nexl
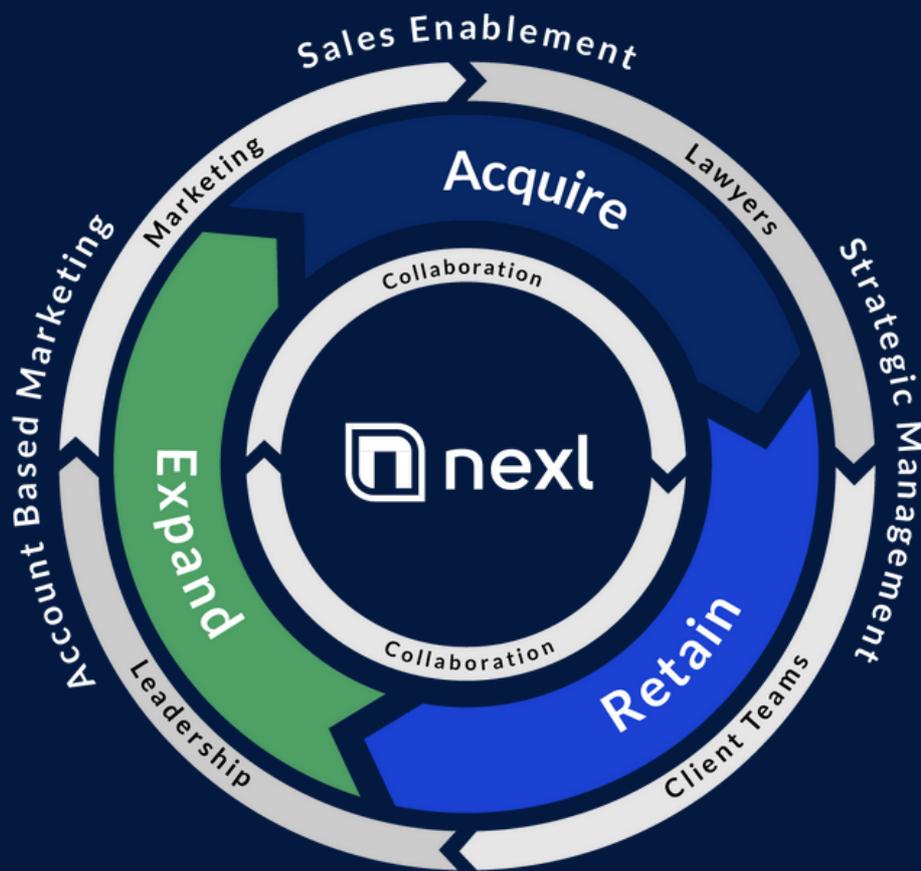
Technical Documentation

Security. Integration, and Implementation Information for Google Workspace
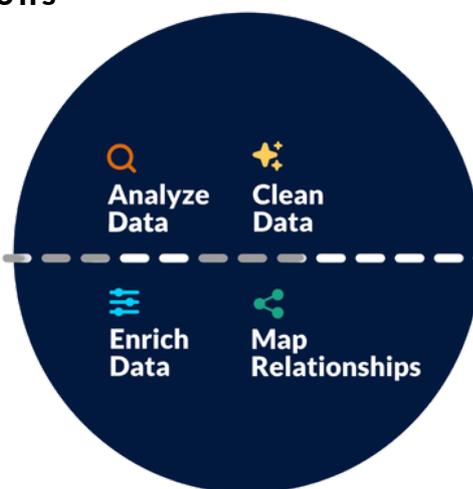
Table of Contents

Introduction

Nexl's products and services are transforming the way law firms grow, but the backbone of our success is providing a safe and trustworthy place for relationship and contact data. Protecting your and your clients' data is at the core of everything we do, from how we build our products to how we serve our clients. This security-centric approach is one of the many ways we've distinguished Nexl as truly purpose-built for law firms, allowing us to help thousands of lawyers around the globe to better manage their relationships.

How Nexl Works

The core value Nexl provides is to deliver automated systems to track relationship information to save valuable time for you and your lawyers. We achieve this by integrating with your email system, which then informs Nexl of sent and received emails and calendar events. We then use advanced data enrichment to map your firm's relationships and add additional information about your contacts, such as job title, industry, location, and more.

But it's not just our automatic data-capture that sets Nexl apart—it's also the type of data we do (and don't) capture. Our systems only receive header information from your email servers—which means we only process the To, From, Cc, and timestamp. Nexl **does not** access or process the email's subject, body content, or attachments. This ensures no confidential, privileged, or sensitive matter-specific information is exposed.

