How to Configure SAML 2.0 for Kirin with Okta

Kirin is an AI security platform that gives engineering and security teams real-time visibility into how developers use AI coding tools such as Cursor, GitHub Copilot, and Claude. It detects risky AI-generated code, enforces security policies, and surfaces unauthorized AI usage across the organization. The Kirin–Okta integration allows your team members to sign in to Kirin using Okta as a Single Sign-On provider — no separate Kirin password is required, and access is governed by your existing Okta MFA and sign-in policies.

Prerequisites

- A Kirin account at app.getkirin.com with the **Owner** or **Manager** role in your organization. SSO settings are not visible to Members.
- Admin access to your Okta organization.
- Your organization's email domain (e.g. `acme.com`).

Supported features

- SP-initiated SSO
- Just-In-Time (JIT) provisioning

The following features are not currently supported:

- IdP-initiated SSO
- SP-initiated SLO (Single Logout)
- Force authentication
- Attribute updates after initial login — if a user's name or email changes in Okta after their first Kirin login, the change will not be reflected in Kirin automatically. See the Troubleshoot section.

For more information on the listed features, visit the Okta Glossary.

Supported SAML attributes

The following attributes are sent in the SAML assertion and are pre-configured in the Okta app template. No additional Profile Editor mapping is required.

Attribute name	Value expression	Description
`email`	`user.email`	User's email address (used as Kirin Login ID)
`userName`	`user.login`	Okta username
`name`	`user.firstName + " " + user.lastName`	User's display name in Kirin

- **Name ID Format**: `EmailAddress`
- **Application username**: `Okta username`

Configuration steps

Step 1 — Generate SP credentials in Kirin

Role required: You must be an **Owner** or **Manager** of your Kirin organization to access SSO settings. Members do not have access to this section.

1. Sign in to Kirin at app.getkirin.com with an account that has the **Owner** or **Manager** role.
2. Navigate to **Organization Settings** → **Integrations** → **SAML SSO Integration**.
3. Under **Step 1**, click **Generate SP credentials**. Kirin creates a dedicated SSO slot for your organization and unlocks the remaining steps.
4. Once generated, expand the **Using Okta (OIN)?** section at the bottom of the card. Copy both values:
   - **Kirin Tenant ID** — your organization's unique identifier in Kirin (format: `T...`).
   - **Kirin SSO ID** — a unique identifier for your SSO connection (format: `S...`). Required for Okta to route SAML assertions correctly.

Keep this browser tab open. You will paste these values into Okta in Step 3.

Step 2 — Add the Kirin app in Okta

1. In your Okta Admin Console, go to **Applications** → **Browse App Catalog**.
2. Search for **Kirin** and click **Add Integration**.
3. Enter a display label (e.g. `Kirin`) and click **Done**.

Step 3 — Enter your Kirin integration variables in Okta

1. Go to the **General** tab of the Kirin app in Okta.
2. In the **App Settings** section, click **Edit**.
3. Under **General Settings** (**General** tab → **App Settings**), you will see two fields:
   - **Kirin Tenant ID** (`tenant_id`) → paste the **Kirin Tenant ID** from Step 1
   - **Kirin SSO ID** (`sso_id`) → paste the **Kirin SSO ID** from Step 1
4. On the **Sign On** tab, set **Application username** to **Okta username**.
5. Click **Save**.

Okta uses these two values to automatically build the correct ACS URL and Entity ID for your organization. You do not need to enter these URLs manually.

Step 4 — Copy the Okta Metadata URL to Kirin

1. Still on the **Sign On** tab in Okta, scroll to **SAML Signing Certificates** (or **Metadata details**).
2. Click **Actions** → **View IdP Metadata**, or right-click the link and copy the Metadata URL. It has the format: `https://<your-okta-domain>/app/<appId>/sso/saml/metadata`
3. Return to Kirin → **Organization Settings** → **Integrations** → **SAML SSO Integration** (requires **Owner** or **Manager** role).
4. Click **Connect your identity provider** to expand the form.
5. Enter your organization's **email domain** (e.g. `acme.com`). Users with this email domain will be automatically redirected to Okta when they sign in to Kirin.
6. Paste the Metadata URL into the **IdP Metadata URL** field.
7. Click **Configure SSO**.

Kirin contacts Okta to fetch the IdP certificate and settings automatically. The card header shows a **Configured** badge when complete.

Step 5 — Assign users in Okta

1. Go to the **Assignments** tab of the Kirin app in Okta.
2. Click **Assign** and assign the users or groups who should have access to Kirin.

Step 6 — Test the integration

1. Open a new **private/incognito** browser window (important — avoids session conflicts with any existing Kirin login).
2. Go to app.getkirin.com.
3. Enter your work email address.
4. You will be redirected to Okta to authenticate.
5. After successful authentication, you will be redirected back to Kirin.

Note: Since only SP-initiated SSO is supported, Okta recommends hiding the Kirin app icon in the Okta dashboard to avoid user confusion.

SP-initiated SSO

Kirin supports SP-initiated SSO only. The login flow is:

1. User visits app.getkirin.com and enters their work email.
2. Kirin detects the registered SSO domain and redirects the user to their Okta org.
3. The user authenticates in Okta (password + MFA per Okta policy).
4. Okta sends a signed SAML assertion back to Kirin.
5. The user is signed in to Kirin.

IdP-initiated login (clicking the Kirin tile in Okta) is not supported. Hide the app tile from the Okta End-User Dashboard to prevent confusion.

Troubleshoot

SSO redirect does not start — user stays on the Kirin login page

- Confirm the **email domain** entered in Kirin's SSO configuration matches the domain in the user's email exactly (e.g. `acme.com` for `alice@acme.com`).
- Ensure the **Configured** badge is visible in the Kirin SSO section. If not, the Metadata URL may not have been saved correctly — repeat Step 4.

"Invalid SAML Response" or Destination mismatch error

- The `sso_id` value in Okta does not match what Kirin expects. Open Kirin **Organization Settings** → **Integrations** → **SAML SSO Integration**, expand the **Using Okta (OIN)?** section, copy the current **Kirin SSO ID**, and re-enter it in Okta under **General** → **App Settings** (Step 3).

"Unable to sign in" after Okta authentication

- Verify both **Kirin Tenant ID** (`tenant_id`) and **Kirin SSO ID** (`sso_id`) are entered correctly in Okta. A single character difference causes the assertion to be rejected.
- Check that the user is assigned to the Kirin app in Okta (Step 5).

The user's name or email is outdated in Kirin

- Kirin reads SAML attributes on first login only. Subsequent changes in Okta (name, email) are not automatically synced to Kirin. Contact support@getkirin.com to update user details manually.

Support

For assistance with this integration, contact support@getkirin.com.