



Insiderlog SSO Azure

(Step by Step Guide)



COMPLYLOG

A EURONEXT COMPANY

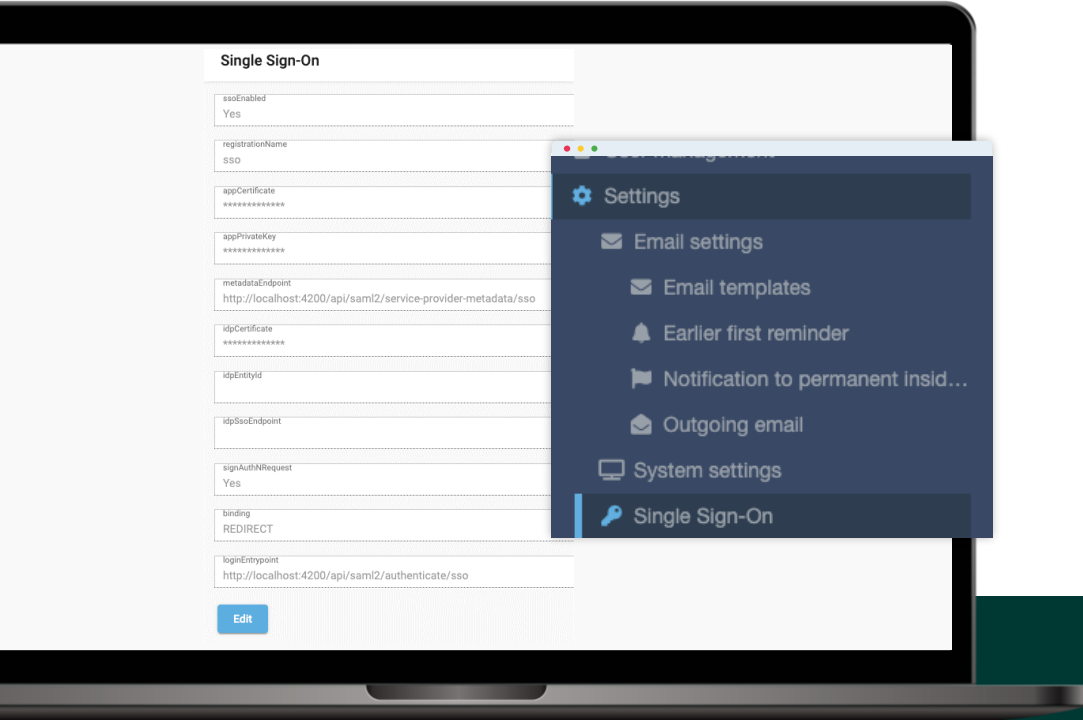
Basic concepts

- 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:

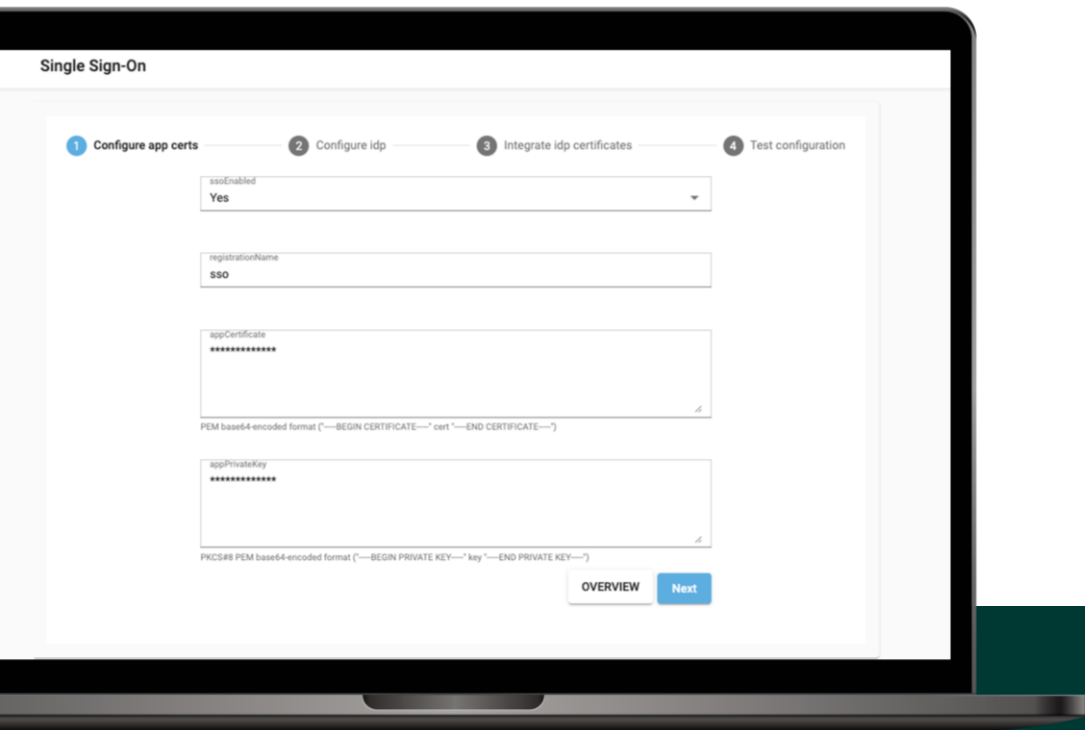
- InsiderLog Application generates a Metadata file based on the configuration (App certs)
- The metadata file contains information needed to register itself as an Enterprise app on Azure (AD). Entity ID, Relay Endpoint.
- Azure AD will generate an Identifier and login URL to initiate authentication
- InsiderLog App needs to register the Azure generated ID and login URL to initiate the Authentication process

