

# Subscribing to an API

## LIMOSS API Gateway

- This document is issued by LIMOSS for guidance purposes. Reasonable care has been taken in providing this information but errors or omissions may exist.
- Queries, corrections and suggested improvements should be sent to the [LIMOSS Service Desk](#).
- All personal and commercial data provided by a Subscriber's organisation, or their partner organisations, whilst using the LIMOSS API Gateway will be processed in accordance with the relevant contractual agreements or the [LIMOSS Privacy Notice](#). LIMOSS will share personal data provided with partner organisations for the sole purpose of delivering the service(s) requested.
- 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 if possible.
- Nothing in this guide is intended to create a new contractual agreement.
- Commercial agreements applicable to this service may refer to LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway under the term "Common Services".

23 Sep 2022

# Contents

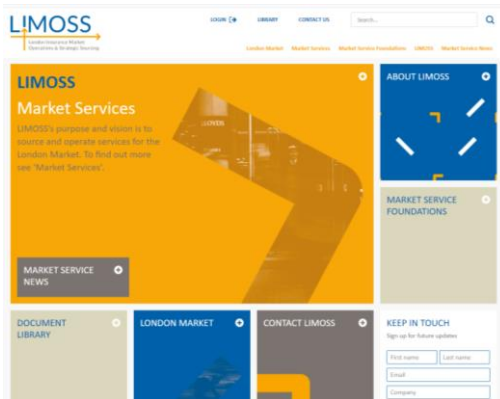
1. [LIMOSS](#)
  2. [LIMOSS SSO](#)
  3. [LIMOSS API Gateway](#)
  4. [Subscribing to an API](#)
  5. [Useful information](#)
  6. [Problem Solving](#)
  7. [Support](#)
- Annex A:** [Response Codes](#)
- Annex B:** [Glossary](#)

## Introduction to LIMOSS

**Mission: Professionally source and operate common market services for the London Market**

### Good to know

- Not-for-Profit
- Single point of contact for key market services: simplifies integration, provides expert advice and reduces costs
- Owned by Lloyd's, IUA and LMA. Cross-market board including LIIBA representation
- Actively seeks market direction (E.g. market governance forums)



### Other LIMOSS Services

- ESP (Electronic Submission Portal)
- SSO (LIMOSS Single Sign On)
- LIMOSS API Gateway
- DDM (Delegated Data Manager)
- MBG (Market Business Glossary)
- SDC (Structured Data Capture)
- ME (Message Exchange)
- Gemini (Expert fees)
- DXC contracts manager for IUA and LMA

Learn more at [LIMOSS.London](https://limoss.london) or email [servicedesk@limoss.london](mailto:servicedesk@limoss.london)

# LIMOSS SSO Suite of Tools

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

## 3 Key Components<sup>1</sup>:



### LIMOSS Single Sign On (SSO)

Users can access LIMOSS and other Market solutions using the same username and password.<sup>2</sup>



### LIMOSS API Gateway

Secure and simple method for integrating market firms' IT systems with LIMOSS and other Market solutions.



### LIMOSS Secure Data Exchange (SDE)

Optional easy-to-use tool for securely exchanging data between Market participants. Can be accessed via online interface or via API.

[SDE User Video](#)

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

<sup>1</sup> – Commercial Agreements may collectively refer to these components as “Common Services”

<sup>2</sup> – LIMOSS SSO does not see or store user passwords

# LIMOSS SSO

## Introduction



# LIMOSS SSO

## Introduction to LIMOSS SSO

### Simple Authentication Solutions

- Provides authentication for multiple market services – E.g. DDM; SDE; LIMOSS API Gateway
- Allows users to [access Lloyd's services with LIMOSS SSO](#) user accounts
- Online registration for [organisations](#) and [users](#)

### Industry Standard Technology

- Uses a managed Azure Active Directory (AAD) tenant with MS-Azure B2B Collaboration
- Tenant contains guested-in user accounts registered within organisational entity groups
- Tenant also holds details of published APIs and registered client apps

### Designed for use by London Market Organisations

- On-boarding involves KYC and contractual protocols
- Access is free to non-Carrier organisations
- Email [servicedesk@LIMOSS.London](mailto:servicedesk@LIMOSS.London) for full charging details

