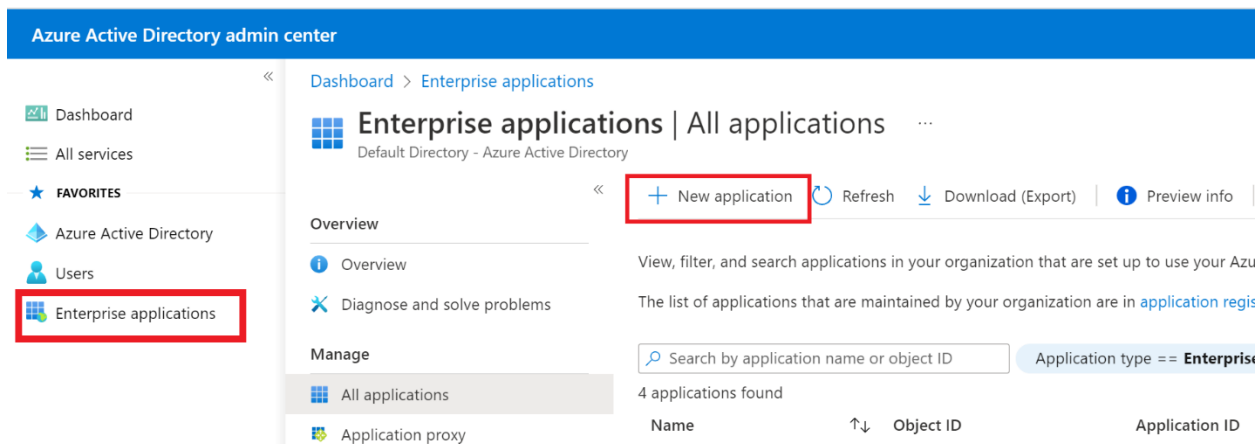


How To Set Up eCompliance SSO with Azure AD

We offer a Single Sign On (SSO) implementation that allows your users to sign into the web version of eCompliance automatically when they are using your company network or intranet. Please contact your eCompliance Account Executive if you are interested in adding the SSO service to your account.

This resource will guide you through the process of setting up SSO with Azure AD.

1. Enable SSO login on eCompliance. Please contact your eCompliance representative to enable Single Sign-On (SSO).
2. Create an application on Azure AD portal:
 1. Login to Azure Active Directory admin center.
 2. Navigate to Enterprise applications.
 3. Click on 'Create new application' > 'Create your own application'



4. A 'Create your own application' panel will open. Input 'eCompliance' as the name of the application and select 'Non-gallery'.

Dashboard > Enterprise applications | All applications

Browse Azure AD Gallery

[+ Create your own application](#) [Got feedback?](#)

The Azure AD App Gallery is a catalog of thousands of app provisioning. When deploying an app from the App Gallery create your own application here. If you are wanting to put discover and use, you can file a request using the process c

Search application

Cloud platforms

Amazon Web Services (AWS)

Oracle

Create your own application

[Got feedback?](#)

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.

What's the name of your app?
eCompliance ✓

What are you looking to do with your application?

Configure Application Proxy for secure remote access to an on-premises application

Register an application to integrate with Azure AD (App you're developing)

