

Configuring SSO with OneLogin

Last Modified on Oct 26, 2020

This article provides a step-by-step guide to configuring SSO between OnceHub and OneLogin.

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 OneLogin. The person configuring in OneLogin 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 OneLogin.

1. Add SAML Test Connector (Advanced)

In OneLogin, go to **Administration** -> **Applications**. Search for **SAML Test Connector (Advanced)** and select (making sure to select the SAML 2.0 version).

onelog	gin _{Users}	Applications	Devices	Authentication	Activity	Security	Settings	Developers	
Find	Applications								
Q sam	d								
M	Adobe Creative Cloud Adobe Systems Inc	(SP initiated SAML)							SAML2.0
Ó	Bitdefender SAML SP OneLogin, Inc.	launcher							Form-based auth , browser extension
3	Google SAML Quicklin Google Inc.	nk							SAML2.0
INTRA UNKS	Intralinks SAML OneLogin, Inc.								SAML2.0
SINGLE SIGN ON	JIRA/Confluence (wit re:solution	h Resolution SAML Si	ngleSignOn)						SAML2.0
3	Pilot Catastrophe SAI OneLogin, Inc.	ML (IdP)							SAML2.0
3	SAML 1.1 Test Conne OneLogin, Inc.	ctor (Advanced)							SAML1.1
٩	SAML Test Connector OneLogin, Inc.	(Advanced)							SAML2.0
0	SAML Test Connector OneLogin, Inc.	(SP Shibboleth)							SAML2.0
3	SCIM Provisioner with OneLogin, Inc.	n SAML (Core Schema	a v1.1)						SAML2.0 , provisioning

Figure 1: Select SAML Test Connector (Advanced)

2. Configuration

Give the app a name (for instance, OnceHub) and fill out the other settings.

OnceHub Support

onelogin Users	Applications Devices Authentication Activity Security Settings Developers
App Listing / Add SAML Test Con	nector (Advanced)
Configuration	Portal Display Name OnceHub Visible in portal
	Retangular Icon Square Icon
	Upload an kon with an aspect-ratio of 2.641 as either a transparent. PNG or .SVG
	200 characters

Figure 3: Display Name settings

3. Configuration - Application details

On the **Application details** page, fill out the SAML settings. You can grab these values in OnceHub, on the **Required by identity provider** step.

onelogin	Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers
Applications / SAML Test C	Connector	(Advanced)						
Info		Applicat	tion details					
Configuration		RelayState						
Parameters								
Rules		Audience ((EntityID)					
SSO		1						
Access		Recipient						
Users								
Privileges		ACS (Cons	umer) URL Vali	dator*				
Setup								
		i *Req	quired.					
		ACS (Cons	umer) URL*					
		(i) *Req	quired					
		Single Log	out URL					
		Jingio Log						
		Login URL						
		(i) Only	required if you	select Service Provider	as the SAML Ini	tiater.		

Figure 4: Configure Application details

In OneLogin	In OnceHub
Audience (EntityID)	Identifier URL
ACS (Consumer) URL Validator	ACS URL
ACS (Consumer) URL	ACS URL

[Not required; OneLogin refers to ACS URL for this function]

Single sign-on URL

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

4. Parameters

Create a new field by clicking the + button. For the **Field name**, use **email** (in lower case). Map this to the **Value** field **Email**. Select **Save**.

onelogin Users A		Security Settings Developers				
		Edit Field email				
	Credentials are Configured by admin Configured by admins and shared by all users	Edit Field email				
	SAML Test Connector (Advanced) Field	Value Email				
		Flags custom parameter				
		Cancel Delete Save				

Figure 5: Select Email as the value

5. Grab information from OneLogin and paste in OnceHub

On the **SSO** step, grab the information you will add in OnceHub. Once added, go back to OneLogin before you click **Verify** in OnceHub.

onelogin	Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers
Applications / SAML Test Co	nnector	(Advanced)						
Info Configuration Parameters Rules SSO Access		Change	thod ficate					
Users Privileges		SHA-1 Issuer URL https://a	op.onelogin.c	om/saml/metadata/5	• 5a74224-7fe	7-4762-998e-ae7c	c2adc471	ß
Setup		SAML 2.0 E	ndpoint (HTTF					
		SLO Endpoi		ev.onelogin.com/trust	t/saml2/http-	redirect/slo/1258	896	6

Figure 6:

Enable SAML 2.0 by grabbing information to paste in OnceHub

OnceHub Support

Certificates / Standard Stre	ngth Cei	rtificate (2048	3-bit)			
Key length						
2048-bit						
SHA fingerprint						
SHA1		•				
Fingerprint						
71:45:F9:96:65:F6:	0A:63:8F:89	:2A:16:F9:2C:60:E7:	70:95:D8:B7		6	
o4HIMIHFMAwGA1Ud cbxhMIGFBgNVHSME A1UECgwMT25jZWh1 BAMMEU9uZUxvZ21u	uL2PsddPV4 EwEB/wQCMAJ fjB8gBRt290 YiB0ZXN0MRI IEFjY291bn(PW6xSQNMdB7YkdWn31 AwHQYDVR00BBYEFG31 CU6qvFEf23JFtsb1a52 UwEwYDVQQLDAxPbmV/ QgghQm3kwekopq7MUI CMQGFEQADpggEBA13	olxTqq8UR/YkW QynG8YaFOpEww Mb2dpbiBJZFAx MW6blvIlIsxxJ	2xuJpJDK SjEVMBMG GjAYBgNV MjAOBgNV	^ I <u>C</u>	
Y27rRtnHKBV8e+Oa	zQWo3kU87vj OM11xvqOe0	pVmInJmH9fyZTpsyV FdQxTIekE2G+y8cP0	a2cdWZmsvSTjW BU8Ia3GjJRSjy	1Yq1Kk/W aP58Mbod		
				ZOSUDOIX		
v2Ig97pX4uM6aeJu		-	-			
v2Ig97pX4uM6aeJu wxbkQdJzrcESfxUb	tI1p8cJf7h	6/CZKvH1K7NgS0dcx: w2kUcREN7ctze8Pd3; ZZeSZUYbiNzKrpgd2;	3tAEOmMb+ls7u	Y5pn15QC		

Figure 7: X.509 Certificate

In OneLogin	In OnceHub
Issuer URL	Entity ID
SAML 2.0 Endpoint (HTTP)	IDP single sign-on URL
X.509 Certificate (select View Details to copy)	Public x509 certificate

Important:

For the Public x509 certificate, include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- syntax in your selection and paste it all into the OnceHub field.

6. Add users

On the Users step, add the relevant users in OneLogin to your new app.

onelogin Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers
Applications / SAML Test Connector	(Advanced)						
Info	Search		All roles	 All group 	08 -		
Configuration	User						
Parameters Rules	thoma	s vdmeulen					
SSO							Showing 1-1 of 1 users
Access							
Users							
Privileges							
Setup							

Figure 8: Add users

Follow the rest of the steps in OneLogin to complete setup.

7. Verify

In OnceHub, click **Verify** to confirm that SAML authentication is verified.

SAML configuration			? ×
Required by identity provider	Required by OnceHub	Verify configuration	
	£\$}~		
SAML au	uthentication verif	ied	
Authentication verified with your identit	y provider		
✓ Identity provider found			
✓ Received SAML response			
			Close

Figure 9: Verify configuration

8. 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 OneLogin 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.