ELTO Employers' Liability Tracing Office

Getting Started Test API and Credential Management guidance

Practical guidance on Test API and Credential Management

11/08/2026

ELTO Employers' Liability Tracing Office

Contents

1. About this guide

This guide helps insurer technical teams get ready to connect to the ELD NextGen test ingestion APIs. It explains the journeys and checks that are likely to be useful, while leaving each insurer free to design its own integration, security controls and internal test plan.

It is intended for developers, system integrators, technical leads and credential managers. It is not a substitute for your organisation's security policies, certificate-management standards, change controls or production-readiness process.

Things to keep in mind

- Portal access should only be set up for individuals who need to access, create, and manage credentials for API integration — not for general business users.
- This release is an Alpha release of the platform. Only the credentials management area is currently accessible; further functionality will be added in upcoming releases.
- If you are experiencing any issues when trying to authenticate / log-in to the portal, or you suspect your organisation or role is not set-up correctly, please contact elto.ishelpdesk@elto.org.uk for support.

2. Before you begin

To access the information within this guide you will need to have an authorised account for the ELD portal and / or be granted access to the Developer Portal.

To get started using the ELD Developer Portal you will need to:

1. Accept the email invite to the ELD Portal
2. Create your Certificate Key Pair
3. Create your API Test Credential adding your public key
4. Securely store your credential information
5. Create your Bearer Token
6. Test your authentication
7. Build and test your endpoints.

3. Accessing the ELD portal

The ELD portal is accessible via: https://eltohub.org.uk/ .

Access to the ELD is provisioned manually, using the email address your organisation shared during onboarding. You do not need to register independently — once your details have been submitted and we have onboarded you; you will receive an email invitation to create your account.

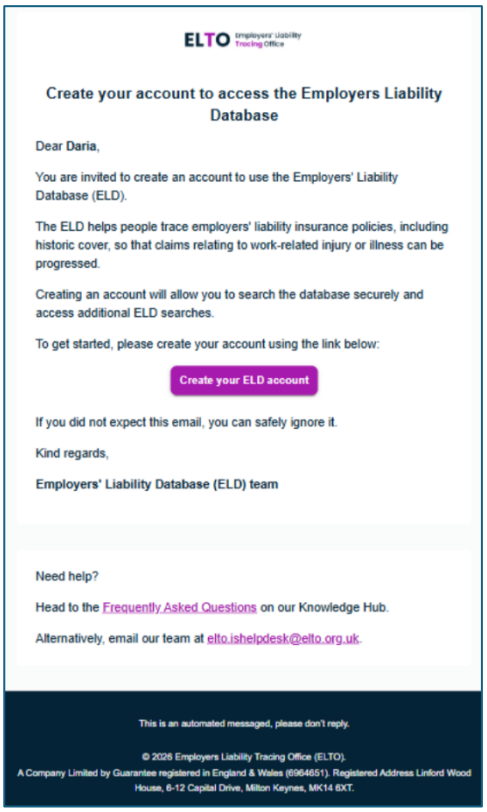
3.1 Receiving your invitation

You will receive an invitation email asking you to create your account to access the Employers' Liability Database (ELD).

The email will appear in your inbox with the subject line: Create your account to access the Employers Liability Database.

Select **"Create your ELD account"** in the email to begin. This will redirect you to Microsoft Entra, which handles sign-in and identity verification for the platform.

Note: Invitations will remain valid for 72 hours; if you try to accept the invitation after 72 hours has passed then you will be presented with an error page when trying to log-in and will need to contact ELTO for another valid invitation to be sent.



ELTO Employers' Liability Tracing Office

Create your account to access the Employers Liability Database

Dear Daria,

You are invited to create an account to use the Employers' Liability Database (ELD).

The ELD helps people trace employers' liability insurance policies, including historic cover, so that claims relating to work-related injury or illness can be progressed.

Creating an account will allow you to search the database securely and access additional ELD searches.

To get started, please create your account using the link below:

Create your ELD account

If you did not expect this email, you can safely ignore it.

Kind regards,

Employers' Liability Database (ELD) team

Need help?

