LIMOSS SSO Business On-boarding Guide
for Business 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	Matt Young
Title	LIMOSS SSO Business On-boarding Guide
Date	01/10/2020
Version	1.0
Description	LIMOSS SSO On-boarding Guide for Business Leads

Table of Contents

1 Select the right guide for you

This guide will assist you through the **Business aspects** of on-boarding onto LIMOSS SSO. Your nominated IT contact is advised to review the 'LIMOSS SSO Technical 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 answering the question below. If you're unsure about your existing Microsoft Azure presence, please check with your IT team.

Does your organisation already have a managed Azure Tenant? (Speak with your IT department if unsure about your Azure usage)	**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.

2   On-boarding WITH a managed Azure Tenant

Initial Checks

2.1   Nominate Authorised Contact(s)

Authorised Contacts are an organisation's approved representatives to liaise with LIMOSS. Authorised Contacts are the only people in an organisation who can add, change or remove users from the LIMOSS SSO system, as well as approve other Service Requests. They can be from an IT or business team. The 'LIMOSS SSO – Authorised Contact Guide' provides useful information for Authorised Contacts.

2.2   Identify users

Identify the names and User Logins of all users that require access to LIMOSS SSO. A User Login can be an email address but, more accurately, is the UPN (User Principal Name) of the user. Please speak with your IT team to clarify which User Login your users should register for LIMOSS SSO. LIMOSS SSO does not support group mailboxes so the User Login provided must be unique for each individual user account.

2.3   Sign the SSO Market User Agreement (MUA)

All organisations on-boarding to LIMOSS SSO must complete and sign the SSO MUA. The MUA will be provided to you during your on-boarding. The default method of signature is via DocuSign. If your nominated Authorised Contact is also authorised to sign the MUA, you can ask to sign the MUA via a click-through screen when the Authorised Contact is first on-boarded to LIMOSS SSO. Please mention this to the LIMOSS Service Desk when on-boarding.

The Market User Agreement details the basis on which LIMOSS processes personal data and the lawful reason for doing so (i.e. Legitimate Interest). When using these services, your Organisation will remain as the Data Controller and LIMOSS will act as Data Processor. For any instances where LIMOSS is a Data Controller, the [LIMOSS Privacy Notice](#) will apply.

2.4   Decide on the use of Secure Data Exchange (SDE)

There is no additional cost for using SDE but you may wish to review the 'LIMOSS SDE Adoption Guidance' to help decide if SDE is right for your organisation. You will be asked to confirm this during your on-boarding. All Authorised Contact(s) will still be able to access SDE even if you choose not to provide it to all other users.

2.5   Ensure Technical Checks are complete

Confirm with your IT department that they have reviewed the 'LIMOSS SSO Technical On-Boarding Guide.'

2.6   Inform all end users

Inform all end users that they will be on-boarded to LIMOSS SSO. Explain that they will receive the invitations email and that they **must**:
a) Check that the email is from invites@microsoft.com
b) Follow the directions within the email and click on the link to complete their registration.

You may wish to inform them that their personal information (name and work email address) will be shared with LIMOSS in order to deliver these services. The 'LIMOSS SSO - User Guide' provides other useful information for end users.

2.7   Decide who should receive Microsoft Invites

As you have a managed Azure presence, you can choose to suppress the invitation emails. Please speak with your IT team as there is more information in Step 2.5 of the 'LIMOSS SSO Technical On-Boarding Guide'. Complete the "Suppress Emails" section of the On-Boarding form if you wish to select this option.

2.8   Share Support Desk details

Ensure your users know who to contact in the event of an issue when using their LIMOSS SSO account. This is likely to be your in-house IT Service Desk or the Service Desk of the Market Application they are using. E.g. DDM. They can also contact ServiceDesk@limoss.london.

2.9   Provide On-boarding details

When you're ready to register, complete the registration form. You will need the following details:

1. Your organisation's legal name, registration number and country of registration
2. Your Organisation's primary role (Eg. Carrier, Broker, Coverholder)
3. Name and email address of a colleague authorised to sign legal agreements
4. Your Authorised Contact(s) name and email address(es)
5. All domains that your user accounts will belong to. Eg. @Brokerabc.com; @Brokerabc.co.uk. See the 'LIMOSS SSO Technical On-Boarding Guide'
6. Whether you wish to use SDE
7. If you wish to suppress emails, the details of a 'Guest Inviter' account

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 Technical 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.

Next Steps

2.11   Confirm your email address

You will receive an email from the LIMOSS Service Desk (ServiceDesk@limoss.london) to authenticate your email address. You must reply to this email before your application can be completed.

