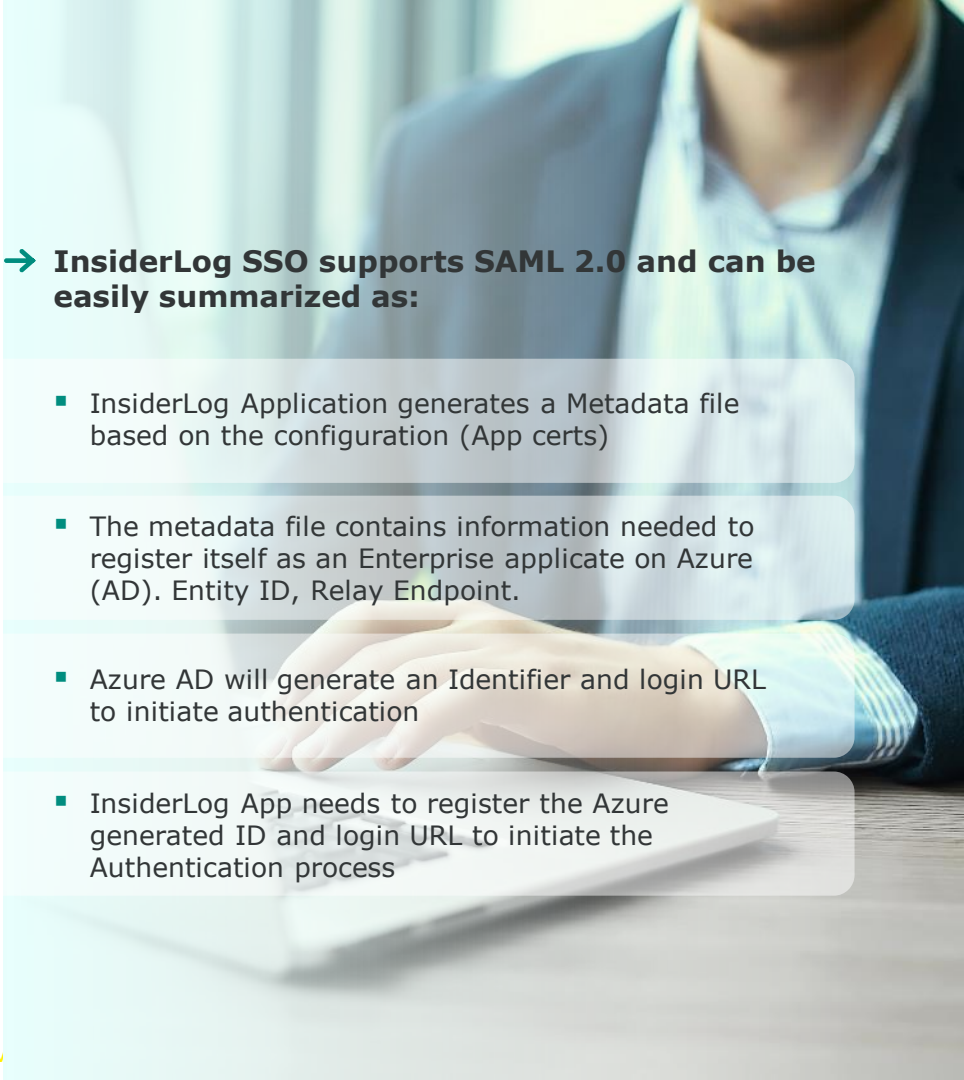
Insiderlog SSO Azure

(Step by Step Guide)

COMPLYLOG
A EURONEXT COMPANY

Basic concepts

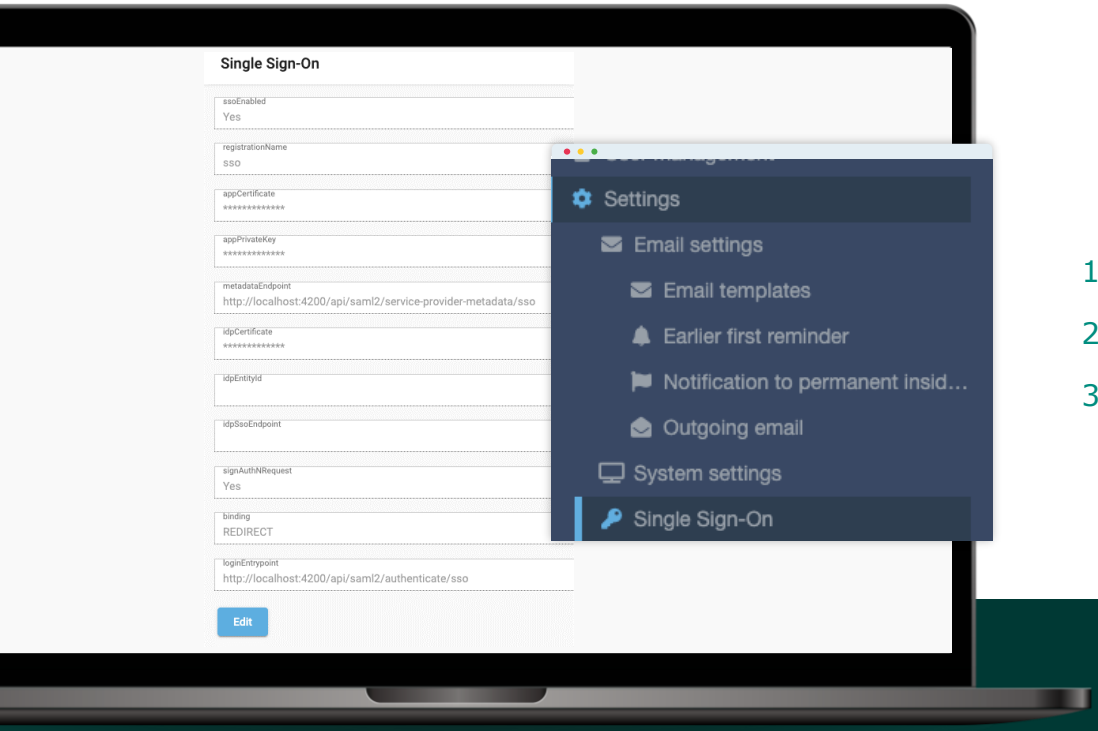
- InsiderLog SSO does not onboard users from any IDP. Users from Azure AD must be pre-onboarded with InsiderLog and assigned in the IDP as users.
  - SSO authentication works by mapping existing users from the AD IDP with the User base of the InsiderLog tenant.
- InsiderLog's SSO is owned by the application owner. ComplyLog does not have access to the application certificates nor the configurations from InsiderLog nor your IDP. Meaning it is self managed by the InsiderLog's admins.
- InsiderLog SSO supports SAML 2.0 and can be easily summarized as:



- **InsiderLog SSO supports SAML 2.0 and can be easily summarized as:**
  - InsiderLog Application generates a Metadata file based on the configuration (App certs)
  - The metadata file contains information needed to register itself as an Enterprise applicate on Azure (AD). Entity ID, Relay Endpoint.
  - Azure AD will generate an Identifier and login URL to initiate authentication
  - InsiderLog App needs to register the Azure generated ID and login URL to initiate the Authentication process

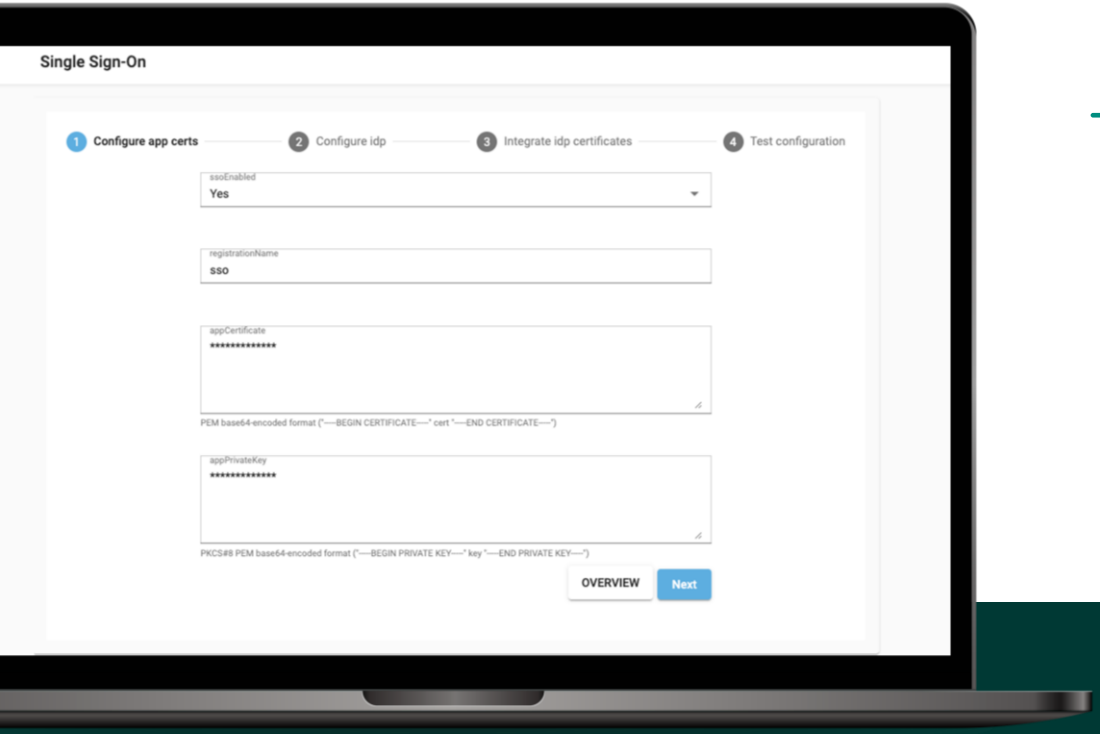
COMPLYLOG
A EURONEXT COMPANY

Step 1: Open SSO configuration



1. Log in to <mycompany>.insider-log.com
2. Click on Settings – Single Sign-on
3. Edit

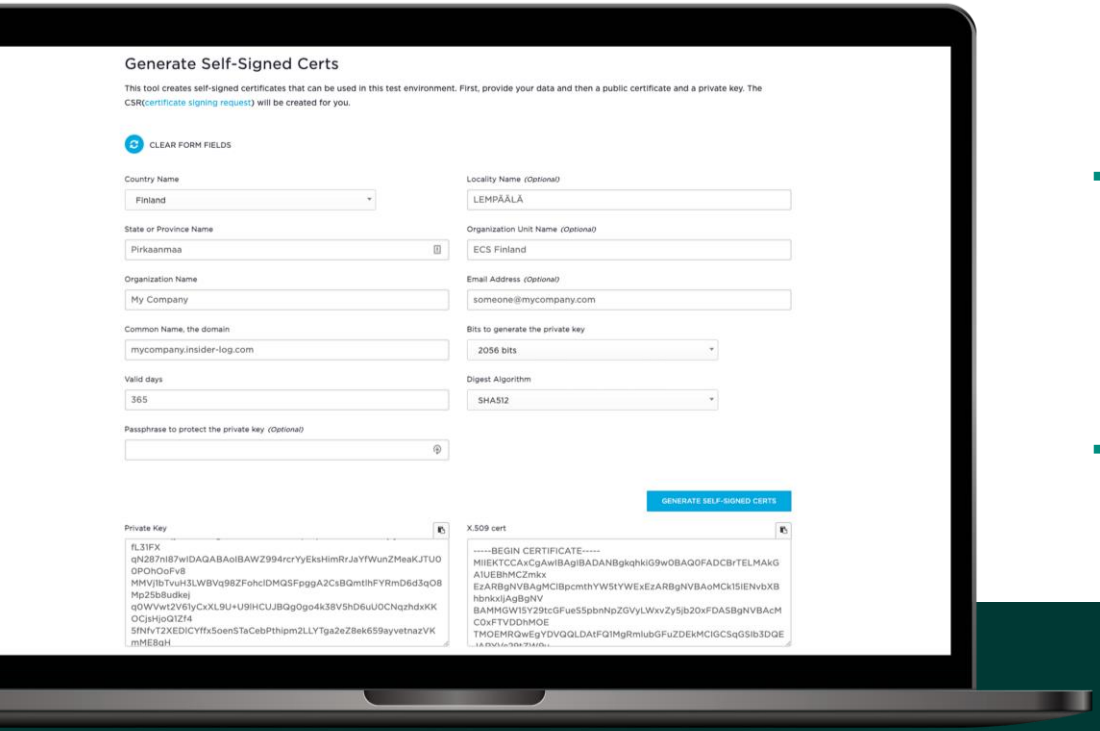
Step 1: Open SSO configuration



→ **You should see a form requesting:**