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 3: Configure certificates

Single Sign-On

1 Configure app certs 2 Configure idp 3 Integrate idp certificates 4 Test configuration

ssoEnabled
Yes

registrationName
SSO

appCertificate
-----BEGIN CERTIFICATE-----
MIIEKTCCAxCgAwIBADANBgkqhkiG9w0BAQ0FADCBTELMAkGA1UEBhMCZmxk
EzARBgNVBAgMCIBpcmhYWSYtYWVWExZARBgNVBAoMCK15IENvbXBhbnRlAgBqNV
BAMMGW15Y29tcGFueS5pbmNpZGVyLWxvZy5jb2Z0FDASBgNVBACMC0xFTVDDhMOE
TMOEMRQwEgYDVQQLDAtFQ1MgRmlubGZuZDEkMCIkGSI3bDQEQEJARYVc29tZW9u
-----END CERTIFICATE-----
PEM base64-encoded format (-----BEGIN CERTIFICATE----- cert -----END CERTIFICATE-----)

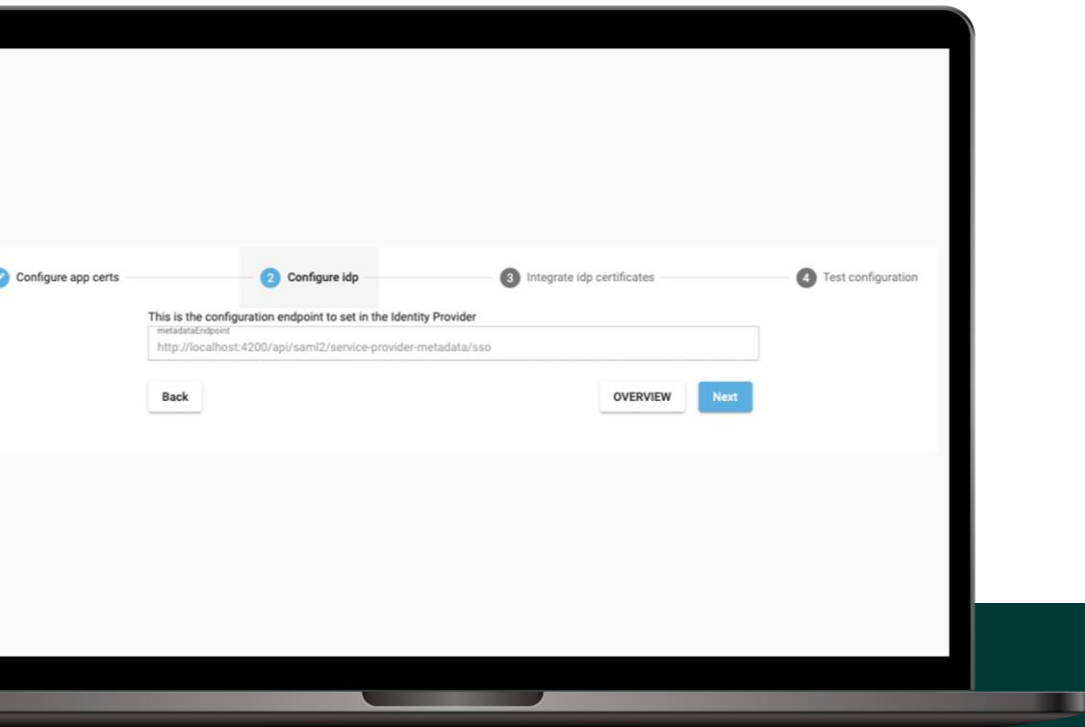
appPrivateKey
-----BEGIN PRIVATE KEY-----
MIIEwAIBADANBgkqhkiG9w0BAQEFAASCBKowggSmAgEAAoIBAgDaU503UVmUQot
mRXWP632Qxf0Rz+JIEYNIAC0HS4IS+W0bWoo2vbc30LN9GJyykw8T9zHNLb3
/h2b0ERXBXWKIGaBUhqc0ceZaatl0CGa7y0DcCrMrYlCeTf5i9nyI70GssR+sZCQ
XsWgQvghWZurkhuuskr73bwin0BSGuhY7zLxfhLIX7ydl/BK+E19IZJYp31kilZjN
-----END PRIVATE KEY-----
PKCS#8 PEM base64-encoded format (-----BEGIN PRIVATE KEY----- key -----END PRIVATE KEY-----)