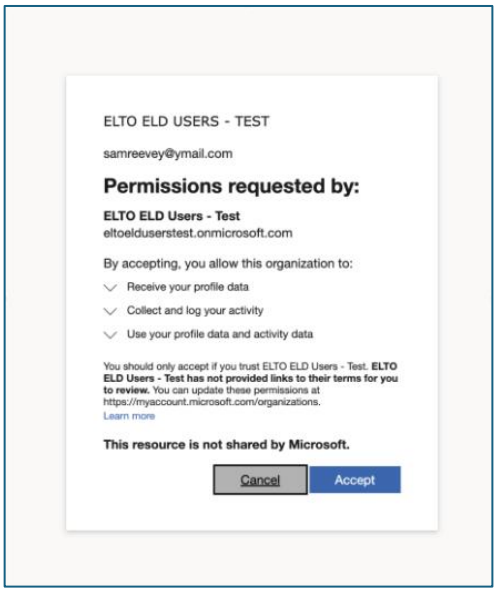
Head to the Frequently Asked Questions on our Knowledge Hub.

Alternatively, email our team at elto.ishelpdesk@elto.org.uk.

This is an automated messaged, please don't reply.

3.2 Creating your account with Microsoft Entra

On selecting "Create your ELD account" in the invite email you will be redirected to the Entra sign-in flow, where you will be asked to enter the email address you shared with ELTO for access, and to accept Microsoft's terms of use as part of setting up the account.



The sign-up flow you see next depends on whether your organisation already has an existing Microsoft Entra tenant:

- **If your organisation has an existing Microsoft Entra tenant:** you will be prompted to sign in using your existing organisational credentials associated with the email address shared with ELTO.
- **If your organisation does not have an existing Microsoft Entra tenant:** you will be prompted to sign in using a one-time password sent to your email address.

3.3 Verifying your email

After entering your email address, you will need to verify your account.

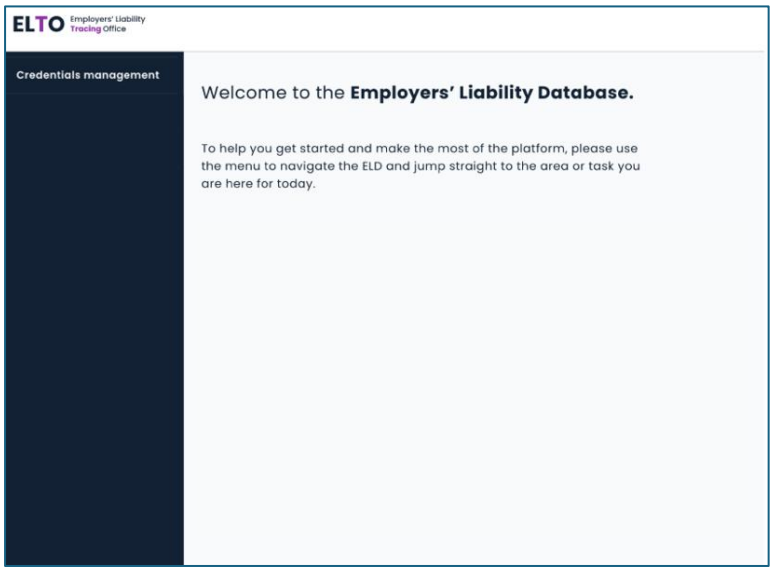
Verification	Steps
If you have an Entra account…	A prompt will appear to enter your account password to verify your access. Once verified you will be prompted for multi-factor authentication.
If you do not have an Entra account…	A one-time passcode (OTP) will be emailed to you, enter this code when prompted. ***Note**: OTP codes are valid for 30 minutes.*

Verification	Steps
	Once verified you will be sent an SMS as part of the multi-factor authentication process. Enter the correct code to complete authentication. ***Note:*** *SMS codes expire after 10 minutes*

3.4 What you can do in the ELD Portal

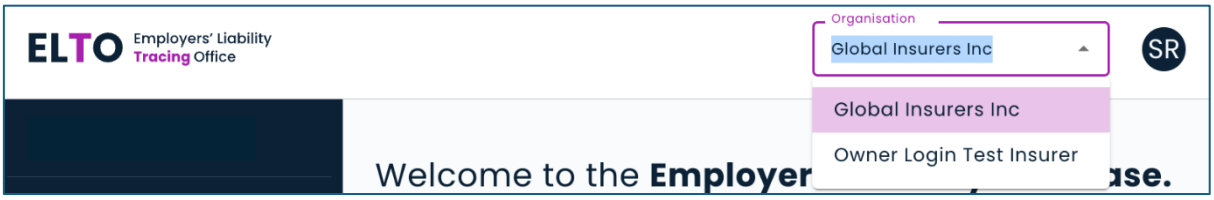
This is an Alpha release and the portal is restricted for the purpose of accessing and managing API Credentials only.

