CLOUD GATEWAY

CONNECT

PSN CONNECTIVITY
SERVICE DEFINITION

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

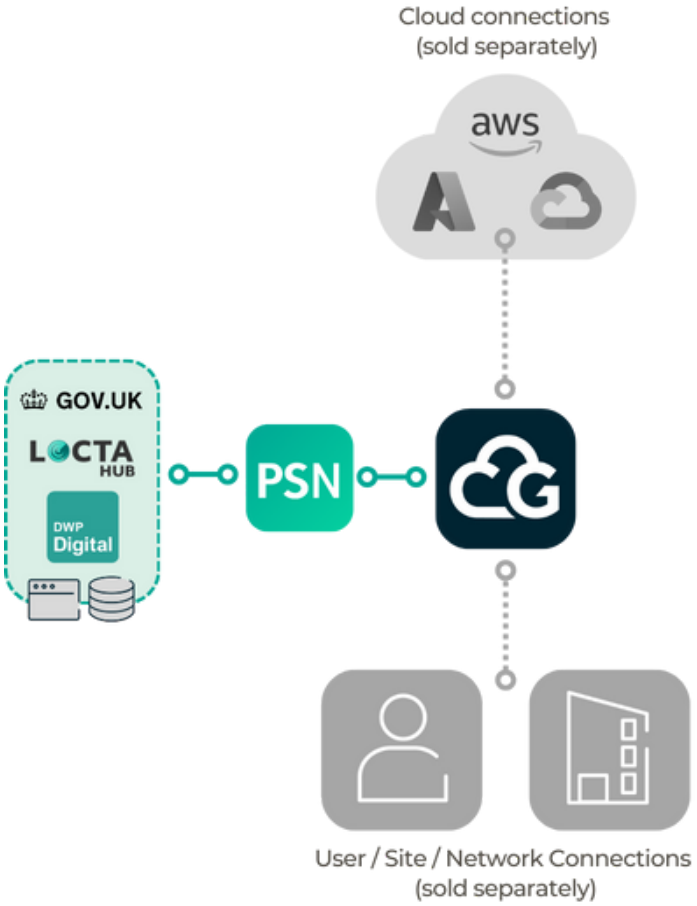
About this document

This document provides a straightforward, clear description of our **PSN Connectivity** 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 PSN Connectivity?

PSN Connectivity is a component service available as part of the Cloud Gateway platform. PSN Connectivity enables you to connect our platform quickly and securely to the Public Services Network.

The service provides a resilient IP connection to the PSN network in line with PSN compliance. By using PSN Connectivity, you can link your cloud environments to other network endpoints. You can also implement security components that protect the traffic to and from the PSN. Additional connectivity and security services are subject to commercial agreement and not included with PSN Connectivity as standard.



Basic operation

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/

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.

Connectivity is provided in a resilient manner by connecting to two geographically diverse data centre locations. All routing and failover is managed by Cloud Gateway.

This service may be used both to consume services on the PSN, or publish hosted services to the PSN (or both).

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

IP connectivity and addressing schemes for Cloud to PSN Connectivity are defined below:

- Network Address Translation (NAT) to a single Cloud Gateway PSN IP (for customers requiring outbound PSN connectivity only).
- IP ranges allocated by the PSN Network's IPAM team (for customers requiring inbound/outbound PSN connectivity).

PSN IP migration

For PSN customers, Cloud Gateway offers the option to use or migrate existing PSN IP ranges. This requires proof of PSN IP subnet ownership and also incurs additional costs associated with the PSN IP migration.

Inbound/Outbound

This service facilitates both outbound traffic for consuming services on the PSN and inbound traffic for accessing your connected and hosted Cloud and Data Centre services from the PSN.

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

Acceptance testing

Acceptance criteria

The acceptance criteria for PSN Connectivity, as part of the platform onboarding are:

- Basic connectivity testing to/from your network endpoint(s) and PSN services
- Failover test between primary and secondary connection

Exclusions

The service does not include:

- Code of Connection. You won't be permitted to utilise Cloud Gateway's Code Of Connection (CoCo) to access the PSN
- Migration of existing PSN IP addresses to our service
- Custom security policy. Custom security policies may be implemented via Foundation Security, Firewall-as-a-Service (FWaaS), Web Application Firewall (WAF) and SWG (Secure Web Gateway). These services are available as separate components of the platform

Customer responsibilities

You are responsible for:

- Providing details of services that are required for incoming and outgoing 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, submitted relevant diagrams and IT Health Check (ITHC) reports
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- 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:

- Resilient IP connectivity to the PSN (PSN-A and/or PSN-P)
- All IP routing including failover and dynamic routing
- 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
- 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 bandwidth basis. PSN Connectivity is sold as a component of our platform, the cost will usually be combined with other components and quoted as a total service cost in the proposal. The bandwidth of the PSN connection will mirror the overall bandwidth capacity of the platform being purchased.

Lead time

Our Service Level Agreement (SLA) to deliver PSN Connectivity 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