LIMOSS
London Insurance Market
Operations & Strategic Sourcing

LIMOSS
One Lime Street
London EC3M 7HA
United Kingdom

LIMOSS Single Sign-On (SSO) - A Technical Overview

A technical overview of LIMOSS SSO for IT and technical support teams

LIMOSS provides a suite of tools to help market participants access shared Market Solutions. Collectively, these services were previously referred to as “Common Services”. The 3 Services are:

1. LIMOSS SSO (Single Sign-On)

Enables users to access shared Market services with a single username and password. This will usually be the same credentials for accessing their own Organisational IT. Once registered for LIMOSS SSO, an Organisation can register for LIMOSS SDE and LIMOSS API Gateway.

2. LIMOSS SDE (Secure Data Exchange)

An optional product that allows simple, secure exchanging of data across the market.
To use LIMOSS SDE, organisations must first register for LIMOSS SSO.

3. LIMOSS API Gateway (Application Programme Interface Gateway)

A secure and simple method for integrating in-house IT systems with shared Market Services.
To use LIMOSS API Gateway, organisations must first register for LIMOSS SSO.

Azure Active Directory

LIMOSS SSO uses Azure B2B services to manage a LIMOSS SSO tenant in Microsoft’s Azure Active Directory (AAD). It holds names and User IDs (Eg. email addresses) but never passwords. The LIMOSS SSO tenant is used to:

- **Organise users.** All on-boarded users who are part of the same organisation are created in that organisation’s user group as a ‘Guest User’ in the LIMOSS tenant.

- **Control user access to Solutions**. Market Solutions can request authentication of users in the LIMOSS SSO tenant. This allows different users within the same organisation to access different shared Market Services depending on their business needs.

- **Authenticate Users**. LIMOSS SSO authenticates that a specific user requesting access to a Market Service is registered with LIMOSS SSO and is providing the correct security credentials (Eg. Password)

For information about Azure, please visit https://azure.microsoft.com

(LIMOSS is not responsible for external sites)

How LIMOSS SSO Authenticates

The authentication method used by LIMOSS SSO depends on an organisation's Azure presence:

1. Existing Azure Active Directory presence

If an organisation has an Existing Azure Active Directory presence, authentication will be made via Azure B2B Collaboration directly with the Organisation's own AAD tenant.

Creating a Presence. Organisations will have an existing AAD presence if:

- The organisation uses Azure AD (may be synchronised with On Premises AD).
- The organisation uses existing Microsoft SaaS products, such as Office 365 or Yammer.

Allowing Authentication. To allow the LIMOSS SSO tenant to authenticate with its own AAD, an organisation must ensure:

- IT security policies support the use of authentication requests by 3rd party AAD Tenants.
- All domains registered in Azure are managed by a designated administrator. There is no need to have a separate AAD for each domain.
- Every user needing access to market applications exists in the Organisation's AAD. The User Principal Name (UPN) held in this AAD must be passed to CS during on-boarding. This UPN may or may not be the same as the user's email address.
- 'Tenancy Restriction' setting in all AADs must allow federation with LIMOSS SSO tenant.

Benefits. This method delivers:

- Seamless delivery of full SSO with an organisation's own IT services and Market Services.
- One set of credentials. Easier for users to remember and for IT teams to manage.
- Improved Identity and Access Management by automatic access restriction for leavers.

2. No Existing Azure Active Directory presence

For organisations without an existing AAD presence, basic Azure accounts are automatically provided during the LIMOSS SSO On-boarding. Authentication requests will be made with this tenant and, in this case, users are in sole control of their account status and password.

Creating a Presence. During the on-boarding process, every user will receive an invitation to create a free Microsoft Live account:

- Basic accounts provide CS functionality but do not incur charges by Microsoft.
- The domain of the user's email address ***must not*** already be registered in Azure.
- LIMOSS Service Desk ***must*** be informed about leavers so that they can be removed from our tenant. Failure to inform LIMOSS could allow leavers to continue accessing Market Services even after they have left the organisation.

Benefits. This method allows:

- An SSO solution for companies that don't have existing Azure services.
- A single set of credentials for all Market Services using LIMOSS SSO.
- Individual users to reset their own passwords via a Microsoft portal.

For further information, visit limoss.london/limoss-sso-sde-and-api-gateway
or contact LIMOSS Service Desk via limoss.london/contact