ets connect UK

User & Redistributor Connectivity Guide DRAFT

25 March 2026
Version 0.1

Contents

CTP User & Redistributor Connectivity Guide

1. Scope

This document provides external-facing technical guidance for authorised recipients of UK Bond Consolidated Tape ("CT") data, including:

- direct Users; and
- Redistributors.

It defines the supported network connectivity models, service locations, routing behaviour, and infrastructure requirements necessary to establish and maintain connectivity to CTP service endpoints.

This document covers network-layer connectivity only. It does not define:

FIX protocol message structure or session behaviour;

- REST API schemas or data formats;
- Rules of Engagement or lifecycle handling obligations.
- Application-layer behaviour is documented separately in the relevant technical specifications and Rules of Engagement.

Connectivity requirements described in this guide apply equally to Users and Redistributors. Redistribution arrangements do not alter CTP endpoint architecture, failover behaviour, or regional design.

All connectivity described in this document is via the public internet.

1.1. Version History

Version	Date	Description
0.1	02/03/2026	Initial draft

2. Service Locations and Protocols

2.1. Service Locations

The CTP operates two independent AWS Regions in a dual-region architecture.

Each region:

- functions as a fully operational CT processing and dissemination site;
- maintains independent infrastructure, networking, and health monitoring;
- is capable of operating without real-time dependency on the other region.

A third, non-AWS tertiary location exists for data backup and disaster recovery purposes. Users and Redistributors do not establish network connectivity to this tertiary location.

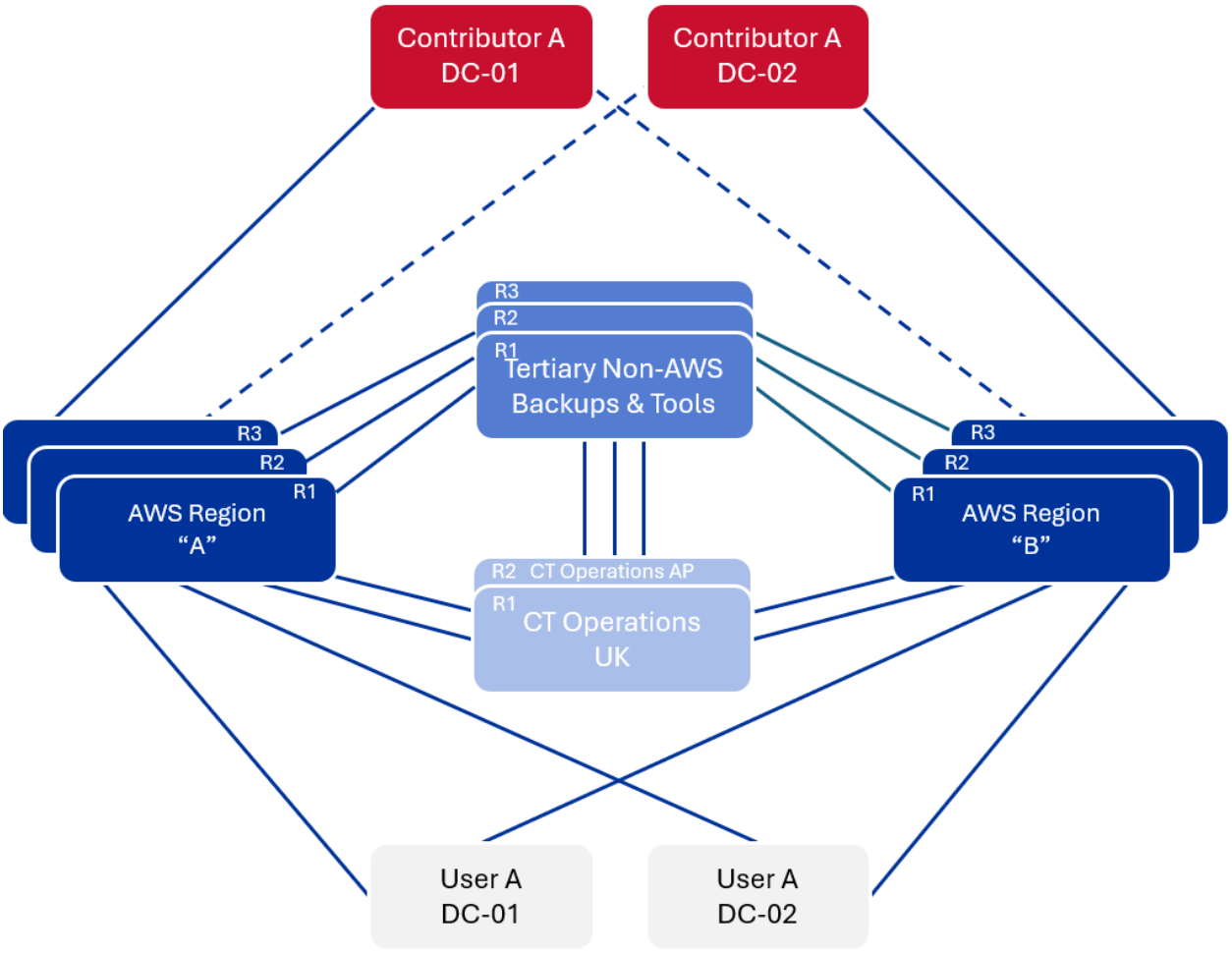
All User and Redistributor connectivity is established via public internet endpoints exposed by the CTP in each active region, or via globally managed endpoints as described in this guide.

