From Door to Desktop

Identity Provider Integration in Action (Google)

Derek Brown - Director of IT
Rochester Hills Public Library

IUG Lightning Round • Chicago 2026

Context: RHPL + Polaris Auth

About Rochester Hills Public Library

Hosted Clarivate customer
We don’t manage the server — Innovative’s team does

Polaris 8.0 / LEAP
Running the latest centralized PolarisAuth service

Google Workspace
All staff use @rhpl.org Google accounts with SSO/MFA

Chrome OS Flex
Transitioned workstations to ChromeOS (flex) for secure and ease

Polaris Auth: What Changed in 7.7+

Centralized Auth Service
One PolarisAuth layer for LEAP, Admin, and ExpressCheck

Multiple IdP Support
ADFS, Azure AD / Entra, Google, Okta — even per-branch

OIDC + PKCE
Standards-based, secure token flow — no passwords in transit

Hosted? No problem
Clarivate Innovative team configures appsettings.json for you

Staff may authenticate using assigned YubiKeys or their own authorized secondary devices.

The Door-to-Desktop Journey

01

Physical Entry

YubiKey + OpenPath
Door access control using hardware security key

02

Workstation Login

Chrome OS Flex
Sign into Google Workspace with same YubiKey

03

LEAP Access

Polaris LEAP auto-authenticates via Google OAuth — no extra password

One identity. One credential. Works on-site and remotely.

IUG 2026 CHICAGO

The Staff Experience

Staff see a familiar, simple flow — no separate passwords to remember.

1

Open LEAP

Click the LEAP shortcut.
Polaris login screen appears with a "Sign In" button.

2

Click Sign In

Google's "Choose an account" screen pops up.
Staff select their @rhpl.org account.

3

YubiKey Verifies

If Chrome OS Flex required the key to login, Google already verified it.

4

Select Branch

Polaris prompts Branch + Workstation — same as always.
Then straight to LEAP.

Google Cloud Console: Setup Steps

The Google-side work — done once, in Google Cloud Console

Step 1 Create / Select a Project

In console.cloud.google.com, create or select your library's GCP project. RHPL used the rhpl.org organization with a dedicated "LEAP Production Connection" project.

Step 2 Enable OAuth Consent Screen

APIs & Services → OAuth consent screen. Set app type to Internal (limits to your Google Workspace domain). Fill in app name, support email, and authorized domain (rhpl.org).

Step 3 Create OAuth 2.0 Client ID

APIs & Services → Credentials → Create Credentials → OAuth Client ID. Choose "Web application". Name it (e.g., "LEAP Integration"). Copy the Client ID and Client Secret — you'll give these to Clarivate.

