P11D Organiser SaaS (Hosted)

Why use the SaaS version of the P11D Organiser

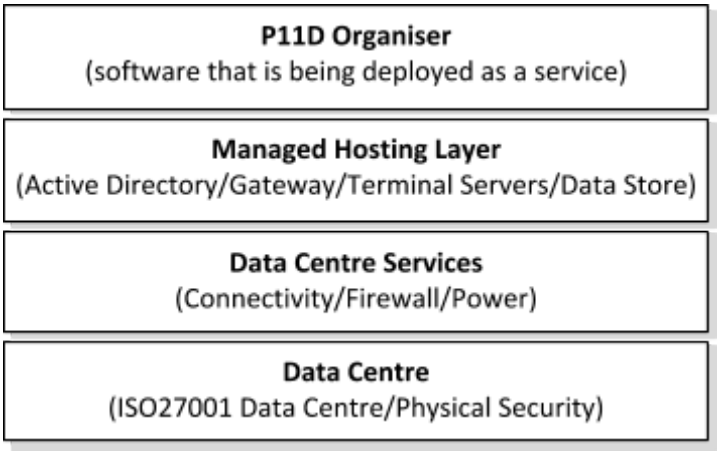
The key benefit of using the SaaS version of the P11D Organiser is simplicity - it means that you have full access to the without any IT constraints - if you have a browser and an internet connection, you can be up and running in minutes.

The are no concerns about where the software is installed and who is maintaining it, PAS Ltd take on all the load whilst you concentrate on running your business. The SaaS version offers:

- **Simplified Management** – all application management is performed centrally.
- **Ease of Deployment** – applications can be instantly delivered to end user's machines via any browser without the need for site visits or IT involvement[1].
- **Security** – all data is kept centrally on the data centre with no data left on laptops or PCs.
- **Availability** – applications can be accessed from any machine that has internet access.
- **Support** – the hosted offering allows PAS Ltd to support users through screen sharing and mirroring (with your consent).
- **Remote Working** – easily provide access to applications from remote locations with local network type performance.
- **Lower TCO (Total Cost of Ownership)** – All operating system, application support and upgrades are handled by PAS Ltd, ensuring the system is always up-to-date and legislatively compliant.

Managing the IT Infrastructure

The shift towards outsourcing of specific IT systems and components to the cloud has increased dramatically in recent years, with companies finding the complexity and rapid movement of the technology market too much for their internal IT teams to undertake and maintain effectively – especially when testing and proving is required.



[1] Assuming no exceptional IT imposed restrictions

The diagram above shows the basic technology stack in use when referring to our SaaS or hosted solution, and demonstrates the various layers that are managed by the outsource supplier, in this case PAS Ltd.

A SaaS (Software as a Service) or hosted offering means that management of the technology platform (operating systems, drivers, patches, communications and security implications) can be handled by experts in those fields. This in turn means that a business can specialise in what they do best, whilst qualified professionals in touch with the software solution maintain the technology.

P11D Organiser

The P11D Organiser software, which is the software that is being delivered, has been developed from the ground up to be deployed via VDI and app servers. It is in use at many large organisations and runs in virtualized environments UK wide. It is this enterprise level development that has been leveraged to create the SaaS solution - where the powerful P11D Organiser application is delivered on top of industry recognised Microsoft Remote Desktop Protocol.

However, to deliver a true 'web based' solution, we have further developed the delivery to ensure that the service can be used without any IT involvement for the end user. They simply log in through and modern browser (Google Chrome, Firefox, Microsoft Edge etc) and we will supply the power or a full Windows application directly into their browser using HTML5 technology.

Managed Hosting Layer

Providing the power and security for the P11D Organiser application is our enterprise grade infrastructure. After accessing our an HTTPS encrypted web site, users are authenticated through Microsoft Active Directory services, before being granted secure access to their own specific data store located on our encrypted storage device.

