Polyguard

Single Sign-On

The Polyguard Console supports single sign-on (SSO) with your organization's identity provider over OpenID Connect. Once connected, your team signs in with their normal work login, and your identity provider's own policies for multi-factor authentication, devices, and offboarding apply to Polyguard as well.

Supported providers are **Okta**, **Google Workspace**, and **Microsoft Entra ID**. The account **owner** configures the connection in the Console under **Settings → Single sign-on**. This page walks an Okta administrator through the Okta side and the Console settings. Google Workspace and Entra ID need no app of your own: pick the provider in the Console and enter your Workspace primary domain or Entra directory ID.

How it works

1. A user enters their work email at console.polyguard.ai and clicks **Continue with single sign-on**.
2. Polyguard looks up the email domain, finds your organization's connection, and sends the browser to your identity provider.
3. Your identity provider authenticates the user and returns them to Polyguard.
4. Polyguard checks that the signed-in identity belongs to your organization and that the email address is on one of your registered domains, then opens the Console.

Users who have never signed in before get a Console account automatically, with the role you chose when the connection was set up (Organizer unless you asked for Admin). Users who already have a Polyguard account keep it: SSO is matched to them by email address.

> **What SSO does not change**
>
> SSO signs administrators and organizers in to the Console. It does not replace identity verification for meeting participants or job candidates, who still verify through Polyguard Mobile.

Before you start

You need:

- An Okta administrator who can create app integrations (typically a **Super Administrator** or **Application Administrator**).
- The Polyguard account **owner**, signed in to the Console. Only the owner can save single sign-on settings.

- Your sign-in email domain, for example `example.com`, added and approved under **Settings → Email domains** in the Console. Sign-in is routed by email domain, so this is what makes the connection reachable.
- About 15 minutes.

You will collect three values from Okta, an **issuer URL**, a **client ID**, and a **client secret**, and enter them in the Console in Step 5.

> **Treat the client secret like a password**
>
> Paste it straight into the Console rather than emailing or messaging it. Polyguard stores it in a secrets vault and never displays it again; the Console only shows that a secret is stored.

Step 1: Create the app integration

1. Sign in to the Okta Admin Console for your organization (the address ends in `-admin.okta.com`).
2. In the left sidebar, open **Applications**, then **Applications**.
3. Click **Create App Integration**.
4. Choose:
    - **Sign-in method:** `OIDC - OpenID Connect`
    - **Application type:** `Web Application`
5. Click **Next**.

Step 2: Configure the integration

On the **New Web App Integration** page, enter the following and leave everything else at its default.

Setting	Value
App integration name	`Polyguard Console`
Grant type	**Authorization Code** (checked by default). Leave the others unchecked.
Sign-in redirect URIs	`https://api.polyguard.ai/sso/callback`
Sign-out redirect URIs	`https://console.polyguard.ai/loggedout` (optional)
Controlled access	The groups or users who should be able to reach the Polyguard Console

Click **Save**.

> **Who should have access?**
>
> Assign the group that contains your recruiters, meeting organizers, and Polyguard administrators. Anyone outside the assignment is refused by Okta before they reach Polyguard, which is the simplest way to control who can sign in.

Step 3: Copy the client credentials

After saving, the integration's **General** tab opens.

1. Under **Client Credentials**, copy the **Client ID**.
2. Under **Client Secrets**, copy the secret using the copy icon. You will paste it into the Console in Step 5.
3. Under **Client authentication**, leave **Client secret** selected. **Require PKCE as additional verification** can stay on or off; Polyguard always uses PKCE.

Step 4: Find your issuer URL

Polyguard needs the address of the Okta authorization server that will issue sign-in tokens.

1. In the left sidebar, open **Security**, then **API**.
2. On the **Authorization Servers** tab, find the server named **default** and copy its **Issuer URI**. It looks like `https://<your-okta-domain>/oauth2/default`.
3. Open **default**, then the **Access Policies** tab, and confirm that a policy applies to the Polyguard Console integration. The built-in **Default Policy** applies to all clients unless it was changed.

> **No Authorization Servers tab?**
>
> Okta organizations without the API Access Management feature use the Org authorization server instead. Its issuer is your Okta domain itself, for example `https://<your-okta-domain>`. Enter that value in Step 5.

Step 5: Enter the details in the Polyguard Console

In the Polyguard Console, signed in as the account owner, open **Settings → Single sign-on** and fill in the card.

Console field	Value
Identity provider	Okta

Console field	Value
Issuer	The Issuer URI from Step 4
Client ID	The Client ID from Step 3
Client secret	The secret from Step 3
Default role for new members	User or Admin
Require SSO	Off until you have tested, see below
Enabled	On

The card also shows the **redirect URI to register**; it is the value you entered in Okta in Step 2. Click **Save single sign-on**.

Require SSO means Polyguard stops sending sign-in links by email for your active domains. Anyone who enters an address on your domain at the login page is sent to Okta instead. Turn it on once you have tested SSO with a few users.

Default role is the role a user receives the first time they sign in with SSO. Existing members keep their role. Promote users afterwards on the Users page.

Step 6: Test the sign-in

1. Go to console.polyguard.ai.
2. Enter your work email address and click **Continue with single sign-on**.
3. Sign in at Okta if prompted.
4. You land on the Console dashboard.

If something goes wrong, the login page or the sign-in completion page shows one of these messages.

Message	Meaning	What to do
Single sign-on is not set up for this email domain.	There is no enabled connection for an account with that domain active.	Check the address. In the Console, confirm the domain is approved under Email domains and the connection is enabled.
Your identity provider did not complete the sign-in.	Okta refused the request or the token exchange failed.	Confirm the user is assigned to the integration and the sign-in redirect URI matches exactly.
Your email domain is not registered with this account.	The Okta account's email is on a domain Polyguard has not registered for you.	Ask Polyguard to add the domain, or sign in with an address on a registered domain.

Message	Meaning	What to do
Your identity provider has not verified your email address.	Okta reported the email address as unverified.	Verify the address in the user's Okta profile.
This identity has been disabled. Contact your administrator.	The Polyguard identity linked to this Okta user was revoked.	Contact Polyguard support.
This sign-in attempt expired. Start again from the login page.	More than ten minutes passed between starting and finishing the sign-in.	Start again from the login page.

Managing users after SSO

- **New users** are created on their first successful sign-in with the default role you chose. Promote them on the **Users** page; see Inviting Users.
- **Offboarding**: unassigning a user from the integration in Okta blocks their next sign-in. A Console session they already hold lasts up to 12 hours.
- **Rotating the client secret**: generate the new secret in Okta, then paste it into the **Client secret** field in the Console and save. Sign-ins fail between the two steps, so do them back to back.

Related Resources

- Account Setup: how administrators create or join an organization
- Inviting Users: roles and invitations for team members who do not use SSO
- Getting Help: contact support