INFOGRAPHIC SERIES

IRAS DIGITAL PARTNERSHIPS

CORPPASS & CALLBACK URL GUIDE

IRAS Corppass API

Corppass is an integrated, **self-service login platform** for business users transacting on Government digital services.

Provides **G2B Authentication** - A convenient & secure means for businesses to transact digitally with government agencies.

Built on the **National Digital Identity (NDI)** Framework.

1. Corppass API Flow

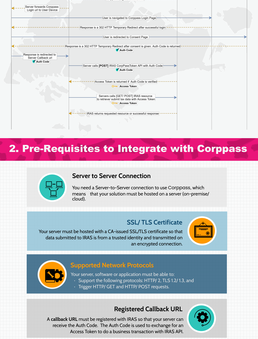
Using Corppass API consist of TWO methods that must be done in sequence:

HTTP GET `/hostauthication/CorpPassAuth`

Returns Auth Code in the URL query parameter, after redirects to Corppass Login and Consent pages

HTTP POST `/hostauthication/CorpPassToken`

Returns Access Token in JSON response body providing the Auth Code



2. Pre-Requisites to Integrate with Corppass

Server to Server Connection

You need a Server-to-Server connection to use Corppass, which means that your solution must be hosted on a server (on-premise/ cloud).

SSL/ TLS Certificate

Your server must be hosted with a CA-issued SSL/TLS certificate so that data submitted to IRAS is from a trusted identity and transmitted on an encrypted connection.

Supported Network Protocols

- Your server, software or application must be able to:
  - Support the following protocols: HTTP 2, TLS 1.2/ 1.3, and
  - Trigger HTTW GET and HTTW POST requests

Registered Callback URL

A **callback URL** must be registered with IRAS so that your server can receive the Auth Code & Access Token. The Auth Code is used to request for an Access Token to do a business transaction with IRAS API.

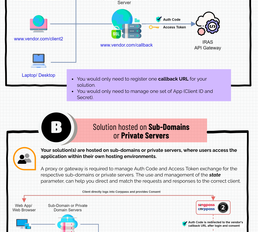
!

- Refer to following guidelines to help you understand how your solution should **interface with IRAS Corppass API** using the **callback URL**.

A

Solution hosted on the **Cloud** or a **Standalone Server**

Your solution is hosted on the cloud or a standalone ('Web/ App') server, where users access the application using their web browser or device (e.g. Desktop/ Laptop).



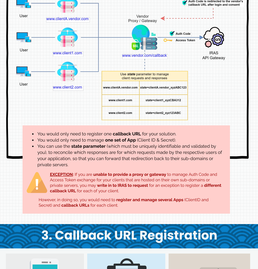
- You would only need to register one **callback URL** for your solution
- You would only need to manage one set of App (Client ID and Secret)

B

Solution hosted on **Sub-Domains** or **Private Servers**

Your solution(s) are hosted on sub-domains or private servers, where users access the application within their own hosting environments.

A proxy or gateway is required to manage Auth Code and Access Token exchange for the respective sub-domains or private servers. The proxy or gateway will determine the **state** parameter, can help plug direct and match the requests and responses to the correct client.



- You would only need to register one **callback URL** for your solution
- You would only need to manage one set of **App** (Client ID & Secret)
- You can use the **state parameter** (which must be uniquely identifiable and validated by you) to reconcile which responses are for which requests made by the respective users of your application, so that you cannot that redirection back to their sub-domains or private servers.

EXCEPTION If you are **unable to provide a proxy or gateway** to manage Auth Code and Access Token exchange for your clients (i.e. hosted on their own sub-domains or private servers), you may **write to IRAS to request** for an exception to register a **different callback URL** for each of your clients.

However, in doing so, you would need to **register and manage several Apps** (ClientID and Secret) and **callback URLs** for each client.

3. Callback URL Registration

CREATE ACCOUNT & APP

Refer to User Guide - https://www.iras.gov.sg/irasgw/help to **create an account & app on API Marketplace**.

After which, you would be provided with a Client ID that is required to register your **callback URL**.

REGISTER CALLBACK URL

Register your **callback URL** with IRAS via **FormSG** - https://form.gov.sg/callbackurl

CATER FOR PROD & SANDBOX ENV

You would need to provide one **callback URL** each for **Sandbox** & **Production** environments. The Sandbox environment is a near-replica of Production environment, designed to simulate closely the requirements for Production.

!

Requirements:

Callback URLs must fulfill the following requirements:

- Must not be same for both Sandbox and Production environments
- Must use Fully Qualified Domain Name (FQDN)
- Must not contain IP address, port number, hash sift or wildcard (*) characters
- Must be unique
- Must be able to accept parameters.
- Must be hosted on a server with a Secure Sockets Layer (SSL) certificate (e.g. https://yourdomain.com/callbackURL)

It takes about 1-2 weeks to register your **callback URL**. IRAS will notify you by email once your **callback URL** has been registered.

