

LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway

An Overview

This document is issued by LIMOSS for guidance purposes. Reasonable care has been taken in providing this information but errors or omissions may exist. Corrections and suggested improvements should be passed to the [LIMOSS Service Desk](#). All URLs are correct at time of publishing. LIMOSS is not responsible for external links. Documentation is constantly updated. To ensure the latest version is always available, this file should be opened from the LIMOSS website where possible. Nothing in this guide is intended to create a contractual agreement. Commercial agreements applicable to this service may refer to LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway under the term “Common Services”.

09 May 2022

London

LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway

3 Services in 1



These LIMOSS Services support integration between a firm's own IT Solutions and shared Market Services

To access SDE or the API Gateway you must first register for LIMOSS SSO

What are the 3 Services?

A strategic level suite of tools making it easier for:

- End users to **access** Market Services
- In-house systems to **integrate** with other LIMOSS/Market solutions
- End users and systems to **securely share** data across the Market

The 3 Key Components are:



**Single Sign On
(SSO)**

Users can access LIMOSS and other Market solutions using the same username and password.*



**Application Programme
Interface Gateway
(API GWY)**

Secure and simple method for integrating your own IT systems with LIMOSS and other Market solutions.



**Secure Data
Exchange
(SDE)**

An optional easy-to-use tool for securely exchanging data between Market participants. Can be accessed via on-line interface or integrated with your systems.

[SDE User Video](#)

(<https://vimeo.com/302815716>)

Benefits of the Services



**Single Sign On
(SSO)**

-  Administrative control remains with the organisation.
-  Only one account per user for IT to manage.
-  Only one username and password to remember.
-  No need to log in repeatedly.



**Application Programme
Interface Gateway
(API GWY)**

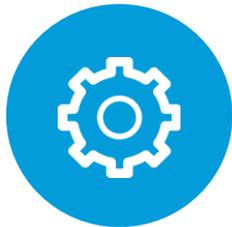
-  Allows in-house and Market Services to interact for straight-through processing without expensive and time-consuming integration.
-  Less re-keying required when using API for straight-through processing.
-  Better user experience between in-house and external systems for faster access to information.



**Secure Data
Exchange
(SDE)**

-  Data can be shared securely with users in accredited Market organisations.
-  Data is securely encrypted and automatically deleted after maximum of two weeks.
-  Large quantities of data (Max 1 Gb per file) can be sent in any file format to multiple participants in other trusted Market organisations. No limit on the number of files sent.
-  Can be integrated with existing IT systems via the API Gateway. Outdated file sharing systems reliant on IT support Eg sFTP are no longer needed.

On-boarding



Reasons to register for SSO

1

Your organisation is on-boarding to a Market Service that *requires* SSO. Eg. DDM*, Lloyd's Insights.

2

Your Organisation *chooses* to use the API Gateway or SDE Eg. To access PPL APIs.



Business Use Case Examples

SSO

A 3rd party software vendor allows easy Market access to its products via SSO.

API GWY

An MA's in-house IT team use PPL APIs to integrate directly with their PAS to support their existing back-office Systems.

SDE

Brokers can share exposure management files (Eg. Video of Drone overflight of insured asset) with multiple potential Underwriters securely and without each underwriter being aware of the others ability to see the video.



Costs

Charges

LIMOSS co-ordinates all charges in line with the annual Charging Model. There are currently no usage charges for brokers, coverholders or vendors. Carriers are covered under the 'User Pays' model. For more information, contact us via <https://limoss.london/contact>

Internal Set up & Run costs

Nil Cost options exist for use of SSO and SDE. API GWY requires a funded Azure system. See the Azure Adoption Guide for further details. The API Gateway requires an in-date Security Certificate.

LIMOSS SSO – How to Register

3 simple Steps to using LIMOSS SSO

Registering for LIMOSS SSO also allows access to LIMOSS SDE and LIMOSS API Gateway

1. Complete the [Registration form](#)
2. LIMOSS Service Desk will guide you through the Registration Process
3. Once registered, you can manage user accounts via [DAP](#) and subscribe to APIs via [Hornbill](#)

Helpful guides are available on the LIMOSS Website
<https://limoss.london/limoss-sso-sde-and-api-gateway>

- [Technical Overview](#)
- [On-Boarding Guides](#)
- [Azure Adoption Guide](#)
- [SDE Adoption Guide](#)
- [SDE User Guide](#)
- [SDE video Tutorial](#)
- [FAQ](#)
- [List of Available APIs](#)
- [API Subscribing Guide](#)
- [Developer's Guide](#)
- [Service Status Page](#)
- [DAP User Guide](#)
- [Accessing Lloyd's Services](#)



If registering for SSO as part of another solution Eg. DDM*, please refer to the on-boarding material for that project

To access PPL APIs, you must complete the onboarding journey at <https://developer.lloyds.com/>

(LIMOSS is not responsible for external sites)

LIMOSS SSO – Account Management



Keeping LIMOSS SSO users safe

To ensure all users accounts are securely managed:

Invites for new users must be accepted within 28 days

- Accounts not activated within 28 days will be automatically deleted
- Once an organisation is registered, their users can [self-register for a new LIMOSS SSO account](#)

Inactive Accounts are disabled after 3 months and deleted after 13 months

- Accounts not used within 3 months will be disabled. Users should contact the [LIMOSS Service Desk](#) to re-enable
- For security and GDPR reasons, accounts inactive for 13 months will be deleted

Organisations must manage their user accounts

- Creation and deletion of LIMOSS SSO user accounts should form part of every organisation's JLM process
- Organisations can securely manage their LIMOSS SSO users via the [Devolved Admin Portal \(DAP\)](#)

For help managing user accounts see the [DAP User guide](#) or contact the [LIMOSS Service Desk](#)



Geographic Restrictions and MFA

To ensure all users accounts are securely managed:

LIMOSS SSO authentications may be blocked from some geographic regions

- Authentication attempts from some regions may be restricted
- Users who believe their access is being geographically blocked unfairly should contact the [LIMOSS Service Desk](#)

Multi-Factor Authentication (MFA) may be required

- MFA involves the use of a second authentication method E.g A one-time passcode sent to a user's phone
- LIMOSS SSO may require MFA when some users access some services
- For support in managing MFA, users should follow on-screen prompts or contact the [LIMOSS Service Desk](#)

Questions ?

From us to you:

- What benefits can LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway bring to your Organisation?
- Who else in your team may benefit from learning about these Services?
- Which of your partners (vendors or clients) could benefit from hearing more?
- What APIs would you like to provide or consume?
 - Reference Data or Micro-Services?
- Is there anything you'd like to know that is not covered in this presentation?

From you to us:

Ask us anything



Get in touch:

- servicedesk@limoss.london
- <https://limoss.london/contact>
- <https://limoss.london/limoss-sso-sde-and-api-gateway>
- <https://customer.hornbill.com/limoss/> (Existing LIMOSS SSO users only)

LIMOSS

London Insurance Market
Operations & Strategic Sourcing