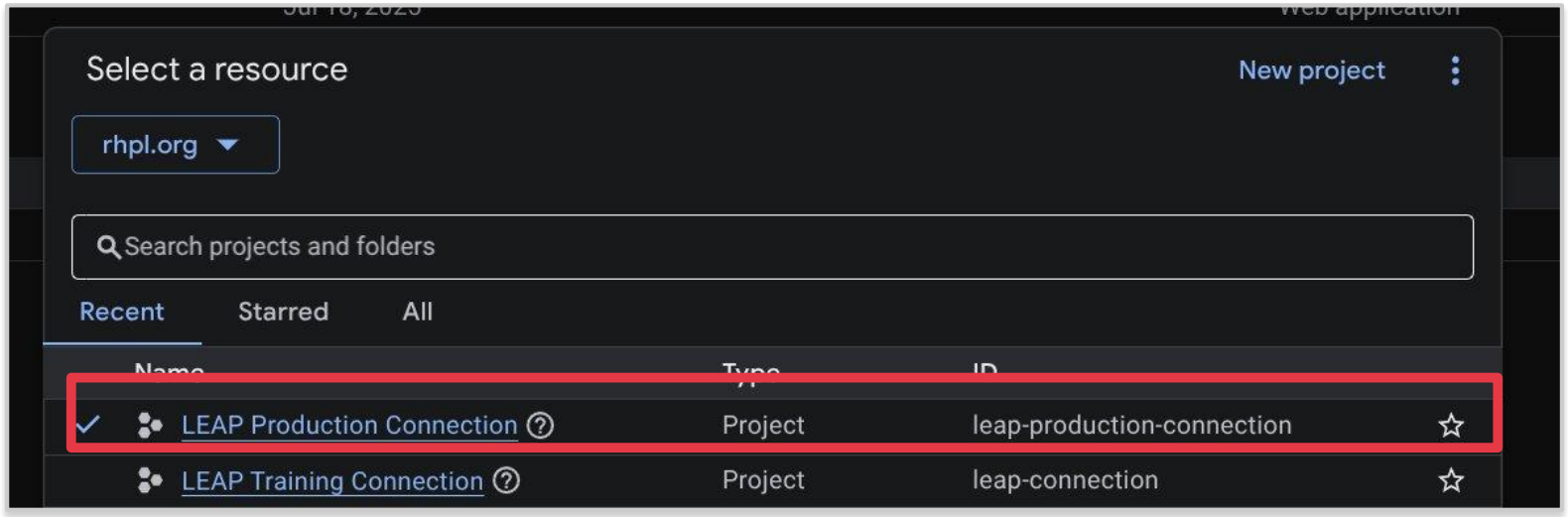
Step 4 Add Authorized Redirect URIs

Add these URIs to the OAuth client:

- https://[your-server]/polarisauth/signin-oidc
- https://[your-server]/polarisauth/login
- https://[your-server]/polarisauth/logout
- https://[your-server]/polarisauth/signout-callback-oidc

Google Cloud Console — Steps 1 & 2 of 4

STEP 1 Create / Select a GCP Project



▶ Use your Google Workspace org (rhpl.org), not a personal account. Create a dedicated project for LEAP.

✔ RHPL uses: "LEAP Production Connection" & "LEAP Training Connection" — keep Training and Production as separate projects.

STEP 2 Configure the OAuth Consent Screen

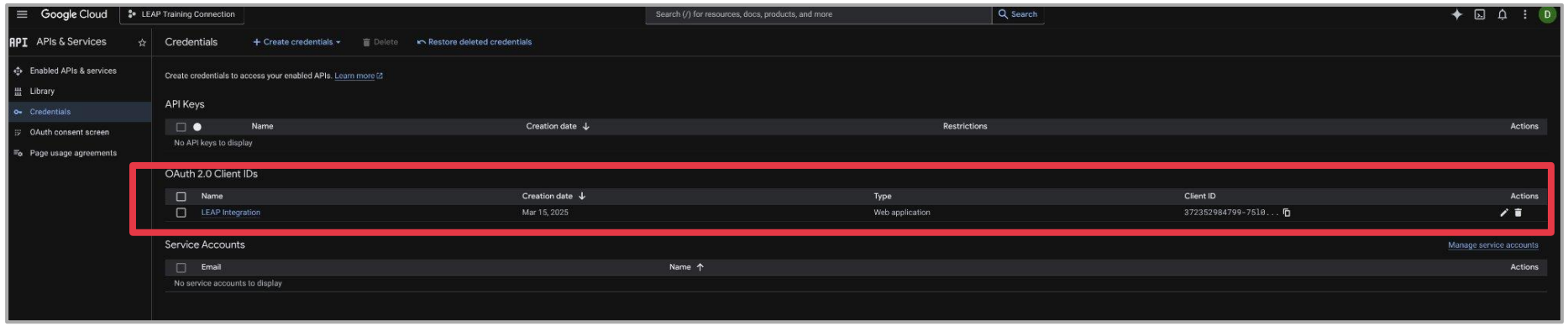
`console.cloud.google.com → APIs & Services → OAuth consent screen → User Type: Internal → App name + support email + authorized domain`

✔ **User Type: Internal** Restricts auth to your Workspace org only — personal Gmail accounts cannot sign in

✔ **Authorized Domain = rhpl.org** Required so the consent screen binds to your domain; Clarivate will need this value

