CUSTOMER INTAKE FORM

Single Sign-On (SSO) Customer Intake Form

Thank you for your interest in setting up Single Sign-On (SSO) for Videri Portal. Please complete this form together with your identity provider (IdP) administrator — several fields require technical details only they can provide — and return it to your Videri account team.

Videri supports SSO with any identity provider that can federate via SAML 2.0 or OIDC, including Okta, Azure AD / Microsoft Entra ID, Google Workspace, OneLogin, PingFederate, and ADFS.

1 Organization details

Company name	
Primary Videri account contact	
Email domain(s) your employees sign in with (list every domain, e.g. acmecorp.com ; include secondary domains like acme-eu.com if applicable)	
Target go-live date	

2 Identity provider details

Which identity provider do you use? (e.g. Okta, Azure AD / Microsoft Entra ID, Google Workspace, OneLogin, PingFederate, ADFS, other)	
Protocol	☐ SAML 2.0 ☐ OIDC
IdP administrator name and email (the technical contact who can generate the items in Section 3)	

3 Required technical items (from your IdP administrator)

We cannot begin configuration without the items below. Please route this section to your IdP administrator directly.

If you selected SAML 2.0:

SAML metadata XML file, or a metadata URL that always serves the current version	

This file contains your IdP's signing certificate, SSO URL, and entity ID — it's typically available for download directly from your IdP admin console under your SAML application's settings.

If you selected OIDC:

OIDC discovery / issuer URL	
Client ID	
Client secret	

Your IdP administrator will need to register "Videri Portal" as an application/integration inside your IdP first, in order to generate these credentials.

Do not paste your client secret or any private key material into this document. Once you have the above, contact your Videri account team and they will share a secure channel for transmitting credentials.

4 Attribute mapping

We need to know which claim/attribute in the token your IdP sends us carries the user's email address — this is what we use to match the signed-in user to their Videri account.

Videri attribute	Our standard default claim	Your IdP's claim name (if different)
email	`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` (SAML) or the standard email claim (OIDC)	

Most enterprise IdPs (including ADFS and Azure AD / Entra ID) emit the default SAML claim above out of the box. Please confirm with your IdP administrator that your configuration sends it, or provide the actual claim name/URI you use instead.

5 A few more questions

Is this email domain shared with another company, agency, or sub-brand that might also use Videri?	
If yes: what display name should we show your users if they need to pick your organization from a list?	
Do any of your users currently sign in to Videri Portal with a password today?	

Note: enabling SSO does not disable password login for your organization — both will work side by side unless you've discussed a different requirement with your account team.

What happens next

1. Return this completed form to your Videri account team.
2. Our engineering team will configure your organization using the details provided and confirm attribute mapping with your IdP administrator.
3. We'll coordinate a test login with you in a non-production environment before going live.
4. Your account team will confirm an estimated timeline once this form is complete — the most common delay is waiting on your IdP administrator to generate the Section 3 items, so the sooner that's done, the sooner we can start.

Questions at any point? Contact your Videri account team.