

<u>In Okta</u> In Wepow

The first step in configuring an application to support SAML based Single Sign-On from Okta is to set up an application in Okta.

In Okta

Here is how to set up a SAML application in Okta:

1. Click on the blue Admin button

okta	Q 🕈 Home 🌲 - 主 Dev -	+ Add Apps	Admin
-	Welcome to Okta Developer Edition		0
1	Here are some useful links to get started:		
	Okta Developer Documentation		
	Create an API token		
	Enable CORS for your domain		
	Create an OpenID Connect web application		
	Create an Authorization Server for API Access Management		

2. Click on the Add Applications shortcut



3. Click on the green Create New App button

okta Deshboerd Di	rectory Applications							Му Ар	plications	•
Back to Applications										
QI		A	авсо	EFGHI	ЈКСМ	NOF	QR	зтυν	wx v	ΥZ
Can't find an app? Create New App	O TELADOC	Teladoc Okta Verified							Add	
Apps you created (0) \rightarrow	&frankly	&frankly Okta Vertfled ~	SAML						Add	
INTEGRATION PROPERTIES	•	10000ft Okta Verified							Add	
Supports SAML Supports Provisioning	[]]/damain	101domains.com Okta Verified							Add	

4. In the dialog that opens, select the SAML 2.0 option, then click the green Create button

Create a New Application Integration		×
Platform	Web	
Sign on method	 Secure Web Authentication (SWA) Users credentials to sign in. This integration works with most apps. 	
	 SAML 2.0 Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it. 	
	OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.	
	Create	4

5. In Step 1 General Settings, enter Example SAML Application in the App name field, then click the green Next button.

1 General Setting:	5	2 Configure SAML		3 Feedback
1 General Settings				
App name	Wepow	v		This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.
App logo (optional) 🔘		Ø		
	Uploa	d Logo	trowse.	
App visibility	Do n	not display application icon to users not display application icon in the Okta Mobile app		
Cancel			Next	

6. In Step 2 Configure SAML, section A SAML Settings, create the Single sign on

URL https://wepowsubdomain.wepowapp.com/sso/saml/consume For the recipient, destination URLs use https://wepowapp.com. For "Audience URI" wepowapp.com. Select "Name ID format" and set to "EmailAddress" and "Application username" set to "Email"

		What does this form do?
SENERAL		This form generates the XML needed for the app's SAML request.
lingle sign on URL 🔘	https://okta.wepowapp.com/sso/sami/consume	Where do I find the info this form needs
	Use this for Recipient URL and Destination URL	The app you're trying to integrate with
	Allow this app to request other S50 URLs	should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you
lecipient URL	https://wepowapp.com	need to specify in this form.
Destination URL	https://wepowapp.com	Okta Certificate
Audience URI (SP Entity ID)	wepowapp.com	Import the Okta certificate to your identity Provider if required.
Default RelayState 🔘		🛓 Download Okta Certificate
	If no value is set, a blank RelayState is sent	
Name ID format	EmailAddress *	
Application username	Email	

Select "Name ID format" and set to "EmailAddress" and "Aplication username" set to "Email"

- 7. In the Attribute Statements section, add three attribute statements:
 - 1. FirstName set to user.firstName
 - 2. LastName set to user.lastName



- 3. Email set to user.email
- 4. "is_owner" set to isMemberOfGroupName("WepowOwner") ? "true" : "false"
- 5. "wepow_team_1" set to "isMemberOfGroupName("Engineering") ? "Engineering" : null" 6. "wepow_role_1" set to "isMemberOfGroupName("Engineering") ? "admin" : null"

Name	Name format (optional)	Value	
first_name	Unspecified v	user.firstName	•
last_name	Unspecified v	user.lastName	-
ls_owner	Unspecified •	isMemberOfGroupName("WepowOwner")? "t	-
wepow_team_1	Unspecified *	isMemberOfGroupName("Engineering") ? "En	-
wepow_role_1	Unspecified *	isMemberOfGroupName("Engineering") ? "ad	-
Email	Unspecified v	user.email	

Click Next to continue.

8. In Step 3 Feedback, select I[™]m an Okta customer adding an internal app, and This is an internal app that we have created, then click Finish.

i this application	Why are you asking me this?
customer adding an internal app	This form provides: Okta Support with us background information about your app Thank you for your helpwe appreciate
n understanding your app integration.	
ternal app that we have created	
	this application customer adding an internal app are vendor. I'd like to integrate my app with Okca in understanding your app integration.



9. The Sign On section of your newly created Example SAML Application application appears. Keep this page open in a separate tab or browser window. You will return to this page later in this guide and copy the Identity Provider metadata link.