2.12   Accept the Invitation Email

Once your email address has been authenticated, your on-boarding request will be processed. We will KYC your organisation and send the commercial Agreement for signature to your nominated Authorised Signatory. Your Authorised Contact(s) will then receive an Invitation Email containing a 'Get Started' link. The Authorised Contact(s) must check the sender's email address is invites@microsoft.com before clicking the link. Your IT department can choose to

prevent the Authorised Contact(s) receiving this email. Further details can be found in the **'**LIMOSS SSO Technical On-Boarding Guide.'

2.13 Add users

Once on-boarded, your Authorised Contact(s) will be able to add standard users and Authorised Contacts in any of the following 3 ways:

1) LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/ - Click on "LIMOSS SSO Support" and then choose "Add a New Standard User" or "Add an Authorised Contact User"

2) By contacting LIMOSS Service Desk. Please email servicedesk@limoss.london and they will assist you with the on-boarding. For GDPR reasons, please do not send the list of users via email. The Service Desk will advise how to securely share your user lists.

3) Devolved Admin Portal (DAP): Due for release in Q4 2020. Further details to follow.

2.14 Confirm accounts are ready

Approximately 5 working days after providing the details of your new users, your Authorised Contact(s) will receive an email confirming user accounts are ready. We suggest confirming and testing with one user before emailing all users to confirm their accounts are live. Unless you have suppressed the invitation emails, each user will need to action their invitation email as explained above. Users can visit https://portal.londonmarketgroup.co.uk to test their account.

After Go-live

2.15 Manage any problems

If any user has problems accessing the portal, check that their details were on the list of users sent to LIMOSS. Your in-house IT Service Desk should check the user's account is working and that the user can logon to resources within your own organisation (i.e. that their account is not locked and that the password is valid). If users are still having problems accessing LIMOSS SSO, please contact ServiceDesk@limoss.london or use the "Report a Problem" tile in the LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/

2.16 Keep your user list up to date

To add, remove or amend users, an Authorised Contact(s) must update LIMOSS in 1 of 3 ways:

1) LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/ - Click on "LIMOSS SSO Support" and then choose "Remove an existing user" or "Change details of an existing user"

2) By contacting LIMOSS Service Desk. Please email servicedesk@limoss.london and they will assist you with the on-boarding. For GDPR reasons, please do not send a list of users via email. The Service Desk will advise how to securely share your user lists.

3) Devolved Admin Portal: Due for release in Q4 2020. Further details to follow.

2.17 Get Support

If you need support at any point, please see the following resources:

- LIMOSS SSO Webpages: https://limoss.london/limoss-sso-sde-and-api-gateway
- LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/ - Click on "LIMOSS SSO Support" and then choose the appropriate tile.
- Email LIMOSS Service Desk on servicedesk@limoss.london
- Call LIMOSS Service Desk on +44 (0) 207 100 5151
- Use the contact form at https://limoss.london/contact
- To Add/Remove users or to update your list of Approved Domains, Authorised Contacts can use the Devolved Admin Portal: Due for release in Q4 2020. Further details to follow.

STOP! Checklist Complete

Once your team have completed the Technical On-boarding guide, you 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

Initial Checks

3.1   Nominate Authorised Contact(s)

Authorised Contacts are an organisation's approved representatives to liaise with LIMOSS. Authorised Contacts are the only people in an organisation who can add, change or remove users from the LIMOSS SSO system, as well as approve other Service Requests. They can be from an IT or business team. The 'LIMOSS SSO – Authorised Contact Guide' provides useful information for Authorised Contacts.

3.2   Identify users

Identify the names and User Logins of all users that require access to LIMOSS SSO. A User Login can be an email address but, more accurately, is the UPN (User Principal Name) of the user. Please speak with your IT team to clarify which User Login your users should register for LIMOSS SSO. LIMOSS SSO does not support group mailboxes so the User Login provided must be unique for each individual user account.

3.3   Sign the SSO Market User Agreement (MUA)

All organisations on-boarding to LIMOSS SSO must complete and sign the SSO MUA. The MUA will be provided to you during your on-boarding. The default method of signature is via DocuSign. If your nominated Authorised Contact is also authorised to sign the MUA, you can ask to sign the MUA via a click-through screen when the Authorised Contact is first on-boarded to LIMOSS SSO. Please mention this to the LIMOSS Service Desk when on-boarding.

The Market User Agreement details the basis on which LIMOSS processes personal data and the lawful reason for doing so (i.e. Legitimate Interest). When using these services, your Organisation will remain as the Data Controller and LIMOSS will act as Data Processor. For any instances where LIMOSS is a Data Controller, the [LIMOSS Privacy Notice](#) will apply.

