Configure OpenID Connect SSO

Last modified on 11/05/2026 11:22 pm EST

Using ClassLink?

If you'd rather not register an app, use KnowledgeOwl's ClassLink app. If your district already has its own app in ClassLink, refer to Configure ClassLink SSO with your district's own app.

These instructions walk you through connecting your own identity provider (IdP) app to KnowledgeOwl with OpenID Connect (OIDC). They work for any provider: Auth0, ClassLink, Clever, Google Workspace, JumpCloud, Keycloak, Microsoft Entra ID, Okta, OneLogin, PingOne, or any other identity provider that supports OpenID Connect. This feature is available on select plans.

New to OpenID Connect? Start with OpenID Connect (OIDC) SSO overview.

Authors with the default **Editor** role, or a custom role with the **Security and access** permission **Update security settings**, can set up OpenID Connect.

You'll need someone who can create an app in your identity provider. The setup has seven steps, all in **Security and access > Access & SSO > OpenID Connect (OIDC)**. Steps don't block each other, but you'll need to pass a test login in step 6 before you can turn OpenID Connect on in step 7.

Step 1: Choose your identity provider

1. Go to **Security and access > Access & SSO**.
2. In the **Login methods** card, select **Set up** (or **Manage**) on the **OpenID Connect (OIDC)** row.
3. In **Choose your identity provider**, select your provider's tile. If your provider isn't listed, select **Other / manual**.

KnowledgeOwl fills in what it knows for that provider, like its issuer, scopes, and the claim names it usually sends, and the remaining steps appear. Nothing is saved until you select **Save changes**.

To pick a different provider later, select **Change provider**. If you've already entered settings, you're asked to confirm, because switching clears the current issuer, client ID, login restrictions, and reader attribute mapping.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

Step 2: Register KnowledgeOwl with your identity provider

In your identity provider, create an OpenID Connect web app for your knowledge base. Then copy these details from KnowledgeOwl into it:

1. Copy the **Redirect URI** and add it exactly as shown to the allowed redirect URIs of your app. It looks like `https://<your knowledge base domain>/reader-sso/oauth2/callback`.
2. *Optional:* If your identity provider has an app launcher or dashboard, copy the **Login link (optional)** and use it as the app's login URL. It looks like `https://<your knowledge base domain>/reader-sso/oauth2/login`.
3. Assign the app to the people who should be able to read your knowledge base.

Register KnowledgeOwl with your identity provider



Custom domains and proxies

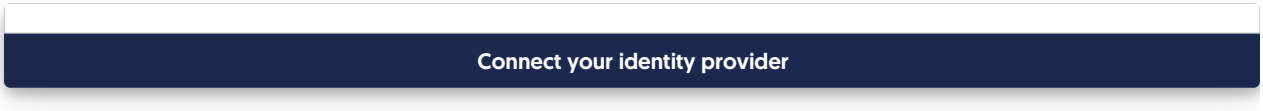
OpenID Connect logins use your knowledge base's custom domain, if it has one, so use the redirect URI exactly as KnowledgeOwl shows it. If you serve your knowledge base through a reverse proxy that only passes certain paths, add `/reader-sso` to the paths it passes.

Step 3: Connect your identity provider

Now enter your identity provider app's details in KnowledgeOwl:

1. Read the **Setting up {provider}** notes at the top of the step, if your provider has any. They're also in the table below.
2. Enter the fields your provider needs to build the issuer URL, like your **Okta domain** or **Directory (tenant) ID**. KnowledgeOwl builds the **Issuer URL** from them.
    - To enter the issuer yourself, select **Use a different issuer URL**. It must match the issuer in your identity provider's discovery document exactly.
    - If you chose **Other / manual**, enter the **Issuer URL**, like `https://idp.example.com`.
3. Enter the **Client ID** from your identity provider app.
4. Enter the **Client secret**. Once saved, it's encrypted and can't be shown again. To change it later, select **Replace**.
5. Select **Save changes**.
6. Select **Test connection**. When it works, you'll see **Connected to your identity provider**, along with the endpoints and signing keys KnowledgeOwl found.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.