Once you have successfully logged in you will land on the home page where you can navigate using the left-hand menu to "Credential Management".



3.5 Switching between organisations

In the ELD NextGen platform, it is possible for a user to belong to multiple organisations. If you do, then an organisation drop-down list will appear on the top-right hand corner of the header area, as shown below.



When you switch between an organisation you will be sent back to the home screen.

Note: When an action is performed in the portal, it will only apply to the organisation that has been selected in the drop-down list at that time.

4. Credential Management

The ELD ingestion API uses a short-lived access token (bearer token) that ensures authentication using your API credentials via a certificate key pair. In addition to authorising your access, the bearer token validates and confirms the insurer you are submitting data for.

To manage your credentials you will need to generate a Certificate Key pair to add to each API Credential in the ELD Portal and programmatically generate your bearer token with each API request to authenticate your access.

Note: Guidance on creating a Certificate and Bearer token can be found on the Developer Portal.

Credential principles

- Test and production credentials are separate. Test credentials will not authenticate to production endpoints.
- A credential can be valid for no more than one year (365 days). A shorter period set in the certificate will be reflected by the portal. A longer period will be capped at 365 days.
- The portal expects the public key/certificate in PEM format. Keep the private key within your organisation's secure control.
- Use a clear naming convention so the owning system, environment and purpose are obvious.
- Create separate credentials where separation of systems, suppliers or operational ownership is needed.
- Plan renewal before expiry and remove credentials that are no longer required.
- The portal should not be treated as a replacement for your internal secrets inventory or renewal process.

Recommended naming convention

A useful pattern is: <organisation>-<system>-<environment>-<purpose>-<expiry year>. For example: ExampleInsurer-PolicyHub-Test-Ingestion-2027.

4.1 View your credentials

Credentials management is the area of the ELD portal where your organisation creates and maintains the API credentials used to authenticate requests to ELD's endpoints. To access click on "Credential Management" in the left-hand menu.

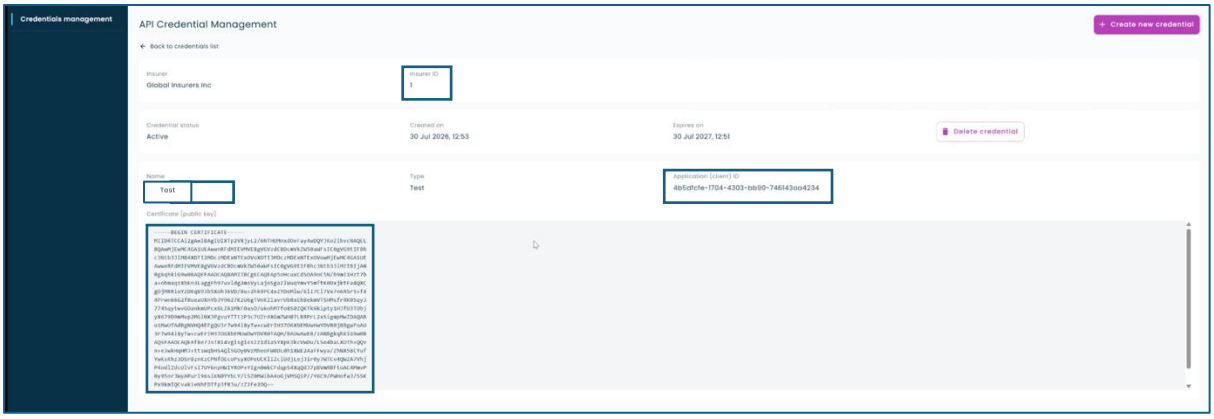
After selecting the Credentials Management, you will be taken to the Credentials Management list page, which lists all credentials created for your organisation

When first logging in, you shouldn't expect to see any credentials listed and will only see them once created.

Credential States

State	Meaning	Action
Active	The credential is within its validity period and can authenticate to the applicable endpoints.	Monitor expiry and use only for its intended environment/system.
Expired	The validity period has ended and the credential can no longer authenticate.	Create a new credential; do not expect the old credential to be reactivated.
Deleted	The credential was actively revoked and associated Entra resources are removed.	Replace it if access is still required and remove old secret material internally.