4. Integrating & Testing Corppass

IRAS will inform you once your **callback URL** has been successfully registered.

You may then proceed to integrate and test your application with Corppass using this walkthrough (link on right)

CLICK HERE!

5. Frequently Asked Questions (FAQ)

1 *"Does the Access Token have an expiry time, is it reusable or one-time only?"*

The access token is valid for 30 mins, and it is re-usable from the same Client ID, State and Scopes that the **Corppass** user is authorised for.

2 *"Can I change my Client ID or callback URL at a later stage or upon failure?"*

Callback URL registration is considered a one-time process, therefore changing it is not recommended. It takes 1-2 weeks to apply the changes, which may result in service interruption. However, you may write to to IRAS if you need to change the callback URL or if your Client ID has been compromised.

3 *"Can we register a callback URL for production environment first, before registering a different one for Production?"*

Yes, in fact the callback URL **is only registered** in Production when you have completed your tests and validation in the Sandbox environment.

4 *"For testing purposes, can we register a localhost URL for a server that does not have a domain name (e.g. http://localhost/ or TLS/ SSL certificate (e.g. https://localhost.com/)?"*

You will not be able to use this service with Corppass as a never-to-server connection with TLS/ SSL is required.

5 *"Can we share the Client ID and Secret with our sub-contractors that are managing our clients' servers and application?"*

No, you may not. The Client ID and Secret that you use and callback URL that you register with IRAS must be wholly owned, managed and maintained by you or your company's authorised representatives/ officers, without disclosure to your customers / clients/ third-parties, or anyone unauthorised by your company.

- You may refer to the IRAS API Terms of Use.

6 *"Can I use self-signed SSL certificate for my testing server in Sandbox?"*

A self-signed certificate is insufficient to assist the requirements of a server-to-server to connection with TLS/ SSL. You would need to use a certificate issued by a trusted CA (Certificate Authority) for both environments.

7 *"Can we use the same App (Client ID and Secret) for my clients that are hosted on our sub-domains (e.g. client1.mydomain.com, client2.mydomain.com)? Managing our clients' servers and application?"*

You may use the same Client ID and Secret if you register a single callback URL to manage all the authentication and authorisation requests for your clients, through a centralised server that acts like a proxy or gateway. If you require a different callback URL for each of your client on the sub-domain, you would need to create and manage a different App (Client ID and Secret) for each of your client.

6. Troubleshooting

CorppassAuth API returns error message: **"400 - Unauthorised Error".**

- The **App** has not **subscribed** to the **API plan** at the API Marketplace.
- The **Client ID and Secret** are incorrect or were **not passed in** the API Header.

CorppassAuth API returns error message: "Callback URL Mismatch with Client Registered Callback URL". OR **"Scope Mismatch with Client Registered Scopes"**

- **App Client ID** and **callback URL** must be **registered** first with IRAS.
- The correct **App Client ID** must be passed in the **API Header** and the correct **callback URL** must be passed in the **API Query Parameter**.

NOTE: Please notify IRAS immediately if your App Client ID has been changed.

CorppassToken API returns error message: **"Internal Server Error Occurred".**

- **Auth code** can be **used only** once to exchange for an access token.

An error message is shown when trying to log in with Corppass: **"Your Corppass Account is not authorised to access this e-Service. (B4J) Portal. Please contact your Corppass Admin."**

- Please contact **Corppass Admin to configure** the **authorisation rights** for the Corppass account used.
- If you are testing the **API in Sandbox**, ensure that the Corppass account used is the "Test" IDIS Corppass Test accounts in the Sandbox environment are not configured to support Tax Agents.

CorppassAuth API returns HTML error page: **"IRAS Website is unavailable, please try again later or refer to IRAS website."**

- The parameter **"content-type=application/json"** is required to be passed in the HTTP Header for calling CorppassAuth API.

USEFUL REFERENCES

Additional references that may come in handy during your onboarding journey with us.

1 Weekly Maintenance Hours:

(Sandbox Environment)				(Production Environment)	
All APIs		Singpass/Corppass APIs		All APIs	
Everyday	1:00 PM – 3:00 PM	Wednesday	3:00 PM – 11:59 PM	Wednesday	2:00 AM – 6:00 AM
Everyday	8:00 PM – 10:00 PM			Sunday	2:00 AM – 8:30 AM
Sunday	8:00 PM – 3:00 AM				

(Accurate as at 1 Oct 2020. For updates, please refer at IRAS Maintenance)

2 Callback URL Registration:

3 Corppass API Specifications:

4 API Marketplace User Guide:

IRAS API Marketplace

Production - apiservices.iras.gov.sg

Sandbox - apisandbox.iras.gov.sg

API Onboarding & Account Matters: Digital_Partnerships@iras.gov.sg

API Technical Support: API_Support@iras.gov.sg