# Configuring SSO with Okta

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

### 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 Okta. The person configuring in Okta 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 Okta.

Make sure you're in the Classic UI. You can select this by going to Developer Console -> Classic UI.

#### 1. Create a New Application Integration

#### In Okta, go to **Applications** -> **Create New App**.

okta Get S	3 Dashboard	Directory Applications			Upgrade	My Apps 🔿
← Back to Applications	<sup>s</sup> cation					Create New App
CATEGORIES		O Search				
Featured		Q Search				
API Management	1	Featured Integrations	5			See all
Apps	1277					0
Apps for Good	11	Active Directo	pry 4	ATLASSIAN	Do	cuSign.
CASB	2	Active Directory	Atlac	sian Cloud	DocuSia	n
Directories and HR S	ystems 10	Provisioning	SAML,	Provisioning	SAML, Prov	isioning
Security Applications	232					
Okta Applications	6					

Figure 1: Create New App

In the popup, select Web. The sign on method should be SAML 2.0. Click Create.

okta Get Starte	3 Dashboard	Directory Applications	Security Workflow Reports Settings	Upgrade My Apps (
← Back to Applications	Create a New .	Application Integration		× Create New A
CATEGORIES	Platform	W	eb 🔹	
Featured API Management	Sign on method	۲	SAML 2.0 Uses the SAML protocol to log users into the ap	p.
Apps Apps for Good CASB		0	OpenID Connect Uses the OpenID Connect protocol to log users you've built.	cu Sign.
Directories and HR Syste Security Applications				risioning
Okta Applications Okta Test Applications			Create	Cancel
VPN		🚏 slack	workday.	zoom
		Slack SAML, Provisioning	Workday SAML, Provisioning	Zoom SAML SAML, Provisioning

Figure 2: Create a New Application Integration

### 2. General Settings

On the Create SAML Integration page, give the app a name (for instance, OnceHub) and fill out the General Settings.

okta	Get Started			Applications					Upgrade	My Apps 😝
👯 Creat	e SAML In	tegration								
	1 General S	Settings			2 Configu	ure SAML			3 Feed	lback
1 Genera	al Settings		OnceHub	9.550						
App logo	(optional) 👔		-	Ö						
			Upload L	.ogo			Brov	VS8		
			Requireme • Must t • Less t	ents De PNG, JPG or G han 1MB	θIF					

Figure 3: General Settings

3. SAML Settings from OnceHub

On the **Configure SAML** step, fill out the SAML Settings. You can grab these values in OnceHub, on the **Required by identity provider** step.

1 General Settings		2 Configure SAML	3 Feedback
SAML Settings			
·			What does this form do?
GENERAL			This form generates the XML needed for the app's SAML request.
Single sign on URL 👔			Where do I find the info this form need
✓ Use t ☐ Allow		his for Recipient URL and Destination URL this app to request other SSO URLs	The app you're trying to Integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information un
Audience URI (SP Entity ID) 👔			need to specify in this form.
Default RelayState 🕘			Okta Certificate
	lf no valu	e is set, a blank RelayState is sent	Import the Okta certificate to your Identit Provider if required.
Name ID format	Unspec	fied v	🛃 Download Okta Certificate

Figure 4: Configure SAML Settings

In Okta	In OnceHub
Audience URI (SP Entity ID)	Identifier URL
Single sign on URL + Select checkbox <b>Use this for Recipient URL and Destination</b> <b>URL</b>	ACS URL
[Not required; Okta refers to ACS URL for this function]	Single sign-on URL

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

#### 4. Add an Attribute Statement

For the Name field, use email (in lower case). Map this to the Value field user.email.

You can keep the Name format on Unspecified.

ATTRIBUTE STAT	EMENTS (OPTIONAL)		LEARN MOR
Name	Name format (optional)	Value	
email	Unspecified 💌	user.email	•
	TE STATEMENTS (OPTIONAL)		
GROUP ATTRIBU	TE STATEMENTS (OPTIONAL)	Filter	
GROUP ATTRIBU	TE STATEMENTS (OPTIONAL)	Filter	

Figure 5: Attribute Statement for email

Once you're ready, click on **Next** and then **Finish**.

#### 5. Grab information from Okta and paste in OnceHub

Click on View Setup instructions, which provide the information you will add in OnceHub.

OnceHub SSO	
General Sign On Mobile Import Assignments	
Settings Edit	
SIGN ON METHODS The sign-on method determines how a user signs into and manages their credentials for an application. Some sign- on methods require additional configuration in the 3rd party application. Application username is determined by the user profile mapping. Configure profile mapping SAML 2.0	
Default Relay State	
<ul> <li>SAML 2.0 is not configured until you complete the setup instructions.</li> <li>View Setup Instructions</li> <li>Identity Provider metadata is available if this application supports dynamic configuration.</li> </ul>	

Figure 6: View Setup Instructions

Hov	v to Configure SAML 2.0 for OnceHub SSO Application
The	following is needed to configure OnceHub SSO
1	Identity Provider Single Sign-On URL:
	https://dev-243907.okta.com/app/oncehubdev243907_oncehubsso_1/exkqluovqUgHJ1c1a4x6/sso/sam1
2	Identity Provider Issuer:
	http://www.okta.com/exkqluovqUgHJicia4x6
3	X.509 Certificate:
	BEGIN CERTIFICATE NIIDDDCCA0V0AWIBADICAXI ETVVVVAARCSdSIb3D0FECwIANICSM05wC0YDVD0GEw.JVU2FTM8FG
	A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
	HBIGA1UECWWLUVINPUHJvdnILXXIXEZARBGNVBAMMCmR10109NDMSMDcxHDAaBgkchkiAgwoBCQEW
	uwiuzmyaoztoisojozowinnonwjawnyiwniazwzmywnonwzawnyiwniazuunywjUBkjELMAKGA1UE BhMCVVMxEzARBgNVBAgMCkNhbG1mb3JuaWExF;AUBgNVBAcMDVNhbiBGcmFuY21zY28xDTALBgNV

Figure 7: Information from Okta required in OnceHub

In Okta	In OnceHub
Identity Provider Issuer	Entity ID
Identity Provider Single Sign-On URL	IDP single sign-on URL
X.509 Certificate	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. Assignments

Before clicking Verify in OnceHub, go back to Okta and access **Assignments**. Click on the **Assign** dropdown and select **Assign to People**.

← Back to Applications OnceHub	SSO View Logs		
General Sign On Mobile	Import Assignments		
Assign 🔻 🖌 Convert Assignments		Q Search	People 🔻
Assign to People	Туре		
Assign to Groups			
Groups	]		

Figure 8: Assign to People

Assign your new OnceHub SAML 2.0 application to the relevant people in Okta.

### 7. Verify

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

SAMI	L configuration			? ×				
	Required by identity provider	Required by OnceHub	Verify configuration					
		<u>{</u>						
	SAML at	uthentication verif	ied					
Authentication verified with your identity provider								
🗸 Ider	✓ Identity provider found							
🗸 Rec	eived 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 Okta 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.