Single Sign-On (SSO)

Implementation Guide — OKRs Tool

Enterprise Authentication for Your Organization

1. Overview

OKRs Tool supports Enterprise Single Sign-On (SSO), allowing organizations to authenticate users through their existing Identity Provider (IdP) — such as Okta, Microsoft Entra ID (Azure AD), Google Workspace, OneLogin, JumpCloud, and others.

With SSO enabled, your team members can sign in to OKRs Tool using the same corporate credentials they use for all other enterprise applications, without needing a separate password.

The SSO implementation is built on industry-standard protocols (SAML and OIDC), and all authentication flows are handled securely through encrypted communication between OKRs Tool and your Identity Provider. Sensitive credentials are never exposed to the browser and all requests are validated with secret keys on our secure backend.

1.1 Key Capabilities

- Connect to any major Identity Provider (Okta, Entra ID, Google Workspace, and more)
- Optional or enforced SSO — choose whether SSO is required for all users or optional
- Just-In-Time (JIT) provisioning — automatically create accounts for new users on their first SSO login
- Domain-based routing — users are automatically redirected to SSO based on their email domain
- Full audit log — every SSO event is recorded for visibility and compliance
- Admin self-service — configure and manage SSO directly from your organization settings

2. How SSO Works

When a user attempts to sign in with SSO, the following flow takes place:

- The user enters their corporate email address on the OKRs Tool login page and clicks 'Continue with SSO'.
- OKRs Tool identifies the organization associated with that email domain and redirects the user to your Identity Provider.

- The user authenticates with their corporate credentials directly on your IdP (OKRs Tool never sees the password).
- After successful authentication, the IdP returns a verified user profile to OKRs Tool.
- OKRs Tool matches the profile to an existing user account or creates a new one (if JIT provisioning is enabled), then logs the user in automatically.

> *The email entered on the login page is used only to identify which organization the user belongs to. The actual authentication and identity verification always happen on your Identity Provider.*

3. Setting Up SSO

SSO is configured from the Security tab in your Organization Settings. Only organization administrators can manage SSO settings.

3.1 Enabling SSO

To begin the SSO setup:

- Go to Settings > Security.
- In the Single Sign-On card, enter your organization's corporate email domain (e.g. company.com).
- Click Enable SSO.

This registers your organization in our authentication system and saves your domain. The SSO card will update to show that SSO is active but an Identity Provider has not yet been connected.

> *Only users whose email matches the configured domain will be able to sign in via SSO. Make sure the domain matches your corporate email addresses exactly.*

3.2 Connecting Your Identity Provider

After enabling SSO, you need to connect your Identity Provider:

- Click Connect Identity Provider in the SSO card.
- A configuration modal will open. Select your Identity Provider from the list (Okta, Microsoft Entra ID, Google Workspace, OneLogin, JumpCloud, AD FS, or Custom Provider).
- Follow the step-by-step instructions shown in the modal to configure the connection on your IdP side. The steps vary by provider but generally include creating an application in your IdP and providing the required metadata.
- Once you have completed all steps and activated the connection in the modal, the SSO card will automatically update to show that the connection is active and ready.

> *The configuration modal guides you through each step for your specific Identity Provider. No technical expertise is required — the instructions are tailored to your chosen provider.*

3.3 SSO Card Status Overview

Status	What It Means
Not Configured	SSO has not been set up. Click Enable SSO to begin.
Active — No Connection	SSO is enabled but no Identity Provider has been connected yet. Click Connect Identity Provider to complete setup.
Active — Ready	SSO is fully configured and users can sign in. Your IdP is connected and the domain is verified.
Disabled	SSO was previously active but has been disabled. Users cannot sign in via SSO until it is re-enabled.

4. SSO Settings

Once SSO is active, you can configure additional settings from the SSO card.

4.1 SSO Mode

You can choose how SSO is enforced for your organization:

Mode	Behavior
Optional (default)	Users can choose to sign in with SSO or with their existing login method (email access link or Google). SSO is available but not required.
Enforced	All users with the configured domain must sign in via SSO. Sign-in via Google is blocked for those users. This is recommended for maximum security compliance.

To change the mode, use the Enforce SSO or Set to Optional buttons in the SSO card.

4.2 Auto-Provisioning (JIT)

Just-In-Time (JIT) provisioning automatically creates a new OKRs Tool account the first time a user from your organization signs in via SSO, without requiring a manual invitation.

- When enabled: Any user with a matching email domain who authenticates successfully via SSO will have an account created automatically as a member of the organization.
- When disabled: Only users who already have an account in OKRs Tool can sign in via SSO. New users will see an error and will need to be invited first.

> *JIT provisioning creates users as standard members. If a pending invitation exists for that user at a leadership level, it will be processed automatically at the time of account creation.*

5. Managing SSO

5.1 Managing Your Identity Provider Connection

Once connected, you can manage your IdP configuration at any time by clicking Manage SSO in the SSO card. This opens the same configuration modal where you can view the current connection status, update settings, or troubleshoot issues.

