ets connect UK

Accredited Partner Programme Technical Specifications v0.1

26 May 2026
Version 0.1

Contents

This document describes the technical interfaces and infrastructure provided by ETS Connect UK (the CTP) to organisations participating in the Accredited Partner programme. It is intended to enable prospective Accredited Partners to assess the technical integration effort and associated costs of joining the programme. It should be read alongside the Accredited Partner Agreement: Draft Principles.

1. Overview

The CTP provides Accredited Partners with a suite of purpose-built interfaces to support the delivery of L1 Support to CTP clients. All interfaces share a single authentication layer (Auth0 OAuth 2.0) and are accessible over the public internet via HTTPS. No dedicated connectivity, VPN or proprietary network infrastructure is required.

Interface	Type	Purpose
Diagnostics API	REST API	Client-scoped operational log access for L1 Support diagnostics
AP Portal	Web application	Integrated management interface covering client accounts, status, Administrative Functions and CTP GUI access

In addition to the above interfaces, the CTP provides a push email notification service for P1 and P2 incident alerts. This is described in Section 3.

All interfaces are subject to the service level commitments set out in Section 7, aligned to the CTP's obligations under the Concession Agreement.

2. Authentication

All Accredited Partner interfaces — the Diagnostics API and the AP Portal — are secured via Auth0 OAuth 2.0 using the Client Credentials grant flow. This is a Machine-to-Machine (M2M) authentication pattern suited to backend services, automated scripts and API integrations where no end-user context is required.

2.1. How it works

The Accredited Partner authenticates by posting a token request to the Auth0 authorisation server. On successful authentication a short-lived Bearer token is returned, which must be included in the Authorization header of all subsequent API requests.

2.1.1. Token Request

```
POST https://<AUTH0_DOMAIN>/oauth/token
Content-Type: application/json


{
  "grant_type": "client_credentials",
  "client_id": "<YOUR_CLIENT_ID>",
  "client_secret": "<YOUR_CLIENT_SECRET>",
  "audience": "<API_AUDIENCE>"
}
```

2.1.2. Successful Response

```
{
  "access_token": "eyJz93a...k4laUWw",
  "token_type": "Bearer",
  "expires_in": 86400
}
```

2.1.3. Using the token

```
Authorization: Bearer <access_token>
```

2.2. Credentials provisioning

Auth0 client credentials (client_id and client_secret) are provisioned by the CTP during the onboarding process. Credentials are scoped to the Accredited Partner's contracted clients and do not provide access to any data outside that scope. Credentials for the test environment are provisioned separately from production credentials.

2.3. Token management

Tokens expire after 86,400 seconds (24 hours). The Accredited Partner is responsible for implementing token refresh logic in its integration. The CTP recommends requesting a new token before expiry rather than waiting for a 401 Unauthorised response.

2.4. Security requirements

Client credentials must be stored securely and must not be embedded in client-side code, shared repositories or unencrypted configuration files. The Accredited Partner must notify the CTP immediately if credentials are suspected to have been compromised. The CTP will revoke and reissue credentials without undue delay upon such notification.

2.5. HTTP requirements

All requests must be made over HTTPS via port 443. HTTP requests will be rejected. The API follows standard HTTP/1.1 status codes:

Code	Meaning
200	Success
400	Bad Request
401	Unauthorised — invalid or expired token
403	Forbidden — valid token but insufficient scope
429	Too Many Requests — rate limit exceeded
5XX	Server error — escalate to CTP if persistent

3. Notifications and Alerts

The CTP operates a push email notification service to ensure Accredited Partners are proactively informed of incidents that may affect their clients, without requiring active monitoring of the CTP Status Dashboard.

3.1. Trigger events

Email notifications are issued automatically for P1 and P2 incidents as classified under the CTP's incident priority framework. P3 and P4 incidents are visible on the CTP Status Dashboard but do not trigger proactive email notification.

3.2. Notification content

Each notification will include where known:

- Incident classification (P1 or P2)
- Nature and scope of the incident
- Services affected
- Estimated time to resolution
- Recommended actions for Accredited Partners to communicate to their clients

Updates will be issued at regular intervals until resolution. A post-incident summary will be published on the AP Portal following resolution of any P1 incident.

