# Setting Up SAML SSO Between Confluent Cloud and Azure AD

The IXCC team is currently conducting a Proof of Concept (PoC) with Confluent Cloud and aims to evaluate Single Sign-On (SSO) capabilities using the Security Assertion Markup Language (SAML). To facilitate this, collaboration with the Azure team is essential to configure Azure groups, establish required principal accounts, and set up SAML.

To proceed with the SSO setup in Confluent Cloud, we require specific information from the Azure team. This includes:

**Upload Signing Certificate**:

Provide the signing certificate and ensure it is uploaded successfully.

**SAML Sign-On URL**:

Specify the Identity Provider sign-on URL that must be accessible by users' web browsers.

**Email Mapping**:

We need email address in the claims to authenticate user.

We would also like to enable MFA.

By obtaining these details, we can seamlessly configure the SSO integration between Confluent Cloud and Azure AD, streamlining user authentication for a more efficient and secure user experience.