

### Configuring SSO with Azure

Last Modified on Oct 26, 2020

This article provides a step-by-step guide to configuring SSO between OnceHub and Azure Active Directory.

### Requirements

To configure SSO in your account, you must be a OnceHub Administrator. However, you do not need a product license. Learn more You must already have an account with Azure AD. The person configuring in Azure AD must be an administrator.

### Step-by-step directions

#### **Request access**

SSO is intended for accounts with multiple users who take the extra security measure of signing into third-party applications using an identity provider. Please contact us to learn more. OnceHub can enable the SSO functionality in your account manually.

#### SAML configuration

You can access SAML configuration at OnceHub Account settings -> In the lefthand sidebar, select Security -> SSO.

OnceHub provides specific field values you can copy and configure within Azure AD:

1. In portal.azure.com, go to Enterprise applications -> Click on + New application.

	resources, services, and docs (G+/)			Þ.	R	Q		
Home > Default Directory > Enterprise application Default Directory - Azure Active Directory								
Overview Overview	+ New application         EE         Colu           Image: Try out the new Enterprise Apps         Column (Column)         Column)	mns Review features Search preview! Click to enable the preview!						
X Diagnose and solve problems	Application type	Applications status	Application visibility	$\overline{}$	Apply		Reset	
Manage  All applications		r applications, enter a display name or						
Application proxy	Name	Homepage URL		Object ID				

Figure 1: New application

2. On the Add an application page, select Non-gallery application.

## **OnceHub** Support

Id your own app Application you're developing Register an app you're working on to integrate it with Azure AD d from the gallery	Microsoft Azure	$\mathcal P$ Search resources, service	es, and docs (G+/)
<ul> <li>Click here to try out the new and improved app gallery. →</li> <li>Id your own app</li> <li>Application you're working on to integrate any pou're working on to integrate any blue secure remote access.</li> <li>Integrate any other agallery on the gallery</li> <li>Integrate any other access.</li> </ul>			l applications >
Image: Second system       Application gapplication gapplication gapplication certain system       On-premises gapplication gapplication         Register an app you're working on to integrate any other application Proxy to enable secure remote access.       Configure Azure AD Application Proxy to enable secure remote access.       Image: Ima			
Application you're developing Register an app you're working on to integrate it with Azure AD d from the gallery Category	Click here to try out the ne	aw and improved app gallery. $\rightarrow$	
developing     Configure Azure AD Application Proxy to enable secure remote access.     Integrate any other application that you don't find in the gallery       Id from the gallery     Category	dd your own app		
Category	you're developing Register an app you're working on to integrate it with Azure AD	Configure Azure AD Application Proxy to enable secure remote	Integrate any other application that you
All (3560) 🗸	Category		
	All (3560)		
Enter a name 🗸	Enter a name		

3. Add the Name (for example, "OnceHub"). Click Add.

■ Microsoft Azure
Home > Default Directory > Enterprise applications   All applications > Add an application >
Add your own application
Name * ①
The display name for your new application
Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.
Supports: ①
SAML-based single sign-on Learn more
Automatic User Provisioning with SCIM Learn more
Password-based single sign-on Learn more
Add

Figure 3: Add name and click Add

4. In the left menu, select **Single sign on**. Click on the **SAML** option.

		All applications > Add an application					
SSO TEST   Single s	sign-on						×
• Uverview	Select a	a single sign-on method	Help me decide				
Deployment Plan	-						
× Diagnose and solve problems	$\bigcirc$	Disabled	درع saw		A	Password-based	
Manage	0	Single sign-on is not enabled. The user won't be able to launch the app from My Apps.	appli	and secure authentication to cations using the SAML (Security rtion Markup Language) protocol.		Password storage and replay using a web browser extension or mobile app.	
H Properties							
A Owners							
Users and groups			-				
Single sign-on		Linked					
Provisioning	S	Link to an application in the Azure					
Application proxy		Active Directory Access Panel and/or Office 365 application launcher.					
Self-service							
Security							
Conditional Access							
2 Dormicrione	*						

Figure 4: SAML option

#### 5. Edit the Basic SAML Configuration section.

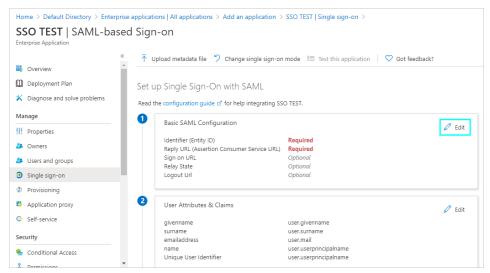


Figure 5: Edit the Basic SAML Configuration section

**6.** On the **Basic SAML Configuration** page, fill in the required fields and save. You can grab these values in OnceHub, on the **Required by entity provider** step.

In Azure AD	In OnceHub
Identifier (Entity ID)	Identifier URL
Reply URL	ACS URL
Sign on URL	Single sign-on URL

These are the only required fields; the rest can be left blank.

