Access to the IPND Web Portal

Document Release History:

Date	Section	Detail of Change
Feb 2023	All	Document created - Penny Waite
Apr 2023	Initial Setup	Document reviewed & Updated - Penny Waite
Jun 2023	All	General update - Penny Waite
Oct 2023	All	General update - Penny Waite
Dec 2023	All	Added provision for CSP access - Penny Waite
Jun 2024	All	General update - Penny Waite
Apr 2025	All	General update - Penny Waite

Table of Contents

Document Purpose:

This document is to provide IPND Data Providers, Carriage Service Providers (CSPs) and Data Users an overview of the Web Portal, as well as the process for requesting access and completing Web Portal User Setup and registration.

Web Portal Overview:

Web Portal Functionality:

The below functionality is available in the Web Portal for registered IPND Data Providers, CSPs, Data Users/Consumers, the Regulator and the IPND Manager:

- Self-service functionality:
  - Schedule data extracts / data refresh and view request history / status *(Data Provider, CSPs & Data User/Data Consumer)*
  - Perform Public Number query and view results *(Data Provider & IPND Manager)*
  - Perform queries for specific errors *(Data Provider)*
  - Register to receive Error Notifications / Subscriptions via email or sms *(Data Provider)*
  - Create User Query's to report an error with a specific Public Number *(Data User/Data Consumer)*
  - Access Management: add new Organisation Admin and General User *(Data Provider, CSPs & Data User/Data Consumer Organisation Admins & IPND Manager)*
  - Access Management: create new Organisations and Organisation Admins *(IPND Manager)*
- View Customer Record Upload File status and errors *(Data Provider & IPND Manager)*
- View Download File status for the various files that the IPND produces for Download to Data Providers, CSPs, Data Users/Consumers, the Regulator and the IPND Manager *(Data Provider, CSPs & Data User/Data Consumer Organisation Admins & IPND Manager)*
- View Error File Status *(Data Provider & IPND Manager)*
- View & Download Error Summary / Trends for further analysis *(Data Provider)*
- Download Change CSP Report *(CSPs only)*
- Download CSP Snapshot File *(CSPs only)*
- Download CSP Soft Error File *(CSPs only)*
- View & Download Management Reports *(IPND Manager & Regulator)*

Web Portal Access Availability:

Web Portal access is available:

- For all active organisations who are registered with the IPND Manager as either a Data Provider, a Data User / Data Consumer or as a CSP.
  - Users requesting access must be a registered contact for their organisation with the IPND Manager.
- 24hrs x 7days for registered user access, however a maintenance window of 12:00 (noon) and 14:00 daily will be reserved.
- User access to the Web Portal is locked after a period of 60 days inactivity. Contact your Organisation Admin or the IPND Manager (via email to IPND.Manager@team.telstra.com) to have access re-enabled.
- User Support is available during Business Hours (AEDT).

Web Portal User Requirements:

To access the IPND Web Portal, users will require:

- Google Authenticator smartphone app for 2 step authentication:
- Their organisations' IPND IIS GPG private key for decrypting download files (CSPs, Regulator and IPND Manager only).
- OpenVPN Client installed.

- Access provided by IPND Manager to authenticated users belonging to registered organizations.

Web Portal Security:

To protect the security of the IPND, the following measures have been created to allow users access to the IPND Web Portal:

- VPN Tunnel via OpenVPN
- 2 Party Authentication via Google Authenticator
- Data encryption for Download files (CSPs, Regulator and IPND Manager only)
- User configuration in the IPND Web Portal by The IPND Manager

Note: Users with restrictions applied to their PC / workspaces should engage their Organisations' IT / Tech Support for assistance for user setup. See Web Portal Troubleshooting for more information.

Web Portal Access Management:

The Web Portal includes functionality to allocate access based on individual access type and role.

The breakdown of access types and roles are as follows:

Access Type	**Role/s**
IPND Manager	• Super Admin
IPND Data Provider	• Organisation Admin • General User
IPND Carriage Service Provider	• Organisation Admin • General User
IPND Data User/Data Consumer	• Organisation Admin • General User
Regulator	• Organisation Admin • General User
Role details:	**Access Management Functionality**
Super Admin: The Super Admin role is allocated to the IPND Manager / IPND Manager Support	• Create Organisations and allocate filesource to each Organisation; • Create / authorise Organisation Admins within all Organisations; • Create / allocate General Users within all Organisations.
Organisation Admin: Organisation Admin/s can be allocated to each Organisation that has been given access to the IPND	• Create / authorise Organisation Admins within their Organisation; • Data Provider Organisation Admins can create General Users and allocate access to specific filesource within their Organisation • CSP Organisation Admins can create General Users and allocate access to specific CSP Code within their Organisation
General User: General Users can be allocated to each Organisation that has been given access to the IPND. General Users' can be allocated access to specific filesource for Data Providers and CSP Code for CSPs within their Organisation	• Access Management Functionality is not enabled for General Users: ○ General Users cannot create or provide access to others within their Organisation

Requesting Web Portal Access:

To obtain access to the Web Portal, engage the IPND Manager via email IPND.Manager@team.telstra.com to request:

a) IPND Web Portal User Access;
b) OpenVPN Credentials (if required) or to request an additional OpenVPN profile/s; and,
c) Exchange and verification of GPG public key (CSPs, Regulator and IPND Manager only). More information regarding user setup for CSPs is available via the IPND Carriage Service Providers Access to Internet Interface Service documentation on the IPND Homepage: https://www.telstra.com.au/consumer-advice/ipnd.