OVERVIEW Next

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.

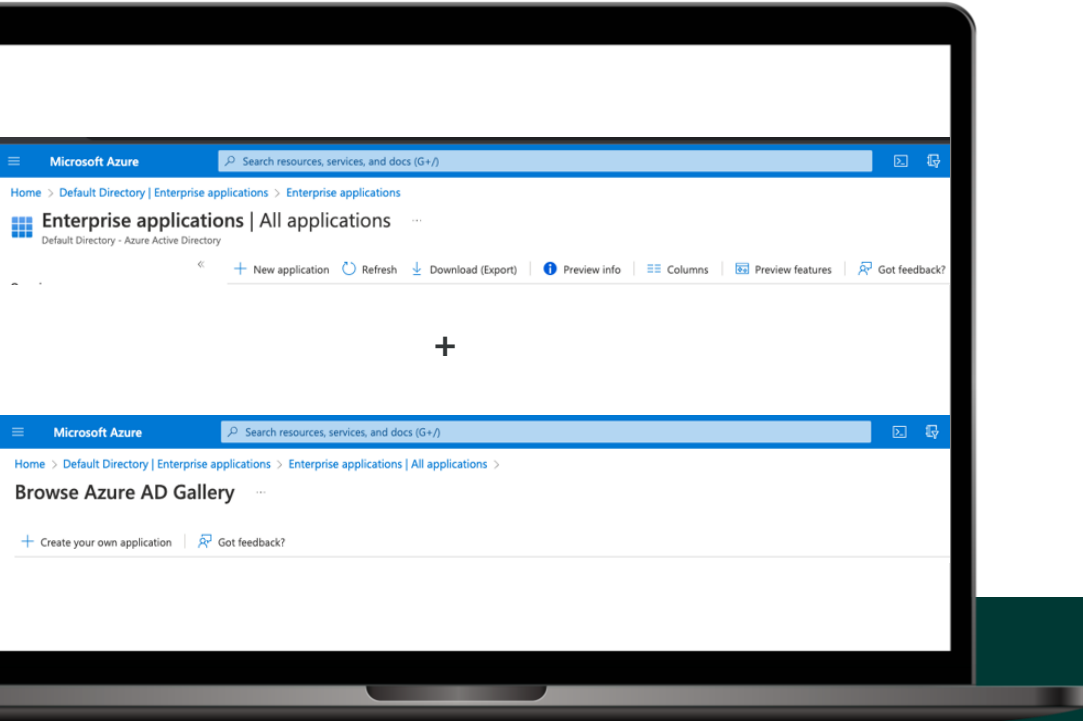
→ **Save the link**

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"