Capture Interactions

Actionable Insights

Analyze Data

Clean Data

Enrich Data

Map Relationships

Align Your Firm

Empower Business Development

Grow Your Revenue

Data Enrichment

Using a stateless API, Nexl enriches your data through our own data systems, as well as third-party data providers. With solely an email address, Nexl is able to search for, find, and populate the following attributes:

Companies

Name	Website	
Description	Email	
Logo	Phone Number	
Employee Count	Address	
Year Founded	LinkedIn URL	
Industry	Twitter URL	
Category	Other profiles	
Keywords		

Contacts

Name	Employer
Age	Job Title
Location	Website
Gender	LinkedIn URL
Education	LinkedIn Bio
Degree	Twitter Username
Photo	Twitter URL

Your contacts are fully owned by you. Nexl's data enrichment is a one-way flow in which you receive data from our data enrichment service, but the data enrichment service cannot access data from users (you).

At no point does Nexl use any of your contact information to enrich other organizations' contacts. Each Nexl tenant's data is stored separately, and we keep strict data guards to ensure no data is shared between tenants.

Tenant A

Tenant B

**Nexl
Data Enrichment**

Tenant C
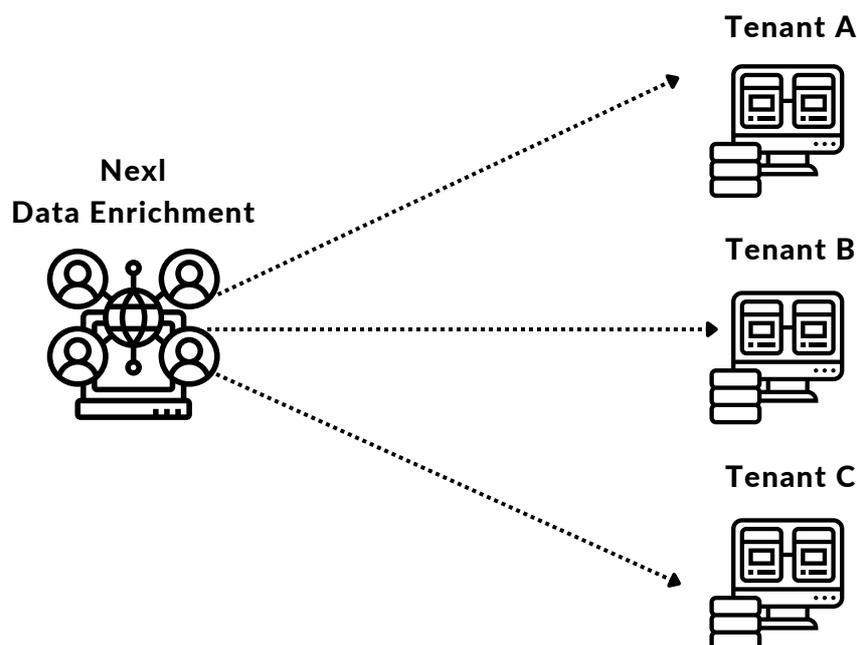
Integration

Nexl integrates with Office 365 and Google Workspace (formerly G Suite), and can also be integrated in a Hybrid Exchange environment. The following sections will review how the **Google Workspace** integration works, as well as the respective steps for setup.

How the Google Workspace Integration Works

Nexl connects with your Google Workspace using Google APIs. Before Nexl can access data using a Google API, it must obtain an access token that grants access to that API.

To integrate your Google Workspace with Nexl, a super-admin of your firm's Google account must grant Nexl the domain-wide delegate authorization required to access information from Gmail. Once permission is granted, the Google Authorization Server sends Nexl an access token and the scope of access granted by that token. After the access token is obtained, Nexl sends the token to a Google API in an HTTP Authorization request header.

The scope of the permission allows Nexl's system to identify your internal users using their profile information in your directory, and to subscribe to change notifications to their mailboxes and calendars. Please note, at all times, Nexl requests read-only permissions to any of your services. Access to email is also limited to Gmail metadata, which prevents Nexl from accessing anything beyond the labels and header information.

