LIMOSS
London Insurance Market
Operations & Strategic Sourcing

LIMOSS SSO Services – An Overview

LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway

20 Apr 2023

London

LIMOSS SSO Services: LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway

3 Services in 1

The LIMOSS SSO 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 LIMOSS SSO Services*?

The “LIMOSS SSO Services” are a strategic 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)

* Commercial Agreements may refer to the LIMOSS SSO services as “Common Services”
** The LIMOSS SSO Services do not see or store user passwords

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 Outdated file sharing systems reliant on IT support Eg sFTP are no longer needed.

* Exact benefits depend on an Organisation's Azure presence.

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.

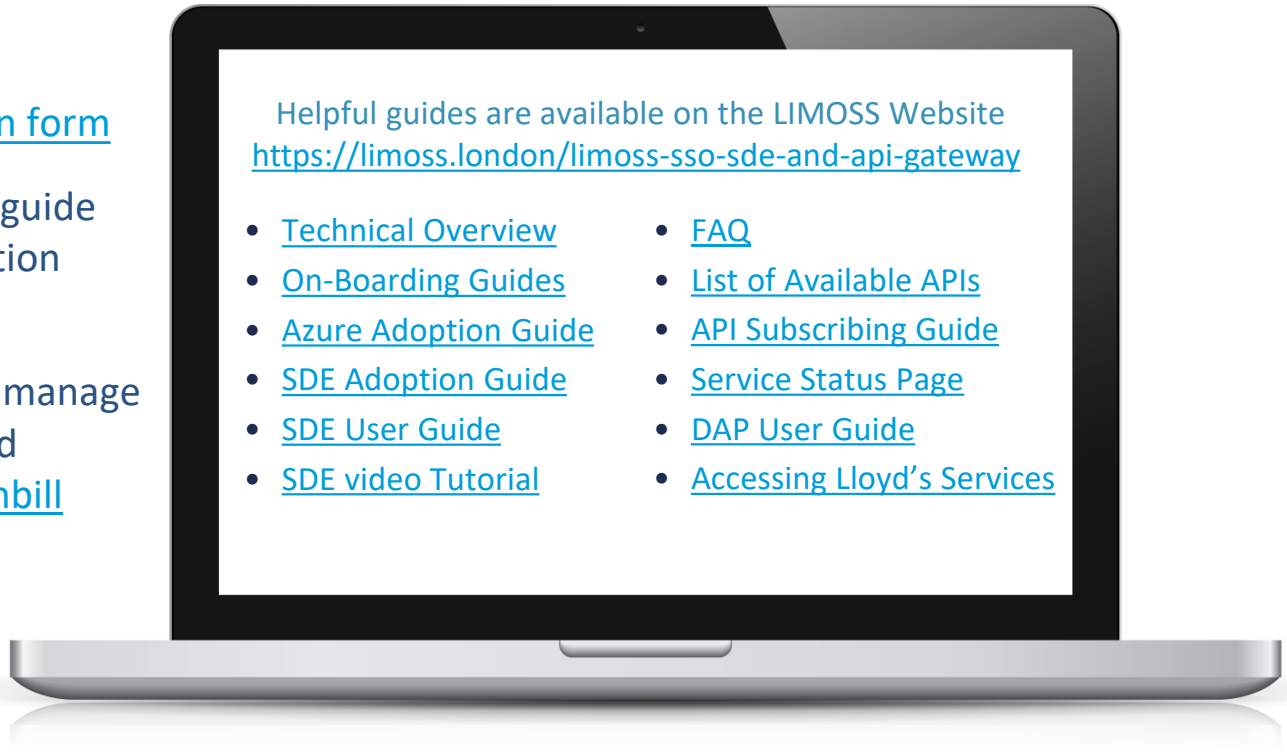
*DDM was previously known as DA SATS

LIMOSS SSO Services – 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



- If registering for SSO as part of another solution Eg. DDM*, please refer to the on-boarding material for that project
- API Gateway Guides (Security & Standards) – available on request to registered orgs only via the LIMOSS Service Desk

To access specific APIs, you must also onboard to the back-end service accessed via the APIs

*DDM was previously known as DA SATS

LIMOSS SSO – Authorised Contacts

All organisations using LIMOSS SSO must nominate an "Authorised Contact"

The role of an Authorised Contact is important:

An "Authorised Contact" is a trusted individual in each firm registered for LIMOSS SSO

