CLOUD GATEWAY

CONNECT

PSN CONNECT: REMOTE ACCESS TO PSN

SERVICE DEFINITION

V2.0
Issue Date: 14/10/2025
Commercial in Confidence

About this document

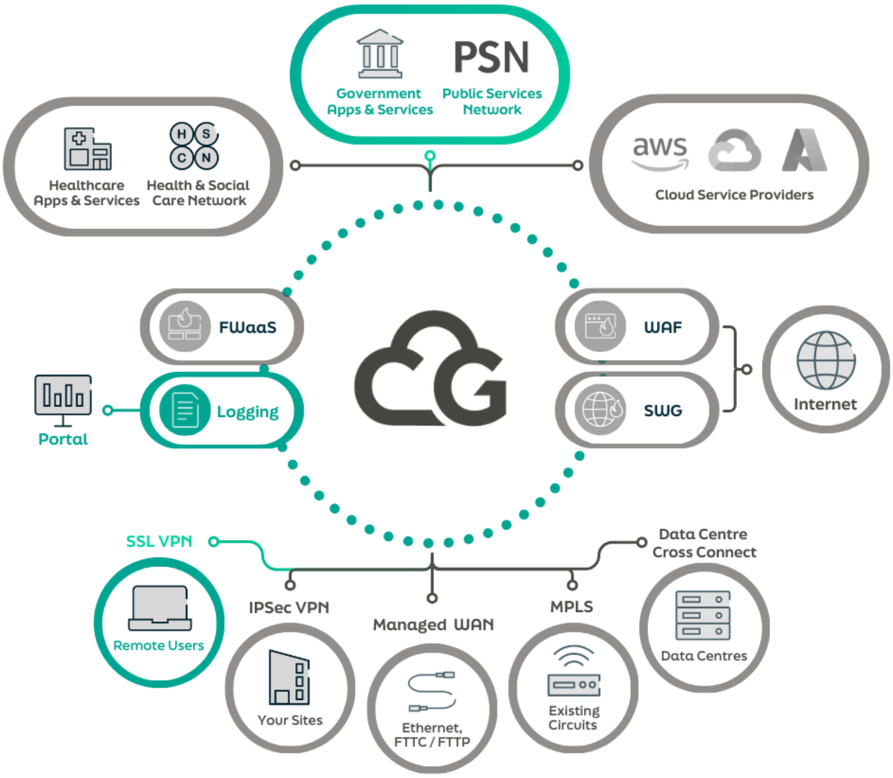
This document provides a straightforward, clear description of our **Remote Access to PSN** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is Remote Access to PSN?

Remote Access to PSN enables access to applications and resources on the Public Services Network (PSN) from remote personal devices.

An encrypted link connects the user over the internet to our shared tenancy. We then provide onward connectivity to the PSN via a resilient private connection.

Traffic is secured via our Foundation Security component, which is included in this service. This set of configurable firewall capabilities manages and controls the traffic passing through the platform from the user to PSN.



Ecosystem View

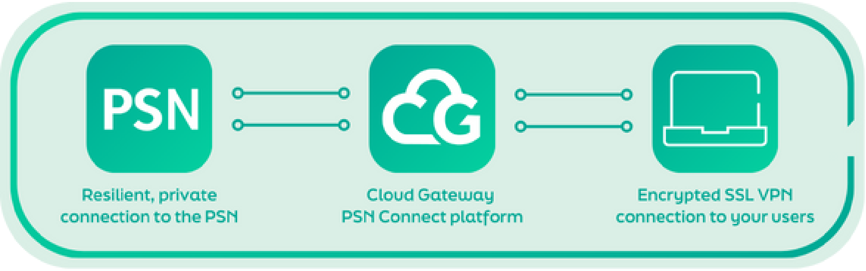

PSN
Resilient, private connection to the PSN
Cloud Gateway PSN Connect platform
Encrypted SSL VPN connection to your users

Diagram View

Basic operation

Remote Access to PSN is achieved through SSL-VPN technology, which requires you to install a piece of software on the end user's laptop, tablet or other device.

When prompted for authentication, the user inputs a username and password provided by us. The software then builds a secure encrypted tunnel over the internet, connecting the user to our platform and on to the PSN.

For extra security, MFA (Multi Factor Authentication) using an authenticator app can be enabled and is included as standard, or SMS with a UK mobile number.

This service can only be used by remote users who require access to consume PSN services; it is not to be used to publish services to the PSN. The access policy is applied across all users for you as a customer; access policies to PSN are not applied per individual user.

PSN Code of Connection (CoCo)

All organisations that require access to the PSN network are required to complete a set of policy documents making up the PSN Code of Connection. This must be completed before PSN Connectivity can be provisioned.

Information should be provided to Cloud Gateway in order for us to establish the connection.

Guidance on obtaining this can be found on our website https://www.cloudgateway.co.uk/knowledge-centre/customer-guides/psn-compliance-process/

SSL VPN software

We will provide you with SSL-VPN software that can be used on Windows 11 and the latest Mac OS. You will be responsible for installing this on your end user's devices.