You will always have full control over the connection between your Google Workspace tenant and Nexl. You can pause or terminate the connection at any time via Google Admin, without needing to speak to anyone at Nexl.
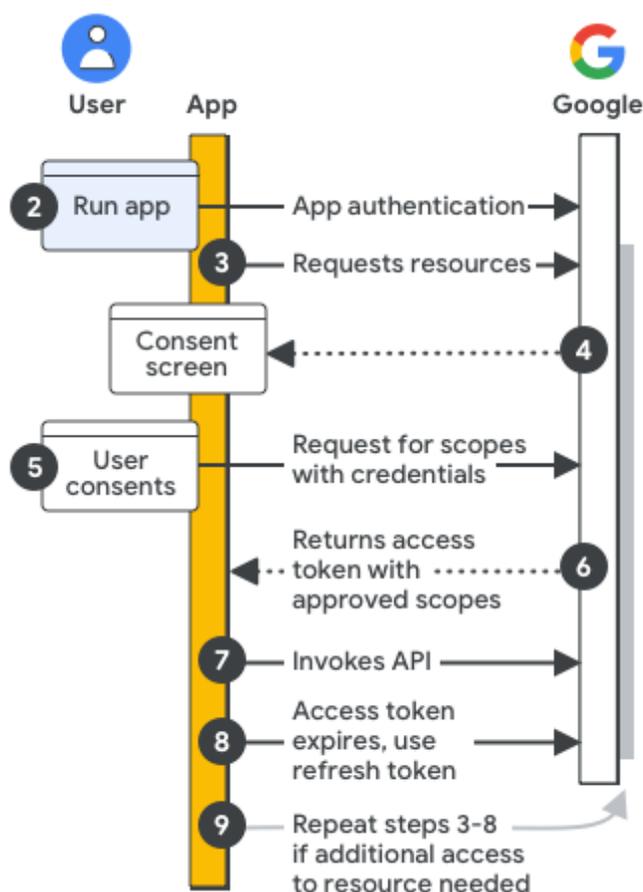
Authentication & Authorization

Since Nexl requires access to secured Google Workspace services, an authentication process is required to show Google Workspace that Nexl has rights to access it. Google APIs use the OAuth 2.0 protocol for authentication and authorization.

An administrator of your firm's Google Workspace account must explicitly grant consent to allow Nexl to access your data using domain-wide delegation. Domain-wide delegation allows applications to access user data across your firm's Google Workspace environment. For this reason, only super-admins can manage domain-wide delegation, and they must specify each API scope that the app can access.

The consent process requires the super-admin to sign in to Google Admin and grant the access permissions Nexl is requesting. Once set up, Nexl continues to request additional access tokens on an ongoing basis, without the need for further super-admin interaction. The access tokens are then passed to the Google APIs to authenticate and authorize Nexl.

The following diagram provides a high-level overview of the authentication and authorization implementation.
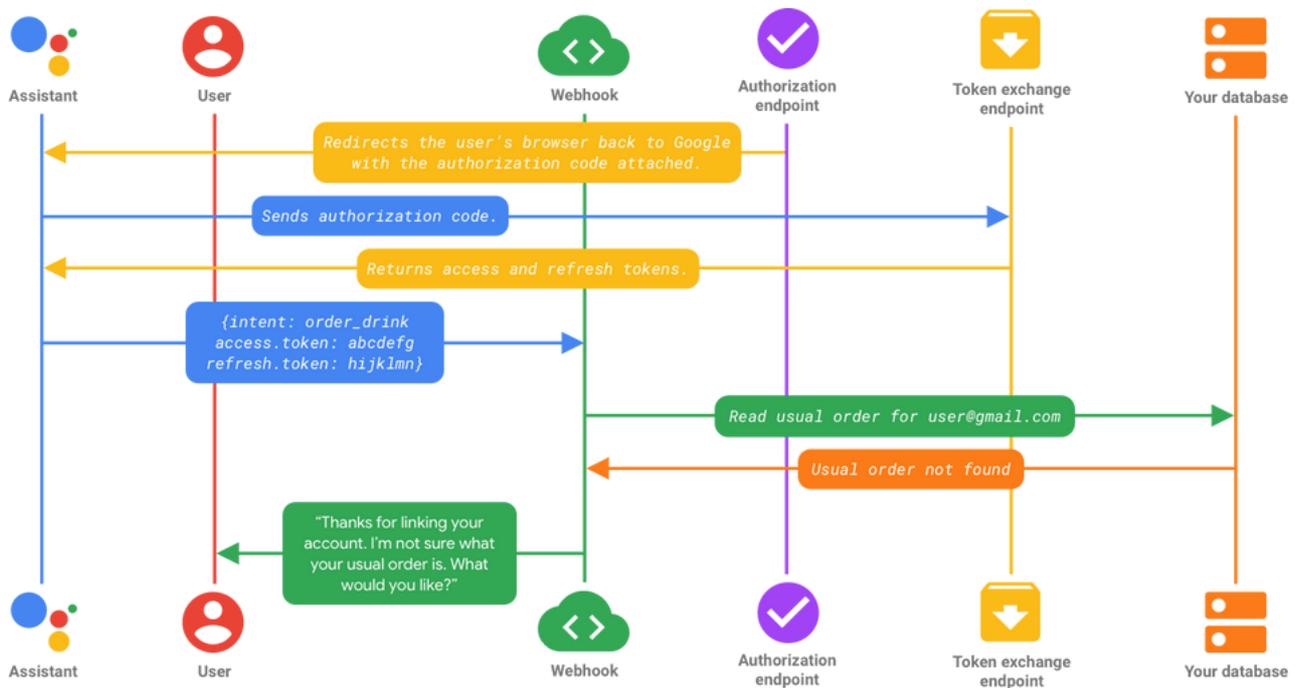
Permissions

For Nexl to access data from Google Workspace, it must have the correct permissions implemented via the authentication and authorization process. This table lists the permissions associated with Nexl's Google Workspace integration.