- Authorised Contacts administer an organisation's LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway settings
- Authorised Contacts must manage all their user accounts and domains via the Devolved Admin Portal (DAP)
- A domain "auto-approval" option exists - Authorised Contacts can ask LIMOSS Service Desk for further details
- Organisations can appoint as many Authorised Contacts as they need

Authorised Contacts are the vital link between an organisation and LIMOSS

- LIMOSS Service Desk will notify Authorised Contacts of any planned maintenance or service issues

Finding your Authorised Contact

- For security and GDPR reasons, LIMOSS do not divulge the details of an organisation's Authorised Contacts
- Users should, in the first instance, ask their internal IT team for details of their Authorised Contact(s)

For help with any Authorised Contact issue, see the DAP User guide or contact the LIMOSS Service Desk

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 deactivated after 3 months and deleted after 13 months

- Accounts not used within 3 months will be deactivated. Users should contact the LIMOSS Service Desk to re-activate
- 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 must securely manage their LIMOSS SSO users via the Devolved Admin Portal (DAP)
- All organisations are advised to review their list of LIMOSS SSO users via DAP at least once every 6 months

For help managing user accounts see the DAP User guide or contact the LIMOSS Service Desk

LIMOSS SSO – Account Management

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 users may need to use this secondary authentication method to access some services
- MFA support is available via on-screen prompts, this Microsoft video or by contacting the LIMOSS Service Desk

MFA Options: SMS, Voice or Microsoft Authenticator App

- Users can MFA via SMS text, voice call or Microsoft Authenticator App
- Authenticator users with a new mobile device should read Microsoft's advice or contact LIMOSS Service Desk

LIMOSS SSO Services – Maintenance

Routine Maintenance

To keep the LIMOSS SSO Services functioning correctly and securely, routine maintenance occurs as below:

SANDBOX Environment (Developers only)

- Routine maintenance may occur on Mondays 17:00 to 23:59 (UK)
- Services may be degraded or unavailable during this window without prior notice

PRE-PROD Environment (Developers and Testers only)

- Routine maintenance may occur on Wednesdays 18:00 to 23:59 (UK)
- Services may be degraded or unavailable during this window without prior notice

PROD/LIVE Environment (End Users only)

- Routine maintenance may occur from Saturday 00:01 to Sunday 23:59 (UK)
- Services may be degraded or unavailable during this window
- Advance notice will be sent to Authorised Contacts and provided on the LIMOSS Market Services Status Page

For further information and support contact the **LIMOSS Service Desk**

Questions ?

From us to you:

- What benefits can the LIMOSS SSO Services 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)

Annex A

Acceptable Use Policy

LIMOSS SSO - Acceptable Use Policy

Any Organisation using LIMOSS SSO Services shall not, and shall instruct all Users not to, use the Services to:

- violate any law or regulation;
- commit a tortious or otherwise wrongful act, including, without limitation the communication of libellous, defamatory, scandalous, threatening, harassing, or private information (without consent) or communicating content that is likely to cause emotional distress;
- communicate content that is obscene, pornographic, lewd, lascivious or violent;
- violate any copyright, patent, trademark, trade secret or other intellectual property rights of others;
- obtain or attempt to obtain unauthorised access, such as attempting to circumvent or circumventing any authentication or other security feature of the Services. This includes accessing data not intended for the User, logging into a server or account the User is not authorised to access, or probing the security of the Services;
- interfere or attempt to interfere with service of the Services by use of any program, script, command or otherwise. This includes “denial of service” attacks, “flooding” of networks, deliberate attempts to overload the Services or to burden excessively;
- introduce viruses, worms, harmful code and/or Trojan horses;
- communicate a message with deceptive, absent or forged header or sender identification information
- propagate chain letters and pyramid schemes, whether or not the recipient wished to receive such mailings; and/or
- process personal data unless there is a lawful basis for such processing.

Annex B

Right to Monitor

LIMOSS SSO – Right to Monitor

- An employer may monitor and audit their employee's use of the LIMOSS SSO Services - including LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway.
- E.g. When a user logs on; when a user uploads, downloads or modifies data or a file; the content of any files; transactions worked on; and similar information for various legitimate business purposes.
- The parties that users collaborate with when using the LIMOSS SSO Services may engage in similar legitimate activities.


LIMOSS
London Insurance Market
Operations & Strategic Sourcing