3.4   Decide on the use of Secure Data Exchange (SDE)

There is no additional cost for using SDE but you may wish to review the 'LIMOSS SDE Adoption Guidance' to help decide if SDE is right for your organisation. You will be asked to confirm this during your on-boarding. All Authorised Contact(s) will still be able to access SDE even if you choose not to provide it to all other users.

3.5   Ensure Technical Checks are complete

Confirm with your IT department that they have reviewed the 'LIMOSS SSO Technical On-Boarding Guide.'

3.6   Inform end users

Inform all end users that they will be on-boarded to LIMOSS SSO. Explain that they will receive the invitations email and that they **must**:
a) Check that the email is from invites@microsoft.com
b) Follow the directions within the email and click on the link to complete their registration.

You may wish to inform them that their personal information (name and work email address) will be shared with LIMOSS in order to deliver these services. The 'LIMOSS SSO - User Guide' provides other useful information for end users.

3.7   Share Support Desk details

Ensure your users know who to contact in the event of an issue when using their LIMOSS SSO account. This is likely to be your in-house IT Service Desk or the Service Desk of the Market Application they are using. E.g. DDM. They can also contact ServiceDesk@limoss.london.

3.8   Provide On-boarding details

When you're ready to register, complete the registration form. You will need the following details:

1. Your organisation's legal name, registration number and country of registration
2. Your Organisation's primary role (Eg. Carrier, Broker, Coverholder)
3. Name and email address of a colleague authorised to sign legal agreements
4. Your Authorised Contact(s) name and email address(es)
5. All domains that your user accounts will belong to. Eg. @Brokerabc.com; @Brokerabc.co.uk. See the 'LIMOSS SSO Technical On-Boarding Guide'
6. Whether you wish to use SDE

3.9   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 Technical 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.

Next Steps

3.10   Confirm your email address

You will receive an email from the LIMOSS Service Desk (ServiceDesk@limoss.london) to authenticate your email address. You must reply to this email before your application can be completed.

3.11   Accept the Invitation Email

Once your email address has been authenticated, your on-boarding request will be processed. We will KYC your organisation and send the commercial Agreement for signature to your nominated Authorised Signatory. Your Authorised Contact(s) will then receive an Invitation Email containing a 'Get Started' link. The Authorised Contact(s) must check the sender's email address is invites@microsoft.com before clicking the link.

3.12   Add users

Once on-boarded, your Authorised Contact(s) will be able to add standard users and Authorised Contacts in any of the following 3 ways:

1) LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/ - Click on "LIMOSS SSO Support" and then choose "Add a New Standard User" or "Add an Authorised Contact User"

2) By contacting LIMOSS Service Desk. Please email servicedesk@limoss.london and they will assist you with the on-boarding. For GDPR reasons, please do not send the list of users via email. The Service Desk will advise how to securely share your user lists.

3) Devolved Admin Portal: Due for release in Q4 2020. Further details to follow.

3.13 Confirm accounts are ready

Approximately 5 working days after providing the details of your new users, your Authorised Contact(s) will receive an email confirming user accounts are ready. We suggest confirming and testing with one user before emailing all users to confirm their accounts are live. Users should be directed to https://portal.londonmarketgroup.co.uk to test their account access.

After Go-live

3.14 Manage any problems

If any user has problems accessing the portal, they should check that their details were on the list of users sent to LIMOSS. If users are still having problems accessing LIMOSS SSO, please contact ServiceDesk@limoss.london or use the "Report a Problem" tile in the LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/

3.15 Keep your user list up to date

To add, remove or amend users, an Authorised Contact(s) must update LIMOSS in 1 of 3 ways:

1) LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/ - Click on "LIMOSS SSO Support" and then choose "Remove an existing user" or "Change details of an existing user"

2) By contacting LIMOSS Service Desk. Please email servicedesk@limoss.london and they will assist you with the on-boarding. For GDPR reasons, please do not send a list of users via email. The Service Desk will advise how to securely share your user lists.

3) Devolved Admin Portal: Due for release in Q4 2020. Further details to follow.

3.16 Get Support

If you need support at any point, please see the following resources:
- LIMOSS SSO Webpages: https://limoss.london/limoss-sso-sde-and-api-gateway
- LIMOSS Self-Service Portal: https://customer.hornbill.com/limoss/ - Click on "LIMOSS SSO Support" and then choose the appropriate tile.
- Email LIMOSS Service Desk on servicedesk@limoss.london
- Call LIMOSS Service Desk on +44 (0) 207 100 5151
- Use the contact form at https://limoss.london/contact
- To Add/Remove users or to update your list of Approved Domains, use the Devolved Admin Portal: Due for release in Q4 2020. Further details to follow.

STOP! Checklist Complete

Once your team have completed the Technical On-boarding guide, you can complete the registration form