2.2. High-Level Architecture

CTP operates an active-active, dual-region architecture where each AWS Region functions as a fully independent post-trade processing site, supplemented by a tertiary region that serves exclusively as a data backup and disaster-recovery repository for both primary regions.

ETS Operations – Asia Pacific and UK, is responsible for managing the active and tertiary regions, ensuring that data processing runs smoothly and that disaster recovery protocols are in place.

The following diagram shows the high-level connectivity model of CTP:



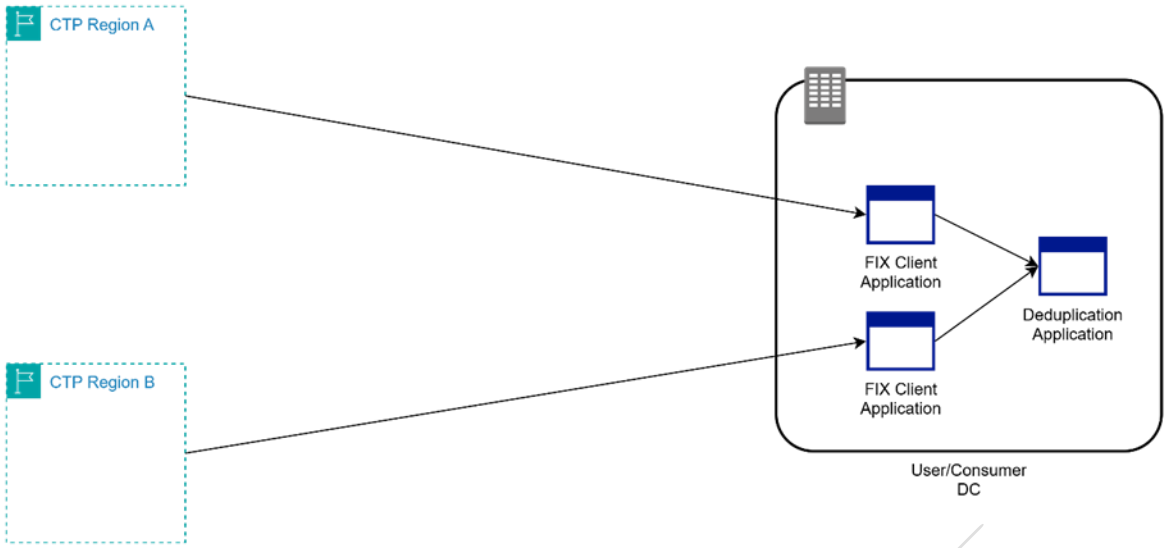
From a User and Redistributor connectivity perspective, the CTP supports two primary architectural patterns:

2.2.1. Dual-Region Active–Active (FIX Only)

- Separate region-specific endpoints are provided for Region A and Region B.
- Users may establish concurrent connections to both regions.
- Each region independently disseminates CT data.
- Duplicate handling is the responsibility of the User (as defined in the RoE).