3.3. Designated contact address

Each Accredited Partner must register a designated contact email address during onboarding via the AP Portal. All incident notifications will be delivered to this address. The Accredited Partner is responsible for:

- Maintaining an accurate and monitored designated contact address
- Ensuring appropriate internal distribution of CTP incident notifications
- Updating the designated contact address promptly if it changes

3.4. Integration requirements

No technical integration is required for this service. The designated contact address must be capable of receiving standard SMTP email. The Accredited Partner should ensure the sending domain is not blocked by its email filtering infrastructure. Sending domain details will be provided by the CTP during onboarding.

4. Diagnostics API

The Diagnostics API is a purpose-built REST API providing Accredited Partners with controlled, client-scoped access to operational log data to support L1 Support diagnostics. It is separate from and should not be confused with the ETS Connect data distribution API used by CTP clients to access bond trade data.

4.1. Base URL and transport

```
Base URL: https://diagnostics-api.ets-connect.co.uk  [to be confirmed]
Transport: HTTPS over port 443
Protocol: HTTP/1.1 (RFC 7231)
```

4.2. API style and format

The Diagnostics API is a RESTful API. All responses are returned in JSON format. The API follows standard REST architectural constraints including statelessness, uniform interface and resource-based addressing.

4.3. Data access scope

Access is strictly client-scoped. An Accredited Partner may only retrieve log data relating to its own contracted CTP clients. The CTP enforces this at the authentication layer — credentials issued to an Accredited Partner are bound to that partner's contracted client set and cannot be used to access any other client's data.

4.4. Key endpoints

Endpoint	Method	Description
/v1/diagnostics/logs	GET	Retrieve client-scoped operational logs
/v1/diagnostics/clients	GET	List contracted clients and their connection status
/v1/diagnostics/clients/{clientId}/logs	GET	Retrieve logs for a specific client
/v1/diagnostics/clients/{clientId}/sessions	GET	Retrieve active and recent session data for a specific client

Endpoint paths are indicative and subject to confirmation in the full Diagnostics API specification published via the AP Portal.

4.5. Pagination

The Diagnostics API supports cursor-based pagination consistent with the ETS Connect data API:

- limit — required integer, maximum 1000 records per request
- after — optional cursor representing the ID of the last record received
- Initial requests without after return the most recent records

4.6. Polling strategy

The Diagnostics API is a pull-based interface. Accredited Partners should implement a polling strategy appropriate to their support workflow:

- Recommended polling interval: every 1 to 5 seconds for active incident diagnosis
- Avoid excessive polling — requests exceeding rate limits will receive a 429 response
- Catch-up mechanism: if the integration has been offline, increase limit and iterate using after until current

4.7. Rate limits

Rate limits will be defined and published in the full Diagnostics API specification available via the AP Portal. Accredited Partners should implement appropriate back-off and retry logic. The CTP reserves the right to adjust rate limits with reasonable notice.

5. Log Data

The Diagnostics API provides access to client-scoped operational logs covering all significant interactions between the client and the CTP platform. Log data is sourced from AWS OpenSearch and is refreshed in near real-time.

5.1. Log categories

Log Category	Description
API / FIX Session Logs	FIX 5.0 session establishment, message activity, disconnections and errors for clients connecting via the CTP API
Authentication Logs	GUI and API login attempts, success and failure events, session token activity
File Activity Logs	Historical data file download requests, delivery confirmations and failures
Administrative Action Logs	All actions taken by the Accredited Partner on behalf of a client via the Administrative Functions, providing a full audit trail

Additional log categories may be added by the CTP as the platform evolves. The full log schema for each category will be published in the Diagnostics API technical specification available via the AP Portal.

5.2. Log format

All log data is returned as JSON. Each log record will include at minimum:

- A unique record identifier
- A timestamp (ISO 8601 format, UTC)
- The client identifier

- Log category
- Event type
- Event detail

5.3. Data volume

Log volume is classified as medium. Accredited Partners should size their storage and processing infrastructure accordingly. Indicative volume guidance will be provided during onboarding.