The customer data store has an NTFS security perimeter ensuring complete separation, and contains not only their data, but a customer specific application, ensuring there can never be 'data leaks' between customers.

Data Centre Services

The platform on which the P11D Organiser SaaS offering runs is not 'piggy backed' on top of third party cloud services such as Microsoft Azure or AWS (Amazon Web Services), all the equipment is use in owned and maintained by PAS Ltd. All firewall rules are created specifically for this application, and the hardware and operating software is maintained and updated by PAS Ltd to documented processes.

Data Centres

We use two independent ISO27001 accredited data centres for the service, each provisioned by a separate supplier. This ensures adequate coverage and backup should there be any issues. The two

installations are replicas of each other with constant replication in play, allowing a 'failover' should the need arise.

Both data centres are supplied by diverse routes from mains electricity board substations and have 2MW back-up generators offering a minimum of 7 days electricity supply should there be any outages at all. Additionally, UPS (uninterruptible power supply) systems ensure that the supply of electricity is completely clean and will manage during a failure to allow the generators start up.

To ensure optimum performance, air conditioning is provided via underfloor systems that control the airflow via grilles to the relevant locations. Even the air conditioning systems are backed up to ensure that should any failure occur, full cooling is maintained.

A full VESDA system that provides early detection of smoke is installed so that any potential fire is detected before it can develop. In the unlikely event that a fire does develop, an FM200 fire suppression system is in place.

External security is strictly controlled, with trained personnel on site 24x7, and these are backed up by off-site staff that can assist in any major events. The whole site is monitored continuously with CCTV cameras, motion detection and a key fob access system ensures multiple layers of security are in place. Any site visits that may be necessary are escorted and pre-arranged.

The data connections into the site are maintained over multiple providers and have multiple entry points to the building, ensuring that even accidental damage to fibre cables (via road work or similar) do not affect the installation.

HTML5 Technology

The communications between the customer and our web site is standard web traffic over HTTPS (port 443). Although technically we are using RDP to access our terminal servers, what is delivered to the user's browser is a plain HTML5 web page. We effectively transfer the 'display' element of the RDP session to an HTML5 canvas for delivery to the end user. This means we do not require Flash, Java, ActiveX, Silverlight or any other setup on the end-user side and can be used from almost any device and any modern browser.

ISO27001

All the data centres that are use by PAS Ltd are fully ISO 27001 assessed. ISO27001 is the formal set of specifications against which organizations seek independent certification of their Information Security Management System (ISMS).

ISO 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system - an overall management and control framework - for managing information security risks.

Penetration Testing

Although the basic level of physical security offered extremely high, much of this can be in vain should the software provision that runs on top of the hardware not be secure. As stated earlier, PAS Ltd deal with personal information that needs the highest level of security, even from the most dedicated 'hacker'.

To ensure our software and systems are secure, we have commissioned 'penetration tests' to be carried out by accredited providers to get documentary proof of the security of customer data for a hosted application. Penetration testing is a widely accepted method of assuring information security

and has become an integral part of many organisations technology risk management programs.

We always use a CREST registered testing company. CREST (Council of Registered Ethical Security Testers) was created in response to the need for regulated and professional security testers to serve the global information security marketplace. CREST's main aim is to represent the information security testing industry and offer a demonstrable level of assurance as to the competency of organisations and individuals within those approved companies.

CREST is a standards-based organisation for penetration test suppliers incorporating a best practice technical certification programme for individual consultants. Additionally CREST provides its members with a framework of guidance including standards, methodologies and recommendations aimed at ensuring the very highest standards of leading-edge security testing.

PAS Ltd encourages our customers to commision their own penetration tests of our service should they need to - a number have taken up this opportunity, and the system has been cleared for use in all cases.

Backup and Redundancy

PAS Ltd run a fully redundant backup system at a separate data centre which is maintained in an identical state to the live system. Our systems are run on top of VMWare, allowing full replication of machines and services, and the HPE Nimble storage devices automatically replicate all data in an encrypted state over a private VPN link.

