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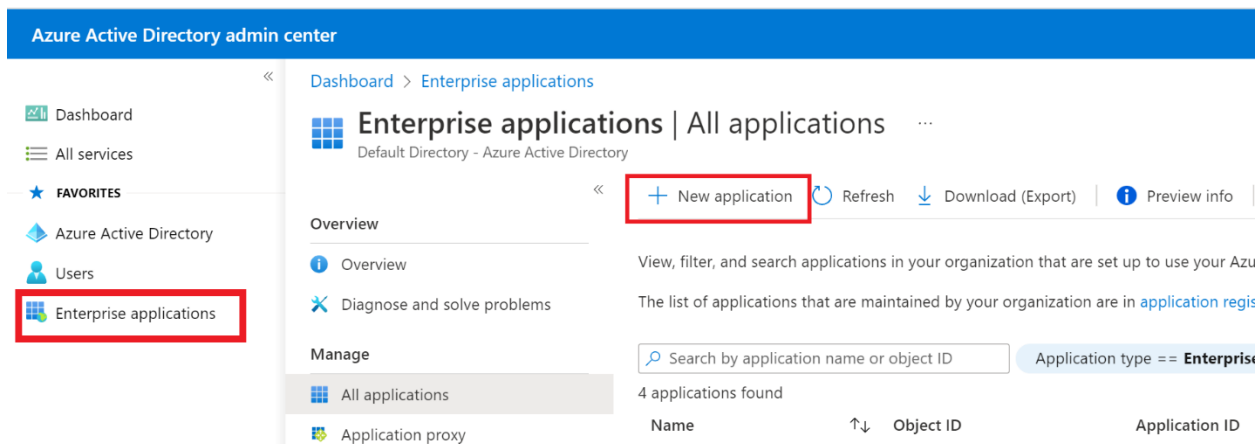
4. A 'Create your own application' panel will open. Input 'eCompliance' as the name of the application and select 'Non-gallery'.

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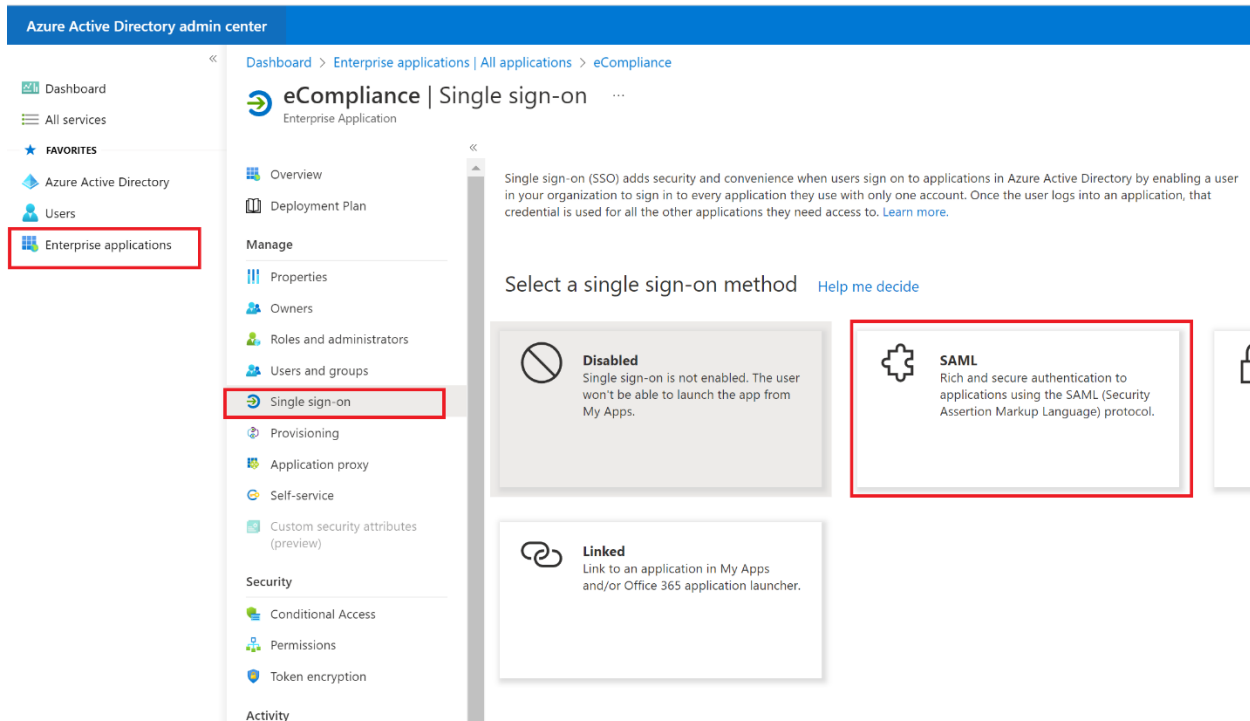
2. In the Set up Single Sign-On with SAML window, scroll to 'SAML Certifications' section and save the value of 'Thumbprint' for later use.
3. In the same window, scroll to 'Set up eCompliance' section. Save the value of 'Login URL' for later use.