5.4. Data retention

Log data is retained by the CTP in accordance with its obligations under the Concession Agreement. Accredited Partners must not retain Accredited Partner Data beyond what is necessary for their L1 Support function. Specific retention periods will be confirmed in the Diagnostics API specification.

5.5. Data scope limitation

Log data returned via the Diagnostics API is strictly scoped to the Accredited Partner's contracted clients. The CTP does not provide access to aggregated, cross-client or platform-wide log data via this interface.

6. AP Portal

The AP Portal is the primary web-based management interface for Accredited Partners. It is an integrated interface delivering four capability areas via a single authenticated session. Access is via standard web browser, no client-side software installation is required.

6.1. Authentication

The AP Portal uses the same Auth0 OAuth 2.0 credentials as the Diagnostics API. Human users authenticate via the Auth0 login flow (username and password with MFA). No separate credential set is required.

6.2. Capability areas

6.2.1. Client Licence and User Account Management

The AP Portal provides the Accredited Partner with visibility of:

- Licence details for each contracted client including licence type, commencement date and status
- All user accounts associated with each client, covering both human users and programmatic/API accounts
- Account status, access permissions and last activity indicators

This enables the Accredited Partner to diagnose access and permission-related support queries without requiring client-side investigation or CTP involvement.

6.2.2. CTP Status Dashboard

A real-time, CTP-wide operational status view available equally to all Accredited Partners, providing:

- Current service status across all CTP platform components
- Planned maintenance windows and scheduled downtime
- Active incident notifications with classification, scope and estimated resolution time
- A rolling change log of recent and upcoming platform changes

The CTP Status Dashboard is the authoritative source of CTP platform status for Accredited Partners. Accredited Partners should monitor the dashboard proactively and use it to inform their clients of any platform status issues, planned maintenance or upcoming changes, enabling them to get ahead of client queries before tickets are raised.

6.2.3. Administrative Functions

A defined set of client-scoped operational actions enabling the Accredited Partner to resolve common L1 Support issues without escalation. The initial function set includes by way of example:

- Reset a client FIX session
- Reset a client user password
- Unlock a client user account

The full function set is defined and published by the CTP via the AP Portal. Each function is documented with its scope, conditions of use, client impact considerations and any required client authorisation. The CTP may extend the function set at its sole discretion.

Accredited Partners may not request additional functions outside the published set. All Administrative Function actions are logged and auditable by the CTP.

6.2.4. CTP GUI Access

Display-only access to the CTP graphical user interface, enabling the Accredited Partner to view bond trade data as seen by the client, for the purpose of handling data-related queries. No actions may be taken via the CTP GUI. Access is read-only and fully audited.

6.3. Browser requirements

The AP Portal supports current versions of major browsers (Chrome, Firefox, Edge, Safari). Specific browser requirements will be confirmed in the AP Portal user guide published at onboarding.

6.4. Availability

The AP Portal is subject to the same availability commitments as the Diagnostics API as set out in Section 7.

7. Availability and SLAs

This section sets out the complete service level framework for Accredited Partners, covering both the CTP's obligations in respect of the AP Portal and Diagnostics API, and the AP's obligations in respect of L1 Support delivery to clients.

7.1. CTP resolution obligations

The following resolution obligations apply to the CTP in respect of the AP Portal and Diagnostics API:

Priority	Description	CTP Resolution Obligation
P1	Complete loss or severe disruption to AP interfaces	2 hours
P2	Significant degradation affecting AP support capability	4 hours
P3	Partial degradation with workaround available	10 hours

Priority	Description	CTP Resolution Obligation
P4	Minor issue with agreed workaround	20 hours

7.2. AP L1 Support SLA cascade

The AP's L1 Support SLA obligations are structured as a percentage of the CTP's own resolution windows, in accordance with the operational level agreement framework set out in ISO/IEC 20000-1:2018. This ensures the AP always has sufficient time to resolve or escalate before the CTP's own obligation deadline is at risk. The AP clock starts when the client raises the ticket.