In this model:

- Region selection and traffic balancing are managed by the User.
- Failover is controlled by the User.



2.2.2. Global Active–Passive (Managed Failover via AWS Global Accelerator)

For selected interfaces, the CTP provides a single globally routed endpoint backed by:

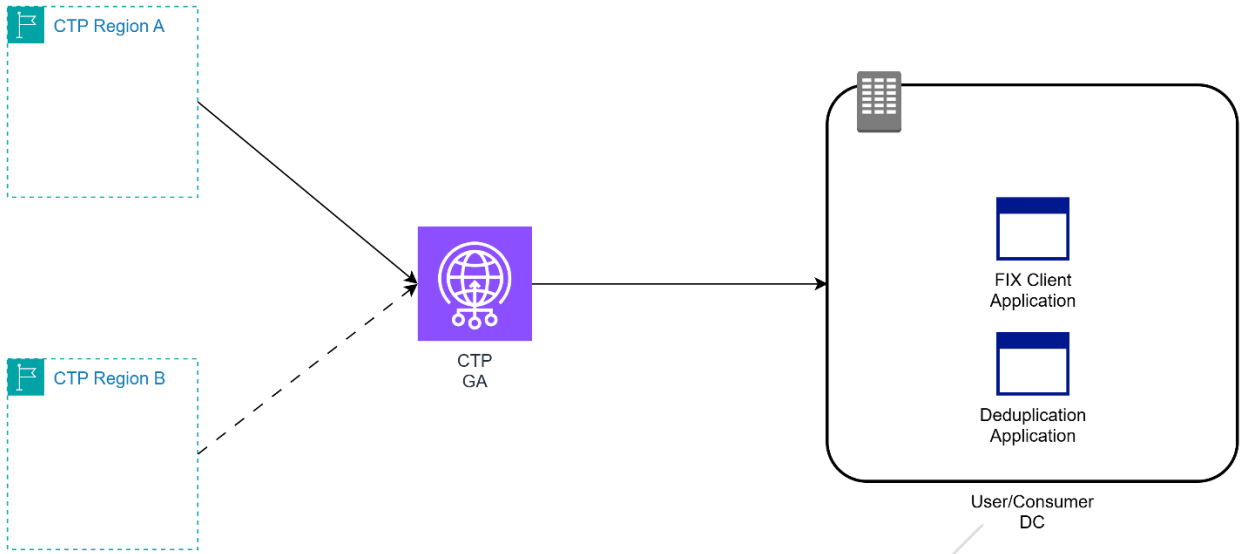
- AWS Global Accelerator (AGA);
- region-level health checks;
- automatic regional failover.

In this model:

- Users connect to a single global DNS endpoint.
- AGA directs traffic to the active healthy region.
- Regional failover is managed by the CTP.
- Users are not required to manage region-level routing.

This model is used for:

- FIX (optional active/passive configuration);
- Real-Time CSV via REST;
- Historical file access via REST.



2.3. Architectural Characteristics

Key characteristics of the CTP user connectivity architecture:

- Dual-region design supports operational resilience and fault isolation.
- Regions operate independently for dissemination.
- No user connectivity is provided to the tertiary disaster recovery location.
- Public internet connectivity is supported exclusively.
- Regional transparency depends on the selected connectivity model (active–active or managed active–passive).

3. FIX Connectivity

This section defines the supported network connectivity models for Users and Redistributors accessing CT data via the FIX Market Data interface.

All FIX connectivity is established over secure TCP using Mutual Transport Layer Security (mTLS) via public internet endpoints.

Application-layer session behaviour is defined separately in the Rules of Engagement.

3.1. Supported Connectivity Models

The CTP supports two FIX connectivity models:

3.1.1. Dual-Region Active–Active (User Managed)

In this model, Users establish independent FIX sessions to both Region A and Region B.

Key characteristics:

- Separate region-specific DNS endpoints are provided.
- Each region independently disseminates CT data.
- Users maintain concurrent FIX sessions to both regions.
- Regional traffic balancing and failover are managed by the User.
- Duplicate handling is required in accordance with the RoE.

This model provides maximum transparency and regional control and is typically used by latency-sensitive or high-availability Users and Redistributors.

