Set up SAML SSO in Vertice with your identity provider

What is SSO?

Single Sign-On (SSO) allows your team to sign in through an identity provider (IdP) using one set of credentials. With SSO, employees can access multiple applications, including Vertice, without needing to manage separate usernames and passwords.

Enabling SSO for your organisation makes it easier to:

- Centralise authentication and reduce password fatigue.
- Minimise the risk of security breaches caused by weak or reused passwords.
- Simplify onboarding and offboarding by allowing access to be granted or removed from one central place.

Follow the steps in this article to configure your identity provider and enable SSO in Vertice.

Supported identity providers

Vertice supports SAML-based SSO with the following identity providers:

- Okta
- Microsoft Entra ID
- OneLogin
- JumpCloud
- Google
- Auth0

Before you begin

Make sure you have the following permissions:

- Admin or security permissions in your identity provider

- Admin access to Vertice

Step 1: Enable SAML SSO in Vertice

First, you need to enable SAML SSO in your Vertice integrations to get the configuration details for your identity provider.

1. Navigate to **Settings > Integrations > Security.**
2. Select **SAML Single Sign-On** and click **Set Up**.
3. The **Application Callback URL** and **SAML configuration JSON** will be displayed. Copy both values; you will need them for your IdP configuration.

Step 2: Configure your identity provider (IdP)

In your identity provider's settings, you need to add Vertice as a new SAML application. You will need the **Application Callback URL** from Step 1.

1. Log into your identity provider's admin panel.
2. Create a new SAML 2.0 application (e.g., "Vertice SSO").
3. Map the following user attributes in your IdP configuration:

Attribute	Value in IdP
user_id	user.id
email	user.email
name	user.firstName + lastName
given_name	user.firstName
family_name	user.lastName

4. Download the **metadata XML file** from your identity provider.

Note: Configuration steps may vary depending on your identity provider. Refer to your IdP's documentation if needed.

Step 3: Upload your SAML metadata to Vertice

After configuring your IdP, you need to upload the metadata file to Vertice.

1. Return to the Vertice SAML SSO settings page (Settings > Integrations > Security).
2. Click **Upload your SAML Metadata**.
3. Select the metadata file, then click **Upload File** and **Next**.

Step 4: Register your SSO domain

Next, register the email domain used by your organisation.

1. Enter your company's email domain (e.g., `yourcompany.com`).
2. Click **Add Domain**, then click **Next.**

Note: Enter the domain only, without the @ symbol. If your domain is rejected, verify your registration settings with your IT team.

Step 5: Migrate and invite users

The final step is to move your existing users over to SSO authentication.

Note: You can skip this step if you are not ready to migrate users yet.

1. Review the list of existing users.
2. Select the users you want to migrate to SSO authentication.
3. Click **Invite Selected**, then click **Done.**

Troubleshooting

I do not have admin access to our identity provider

If you cannot access your identity provider (such as Okta), ask your IT or security team to configure the SAML application using the **Application Callback URL** and **SAML configuration JSON** provided by Vertice in Step 1.

My domain was rejected when I tried to add it

Make sure you are entering just the domain, without the @ symbol.

- Correct: `yourcompany.com`
- Incorrect: `@yourcompany.com`

If the issue persists, contact your IT team or reach out to Vertice support.

How do I update my SSO configuration after setup?

You can edit your configuration at any time. Go to **Settings > Integrations > Security > SAML Single Sign-On** and click **Edit Config**.

FAQs

Does Vertice support automatic user provisioning?

Yes. Vertice supports SCIM provisioning for Okta, OneLogin, JumpCloud, and Microsoft Entra ID. To enable this, go to **Settings > Integrations > Security** and click the **SCIM User Provisioning** tile.

Can users log in to Vertice directly from their identity provider dashboard?

Yes. To set this up, paste the **Relay State** value provided by Vertice into your identity provider's SAML configuration. This allows your team to launch Vertice directly from their identity provider dashboard without needing to sign in separately.

For the Reviewer

What I chose to do

- Updated the introduction to make it clearer what SSO is, while keeping the core message from the original.
- Added a “Supported identity providers” section so readers can confirm their IdP before starting.
- Added a “Before you begin” section to state prerequisites.
- Added a short intro sentence for each step to provide context.
- Moved the Application Callback URL and SAML configuration JSON from Step 2 to Step 1, as they are generated when SAML SSO is first enabled in Vertice.
- Moved the metadata XML download from Step 3 to Step 2 so that all identity provider configuration steps are grouped together before returning to Vertice.
- Added notes where needed, such as the domain format warning and the option to skip user migration.
- Split Troubleshooting and FAQs into separate sections. The troubleshooting section focuses on common issues written as problem statements, while the FAQ section answers general questions about the feature.
- Removed the line encouraging users to consult external IdP documentation, as it weakened the article, and instead added a note acknowledging that configuration steps may vary by identity provider.
- Used a slightly warmer, user-focused tone, referring directly to the reader (“you”) to make the guide feel more approachable and easier to follow.