### Works for all Azure Presences

- LIMOSS SSO works for all end users, even if they do not have a [managed Azure presence](#)
- A managed Azure presence *is* required for user accounts calling the LIMOSS API Gateway

**See the [LIMOSS SSO Overview](#) for further details**

### “Authorised Contact” Approval Process

- All Service Requests must be approved by an “Authorised Contact” in each organisation.
  - E.g. Approval to add/remove user accounts; Approval to subscribe to an API
- Organisations must have a minimum of 1 Authorised Contact but there is no upper limit
- LIMOSS Recommends having different Authorised Contacts in lower environments

### Authentication not Authorisation

- Having a LIMOSS SSO account gets a user account ‘into the lobby’
- Accounts can’t access an SSO protected App/API unless the relevant service owner allows it

LIMOSS SSO (including SDE and the API Gateway) exists in 3 environments:

1. **SANDBOX** – Development environment suitable for building APIs and Apps. This environment is suitable for developers but not for business users or live data
  2. **PRE-PROD** – Test environment for integrating APIs and Applications. This environment is suitable for developers but not for business users (except for UAT/MAT) or live data.
  3. **PROD** – Live production environment where business users and live APIs/Applications exist. APIs/Apps in development cannot be added to the PROD environment.
- Organisations must be on-boarded in PROD before accessing SANDBOX or PRE-PROD
  - Environments are standalone. E.g. An App in SANDBOX cannot call an API in PRE-PROD

# LIMOSS API Gateway

## Introduction





# LIMOSS API Gateway

## A brief introduction

- LIMOSS API Gateway provides a secure, standardised interface for publishing and consuming APIs relevant to the London insurance Market
- A synchronous, RESTful-based API Gateway is provided via Microsoft Azure API Management
- “Subscribers” in approved organisations can securely call numerous API Endpoints provided by multiple API “Publishers” E.g. PPL is a Publisher; Vendors/Market Firms are Subscribers
- The API Gateway enforces 4 requirements for every API call:
  1. The organisation is known and registered for the API Gateway (using X509 SSL certs)
  2. The user account calling the API is known and authenticated
    - Depending on how the APIs are published and how the subscribing app is developed, the account can be a service account OR an end user’s account
    - Whichever model is used, the calling account must be registered in LIMOSS SSO<sup>1</sup>
  3. The application calling the APIs is registered in LIMOSS SSO
  4. The organisation is authorised to call the specific API
- A successful API call will be passed to the back-end platform E.g. PPL
- The platform may perform additional authorisation checks on the calling account
- A list of response codes and suggested actions is at Annex A
- 3 independent instances of the API Gateway exist: SANDBOX, PRE-PROD and PROD

