CLOUD GATEWAY

CONNECT

HSCN CONNECTIVITY

SERVICE DEFINITION

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

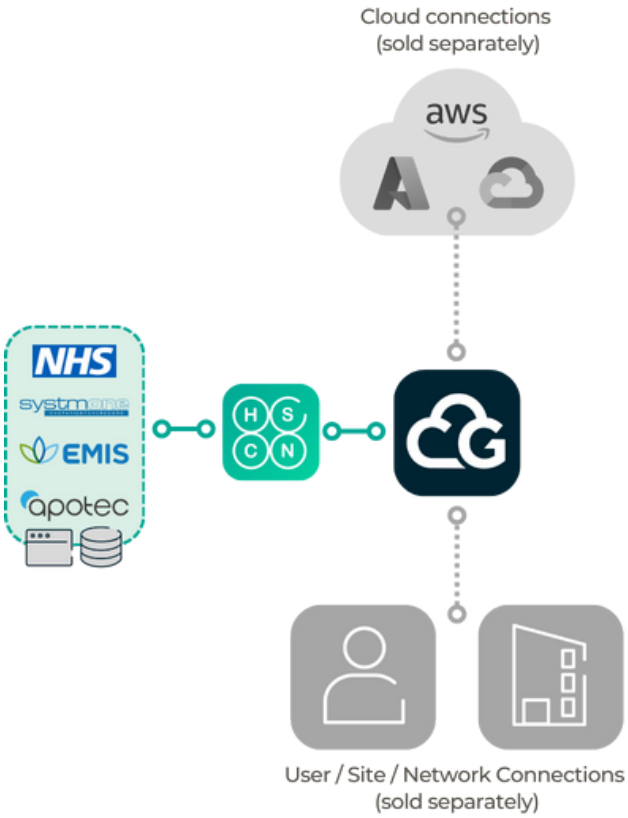
About this document

This document is designed to provide a straightforward, clear description of our **HSCN 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 HSCN Connectivity?

HSCN Connectivity is a component service available as part of the Cloud Gateway platform. HSCN Connectivity enables you to connect quickly and securely to The Health and Social Care Network (HSCN).

The HSCN Connectivity Service provides an IP connection to the HSCN network in line with the HSCN Compliance Framework. By using HSCN Connectivity, you can link your HSCN environment(s) to other network endpoints. You can also implement security components that protect the traffic to and from the HSCN. Additional connectivity and security services are subject to commercial agreement and not included with Cloud Connectivity as standard.Connectivity as standard.



Basic operation

Our HSCN Connectivity service is deployed over our core network, which provides private IP connectivity to the HSCN and optionally to the internet.

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.

ODS Code and Connection Agreement

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

Further information can be found here.

Optional Internet Connectivity

Outbound monitored and filtered Internet connectivity may be purchased as part of HSCN Connectivity, if you require outbound internet via the same physical or logical connection as the HSCN service.

Note that this service is centralised, offered by NHS Digital in conjunction with NHS Digital's appointed Advanced Network Monitoring (ANM) supplier.

We will route internet bound traffic via the ANM supplier over our HSCN Connectivity service, if purchased. Note that inbound internet is not available. The ANM service includes a standard deny list, IP reputation filter list and inline malware scanning and sandboxing for non-encrypted internet traffic.

Inbound and non-ANM filtered / monitored outbound Internet may be purchased as a separate 'overlay' service. For inbound internet, see our Secure Web Gateway (SWG) Service Definition.

IP Addressing

Details of IP addressing schemes for HSCN Connectivity are defined below:

You request an IP range (RFC1918) from NHS Digital or you may already have RFC1918 allocated by NHS Digital

We can use your RIPE range to advertise into HSCN (publically unique address from RIPE)

We can provide IP maximum of 1 (used for NAT into HSCN)

Note: where public RIPE addressing is allocated for use on HSCN, that address range must not be reachable via the public internet. The address block must not be dual allocated for use on both the public internet and the HSCN network.

Inbound / Outbound

This service can support traffic from your network to the HSCN (outbound, for consuming services), and/or traffic from the HSCN to your estate (inbound, for publishing services). The permitted direction(s) will be defined during onboarding and governed by your use case and firewall policy. If in doubt, please speak to your Cloud Gateway representative to ensure alignment with HSCN policy requirements.

Acceptance testing

Acceptance criteria

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

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

Exclusions

The service does not include:

- 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:

- Completing and evidencing the HSCN Connection Agreement and ODS Code
- Provision of IP addresses and/or FQDN (Fully Qualified Domain Name) of HSCN services that you require access to
- Requesting an IP address from NHS Digital if using more than one IP
- Defining and managing changes to internet policy with the ANM supplier (if purchased)
- 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:

- Ensuring our HSCN IP Connectivity is Resilient and ready for you to connect to
- Ensuring you've completed the HSCN Connection agreement prior to live service commencing
- All IP routing including failover and dynamic routing
- 24/7 proactive monitoring of the service
- 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. HSCN 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 HSCN connection will mirror the overall bandwidth capacity of the platform being purchased.

Lead time

Our Service Level Agreement (SLA) to deliver HSCN 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. The SLA timer will be paused when there is a dependency on you to provide information or input.

Service management

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 such as utilisation and traffic log reports are provided by the portal. You can request other reports 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