# Set up single sign-on (SAML) with Entra ID, Okta or Google

Connect HIPAA Certify to your identity provider so employees sign in with their work account.

For: Administrators, Managers · Updated November 17, 2026 · https://hipaacertify.com/support/article/sso-setup

HIPAA Certify supports **SAML 2.0** single sign-on. You'll need someone who can add an "enterprise application" or "SAML app" in your identity provider (IdP), usually your IT team.

## 1. Copy HIPAA Certify's details

1. Click **SSO Settings** in the sidebar.
2. Under **Service Provider (SP) Information**, copy:
   - **SP Entity ID / Audience URI**
   - **ACS URL (Assertion Consumer Service)**
   - **SP Metadata URL** (some IdPs can import everything from this)

## 2. Create the app in your identity provider

In Entra ID, Okta, Google Workspace or another IdP, create a SAML app and paste in the values from step 1:

- **Identifier / Entity ID / Audience** = the SP Entity ID
- **Reply URL / ACS URL / Single sign-on URL** = the ACS URL
- **Name ID** = the user's **email address**. Or send an `email` attribute.

Assign the app to the people who need HIPAA training.

## 3. Paste your IdP's details into HIPAA Certify

Back on **SSO Settings**, under **Identity Provider (IdP) Configuration**:

1. **IdP Entity ID**: also called the Issuer or Microsoft Entra Identifier
2. **IdP SSO URL**: also called the Login URL or SAML 2.0 Endpoint



Downloaded Nov 17, 2026 — check the link above for the latest version.

3. **IdP X.509 Certificate**: open the Base64 signing certificate in a text editor and paste it, with or without the BEGIN/END lines
4. **IdP Single Logout URL**: optional
5. Click **Save Settings**, then **Test Configuration**. You should see **SSO configuration looks valid.**
6. Turn on **Enable SSO for this organization** and click **Save Settings**.

## 4. Choose how accounts are created

- **Just-In-Time (JIT) Provisioning off (recommended):** people must already be on your Employees list, with the **same email** your IdP sends. You can assign training before they ever sign in.
- **JIT on:** anyone your IdP lets in gets an account on their first sign-in, with the **Default Role** you choose. You'll need to assign their training afterward.

## 5. Test before you announce it

Open your organization's login page in a private or incognito window, click **Sign in with SSO**, and sign in as one test user. Once that works, share the login page link with staff. See Sign in with SSO.

> **IMPORTANT**
>
> If the test sign-in fails, or you see **Page Expired** after signing in at your identity provider, keep SSO turned off and contact support. Include your IdP's name. Employees can keep using their passwords in the meantime.

Need more help? Visit https://hipaacertify.com/support or contact us at https://hipaacertify.com/contact.


Downloaded Nov 17, 2026 — check the link above for the latest version.