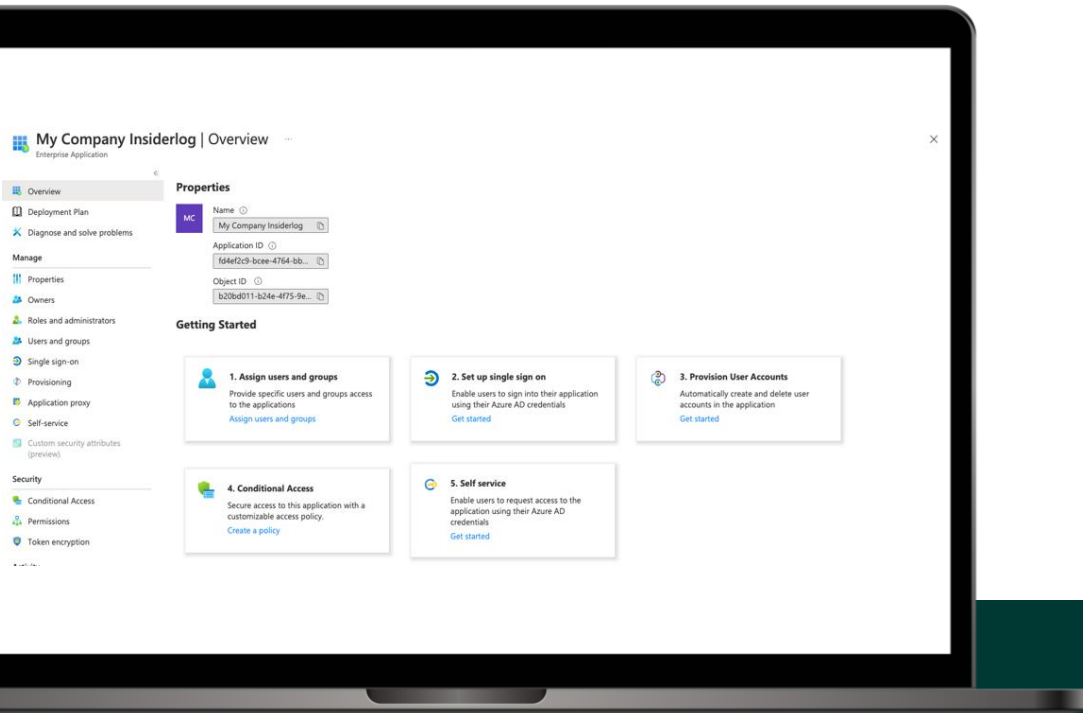
Step 4.2: Configure Active Directory

The screenshot shows the Azure AD Gallery interface. On the left, there's a 'Browse Azure AD Gallery' section with a search bar and filters for 'Single Sign-on: All', 'User Account Management: All', and 'Categories: All'. Below this are sections for 'Cloud platforms' (Amazon Web Services (AWS), Google Cloud Platform, Oracle), 'On-premises applications' (Add an on-premises application, Learn about Application Proxy), and 'Featured applications' (Adobe Identity Management (SAML), Atlassian Cloud, AWS Single-Account Access).

The 'Create your own application' dialog box is open on the right. It has a 'Got feedback?' link at the top. Below that, it says: 'If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.' There is a text input field for 'What's the name of your app?' with the value 'My Company Insiderlog'. Below this is a section 'What are you looking to do with your application?' with three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Azure AD (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected. At the bottom right of the dialog is a 'Create' button.