# Subscribing to an API

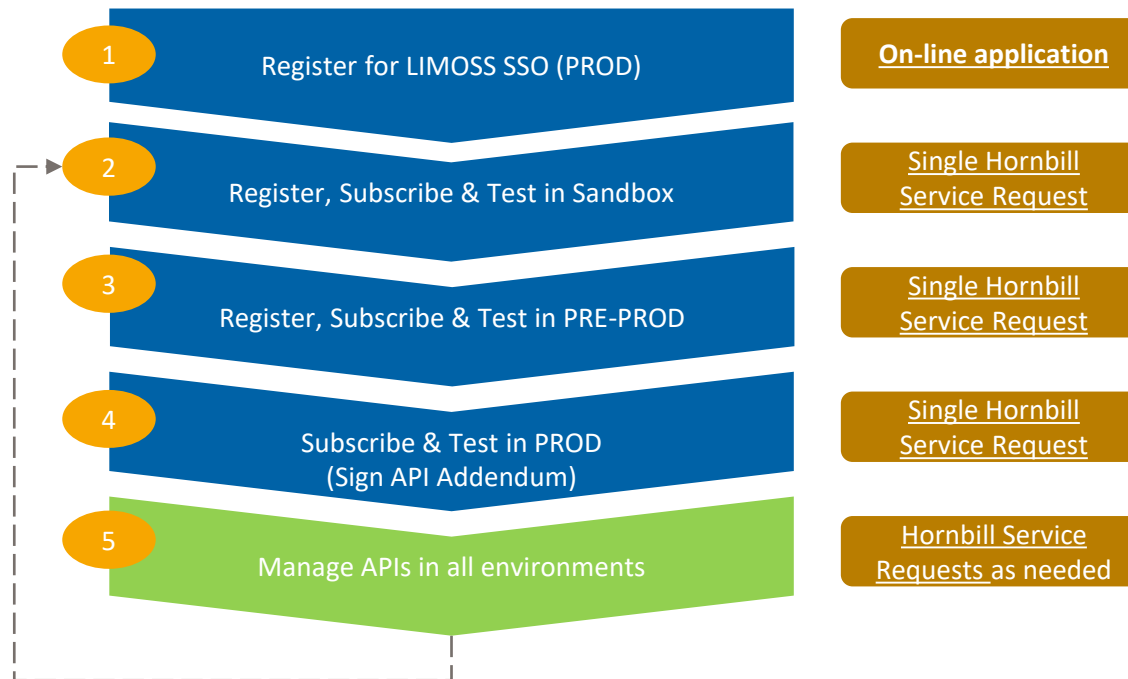
## Overview



# Subscribing to an API

## High level view of Subscribing to an API

- Subscribing to an API via the LIMOSS API Gateway is a 5-step process:
  - First step is to register for SSO in PROD (one-time only)
  - Steps 2-5 can be repeated as often as necessary for multiple different APIs
  - 3-5 working days should be allowed for each Service Request to be fulfilled



For help with the [on-line application](#) or [Hornbill](#) contact [servicedesk@LIMOSS.London](mailto:servicedesk@LIMOSS.London)

# Subscribe to an API - Breakdown

## Individual steps involved in Subscribing to an API

### “Subscribe to API” Hornbill Ticket



Tasks 1-5 are actioned by LIMOSS after a ‘[Subscribe to API](#)’ request is submitted via Hornbill

#### Notes

- 1 – Actioned automatically if organisation is not already registered in that environment
- 2 – Additional user accounts can be added/edited/removed at any time
- 3 – The subscribing organisation must provide an [X.509 SSL Certificate](#) for each environment
- 4 – At least one web app or native app must be registered. This will generate the App-ID and App-Secret needed when the client app calls an API.
- 5 – Devs can select from the [list of available APIs](#) in each environment. API subscribers must sign the “LIMOSS API Addendum” to access APIs in PROD and may need to sign API Publishers’ commercial agreements. Design/security standards for the Gateway and specific API Specs are available to approved API subscribers.
- 6 – API Publishers may require test evidence before allowing API registration in PRE-PROD/PROD

# Hornbill



Dear Matthew, thank you for contacting the LIMOSS Service Desk to Subscribe to an API via the LIMOSS API Gateway.

This option allows you to setup a new Subscription to an available API or to amend an existing Subscription.

For all new Subscriptions, you will need to provide the following information:

- Details of all user accounts that will need to use the API
- The Common Name of an X.509 SSL Certificate owned by your organisation
- Name and Email address of an Authorised Signatory in your organisation
- Details of any Applications you wish to use to call the APIs

If you don't have all this information now, don't worry. You can still create a Service Request and provide any missing information later. More information is available in the "Subscribing to an API" User Guide.

Your request will need approval by a LIMOSS SSO Authorised Contact in your organisation. If you are not an Authorised Contact, your request will be passed to your nominated Authorised Contact(s) for approval. Approval will also be needed from the API Publisher, which LIMOSS will request on your behalf.