Google Cloud Console — Steps 3 & 4 of 4

STEP 3 Create OAuth 2.0 Client ID



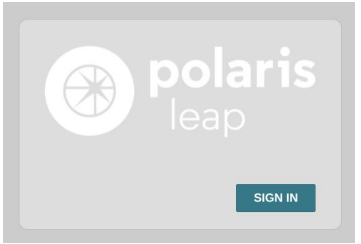
APIs & Services → Credentials → Create Credentials → OAuth Client ID → Web application

❗ Copy Client ID + Secret immediately — only shown once. Give both to Clarivate Innovative team.

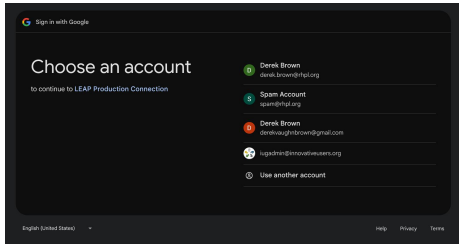
STEP 4 Add Authorized Redirect URIs

```
Authorized Redirect URIs (add all four):
https://[your-server]/polarisauth/signin-oidc
https://[your-server]/polarisauth/login
https://[your-server]/polarisauth/logout
https://[your-server]/polarisauth/signout-callback-oidc
```

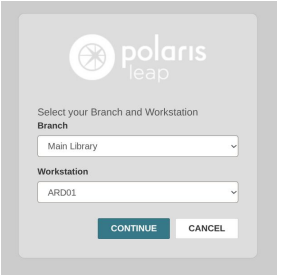
What staff see after setup:



1. LEAP Login



2. Pick Account



3. Branch & WS

Quick demonstration video of leveraging our physical security with our OAUTH security at RHPL.

IUG 2026 CHICAGO

The Polaris Side: What Clarivate Configures

As a hosted customer, you provide the credentials — Clarivate's Innovative team does the rest!

Key Google OAuth settings in appsettings.json

```
"OAuth": {
  "Enabled": true,  "ForceIDPLogin": true,
  "ForceIDPLogout": false,  "Name": "Google IAM",
  "SupportedDomains": [ "rhpl.org" ],
  "MetaAddress": "https://accounts.google.com/
    .well-known/openid-configuration",
  "ClientId": "[YOUR-CLIENT-ID]",
  "AlternateUpnClaimType": "preferred_username"
}
```

Key decisions to highlight

`ForceIDPLogin: true` Always prompt Google sign-in screen, preventing shared sessions

`ForceIDPLogout: false` Google doesn't truly end sessions via logout URI — leave false

