### Configuring SSO with Azure

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.

≡ Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)	▶_	R	Q			
Home > Default Directory >							
Enterprise ap Default Directory - Azure A	plications   All applications						
Overview	How application     E     Columns     Kei Preview features     Got feedback?						
0 Overview	🖉 Try out the new Enterprise Apps search preview! Click to enable the preview. $ ightarrow$						
× Diagnose and solve problem	15 Application type Applications status Application visibility						
Manage	Enterprise Applications V Any V Any	~	Appl	/	Rese	ſt	
All applications	First 50 shown, to search all of your applications, enter a display name or the application ID.	First 50 shown, to search all of your applications, enter a display name or the application ID.					
Application proxy	Name Homepage URL O	bject ID					

Figure 1: New application

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

■ Microsoft Azure	$\mathcal P$ Search resources, services	s, and docs (G+/)	
Home > Default Directory > Add an applicati	Enterprise applications   All     On	applications >	
Click here to try out the n	ew and improved app gallery. $\rightarrow$		
Add your own app			
Application you're developing Register an app you're working on to integrate it with Azure AD	On-premises application Configure Azure AD Application Proxy to enable secure remote access.	Non-gallery application	
Add from the gallery			
Category			_
All (3560)		````	×
Enter a name			$\checkmark$

Figure 2: Non-gallery application

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 * 🕕	
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: (i)	
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.

Home > Default Directory > Enterprise ap	oplications   All applications > Add an application >		
SSO TEST   Single sign	n-on		×
🗰 Overview	Select a single sign-on method	Help me decide	
Deployment Plan	-		
X Diagnose and solve problems	Disabled	C SAML	Password-based
Manage	won't be able to launch the app from	applications using the SAML (Security	web browser extension or mobile app.
Properties	My Apps.	Assertion Markup Language) protocol.	
A Owners			
Users and groups			
Single sign-on			
Provisioning	Linked Link to an application in the Azure		
Application proxy	Active Directory Access Panel and/or Office 365 application launcher.		
G 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.

Basic SAML	Configura	tion			
Save					
dentifier (Entity	D)* i				
The default identifier	will be the audiend	e of the SAML re	sponse for IDP-i	nitiated SSO	
Reply URL (Asser	ion Consumer :	Service URL)	• ()		
Reply URL (Asser The default reply URI	ion Consumer : will be the destina	Service URL)	i) response for IDI	P-initiated SSO	
Reply URL (Asser	ion Consumer s	Service URL)	i response for ID	P-initiated SSO	
Reply URL (Asser	ion Consumer (	Service URL) tion in the SAML	۲۰ آن response for IDI	P-initiated SSO	
Reply URL (Asser	ion Consumer (	Service URL) tion in the SAML	* ① . response for ID	P-initiated SSO	
Reply URL (Asser The default reply URL	ion Consumer	Service URL)	response for IDI	P-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.

■ Microsoft Azure	pcs (G+/)	$\geq$
Home > Default Directory > Enterprise applications   All applicat	ions $>$ Add an application $>$ SSO TEST   Single sign-on $>$ SAML-based Sign-	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**

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

#### Figure 9: Manage claim

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

= Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)	E 🖟 🗘 🔅 ? 😊
Home > Default Directory	Enterprise applications   All applications $>$ Add an application $>$ SSO T	'EST   Single sign-on >
SSO TEST   SAM	based Sign-on	
. Overview		I Test this application Soft feedback?
Deployment Plan	email user.n Unique User Identifier user.u	nail userprincipalname
🗙 Diagnose and solve probl	ms	
Manage	3 SAML Signing Certificate	🖉 Edit
Properties	Status Active	2
A Owners	Thumbprint 6BFD Expiration 8/18/	CA0C330A751F94E43D876A13BA8316C47A74 (2023. 5:11:21 PM
Users and groups	Notification Email n App Federation Metadata Url	1@gmail.com
Single sign-on	Certificate (Base64) Down	Non the solution of the soluti
Provisioning	Certificate (Raw) Down	Noad
Application proxy		1000
Self-service	4 Set up SSO TEST	
Security	You'll need to configure the application to link with A	Azure AD.
🍨 Conditional Access	Login URL http	ps://login.microsoftonline.com/5c5d8bcc-61d6
2 Dormissions	<ul> <li>Azura AD Identifiar</li> </ul>	

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**.

■ Microsoft Azure P Search resource	es, services, and docs (G+/)		⊵	Ŗ	Ç		$\odot$
Home > Default Directory > Enterprise applicat	ions   All applications > Add an applicat	ion > SSO TEST   Single sign-on >					
SSO TEST   SAML-based Sign	n-on						
×	Upload metadata file 🏼 🏷 Change single si	gn-on mode 🛛 🗏 Test this application 🗍 🛇 Got feed	back?				
III Overview	Certificate (Raw)	Download					
Deployment Plan	Federation Metadata XML	Download					
X Diagnose and solve problems	Cabura SCO TEST				-		
Manage	Set up SSO TEST						
+ Properties	You'll need to configure the application	to link with Azure AD.					
• •	Login URL	https://login.microsoftonline.com/5c5d8bcc-61d	6 🗈				
Whens Owners	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	Test single sign-on with SSO TEST						
⊖ Self-service	Test to see if single sign-on is working.	Jsers 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 Azure AD	In OnceHub
Azure AD Identifier	Entity ID
Login URL	IDP single sign-on URL
Certificate (Base64) - Download and copy/paste whole contents	Public x509 certificate

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



SSU IEST - Notepad	
File Edit Format View Help	
BEGIN CERTIFICATE	
MIIC8DCCAdigAwIBAgIQFbyxIQ8paYVBYzvdVnTcvzANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD	
Ey1NaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMDA4MTgxMTQx	
MjFaFw0yMzA4MTgxMTQxMjFaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWR1cmF0ZWQg	
U1NPIEN1cnRpZmljYXR1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0GFnpwsSjMp3	
v982UjaaA1DLFb/Cxag2G6YY/9c0J6liz/lnxCeeuWV2R7S2LSc7PG80s48GeD7HL8UvvWgrtqYL	
KXrG5s3zc3hYIjG6bkxgiBr3ziT6eCee+2ylw1q6Pkrh0rdpcKixqqGh0qIQ0fKvXPo5TXcqAEF7	
CdnG7CLh2CTo8hx1giBwC81Ctsu7yeU0rHkeWVULKEandCZMPJfoC+qmSWVTFsPh61M+dP/1MZgw	
kAlLxLEm5D/CGwRW6eUO3rL4CKmRHzM4WI970wtFNjyVH1E1J8oNV/vMwD7U42+7RoaHulAvHPlm	
BJh5E8h8tBeJVizrCLU1auhQkQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBmtmZ0FnPhoFFWTT2b	
4cNz00uJtD0Z011PYn0QmwmdJ9Vx60gTNEx3JgawftNW0IWPsDDbjKoUU5aKI0EbNeLwFZFISnV+	
2buH87c7T7NyI0m3kw77Hs7VXBe/vT+uYorURksBY2fYGpFhD+A0C1oXzgAJo1TL1UMxuE3RKU+d	
5Q9TVFlqVfBelg0xSQeu+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>	K → Add user      C Edit      Edit      Prepapilication will appear on the Access Panel for assigned users. Set Visible to users? to no in properties to prevent this. →      First 100 shown to search all users & oncours enter a disclar name.			
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	
SAML a	uthentication verif	ïed	
Authentication verified with your ident	ity provider		
✓ Identity provider found			
✓ Received SAML response			
			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 Setup
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.