**Do you wish to setup a new Subscription to an API or amend an existing subscription?**

Setup a new API Subscription

**Which environment does your request relate to?**

LIMOSS PRE-PROD Environment

Next

Online intuitive portal

Available to users with LIMOSS SSO PROD accounts

Users can raise Service Requests and Incidents for most LIMOSS Services

Guides users through relevant questions when subscribing to an API

Accessible at [customer.hornbill.com/limoss](https://customer.hornbill.com/limoss) and from the [LIMOSS SSO Portal](#)

For help with [Hornbill](#) contact [servicedesk@LIMOSS.London](mailto:servicedesk@LIMOSS.London)

# Information needed

[Click Here to Subscribe to an API Now](#)

- The link above will allow registered users to subscribe to an API
- You will be asked to provide the following information:
  - The user account(s) that will call the API
    - See [user accounts guidance](#)
  - An X.509 SSL Certificate that will identify your organisation
    - See [certificate guidance](#)
  - An Application that will call the API
    - See [application guidance](#)

If you don't have all the information now, you can still create your request and provide additional information later.

# Devolved Admin Portal (DAP)

DAP is a self-service tool for adding, editing and removing User Accounts in LIMOSS SSO

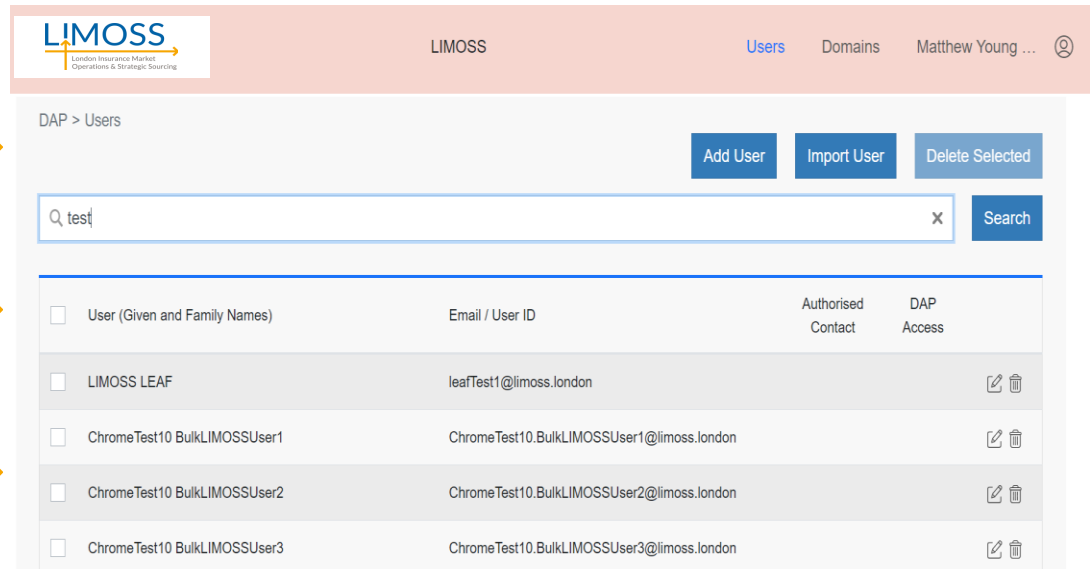
Online intuitive portal

Accessible to Authorised  
Contacts only

Real-time management of user  
accounts and approved domains

Learn more at [DAP User Guide](#)

Available in [SANDBOX](#), [PRE-PROD](#) and [PROD](#) environments



The screenshot shows the LIMOSS DAP Users management interface. At the top, there is a navigation bar with the LIMOSS logo, the text 'LIMOSS', and user information 'Users Domains Matthew Young ...'. Below the navigation bar, the page title is 'DAP > Users'. There are three buttons: 'Add User', 'Import User', and 'Delete Selected'. A search bar contains the text 'test' and a 'Search' button. Below the search bar is a table with the following columns: 'User (Given and Family Names)', 'Email / User ID', 'Authorised Contact', and 'DAP Access'. The table contains five rows of user data, each with a checkbox on the left and edit/delete icons on the right.