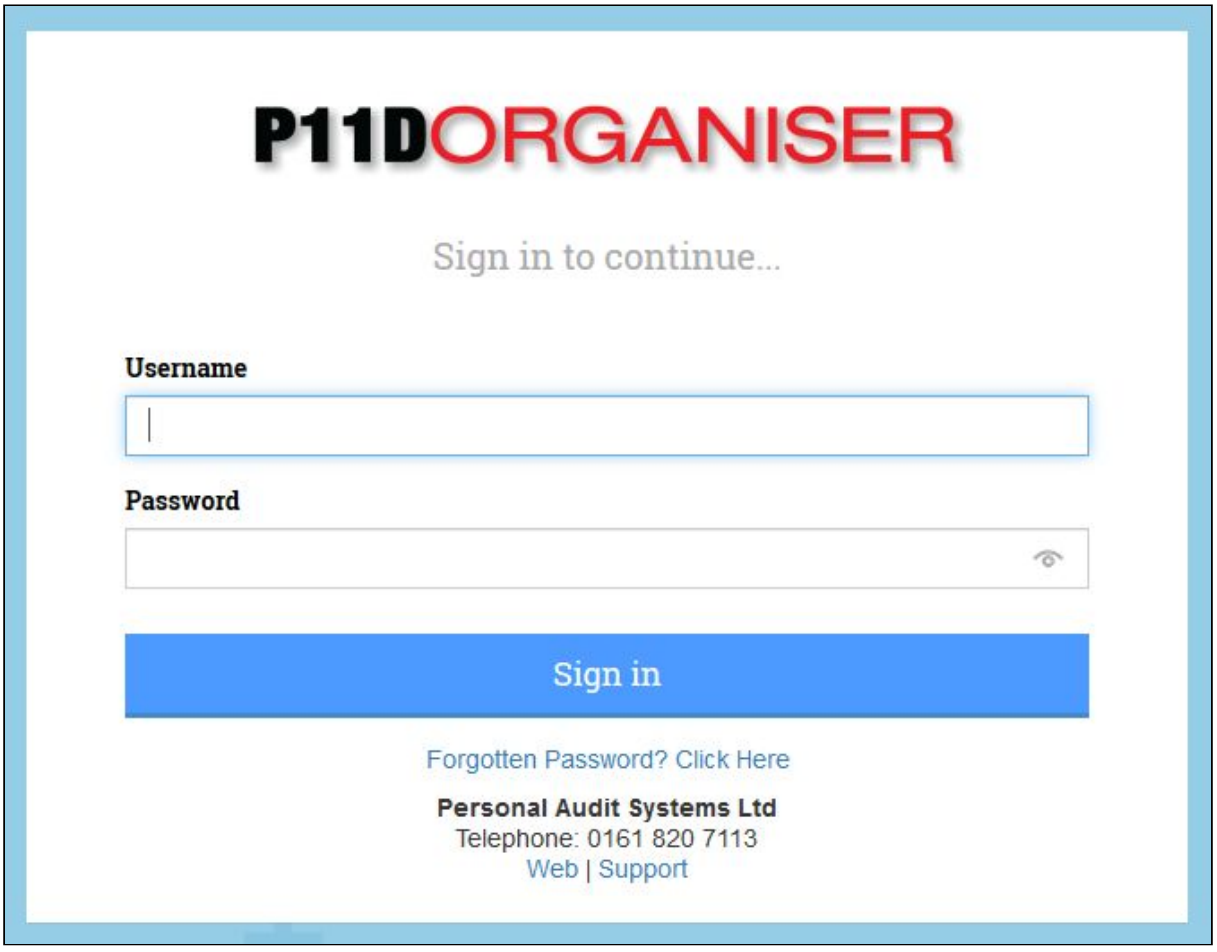
In the event of a catastrophic failure at the main data centre, we are able to fail over to the replicated system and bring it online with a minimum of downtime for the user.