### **OnceHub** Support

Dasic SAIVIL	Configuration
Save	
Identifier (Entity I	* 🛈
The default identifier	l be the audience of the SAML response for IDP-initiated SSO
Reply URL (Assert	n Consumer Service URL) * 💿
	ll be the destination in the SAML response for IDP-initiated SSO
	u be the destination in the SAML response for IDP-initiated SSO
	II be the destination in the SAML response for IDP-initiated SSO
The default reply URL	u be the destination in the SAML response for IDP-initiated SSO
	II be the destination in the SAML response for IDP-initiated SSO

Figure 6: Basic SAML Configuration

#### 7. Edit the User Attributes & Claims section.

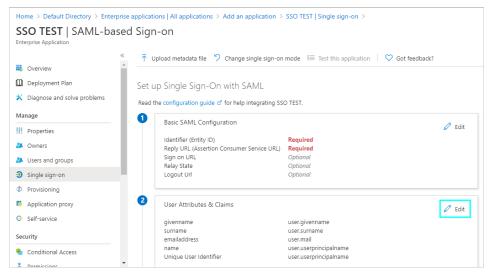


Figure 7: Edit the User Attributes & Claims section

#### 8. Select + Add new claim.

E Microsoft Azure      P Search resource	es, services, and docs (G+/)	$\sum$
Home > Default Directory > Enterprise applicat	ions   All applications $ ightarrow$ Add an application $ ightarrow$ SSO TEST   Single sign-on $ ightarrow$ SAML-based Sign-o	on >
User Attributes & Claims		
+ Add new claim + Add a group claim ≡≣	Columns	
Required claim		
Claim name	Value	
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for ***	
Additional claims		
Claim name	Value	
Figure 8: Add new claim		



#### 9. On the Manage claim page, enter these values:

#### Name: email

Note: Write 'email' in lower-case letters only.

#### Source: Attribute

#### Source attribute: **user.mail**

	applications   All applications > Add an application > SSO TEST   Single sign-on > SAML-based Sign-on > User Attributes & Claims >	
Manage claim		×
🔚 Save 🗙 Discard changes		
Name *	email	~
Namespace	Enter a namespace URI	~
Source *	Attribute      Transformation	
Source attribute *	usermail	$\sim$
✓ Claim conditions		

#### Figure 9: Manage claim

Once you've defined these values, click **Save**.

≡ Microsoft Azure	∠P Search resources, services, and docs (G+/)	Σ	Ŗ	Ç2	۲	?	$\odot$				
Home > Default Directory	> Enterprise applications   All applications $>$ Add an application $>$ SSO TEST   Single sign-on $>$										
SSO TEST   SAM	O TEST   SAML-based Sign-on										
Sverview		ck?									
Deployment Plan	email user.mail Unique User Identifier user.userprincipalname										
🗙 Diagnose and solve probl	ems										
Manage	3 SAML Signing Certificate		🧷 Edi	it.							
Properties	Status Active										
A Owners	Thumbprint 6BFDCA0C330A751F94E43D876A13BA8316C47A74 Expiration 8/18/2023, 5:11:21 PM										
Users and groups	Notification Email n v@gmail.com App Federation Metadata Url https://login.microsoftonline.com/5c5d8bcc-61d6	D									
Single sign-on	Certificate (Base64) Download										
Provisioning	Certificate (Raw) Download Federation Metadata XML Download										
Application proxy	Federation Metadata XML Download										
Self-service	4 Set up SSO TEST										
Security	You'll need to configure the application to link with Azure AD.										
🍨 Conditional Access	Login URL https://login.microsoftonline.com/5c5d8bcc-61d6	D									
2 Dormissions	<ul> <li>Azura AD Idantifiar</li> </ul>	E.									

10. Access the SAML Signing Certificate by downloading the Certificate (Base64) option.

Figure 10: Download certificate

**11.** Go to OnceHub. You've already taken care of the first part, **Required by identity provider**, within Azure AD. In the second part, **Required by OnceHub**, you'll need specific field values from Azure AD that you can copy and configure within OnceHub.

This includes the **Entity ID**, **Single sign-on URL**, and the **Public x509 certificate**. You've already downloaded the certificate. You can grab the other values in Azure AD next to the **4**.

	n resources, services, and docs (G+/)	≥_		P		
Home > Default Directory > Enterpris	applications   All applications $>$ Add an application $>$ SSO TEST   Single sign-on $>$					
SSO TEST   SAML-base	d Sign-on					
«	↑ Upload metadata file ? Change single sign-on mode I Test this application Soft feed	back?				
III. Overview	Certificate (Raw) Download Federation Metadata XML Download					
Deployment Plan	Federation Metadata XML Download					
X Diagnose and solve problems	Set up SSO TEST			۲		
Manage				_		
H Properties	You'll need to configure the application to link with Azure AD.			_		
A Owners	Login URL https://login.microsoftonline.com/5c5d8bcc-61d	6 🗈		_		
	Azure AD Identifier https://sts.windows.net/5c5d8bcc-61d6-4dca-b3	8 🗅		_		
Users and groups	Logout URL https://login.microsoftonline.com/common/wsfe	d 🗈		_		
Single sign-on	View step-by-step instructions					
Provisioning				_		
Application proxy	5 Test single sign-on with SSO TEST					
Self-service	Test to see if single sign-on is working. Users will need to be added to Users and groups before th	ey can si	gn in.			
Security	Test					
Conditional Access				_		