<input type="checkbox"/>	User (Given and Family Names)	Email / User ID	Authorised Contact	DAP Access
<input type="checkbox"/>	LIMOSS LEAF	leafTest1@limoss.london		
<input type="checkbox"/>	ChromeTest10 BulkLIMOSSUser1	ChromeTest10.BulkLIMOSSUser1@limoss.london		
<input type="checkbox"/>	ChromeTest10 BulkLIMOSSUser2	ChromeTest10.BulkLIMOSSUser2@limoss.london		
<input type="checkbox"/>	ChromeTest10 BulkLIMOSSUser3	ChromeTest10.BulkLIMOSSUser3@limoss.london		

See the [DAP User Guide](#) or contact [servicedesk@LIMOSS.London](mailto:servicedesk@LIMOSS.London) for help using DAP

# LIMOSS API Gateway

## Useful Information





## Certificates

### X509 Certificates

- All organisations using the API Gateway must provide an X509 certificate for each environment
- Both the cert Common Name (CN) and Public Key must be shared with LIMOSS
- Same certificate *may* be used in SANDBOX & PRE-PROD (although LIMOSS advise against this).
- The certificate provided for PROD must not be used in SANDBOX or PRE-PROD
- It is the organisation's responsibility to ensure certificates are kept in-date and that any changes to the CN (Certificate Name) are passed to LIMOSS Service Desk 4 weeks in advance
- X509 certificate must not be self-signed, wildcard or SAN certificate
  - SAN certificates can be used for a single path only
- Certificates must be sourced from a certificate Authority on the [Microsoft list of approved CAs](#)
- The price of certificates can vary but free certificates do exist
  - E.g. <https://letsencrypt.org>
  - LetsEncrypt appears under "Internet Security Research Group (ISRG)" on MS list
- The decision of which CA to use lies with the subscribing organisation.
- LIMOSS does not recommend or endorse any CA

## Certificate File Types; Grant Flow Methods; API Specs

### Certificate Files

- Microsoft Azure cloud platform requires certificates files in a single PKCS#12/PFX format. The PKCS#12 certificates are in binary form, contained in .pfx or .p12 files. When sending certificates in API Gateway requests, the certificate format should be binary encoded. The binary encoded formats are DER(.der, .cer) and PKCS#12(.pfx, .p12).
- A cert thumbprint cannot be passed to the API Gateway as this is not a valid certificate format.

### Grant Flow Methods

- LIMOSS API Gateway supports ROPC Grant Method and will shortly support Client Credentials Flow and App Credential Flow
- Further guidance on Grant Flow methods is available from LIMOSS Service Desk

### API Specs

- All APIs published via the LIMOSS API Gateway have an API Specification document/Swagger
- The API Spec will be provided to firms, once they have subscribed to a specific API
- These will be provided either by the LIMOSS Service Desk or the API Publisher
- The API Spec details the business use case of the API, how to call it, expected responses and code samples
- LIMOSS is not responsible API Specs relating to 3<sup>rd</sup> party APIs

# Useful Information

## Throttling; Security Model Review; Security Essentials

### Throttling

- Throttling prevents a back-end solution being overwhelmed by a large volume of API calls
- Throttling is activated now for some APIs
- All client apps should be able to handle Response Code 429 (See [Annex A](#))
- Throttling is not an exact science - some calls either side of throttling rate may be accepted/rejected: <https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies#LimitCallRateByKey>

### LIMOSS API Security Model Review

- LIMOSS is conducting a market-wide review of the current API Gateway security model
  - E.g. Possible relaxation of need for X509 certificates in lower environments
- Any changes will require full governance approval
- Current design will allow greater flexibility and easier on-boarding for developers but is intended to allow backwards compatibility

### Security Essentials

- Organisations must not share the following information with any 3<sup>rd</sup> parties:
  - App-ID and App-Secret
  - User account passwords
  - X509 Private Key
- Inform the LIMOSS Service Desk immediately if any of these details are compromised

# Useful Information

## API Call Logging

### API Call Logging

- All API Subscribers are advised to include a logging function in their client application
- As a minimum, the logging should include: Date/Time of all API calls; API Response Code; API Transaction ID
- This logging will assist subscribers, LIMOSS and 3<sup>rd</sup> party API publishers to triage any problems or incidents involving API calls

# Useful Information

## Email Invitations; Aligning User IDs;

### Email Invitations

- All LIMOSS SSO accounts receive an email that they must click to confirm their registration
- All accounts in LIMOSS SSO should have an SMTP email that matches their User ID
- 2 exceptions apply in all Environments:
  - For Service Accounts only: Request user invite link via LIMOSS Service Desk
  - For any account: Use Azure 'Guest Inviter' status as detailed in [On-Boarding Guide](#)