Priority	CTP Resolution Obligation	AP Resolve or Escalate	AP Window
P1	2 hours	25%	30 minutes
P2	4 hours	25%	1 hour
P3	10 hours	30%	3 hours
P4	20 hours	50%	10 hours

Where an AP cannot resolve an L1 Support ticket within its window, it must escalate to the CTP immediately via the dedicated escalation mailbox, with full ticket details using the standard escalation template. Failure to escalate within the AP window constitutes a breach of the Accredited Partner Agreement.

7.3. Planned maintenance

Planned maintenance will be communicated via the CTP Status Dashboard and email notification with a minimum of [90 Business Days] notice, except in the case of emergency maintenance required to address a Security Incident or critical vulnerability.

8. 8. Ticketing and Escalation

8.1. AP to client ticketing

Accredited Partners may use their own ticketing platform of choice for managing client support interactions. There is no mandated ticketing platform.

8.2. Ticket visibility — CTP-provisioned mailboxes

To give the CTP full visibility of AP ticket activity for performance reporting and quality assurance purposes, the CTP will provision each Accredited Partner with two dedicated email mailboxes at onboarding:

- Closure Mailbox: receives auto-generated closure notifications from the AP's ticketing platform when a ticket is resolved at L1.
- Escalation Mailbox: receives escalation notifications from the AP's ticketing platform when a ticket is escalated to the CTP.

Both mailboxes are provisioned and managed by the CTP. The AP is responsible for configuring its ticketing platform to auto-forward to the relevant mailbox at the appropriate trigger event. No API integration is required.

8.3. Closure template

All closure notifications must be sent to the CTP-provisioned closure mailbox using the standard closure template published via the AP Portal. At minimum each closure notification must include:

Field	Description
Client ID	The CTP client identifier for the affected client
Priority	P1 / P2 / P3 / P4 per the incident priority framework
Issue Type	Category of issue (e.g. API connectivity, authentication, data query, account access)
Opened Timestamp	When the client raised the ticket (UTC)
Closed Timestamp	When the AP resolved the ticket (UTC)

Field	Description
Resolution Summary	Brief description of the action taken and resolution achieved
AP Reference	The Accredited Partner's own ticket reference for cross-referencing

8.4. Escalation template

All escalation notifications must be sent to the CTP-provisioned escalation mailbox using the standard escalation template published via the AP Portal. At minimum each escalation notification must include:

Field	Description
Client ID	The CTP client identifier for the affected client
Priority	P1 / P2 / P3 / P4 per the incident priority framework
Issue Type	Category of issue (e.g. API connectivity, authentication, data query, account access)
Opened Timestamp	When the client raised the ticket (UTC)
Escalation Timestamp	When the AP escalated the ticket (UTC)
Description	Clear description of the issue, steps taken by the AP and outcome of each step
AP Reference	The Accredited Partner's own ticket reference for cross-referencing

8.5. Escalation SLA

Escalations must be raised within the AP's SLA window as defined in Section 7.2. Failure to escalate within the applicable window constitutes a breach of the Accredited Partner Agreement.

8.6. CTP response

The CTP will acknowledge all escalations and respond within the remaining resolution window for the applicable priority level. The CTP will update the Accredited Partner at regular intervals until resolution and will publish a post-incident summary on the AP Portal for all P1 incidents.

9. Environments

The CTP provides two environments for Accredited Partners:

Environment	Purpose	Access
Test	Integration development, onboarding validation and ongoing regression testing	Provisioned during onboarding
Production	Live client support operations	Provisioned following go-live sign-off

9.1. Test environment

The test environment replicates the production AP Portal and Diagnostics API with representative but synthetic log data. It is available for use throughout the Accredited Partner relationship for integration testing and staff training. Test environment credentials are issued separately from production credentials and are provisioned by the CTP as the first step of the onboarding process.

