CLOUD GATEWAY

CONNECT

HEALTH CONNECT: REMOTE ACCESS TO HSCN

SERVICE DEFINITION

V2.0
Issue Date: 10/07/2025
Commercial in Confidence

About this document

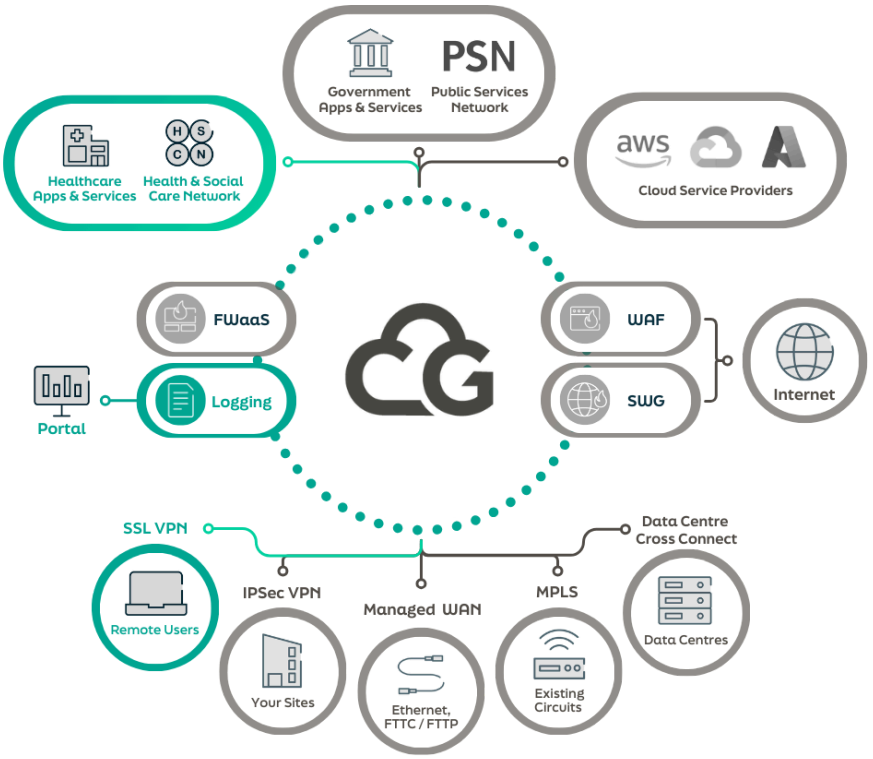
This document provides a straightforward, clear description of our **Remote Access to HSCN** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is Remote Access to HSCN?

Remote Access to HSCN enables access to applications and resources on the Health and Social Care Network (HSCN) from remote personal devices.

An encrypted link connects the user over the internet to our shared Health Connect tenancy. We then provide onward connectivity to the HSCN 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 HSCN to the user.



Ecosystem View

Diagram View

Basic operation

Remote Access to HSCN 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 HSCN.

For extra security, MFA (Multi Factor Authentication) using an authenticator app can be enabled too.

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

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.

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.

If MFA is enabled, this is delivered through one-time codes on an authenticator app. 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.

Email Address Policy

Users accessing HSCN via Remote Access Service (RAS) must authenticate using a corporate or business email address. Use of personal email addresses (e.g., Gmail, Hotmail, Yahoo) is prohibited.

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 HSCN

We provide an IP connection to the HSCN network in line with the HSCN Compliance Framework.

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.

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

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 HSCN.

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 HSCN, as part of the platform onboarding are:

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

Exclusions

The service does not include:

- Internet or MPLS connectivity
- Hardware
- When purchasing a Remote Access to HSCN, 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:

- 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
- Providing us with the individual user details to add to the platform. You should give us with 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, 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 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:

- 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
- 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 details
- 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 HSCN services requiring a firewall change. A standard Service Request charge will also apply if you wish to remove access to any HSCN 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. 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 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