Ciphr HR Sign-In

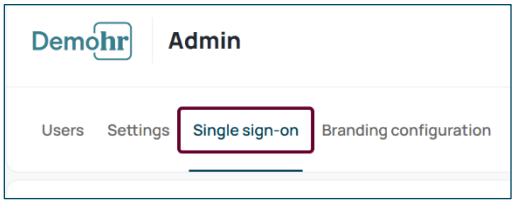
SAML configuration for SSO

12 February 2025 | V1.0

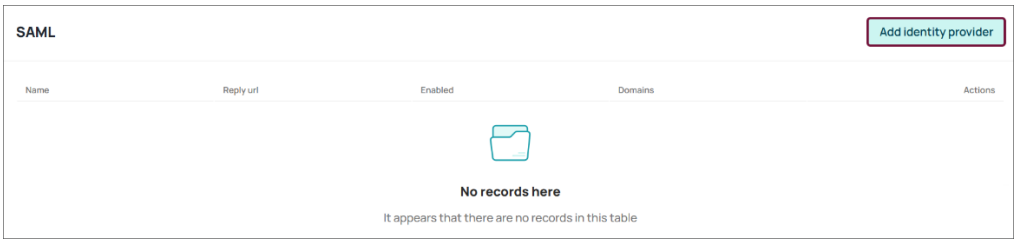
Ciphr Limited
3rd Floor, 33 Blagrave Street, Reading, RG1 1PW | +44 (0)1628 814000 | info@ciphr.com | ciphr.com

How to set up SAML configuration for SSO

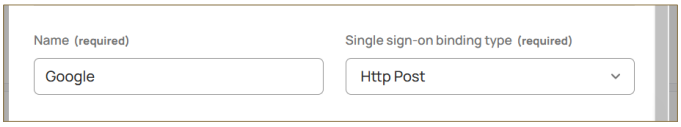
1. Click on the **Single Sign On** tab in Ciphr Sign-In



2. To add a new identity provider, under SAML click **Add identity provider**

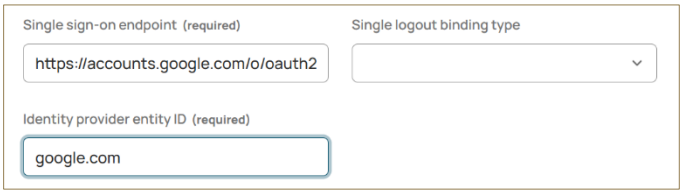


3. Add a **Name** (this is for your reference only) ie Google. Adding this will also update the **Reply url**, which is a piece of information required by the **identity provider**. This is the location where the authentication server sends the user once they have successfully been authorised

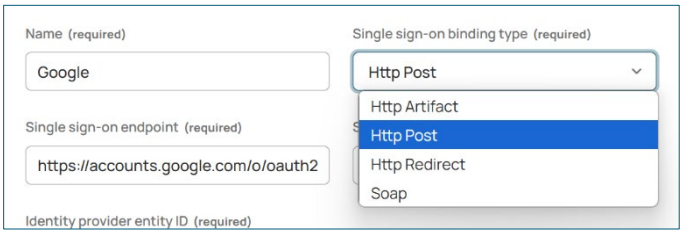


4. Add your **Single sign on endpoint** from your identity provider's configuration. This is a specific URL where authentication requests and responses are sent between an identity provider and a service provider to enable secure user login

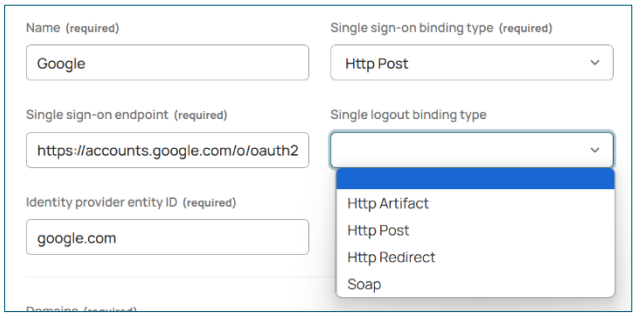
5. Next, add your **Identity provider entity ID** from your provider's configuration. This is a unique identifier (often a URL or string) that distinguishes the identity provider in SSO configurations and ensures the service provider knows which IdP to trust for authentication