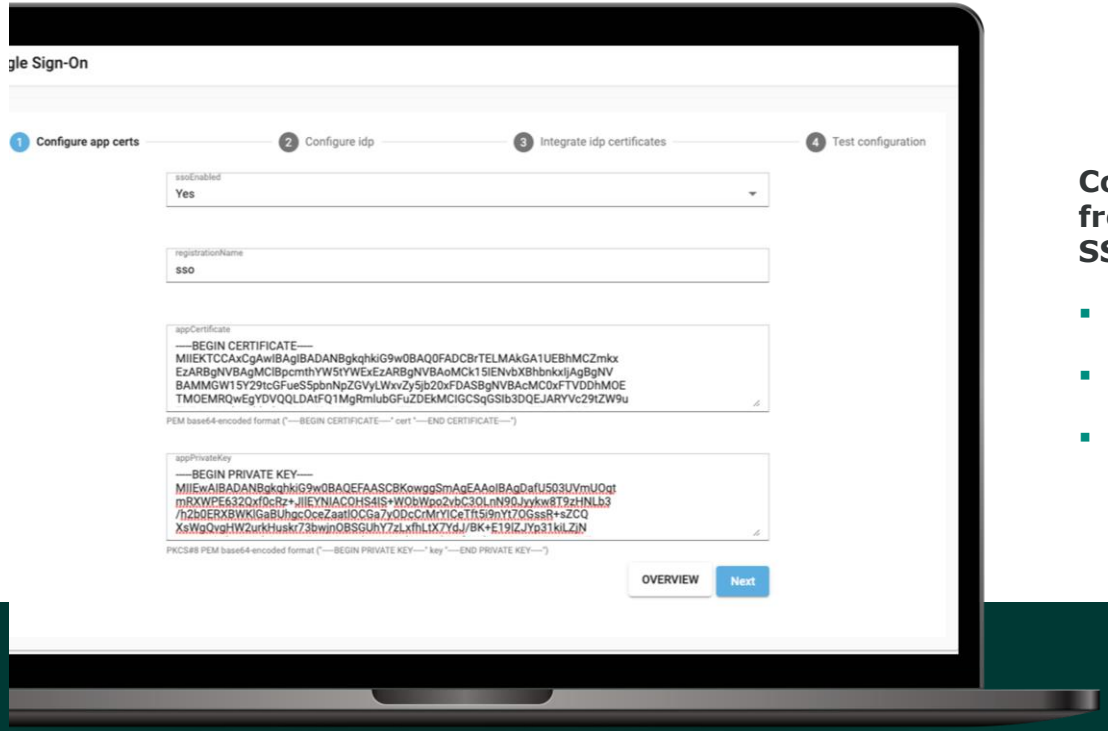
- Enable SSO access
- Registration name: reflects on the metadata EntityId and endpoints. Can remain as "SSO" by default.
- App certificate: PEM base64-encoded format
- App Private key: PKCS#8 PEM base64-encoded format

Step 2: Generate certificates



- As long as the certificates are generated in the right format PEM and PKCS#8 PEM base64-encoded. One can use any tool to generate this certificates. For simplicity we will use https://www.samltool.com/self_signed_certs.php
- Fill the form and Generate.

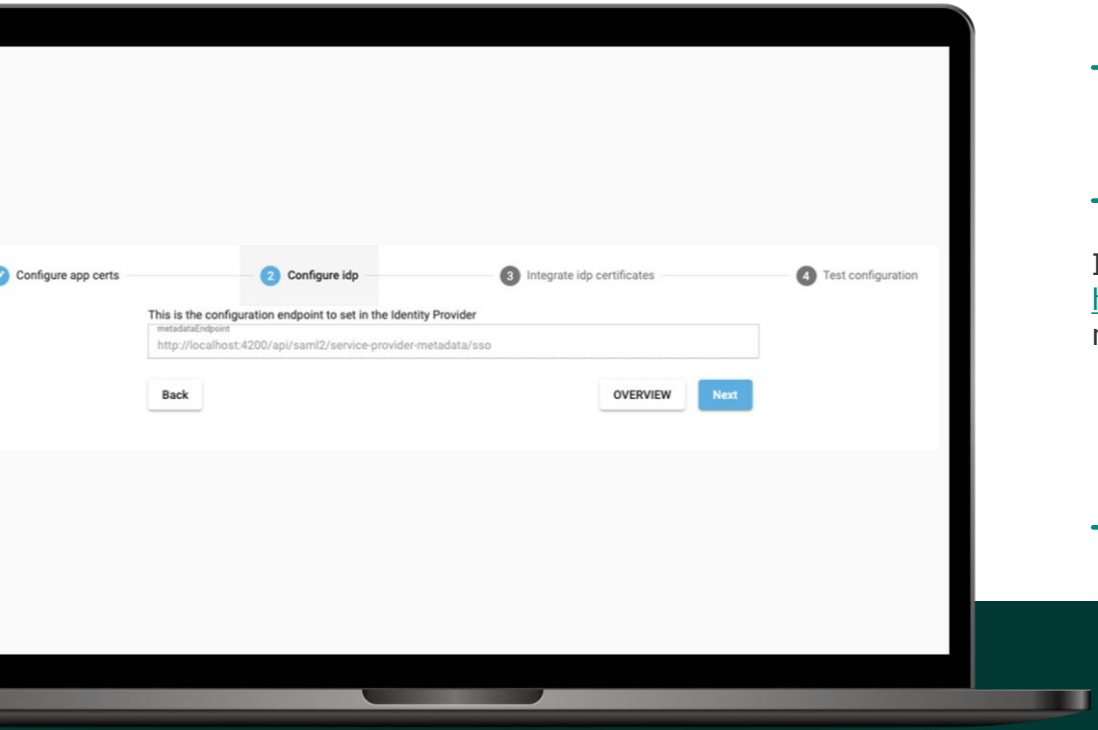
Step 3: Configure certificates



Copy the certificates and private keys from the previous steps into InsiderLog SSO configuration:

- Private key is the App private key
- X.509 cert is the App certificate
- Click Next

