

How to Set Up Single Sign-On (SSO) in MyPressable

SAML SSO AND SCIM PROVISIONING

Single Sign-On (SSO) lets your team sign in to MyPressable through your company's SAML identity provider. Setup takes five steps, and nothing changes for your team until you turn on enforcement. SSO and SCIM provisioning are included on every Pressable plan.

- STEP 1** Copy your Pressable settings
- STEP 2** Connect your identity provider
- STEP 3** Verify your email domain
- STEP 4** Run a test login
- STEP 5** Turn on enforcement
- OPTIONAL** Connect SCIM provisioning

PROVIDER NOTES INCLUDED FOR

SAML 2.0

Okta

SAML 2.0

**Microsoft Entra
ID**

SAML 2.0

**Google
Workspace**

SAML 2.0

Auth0

START HERE

Before you start

Single Sign-On (SSO) lets your team sign in to MyPressable through your company's SAML identity provider. Setup takes five steps, and nothing changes for your team until you turn on enforcement. SSO and SCIM provisioning are included on every Pressable plan.

YOU'LL NEED

- ✓ Owner or Account Administrator access to the Pressable account, or a collaborator with the Manage Single Sign-On permission.
- ✓ Admin access to your identity provider, such as Okta, Microsoft Entra ID, Google Workspace, or Auth0.
- ✓ Access to your domain's DNS settings, so you can add a TXT record.
- ✓ Your own account in your identity provider. Once SSO is enforced, account owners sign in through it too.

IN THIS GUIDE

STEP 1	Copy your Pressable settings	Includes provider notes
STEP 2	Connect your identity provider	
STEP 3	Verify your email domain	
STEP 4	Run a test login	
STEP 5	Turn on enforcement	
OPTIONAL	Connect SCIM provisioning	
ACCESS	Letting a collaborator manage SSO	
AFTER	What changes for people who sign in with SSO	
REFERENCE	Troubleshooting and FAQ	

1 STEP 1 Copy your Pressable settings

- 1 In MyPressable, go to **Tools > Single Sign-On**. If you manage more than one account, choose the account from the account selector first.
- 2 Copy the **Entity ID** and **Assertion Consumer Service (ACS) URL** from the SSO page.
- 3 In your identity provider, create a new SAML application for Pressable and paste in the Entity ID and ACS URL. See the provider notes below.

STEP 1, CONTINUED

Provider notes

Each identity provider sends user details a little differently. The setting that matters most is the user identifier, because MyPressable matches people by their email address on first sign-in. Identity provider menus change over time, so if a path below doesn't match what you see, check your provider's documentation.

PROVIDER	WHERE TO CREATE THE APP	WHAT TO CHECK
Okta	Applications > Create App Integration > SAML 2.0	Okta sends the Okta username by default, which may not be an email. Set the application username to the user's email.
Microsoft Entra ID	Enterprise applications > New application > Create your own application, then set up single sign-on with SAML	Entra users are matched by email by default. To match on Entra's object ID instead, enter its claim name in the Stable subject attribute field. SCIM provisioning requires Entra ID P1 or P2.
Google Workspace	Admin console > Apps > Web and mobile apps > Add custom SAML app	Map the user's primary email. Google doesn't send any other attributes by default.
Auth0	Applications > create an application, then turn on the SAML2 Web App add-on	Map the user's email, and make sure emails are verified in Auth0.

OTHER SAML 2.0 PROVIDERS

Using a different SAML 2.0 identity provider? Use the same Entity ID and ACS URL, and make sure it sends each user's email address.

STEP 2

2

Connect your identity provider

- 1 On the SSO page, under **How do you want to connect?**, choose **Use a metadata URL** (recommended) or **Enter the details by hand**.
- 2 **Metadata URL:** Paste your identity provider's metadata URL into the **Metadata URL** field, then click **Save and fetch metadata**.
- 3 **By hand:** Fill in **Identity provider entity ID (issuer)**, **Sign-on URL**, and **Signing certificate**, then click **Save configuration**.

RECOMMENDED • USE A METADATA URL

Using a metadata URL is recommended. MyPressable checks it every day, so when your identity provider rotates its signing certificate, the new certificate is picked up automatically.

STEP 3

3

Verify your email domain

Verifying your domain proves you own it. SSO only applies to email addresses on domains you've verified.

- 1 On the SSO page, enter the email domain your team uses, such as **yourcompany.com**, in the **Add a domain** field and click **Claim domain**.
- 2 Copy the TXT record MyPressable shows you.
- 3 Add the TXT record in your domain's DNS settings at the apex (host @), alongside any existing TXT records.
- 4 Back on the SSO page, click **Verify**. DNS changes can take a while to appear, so try again later if it doesn't verify right away.

MORE THAN ONE DOMAIN

You can verify more than one domain if your team uses several. Each domain can only be claimed by one Pressable account. If another account has already claimed your domain, contact Pressable support.

4 STEP 4 Run a test login

A test login confirms MyPressable and your identity provider are talking to each other. It doesn't change how anyone signs in.