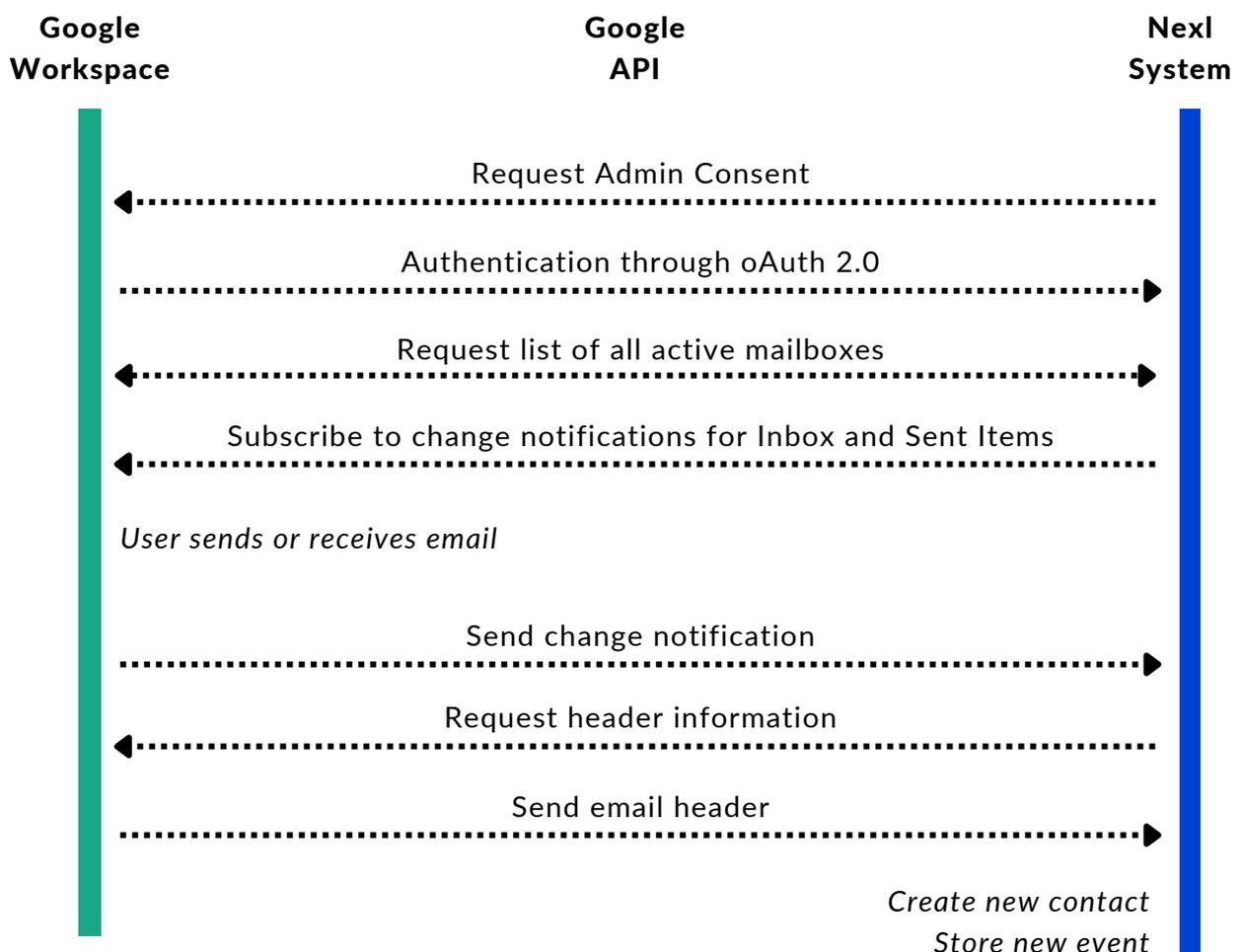| Permission	Scope
userinfo.profile	Allows Nexl to view your users' profile information (name, profile picture, username).
userinfo.email	Allows Nexl to view your users' primary email address.
calendar.events.readonly	Allows Nexl to view events on your users' calendars.
gmail.metadata	Allows Nexl to view email message metadata such as labels and headers, **not** the body or attachments.
admin.directory.user	Allows Nexl to view the provisioning of users on your domain.
admin.directory.group	Allows Nexl to view the provisioning of groups on your domain.