Step 3.1: Configure certificates



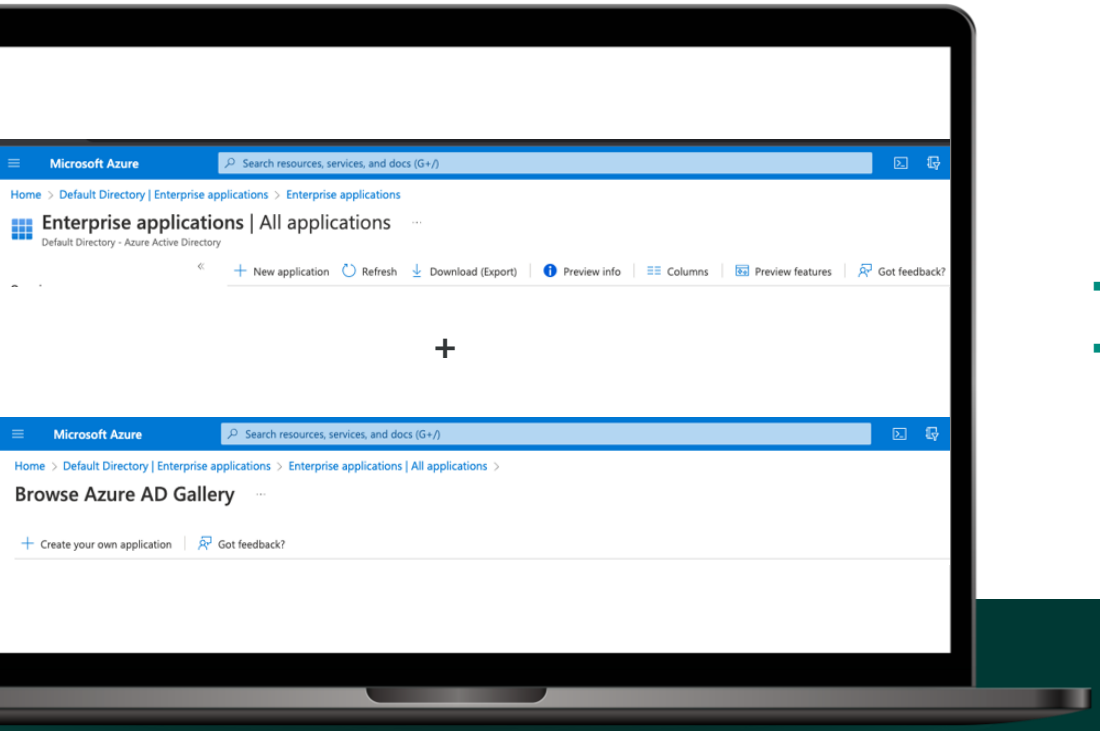
- The next step in the SSO configuration shows the application generated Metadata.
- **Save the link**

If your domain is https://mycompany.insider-log.com, The metadata endpoint will be:

  - https://mycompany.insider-log.com/api/saml2/service-provider-metadata/sso

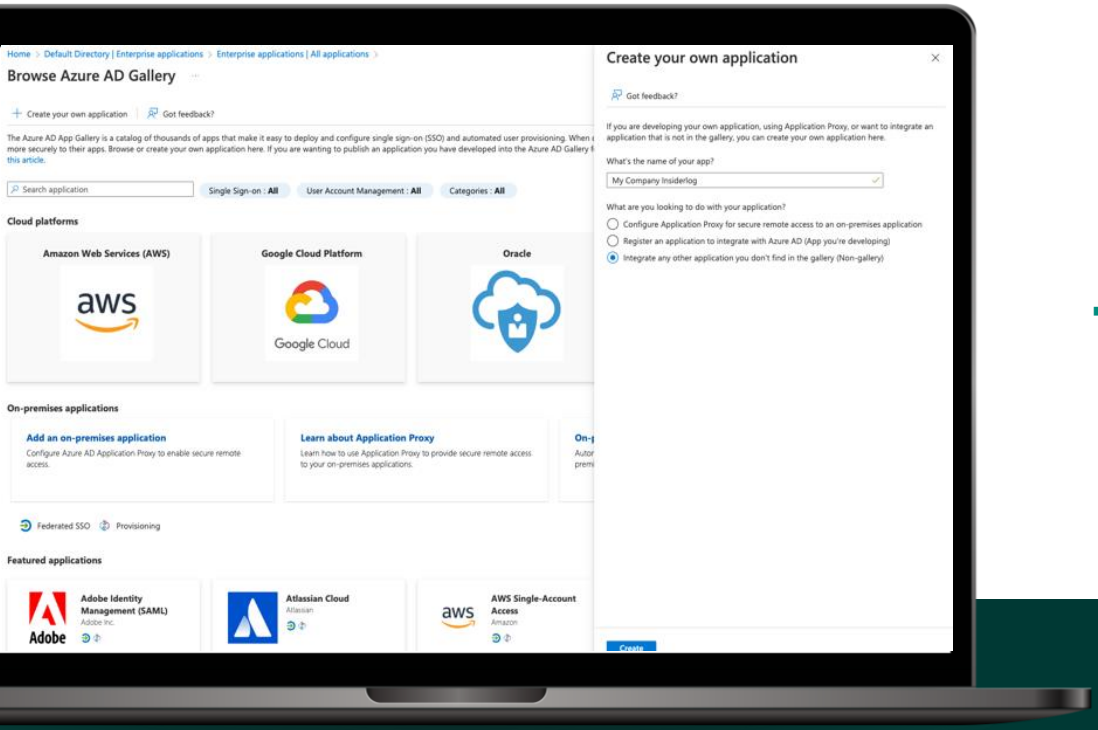
- **Click next**

Step 4.1: Configure Active Directory



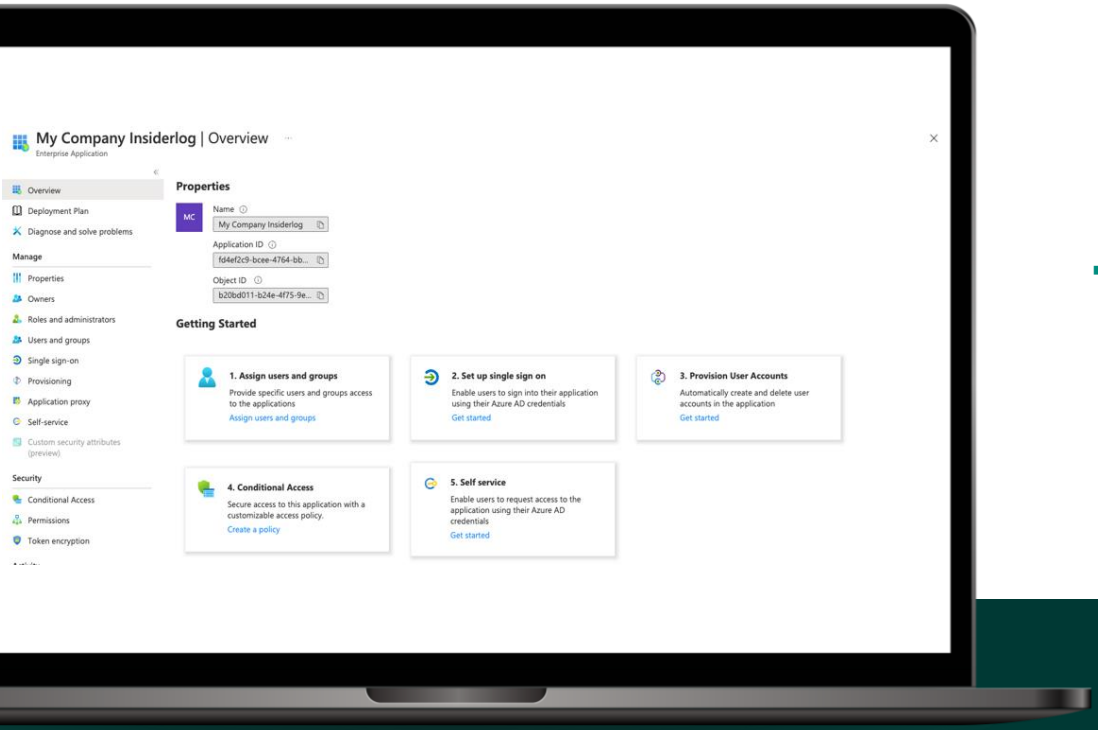
- Create "+ New application"
- Create "+ Create your own application"