### Aligning User IDs

- The User IDs registered in LIMOSS SSO should match the User ID held in the market service
- All user accounts in LIMOSS SSO should have an SMTP email that match their User ID
- When using a "Native application" (a non-web based application) in the LIMOSS API Gateway, all user accounts must be created in a managed Azure Active Directory

### App Logos

- If you wish to display your App in the SSO Portal, an App Logo must be provided
- The logo can be provided in .jpg, .svg, and .png formats with width 35px and height 33px
- Logos should be designed to fit within a square without being stretched in either direction

Contact [servicedesk@LIMOSS.London](mailto:servicedesk@LIMOSS.London) for further details

# App Registration – App Type

## “Native Apps” and “Web Apps”

### Web App

- A Web App is any app or solution that is accessed via a URL

### Native App

- A Native App is any app or solution that is not accessed via a URL
- All apps that exist as a standalone instance on a local computer or server are Native

### Web Apps vs Native Apps

- The App Type (Web or Native) is needed when registering an App in the LIMOSS API Gateway
- Once registered, the “App Id” will be returned by the LIMOSS Service Desk

An App ID provided for a Web App can NOT be used with a Native App  
 An App ID provided for a Native App can NOT be used with a Web App

- If Postman is used to conduct Dev/Testing, the Postman App must be registered as a ‘Native App’ (assuming that it is a local instance of Postman, running on a developer’s own computer/server and not a web-based instance of Postman)
- If the solution being developed will be a web-based app (accessible via URL), then this app must be registered as a ‘Web App’ **only if** the web app itself will call APIs
- If the solution being developed is web-based – but it integrates with a native backend app – and only the back-end app calls the APIs, the app must be registered as a ‘Native App’
- Contact [servicedesk@LIMOSS.London](mailto:servicedesk@LIMOSS.London) for further advice

# App Registration – App Settings

## Sign-In URL; App Credentials

### Application Homepage URL

- For Native Apps: OPTIONAL: Put https://localhost/[port number] or 'N/A'
- For Web Apps: MANDATORY: Provide the homepage URL for your App

### Sign-In URL

- For Native Apps: NOT REQUIRED
- For Web Apps: MANDATORY: Provide the URL where users are expected to sign-in to your app. This URL may also be known as the 'Reply URL' and may be the same as the Application Homepage URL

### App Credentials

- Once an App has been registered, the following App Credentials will be provided:
  - Tenant ID
  - App ID (or Client ID)
  - App Secret (or Client Secret)

**The App Secret must NOT be included in API calls when using Native apps  
The App Secret MAY be included in API calls when using a web app**

- App Credentials must be securely protected and never shared with unauthorised parties
- The LIMOSS Service Desk must be informed immediately if App Credentials are compromised

# Testing

## Pre-Testing Checks

Before running major testing, pre-test API calls should be run to ensure the following 4 criteria:

### 1 - Valid certificate registered:

- The X.509 cert must be registered in the environment where testing will take place
- The certificate Common Name used in the API call must match the details held by LIMOSS
- The certificate must be in-date and the correct Private Key<sup>1</sup> must be used in the API call

### 2 - Organisation subscribed to API(s):

- The organisation that has registered the certificate must be subscribed to the relevant API(s) in the environment where testing will take place

### 3 - User account(s) registered:

- The user account(s) that will call the API(s) must be registered and activated in the environment where testing will take place
- The accounts must be borne in Azure and must NOT have MFA activated
- To check if an account is registered, log-in to the relevant portal with the account's credentials: [Sandbox Portal](#); [Pre-Prod Portal](#); [Prod Portal](#)
- If needed, user account(s) must also be registered with the API publisher

### 4 - App registered:

- The App used for testing must be registered in the environment where testing will take place
- The correct App credentials must be entered in the API call



# LIMOSS API Gateway

## Problem Solving



# Trying to call an API?

A successful API call needs the user account, the API subscription, the X.509 certificate *and* the client app to be registered correctly in the current environment