9.2. Production environment

Production credentials and access are provisioned only following successful completion of the onboarding process and go-live sign-off by the CTP. Go-live sign-off requires the Accredited Partner to demonstrate successful integration with the test environment, completion of the onboarding training programme and readiness to deliver L1 Support in accordance with the Accredited Partner Agreement.

9.3. Environment availability

The production environment is subject to the SLA commitments in Section 7. The test environment is provided on a reasonable endeavours basis and is not subject to the same SLA commitments.

10. Security and Connectivity

10.1. Connectivity

All Accredited Partner interfaces are accessible over the public internet. No dedicated connectivity, leased lines, VPN or proprietary network infrastructure is required, significantly reducing the Accredited Partner's connectivity costs and setup time.

10.2. Transport security

All connections must use HTTPS over TLS 1.2 or higher. Connections using TLS 1.0 or 1.1 will be rejected. The CTP operates certificate management in accordance with industry best practice.

10.3. IP whitelisting

The CTP does not currently require Accredited Partners to register static IP addresses. However the CTP reserves the right to introduce IP whitelisting requirements in future with reasonable notice, should this be required for security or regulatory reasons.

10.4. Firewall requirements

Accredited Partners must ensure their own firewall and network configuration permits outbound HTTPS connections to the CTP API and portal domains over port 443. Specific domains to be whitelisted will be provided during onboarding.

10.5. 10.5 Credential security

Auth0 client credentials must be stored securely using appropriate secrets management tooling (e.g. AWS Secrets Manager, Azure Key Vault, HashiCorp Vault or equivalent).

Credentials must not be stored in source code, version control repositories or unencrypted configuration files.

11. AP Infrastructure Requirements

This section summarises what a prospective Accredited Partner needs to build, integrate and operate in order to participate in the programme. It is intended to support cost and effort assessment.

11.1. What the CTP provides

Component	Provided by CTP	Notes
Diagnostics API	Yes	REST API, AWS API Gateway, public internet
AP Portal	Yes	Web application, browser-based, no client install required
Auth0 credentials	Yes	Provisioned during onboarding, test and production separately
Test environment	Yes	Synthetic data, available throughout the AP relationship
Onboarding training	Yes	Structured programme prior to go-live
API and portal documentation	Yes	Published via AP Portal
Closure and escalation email templates	Yes	Published via AP Portal
Dedicated closure mailbox	Yes	CTP-provisioned, provided at onboarding
Dedicated escalation mailbox	Yes	CTP-provisioned, provided at onboarding
Incident email notifications	Yes	Push email for P1 and P2 incidents, no integration required

11.2. What the AP must build and integrate

Component	AP Responsibility	Notes
Auth0 OAuth 2.0 integration	Required	Client Credentials grant flow, token refresh logic
Diagnostics API integration	Required	REST client, polling logic, JSON parsing
Log storage and processing	Required	Sized for medium volume
Helpdesk / ticketing platform	Required	Any platform, AP's choice
Auto-forward to CTP closure mailbox	Required	Triggered on ticket closure, standard template
Auto-forward to CTP escalation mailbox	Required	Triggered on escalation, standard template
Secrets management	Required	For secure Auth0 credential storage
Staff training and onboarding	Required	Using CTP-provided materials and programme

11.3. What the AP must operate and maintain

Component	AP Responsibility	Notes
ISO 27001 or SOC 2 Type II certification	Required	Scoped to CTP support function — see Draft Principles Principle 3
ISO 20000 or equivalent service management	Required	Scoped to CTP support function — see Draft Principles Principle 3
Designated contact email address	Required	Must be monitored and kept current

Component	AP Responsibility	Notes
Auth0 credential security	Required	Secrets management, immediate incident notification obligation
Accredited Partner Data retention controls	Required	Must not retain beyond support function need
Annual certification renewal and scope statement	Required	Submitted to CTP at each annual renewal

11.4. Technology stack

The CTP does not mandate a specific technology stack, cloud provider or infrastructure platform for Accredited Partners, provided the security and certification requirements set out in the Accredited Partner Agreement: Draft Principles are met. Accredited Partners are free to integrate the Diagnostics API and AP Portal into their existing support infrastructure.