Step 4.2: Configure Active Directory



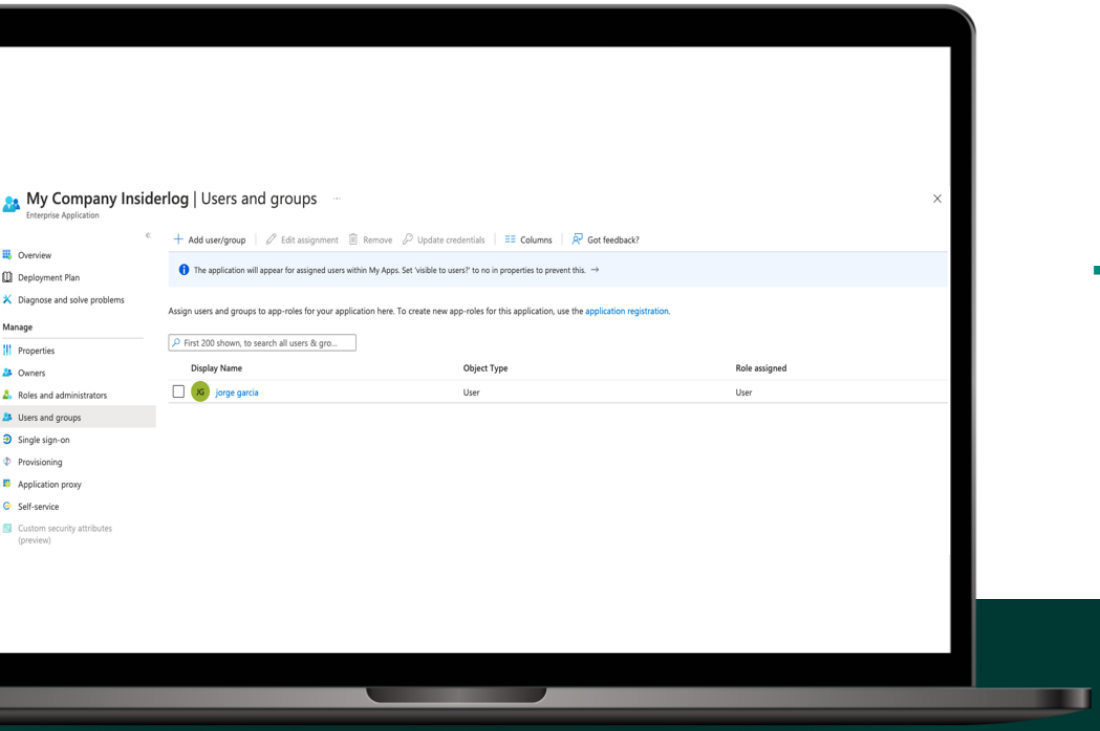
- Name the application and click create

Step 4.3: Configure Active Directory



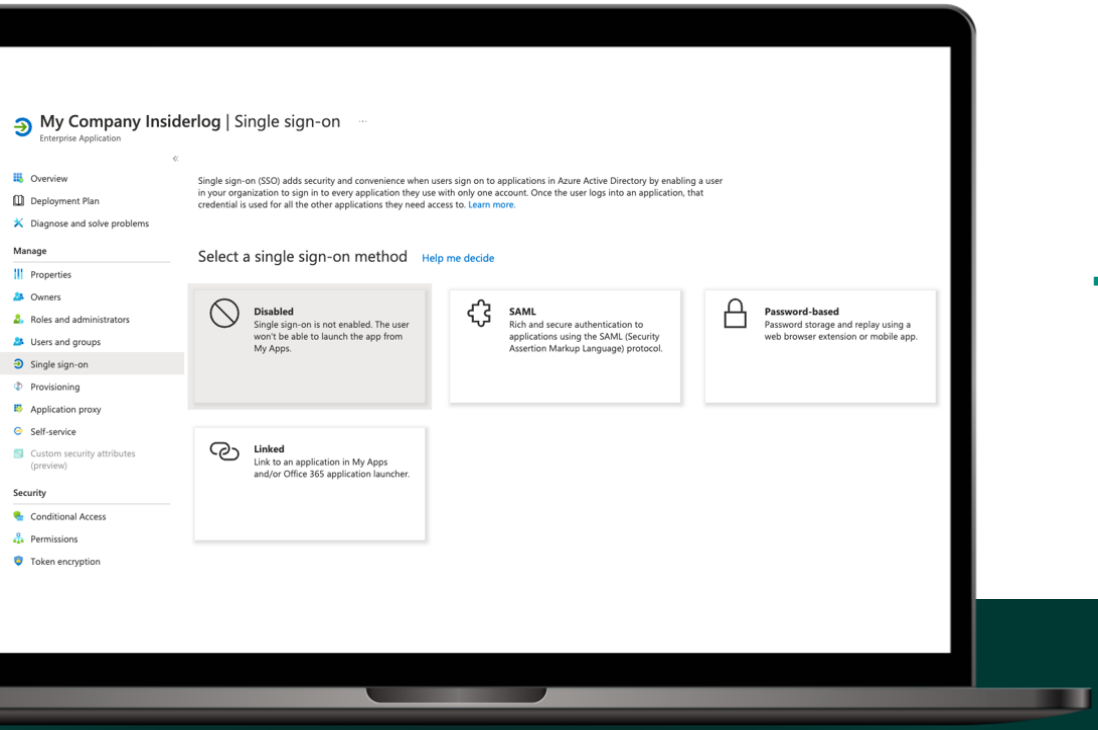
- Configure the owners, Roles and administrators and Users and groups according to your organization needs