Figure 11: Required by OnceHub step

In OnceHub
Entity ID
IDP single sign-on URL
Public x509 certificate

**12.** For the certificate field, open the downloaded certificate and copy all contents.



SSO TEST - Notepad
File Edit Format View Help
BEGIN CERTIFICATE
MIIC8DCCAdigAwIBAgIQFbyxIQ8paYVBYzvdVnTcvzANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
Ey1NaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMDA4MTgxMTQx
MjFaFw0yMzA4MTgxMTQxMjFaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWR1cmF0ZWQg
U1NPIENlcnRpZmljYXR1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0GFnpwsSjMp3
v982UjaaA1DLFb/Cxag2G6YY/9c0J61iz/1nxCeeuWV2R7S2LSc7PG80s48GeD7HL8UvvWgrtqYL
KXrG5s3zc3hYIjG6bkxgiBr3ziT6eCee+2ylw1q6Pkrh0rdpcKixqqGh0qIQ0fKvXPo5TXcqAEF7
CdnG7CLh2CTo8hx1giBwC81Ctsu7yeU0rHkeWVULKEandCZMPJfoC+qmSWVTFsPh61M+dP/1MZgw
kAlLxLEm5D/CGwRW6eUO3rL4CKmRHzM4WI970wtFNjyVH1E1J8oNV/vMwD7U42+7RoaHu1AvHP1m
BJh5E8h8tBeJVizrCLU1auhQkQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBmtmZ0FnPhoFFWTT2b
4cNz00uJtD0Z011PYn0QmwmdJ9Vx60gTNEx3JgawftNW0IWPsDDbjKoUU5aKI0EbNeLwFZFISnV+
2buH87c7T7NyI0m3kw77Hs7VXBe/vT+uYorURksBY2fYGpFhD+A0C1oXzgAJo1TL1UMxuE3RKU+d
5Q9TVF1qVfBe1g0xSQeu+BoIYTJ5LjA5hNJGCQ/4amiL8HMJ0mHuf0ufTIJdGrIofVaJ/9SQTOge
v/WfS8jr2EFtUi2LMvvdXgimeA0t8WuvABUgct2UJ17rhx6esyZwyxS26A8iE0KzOCeBPgEQHfX9
shasvOkkN3oTBcZuOzjm
END CERTIFICATE

Figure 12: Copy whole contents of certificate text

13. In Azure AD, go to the left menu and select Users and groups. On that page, select + Add user.

Home > Default Directory > Enterp	rise applications   All applications $\geq$ Add an app	lication >		
SSO TEST   Users	and groups			×
<ul> <li>Overview</li> <li>Deployment Plan</li> <li>Diagnose and solve problems</li> </ul>	<ul> <li>Add user  Ø Edit    Remove  Ø Update Credentials      E Columns    ♥ Got feedback?</li> <li>The application will appear on the Access Ranel For assigned users. Set Visible to users? to no in properties to prevent this. →</li> <li>First 100 shown, to search all users &amp; groups, enter a display name.</li> </ul>			
Manage	Display Name	Object Type	Role assigned	
Properties	No application assignments found			
A Owners				
Users and groups				
Single sign-on				
Provisioning				
Application proxy				
Self-service				
Security				
Conditional Access				

14. On the Add Assignment page, search for relevant users or groups. Select them and click Assign when ready.

#### Verify configuration

OnceHub will speak to your identity provider and verify that the configuration has the correct values on both sides to proceed.

SAML configuration			? ×
Required by identity provider	Required by OnceHub	Verify configuration	
	<u>نې</u>		
SAML a	uthentication verif	ied	
Authentication verified with your identi	ty provider		
<ul> <li>✓ Identity provider found</li> </ul>			
<ul> <li>Received SAML response</li> </ul>			
			Close

Figure 14: Verify configuration

#### Enable SSO for all users

Once you've verified your SSO configuration, you can select the **Enable SSO for all users** toggle. All Users in your OnceHub account can now access their account using SSO.

### ! Important:

Before you enable the account, make sure all your Users have matching email addresses for their OnceHub User profile and their Azure profile.

Once SSO is enabled, they **will not** be able to change their OnceHub email.

If their OnceHub email does not match the email in their IDP profile, they **will not** be able to log in.

Security
SSO
SAML-based SSO allows your Users to sign into OnceHub using your organization's identity provider. Learn more
Setup SAML configuration for SSO
Enable SSO for all users
(i) Once SSO is enabled, all users in your account will require to sign in with SSO and won't be able to sign in using password.

Figure 15: Enable SSO for all users

### (i) Note:

If existing Users were already signing into OnceHub using an email and password, they will no longer be able to do so. They will only be able to sign in using SSO.