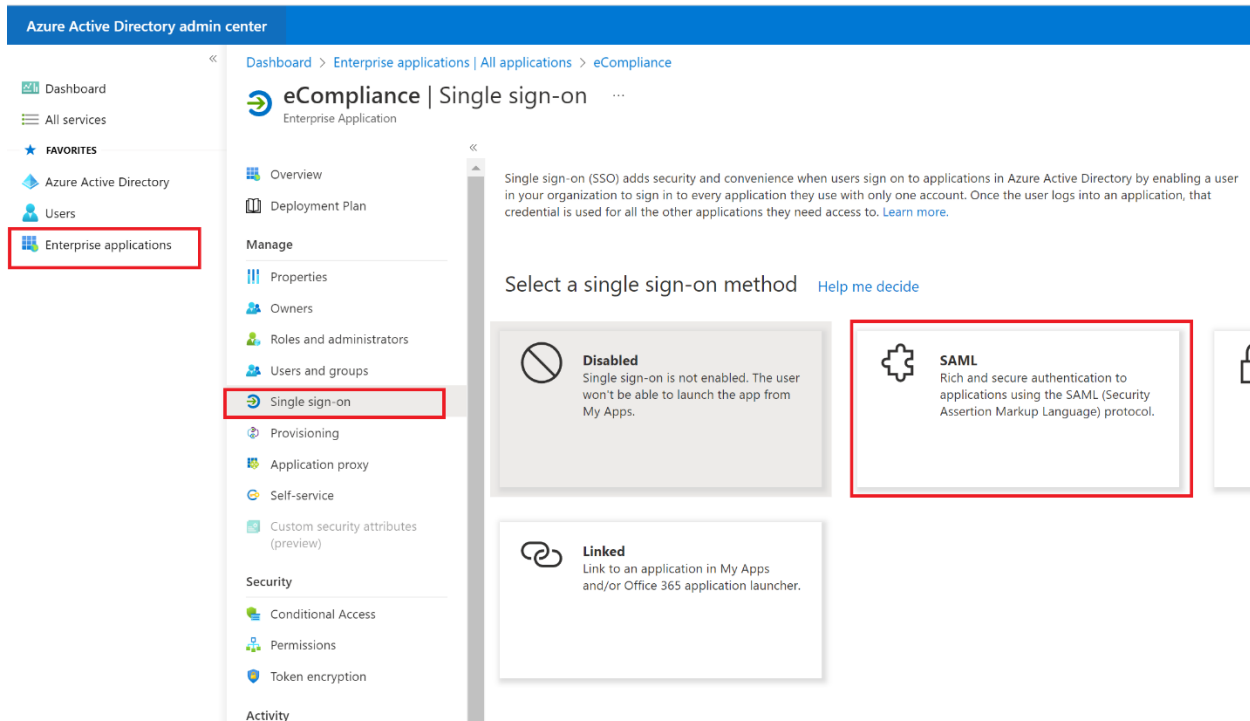
Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry
We recommend using gallery applications when possible.

- Field ID
- Compliance ELF
- MyCompliance Cloud
- Complan Complion
- Zix Compliance and Capture

[Create](#)

5. Click 'Create'
 6. Navigate back to Enterprise applications. 'eCompliance' should be in the list of applications.
3. Enable Single Sign-on for new application:
1. In Azure AD find 'Enterprise applications' from the left settings blade. Navigate to 'eCompliance' > Single sign-on > SAML.



2. In the Set up Single Sign-On with SAML window, scroll to 'SAML Certifications' section and save the value of 'Thumbprint' for later use.
3. In the same window, scroll to 'Set up eCompliance' section. Save the value of 'Login URL' for later use.

Azure Active Directory admin center

Dashboard > Enterprise applications | All applications > eCompliance >

eCompliance | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Troubleshooting + Support

SAML Certificates

Token signing certificate Active [Edit](#)

Thumbprint	D99429
Expiration	5/22/2027, 10:02:49 PM
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/273be8fe-0181-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) (Preview) [Edit](#)

Required	No
Active	0
Expired	0

4 Set up eCompliance

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

Login URL	https://login.microsoftonline.com/273be8fe-0181-...
Azure AD Identifier	https://sts.windows.net/273be8fe-0181-41bd-a7c...
Logout URL	https://login.microsoftonline.com/273be8fe-0181-...

5 Test single sign-on with eCompliance

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

▲ Fill out required fields in Step 1

[Test](#)

4. Set up SSO on eCompliance web:

1. In eCompliance web, navigate to Settings > SSO Settings.
2. Fill in 'Certificate Fingerprint' with value saved from step 3.2.
3. Fill in 'SAML SSO URL' with value saved from step 3.3.
4. Click 'Save' and an 'Assertion Consumer Service URL' should be supplied in a new textbox. Copy this value for later use.

