Set up single sign-on (SSO)

Let members sign in to Ovation with the school or work account they already use, through your organization's identity provider.

For organization administrators and the identity team that manages your identity provider. You need the organization administrator role in Ovation and an administrator for your identity provider.

How SSO works with Ovation

Single sign-on (SSO) sends people to your identity provider, the service that already holds their school or work accounts, such as Okta, Microsoft Entra ID, or Google Workspace. Once the provider confirms who they are, Ovation signs them in to the Ovation account with the same email address. SSO doesn't create accounts; each person gets one in one of three ways:

Add or invite them	Add people on the Members page before they sign in, as in Student Management Quick Start. Each person's Ovation email must be the same address your identity provider sends.
Create accounts at first sign-in	With **Account creation** on, anyone your provider signs in whose email is on one of your organization's eligible domains gets an account automatically.
Provision them from your directory	Your directory creates, updates, and turns off accounts through SCIM; see Set up account provisioning (SCIM).

Ovation works with any provider that supports SAML 2.0 or OpenID Connect (OIDC). Use whichever your identity team prefers; most school and company providers offer SAML 2.0, which the steps below use.

BEFORE YOU BEGIN

Before you start

- [ ] You can sign in to Ovation as your organization's administrator.
- [ ] Someone on your identity team can create a SAML 2.0 or OpenID Connect application for Ovation in your provider and assign people to it.
- [ ] Two pilot people are ready to test: a learner and an administrator. Each has an Ovation account whose email matches the email your provider sends for them.

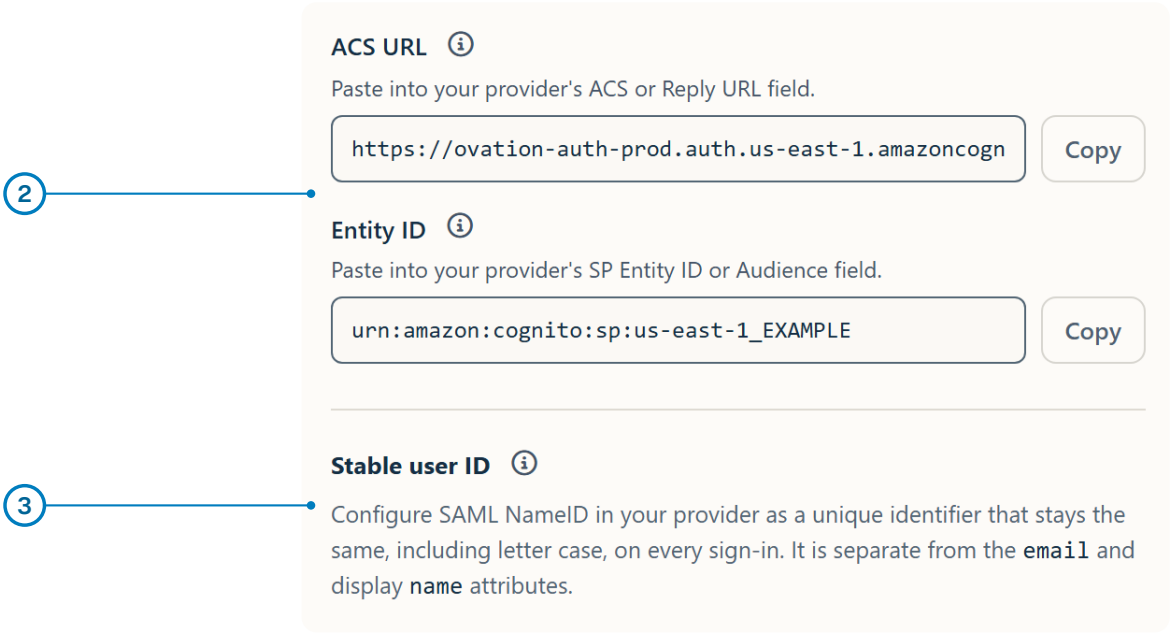
STEP 1

Add the SSO connection

Go to **Organization › Settings › SSO**

Keep your provider's admin console open in another tab. You copy two values from Ovation into your provider, then bring your provider's metadata back. These steps use SAML 2.0; OpenID Connect differences follow them.

