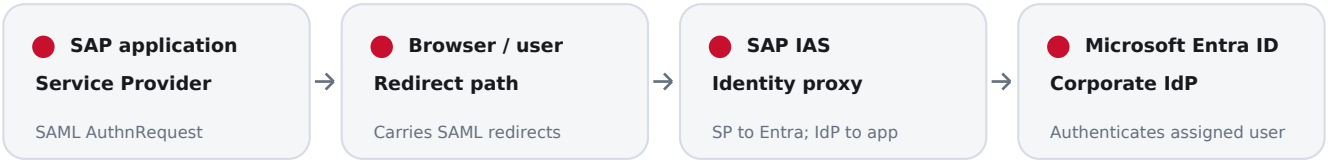
SAP SSO Trust Model: IAS and Entra ID

IAS acts as proxy IdP to the SAP application and SAML SP to the corporate identity provider.

Authentication and trust flow



Configuration sequence

1 DEFINE

Confirm SAP application, user population, login flow, identifier and environment scope.

2 CONFIGURE IAS

Set up the application trust and add Microsoft Entra ID as the corporate IdP.

3 CONFIGURE ENTRA

Import IAS metadata; set the SAML reply URL, identifier, claims and pilot assignment.

4 VALIDATE

Test SSO end to end; review Entra sign-in logs, IAS traces and application access.

Technical coverage

AREA	CONFIGURATION / CHECK	EVIDENCE / VALIDATION
Metadata and trust	Match IAS SP metadata, Entra IdP metadata, issuer/entity ID, ACS/reply URL and audience.	Metadata files and SAML response values
User identity	Agree NameID source/format and map only application-required attributes such as email or name.	Entra Attributes & Claims and IAS user mapping
IAS proxy routing	Trust the corporate IdP and select the appropriate default or conditional authentication flow.	IAS application settings and corporate IdP trust
Certificates	Track Entra signing certificate validity, metadata refresh and coordinated rollover steps.	Certificate status, expiry date and trust validation
Access assignment	Assign pilot users/groups and verify matching SAP application accounts and entitlements.	Entra assignment and application user lookup

Operational note: SAML endpoints, identifiers, NameID formats and claims are application-specific. Confirm values from current SAP application metadata and the Entra enterprise app before testing.