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'

Azure Active Directory admin center				
«	Dashboard > Enterprise applications			
📶 Dashboard	Enterprise applications All applications Default Directory - Azure Active Directory			
E All services				
† FAVORITES	»»	+ New application 💍 Refresh 🞍 Downloa	d (Export) () Preview info	
🔶 Azure Active Directory	Overview	L		
🔒 Users	(i) Overview	View, filter, and search applications in your organiza	tion that are set up to use your Azu	
Enterprise applications	✗ Diagnose and solve problems	The list of applications that are maintained by your	organization are in application regis	
	Manage	$\begin{tabular}{ c c c c } \label{eq:powerset} \end{tabular}$ Search by application name or object ID Application type == I		
	All applications	4 applications found		
	Application proxy	Name ↑↓ Object ID	Application ID	

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	Create your own application ×		
Z Dashboard	Browse Azure AD Gallery			
E All services	,	🖗 Got feedback?		
★ FAVORITES	+ Create your own application 🔗 Got feedback?			
Azure Active Directory	The Azure AD App Gallery is a catalog of thousands of app provisioning. When deploying an app from the App Gallery	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.		
	create your own application here. If you are wanting to put	What's the name of your app?		
Enterprise applications	discover and use, you can file a request using the process c	eCompliance 🗸		
	Search application	What are you looking to do with your application?		
		Configure Application Proxy for secure remote access to an on-premises application		
	Cloud platforms	Register an application to integrate with Azure AD (App you're developing)		
	Amazon Web Services (AWS)	Integrate any other application you don't find in the gallery (Non-gallery)		
	aws	We found the following applications that may match your entry We recommend using gallery applications when possible. Image: Complex		
	Oracle	*Complion Complion		
	Ø	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.



- 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.

Your Accounts / Account Information					
ACCOUNT INFORMATION					
13 STATUS	L CONTACT	<u> </u>	\$ PRICING	PAYMENT PROFILE	SSO SETTINGS
SSO Settings					
Single Sign On is implemented	d using SAML.SAML is an i	ndustry standard SSO framewo	ork typically used by large en	terprises for communicating identi	ties across the internet
Yes, I want to	enable Single Sign On	2			
	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 Consum	ner Service (ACS) URL:	https://my.ecompliance.com/sa			
	I	Save			

- 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

«	Dashboard > Enterprise applications A	All applications > eCompliance >	Basic SAML Configuration		
Dashboard	eCompliance SAML-based Sign-on		save		
★ FAVORITES Azure Active Directory	«	$\overline{\uparrow}$ Upload metadata file $~~>~~$ Change single sign-on mo	\ref{start} Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. $ ightarrow$		
🚨 Users	Deployment Plan	Set up Single Sign-On with SAML	Identifier (Entity ID) * 💿		
Enterprise applications	Manage	An SSO implementation based on federation protocols impl	The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in		
	Properties	implement. Choose SAML single sign-on whenever possible more.	your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.		
	24 Owners	Read the configuration guide C for help integrating eCom	Default		
	🙇 Roles and administrators		http://ecompliance.com		
	Users and groups	Basic SAML Configuration	Add identifier		
	Single sign-on	Identifier (Entity ID) Re	Reply URL (Assertion Consumer Service URL) * The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML. Index Default		
	Provisioning	Reply URL (Assertion Consumer Service URL) R Sign on URL O, Relay State (Optional) O, Logout Url (Optional) O,			
	Application proxy				
	G Self-service				
	 Custom security attributes (preview) 	2 Attributes & Claims	https://my.ecompliance.com/sami/receivesami/xxxxx		
	Security	Fill out required fields in Step 1	Add reply URL		
	Seconditional Access	givenname us surname us	Sign on URL (Optional) Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.		
	Permissions	emailaddress us name us			
	Token encryption	Unique User Identifier us	your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on. Enter a sign on URL		
	a		Enter v alger on one		

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

×	Dashboard > Enterprise applications All applications > eCompliance SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >			
📶 Dashboard	Manage claim			
All services	-			
★ FAVORITES	🔜 Save 🗙 Discard changes 🛛 🖗 Got feedback?			
Azure Active Directory	Name	nameidentifier http://schemas.xmlsoap.org/ws/2005/05/identity/claims		
Users Enterprise applications	Namespace			
	∧ Choose name identifier format			
	Name identifier format *	Email address		
	Source *	• Attribute C Transformation	_	
	Source attribute *	user.mail		
	✓ Claim conditions		-	

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

Dashboard > Enterprise applications All applications > eCompliance > eCompliance SAML-based Sign-on … Enterprise Application		SAML Signing Certificate Manage the certificate used by Azure AD to sign SAML tokens issued to your app				
			🔜 Save 🕂 New Certificate 🕺 Timport Certificate 🦷 🖗 Got feedback?			
Uverview	↑ Upload metadata file	on ma	Status Expiration D	ate Thumbprint		
Deployment Plan	Attributes & Claims		Active 9/16/2025, 3:	47:56 PM		
Manage	givenname	us	Signing Option	Sign SAML response and assertion		
Properties	surname emailaddress	us Us	Signing Algorithm	SHA-256		
A Owners	name	us	Signing Algorithm	200 AHZ		
🍰 Roles and administrators	Unique User Identifier u		Notification Email Addresses			
A Users and groups			tansaglan@hotmail.ca			
Single sign-on	SAML Certificates					
Provisioning	Token signing certificate Status					
Application proxy	Thumbprint	OE				
Self-service	Expiration Notification Email	9/				
Custom security attributes	App Federation Metadata Url	la				
(preview)	Certificate (Base64) Certificate (Raw)	D				
Security	Federation Metadata XML	D				

- 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.