Important Notes:

- Organisations are added to the Web Portal with an Access Type of Data Provider (DP), Carriage Service Provider (CSP), Data User / Data Consumer (DC) or Regulator (REG).
- User access is based on the Organisation Access Type.
- The ability to download reports and data extracts from the Web Portal is restricted to CSPs only.
- Data Providers are required to use the existing process for accessing reports and data extract files from the IPND via the FTS.
- Access to Web Portal User Test and Web Portal Production environments require Users to complete a separate registration for each Web Portal environment.
- During registration, Users will be prompted to create a unique Google Authenticator token for each environment (User Test and Production).

The IPND Manager will require the below information for each user requiring access:

Please advise: Do you require a new OpenVPN Account for this request: **Y / N**

Web Portal Access Details						
Organisation Details						
Organisation Name				**Organisation Access Type (Select One)**		
Example CSP test org Pty Ltd				(DP) Data Provider	(CSP) Carriage Service Provider	(DC) Data User / Consumer
User Details						
First Name	**Last Name**	**Phone No**	**Email address**	**Role: Org Admin / General User**	**Filesource / CSP Code (General Users)**	**Web Portal Env (User Test / Production)**
Example	Test	047777777	Test@ipnd.com	General User	002	Prod only

Once the IPND Manager provisions access in the Web Portal, users will be required to complete registration to log in.

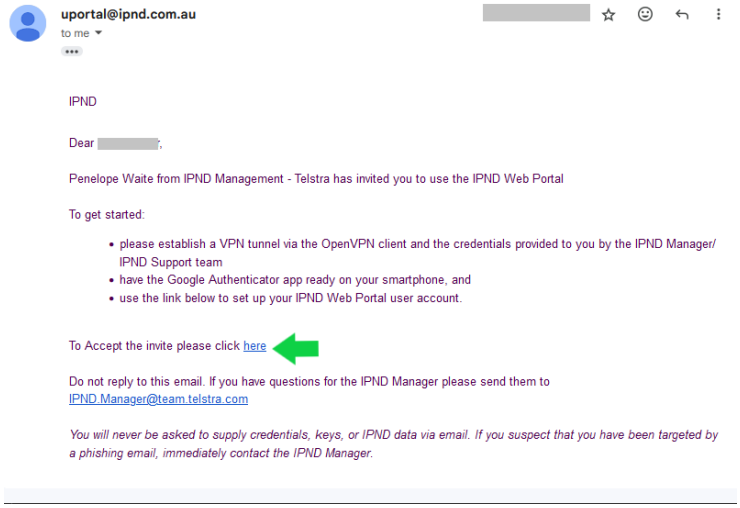
Web Portal First Time User Setup / Registration:

The IPND Manager must configure a users' details in the Web Portal using the details provided on their access request. An OpenVPN account will be issued to the user by the IPND Support Team if included on the access request.

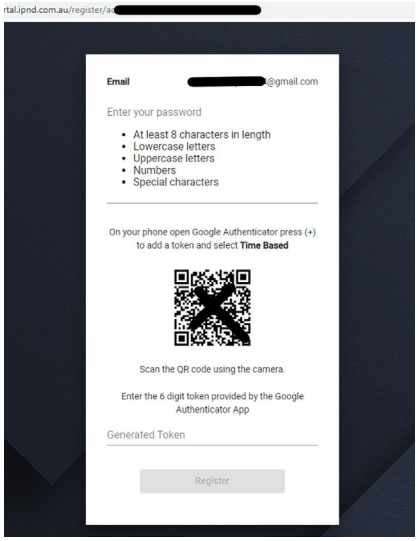
CSPs need to perform additional steps to generate, exchange and verify a GPG public key. More information regarding user setup for CSPs is available via the IPND Carriage Service Providers Access to Internet Interface Service documentation on the IPND Homepage: https://www.telstra.com.au/consumer-advice/ipnd.

Once the IPND Support team confirm that the user has an active OpenVPN account, the IPND Manager will issue an email from the Web Portal to their email address: 'Account Access Invite: IPND Web Portal'. To complete Web Portal registration and log in, the user will be required to carry out the following:

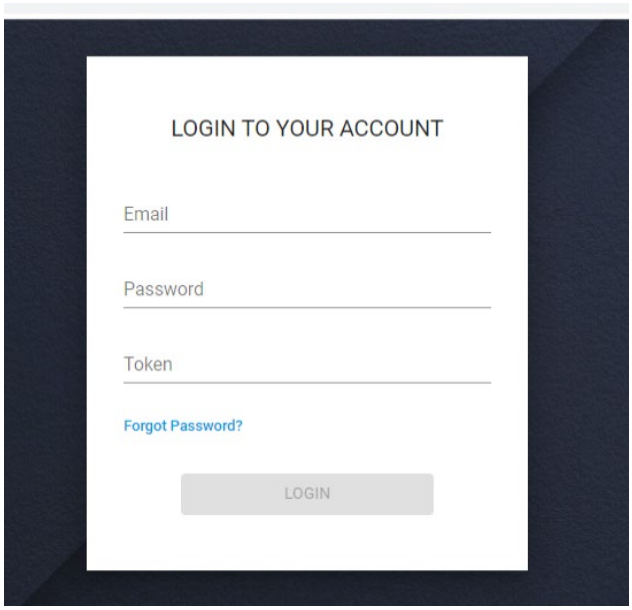
1. Establish a VPN tunnel via the OpenVPN Client.
2. On the 'Account Access Invite: IPND Web Portal' email, click the hyperlink = To Accept the invite and please click here



3. Complete Web Portal registration via the screen pop which contains the pre-populated email address as provided to the IPND Manager:
    a. In the *'Enter your password'* field, create a new password using the Google password rules provided. (Tip: do not use a # in the password);
    b. Access the Google Authenticator smartphone app;
    c. press (+) to add the token and select 'time based';
    d. scan the QR code;
    e. enter the 6 digit token/secret key provided from the Google Authenticator app into '*Generated Token*' field;
    f. click '*Register*':



4. The Web Portal login screen will appear:
    a. Complete the '*Email*' and '*Password*' fields using the registered email address and newly created password from the previous step.
    b. Access the Google Authenticator smartphone app and enter the refreshed 6 digit token/secret key provided.
    Note: users may have multiple tokens/secret keys.
    Google Authenticator will allow users to assign an account name to each for the relevant application.
    c. Click '*LOGIN*'



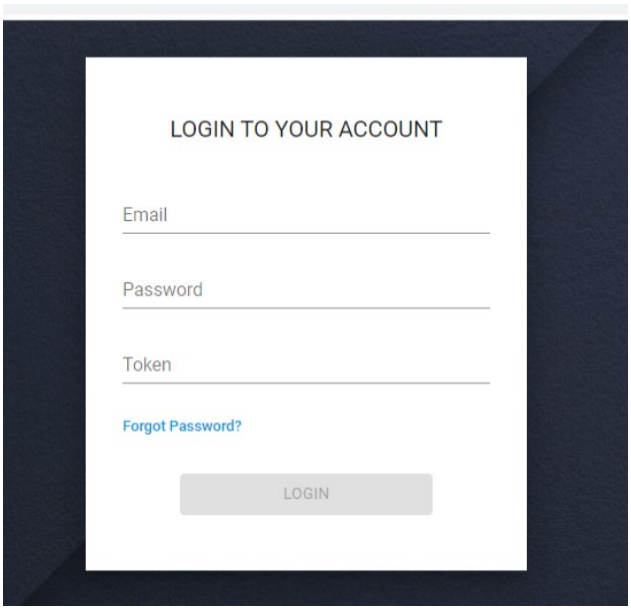
5. Read and Accept the Terms and Conditions.
6. Once successfully logged in, users will be presented the IPND Web Portal Dashboard.

Web Portal Login (once First Time User Setup / Registration is Complete)

Once the user has completed Web Portal registration and first time log in, they can log into the Web Portal using the following steps:

1. Establish a VPN tunnel via the OpenVPN Client;
2. Log into the Web Portal using the below URLs (recommend saving to favourites for later use): https://portal.ipnd.com.au

Environment	URL	IP Address
User Test	https://uportal.ipnd.com.au	https://10.11.110.31
Production	https://portal.ipnd.com.au	https://10.10.110.31



3. Complete the '*Email*' and '*Password*' fields using the registered email address and the password created during User Setup / Registration;
4. Access the Google Authenticator smartphone app and enter 6 digit token/secret key provided;
5. Read and Accept the Terms and Conditions.

Web Portal Troubleshooting:

Due to the security measures applied to protect the IPND Web Portal, some people may require assistance resolve their workplace IT restrictions.

Restrictions may apply to employee workspaces by organisations' IT to prevent the installation of non-standard applications and access to unknown sites in browsers, thereby ensuring the safety and security of the organisations IT network and data.

We strongly recommend that you consult with your organisation's IT services and obtain technical support to permit access to the IPND Web Portal.

Telstra IT carried out the below to enable their IPND Ops team access to the Web Portal:

1. Enable OpenVPN Client install on user PC (Client install maybe blocked as non-SOE);
2. Configure OpenVPN Client with proxy/proxies to enable the user to establish an OpenVPN tunnel;
3. Update to organisation Web Proxies PAC files (Proxy Auto Config);
4. Update to user PC local hosts file: adding Web Portal details:

IPND Web Portal Environment	Content for hosts file
User Test	10.11.110.31 uportal.ipnd.com.au 10.11.110.31 uportal-help.ipnd.com.au
Production	10.10.110.31 portal.ipnd.com.au 10.10.110.31 portal-help.ipnd.com.au

If further support is required, please contact the IPND Manager via email:
IPND.Manager@team.telstra.com