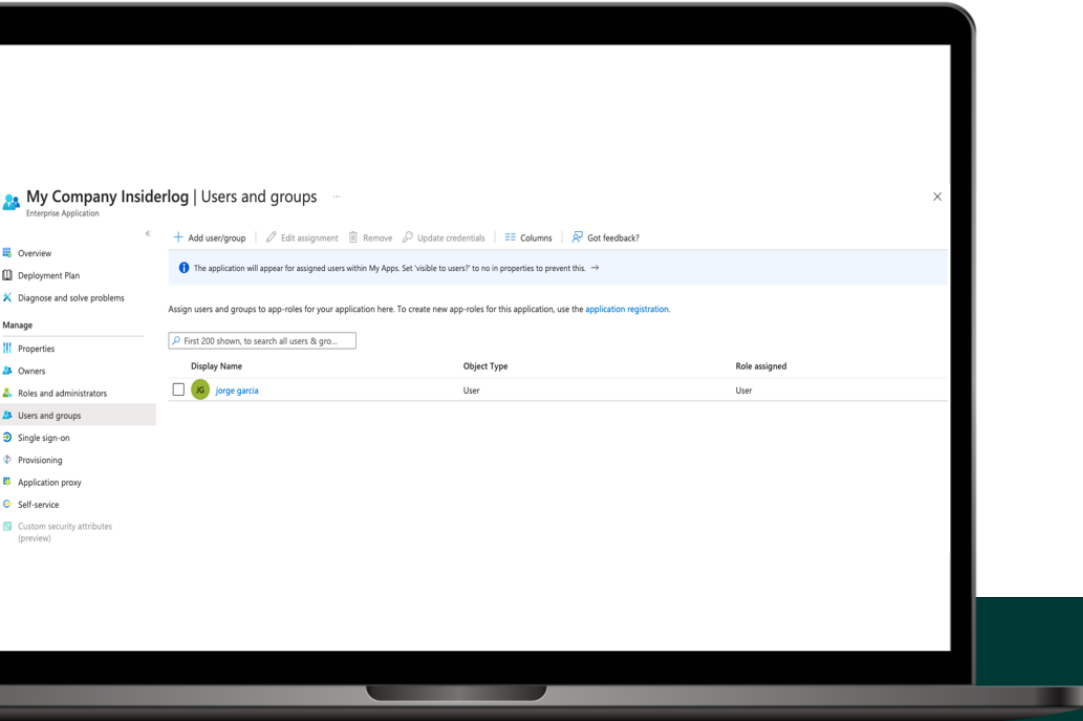
- Name the application and click create

Step 4.3: Configure Active Directory



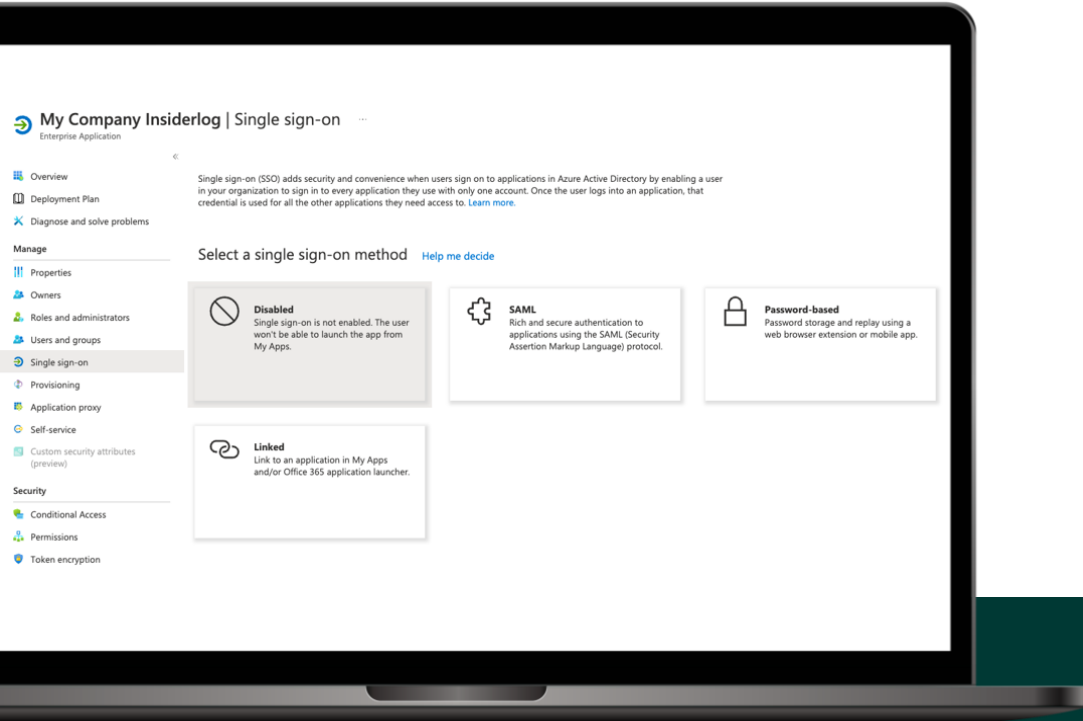
- Configure the owners, Roles and administrators and Users and groups according to your organization needs

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

The screenshot displays the Azure AD portal interface for configuring SAML-based Sign-on for an application named 'My Company Insiderlog'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on (selected), Provisioning, Application proxy, Self-service, Custom security attributes, Security, Conditional Access, Permissions, Token encryption, Activity, Sign-in logs, Usage & insights, Audit logs, Provisioning logs, Access reviews, and Troubleshooting + Support. The main content area is titled 'Set up Single Sign-On with SAML' and contains several configuration steps:

- Basic SAML Configuration:** A table with fields for Identifier (Entity ID), Reply URL (Assertion Consumer Service URL), Sign-on URL, Relay State (Optional), and Logout URL (Optional). The Identifier and Reply URL fields are marked as 'Required'.
- Attributes & Claims:** A section with a warning icon and the text 'Fill out required fields in Step 1'. It lists attributes like givenname, surname, emailaddress, name, and Unique User Identifier, each with a corresponding user attribute name.
- SAML Certificates:** A section for 'Taken signing certificate' with fields for Status, Thumbprint, Expiration, Notification Email, and App Federation Metadata URL. Below this, there are download links for Certificate (Base64), Certificate Base6, and Federation Metadata XML.
- Verification certificates (optional) (Preview):** A table with fields for Required, Active, and Expired, each with a dropdown menu.

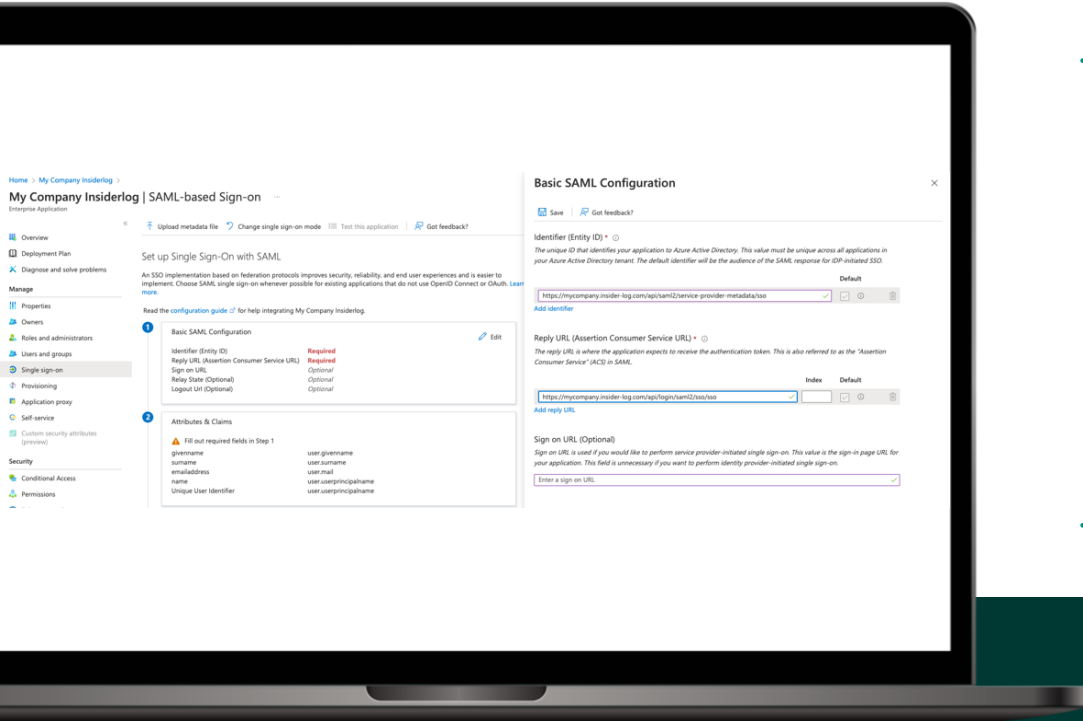
On the right side of the configuration area, there are two panels: 'Set up My Company Insiderlog' and 'Test single sign-on with My Company Insiderlog'. The 'Set up' panel includes fields for Login URL, Azure AD Identifier, and Logout URL, each with a dropdown menu. The 'Test' panel includes a 'Test' button and a warning icon with the text 'Fill out required fields in Step 1'.

