LIMOSS
One Lime Street
London EC3M 7HA
United Kingdom

LIMOSS SSO Technical On-boarding Guide

for Technical Leads

- Reasonable care has been taken in providing this information but LIMOSS does not give express or implied warranty as to its accuracy. We do not accept any liability for errors or omissions.
- If you notice any errors – or have suggestions on how to improve this guide – please email ServiceDesk@limoss.london.
- All URLs are correct at time of publishing. LIMOSS is not responsible for external links.
- Documentation is constantly under review to ensure the latest information is provided. Please visit https://limoss.london to ensure you have the latest version of this document.
- Commercial agreements applicable to this service refer to LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway under the term "Common Services".

Prepared by	Alistair Murray
Title	LIMOSS SSO Technical On-boarding Guide
Date	01/10/2020
Version	1.0
Description	LIMOSS SSO On-boarding Guide for Technical Leads

Table of Contents

1 Select the right guide for you

This document will guide you through the **Technical aspects** of on-boarding onto LIMOSS SSO. Your nominated Business contact is advised to review the 'LIMOSS SSO Business On-boarding Guide'.

If you are joining LIMOSS SSO as part of another project roll-out Eg. DDM or DCOM, please also refer to the relevant publications for that project.

There are 2 versions of this guide. Please select the correct version for your organisation by confirming your company's existing Azure presence.

You do not need to have an Azure Active Directory (AAD) to use LIMOSS SSO, LIMOSS SDE or LIMOSS API Gateway[1] – but using your own AAD will provide the maximum benefits. The 'LIMOSS SSO - Azure Adoption guide' has been produced to help organisations understand their Azure options.

Your business on-boarding lead will need to know your current Azure Status. There are 2 possibilities:

a) Existing Managed Azure Tenant

This is likely if your organisation has done any of the following:
- *Holds an active subscription to a Microsoft Cloud product, such as MS Office 365.*
- *Your organisation synchronises it's on premises Active Directory (AD) with Azure (AD Connect or ADFS).*
- *Your organisation has purchased an Azure Tenant.*

- To test this, change the password for a specific user on your organisation's main Active Directory. If it changes the password they use to access their Cloud product (E.g. MS Office 365), then your Azure Active Directory (AAD) tenant is managed and you must use the checklist in chapter 2.

b) No Azure Presence

- If you are certain that your organisation has no Azure presence, you can either look to create a managed Azure Tenant before on-boarding (and follow Chapter 2) OR go to chapter 3, where free basic Azure accounts will be created automatically for all users during the on-boarding process.

Selecting the Correct Checklist:

Does your organisation already have a managed Azure Tenant?	**Yes**	Go to chapter 2
	No	Go to chapter 3

For help at any stage, please contact the LIMOSS Service Desk via https://limoss.london/contact or email ServiceDesk@limoss.london.

[1] The only exception is for the LIMOSS API Gateway: When using a Native application (i.e. a non-web based application), all user accounts must be created in a managed Azure Active Directory.

2 On-boarding WITH a managed Azure Tenant

2.1 Read the information guides

Read the 'LIMOSS SSO Technical overview' and, if necessary, the 'LIMOSS SSO - Azure Adoption guide'. For information about Azure, visit https://azure.microsoft.com.

2.2 Check your web browsers

Ensure all users have the latest version (or latest minus one) of any of the following browsers:

- **Google Chrome**
- **Microsoft Edge**
- **Internet Explorer**
- **Safari**

Users with a different browser, or an older version of the browsers listed, may find that some LIMOSS SSO webpages do not appear or function as expected. LIMOSS will also be unable to provide the latest security updates.

2.3 Confirm Approved Domains

When you ask to on-board a new user, LIMOSS will check that the domain of the user's Login ID is on a list of approved domains provided by your company. This reduces the chance of an unauthorised account being added to LIMOSS SSO. To enable this, please identify all domain names that your potential users of LIMOSS SSO may have. e.g. ABC.Com, ABCGroup.com, ABC.fr etc. The approved list should not include shared email services e.g. Hotmail.com or Gmail.com, although users can have such accounts with your company's permission. Domains belonging to other organisations should not be registered without the approval from the domain's owner.