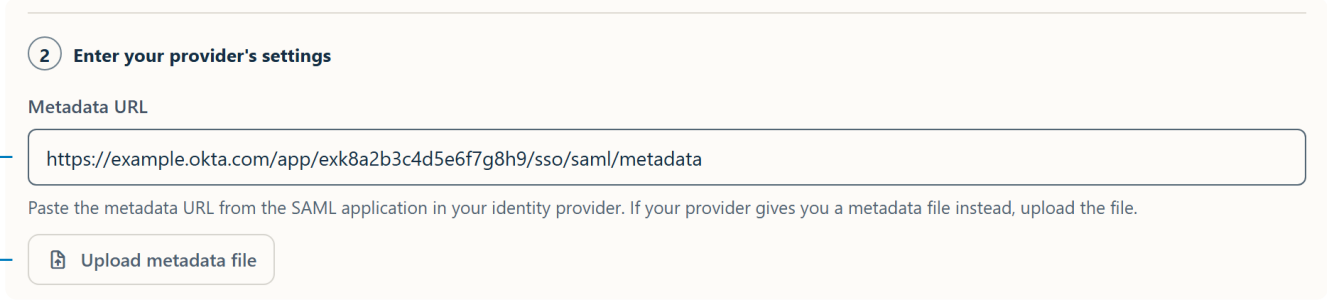
1. Select **Add SSO Connection**. Enter a **Connection name** your members will recognize, such as your school's name, because their sign-in button shows it. Choose **SAML 2.0**, then select **Continue**.
2. In your identity provider, create a SAML application for Ovation. Use the **Copy** buttons to copy Ovation's **ACS URL** and **Entity ID** into it. The info button beside each names the matching field in common providers.
3. Set the application's NameID to a value that is unique to each person and never changes, such as their directory object ID. Ovation uses it to recognize the same person at every later sign-in.



4. Add the four **Attribute statements** with the exact names shown. Only **email** is required; the other three fill in members' names. Choose your provider under **Identity provider** to see which of its fields to use for each.



5. Under **Enter your provider's settings**, paste the application's metadata URL into **Metadata URL**. If your provider gives you a file instead, select **Upload metadata file** and choose it. Then select **Continue**.



6. Check the name and protocol on **Review and enable**, then select **Save and enable** and confirm. The new connection card shows **Active**.
7. In your identity provider, assign the people who will use Ovation to the application, starting with your two pilot people.

Active means Ovation accepted your provider's settings. It does not check what your provider sends when someone signs in, so test with your pilot people before you tell everyone.

ALTERNATIVE: OPENID CONNECT

If you use OpenID Connect

1. Choose **OpenID Connect** in step 1. In step 2, copy the **Redirect URI** into your provider's application, and allow the openid, email, and profile scopes.
2. Enter the application's **Issuer URL**, **Client ID**, and **Client secret**. Then select **Continue**, and **Save and enable** on the review page.

Your provider must return the **email** claim; **given_name**, **family_name**, and **name** fill in members' names. **Account creation** also needs **email_verified** as true, which Okta and Google send but Microsoft Entra ID doesn't by default, so use SAML 2.0 with Entra if you want it.

Ovation keeps no copy of the client secret that it can show you, so store it in your password manager; changing the issuer URL or client ID later requires it.