User Journey

The details below take you through the basic user journey when using the SaaS system. This details the technical workflow as well as explaining the infrastructure that is used to deploy the system.

Login

Users of the SaaS P11D Organiser log in by navigating to a secure web site over an HTTPS connection (port 443).



The web server is located in ISO27001 accredited data centres and incoming traffic is routed through a managed Cisco firewall.

Users of the system are generated by the PAS Ltd support team, and are invited to set up their account and generate a conforming password. Password complexity can be configured on a 'per licence' basis, but the defaults are:

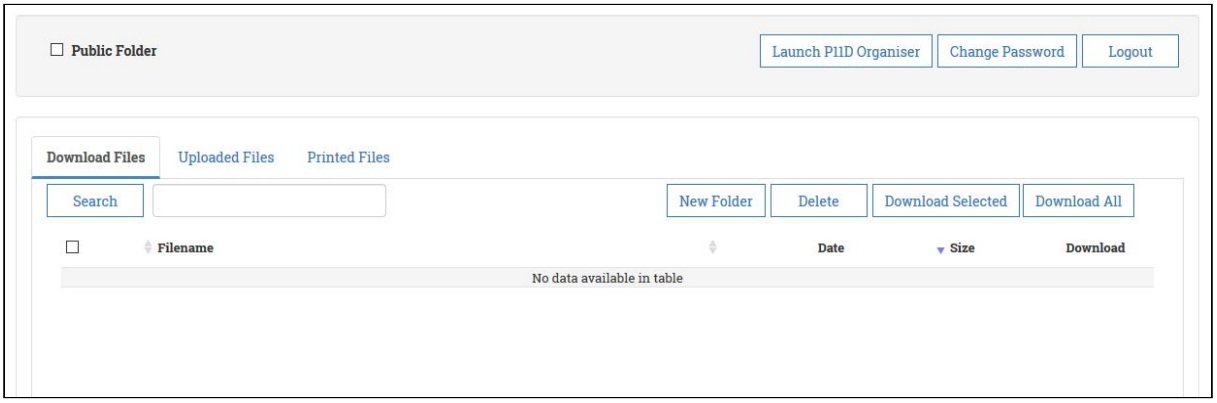
Password Category	Setting
Minimum password length	7 Characters
Maximum password length	32 Characters
Days before expiry	30

Maximum invalid attempts	5
Number of previous passwords	5
Must include special characters	Yes
Must be mixed case	Yes
Must include numeric values	Yes

Users are authenticated against a Microsoft Active Directory server, and based on this are granted access to the main MyP11D.com website. This also grants them access to a NTFS protected file store located on our encrypted HPE Nimble storage device - everything related to the customer is stored within this protected area.

DataExchange

After login users are presented their DataExchange area, this is their 'window' into our secure SaaS platform, and allows data (in the form of spreadsheets, PDFs, images etc) to be uploaded or downloaded. The SaaS P11D Organiser application has no access to any local resources of the users (shared drives, printers etc), and data to be introduced or removed from the system is user controlled.



Users will upload data that they are intending to import into the P11D Organiser (such as .CSV, .XLS and .XLS files), and will also use this facility for downloading data (such as PDFs and Excel files).