The list of Approved Domains should be passed to your business lead, who will need this information when completing the onboarding form. Once an organisation is onboarded to LIMOSS SSO, your Authorised Contacts can amend the list of Approved Domains.

2.4 Update relevant IT colleagues

Ensure that all your IT colleagues are aware that your organisation will shortly onboard to LIMOSS SSO. The implications of any future changes to both individual user accounts and the company's Azure Active Directory should be clarified with relevant IT team members. Unplanned changes may suspend the LIMOSS SSO accounts of all your on-boarded users.

2.5 Decide on Microsoft email invitations

As part of the user on-boarding process, every user account will receive an email invitation from invites@microsoft.com. Users should be encouraged to check that the invite is from the address shown before opening the email. Each user must click on the 'Get Started' link within the email in order to activate their LIMOSS SSO account.

Organisations with a managed AAD can suppress these emails for most user accounts. To do this, one account in your Azure tenant must be given 'Guest Inviter' permissions in Azure. The UPN of this account must be given to your Business lead as this is needed when completing

the onboarding form. The Guest Inviter will be on-boarded first and will receive an email invite as above. The Guest Inviter must accept this invite and – depending on Azure settings – may also receive invitations for all other users.

2.6 Ensure Microsoft email invitations are not caught in spam filters

To ensure email invites are not caught in a spam filter, we suggest that you add invites@microsoft.com as a known sender.

2.7 Ensure all potential LIMOSS SSO users are in your Azure tenant

As with all cloud logins, LIMOSS SSO will only work if the identity provided during a user's on-boarding is the User Principal Name (UPN) held in your Azure Active Directory. Each individual user must have their own UPN setup in your Azure Active Directory. Ensure that all UPNs are able to receive email addresses unless you are using the email suppression option in Section 2.5 above.

Please check the list of UPNs matches exactly the list provided by your business lead for on-boarding. If you wish to on-board a user's secondary email addresses, your AAD must allow use of this email address as an alternate UPN.

Please refer to Azure documentation linked here for coverage of User UPNs.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-userprincipalname

2.8 Synchronise and Manage passwords

If your accounts in Azure are in the Cloud only (e.g. Office 365 specific), or not synchronised to your corporate ID, ensure the user knows which password to use and how to reset it. Consider checking that your service desk know how to process password reset requests.

2.9 Check 'Tenant Restrictions' setting in your Azure Active Directory tenant

The 'Tenant Restrictions' setting in your Azure Active Directory tenant must not prevent interaction with external tenants. LIMOSS SSO will be unable to provide service if this setting does not permit such interaction. You may need to provide the tenancy ID for the LIMOSS SSO Azure tenant, which is **LIMOSS.onmicrosoft.com**.

2.10 Review your "Joiners Leavers Movers" process

LIMOSS must be informed of any LIMOSS SSO user who joins or leaves your company. These notifications should come from the Authorised Contacts nominated by your company. You may wish to discuss this with your Business Lead and revise your organisation's "Joiners Leavers Movers" process to ensure such notifications are passed to the LIMOSS Service Desk in a timely manner.

Post Go-live

2.11 Manage any problems

If any user has problems accessing the portal, check that their User ID was on the list of users sent to LIMOSS and was correctly spelt. Then check that the user's account is registered in your AAD tenant as a UPN or alias. It is also worth confirming that the account is unlocked and

resetting the user's password if needed. If users are still having problems accessing LIMOSS SSO, contact ServiceDesk@limoss.london.

2.12 Inform LIMOSS Service Desk of any planned changes to User IDs

Once a user is in LIMOSS SSO, any changes to their User ID (UPN) will break the underlying link between your AAD tenant and the LIMOSS SSO AAD tenant. This means that they will be unable to authenticate via LIMOSS SSO – and will therefore be unable to access any market services using their LIMOSS SSO account.

