OpenID Connect (OIDC) SSO overview

Last modified on 11/05/2026 9:23 pm EST

OpenID Connect (OIDC) is a single sign-on (SSO) login method that lets readers log in to your knowledge base with an account they already have, such as their ClassLink, Microsoft Entra ID, Okta, or Google Workspace account. This feature is available on select plans.

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

What is OpenID Connect?

OpenID Connect is a standard way for an identity provider (IdP) to tell another app who someone is. When a reader logs in with OpenID Connect:

1. KnowledgeOwl sends the reader to your identity provider.
2. The reader logs in there, the same way they log in to your other apps.
3. Your identity provider sends the reader back with a signed ID token. The token includes claims about the reader, like their email address, name, and groups.
4. KnowledgeOwl checks the token, creates or updates the reader's account, and logs them in.

Readers don't need a separate KnowledgeOwl password, and you don't need to create reader accounts ahead of time.

OpenID Connect or SAML?

Both OpenID Connect and SAML let readers log in with your identity provider, and both are available on the same plans. The main differences:

	OpenID Connect	SAML
What you exchange with your IdP	A redirect URI one way, and an issuer URL, client ID, and client secret the other way	Entity IDs, login and logout URLs, metadata, and a certificate in each direction

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

	OpenID Connect	SAML
Certificates	None to upload or renew. KnowledgeOwl finds your IdP's signing keys automatically.	You upload your IdP's certificate and update it when it expires
Reader information	Claims, like `email` and `given_name`	Attributes, with names you or your IdP choose
Checking your setup	A test login and a history of recent logins, always on	Debug mode, which keeps the last login's attributes for five minutes
Good fit for	ClassLink, Clever, and modern IdPs that make OpenID Connect apps easy to create	IdPs where you already use SAML apps, or when you need groups from Google Workspace

You can use both at once, for example SAML for staff and OpenID Connect for students.

Supported identity providers

When you set up OpenID Connect, you start by choosing your identity provider. KnowledgeOwl fills in what it knows for that provider and shows notes to help you set up its app. You can choose from:

- Auth0
- ClassLink
- Clever
- Google Workspace
- JumpCloud
- Keycloak
- Microsoft Entra ID (Azure AD)
- Okta
- OneLogin
- PingOne
- **Other / manual**, for any other identity provider that supports OpenID Connect

For most providers, you create an app in your identity provider and connect it to KnowledgeOwl. Refer to Configure OpenID Connect SSO.

ClassLink

ClassLink gives you two ways to connect:

- **KnowledgeOwl's ClassLink app**: There's nothing to register. You add your districts by ClassLink tenant ID, and each district's ClassLink Tenant Administrator approves your knowledge base. Refer to Set up KnowledgeOwl's ClassLink app.
- **Your district's own app**: Your district creates an OpenID Connect app in ClassLink and gives you its details. Refer to Configure ClassLink SSO with your district's own app.

How readers are matched to accounts

Each OpenID Connect reader is identified by their SSO ID from your identity provider. By default, the SSO ID is the

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

standard `sub` claim, which is unique for each user at your identity provider. You can map a different claim in the **Map reader attributes** step.

For some providers, KnowledgeOwl sets the SSO ID for you and locks it, so each person is matched to a single reader. This applies to ClassLink, Clever, Google Workspace, and Microsoft Entra ID. On these providers, the SSO ID field is locked, with a note that each user is matched to a single reader.

Login restrictions

By default, anyone who can log in to your identity provider can log in to your knowledge base. In the **Restrict who can log in** step, you can require readers to have certain claim values, like a group or role.

Some identity providers log in users from every organization that uses them. For these, a login restriction to your own organization is required:

Provider	Restriction KnowledgeOwl prefills
ClassLink (your district's own app)	Your ClassLink tenant ID, on the `classLink_tenant_id` claim
Clever	Your district ID, on the `district_id` claim (Clever also uses `district`)
Google Workspace	Your Workspace domain, on the `hd` claim

Without that restriction, you can't turn OpenID Connect on, and logins are blocked. For Microsoft Entra ID, use your own tenant's issuer rather than the shared `common`, `organizations`, or `consumers` endpoints.

KnowledgeOwl's ClassLink app is different: only readers from your active, approved districts can log in, so no extra restriction is required.

How readers log in

Once OpenID Connect is **Available** or **Required**, readers can reach it in any of these ways:

- **The login link:** `https://<your knowledge base domain>/reader-sso/oauth2/login`. Share it, or add it to your website or intranet. You'll find it in the OpenID Connect setup, and on the **OpenID Connect (OIDC)** row of the **Login methods** card.
- **The Log in link** in your knowledge base header, when it goes to OpenID Connect. For example, when you choose **OpenID Connect login** under **Send readers who aren't logged in to**.
- **A redirect:** When OpenID Connect is **Required for all readers**, or chosen under **Send readers who aren't logged in to**, readers who open restricted content are sent straight to your identity provider.
- **Your identity provider's app launcher**, like the KnowledgeOwl tile on a ClassLink LaunchPad or an app on an Okta dashboard.



No button on the reader login page

The reader login page doesn't show an OpenID Connect option. To let readers choose between their username and password and OpenID Connect, share the login link, or add it as a link on your website or in your knowledge base.

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

If a reader's login fails, they see your knowledge base's no access page. The reason is saved in the **Recent logins** list in your OpenID Connect settings. Refer to Troubleshoot OpenID Connect logins.

OAuth 2.0 mode

A few identity providers support OAuth 2.0 but don't issue OpenID Connect ID tokens. For those, you can choose **Other / manual** and then the **OAuth 2.0 (no ID token)** protocol. In this mode, you enter the identity provider's endpoints yourself, and readers are identified by the userinfo response instead of a signed ID token.



Only use OAuth 2.0 mode when you have to

OAuth 2.0 mode is less secure than OpenID Connect. Use **OpenID Connect (recommended)** whenever your identity provider supports it.

Next steps

- Configure OpenID Connect SSO
- Set up KnowledgeOwl's ClassLink app
- Configure ClassLink SSO with your district's own app
- Troubleshoot OpenID Connect logins
- Access & SSO page overview

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