ACCOUNT INFORMATION

STATUS
 CONTACT
 USAGE
 PRICING
 PAYMENT PROFILE
 SSO SETTINGS

SSO Settings

Single Sign On is implemented using SAML.SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet

Yes, I want to enable Single Sign On

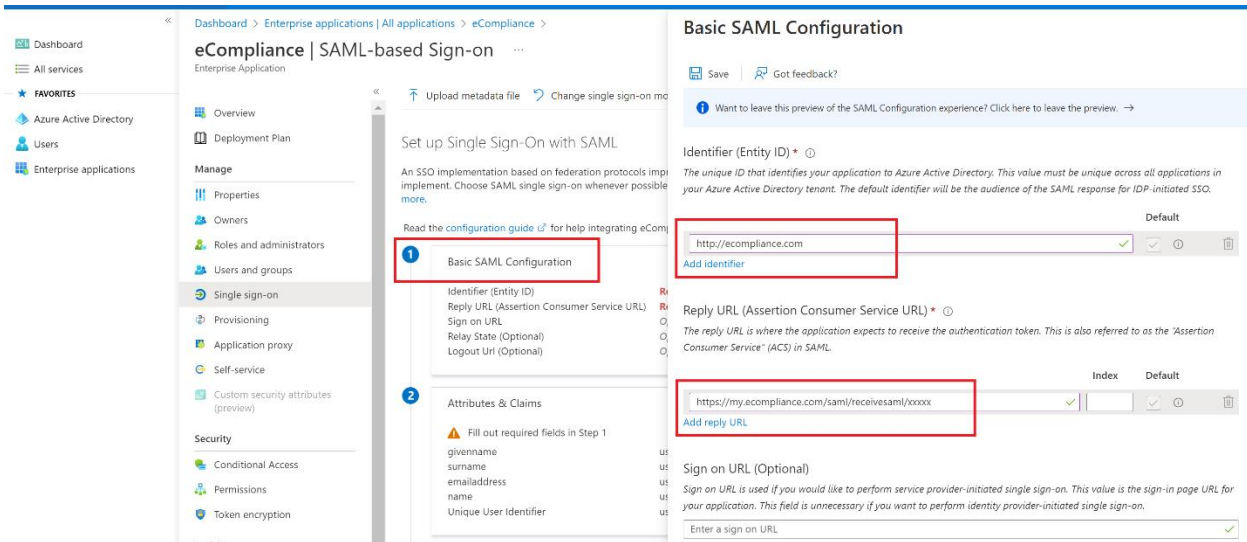
Certificate Fingerprint: THUMBPRINT HERE
 The SHA1 fingerprint of the SAML certificate. The fingerprint is required to verify the SSO response

SAML SSO URL: https://login.microsoftonline.com/application-id/saml2
 This is the URL that eCompliance will invoke to redirect users to your identity provider

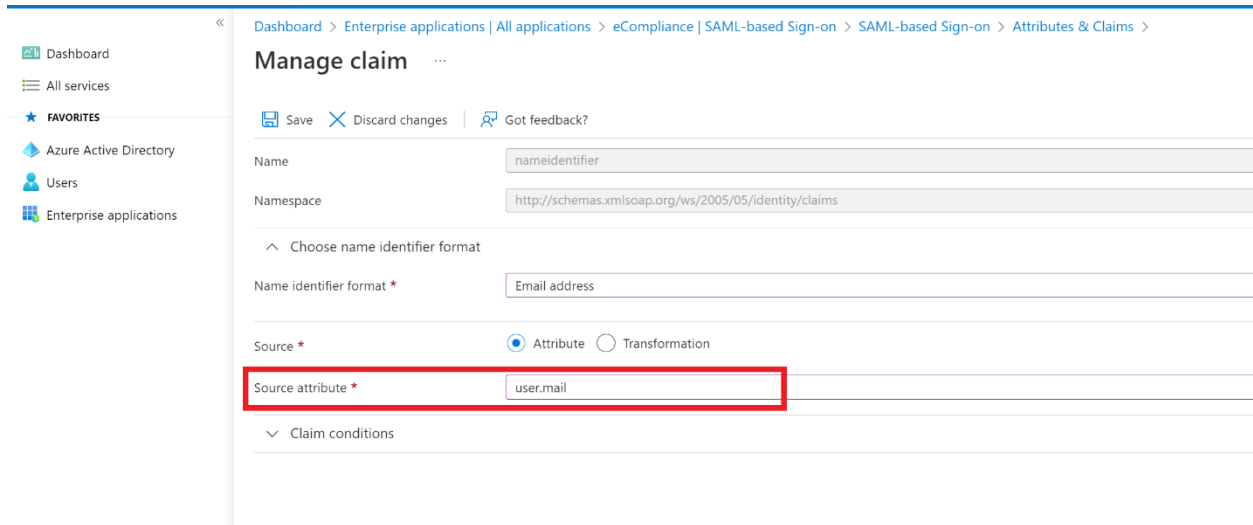
Assertion Consumer Service (ACS) URL: https://my.ecompliance.com/saml/receivesaml/xxxxx
 This is the URL you have to send the SAML Response to.