Notes for common identity providers

Provider	Where Ovation's values go	NameID, attributes, and metadata
Okta	In the SAML app's **Configure SAML** step, paste the ACS URL into **Single sign-on URL** and the Entity ID into **Audience URI (SP Entity ID)**.	Choose an **Application username** that doesn't change; it becomes the NameID. In **Attribute Statements**, map email to user.email, given_name to user.firstName, and family_name to user.lastName, with **Name format** Unspecified. The **Metadata URL** is on the app's **Sign On** tab.
Microsoft Entra ID	In the enterprise app, open **Single sign-on** > **SAML** > **Basic SAML Configuration**. Paste the Entity ID into **Identifier (Entity ID)** and the ACS URL into **Reply URL (Assertion Consumer Service URL)**.	Set **Unique User Identifier (Name ID)** to user.objectid. In **Attributes & Claims**, add email, given_name, family_name, and name with **Namespace** left blank. Map email to user.userprincipalname, or to user.mail when that is the person's Ovation email. Copy **App Federation Metadata Url** from **SAML Certificates**.
Google Workspace	In the custom SAML app's **Service provider details**, paste the ACS URL into **ACS URL** and the Entity ID into **Entity ID**.	Google sets the NameID to the primary email. Map **Primary email**, **First name**, and **Last name** to email, given_name, and family_name. Google offers its metadata only as a file: on the **Google Identity Provider details** page, select **Download metadata**, then select **Upload metadata file** in Ovation and choose that file.
Others	OneLogin, Cisco Duo, JumpCloud, PingOne, PingFederate, Microsoft AD FS, Shibboleth and InCommon, Auth0, and Keycloak are in the **Identity provider** list.	Choose yours to see its fields, then select the info buttons beside **ACS URL**, **Entity ID**, and **Stable user ID** for the matching settings and a link to the provider's own guide.

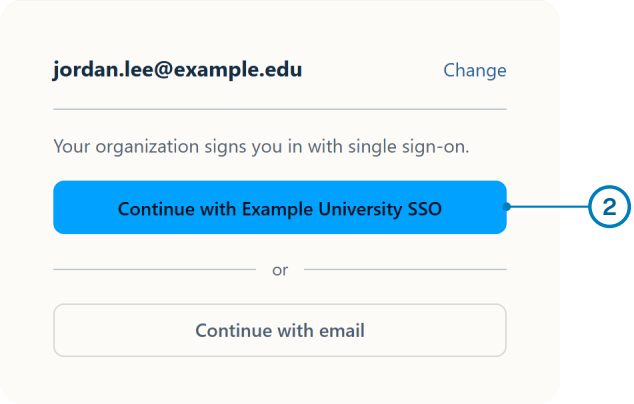
To give members a dashboard tile, use the connection's sign-in link: select **Copy** next to **Sign-in link** on the connection card. In Entra, enter it as **Sign on URL** in **Basic SAML Configuration**; in Okta, select **Do not display application icon to users** for the SAML app and add a **Bookmark App** with that link. The first time someone uses the tile on a browser, Ovation asks for their work email; after that, the tile signs them in directly. Ovation doesn't accept sign-ins that the provider starts on its own (IdP-initiated), because it can't confirm that the person at that browser asked to sign in.

STEP 2

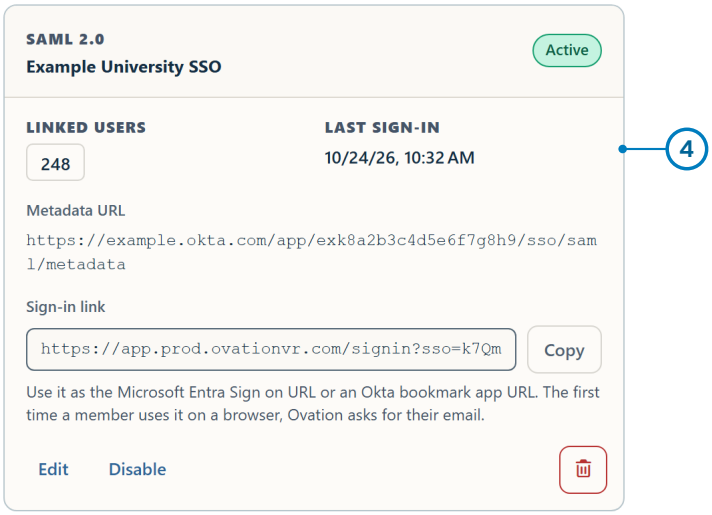
Test with your pilot people

Every member who enters their email on the sign-in page sees **Continue with** and your connection name, so your provider's assignments decide who gets through. Until you turn on **SSO Only**, they can also choose **Continue with email** to use their Ovation password or a one-time link.