User Authentication

When a user logs into Nexl, they get redirected to Google. The user then enters their username and password, and after a successful authentication, they will be redirected back to Nexl. The diagram below provides a high-level overview of the sign-in authentication flow.

Change Notifications

Once the permissions for your Google Workspace have been granted, Nexl retrieves a list of users and active mailboxes. Once a mailbox becomes active, Nexl uses the Google APIs to subscribe to change notifications on the mailbox's Inbox and Sent Items folders. This allows Nexl to to capture relationship information, as well as sent and received email items.

When there's a change to the subscribed mailbox folder (e.g., a new email is received), a notification is sent to Nexl's system which includes the email's unique identifier. Nexl then requests the email header with the matching ID and creates a new event. Each event includes To, From and Cc email addresses, as well as the date of the event. The diagram below provides an overview of the change notification process.

Google Workspace	Google API	Nexl System
	Request Admin Consent	
	Authentication through oAuth 2.0	
	Request list of all active mailboxes	
	Subscribe to change notifications for Inbox and Sent Items	
User sends or receives email		
	Send change notification	
	Request header information	
	Send email header	
		Create new contact *Store new event*

Information Security

By selecting our platform, you are choosing a cloud platform that is hosted on a fully audited and accredited cloud infrastructure to meet information security standards, including ISO2700, which ensures the controls and processes are in place to protect your data. We have robust security measures including disaster recovery, data backup, and a fully redundant infrastructure to guarantee uptime.

Infrastructure Security

- Hosted on leading infrastructure providers (AWS, Azure)
- Network and Perimiter Protection
- Regional servers (EU, US, AUS)

Customer Data Protection

- Logical Tenant Separation (Private Cloud Available)
- Encryption In Transit (TLS 1.2, TLS 1.3)
- Encryption At Rest (AES-256)

Application Protection

- Web Application Firewall (WAF)
- Distributed Denial of Service (DDoS) Protections
- Regular Penetration Testing and Vulnerability Scanning

Application Protection

- 24/7 Monitoring and Incident Response
- Security Education and Awareness Training

Your Office 365 Tenant

Office 365

Exchange

Email headers sent to Nexl via Microsoft Graph API

Read-only permissions Subjects/bodies not processed

Public Data Enrichment Service

One-way sync of data

nexl

Application Layer

CLOUDFLARE

| Virtual Tenant A | Virtual Tenant B |

Scoping & Data Segregation

Database Layer

Microsoft Azure aws

EU, US or AUS server

Nexl data sent to integrations via Nexl oData API

Power BI

Microsoft Teams

mailchimp

eventogy

ISO 27001

GDPR COMPLIANT

SECURE SSL ENCRYPTION

Information Security

For more details regarding Nexl's information security, as well as links to our Privacy Policy and Data Processing Agreement, please refer to the chart below.

Information Security	Details
Main Cloud Infrastructure	AWS (EU, Australia), Azure (US), Digital Ocean (Canada)
Available Server Locations	EU, Australia, USA, Canada
Encryption	DB and File encryption enabled (transit and rest) All traffic through HTTPS only
Security	24/7 Security monitoring and threat detection though Cloudflare and Rollbar
Email Notification Delivery	SendGrid
Data Backups	Daily backups are retained for 7 days. Weekly backups are retained for 4 weeks.
Data Accessibility	Data can be accessed 30 days after termination with possible extension up to 90 days. Alternatively, Nexl can provide an extract of customer data.
Planned Downtime	All customers will be informed at least 2 weeks before a planned downtime.
Privacy Policy	https://nexl.cloud/privacy-policy/
Data Processing Agreement	https://nexl.cloud/data-processing-agreement/

Setup Guide

Nexl is a purely web-based system, which makes it quick and easy to set up Nexl's Google Workspace integration. Please see below for system requirements and a step-by-step guide to implementation.

System Requirements

Before you begin your integration, please review the following system requirements and confirm that all requirements are met:

- Internet access
- Recent version of Google Chrome, Firefox, Safari, or Edge

***Note:** It is possible to access and use Nexl using Internet Explorer 11 but we do not officially support it.

Implementation
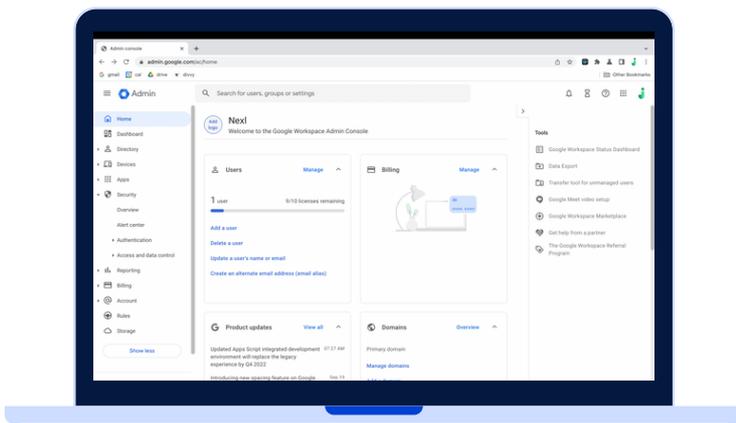
Step 1:
Sign into your Google Admin console