5. Finish Single Sign-on settings on Azure AD:

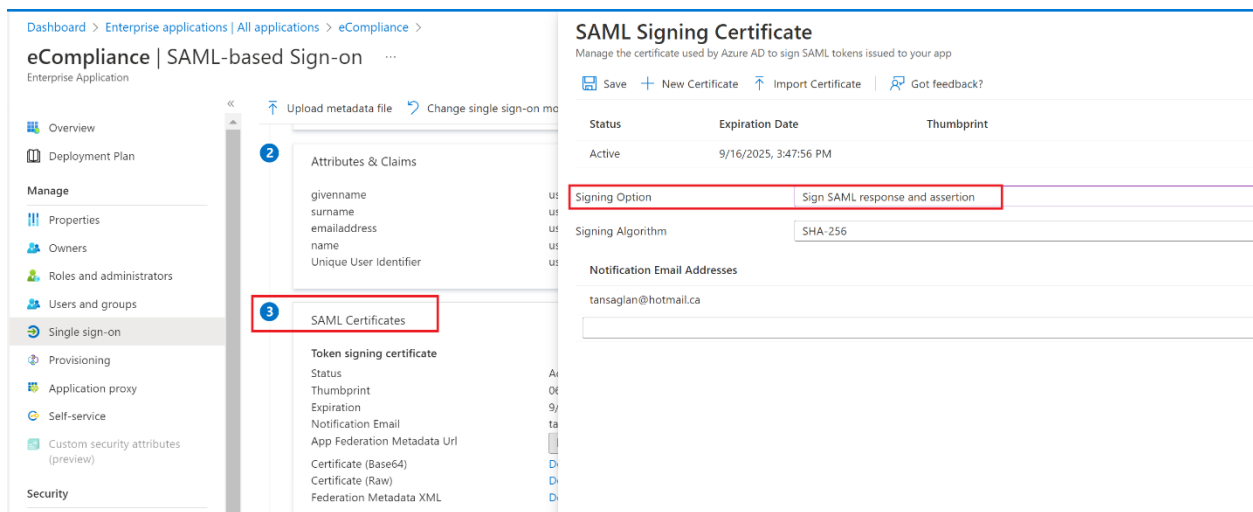
1. Modify in 'Basic SAML configuration' section:
 - i. Identifier: enter 'http://ecompliance.com'
 - ii. Reply url: fill in value saved from step 4.4



2. Modify 'Attributes & Claims' section:
 - i. Update 'Unique User Identifier (Name ID)' claim
 - ii. Change 'Source attribute' to 'user.mail' and save changes



3. Modify `SAML Certificates` section:
 - i. Update signing option to `Sign SAML response and assertion`



6. Test login:
 1. In Azure AD, add a test user to `eCompliance` application.
 2. In eCompliance web, ensure the test user has an account in your organization with the same email address.
 3. Log in as the test user on Azure AD portal and eCompliance icon should be displayed. Clicking that icon will open a new tab and log you in into eCompliance.

Apps

Edit List view



eCompliance