Technical Deployment Guide
Setting up Single Sign-on for Kinly Cloud

Kinly

kinly.com

Technical Deployment Guide
Setting up Single Sign-on for Kinly Cloud

Table of Contents

Legal Disclaimer

The specification and information regarding the products in this Technical Deployment Guide are subject to change without notice. All statements, information and recommendations are believed to be accurate but are presented without warranty of any kind. Users must take full responsibility for their application of any products. All use of the trial- or paid services, and associated software are conditioned upon the compliance with, and acceptance of our terms of service.

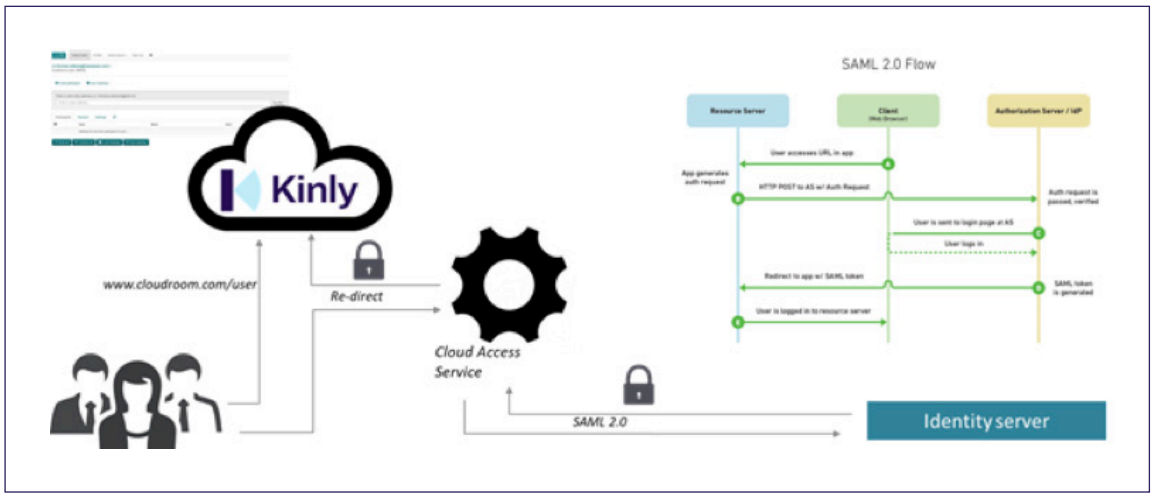
Technical Deployment Guide
Setting up Single Sign-on for Kinly Cloud

1 Purpose of this document

The purpose of this document is to guide you through setting up Single Sign-on for Kinly Cloud.

2 SAML 2.0 / Single Sign-on (SSO)

Kinly Cloud supports SAML 2.0 ad-hoc user activation and will establish a trusted link between Kinly Cloud and the customer, utilizing authentication on the customer side. This allows for single sign-on for the end users. Using SAML means all user authorization and authentication is done locally at the customer end, and no sensitive user data is sent to Kinly Cloud.



To access SSO, you need to have a SAML 2.0-compliant authentication source, for example Azure AD.

You will then need to agree with Kinly what which data we will receive.

This can be:

a. LDAP Attribute: **E-Mail-Addresses**, Outgoing Claim Type: **E-mail Address (mandatory)**
b. LDAP Attribute: **Given-Name**, Outgoing Claim Type: **Given Name (mandatory)**
c. LDAP Attribute: **Surname**, Outgoing Claim Type: **Surname (mandatory)**
d. LDAP Attribute: **mobile-number**, Outgoing Claim Type: **mobile (optional)**
e. LDAP Attribute: **location**, Outgoing Claim Type: **office location (optional)**
f. LDAP Attribute: **role**, Outgoing Claim Type: **employee role (optional)**

Communication between SSO and Kinly will use SHA 256 encryption algorithm

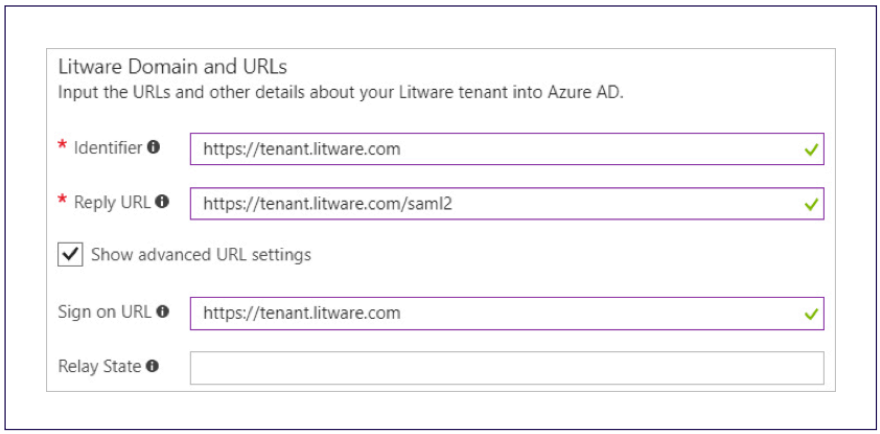
In order to set up SSO the Customer needs to provide Kinly with an AD test user.
This is for setup and testing purposes only, and the user can be disabled after completed setup.

You will be required to supply Kinly with the App Federation Metadata.

Technical Deployment Guide
Setting up Single Sign-on for Kinly Cloud

2 SAML 2.0 / Single Sign-on (SSO)

(Example from Azure AD).



Identifier (Entity ID): https://meet.<customerdomain>.com/saml2/metadata/

Reply URL (Assertion Consumer Service URL): https://meet.<customerdomain>.com/saml2/acs/

Sign on URL: https://meet.<customerdomain>.com

).