If the test fails, check the message, fix the setting, save, and try again. Refer to Troubleshoot OpenID Connect logins for what each message means.

Provider notes

Provider	Fields you enter	Notes
Auth0	**Auth0 domain**	• Keep the slash at the end of the issuer. Auth0 needs it. • Using a custom domain? Enter it instead of your auth0.com domain.
ClassLink	None. The issuer is filled in for you.	• ClassLink logs in users from every district, so we prefill a login restriction on your ClassLink tenant ID. Enter your tenant ID in step 4. For the full walkthrough, refer to Configure ClassLink SSO with your district's own app.
Clever	None. The issuer is filled in for you.	• Ask Clever Support to turn on OpenID Connect for your Clever app first. • Clever logs in users from every district, so we prefill a login restriction on your district ID. Enter it in step 4, then do a test login to check the claim name (Clever's docs use both district and district_id).
Google Workspace	**Your Google Workspace domain**, like `school.org`	• Any Google account can use a Google app, so we prefill a login restriction on your Workspace domain. • Google doesn't send groups over OpenID Connect. Use SAML if you need them.
JumpCloud	**JumpCloud OIDC host** (default `oauth.id.jumpcloud.com`)	• EU and India organizations: use oauth.id.eu.jumpcloud.com or oauth.id.in.jumpcloud.com. • You name the groups claim in JumpCloud, so if you send groups, add the Reader groups field yourself.
Keycloak	**Keycloak host, Realm**	• On Keycloak versions before 17, add /auth before /realms in the issuer. • In Keycloak, add a group membership mapper to the client. Keycloak doesn't send groups otherwise.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

Provider	Fields you enter	Notes
Microsoft Entra ID (Azure AD)	**Directory (tenant) ID**	• Enter your directory (tenant) ID, not "common" or "organizations". • In your Entra app registration, add the email, given_name and family_name optional claims. Entra doesn't send them otherwise. • Entra sends groups as IDs, not names, so assign reader groups with custom map rules instead.
Okta	**Okta domain**, **Authorization server ID** (default `default`)	• Using Okta's org authorization server? Change the issuer to just your Okta domain, for example https://yourcompany.okta.com. • In Okta, add a groups claim filter to your app (for example the regex .*). Okta doesn't send groups otherwise. • Okta sends names and groups through its userinfo endpoint, so we turn on "Also read claims from the userinfo endpoint" for you.
OneLogin	**OneLogin subdomain**	No extra notes.
PingOne	**PingOne auth host**, **Environment ID**	• Your host depends on your region (for example auth.pingone.eu), or is your custom domain.
Other / manual	**Issuer URL**	Choose the **Protocol: OpenID Connect (recommended)** or **OAuth 2.0 (no ID token)**. Refer to Use OAuth 2.0 mode.

Step 4: Restrict who can log in

By default, anyone who can log in to your identity provider can read your knowledge base. Use this step to limit logins to readers with certain claim values.



Required for ClassLink, Clever, and Google Workspace

These providers log in users from every organization that uses them. KnowledgeOwl prefills a restriction for your organization: enter your own value, like your tenant ID, district ID, or Workspace domain. Without it, you can't turn OpenID Connect on and logins are blocked.

To add a restriction:

1. Select **Add restriction**.
2. Enter the **Claim** name, like `groups` or `hd`.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

3. In **Match**, choose **Is one of** or **Matches regex**.

4. Enter the **Allowed values**. Separate several values with commas: a reader who matches any one of them passes.

5. Select **Save changes**.

Readers must match every restriction. To allow several values for the same claim, like more than one tenant, put them all in one row instead of adding a second row for that claim.

Step 5: Map reader attributes

For each reader field, enter the claim name your identity provider sends. KnowledgeOwl prefills the usual claim names for the provider you chose.

- **SSO ID**: Leave blank to use the standard `sub` claim, which is unique for each user at your identity provider. To combine claims, put each in braces, like `{tenant_id}:{user_id}`. For ClassLink, Clever, Google Workspace, and Microsoft Entra ID, the SSO ID is locked so each user is matched to a single reader.
- **Username / email**, **First name**, **Last name**: Usually `email`, `given_name`, and `family_name`.
- To map more fields, like **Reader groups**, **Reader icon**, or a custom field, select **Add field**. Reader group names must match your reader groups exactly.
- For a claim inside another claim, use dots, like `tenant.id`.