1. Navigate to https://admin.google.com.

2. Log in using your Google credentials. For help signing into your Google Admin account, click here.

Setup Guide
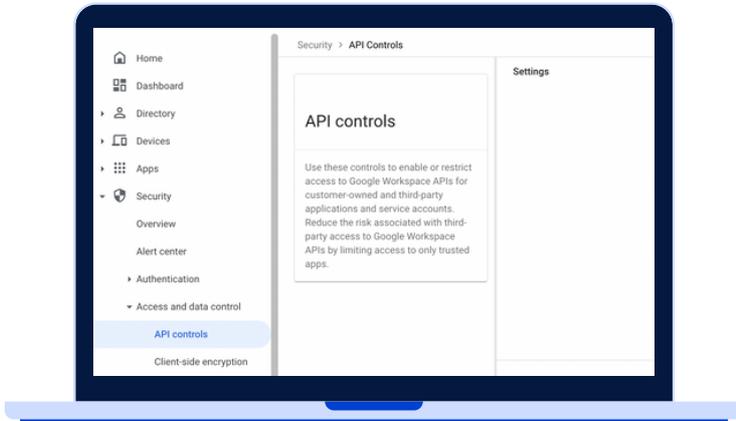
Step 2:
Navigate to API Controls

1. From the lefthand menu, select
   Security > **Access and data control**
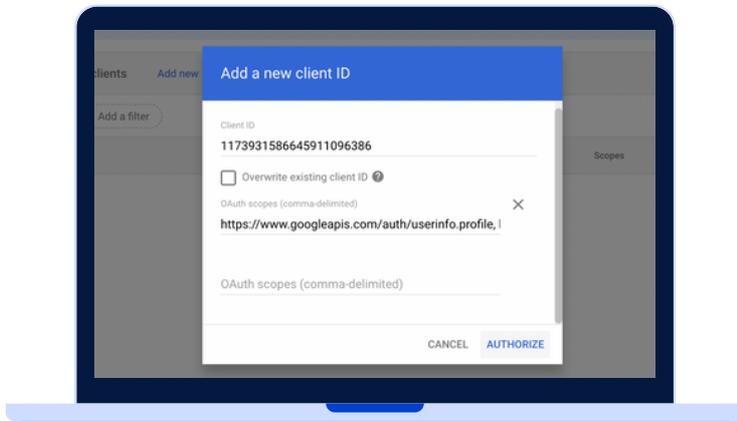   > **API controls.**
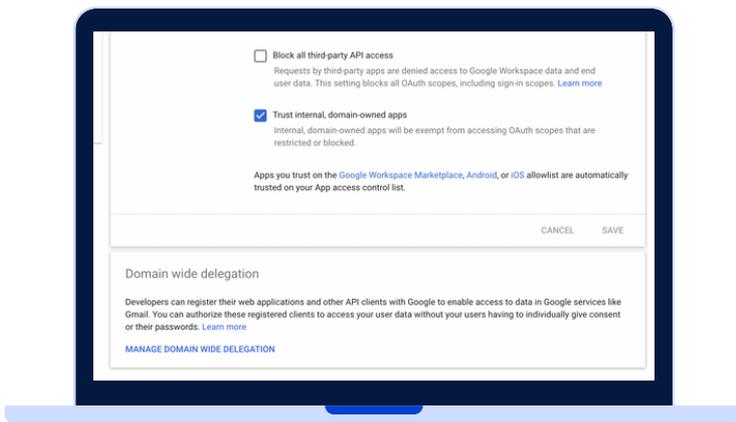
Step 3:
Add a new domain-wide delegation

1. Scroll down to the bottom of the
   page and click '**MANAGE DOMAIN
   WIDE DELEGATION**'.
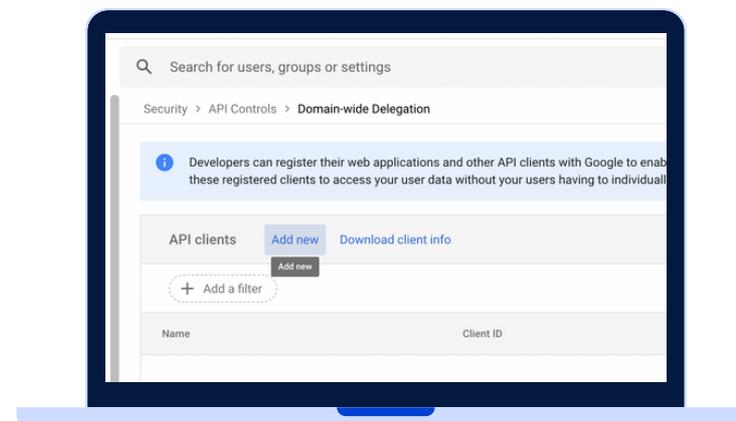
2. From the domain-wide delegation
   page, click '**Add new**'.