Step 4.4: Configure IDP



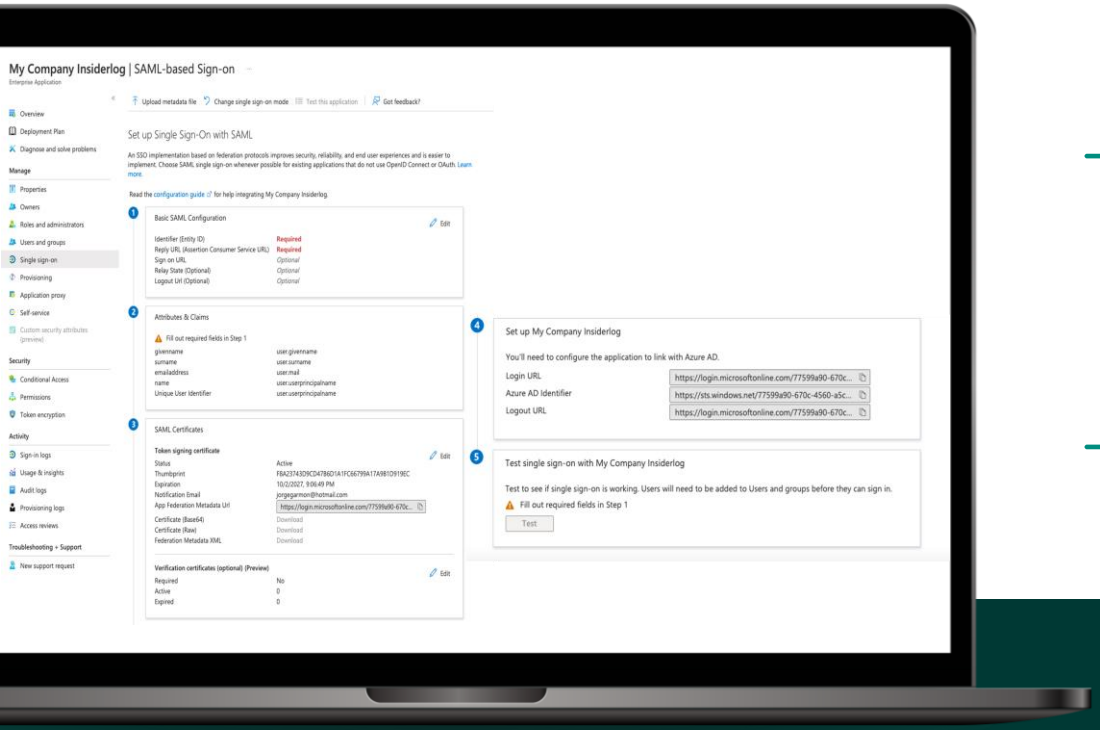
- It is important that the users assigned to this Enterprise App match the Admins configured in InsiderLog. Specially the Email.

Step 5: Configure Azure AD SSO



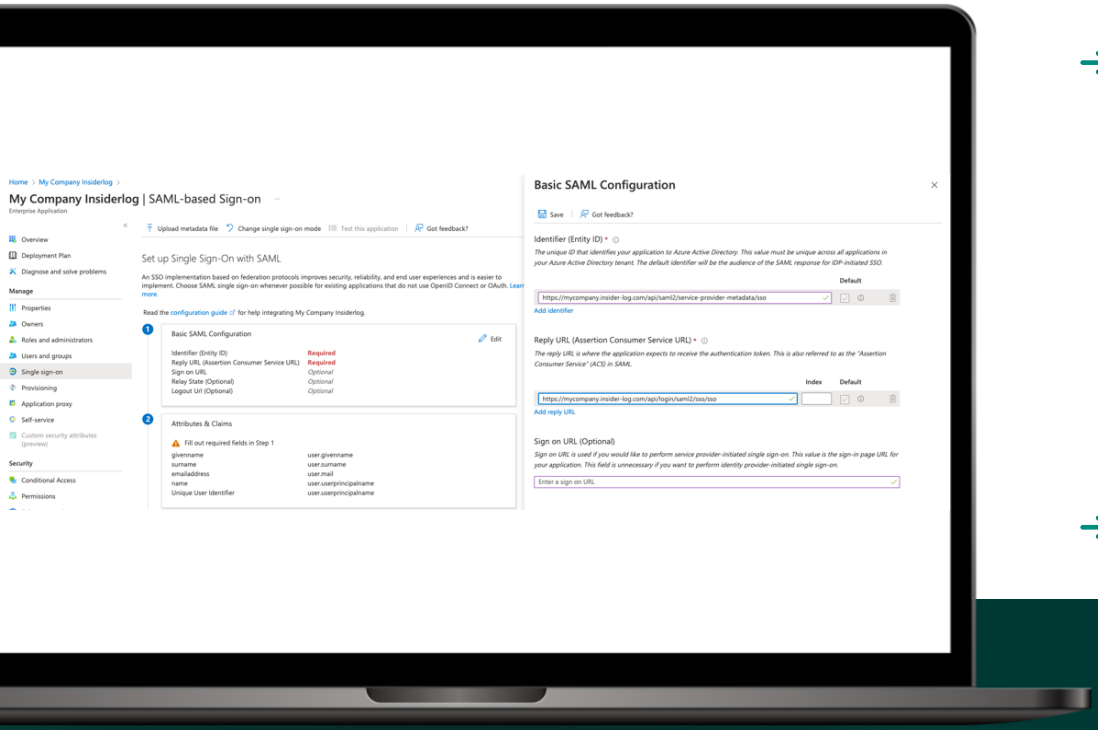
- Select Single sign-on on menu and enable SAML

Step 5.1: Configure Azure AD SSO



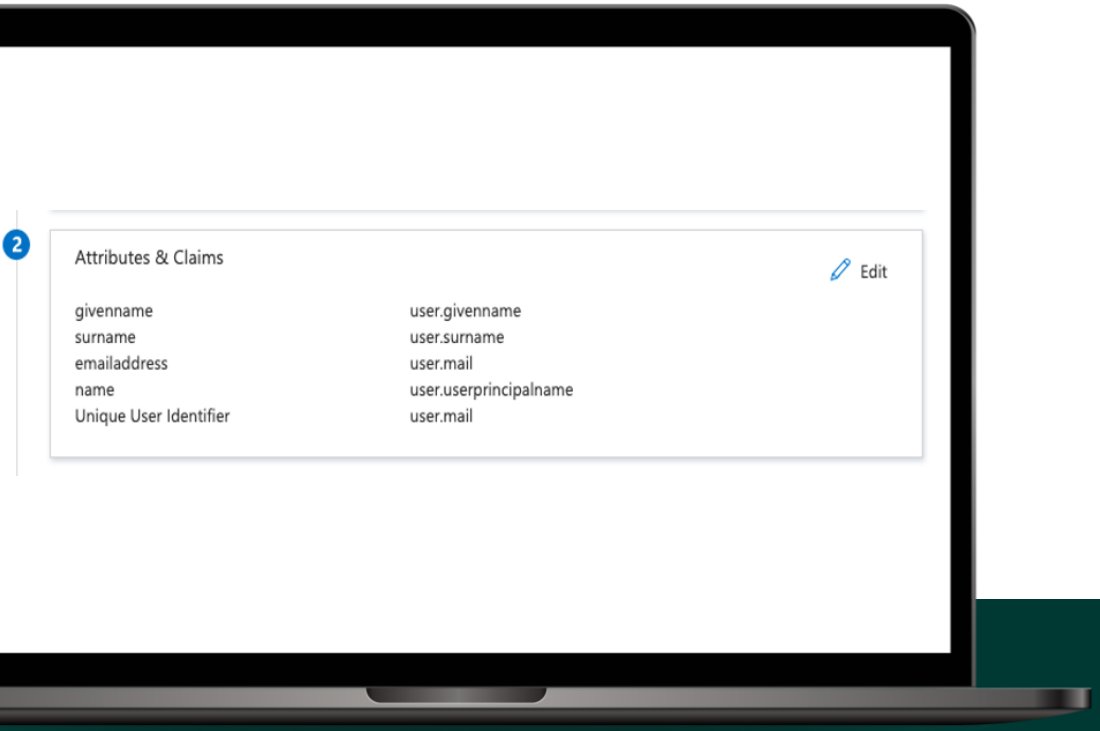
- Azure AD will show the SSO configuration with some required fields. Under Basic SAML Configuration
  - Identifier (Entity ID)
  - Reply URL (Assertion Consumer Service URL)
- Click Edit