If any of these components are incorrectly configured, the API call will fail

1 Are the environments aligned?	2 Is the user account active?	3 Is the organisation subscribed to the API?	4 Is the X.509 certificate correctly registered?	5 Is the client app correctly registered?	Successful API Call?
✓	✓	✓	✓	✓	YES 😊
✗	✓	✓	✓	✓	No 😞
✓	✗	✓	✓	✓	No 😞
✓	✓	✗	✓	✓	No 😞
✓	✓	✓	✗	✓	No 😞
✓	✓	✓	✓	✗	No 😞

# API Call Problems

- 1) **Environment:** Confirm which LIMOSS SSO environment the API is being called in: SANDBOX, PRE-PROD or PROD
  - The 3 LIMOSS environments are totally separate. Credentials registered in one environment won't work in any other
  
- 2) **User Account:** Check the account calling the API is active by logging-in to the relevant portal with the account's credentials:
  - [Sandbox Portal](#); [Pre-Prod Portal](#); [Prod Portal](#)
  - If the portal can be accessed with the account credentials, the account is active in this environment
  - Are account credentials mis-typed in the Postman call or App coding? If needed, is account registered with API publisher?
  - Is the account hosted in an Azure tenant and is MFA inactive for the account in that tenant?
  
- 3) **API subscription:** Ask LIMOSS Service Desk to check that your organisation is subscribed to the relevant API in this environment AND ask them to confirm the URI for the API
  - Is the API URI provided by LIMOSS mis-typed in the Postman call or App coding?
  
- 4) **X.509 certificate:** Ask LIMOSS Service Desk to confirm the Common Name (CN) for all certificates registered for your organisation in this environment
  - Is the certificate "Private Key<sup>1</sup>" mis-typed in the Postman call or App coding?
  - Is the cert in-date?
  - Read the guidance on [X.509 certs](#)
  
- 5) **App registration:** Ask LIMOSS Service Desk to confirm the App Credentials<sup>1</sup> for the App in this environment AND whether the App is registered as a Native or Web App?
  - Is the "App ID<sup>1</sup>" or "App Secret<sup>1</sup>" mis-typed in the Postman call or App coding?
  - Is the App being used to call the API the same type (Native/Web) as the App registered in LIMOSS?
  - Read the guidance on [App types](#) and [App Settings](#)
  
- 6) **Check the API Response Code:** If you are able to make an API call, you will receive an API response code.
  - Check the response received against the list of [API Response codes](#) and complete the suggested actions

**Still not working? Email [servicedesk@LIMOSS.London](mailto:servicedesk@LIMOSS.London) to report a defect (SANDBOX/PRE-PROD) or Incident (PROD)**

# LIMOSS Support

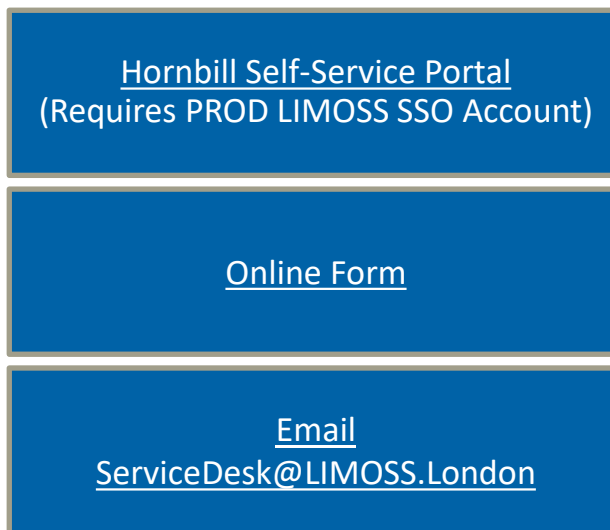
## Service Desk



# LIMOSS Support

## Support Points

LIMOSS Service Desk provides support for LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway



**Open 8am-6pm (UK) Mon-Fri (excluding English Bank Holidays)**

## Incident Priority Definitions

**P1 - All** APIs via the PROD (LIVE) LIMOSS API Gateway are unavailable or severely degraded. P1 Tickets reported during LIMOSS working hours will receive support 24/7/365 until resolved.