1. Open a private browser window, so no earlier session is used, and go to the Ovation sign-in page.
2. Enter the pilot learner's email and select **Continue**. Select **Continue with** followed by your connection name, then sign in at your provider.
3. Confirm the learner arrives in your organization in Ovation. Repeat with the pilot administrator in a new private window.



4. Back on the **SSO** tab, check the connection card. **Last sign-in** shows when someone last signed in through it, and **Linked users** counts everyone who has. Select the count to list them on the **Members** page.



SSO sign-ins last seven days before Ovation asks members to sign in again.

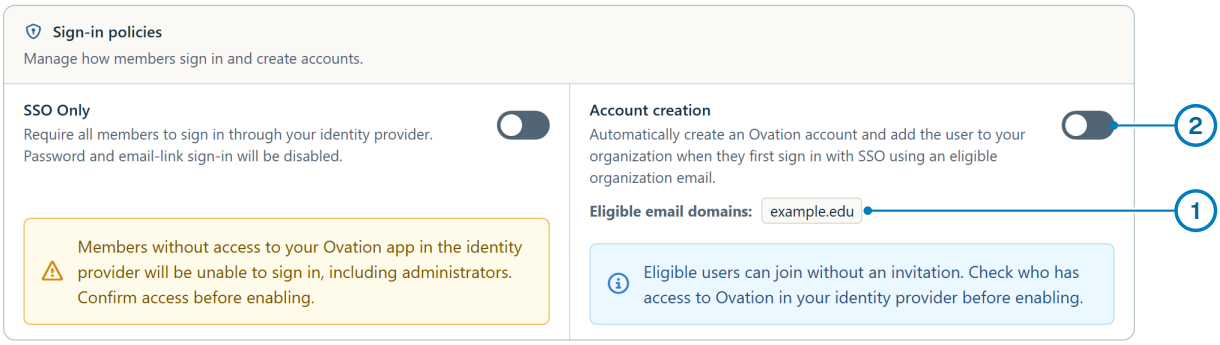
OPTIONAL

Create accounts at first sign-in (optional)

Go to **Organization › Settings › SSO › Sign-in policies**

Turn on **Account creation** when anyone your provider signs in should get an Ovation account, without your adding them first.

1. Check the domains beside **Eligible email domains**. Ovation sets this list for your organization; to add or change a domain, contact Ovation.
2. Turn on **Account creation**, then select **Allow account creation** to confirm. The switch is available once a connection is enabled and at least one domain is listed.



A new account needs an enabled connection, an email on an eligible domain, and a successful sign-in at your provider, plus **email_verified** as true with OpenID Connect. Anyone your provider lets sign in can join, so check who is assigned to the application first.

People who join this way get the **Default** role, which lets them practice but not manage anything, **Full** access, and every Ovation app, regardless of your **Member Defaults**. Before they start, a **Complete Your Account** page asks them to confirm their name and accept the EULA and Privacy Policy. Change anyone's role, access, or apps later on the Members page.

Require SSO for everyone (optional)

Go to **Organization › Settings › SSO › Sign-in policies**

SSO Only makes every member of your organization, administrators included, sign in through your identity provider.

1. Confirm both pilot people signed in through SSO, and that your own administrator account is assigned to the application in your provider.
2. Turn on **SSO Only**, then select **Enable SSO Only** to confirm.

With **SSO Only** on, the sign-in page shows only your connections. Ovation passwords, email sign-in links, and password resets stop working for your members, and anyone signed in with a password is asked to sign in again through your organization.

