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 24, 2026 · https://hipaacertify.com/index.php/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.

IT teams who want the protocol details (bindings, signing rules, what is validated, and limits) can go straight to the SSO technical reference.

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.

> **NOTE**

Downloaded Nov 24, 2026 — check the link above for the latest version.

> Guest (B2B) accounts in Entra ID can sign in too, as long as the Name ID your tenant sends is the person's email address.

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
3. **IdP X.509 Certificate**: the signing certificate for **the app you created in step 2**. Open the Base64 certificate in a text editor and paste it, with or without the BEGIN/END lines. See **Which certificate to use** below.
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**.

Which certificate to use

Use the SAML signing certificate that belongs to the app itself:

- **Entra ID:** open **Enterprise applications**, select your app, then **Single sign-on**. In the **SAML Certificates** section, download **Certificate (Base64)**.
- **Okta, Google Workspace and others:** use the signing certificate shown on that SAML app's own setup page.

> **WARNING**
>
> Don't use a certificate from your tenant's general federation metadata. It looks valid and passes **Test Configuration**, but every sign-in then fails with **SSO authentication failed**.

> **NOTE**
>
> **Test Configuration** checks that the fields are filled in and that the certificate is readable. It can't confirm it is the right certificate. The test sign-in in step 5 does that.

Downloaded Nov 24, 2026 — check the link above for the latest version.

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.

Two things to know about JIT:

- **Training emails wait for an invitation.** People created by JIT aren't marked as invited, so they don't receive training-assigned or reminder emails until you click **Send Invite** for them on the Employees page. The invitation email includes a password setup link; people who use SSO can ignore it and use **Sign in with SSO** on your login page.
- **Free university and government accounts** only create people whose email ends in `.edu` or `.gov`. Anyone else sees **No account found for this email.**

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. Use a private window because a browser that is already signed in to HIPAA Certify goes straight to the dashboard and doesn't test SSO.

Once that works, share the login page link with staff. See Sign in with SSO.

If the test sign-in fails

Message	What it means	What to do
SSO authentication failed. Please try again.	HIPAA Certify couldn't verify the response from your IdP. When it happens on every attempt, it is almost always the wrong certificate.	Paste the app's own signing certificate (step 3) and save. Also confirm the Entity ID and ACS URL in your IdP match step 1 exactly.
Could not retrieve email from SSO response.	The Name ID isn't an email address, and no email attribute was sent.	Set the Name ID to the user's email address (step 2).

Downloaded Nov 24, 2026 — check the link above for the latest version.

Message	What it means	What to do
No account found for this email. Please contact your administrator.	The person isn't on your Employees list with that exact email, and JIT is off or can't create them.	Add the person, correct their email, or turn JIT on (step 4).
Your account has been deactivated…	That person's account is turned off.	Reactivate them. See Deactivate or reactivate an employee.
An error occurred during SSO authentication.	Something unexpected went wrong on our side.	Contact support with the date and time of the attempt.

IMPORTANT

Still stuck? Contact support with your IdP's name and the date and time of a failed attempt, and we can look up the exact reason. Employees who have a password can keep using it in the meantime.

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

Downloaded Nov 24, 2026 — check the link above for the latest version.