Step 5.2: Configure Azure AD SSO



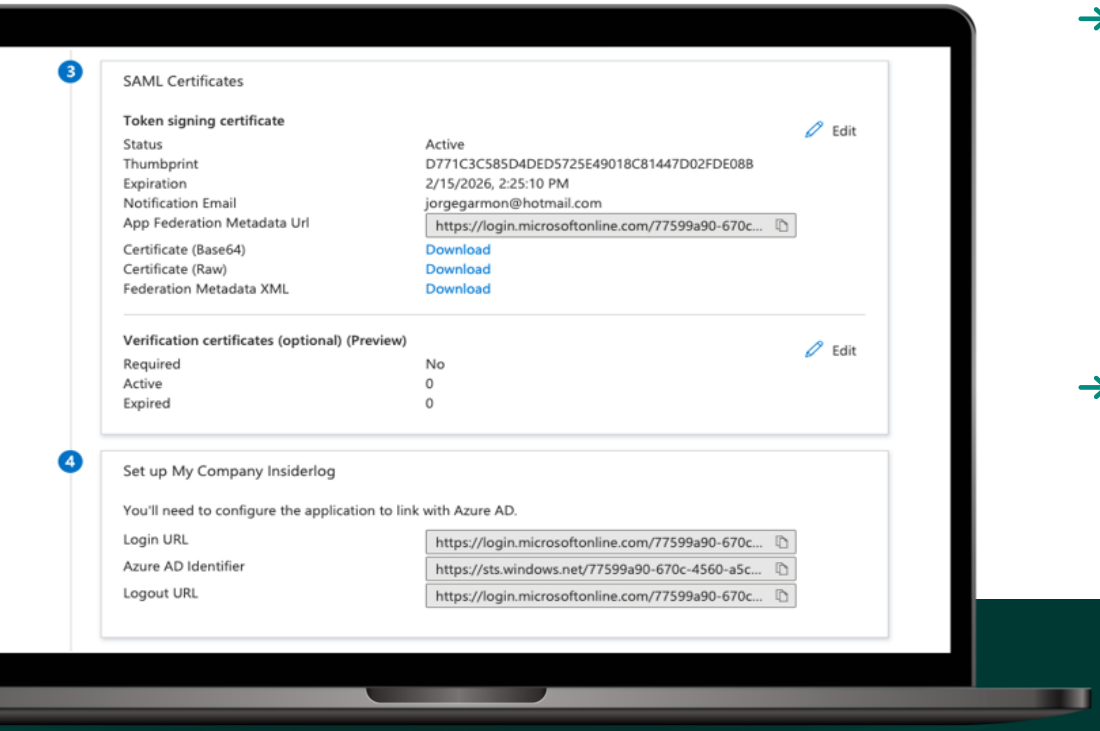
- Configure the Basic SAML Configuration using the following URL templates. In our case our tenant subdomain is “mycompany” and the Insiderlog SSO registration name is “sso”
  - Identifier (Entity ID)
    - https://<tenant.subdomain>.insider-log.com/api/saml2/service-provider-metadata/<insiderlogsso.registrationName>
  - Reply URL (Assertion Consumer Service URL)
    - https://<mycompanysubdomain>.insider-log.com/api/login/saml2/sso/<insiderlogsso.registrationName>
- Save

Step 5.3: Configure Azure AD SSO



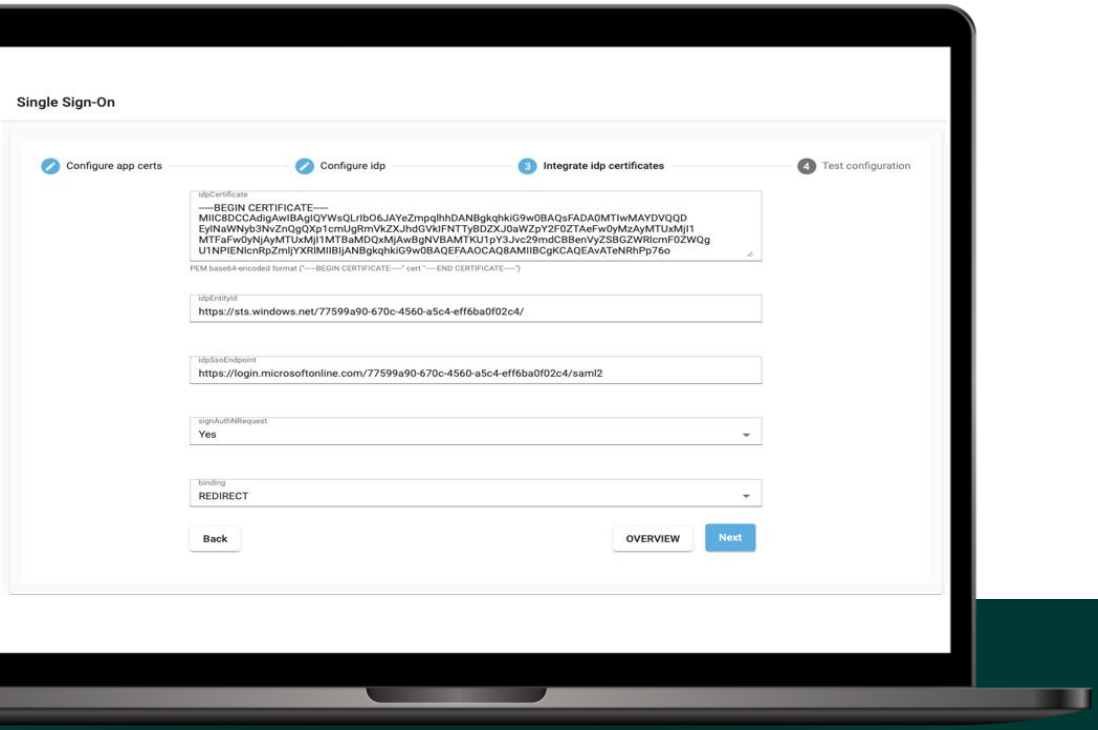
- Edit accordingly so that the attributes & claims has the following:
  - Unique User Identifier: Format Email
  - Unique User Identifier: Attribute user.mail

