NLIS
next generation

**FOR L2 & L3 LOCAL AUTHORITIES**

Action required from
local authority IT teams:

# Prepare for Switchover to Next Gen NLIS

In March 2027 all local authorities will switch over from the existing National Land Information Service (NLIS) connection which they've used for the past 25 years, to the new Next Gen NLIS integration.

Funded by
UK Government

**VERSION TWO** - SEPTEMBER 2026

## Why access to Next Gen NLIS is needed

Moving to this new platform from the existing NLIS Hub will ensure local authority local land charges (LLC) teams can continue to receive requests for Official land and property data from conveyancers – a critical part of the home buying and selling process. Next Gen NLIS will bring efficiency to the way Official searches are received, processed and managed by LLC teams.

## How Next Gen NLIS differs from the existing NLIS Hub

Next Gen NLIS is being built on the Land Data Trust Framework which ensures all parties wishing to use the platform are certified and that all data accessed through the platform is trusted, standardised and interoperable.

## Actions required by the end of September

Complete the following three actions before the end of August so your local land charges teams can take part in Next Gen NLIS training and onboarding from September 2026.

1. **Whitelist the following URLs for the Next Gen NLIS live and sandbox environments:**
   - https://app.nlis.org.uk
   - https://app.sandbox.nlis.org.uk

---

2. **Contact relevant back-office software suppliers, asking when they will offer integration testing to Next Gen NLIS.**
   *This only applies if your local authority accesses NLIS through integrated back-office software (level 3) rather than directly through the portal.*

---

3. **Provide administrative consent for your local land charges team to authenticate against the Data Clan Microsoft Entra tenant or Google Cloud Entity Organisation (see next page).**

# Set up the single sign-on for Next Gen NLIS

## To enable Single Sign-On (SSO) with Microsoft 365:

1. An Entra administrator should open the appropriate Admin Consent URL below and approve the application for your organisation:

   **Sandbox:**
   https://login.microsoftonline.com/organizations/adminconsent?client_id=5a531f6e-4fe2-4e20-830d-11330f88266b

   **Production:**
   https://login.microsoftonline.com/organizations/adminconsent?client_id=0e2f2680-06f6-417c-bd7c-72c33f62def6

2. Once consent is granted, theNLIS Enterprise Applicationwill be created automatically in your Entra tenant.
   You can find it in Microsoft Entra admin centre > Enterprise applications > All applications.

## To enable Single Sign-On (SSO) with Google Workspace:

1. If your organisation restricts third-party applications, a Google Workspace administrator should open the Google Admin console and navigate to Security → Access and data control → API controls → Manage App Access.

2. Select Add app, search using the appropriate OAuth client ID below, and select the application:

   **Sandbox:**
   862530188893-l85fqluub7f8k9vq5qquofa85fheldrj.apps.googleusercontent.com

   **Production:**
   862530188893-j9djhdsthi6tlft7objr90na8pasfift.apps.googleusercontent.com

3. Enable access for the relevant organisational units. Select Specific Google data and allow the basic sign-in permissions: openid, profile and email.

   Admin approval may not be necessary if your organisation already permits basic Sign in with Google. These steps follow Google's app access guidance.

# FAQS

The following are the typical questions and answers requested when setting up OAuth2 single sign-on via Microsoft.

## APPLICATION IDENTITY & VERIFICATION

**Application (Client) ID:** 0e2f2680-06f6-417c-bd7c-72c33f62def6

**Publisher Status:** Is the application a "Microsoft Verified Publisher"?

Yes – Data Clan is a Microsoft Verified Publisher

**Tenant Type:** Is this a multi-tenant application hosted by your organisation, or does it require a single-tenant deployment? This supports any Entra ID Tenant (aka 'multi-tenant').

## SCOPES AND PERMISSIONS (LEAST PRIVILEGE)

**Required Permissions:** Provide a complete list of the OAuth 2.0 Scopes (Graph API permissions) requested (e.g., User.Read, Directory.Read.All, Files.Read.All).

**email**

**profile**

**User.Read**

**Consent Level:** Can the application function using User Consent for specific resources, or is Tenant-Wide Admin Consent strictly required? User level consent is allowed – this is a decision based on your local authority's administrative policies.

## DATA GOVERNANCE & RESIDENCY

**Data Flow:** Does the application egress data from our tenant to your infrastructure? If so, please provide a high-level Data Flow Diagram. No – the only needs are for user authentication.

**Encryption:** Confirm that data is encrypted both in transit (TLS 1.2+) and at rest (AES-256). Confirmed.

**Compliance Audits:** Please share your most recent SOC2 Type II or ISO 27001 summary report or Bridge Letter.

Please refer to the Cyferd ISO 27001 certification ↗ and Cyferd ISO 9001 certification ↗.

## IDENTITY SECURITY

**Secret Management:** How are the application's credentials/certificates managed and rotated? Keys are rotated annually.

**Logging:** Does the application support sending activity logs to a SIEM (e.g., Azure Sentinel) via an API? No.

NLIS
next generation

# Need help?

If you have any questions about the information in this guide, please get in touch.

nlis@land-data.org.uk