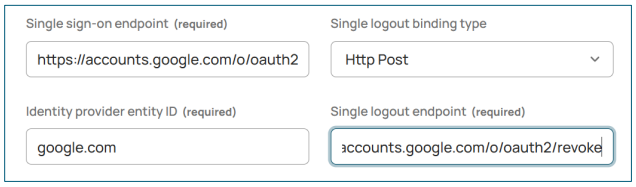
6. Select the **Single sign-on binding type** required. This refers to the methods used to send and receive authentication messages between the identity provider and the service provider:
    a. **HTTP Artifact**: Sends references via the browser
    b. **HTTP Redirect**: Sends messages in URLs
    c. **HTTP POST**: Sends messages in form data, which is often a typical configuration
    d. **SOAP**: Direct, server-to-server communication for sensitive operations



7. If you wish to log out from the identity provider, ie Google, when logging out from Ciphr, select your **Single logout binding type** as required:
    a. **HTTP Artifact**: Sends a reference to retrieve the logout message securely
    b. **HTTP POST**: Sends logout messages via form submission
    c. **HTTP Redirect**: Sends logout messages via URL
    d. **SOAP**: Uses direct server-to-server communication



8. Next, add your **Single logout endpoint.** This is a URL provided by an identity provider or service provider where logout requests and responses are sent to ensure all connected systems log out a user simultaneously

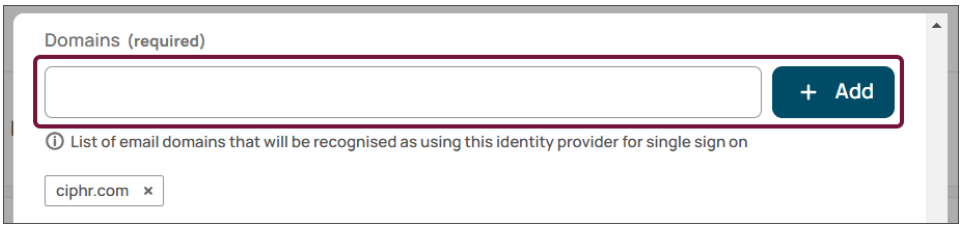


9. Your identity provider will need the **Entity ID** and **Reply URL** in order to complete the setup. You can use the copy buttons and paste them in the relevant sections of the identity provider configuration.

   The **Entity ID** uniquely identifies an identity provider or service provider. It is used to establish trust between entities and ensure assertions are exchanged with the correct party. The Reply URL tells your identity provider where to send the assertions

10. Next, add the recognised domains associated with the identity provider for SSO. Ciphr recognises which identity provider to redirect a user to by that user's email address. Enter any email domains that should be associated with this identity provider

11. Use the **+Add** button to add multiple domains



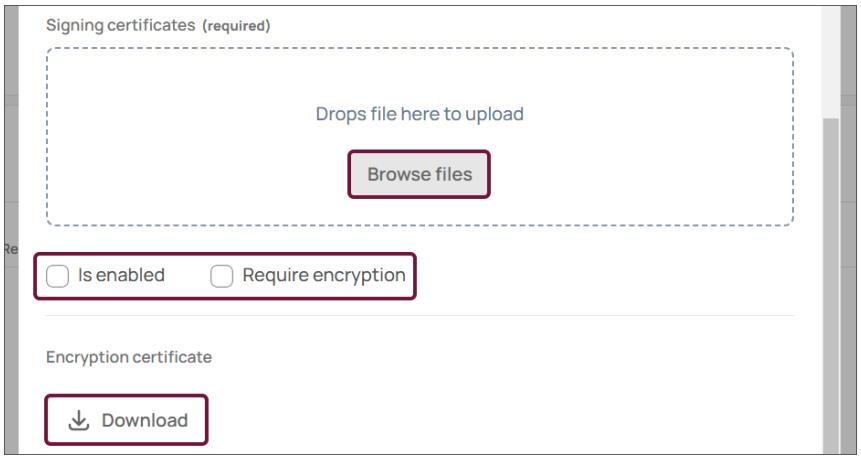
12. Obtain the public certificate generated by the identity provider and upload it by clicking on the **Browse** files button

13. Select **Is enabled** to activate the configuration. Once activated, users logging in with an email from a previously configured domain will no longer be able to access the system using a username and password.

    To ensure the setup works correctly, it's good practice to have someone else test it. This allows the person who configured it to disable or modify the settings if necessary

14. If **Require encryption** is enabled, Ciphr Sign-In will require all assertions sent from the identity provider to be encrypted using the encryption certificate available for download below. This is typically used to protect sensitive information within the assertion. However, most setups may not require this level of encryption, as all requests are already transmitted securely over HTTPS

15. If your identity provider requires an encryption certificate for setup, you can download it using the download button. Once downloaded, upload the certificate to your identity provider and then delete it from your local machine for security



16. This is now available to upload to the provider's service

17. Click **Submit** to save your SAML configuration

By following these steps, you'll have successfully configured SAML for SSO