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.

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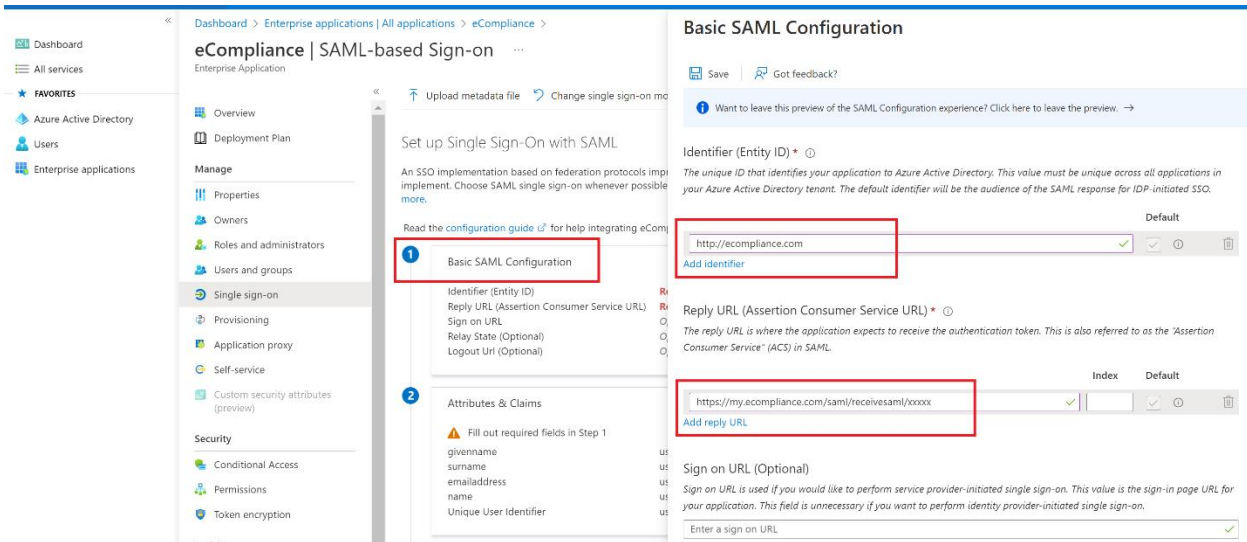
    2. Modify 'Attributes & Claims' section:
        i. Update 'Unique User Identifier (Name ID)' claim
        ii. Change 'Source attribute' to 'user.mail' and save changes

Manage claim ···

Save ✕ Discard changes | ⚲ Got feedback?