- 1 Make sure your own user is assigned to the Pressable app in your identity provider.
- 2 On the SSO page, click **Test login**.
- 3 Sign in with your identity provider when prompted.

PASS OR FAIL

If the test succeeds, you're ready for enforcement. If it fails, check Troubleshooting and FAQ at the end of this guide. The most common cause is the identity provider sending a username instead of an email address.

ACCESS

Letting a collaborator manage SSO

Account owners and Account Administrators can manage SSO by default. To hand setup to someone else, such as an IT or security lead, give them the **Manage Single Sign-On** permission when you add or edit them as a collaborator.

They'll then see **Tools > Single Sign-On** for your account and can complete every step in this guide.

STEP 5

5

Turn on enforcement

Enforcement is the step that changes how your team signs in. Until you turn it on, everyone keeps signing in the way they do today. People on your verified domains also see a **Continue with single sign-on** button next to the password field, so your team can try SSO before you require it.

- 1 On the SSO page, click **Check who it covers**. This opens the Collaborators tab, where the **Who enforcement will cover** card shows who enforcement will affect and which collaborators are outside your verified domains.
- 2 Make sure everyone it lists is assigned to the Pressable app in your identity provider, including yourself.
- 3 Click **Enable enforcement**. You can click **Turn enforcement off** on the same page at any time.

ONCE ENFORCEMENT IS ON

Once enforcement is on, everyone on your verified domains signs in through your identity provider, and other sign-in methods are turned off for them. This includes the account owner.

WHAT THIS VIEW CAN'T SEE

Who enforcement will cover only shows your collaborators. It can't see everyone on your domain, and it can't confirm each person has an account in your identity provider. Connection status on the SSO page shows where setup stands at any time.

OPTIONAL

Connect SCIM provisioning

SCIM keeps MyPressable in sync with your identity provider. When you add someone there, SCIM creates their MyPressable account. When you deactivate someone, their SSO sign-in is blocked and their active sessions and API access end. If enforcement is on, they can no longer sign in to MyPressable at all. If it isn't, they can still sign in with a password, passkey, or social login. Either way, they stay on your collaborator list until you remove them in MyPressable.

- 1 On the SSO page, find the **Directory synchronization (SCIM)** section and generate a token.
- 2 **Copy the token right away.** It's shown only once. If you lose it, rotate it to get a new one.
- 3 In your identity provider, turn on provisioning for the Pressable app and paste in the SCIM URL and token.
- 4 Assign the people and groups who should have MyPressable accounts.

ACCOUNTS, NOT SITE ACCESS

SCIM creates accounts, but it doesn't grant access to sites. After someone is provisioned, an account owner gives them access through collaborator roles.

AFTER ENFORCEMENT

What changes for people who sign in with SSO

Signing in

They enter their work email on the MyPressable login page and are sent to your identity provider. Passwords, passkeys, and GitHub, Google, or WordPress.com login stop working for them.

Two-factor authentication

Your identity provider handles MFA. MyPressable's own two-factor prompt doesn't apply to SSO users.

Passwords and email

SSO users don't have a MyPressable password to change, and they can't change their own email address. Make those changes in your identity provider.

Account cancellations and site transfers

Before canceling an account or transferring a site, SSO users sign in through your identity provider again to confirm.

Access to sites

SSO controls how people sign in. What each person can access is still set with collaborator roles.

New team members

Someone new needs an invitation or SCIM provisioning before they can sign in. Signing in through SSO alone won't create an account. They'll see a message asking them to contact their administrator. People who already have a MyPressable account can sign in with SSO right away.

Collaborators on other domains

Enforcement only applies to your verified domains. A contractor using their own company email keeps signing in as they do today.

REFERENCE

Troubleshooting and FAQ

The test login fails and no user is matched.

Your identity provider is probably sending a username instead of an email address. In Okta, set the application username to the user's email. In other providers, check that the user's email is mapped.

My domain won't verify.

DNS changes can take time to appear. Check that the TXT record was added at the apex (host @) of the right domain and that the value matches exactly, then click **Verify** again.

A team member sees "contact your administrator."

They don't have a MyPressable account yet. Invite them as a collaborator, or assign them to the Pressable app in your identity provider if SCIM is connected.

I got a certificate expiration notice.

Once SSO is enforced, the account owner and anyone who manages SSO get an email before a certificate expires. If you connected with a metadata URL, MyPressable picks up the new certificate once your identity provider publishes it. If you entered details manually, paste in the new certificate on the SSO page.

SUPPORTED FEATURES

Do you support Single Logout or encrypted SAML assertions?

No. Assertions must be signed and are sent over HTTPS. To cut off someone's sign-in, turn on enforcement and deactivate them in your identity provider with SCIM connected. To remove their collaborator access, remove them in MyPressable.

Can I map identity provider groups to collaborator roles?

Not today. Use collaborator roles in MyPressable to set what each person can access.

LOCKED OUT

I'm locked out after turning on enforcement.

Contact Pressable support. Our team can restore access to your account. If your identity provider goes down, support can turn enforcement off.

