CLOUD GATEWAY

CONNECT

CLOUD 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 **Cloud 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 Cloud Connectivity?

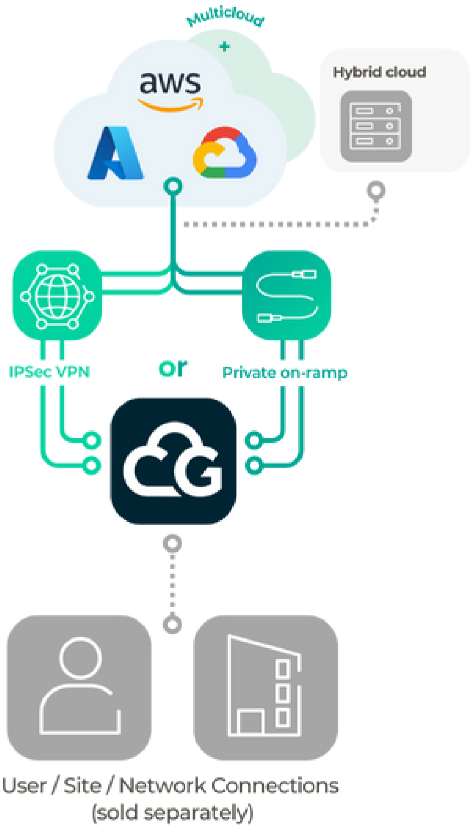
Cloud Connectivity is a component service available as part of the Cloud Gateway platform. Cloud Connectivity enables you to connect quickly and securely to a wide range of Cloud Service Providers (CSPs).

Cloud Connectivity can be deployed in three ways:

- A private connection via a dedicated on-ramp through our UK data centre presence
- Via IPSec VPN deployed over the internet
- Via IPsec VPN deployed over the public cloud providers private connectivity method. E.g. Azure, over Express Route

By using Cloud 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 cloud. Additional connectivity and security services are subject to commercial agreement and not included with Cloud Connectivity as standard.

This is a network connectivity service. You are responsible for contracting with the CSP(s) directly to obtain their cloud services. This includes any charges that might be incurred.



Basic operation

We will provide connectivity to your chosen CSP(s). Each individual connection is defined as a **connected cloud instance**, irrespective of specific cloud vendor. For example, if you are running two separate environments in AWS, they will be classed as two separate connections, not one.

Establishing connectivity from cloud environments is usually a straightforward process, although this may vary depending on the CSP we are connecting to.

Private connectivity to cloud (on-ramp)

To connect to your cloud environment privately, we use a dedicated on-ramp within our data centre presence. This on-ramp gives us access to an aggregated fabric of CSPs.

Each cloud provider has a different method to establish network connectivity. As part of the service, we will engage with you to provide technical guidance during the setup process.

In most cases, while you are required to initiate certain elements within their cloud environment (such as generating pairing keys or providing service identifiers), the underlying network connections, such as AWS Direct Connect, Azure ExpressRoute, or Google Cloud Interconnect - are provisioned as part of our service and do not require separate procurement. Below are some examples of Cloud Connect (the list is not exhaustive):

Amazon Web Services (Direct Connect)

- You provide the AWS account number that needs to be connected
- **We deploy a Direct Connect (DX) network connection** and trigger an invitation to your AWS console using the account number provided
- You provide the AWS Environment BGP ASN (Autonomous System Number) and password
- You also provide two /30 IP prefixes, which are used to connect each side of the cloud connection
- Upon acceptance of the connection invitation, connectivity will be established between the cloud and the platform

Microsoft Azure (Express Route)

- You are responsible for provisioning an Express Route and providing the Azure service keys
- Once granted access, **we connect the Express Route connection to the platform**
- When the connection is ready, we will provide a VLAN ID for use when completing the virtual connection setup in Azure
- You provide the Azure Environment BGP ASN (Autonomous System Number) and password
- You also provide two /30 IP prefixes, which are used to connect each side of the cloud connection

Google Cloud Platform (Cloud Interconnect)

- You provision a Partner Interconnect link in Zone 1 and Zone 2 within your GCP environment.
- You then provide us with the pairing key for the connection

- Once provisioned, Google allocates two IP address ranges (one per zone) in the your GCP console. You needs to pass this information back to us, including any BGP information
- Once this information is received, **we can provision the connection to the platform**

Public connectivity to cloud (IPSec VPN)

IPSec VPN and routing configuration

The IPSec VPN configuration will meet or exceed NCSC Foundation Grade design guidance.

We will configure BGP (Border Gateway Protocol) or VTI (Virtual Tunnel Interface) type tunnels rather than static crypto-maps - also known as policy-based VPN.

BGP / VTI routing

In order to control traffic paths and allow for dynamic failover should there be any Priority 1 service affecting issues at any point during live service, BGP will be configured across the VPN tunnels. BGP configuration parameters dictate that our London data centre is the primary path for all traffic, with our Manchester data centre as a backup for failover.

BGP AS-PATH prepend will be the main traffic path manipulation technique.

Acceptance testing

Acceptance criteria

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

- Basic connectivity testing to/from cloud services and other network endpoints
- Failover test between primary and secondary cloud 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
- Cloud services, virtual machines or cloud storage. This service provides network connectivity only. It does not include cloud-based services including but not limited to cloud data storage, virtual machines or applications

Customer responsibilities

You are responsible for:

- Setting up and preparing the cloud environment(s) to which the service is connecting

- Providing us with the name of the CSP(s) with which you wish to connect
- Following any instructions provided by us, or the CSP to establish network connectivity. Some steps in the setup process will rely on you, including (but not limited to) acceptance of invitations, and supplying service keys
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- All negotiation, contracts and costs relating to your CSP, including (but not limited to) ingress and egress charges, application running costs and data storage costs
- Ensuring there is no overlapping IP addressing between any networks connecting to the service
- Backups. You are responsible for backing up your own systems. We do not provide data backup services. 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:

- Design, installation and configuration of Cloud Connectivity to your chosen cloud environment(s)
- 24/7 proactive monitoring of the service
- Failover. In the event of the primary Cloud Connection path failing, the secondary path will be used for forward traffic
- 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-connection basis. Cloud 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 each cloud connection will mirror the overall bandwidth capacity of the platform being purchased.

Lead time

Our Service Level Agreement (SLA) to deliver Cloud 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