**P2** - One or more APIs are unavailable via the PROD (LIVE) LIMOSS API Gateway or severely degraded but at least one API remains available. P2 Tickets reported during LIMOSS working hours will receive support 8am-8pm (UK) until resolved.

**P3/P4** - Minor Degradation of API Service and all API incidents in non-production environments. P3/P4 Tickets reported during LIMOSS working hours will receive support 8am-6pm (UK) until resolved.

# LIMOSS

London Insurance Market  
Operations & Strategic Sourcing

# Annex A

## API Gateway Response Codes



# LIMOSS API Gateway Response Codes 1/2

Code	Response	Response Description	Suggested Action
200	OK	Standard response for successful requests	No action needed
403	Token validation failed: malformed token or empty issuer	Error is thrown when the provided failed to parse token or token doesn't have issuer	Raise to LIMOSS Service Desk as Incident
404	API operations not found	Error is thrown when the provided API operation isn't found	Raise to LIMOSS Service Desk as Incident
429	Throttling Rate Exceeded	The number of calls per min has exceeded the throttling limit set by the API publisher	Wait for number of seconds stated in header and re-submit API call
500	Gateway error	Investigation by LIMOSS SSO Vendor is needed	Raise to LIMOSS Service Desk as Incident
500	Gateway error: multiple MPOs found		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: Gateway error		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: OpenID has no public keys		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: error calling JWKS url		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: no jwks in OpenID		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: error calling OpenID url		Raise to LIMOSS Service Desk as Incident
500	Error validating token: Gateway error		Raise to LIMOSS Service Desk as Incident



# LIMOSS API Gateway Response Codes 2/2

Code	Response	Response Description	Suggested Action
400	Error validating token: malformed amr	Error is thrown when the provided token's AMR claim values are incorrect	Raise to LIMOSS Service Desk as Incident
400	Error validating token: malformed appid	Error is thrown when the provided token's AppId claim value is incorrect	Raise to LIMOSS Service Desk as Incident
400	Trace header length exceeded	Error is thrown when the provided trace header length is more than 24 symbols	Raise to LIMOSS Service Desk as Incident
401	Bearer missing in Authorization token	Error is thrown when the provided token Bearer prefix is missed	Raise to LIMOSS Service Desk as Incident
401	Client certificate is missing	Error is thrown when the certificate is missed	Check X509 Certificate is correct, in date and registered with LIMOSS Service Desk
401	Authorization token is missing	Error is thrown when the token is missed	Raise to LIMOSS Service Desk as Incident
403	Authorization failed	Error is thrown when the token validation is failed	Raise to LIMOSS Service Desk as Incident
403	Client certificate validation failed: expired certificate	Error is thrown when the provided certificate is expired	Check X509 Certificate is correct, in date and registered with LIMOSS Service Desk - specifically certificate expiry date
403	Client certificate validation failed: incorrect start date	Error is thrown when the provided certificate start date is incorrect	Check X509 Certificate is correct, in date and registered with LIMOSS Service Desk - specifically certificate start date
403	Client certificate validation failed: untrusted certificate	Error is thrown when the provided certificate is untrusted	Check X509 Certificate is correct, in date and registered with LIMOSS Service Desk
403	Client certificate validation failed: unknown domain	Error is thrown when the provided certificate CN isn't set in MPO object	Check X509 Certificate is correct, in date and registered with LIMOSS Service Desk Check that correct domain name has been provided in API Call

# Annex B

## Glossary



# Glossary

## LIMOSS SSO – terms and definitions

Term	Definition
Authorised Contact	A trusted person in a client's organisation that is authorised to approve any Service Request for that organisation within the LIMOSS SSO suite of tools.
API	Application Programming Interface
App	Application
CH	Change
CR	Change Request
CS	Common Services. This term may be used in legal and other documentation to refer to LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway
CSV	Comma Separated Values
DAP	Devolved Admin Portal
IE	Internet Explorer
LIMOSS	London Insurance Market Operations & Strategic Sourcing
MPO	Market Participant Organisation
MUA	Master User Agreement
SDE	Secure Document Exchange
SSO	Single Sign On
T&C's	Terms and Conditions
URI	Uniform Resource Identifier
URL	Uniform Resource Locator