Setup Guide

3. Enter Nexl's Client ID:
   117393158664591109638

4. Under OAuth scopes, copy and
   paste the list below. Please
   note that we have already included
   the comma separation.

5. Click '**Authorize**'.

OAuth Scopes:

https://www.googleapis.com/auth/userinfo.profile,
https://www.googleapis.com/auth/userinfo.email,
https://www.googleapis.com/auth/calendar.events.readonly,
https://www.googleapis.com/auth/gmail.metadata,
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/admin.directory.group

If you receive an error, double check that the Client ID and Scopes list are correct.
Please contact Nexl's Client Services team if you continue to receive an error.
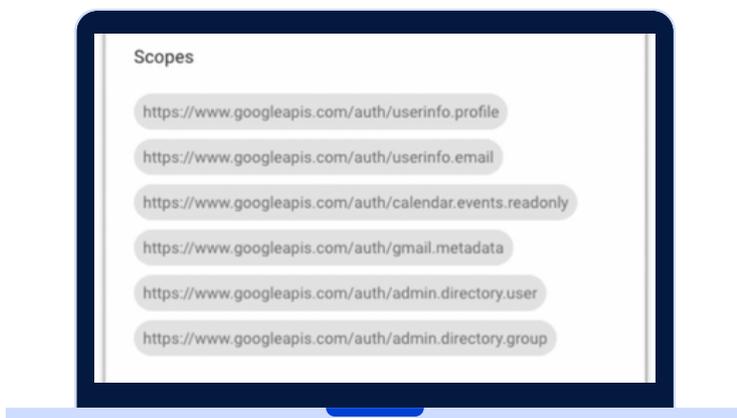
6. Select the new ClientID and click
   'View details' to confirm that all of
   the scopes have been added. If any
   are missing, click 'Edit' to enter
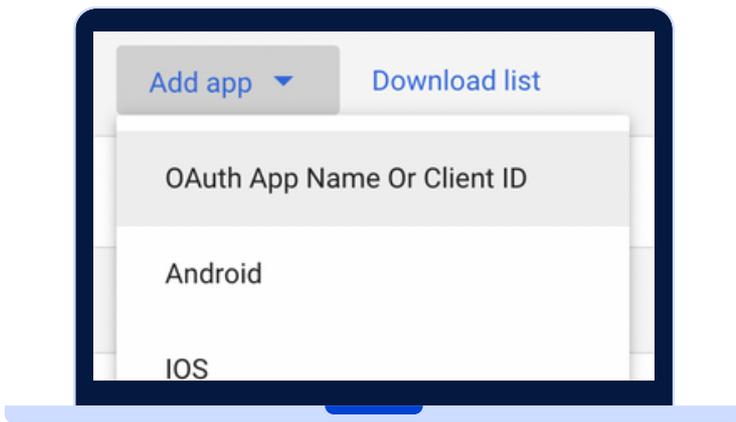   them, and click 'Authorize'.

   Please note that the ClientID
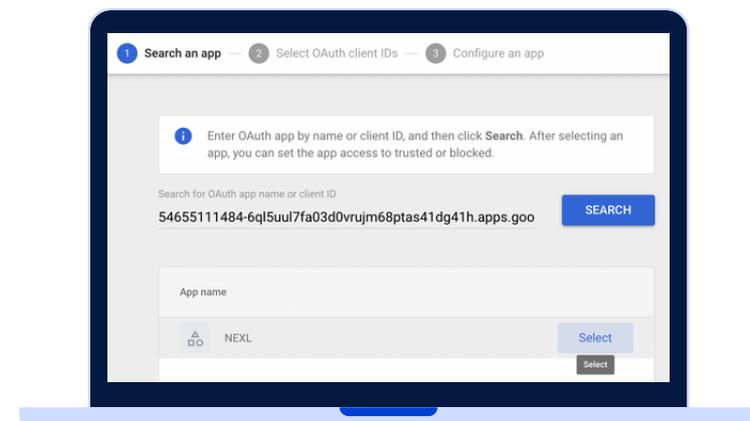   cannot be edited.