After the first login, each field shows its value from the last login, and the arrow at the right end of each field lists the claims your identity provider sent, so you can pick one instead of typing it. That's a quick way to check your mapping after the test login in step 6.

To set reader fields based on claim values, for example to put readers whose department is `faculty` in a Teachers reader group, select **Set reader fields with rules**. Rules work the same way as for SAML: refer to Custom attribute map rules. With OpenID Connect, if a field is also mapped to a claim, the rule only applies when a login doesn't include that claim. Rules save as soon as you create, edit, or delete them.

Select **Save changes** when you're done.

Step 6: Test login

Run a test login to check the whole connection. You log in as yourself, and you won't be logged in to the knowledge base.

1. Make sure you've saved your changes. **Run a test login** is available once step 3 has an issuer, client ID, and client secret, and **Test connection** should work first.

2. Select **Run a test login**. A new window opens to your identity provider.

3. Log in. When you see **Test login finished**, you can close that window.

4. Back in KnowledgeOwl, check the result under **Recent logins**. Select **Show claims** to see exactly what your

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

identity provider sent.

A test login still passes if you don't match your own login restrictions. You'll see a note that you don't match them yourself.



Run the test again after changes

If you change the issuer, client ID, or SSO ID mapping after a test, and OpenID Connect isn't on yet, you'll see **Your settings changed since the last test login. Run it again before turning OpenID Connect on.**

If the test fails, refer to Troubleshoot OpenID Connect logins.

Step 7: Turn on OpenID Connect

Once your test login passes, choose how readers use OpenID Connect:

1. In **Turn on OpenID Connect**, choose one:
    - **Off**: Readers can't use this method.
    - **Available**: Readers can log in with the login link or from your identity provider. Restricted content on a public knowledge base can send them here too.
    - **Required for all readers**: Anyone who isn't logged in is sent straight to your identity provider.
2. Select **Save changes**.

If **Available** and **Required for all readers** can't be selected, a message explains what's missing, like finishing step 3 or passing a test login in step 6.

Some things to know:

- If SAML is also Required, SAML takes priority and readers who aren't logged in are sent there. Readers can still use the OpenID Connect login link from step 2.
- When OpenID Connect is Required, the reader login page sends readers to your identity provider. To let readers still use a username and password, go to **Access & SSO > Direct login** and select **Allow direct log ins while OpenID Connect is required**.
- When OpenID Connect is Available, you can send readers who aren't logged in to it by choosing **OpenID Connect login** under **Send readers who aren't logged in to** on the **Access & SSO** overview.

Advanced options

Most identity providers don't need these. Expand **Advanced options** below the steps to change them:

- **Client authentication**: How KnowledgeOwl sends the client secret: **HTTP Basic (client_secret_basic)** or **Form post (client_secret_post)**.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

- **Scopes:** The scopes KnowledgeOwl asks for, like `openid profile email`.
- **Also read claims from the userinfo endpoint:** Leave off unless your identity provider only sends some claims through userinfo. Picking Okta as your identity provider turns this on.
- **Also log readers out of your identity provider when they log out:** Only works if your identity provider has a logout endpoint. **Test connection** in step 3 shows whether it does.

Use OAuth 2.0 mode

If your identity provider supports OAuth 2.0 but doesn't issue ID tokens, choose **Other / manual** in step 1, then choose **OAuth 2.0 (no ID token)** as the **Protocol** in step 3. Then enter:

- **Issuer identifier:** A unique name for this identity provider. Reader accounts are tied to it.
- **Client ID** and **Client secret**
- **Authorization endpoint**, **Token endpoint**, and **Userinfo endpoint**
- **Logout endpoint (optional)**

All endpoints must be https URLs.



Less secure

In OAuth 2.0 mode, readers are identified by the userinfo response instead of a signed ID token. Only use it for identity providers that don't issue ID tokens.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.