Name   nameidentifier

Namespace   http://schemas.xmlsoap.org/ws/2005/05/identity/claims

∧ Choose name identifier format

Name identifier format *   Email address

Source *   ● Attribute ○ Transformation

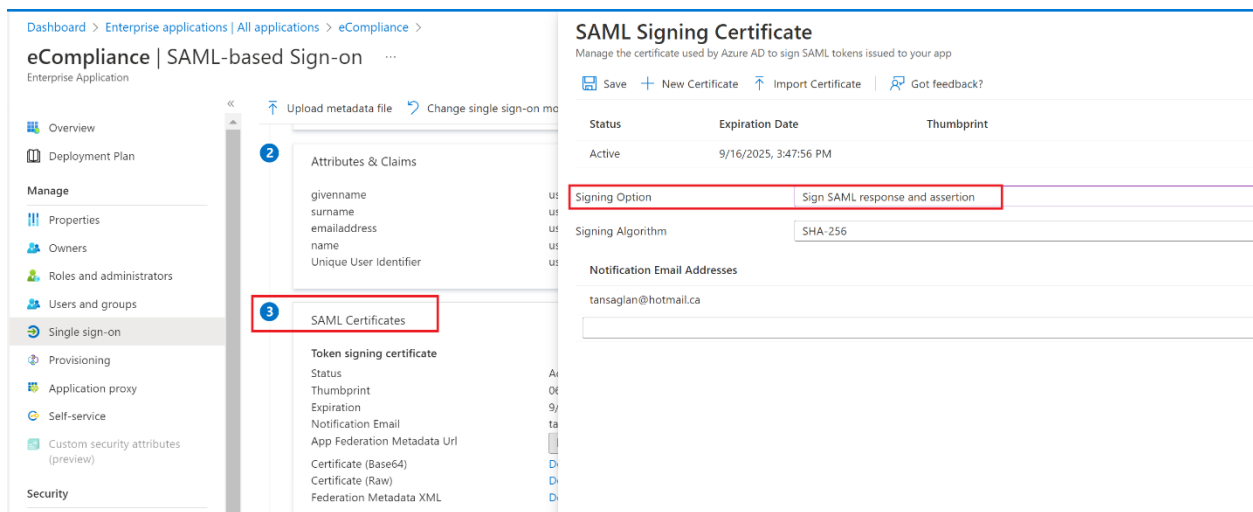Source attribute *   user.mail

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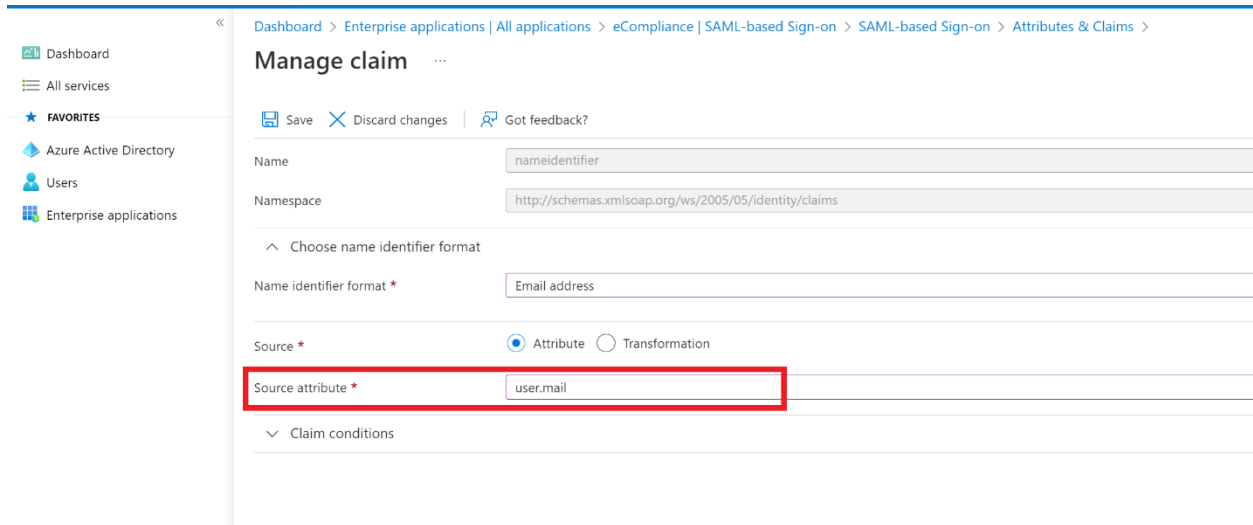
3. Modify `SAML Certificates` section:
    i. Update signing option to `Sign SAML response and assertion`

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.

6

🔍 Search apps

Apps ∨ ⊕

✏ Edit   ≡ List view   • • •

eCompliance