Step 5.4: Configure Azure AD SSO



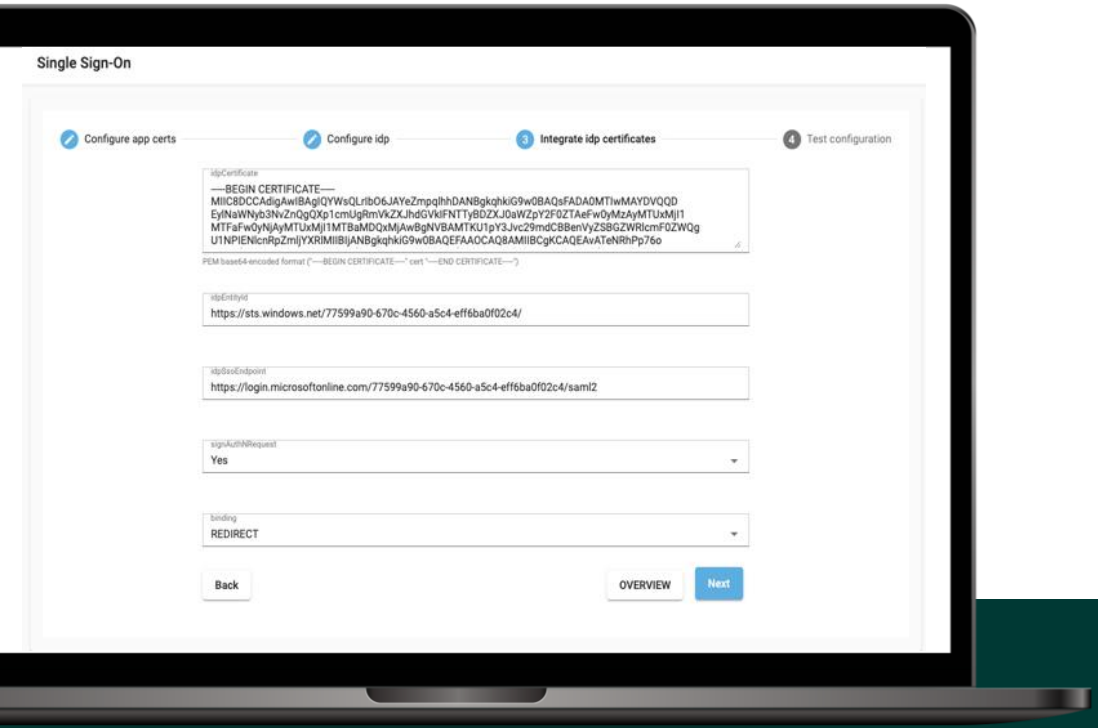
- On point 3 and 4 you will find the last configuration settings for InsiderLog SSO configuration
  - On Point 3 you will find the SAML certificates. Download the Base64 version.
  - On the Point 4 of Azure AD Saml-based Sign-on. You will find the following endpoints
    - Login URL
    - Azure AD Identifier
- **On the Insiderlog SSO config:**
  - Login URL = idpSsoEndpoint
  - Azure AD identifier = idpEntityId
  - Certificate (Base64) = idpCertificate

Step 6: Complete InsiderLog's SSO configuration



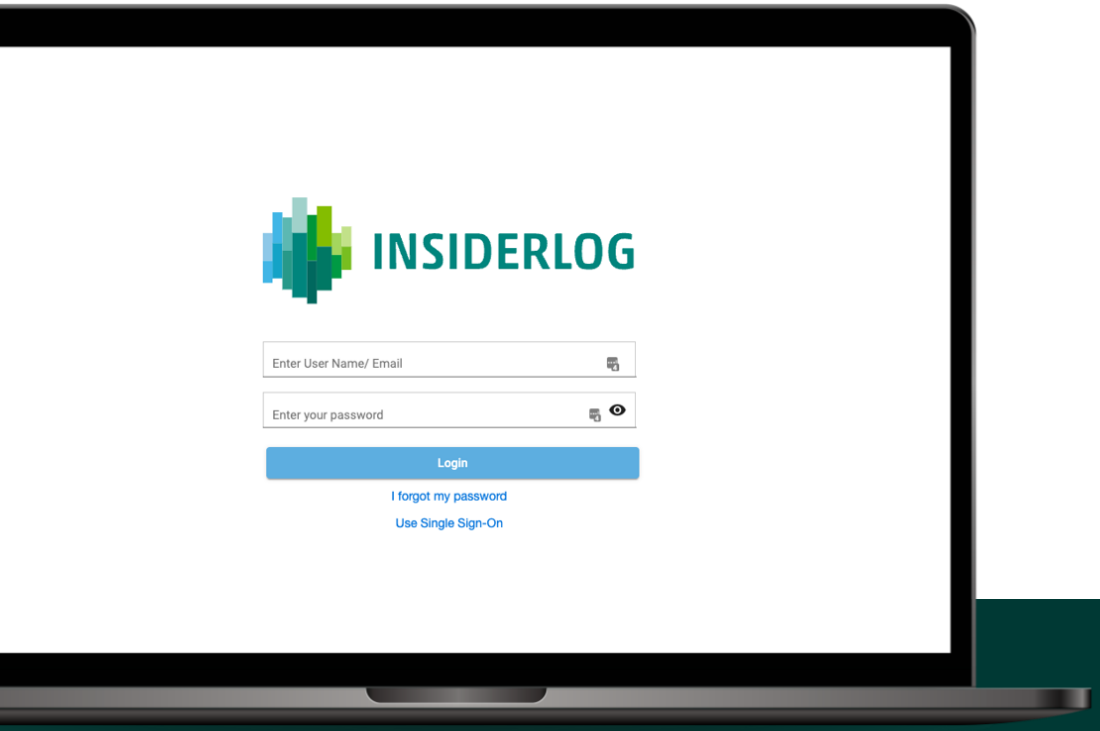
- Use the Urls and certificates from the last steps to configure Insiderlog and click next

Step 6.1: Complete InsiderLog's SSO configuration



- Use the URLs and certificates from the last step 5.4 to complete InsiderLog's SSO configuration
- click Next

Step 7: Test your SSO integration



- Click on **"Use Single Sign-on"** and you must be redirected to your AD authentication, or if already logged in to the InsiderLog's Home dashboard.
- Remember only users that are registered with InsiderLog and that match the Unique Identifier claim will be granted access.


COMPLYLOG
A EURONEXT COMPANY