Setup Guide
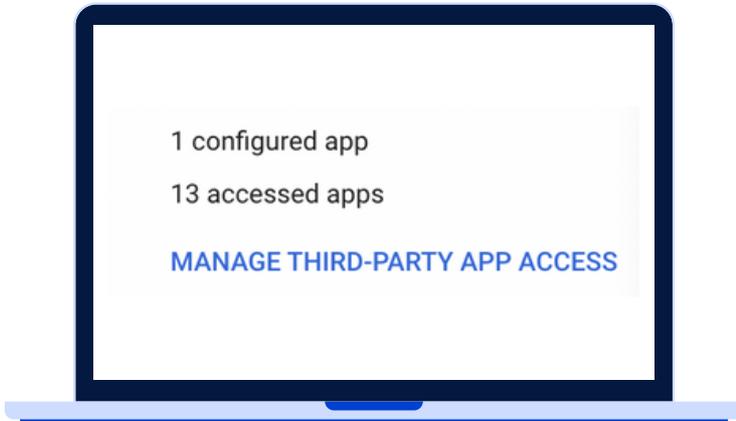
Step 4:
Add Nexl's OAuth application to your trusted API applications.

1. Navigate back to the API Controls page. Under 'App access control', click **'MANAGE THIRD-PARTY APP ACCESS'**.

2. Click the '**Configure new app**' dropdown and select '**OAuth App Name Or Client ID**'.
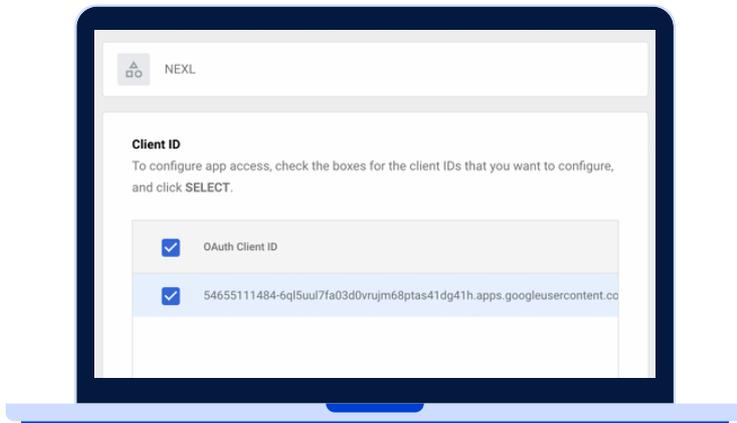

3. Copy and paste the following into the search bar, then click '**SEARCH**':
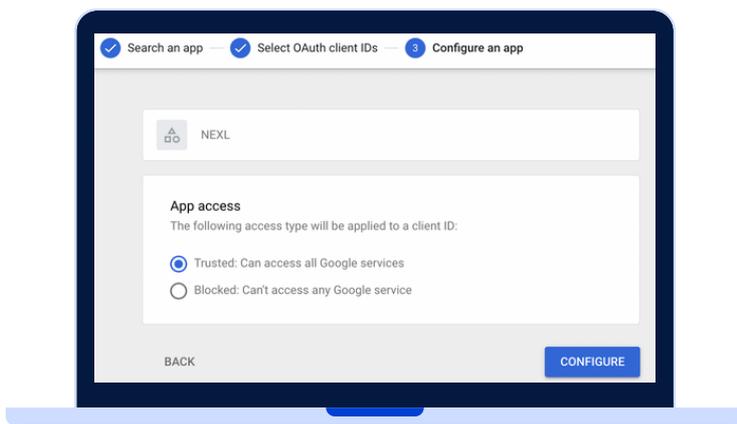
   295841496566-r8punf3raj0odn2p9sk0plfauvpmfs76.apps.googleusercontent.com

4. Hover over the search result '**NEXL**', then click '**Select**'.

Setup Guide

5. Click the checkboxes to ensure both are selected, then click '**SELECT**'.

6. Select '**Trusted**', then click '**CONFIGURE**'.

Training

All of Nexl's training sessions will be held virtually in a webinar-style event for all participating users. Our training sessions focus heavily on specific BD and Marketing strategies to help your lawyers improve their business development efforts. Upon request, sessions can be recorded and made available to you.

For a high-level overview of our training and implementation process, please see the diagram below.

Resources

In addition to our live training events, we also offer a number of 24/7 resources to help you learn and troubleshoot.

Training Videos

We offer a number of self-paced video courses for both beginners and admin users. You can access our training videos at https://nexl.cloud/learn.

Live Chat Support

We offer in-app chat support to answer your questions in real time. You can find our chat support on any page or section within Nexl, in the bottom right corner.

Help Center

Nexl's Help Center is a collection of articles and how-to's that you can easily browse or search.

You can access Nexl's Help Center at https://help.nexl.cloud, as well as via our in-app chat support widget.