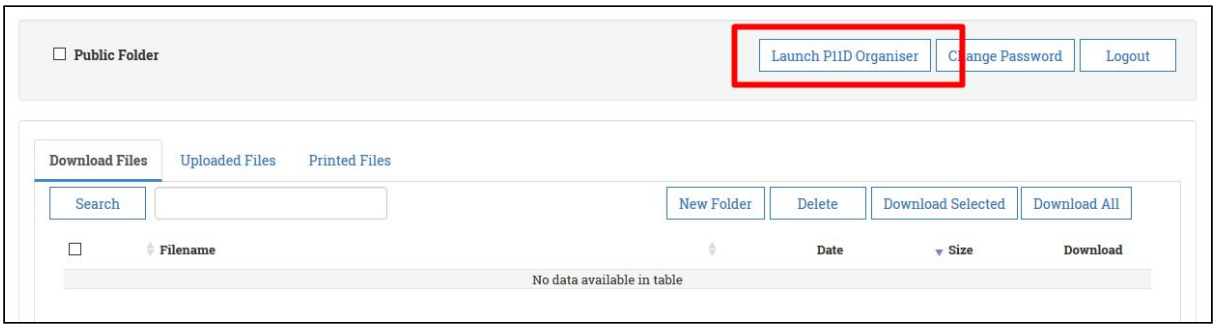
Upload	Download
CSV | XLS | XLSX | TXT | JPG | PNG | BMP	CSV | XLS | XLSX | PDF | ZIP

Permissible file types and sizes are restricted, and all uploaded files are passed through a virus scanner in a temporary location before being introduced into the secure area.

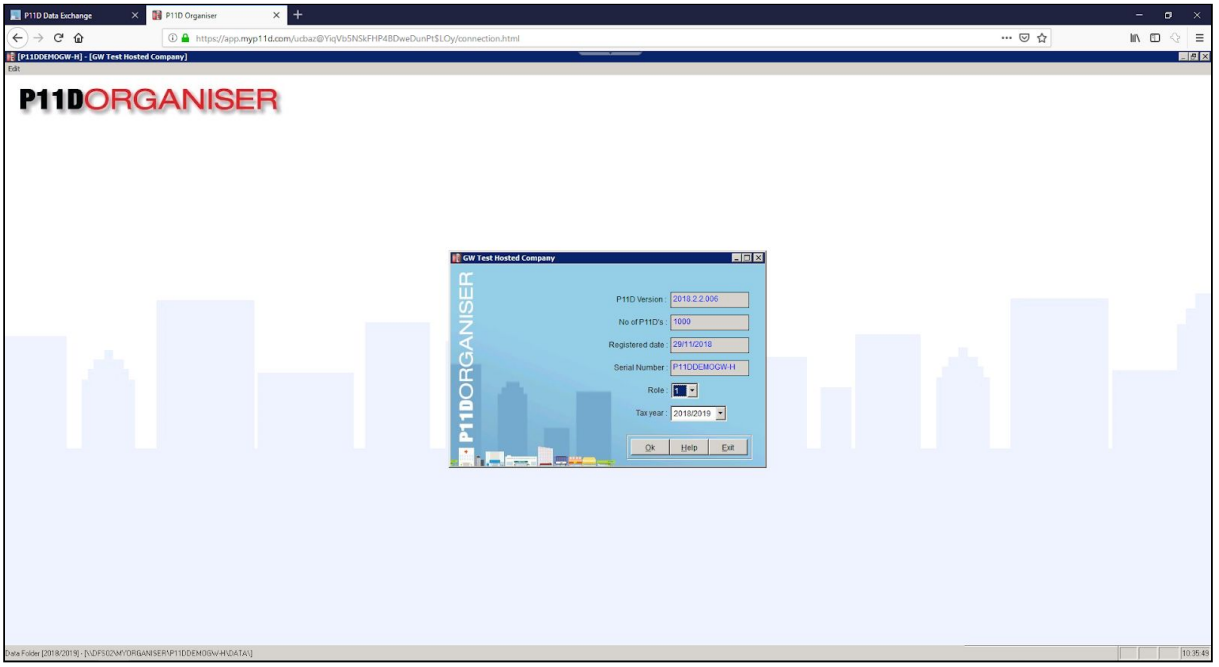
DataExchange is designed as a 'holding area' for data going into and out of the system, and although file storage on DataExchange is fully user controlled (they have control over deletion), we also have a licence specific 'sweep' process that deletes files over 30 days old.

