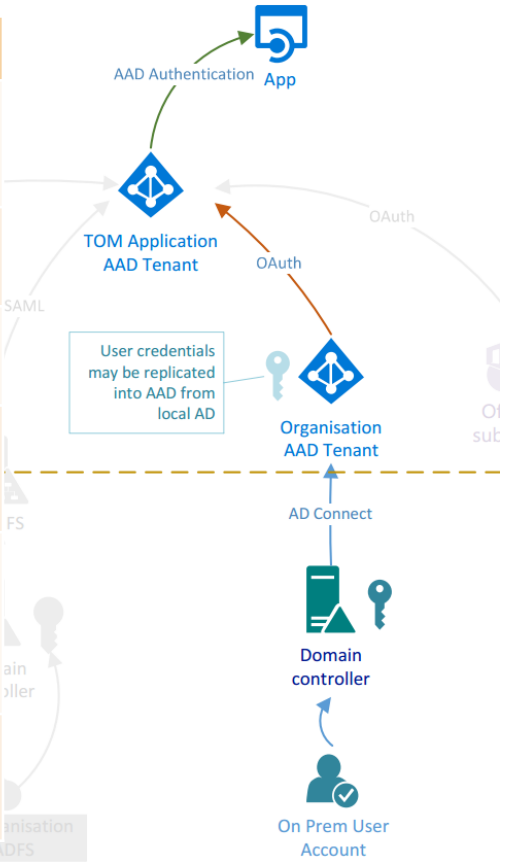
Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Option 3: AD Connect – "Hash Password Sync"

- Microsoft's simplest option for integrating On-Prem accounts to Cloud Applications hosted in Azure (both LIMOSS and Industry-Wide).

- "Hash Password Sync" option securely synchronises a hashed (non-reversable) version of account passwords to the Cloud.

AD Connect "Password Sync" Option	
Description	• Market participants can synchronise accounts for use in the Cloud (and also gain resilience in ability to sign into Cloud based resources during local infra outages) • Cloud authentication requests are handled in Azure • Note : Account / Password *expiry* are not Sync'd, though Account Disabled Status is).
Suitability	• Organisation wishes to provision low complexity Single Sign On in the Cloud and retain control of user accounts • Enforces password policies (passwords are only reset on existing infrastructure)
Utilises Users Existing Account	• Yes
New infrastructure	• A licence-free AD Connect Agent is deployed on site (in existing AD Servers or a new virtual server). This infrastructure is used only for account synchronisation (not authentication), so does not need to be as resilient as other options . • Azure Tenant (Free)
Administration	• Password resets and account maintenance "on prem" is unchanged. Password Policies are still enforced • Disabling an account will remove LIMOSS SSO access on next sync cycle (on average in 15mins ; sync interval default 30 mins) • Service Request removal of LIMOSS guest account requested as "housekeeping" and extra security
New Cost Items	• Deployment of a non-critical virtual server to host AD Connect, • Azure Basic AD Licence @ £0.74/user/month (Free accounts available though with no SLA) • MFA optional (billed through LIMOSS)

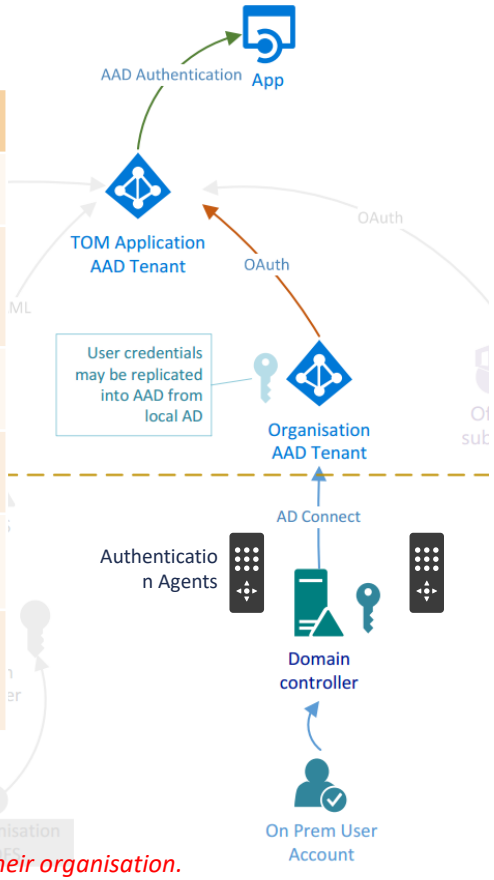


Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Option 4: AD Connect – "Passthrough Authentication"

- Providing an enhanced mode of AD Connect , "Passthrough Authentication" option does NOT synchronise passwords in any form.
- Authentication requests are confirmed with on site / existing AD infrastructure via "Authentication Agents" on each login.