By selecting one of the credentials in the list, you will be directed to the credentials details page.

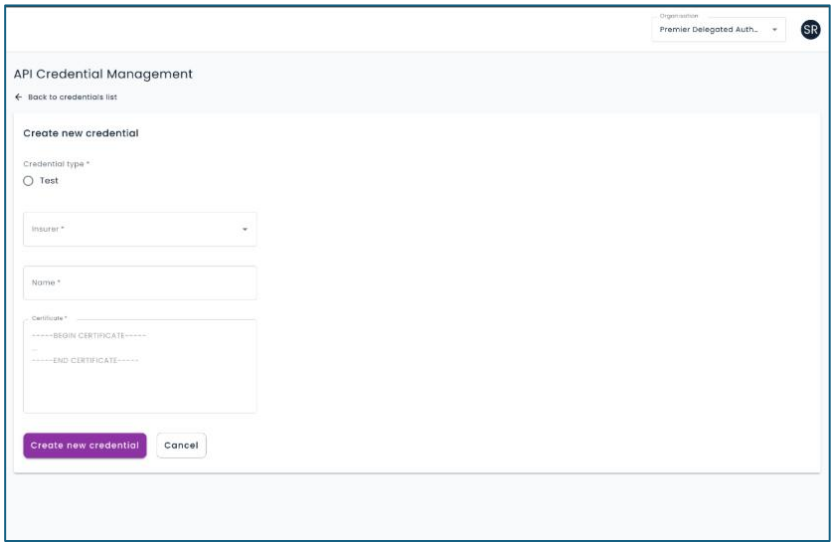


On the credentials details page you will find:

- Your Insurer ID
- Your Application (client) ID
- Your Certificate Public Key that you entered.

4.2 Create a new test credential

To create a new test credential you must first generate / obtain your certificate key pair (see guidance in the Developer portal under creating a bearer token).



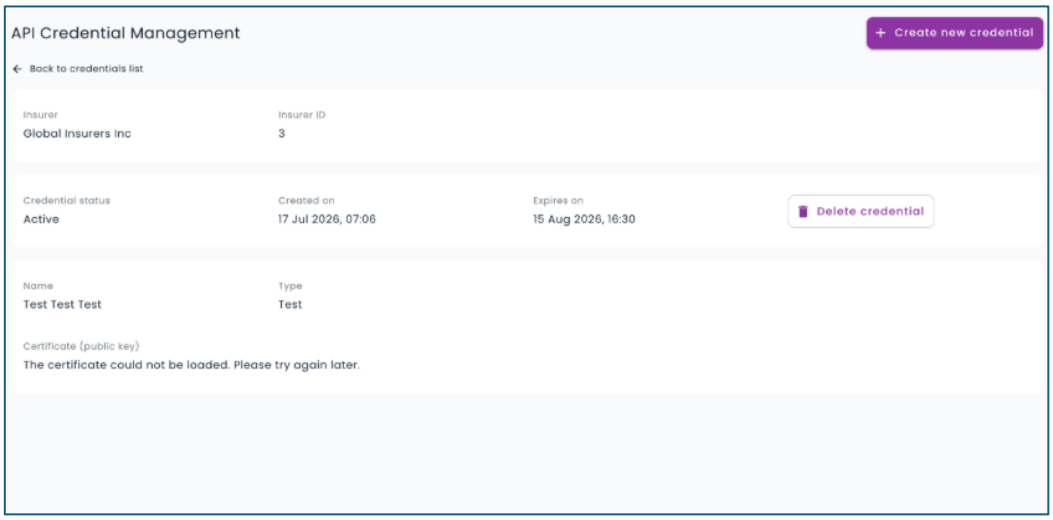
To create a new API credential:

1. On the credentials management landing page, click "+ Create new credential" in the top right of the screen.
2. Select Test
3. If your organisation supplies for more than one insurer select the insurer the credential is for using the drop down.
   ***Note**: If you only supply for one insurer you will not see this drop down*
4. Enter a meaningful credential name (see guidance below)
5. Paste the full the corresponding public key.
6. Review the details and if correct click "Create new credential".
7. Record the returned credential details Application (Client) ID and insurer ID in your approved secrets management solution.
   ***Note**: Do not place secrets in email, source control, tickets, or test evidence.*

4.3 Delete/revoke a credential

Credentials can be deleted from the same area once they are no longer required. Deleting a credential is a deliberate way to revoke access before its natural expiry date.