P11D Organiser

The user has the ability to start the SaaS version of the P11D Organiser from this screen. When the user starts a P11D Organiser applications, the session goes through a gateway server which then initiates an RDP (Remote Desktop Protocol) session to a bank of Terminal Servers, these in turn access the users secure storage area to start the P11D Organiser application.



Due to the IT and security implications of using an ActiveX control to deliver an RDP session within a browser, the SaaS solution uses a new facility to deliver the application interface to the user. In the SaaS P11D Organiser solutions we translate the screen display into an HTML5 canvas that is then delivered over the HTTPS connection to the user's browser.



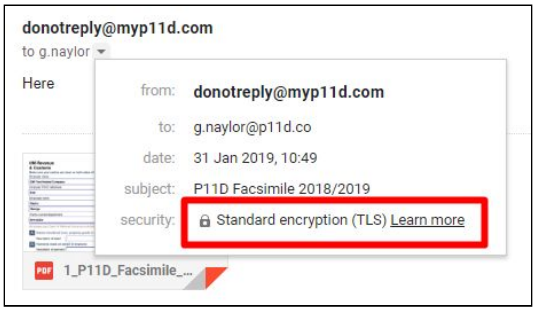
Everything is delivered to the user within the same secure HTTPS controlled web connection (via port 443), and by using HTML5 for the delivery, we can make this system available within any modern browser, including:

- Google Chrome
- Microsoft Edge
- Firefox
- Apple Safari
- Internet Explorer (version 11 only)

When using the software, all data is retained within the data centre environment, with only screen contents being delivered to the end used - no actual personal data is being transferred, it is purely video content.

Email to Employees

A majority of customers choose to email benefits statements and P11Ds to their employees, this is the fastest and convenient way to impart the information. As a SaaS solution, the P11D Organiser has no ability to communicate with your local mail systems, we therefore send all mail from our dedicated SMTP servers, which are located on the same data centre infrastructure as our other servers. All mail from the SaaS P11D Organiser is sent with standard TLS encryption applied



Submission to HMRC

The SaaS P11D Organiser needs to be able to communicate with HMRC via the Government Gateway to report P11D information. Connection to the Government Gateway is achieved over an outbound HTTPS connection - this is the ONLY way data can be exchanged with HMRC.

Data Clarification

All data entered into the P11D Organiser is managed by the client, PAS Ltd have no access to the data (unless specifically granted) and do not have any control over said data - PAS Ltd are providing a platform for data to be processed by the user, and the breadth and content of the information is solely at the discretion of the user.

Data Sharing

The following as the data sharing section of the terms and conditions for the SaaS version of the P11D Organiser.

Personal Data sharing purpose	The Software/Services allow(s) the Licensee/Customer to report information to HMRC on expenses and benefits received by employees.
Objectives and benefits of Personal Data sharing	To ensure legislative compliance with Income Tax (Earnings and Pensions) Act 2003.
Personal Data being shared	National Insurance Number, Date of Birth, Gender, Name, Address, email address.
The Licensee's justification for Processing Personal Data, in accordance with Article 6 GDPR	To ensure legislative compliance with Income Tax (Earnings and Pensions) Act 2003.
Sensitive Personal Data being shared	Not Applicable.
Media for sharing Personal Data	Internet/web via an HTTPS connection.
Persons between whom Personal Data will be transferred	Licensee, their employees and HMRC. PAS Ltd based on authorisation of a support request.
Frequency of Personal Data transfer	When Licensee chooses to send data to HMRC or when they request and authorise support from PAS Ltd.
How Personal Data is stored by the Supplier	The data is stored in a database hosted at an ISO27001 data centre and protected by NTFS and Windows Group Policy.
How long Personal Data is stored by the Supplier	At the discretion of the licensee (in line with HMRC recommendations).
How the Supplier will destroy Personal Data	Data is destroyed in line with the published Procedure for the Disposal and Destruction of Sensitive Data on Termination or request.