3.1.2. Managed Active–Passive (AWS Global Accelerator)

In this model, the CTP provides a single global FIX endpoint backed by AWS Global Accelerator (AGA).

Key characteristics:

- A single DNS/IP endpoint is presented to the User.
- AGA performs regional health checks.
- Traffic is routed to the active healthy region.
- Regional failover is managed by the CTP.
- Users are not required to manage regional routing.
- Duplicate handling is not required during steady-state operation.

During a regional failover event:

- TCP sessions may disconnect.
- Users must re-establish FIX sessions.
- Replay behaviour follows standard FIX recovery mechanisms.

This model simplifies user connectivity and abstracts regional topology.

3.1.3. Model Selection

Users and Redistributors may select either connectivity model during onboarding.

Model selection does not alter:

- the underlying regional architecture;
- service availability targets;

- FIX protocol behaviour.

3.2. FIX Endpoint Details

Endpoint details are environment-specific.

3.2.1. UAT Endpoints

Region	DNS	IP	TCP Port	Protocol
UK Region A	N/A	35.176.86.84	7103	TCP/IP

3.2.2. Production – Region-Specific Endpoints (Active–Active Model)

Region	DNS	IP	TCP Port	Protocol
UK Region A	N/A	167.254.162.44	15003	TCP/IP
EU Region B	N/A	167.254.163.44	15003	TCP/IP

3.2.3. Production – Managed Active–Passive (AGA) Model

Region	DNS	IP	TCP Port	Protocol
Global	N/A	167.254.164.44 167.254.164.45	15003	TCP/IP

3.3. FIX Security Requirements

Requirements:

- TLS 1.2 or higher.
- X.509 certificates presented by both client and server.
- Successful TLS handshake prior to FIX session establishment.
- Certificates must be issued by a trusted certificate authority as defined during onboarding.

Users and Redistributors must:

- Protect private keys associated with client certificates.
- Renew certificates prior to expiry.
- Notify the CTP immediately in the event of suspected compromise.

Sessions will not be established where certificate validation fails.

mTLS requirements apply to:

- Dual-region active–active connections.
- Managed active–passive (AGA) connections.

3.4. Network Requirements

Users must ensure:

- Persistent TCP connectivity.
- Support for mTLS handshake.
- Minimum MTU: 1500 bytes.
- Redundant internet connectivity recommended.
- Proper handling of TCP session resets during failover events.

3.5. IP Addressing and Access Controls

All FIX connectivity requires successful Mutual TLS (mTLS) authentication.

mTLS is the primary access control mechanism for FIX connectivity over the public internet.

Users and Redistributors must provide source IP address ranges during onboarding. Where feasible, the CTP may apply source IP allowlisting as a secondary security control.

Due to the scale and variability of client infrastructure, IP allowlisting may be limited to stable and declared egress ranges.

In addition to mTLS authentication, the CTP may implement per-client operational controls, including:

- limits on concurrent FIX sessions;
- connection rate protections;
- abnormal reconnect detection.

Access controls are applied consistently across Users and Redistributors within the same connectivity model.

4. Real-Time CSV Connectivity

4.1. Architecture Overview

The Real-Time CSV interface provides incremental CT data via HTTPS over the public internet.

This interface operates in a managed active–passive configuration using:

- Amazon S3 for object storage;
- Amazon CloudFront for edge distribution and performance optimisation.

Users and Redistributors connect to a single global endpoint.

Regional failover is managed by the CTP. Users are not required to manage region-specific routing.

During a regional failover event:

- The global endpoint remains unchanged.
- Traffic is automatically routed to the healthy region.
- HTTPS sessions may briefly reset and should be retried using exponential backoff.

4.2. Endpoint Details

Endpoint details are environment-specific.

4.2.1. UAT – Real-Time CSV

Region	DNS	IP	TCP Port	Protocol
UK Region A	bonds.downloads.uat.ets-connect.co.uk	N/A	443	HTTPS

4.2.2. Production – Real-Time CSV

Region	DNS	IP	TCP Port	Protocol
Global	bonds.downloads.ets-connect.co.uk	N/A	443	HTTPS

AWS CloudFront provides a globally distributed content delivery endpoint for each environment. Access is made via the designated DNS name.