Note: *Deleting a credential is an active revocation. It cannot be reactivated; a new credential must be created.*



To delete / revoke a credential

1. Confirm that the credential is no longer required or has been replaced.
2. Select the credential you wish to delete
3. In the credential details page click "Delete credential" button.
4. Confirm the action
5. Test that the credential can no longer authenticate.
6. Remove the related secret/private key from dependent systems and update your internal records.

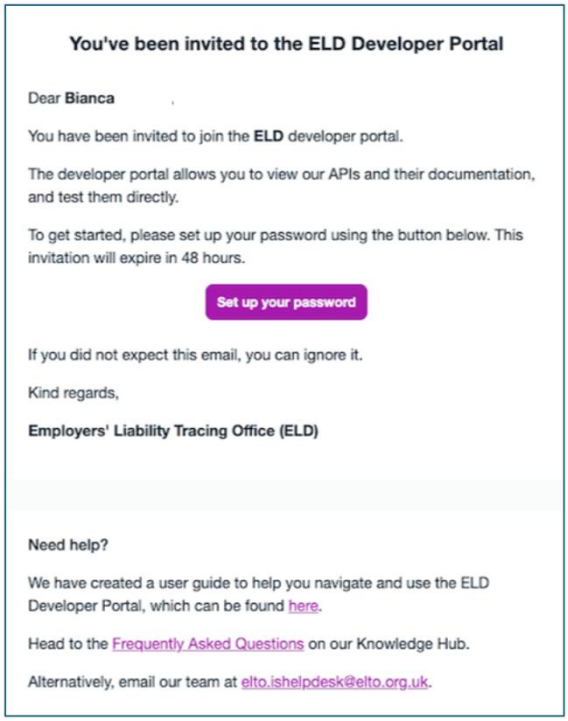
5. Developer Portal

The developer portal is where you can explore API documentation and try out test endpoints ahead of building your integration. It is accessed separately from the main ELD portal, at: https://developer.eltohub.org.uk .

The Developer Portal is the authoritative technical specification for the ELD APIs. For each endpoint, developers will find:

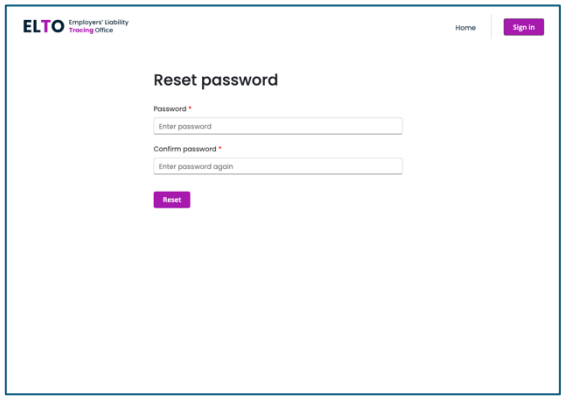
- HTTP method and endpoint URL;
- required path parameters;
- required and optional headers;
- request schema;
- working request example;
- successful response example;
- validation/error response example;
- HTTP response codes;
- size/rate limits where applicable;
- retry and idempotency behaviour;
- test-specific behaviour.

5.1 Signing in



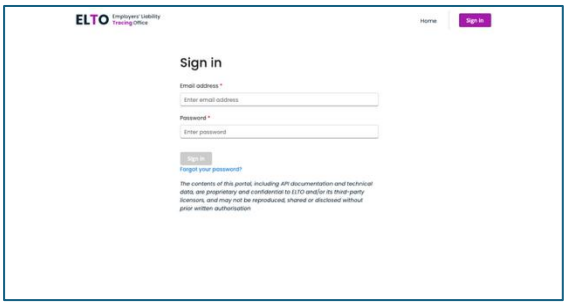
Similarly to the ELD platform, access to the Developer Portal is provisioned manually, using the email address your organisation shared during onboarding. Once your details have been submitted and we have onboarded you, you will receive an email invitation to create your Developer Portal account.

The developer portal uses a separate authentication service to the ELD portal, and therefore separate credentials are required to be used.