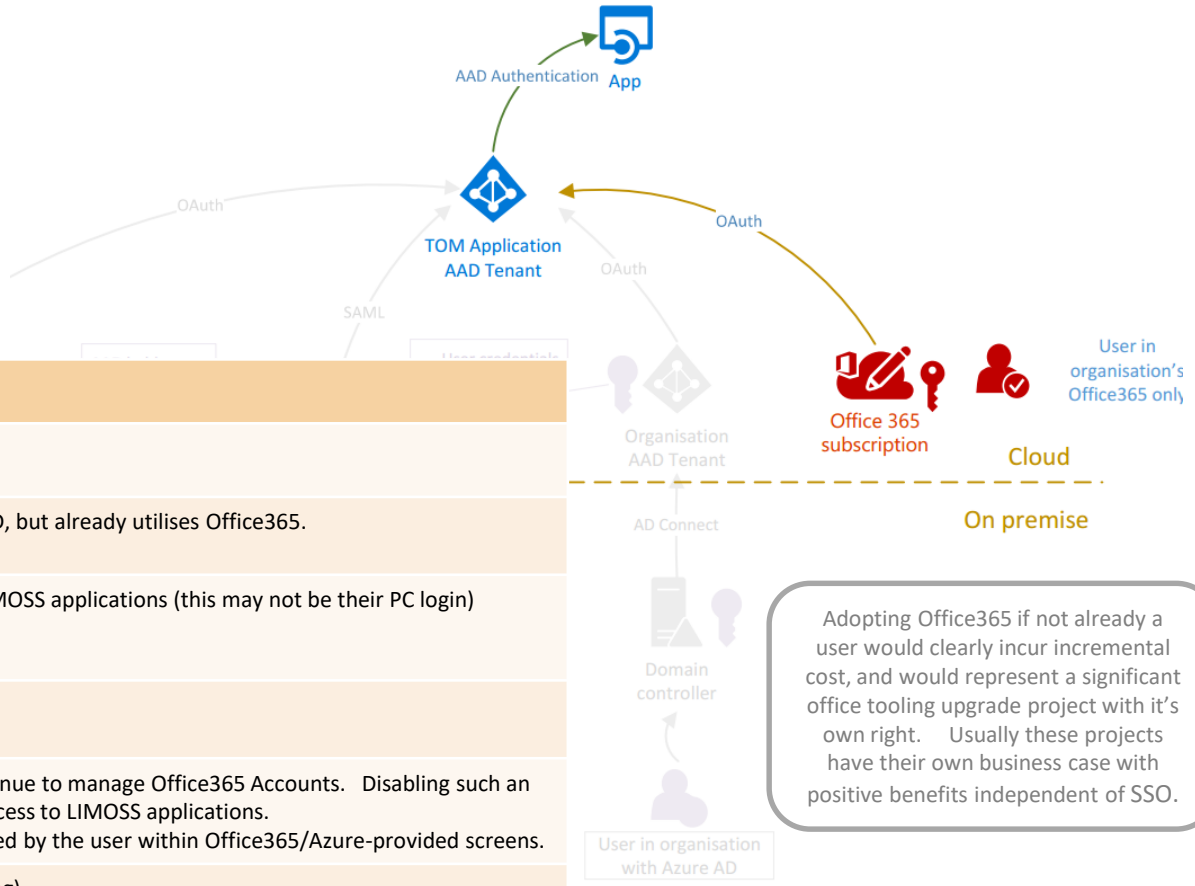
AD Connect Passthrough Authentication	
Description	• Market participants can synchronise accounts for use in the Cloud • Cloud authentication passed back to the organisation
Suitability	• To eliminate delays in "Account Disable" taking effect, and/or ensure Password Expiry/Account Locked status automatically in effect for Cloud logins • To restrict login hours or check on apply conditional MFA requirements (e.g. MFA needed if logging in from …..) • The organisation does not wish to synchronise passwords to the cloud (even in secure hashed form)
Utilises Users Existing Account	Yes
New infrastructure	Medium. In addition to AD Connect "non critical" sync infrastructure, authentication agents are required to handle requests from the Cloud (outage impact = user inability to sign into Cloud applications)
Administration	• Password resets and account maintenance "on prem" is unchanged. • Disabling an account will remove LIMOSS SSO access immediately (on prem authentication would be refused) • Service Request removal of LIMOSS guest account requested as "housekeeping" and extra security
New Cost Items	• Deployment of a non-critical virtual server to host AD Connect • Deployment of resilient authentication agents • Azure Basic AD Licence @ £0.74/user/month • MFA optional (billed through LIMOSS)



Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Option 5: Office365 Account Usage (Zero Incremental Cost for O365 users)

Organisations who have no On-Premise AD infrastructure, but have Office365 are already in a position to adopt LIMOSS SSO with no incremental cost.



EXISTING Office365 Users	
Description	Market Participant using Office365
Suitability	The organisation has no On-Prem AD, but already utilises Office365.
Utilises Users Existing Account	Yes. Uses Office365 accounts for LIMOSS applications (this may not be their PC login)
New infrastructure	NONE
Administration	• The Market participant will continue to manage Office365 Accounts. Disabling such an account will instantly remove access to LIMOSS applications. • Password resets can be performed by the user within Office365/Azure-provided screens.
New Cost Items	NONE (other than Office365 licensing)

Adopting Office365 if not already a user would clearly incur incremental cost, and would represent a significant office tooling upgrade project with it's own right. Usually these projects have their own business case with positive benefits independent of SSO.

Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.

Next steps

- You may wish to discuss your preferred solution with IT/business colleagues.

- You can find further advice and guidance at https://limoss.london/limoss-sso-sde-and-api-gateway including:
  - On-Boarding Business and Technical Guides
  - Overview of LIMOSS SSO
  - Technical Overview of LIMOSS SSO
  - FAQ

- If you have additional questions, please contact servicedesk@limoss.london or https://limoss.london/contact

Market firms are advised to make their own assessment of which Azure solution is best for their organisation.
LIMOSS does not offer any advice or make any recommendations in relation to Azure solutions.


LIMOSS
London Insurance Market
Operations & Strategic Sourcing