→ 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

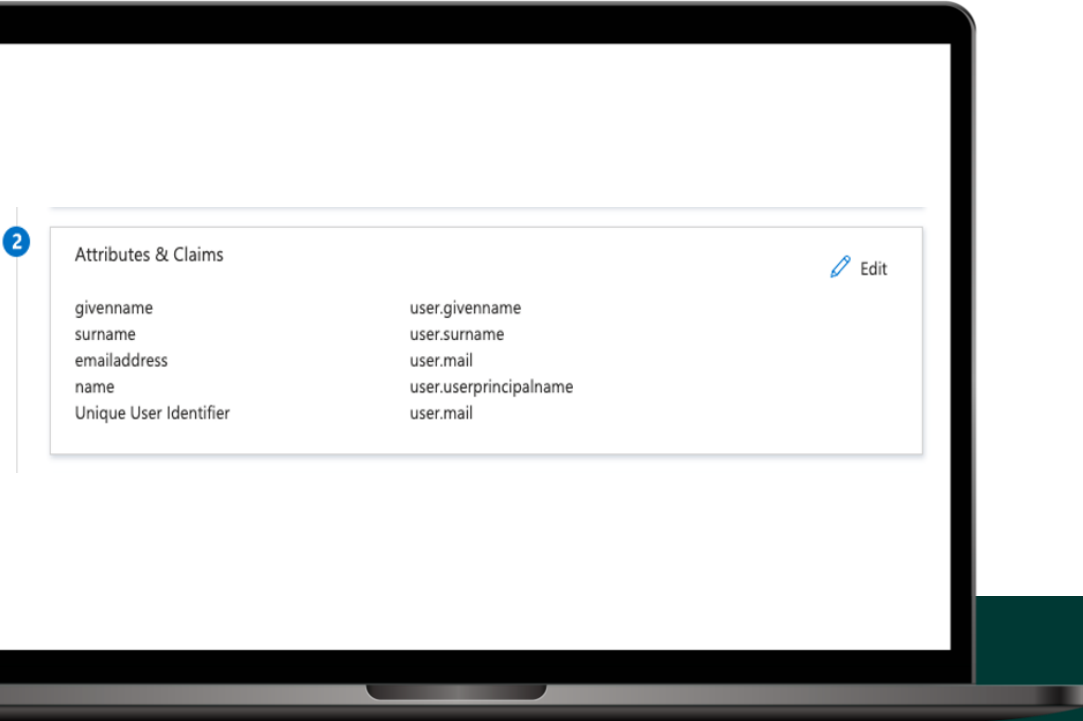


→ Configure the Basic SAML Configuration using the following URL templates. In our case our tenant subdomain is "mycompany" and the Insiderlog SSO registration name is "sso"

- Identifier (Entity ID)
 - `https://<tenant.subdomain>.insiderlog.com/api/saml2/service-provider-metadata/<insiderlog.sso.registrationName>`
- Reply URL (Assertion Consumer Service URL)
 - `https://<mycompanysubdomain>.insiderlog.com/api/login/saml2/sso/<insiderlog.sso.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

The screenshot displays the Azure AD SSO configuration interface. It is divided into two main sections, labeled 3 and 4.

Section 3: SAML Certificates

Token signing certificate		Edit
Status	Active	
Thumbprint	D771C3C585D4DED5725E49018C81447D02FDE08B	
Expiration	2/15/2026, 2:25:10 PM	
Notification Email	jorgegarmon@hotmail.com	
App Federation Metadata Url	https://login.microsoftonline.com/77599a90-670c...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Section 4: Set up My Company Insiderlog

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/77599a90-670c...
Azure AD Identifier	https://sts.windows.net/77599a90-670c-4560-a5c...
Logout URL	https://login.microsoftonline.com/77599a90-670c...

- 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 7: Test your SSO integration



Enter User Name/ Email

Enter your password

Login

[I forgot my password](#)

[Use Single Sign-On](#)

- 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

This publication is for information purposes only and is not a recommendation to engage in investment activities. This publication is provided “as is” without representation or warranty of any kind. Whilst all reasonable care has been taken to ensure the accuracy of the content, Euronext does not guarantee its accuracy or completeness. Euronext will not be held liable for any loss or damages of any nature ensuing from using, trusting or acting on information provided. No information set out or referred to in this publication shall form the basis of any contract. The creation of rights and obligations in respect of financial products that are traded on the exchanges operated by Euronext’s subsidiaries shall depend solely on the applicable rules of the market operator. All proprietary rights and interest in or connected with this publication shall vest in Euronext. No part of it may be redistributed or reproduced in any form without the prior written permission of Euronext. Euronext refers to Euronext N.V. and its affiliates. Information regarding trademarks and intellectual property rights of Euronext is located at www.euronext.com/terms-use

© 2023, Euronext N.V. - All rights reserved.