`SupportedDomains` Lock to rhpl.org only — prevents personal Gmail accounts

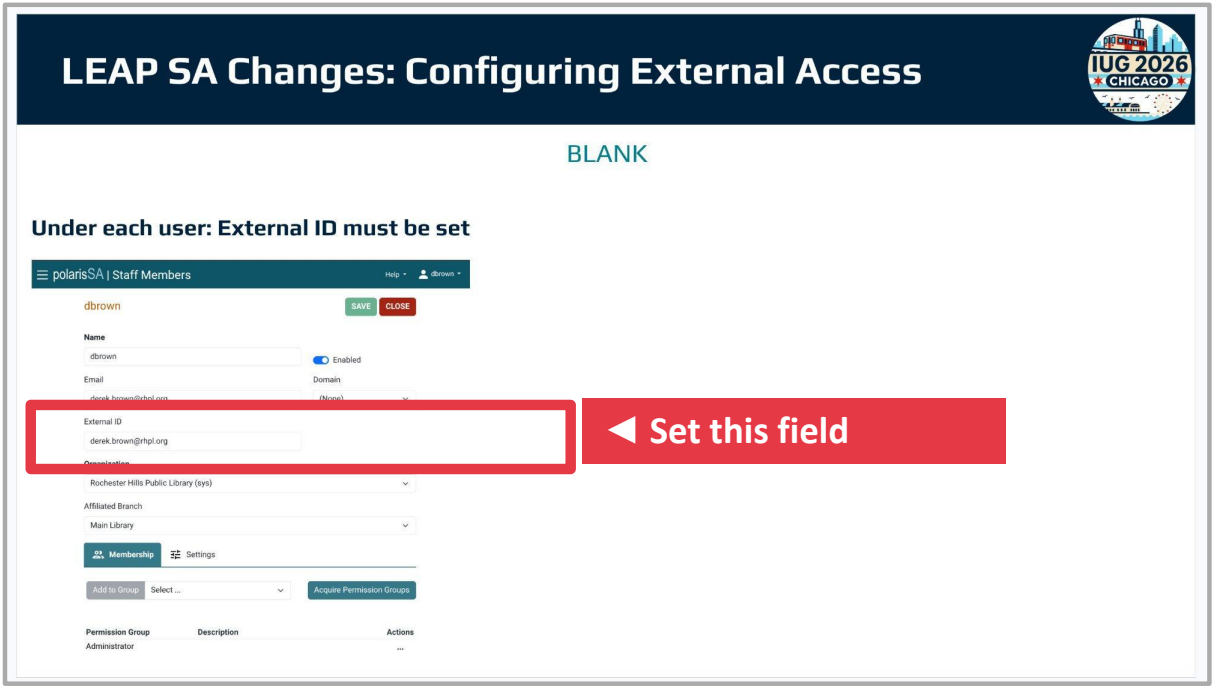
`AlternateUpnClaimType` Use preferred_username to map Google email to Polaris UPN

`UseOidc: true + PKCE` Full OIDC flow with PKCE — most secure Google integration

LEAP SA Changes: Configuring External Access

Where to find this in Polaris SA:

`Polaris SA → Staff Members → [username] → External ID`



What you need to know:

How Polaris matches a Google login to a user

Google JWT → `preferred_username` → External ID

Must be their exact Google Workspace email: `firstname.lastname@rhpl.org`

❗ If External ID is missing or wrong:

"User is not a valid Polaris user."

Staff see this on every login. Field is case-sensitive — match exactly as Google returns it.

⚠️ Plan ahead — no bulk update option

One user at a time in Polaris SA. Complete **all staff** before Clarivate enables OAuth — or those users are locked out on day one.

ℹ Domain field (None) ≠ SupportedDomains in config

The SA Domain field does not control OAuth access. Leave it as-is.

`SupportedDomains` in the PolarisAuth config is what restricts logins to rhpl.org.

What We Learned: Tips & Gotchas

✔ Open a Supportal ticket early

As a hosted customer, start by contacting Clarivate. They need the Client ID, Client Secret, and your redirect URIs. The ticket can take 1–2 weeks to fully configure.

✔ ForceIDPLogout = false for Google

Google's logout URI only revokes tokens, it doesn't end the session. Leaving this false prevents broken logout errors while keeping Polaris logout clean.

⬆️ Staff may see multiple Google accounts

If staff have personal Gmail logged in the same browser/profile, they'll see it in the account picker. Enforce Workspace profile separation using Chrome OS Flex managed profiles.

⚡ YubiKey doubles as LEAP auth

When staff authenticate to Chrome OS Flex with a YubiKey, Google already validated them. LEAP inherits that session — no second factor needed for LEAP itself.

⚡ Remote access works identically

Staff working from home use the same LEAP URL. Google redirects, they pick their @rhpl.org account, verify if needed, and land in LEAP — from any device.

💡 On the horizon: passwordless

Chrome OS Flex + YubiKey + Google Workspace = no typed passwords at all. We're exploring WebAuthn passkeys as the next step in the journey.

Questions?

Derek Brown
Director of IT | Rochester Hills Public Library
derek.brown@rhpl.org

Resources & References

- Polaris Authentication Integration Guide 8.0 (Clarivate)
- Google Cloud Console: console.cloud.google.com
- RHPL also demoed: OpenPath + YubiKey + Chrome OS Flex
- Innovative also supports: Azure AD / Entra, ADFS, Okta, and more