CLOUD GATEWAY

CONNECT

DATA CENTRE CONNECTIVITY

SERVICE DEFINITION

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

About this document

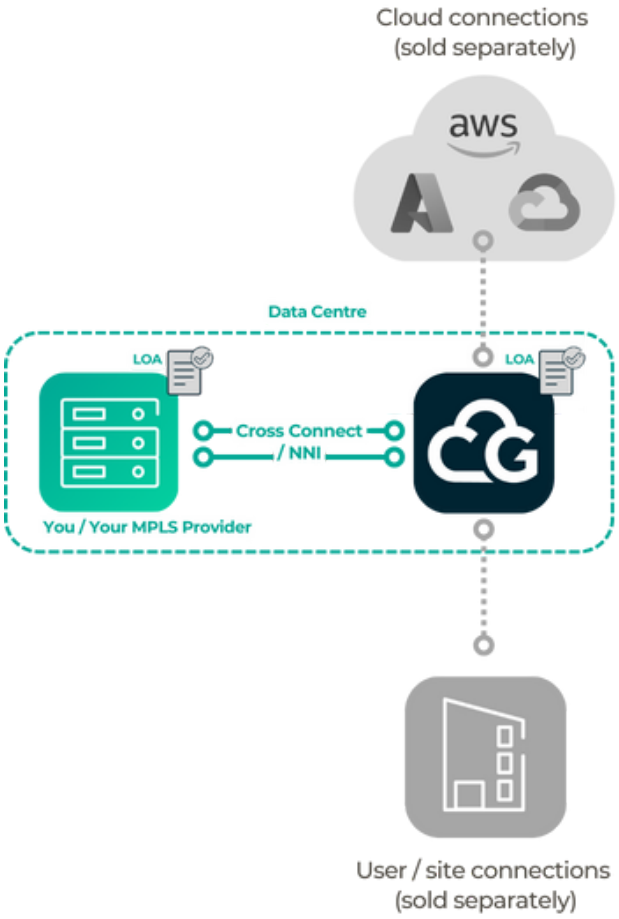
This document is designed to provide a straightforward, clear description of our **Data Centre Connectivity** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is Data Centre Connectivity?

Data Centre Connectivity is a component service available as part of the Cloud Gateway platform. Data Centre Connectivity enables you to connect our platform to your own data centre presence, or that of an existing MPLS network provider.

If you, (or your MPLS provider) is present in the same carrier-neutral data centres as Cloud Gateway, we can establish connectivity and extend it to your other network endpoints as required.

You can also implement security components that protect the traffic to and from the data centre. Additional connectivity and security services are subject to commercial agreement and not included with Data Centre Connectivity as standard.



Basic operation

Our data centre presence

Cloud Gateway currently has a carrier-neutral presence in these UK data centres:

- Equinix LD8 (London)
- Equinix MA3 (Manchester)
- Ark Cody Park (Farnborough)
- Ark Spring Park (Corsham)
- Telehouse North (London)

Assuming you or your MPLS provider has a presence in the same facility - a connection can easily be established to the Cloud Gateway platform.

Connecting to you (Data Centre Cross Connect)

All cross connects are provisioned by a member of data centre provider staff.

If you connect to Cloud Gateway

We will produce a Letter of Authority (LOA) which grants you the capability to terminate a fibre cable in our rack. It's then up to you to make arrangements with the data centre provider to run the cable from one rack to another.

If Cloud Gateway connects to you

You will need to produce a Letter of Authority (LOA) which grants us the capability to terminate a fibre cable in your rack. We may pass on a charge for the cross connect, subject to the terms of the contract. We will then make arrangements with the data centre provider to run the cable from one rack to another.

Connecting to a third party provider (Network-Network Interface - NNI)

The Letter of Authority (LOA) process is the same for a connection to a third party MPLS provider. The LOA will give permission for us to connect to their rack, or vice versa.

We will work with the MPLS provider to create the connection and associated design. You will also need to be involved in this process, and you will be expected to manage the communication and relationship between us and your provider.

Acceptance testing

Acceptance criteria

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

- Basic connectivity testing to/from your network and our platform (if applicable)
- Basic connectivity testing to/from a Third Party network and our platform (if applicable)

- Failover testing between primary and secondary connections

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
- Patching. The cross connect is provided rack-to-rack. You (or your MPLS provider) will need to patch the cross connect into equipment within the rack itself.

Customer responsibilities

You are responsible for:

- All applicable charges relevant to your own MPLS provider
- Managing the relationship between Cloud Gateway and any third party MPLS provider(s)
- Any cross connect fibre you may order and provision (i.e. if you connect to us)
- Production of Letter of Authority (LOA) to grant us the capability to terminate a fibre cable in your rack (if we connect to you)
- All IT equipment beyond the connection within your own rack / data centre location
- Any User Acceptance Testing (UAT) before, during or after the service goes live
- Provision of site / rack access when required
- 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:

- Design, installation and configuration of Data Centre Connectivity
- Any cross connect fibre we may order and provision (i.e. if we connect to you)
- Production of Letter of Authority (LOA) to grant you the capability to terminate a fibre cable in our rack (if you connect to us)
- 24/7 proactive monitoring of the service
- Failover. In the event of the primary connection 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 bandwidth basis. Data Centre 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 cross connect / NNI will mirror the overall bandwidth capacity of the platform being purchased.

Lead time

Under normal circumstances, we aim to deliver Data Centre Connectivity in approximately 20 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. This includes delays or extended lead times caused by data centre operators or third party MPLS providers.

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 ISO27001 and ISO9001 accredited. We are also compliant with Cyber Essentials 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