We suggest contacting the LIMOSS Service Desk before changing a User ID or any major changes to your organisation's AAD.

STOP! Checklist Complete

Please inform your Business Lead that you have completed the Technical On-boarding guide. Once they have completed the Business On-boarding guide, they can complete the registration form.

Please ignore Chapter 3, which is for organisations that do not have an existing Azure presence.

3 On-boarding WITHOUT a managed Azure Tenant

3.1 Read the information guides

Read the 'LIMOSS SSO Technical overview' and, if necessary, the 'LIMOSS SSO - Azure Adoption guide'. For information about Azure, visit https://azure.microsoft.com.

3.2 Check the browser

Ensure all users have the latest version (or latest minus one) of any of the following browsers:

- **Google Chrome**
- **Microsoft Edge**
- **Internet Explorer**
- **Safari**

Users with a different browser, or an older version of the browsers listed, may find that some LIMOSS SSO webpages do not appear or function as expected. LIMOSS will also be unable to provide the latest security updates.

3.3 Confirm your list of Approved Domains

When you ask to on-board a new user, LIMOSS will check that the domain of the user's Login ID is on a list of approved domains provided by your company. This reduces the chance of an unauthorised account being added to LIMOSS SSO. To enable this, please identify all domain names that your potential users of LIMOSS SSO may have. e.g. ABC.Com, ABCGroup.com, ABC.fr etc. The approved list should not include shared email services e.g. Hotmail.com or Gmail.com, although users can have such accounts with your company's permission. Domains belonging to other organisations should not be registered without the approval from the domain's owner.

The list of Approved Domains should be passed to your business lead, who will need this information when completing the onboarding form. Once an organisation is onboarded to LIMOSS SSO, your Authorised Contacts can amend the list of Approved Domains.

3.4 Update relevant IT colleagues

Ensure that all your IT colleagues are aware that your organisation will shortly onboard to LIMOSS SSO. By on-boarding to LIMOSS SSO without an existing Azure presence, a basic Microsoft Azure account will be created for each user. As these will not be centrally managed, your IT department will not be able to conduct password resets on these accounts, but users will be able to complete password resets themselves via the Microsoft Azure website.

3.5 Ensure Microsoft email invitations are not caught in spam filters

All users added to LIMOSS SSO will receive an email from invites@microsoft.com. If you use a spam filter, we suggest adding this email account as a known sender. Users should be encouraged to check that the invite is from the address shown before opening the email. Each

user must open the email and click on the 'Get Started' link in order to gain access to LIMOSS SSO.

3.6 Review your "Joiners/Leavers/Movers" process

LIMOSS must be informed of any LIMOSS SSO user who joins or leaves your company. These notifications should come from the Authorised Contacts nominated by your company. You may wish to discuss this with your Business Lead and revise your organisation's "Joiners Leavers Movers" process to ensure such notifications are passed to the LIMOSS Service Desk in a timely manner.

Post Go-live

3.7 Manage any problems

If any user has problems accessing the portal, check that their User ID was on the list of users sent by your Authorised Contact(s) to LIMOSS. The user should also reset their password via the Azure website. If users are still having problems accessing LIMOSS SSO, contact ServiceDesk@limoss.london

3.8 Inform LIMOSS Service Desk if you adopt Azure

If you choose to adopt Microsoft Azure after you start using LIMOSS SSO, please contact the LIMOSS Service Desk (ServiceDesk@limoss.london) to discuss any changes in advance. Moving to Azure without discussing your move with LIMOSS is likely to disable all LIMOSS SSO accounts belonging to your users. This will prevent your users being able to authenticate to any market services using their LIMOSS SSO account.

STOP! Checklist Complete

Please inform your Business Lead that you have completed the Technical On-boarding guide. Once they have completed the Business On-boarding guide, they can complete the registration form.