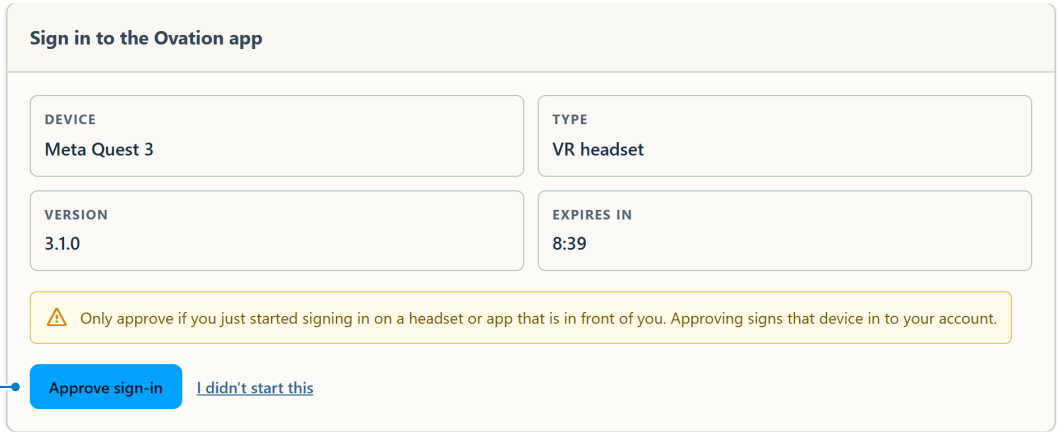
There is no password fallback, even during a provider outage. If no administrator can sign in, email support@ovationvr.com and Ovation can turn **SSO Only** off. Turning it off yourself restores passwords and email links right away.

STEP 3

Sign in to the VR and Desktop apps

The VR headset and Desktop apps send members to your provider through a browser on a phone or computer.

1. In the app, the member enters their email and chooses **Sign in with your organization**. With **SSO Only** on, this starts by itself.
2. The app shows a six-digit code. On a phone or computer, they go to ovationvr.com/sso, enter the code, and sign in through your provider.
3. They check the device details, select **Approve sign-in**, and return to the app, which finishes signing them in.



Members can also start in the browser: sign in to the Ovation portal, open **My Account** > **App Sign In**, select **Get code**, and enter that code in the app within five minutes.

Manage your connections

Edit	Rename a connection or change its provider settings. Changing an OpenID Connect issuer URL or client ID needs the current or a new client secret. To change protocol, add a new connection. A metadata file doesn't update itself: before the signing certificate date on the card, select **Replace metadata file** with a new download.
Disable	Removes the connection from the sign-in page until you select **Enable**. Ovation won't disable your last enabled connection while **SSO Only** or **Account creation** is on; turn those off first.
Delete	Removes the connection and its links to members. Members keep their accounts and their work. If no enabled connection is left, **SSO Only** turns off. SCIM connections don't change.
Add another	Add a connection for each provider application, such as one for staff and one for students. Members see every enabled connection by name, with the one they used before listed first.

If something goes wrong

What's happening	Likely cause and what to do
There is no **SSO** tab	Only your organization's administrator can open **Settings**. If that's you, contact Ovation.
No **Continue with** button after entering an email	Ovation offers SSO only to members of your organization, or with **Account creation** on, to emails on an eligible domain. Add the person, and check that the connection is **Active**.
Organization sign-in did not allow this account	Your provider refused or canceled the sign-in. Check that the person is assigned to the application and that the ACS URL and Entity ID, or redirect URI, in your provider match Ovation's.
We couldn't sign you in as jordan.lee@example.edu	Your provider returned a different email than the one entered, often because the browser is signed in to the provider as someone else. Check the **email** mapping, sign out of the provider, and try again.
Organization sign-in could not be completed	Ovation found no member to sign in: the email doesn't match an Ovation member, the member was removed, the connection is disabled, or a new account didn't meet the **Account creation** conditions.
An OpenID Connect connection doesn't create accounts	Check that your provider sends **email_verified** as true; with Microsoft Entra ID, use SAML 2.0 instead. If it does, select **Edit** on the connection card, then **Update connection**, and confirm. That applies Ovation's current settings, and you don't need the client secret.
Single sign-on could not be completed, with a reference	The sign-in took more than 10 minutes or finished in a different browser. Start again from the sign-in page, and send the reference to support if it repeats.

Need help?

For setup help, contact Ovation support with your organization, the connection name, the protocol, the affected person's email, and when it failed. Never send passwords or client secrets.