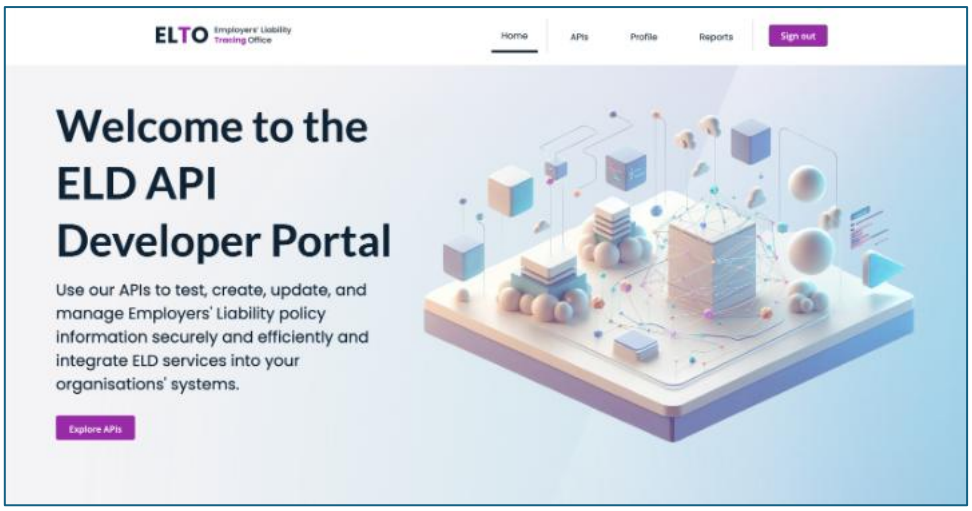
After clicking the link on the invite, you will be redirected to set a password for the account. Please choose your own secure password to manage. If at any point you forget your password, then there is a password reset function available on the Developer Portal log-in page.

Once you have set a password for the account and selected reset, you will be asked to sign-in using the credentials you just created.



Note: *The email address to enter here must be the same one you provided to ELTO, and that you use to log-in to the ELD portal.*

Once you have successfully logged into the Developer portal, you will be navigated to the landing page.



5.2 Navigating the Developer Portal

Once signed in, the navigation menu at the top of the page gives you access to the different areas of the developer portal:

Area	Purpose
Home	From the home screen you can access key resources.
API	From the API area you can access all the API documentation and test the endpoints.
Profile	The Profile section lets you see details about the account you are currently signed in as.
Reports	The reports section lets you see API calls and request data including response times.

Key Resources

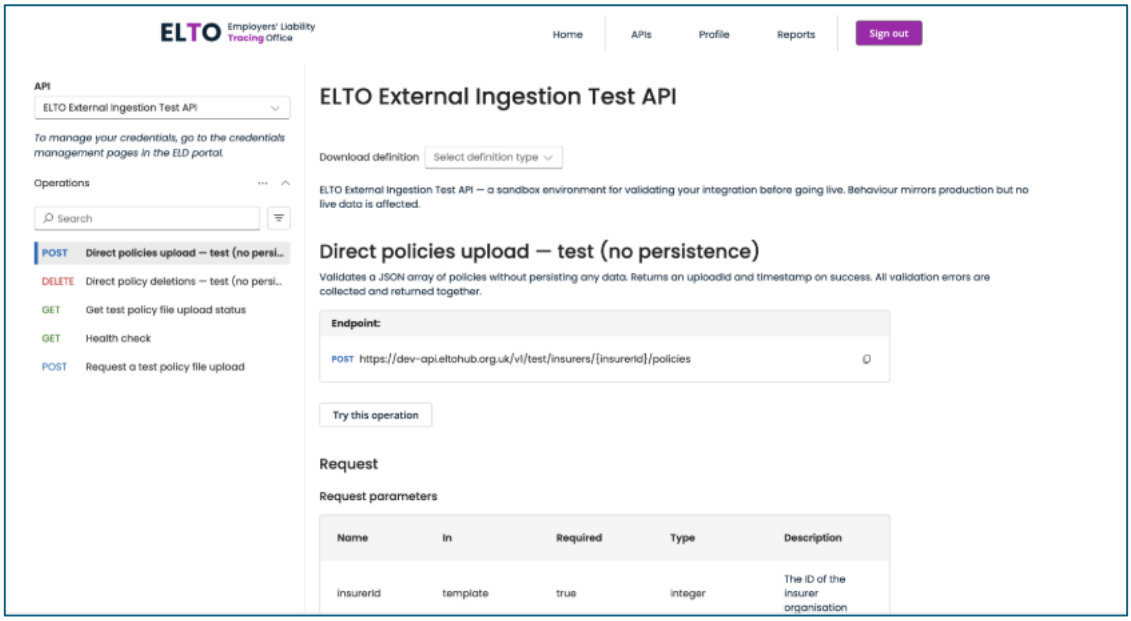
There are resources available on the developer portal for support, including:

- **Getting Started** – this will link you back to this guide
- **Create credentials –** this will navigate you directly to the ELD portal; if you already have a valid token session in the ELD portal then you will be routed directly through to the credentials list page. If not, it will direct you to the ELD portal landing page.

- **Create bearer token** – this will navigate you to a guide in the Developer Portal explaining how to generate Certificate key pairs and how to create a bearer token.
- **Schema** – this will navigate you to a guide explaining the policy schema, what each field is used for and how the legacy system maps to ELD NextGen.
- **File Transfer** – this will navigate you to a guide explaining how to set up your file should you wish to send policy data via file using the Policy File upload API.
- **Contact Us** – an email to contact ELTO support team if there are any issues.

5.3 Exploring the APIs

The APIs section lists the test endpoints that will be supported for ELD NextGen, so you can review what is available before starting your integration work:



From within an API, the left-hand side bar lets you move between the different endpoints covered by that API's documentation and you can also download the full specification from the menu in your preferred definition type.

End Point	Purpose
Health check	Checks all endpoints and their status.
Direct policies upload	Used for loading policies directly via JSON
Direct policy deletions	Used for deleting policies directly via JSON

End Point	Purpose
Request a test policy file upload	Used for requesting the URL for policy file loading
Get test policy file upload status	Used for validating the status of a policy file upload.

For each endpoint, the documentation describes how the API functions, including:

- Request parameters — the inputs an endpoint accepts, and whether each one is required.
- Request body — the structure of the data you need to send, where applicable.
- Response types — the possible responses you may receive back, including success and error cases.
- Definitions — the shape of the data objects used across requests and responses.

Reviewing this documentation for each endpoint you plan to use is a good first step before writing any integration code, as it sets out exactly what your systems will need to send and what they can expect to receive back.

5.4 API Limits

The following limits apply to the API endpoints:

Item	Limit
JSON Payload Limit	2MB
File Size Limit	No set limit
Record Count Limit	No set limit but must not exceed other limits
SAS URL lifetime	60 minutes
API throttling (request / time period)	60 rpm / 5,000 rpd
Polling Interval	No more than once every 30 seconds

6. Authenticating to the endpoint

When you call the ELD Ingestion API, you do not send your certificate or credential directly with each request. Instead, authentication works in two stages:

1. You request a short-lived access token (bearer token). This proves your identity using the private key that corresponds to the public certificate you uploaded when creating your credential in the ELD portal. Microsoft Entra ID validates your identity and issues a temporary token.
2. You include this bearer token in the header of every API request. The ELD platform checks that the token is valid, has not expired, and belongs to a credential that is active and authorised for the insurer you are submitting data for.

Token lifecycles and good practice

These practices are to provide guidance and should not be a substitute for your organisation's security policies:

- Request tokens programmatically: Your integration should request a new token each time it needs one, rather than storing a token value long-term.
- Do not reuse expired tokens: If a request returns a 401 response, obtain a fresh token and retry.
- Keep the private key secure: The private key is the most sensitive part of your integration. Store it in your organisation's approved secrets management solution. Never embed it in source code, configuration files, or test evidence.
- Renew credentials before expiry: When a credential approaches its expiry date, create a new credential with a new certificate and update your integration to use the new private key. Plan this renewal in advance to avoid any interruption to your API access.
- Do not share tokens: Bearer tokens are specific to the credential and environment they were requested for. They should not be shared between systems or individuals.

NOTE: Full guidance on generating bearer tokens can be found in the resource section of the Developer Portal.

7. Recommended test approach

Insurers should tailor testing to their own architecture and risk. The sequence below is a practical starting point rather than a mandatory script.

Before calling an endpoint

- Confirm you are using a /test/ endpoint and a test credential.
- Confirm the insurerId belongs to the organisation you are testing for, this can be found on the credentials management page in the ELD.
- Use synthetic data and make the test record identifiable without using personal data.
- Capture the request timestamp and correlation/request identifier for support queries.

