SSO technical reference (SAML details for IT teams)

The SAML 2.0 details an identity team needs: endpoints, bindings, signing rules, what HIPAA Certify validates, how users are matched, and current limits.

For: Administrators, Managers · Updated November 21, 2026 · https://hipaacertify.com/index.php/support/article/sso-technical-reference

This page is for the person configuring your identity provider (IdP). For the step-by-step walkthrough, see Set up single sign-on.

HIPAA Certify is a **SAML 2.0 service provider (SP)**. Each organization has its own endpoints and its own IdP settings.

Service provider endpoints

Replace `your-organization` with the last part of your organization's login address. The exact values are shown on **SSO Settings**.

Item	Value	Binding
SP Entity ID / Audience	`https://hipaacertify.com/org/your-organization/sso/metadata`	
ACS URL (Reply URL)	`https://hipaacertify.com/org/your-organization/sso/acs`	HTTP-POST
SP metadata (XML)	`https://hipaacertify.com/org/your-organization/sso/metadata`	
Start sign-in (SP-initiated)	`https://hipaacertify.com/org/your-organization/sso/login`	
Logout endpoint	`https://hipaacertify.com/org/your-organization/sso/sls`	HTTP-Redirect

The sign-in request we send

- Sent to your **IdP SSO URL** with the **HTTP-Redirect** binding.

Downloaded Nov 22, 2026 — check the link above for the latest version.

- **Not signed.**
- Asks for the Name ID format `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
- Does not request a specific authentication context, so your IdP's own MFA and conditional access policies apply.
- RelayState is not used. After sign-in, people land on their own dashboard.

What your IdP's response must contain

- Delivered to the ACS URL with the **HTTP-POST** binding.
- A **signature** on the response, on the assertion, or on both. RSA-SHA256 is recommended.
- **Not encrypted.** Leave assertion encryption turned off.
- A **Name ID**. It should be the person's email address.

What HIPAA Certify validates

Every response is checked in strict mode. A response that fails any check is rejected, and the person sees **SSO authentication failed**.

Check	Must match
Signature	The certificate saved in **IdP X.509 Certificate**
Issuer	The value saved in **IdP Entity ID**
Audience	The SP Entity ID
Destination and Recipient	The ACS URL
Validity window	The current time. Small clock differences are tolerated.
XML structure	The SAML 2.0 schema

Everything else in the assertion is ignored. That includes group and role claims, tenant ID claims, and the `identityprovider` claim that Entra ID adds for guest users.

How the person is matched to an account

1. The email address is taken from the **Name ID** if it is a valid email address.
2. Otherwise, the first of these attributes that holds a valid email address is used: `email`, `Email`, `emailAddress`, `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`,

Downloaded Nov 22, 2026 — check the link above for the latest version.

`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`, `http://schemas.microsoft.com/identity/claims/emailaddress`, `mail`, `Mail`.

3. The address is lowercased and matched against the people in **your organization only**.
4. A deactivated account is refused.

If no account matches and Just-In-Time (JIT) provisioning is on, an account is created:

- **Name:** taken from `name`, `displayName`, `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`, `http://schemas.microsoft.com/identity/claims/displayname`, `cn` or `givenName`. If none is sent, first and last name attributes are combined. If those are missing too, the part of the email before the `@` is used.
- **Role:** the **Default Role** chosen on **SSO Settings**.
- **Password:** none that anyone knows. The person signs in with SSO.
- **Invitation status:** not invited, so training emails wait until an administrator sends an invitation.

Existing accounts are not changed by a sign-in. Names and roles are not updated from claims.

Microsoft Entra ID field mapping

In Entra ID	Use
Identifier (Entity ID)	The SP Entity ID
Reply URL (Assertion Consumer Service URL)	The ACS URL
Sign on URL (optional)	The "Start sign-in" address above
Unique User Identifier (Name ID)	`user.mail`, format **Email address**
Microsoft Entra Identifier	Paste into **IdP Entity ID**. It looks like `https://sts.windows.net/your-tenant-id/`
Login URL	Paste into **IdP SSO URL**. It looks like `https://login.microsoftonline.com/your-tenant-id/saml2`

Downloaded Nov 22, 2026 — check the link above for the latest version.

In Entra ID	Use
Certificate (Base64), under SAML Certificates	Paste into **IdP X.509 Certificate**

Guest (B2B) accounts work. The response is still issued and signed by your tenant, which is what HIPAA Certify checks.

Certificate rollover

HIPAA Certify stores **one** signing certificate per organization.

> **WARNING**
> When your IdP's signing certificate is renewed or replaced, sign-ins fail with **SSO authentication failed** until the new certificate is pasted into **SSO Settings**. Plan to update it at the moment you make the new certificate active.

Current limits

- **No SCIM provisioning.** Add people with JIT, a CSV import, or the Employee API on plans that include it.
- **No group or role mapping.** Roles are set in HIPAA Certify.
- **SSO can't be made the only way in.** The email and password form stays on your organization's login page.
- **One identity provider per organization.**
- **The SSO button is only on your organization's own login page**, not on the general login page.
- **Free university and government accounts** only create `.edu` and `.gov` addresses with JIT.

Not yet confirmed

These have not been verified in a live setup. Test them before you rely on them.

- **IdP-initiated sign-in**, such as launching from an app tile without a Sign on URL.
- **Single logout.** Plan on people signing out of HIPAA Certify only.
- **Okta and Google Workspace.** The settings above apply to any SAML 2.0 IdP, but only Microsoft Entra ID has been through a production setup so far.

Downloaded Nov 22, 2026 — check the link above for the latest version.

What to send support

If a sign-in fails and the cause isn't clear, contact support with:

- Your organization's login address
- Your IdP's name
- The date and time of a failed attempt, with the time zone
- The exact message shown

Our logs record the specific check that failed for each attempt. A SAML trace helps but isn't required. Never send passwords or private keys.

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

Downloaded Nov 22, 2026 — check the link above for the latest version.