CloudFront does not provide dedicated or static IP addresses. Users must therefore allowlist the fully qualified domain name (FQDN) rather than individual IP addresses. Where firewall policies require IP-based controls, Users must rely on AWS-published CloudFront IP ranges, acknowledging that these ranges may change over time.

4.3. Authentication and Security

Real-Time CSV access requires:

- TLS 1.2 or higher.
- Strong client authentication as defined during onboarding (e.g., API token, signed request, or mTLS if applicable).

Authentication mechanisms are environment-specific and are provided during onboarding.

CloudFront and AWS WAF may be used to enforce:

- request validation;
- rate-based protections;
- abuse mitigation;
- geographic or IP-based controls where required.

4.4. Network Requirements

Users and Redistributors must ensure:

- HTTPS outbound connectivity over port 443;
- support for TLS 1.2+;
- appropriate handling of HTTP 3xx/4xx/5xx responses;
- retry logic with exponential backoff;
- efficient polling behaviour consistent with the Rules of Engagement.

Persistent connections are not required for this interface.

4.5. IP Addressing and Access Controls

The Real-Time CSV service is accessed via a single global HTTPS endpoint fronted by AWS Global Accelerator.

The service uses CTP-managed static Anycast IP addresses (BYOIP). These IP addresses are fixed and may be used by Users and Redistributors for outbound firewall allowlisting.

Access to the service requires:

- TLS 1.2 or higher;
- valid authentication credentials.

IP allowlisting may be used as a secondary control where required. Authentication remains the primary access control mechanism.

Users should allow outbound HTTPS (port 443) connectivity to the published global endpoint and associated static IP addresses.

5. Historical Data Connectivity

5.1. Architecture Overview

The Historical Data interface provides periodic and on-demand access to full-day and backfill CT datasets via HTTPS over the public internet.

This interface operates in a managed active–passive configuration using:

- Amazon S3 for object storage;
- Amazon CloudFront for distribution and performance optimisation.

Users and Redistributors connect to a single global HTTPS endpoint.

Regional failover is managed by the CTP. Users are not required to manage region-specific routing.

During a regional failover event:

- The global endpoint remains unchanged.
- Traffic is automatically routed to the healthy region.
- Download sessions may reset and should be retried using appropriate retry logic.

5.2. Endpoint Details

5.2.1. UAT – Historical Data

Region	DNS	IP	TCP Port	Protocol
UK Region A	bonds.historical.uat.ets-connect.co.uk	N/A	443	HTTPS

5.2.2. Production – Historical Data

Region	DNS	IP	TCP Port	Protocol
Global	bonds.historical.ets-connect.co.uk	N/A	443	HTTPS

AWS CloudFront provides a globally distributed content delivery endpoint for each environment. Access is made via the designated DNS name.

CloudFront does not provide dedicated or static IP addresses. Users must therefore allowlist the fully qualified domain name (FQDN) rather than individual IP addresses. Where firewall policies require IP-based controls, Users must rely on AWS-published CloudFront IP ranges, acknowledging that these ranges may change over time.

5.3. File Characteristics

Historical files:

- are made available on a defined UTC schedule;
- represent complete datasets for the relevant business day;
- may include New, Amend, and Cancel records;
- may be large in size depending on dataset scope.

Users and Redistributors are responsible for:

- verifying file completeness;
- validating checksums where provided;
- ensuring lifecycle integrity in downstream processing.

5.4. Network and Download Requirements

Users must ensure:

- outbound HTTPS connectivity over port 443;
- support for TLS 1.2 or higher;
- ability to download large files efficiently;
- support for resumable downloads (recommended);
- appropriate retry behaviour with exponential backoff.

Repeated or automated full-day re-downloads without operational need should be avoided.

5.5. IP Addressing and Access Controls

The Historical Data service is accessed via a single global HTTPS endpoint fronted by AWS Global Accelerator.

Access to historical datasets requires:

- valid authentication credentials; and
- compliance with operational usage expectations defined in the Rules of Engagement.

Operational controls, including rate protections and session controls, may be applied to preserve platform stability and equitable access.

Authentication remains the primary access control mechanism.

6. Contacts

This section defines the primary points of contact for matters related to CTP network connectivity.

For general connectivity concerns please contact For general connectivity concerns please contact info@ets-connect.co.uk