5.2 Disabling SSO

To temporarily disable SSO without losing your configuration:

- Click Disable SSO in the SSO card.
- SSO will be deactivated both in OKRs Tool and on the Identity Provider side. Users will not be able to sign in via SSO while it is disabled.
- All configuration is preserved. You can re-enable SSO at any time by clicking Re-enable SSO.

> *Disabling SSO does not delete your Identity Provider connection. Your setup is saved and can be restored instantly.*

5.3 Removing Your Identity Provider

If you want to switch to a different Identity Provider without deleting your entire SSO setup:

- Click Remove Identity Provider in the SSO card.
- A confirmation dialog will appear warning that users will not be able to sign in via SSO until a new provider is connected.
- After confirming, the current Identity Provider connection is removed. Your domain and organization settings are preserved.
- You can then connect a new Identity Provider following the steps in Section 3.2.

5.4 Deleting SSO Configuration Permanently

To completely remove all SSO settings and start from scratch:

- Click Delete SSO Configuration in the SSO card (available when SSO is disabled).
- A confirmation dialog will appear with a warning that this action cannot be undone.
- After confirming, all SSO configuration is permanently deleted — including the domain, Identity Provider connection, and organization registration.
- The SSO card returns to the Not Configured state. You can set up SSO again from the beginning if needed.

> *This action is permanent and cannot be undone. All users currently relying on SSO to sign in will lose access immediately. Make sure to communicate this change to your team before proceeding.*

6. User Login Experience

For end users, the SSO login experience is straightforward:

- On the OKRs Tool login page, click Sign in with SSO.
- Enter your corporate email address and click Continue.
- You will be redirected to your organization's Identity Provider login page.
- Enter your corporate credentials as usual.
- After successful authentication, you will be automatically signed in to OKRs Tool.

> *If your administrator has set SSO to Enforced mode, you will be automatically redirected to the SSO login flow when you attempt to sign in with Google. Direct Google login will not be available.*

7. SSO Audit Log

All SSO-related events are recorded in the audit log, available to organization administrators. The following events are tracked:

Event	Description
Setup Started	An administrator initiated the SSO setup process.
Setup Completed	The Identity Provider connection was successfully configured and activated.
Login Success	A user successfully authenticated via SSO.
Login Failed	An SSO login attempt failed (e.g. user not found, wrong organization).
User Created	A new user account was automatically created via JIT provisioning.
SSO Enabled	SSO was re-enabled after being disabled.
SSO Disabled	SSO was disabled by an administrator or via the Identity Provider portal.
SSO Disconnected	The Identity Provider connection was removed.

Event	Description
Connection Disabled	The Identity Provider connection was deactivated.
Mode Changed to Enforced	SSO mode was changed to Enforced.
Mode Changed to Optional	SSO mode was changed to Optional.
JIT Enabled	Auto-provisioning was turned on.
JIT Disabled	Auto-provisioning was turned off.

8. Error Reference

If a user encounters an error during SSO login, they will see one of the following messages on the error page:

Error	Cause & Resolution
SSO not configured	The email domain entered is not associated with an SSO configuration. Verify the domain is correct or contact your administrator to confirm SSO is set up.
SSO unavailable	SSO is configured but the Identity Provider connection is currently inactive. Contact your administrator to re-enable the connection.
Authentication failed	An error occurred during authentication with the Identity Provider. Try again or contact your administrator if the issue persists.
Wrong organization	The authenticated user belongs to a different organization. Make sure you are signing in with the correct account.
Access not provisioned	Your account does not exist in OKRs Tool and auto-provisioning is disabled. Contact your administrator to be invited.
Invalid or expired session	The login session expired (sessions are valid for 5 minutes). Try signing in again.

9. Security

The SSO implementation follows industry best practices to ensure the security of your authentication flow:

- All communication between OKRs Tool and your Identity Provider uses encrypted HTTPS connections.
- A unique, time-limited state token is generated for each login attempt to prevent replay and CSRF attacks. Tokens expire after 5 minutes.
- Webhook events from the Identity Provider are verified using HMAC-SHA256 signatures, ensuring that only legitimate events from your IdP are processed.

- Secret keys used for backend communication are never exposed to users or browsers — all sensitive operations happen server-side.
- When SSO Enforced mode is active, OKRs Tool automatically blocks alternative sign-in methods (such as Google login) for users in the configured domain.
- All SSO events are logged with timestamps and user information for audit and compliance purposes.

10. Supported Identity Providers

OKRs Tool supports the following Identity Providers out of the box:

Identity Provider	Protocol
Okta	SAML or OIDC
Microsoft Entra ID (Azure AD)	SAML or OIDC
Google Workspace	OIDC
OneLogin	SAML or OIDC
JumpCloud	SAML or OIDC
AD FS (Active Directory Federation Services)	SAML
Custom Provider	SAML or OIDC

> *If your Identity Provider is not listed above, you can still connect it using the Custom Provider option, as long as it supports SAML 2.0 or OIDC.*

For additional support, contact the OKRs Tool team.