Stage	Recommended checks
1. Connectivity	Authenticate successfully to a simple test request; confirm invalid or missing credentials are rejected.
2. Valid direct request	Submit a valid UPSERT to POST /test/insurers/{insurerId}/policies and compare the response with the specification.
3. DELETE	Submit a representative DELETE to the test endpoint and check both valid and invalid cases.
4. File flow	Initiate an upload, use the returned SAS URL, poll status and retrieve the validation results.
5. Mixed/invalid files	Use files containing valid records, invalid records, s, blank values and malformed content.
6. Repetition and modest volume	Repeat requests and use representative record volumes to understand retry, duplicate and processing behaviour. Keep within published limits.
7. Operational readiness	Test credential replacement, deletion, logging, support evidence and recovery from failed uploads/timeouts.

Suggested edge cases

Area	Examples
Authentication	Missing, malformed, expired/deleted, wrong environment and wrong organisation.
Text values	Blank, whitespace-only, leading/trailing spaces, maximum length, maximum+1, apostrophes, ampersands and Unicode.
Dates	Wrong format, impossible dates, leap day and restricted future/past values.

Identifiers	Malformed identifiers, duplicates, case differences and unknown values.
JSON/schema	Empty body, malformed JSON, wrong type, null versus omitted and additional properties.
Files	Zero-byte, wrong schema/type, corrupted content, no upload after initiation, expired upload URL and representative larger files.
Polling	Unknown uploadId, polling before upload, repeated polling and polling after completion.
Error messages	Status code, message, field/path, correlation identifier and absence of sensitive implementation detail.

Note: we will not be storing any data that is sent via the test endpoints, therefore concurrent invocations or duplicate retry testing cannot be carried out at this stage.

7.1 What the test service is expected to demonstrate

- Requests are authenticated and authorised correctly.
- The same validation rules intended for production are applied by the test endpoints.
- Useful validation/error responses are returned.
- For file tests, status progression and results retrieval can be integrated and monitored.

7.3 What is stored when I use the Test API?

Direct test UPSERT and DELETE

Requests are validated using the same validation rules as the equivalent production endpoint. The submitted policy data is not written into the ELD and goes no further than the test endpoint.

Test file upload

A test file is temporarily stored in the test environment so that asynchronous validation and status reporting can take place. Test-specific processing records and validation results are retained in test-only storage for 8 weeks. No test files are progressed to the ELD policy layer.

8. Common problems and good practice

Symptom	Checks to make before raising a support request
401/403 response	Credential state; environment; authorisation role; insurerId; token/authentication construction; IP allow-list.
429 response	Wait number of seconds specified in response before retrying.
Connection blocked	VPN/egress IP; firewall/proxy; DNS/TLS inspection; correct hostname and environment.
Validation differs from expectation	Latest API version/specification; exact field path; null vs omitted; whitespace; data type; enumeration case.
File upload fails	SAS URL expiry; upload method/headers; file size/type; whether the URL has already been used or modified.
Status does not progress	File actually uploaded; uploadId matches; polling interval; terminal failure details; environment availability.
Credential unexpectedly fails	Expired or deleted state; certificate validity; secret rotation; system clock; test vs production mismatch.
Duplicate outcome uncertain	Check documentation for business-key/idempotency behaviour and retain request/correlation identifiers.

8.1 Evidence to include in a support request

Should you experience any issues during your testing and need to raise a support request with us. Email your request to elto.ishelpdesk@elto.org.uk including the following:

- Organisation and insurerId.
- Environment and endpoint path.
- Timestamp including timezone.
- HTTP method and status code.
- Correlation/request identifier.
- Sanitised request and response.
- UploadId for file flows.
- Credential name only - never private keys, client secrets or full tokens.
- Clear expected-versus-actual result and whether the issue is repeatable.

9. Readiness checklist

☐ Named credential manager and technical owner are confirmed.

☐ Test portal and developer portal access work for the required people.

☐ Network/IP requirements are met.

☐ Test credential is stored securely and renewal/expiry is recorded.

☐ A valid direct request and a valid file upload have completed.

☐ Negative validation and authentication tests have been completed.

☐ Retry, duplicate and polling behaviour is understood by the integration team.

☐ Logging captures timestamp, response status and correlation/request identifier without exposing secrets.

☐ Open questions or defects have been raised.