It's important that you keep the software up to date, to maintain security and integrity of your data. We need you to deploy updates within 24 business hours of our request

Authentication

Authentication is done via username/password provided by Cloud Gateway. You may select your own username, this is generally an email address.

If MFA is enabled, this is delivered through one-time codes on an authenticator app or via SMS text message. We don't issue physical MFA tokens.

After 5 failed login attempts, the VPN software will block the user for 15 minutes, before allowing them to reattempt. If a password is forgotten and needs resetting, this can be requested via the Cloud Gateway Portal.

Simultaneous use

Simultaneous sessions of a single user's account is not permitted; a single user can only connect one device at any point in time.

Connecting to the PSN

PSN Connectivity connects our platform tenancy to the PSN networks. We can connect you to both PSN Assured (PSN-A) and PSN Protect (PSN-P).

Our PSN Connectivity Service has been through the PSN Assurance process, specifically Cabinet Office PSN-Compliance offering SRV_0454.

Cloud Gateway supports the connection of a customer via our remote access service (SSL VPN), Internet IPSec VPN or NNI to their own virtualized instance of the Security Enforcement Core (SEC), with onward connection to AWS, Internet, other cloud providers and the proposed PSN connection. All connectivity goes through the SEC and must be configured to allow onward connections.

IP Addressing

Details of IP connectivity and addressing schemes for Remote Access to PSN are defined below:

- RAS VPN users PSN traffic will be NAT translated to an allocated Cloud Gateway PSN IP (for PSN outbound access).

This service can support connectivity from your remote users to the PSN (outbound, for consuming services). For inbound connectivity, a different service will be required that allows the hosting of PSN facing services. Please ask us for details.

Security arrangements

A Security Incident is an event that compromises the confidentiality, integrity, or availability of information or information systems. It typically involves unauthorised access, use, disclosure, modification, or destruction of data, or interference with system operations.

Where network vulnerabilities are identified, Cloud Gateway will utilise its vulnerability management process and aim to address the vulnerability within the following timescales:

Severity	Base Score (CVE)	Remediation Target
None	0	N/A
Low	0.1 - 3.9	60 days
Medium	4.0 - 6.9	60 days
High	7.0 - 8.9	30 days
Critical	9.0 - 10	14 days

Foundation Security

Layer 3 / Layer 4 firewall monitors and controls incoming and outgoing network traffic, based on predetermined security rules. It is designed to establish a barrier between your users and the PSN.

The below information is required in order to configure firewall policies to allow specific traffic through the platform:

- **Rule Name** - *for example 'ACME RULE'*

- **Source (IP address)** - *for example '1.2.3.4/32'*
- **Destination (IP address)** - *for example '1.1.1.1/32'*
- **Service (Protocol/Port)** - *for example 'TCP/443'*

Acceptance testing

Acceptance criteria

The acceptance criteria for Remote Access to PSN, as part of the platform onboarding are:

- Successful installation of the Remote Access software on a single end user device
- The test user is able to authenticate themselves on the Remote Access software
- The software establishes a successful VPN connection
- The test user is able to access predetermined resources on the PSN

Exclusions

The service does not include:

- Code of Connection. Cloud Gateway have a PSN certificate themselves as a PSN connectivity provider, you will require your own PSN certificate to access the PSN too.
- Hardware
- The licensing or right-to-use PSN applications
- Internet or MPLS connectivity
- When purchasing a Remote Access to PSN you will receive a lighter version of the Cloud Gateway portal, with some capability restrictions. Therefore some portal features are excluded from this service.

Customer responsibilities

You are responsible for:

- Providing details of services that are required for traffic to PSN. We'll capture this during our engagement with you
- Providing a PSN connection compliance certificate to Cloud Gateway. This document proves you have completed the PSN CoCo
- Providing us with the individual user details to add to the platform. You should give us as many of the user details as possible before going live, as any subsequent requests to add further users may be subject to a charge
- Providing suitable internet connectivity for the end users
- Managing your own end user devices
- Distributing, setting-up and supporting the SSL-VPN software
- Supporting your End Users. Cloud Gateway provides support to you directly and it is your responsibility to support your End Users
- User base management via The Cloud Gateway Portal, i.e. requesting additions, deletions, changes
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- Deploying updates to the SSL-VPN software. It's important that you keep the software up to date, to maintain security and integrity of your data. We need you to deploy updates within 24 business hours of our request
- Providing Rule Name, Source (IP), Destination (IP) and Service (Protocol/Port) for each firewall rule that is to be applied
- Ongoing maintenance, management and/or decommissioning of your other security capabilities
- Backups. You are responsible for backing up your own systems. We don't hold customer data. We will back up our own platform, and will store logs as detailed in the Log Storage section below

Cloud Gateway responsibilities

We are responsible for:

- Encrypted IP connectivity to the PSN-A or PSN-P over the internet
- Ensuring you've completed the PSN CoCo prior to live service commencing
- 24/7 proactive monitoring of the service
- Where network vulnerabilities are identified, Cloud Gateway will utilise its vulnerability management process and aim to address the vulnerability in accordance with the Security arrangements section
- Application and management of firewall rules gathered during onboarding process
- Configuring your environment on the Remote Access component of our platform
- Maintaining resilient centralised authentication

- Adding and maintaining end user accounts
- Providing you with the SSL-VPN software via a self-service portal or hyperlink
- Providing a user guide to help end-users install and use the SSL-VPN software
- Providing access to the Cloud Gateway Portal (subject to the Terms of Use)

Ordering and lead time

Ordering and volume

We calculate your cost on a per user basis. The user volumes available to purchase are:

- 5 users
- 10 users
- 25 users
- 35 users
- 50 users
- 100 users
- 500 users

You can request an increase in user volume from our Sales Team, or via the Cloud Gateway Portal. During the service contract term, you will not be able to reduce the user volume.

You will be billed for the user license tier that has been contracted for, not the actual number of users set up on the authentication platform. The service is based upon named user accounts rather than concurrent users.

A standard service request charge applies to PSN services requiring a firewall change. A standard Service Request charge will also apply if you wish to remove access to any PSN services.

Lead time

Our Service Level Agreement (SLA) to deliver the service is 5 working days. The lead time is measured from receipt of a valid Purchase Order (PO) and contract acceptance, to live service ready for any acceptance testing. Please be aware that third parties are involved in the process of you obtaining a PSN compliance certificate, therefore we recommend starting this process as early as possible to mitigate any risk of delay to your service provision. The SLA timer will be paused when there is a dependency on you or external parties to provide information or input.

Service management

Secure service administration

Secure service administration is carried out by appropriately cleared Service and Technical professionals, with clearance levels such as BPSS, SC or NPPV3 depending on client requirements.

Role separation is maintained to ensure individuals access only the information necessary for their duties.

Changes are managed using systems including the Service Management Platform and specialised platforms for technical components. A dedicated Service Desk team engages with both the system and end users, working alongside the engineering team to investigate issues and implement solutions.

Service support

We have an experienced Service Desk team who are responsible for the day-to-day operational service between you and us.

The Service Desk team's primary responsibility is to provide a single point of contact within Cloud Gateway – to which issues surrounding satisfaction of service may be escalated and resolved.

Support escalations

We strive to ensure that all incidents, service requests, or simple advice and guidance requests from our customers are fulfilled efficiently and effectively within our published timescales.

If you feel that a request is not being managed effectively or would like to escalate a particular issue, this can be raised with our Service Management team.

Complaints

We take complaints seriously and ask that any customer wishing to raise a formal complaint does so in writing to service@cloudgateway.co.uk.

Full details of our complaints procedure can be found within the Cloud Gateway Customer Service Pack, which you will receive during the onboarding process.

Reporting

Various types of reports can be provided. You can request these by contacting service@cloudgateway.co.uk, or raising a ticket via the Cloud Gateway Portal. Charges may apply.

Service levels

The service levels that apply to this service are available in our Service level Agreement (SLA).

Data processing

The data processing terms that apply to this service are available in the Cloud Gateway MSA, found here: https://www.cloudgateway.co.uk/compliance/msa/.

Security arrangements

- The core platform infrastructure that supports this component service is hosted in geographically diverse UK data centres. All data remains within UK sovereignty (with exception if endpoints connect to our platform via the internet)

- We are ISO 27001 and ISO 9001 accredited. We are also compliant with CyberEssentials Plus

Log storage

- All traffic logs and policy controlled events are stored in our Log Aggregation Platform (LAP)
- Logs are retained for 62 days as standard, and are used to populate graphs and visualisations in the Cloud Gateway Portal

Business continuity and disaster recovery

Cloud Gateway maintains a comprehensive approach to operational resilience, ensuring continuity of service through robust business continuity and disaster recovery planning. Our internal continuity and disaster recovery plans are reviewed and tested regularly, and staff receive training to ensure they can respond effectively to a disruption.

Our infrastructure is designed for high availability across data centres. Network component configurations are backed up regularly and can be used to recover from disruptive scenarios. Supplier relationships are governed by rigorous due diligence, including reviews of the supplier’s own continuity and recovery practices. Data centres and hosting providers, where under our selection, are selected based on secure practices and continuity capabilities. Certifications held by the supplier are reviewed, such as ISO 22301, ISO 27001, ISO 9001 and ISO 14001.

Our operational model supports full remote working, whereby all staff are equipped to operate securely from the office, home or other locations.

CLOUD GATEWAY

cloudgateway.co.uk

+44 (0)20 3870 2444

sales@cloudgateway.co.uk

Cloud Gateway
The Ministry, Borough
79 Borough Rd, London SE1 1DN