(To copy that link, right-click on the Identity Provider metadata link and select Copy)

ellelal	Sign On Import	Assignments	
Settings			Edit
SIGN ON	METHODS		
The sign- on metho	on method determines ho ods require additional confi	w a user signs into and manages their credenti guration in the 3rd party application.	als for an application. Some sign-
SAN	/IL 2.0		
I	Default Relay State		
⊜	SAML 2.0 is not config	ured until you complete the setup instructions.	
	View Setup Instruction	ata Copy this link ports dyna	amic configuration.
CREDEN	ITIALS DETAILS		
Applicatio	on username format	Email	

10. Right-click on the Assign Application section and select Open Link In New Tab (so that you can come back to the Sign On section later).

In the new tab that opens, click on the Assign button



11. A dialog titled Assign to people will open. Type your username into the search box, select the checkbox next to your username, then click the green Next button



General Sign Or	n Import	Assignments				
Assign 🔹 🥜 Cor	wert Assignments				Q Search	People *
Assign to People	Person			Туре		
Assign to Groups						
Groups						
				01101110 01101111 0110100 0110100 011011		
			Nº	o users tound		

12. You will be prompted to Enter user-specific attributes. Just click the green Confirm Assignments button to keep the defaults.

Assign TestWepow to People	×
Dev Ruiz	Assign
Guillermo Romero	Assign

You are now ready to configure SAML in your application. The information in the tab you opened in step #9 contains the information that you™II need to configure SAML in your application.

In Wepow

1. Enter to the Wepow App, and go to "My preferences"



	?	2 ~	
	My Preferences		
	Settings		
Soc	Switch Account		
	Sign out		

2. From the section "Organization Settings" click on Single Sign-on

Organization Settings
Organization Information
Teams
Privacy
Single Sign-on

3. Select the option "SAML 2.0 and go back to Okta and pull the information from step #9.



SAML 2.0

Wepow can be configured for SSO by Identity Providers such as OneLogin, Okta, Ping Identity and others using SAML 2.0 protocol.

X.509 Certificate

-----BEGIN CERTIFICATE

MIIDpDCCAoygAwlBAglGAV0uWN+JMA0GCSqGSIb3DQEBCwUAMlGSMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU MBIGA1UECwwLU1NPUHJvdmlKZXIxEzARBgNVBAMMCmRldi0xNDA5NTIxHDAaBgkqhkiG9w0BCQEW DWIuZm9Ab2t0YS5jb20wHhcNMTcwNzEwMjExMTQyWhcNMjcwNzEwMjExMjQyWjCBkjELMAkGA1UE BhMCVVMxEzARBgNVBAgMCkNhbGImb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2IzY28xDTALBgNV BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb32pZGVyMRIWEQYDVQQDDApkZYtIMTQwOTUyMRwwGgYJ KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMllBCgKCAQEA hj8KagfbOMNFkaYIOEc0bGcDDQxpf4ud9gtlDcJWnX3setZogyOX2p2sTmHC+NvZB4T9WfoAnP dJ1xqNPiAK9QGrV3hFWsDu6R26xhe0OFNi1De0PXzJKVuLj/+gDKPc090KFYfgRAEnRewLyxeWcs gL6SqLfeK19Xlo+mgKKhINKd3gR4BQGzZTSjEvdIhN3yF/hU+P73qlOum+fiBLjLekHwFDuE/VG GEEyTZb84vuQJ3ohP+rxrg1aYlosvZJinJnirNZJyFjIGSADFWRSikWsvBipqwrthVLWrWc/RmRk +zAkiSiqcODrZj/j9MBcaephIHIaiFYv+xBK8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBLpQPw EEVG3/6NHQCJ4XgiC6jo3hbRuHAjjkkykWjqSKbRK/A2IUSXo5L+NvXIzkQUFPDban6VGVEzja0 vUzAHRQ9dWGi2G0BQ-JBjBnHHESO+wqDBAvY/wriIZ069uLc9cHsEugnQBKuISXAcZAXgPfnUQj7 Trlav78YqouRj5NkCfdkPqrYTH2tr++FARNYVIO92/PEQR4k1/MfPhg2C7iKB5ztaWTFb0kd48 yXK83o1F52GdBdBMXndymzasZXrpFxut0wON4RFAyCcgHeKH8kXhQ/CszliOP6bHhMKpfhmV9MS0 tadViynVWz2Gwtaq5Cuk5FTHJAwD/1s ----END CERTIFICATE-----

SAML 2.0 Endpoint (HTTP)

https://dev-140952.oktapreview.com/app/wepowdev140952_wepow_1/exkb48w5tkMdeDN2o0h7/sso/saml

SLO Endpoint (HTTP)

Single Sign-on URL

https://oktappichardo.wepowapp.com/sso/saml/init?locale=en

Single Logout URL

https://oktappichardo.wepowapp.com/en/logout

Allow email/password login

Turn this off when you have completed testing login via your Identity Provider

Auto-provision users and teams

Automatically creates users and teams that match those on your Identity Provider

If "Auto-provision" is enabled, users should be created from Okta.

Thank you for using the Wepow Help Center! Our goal is to provide you with excellent customer service, and improve your experience when applying for a new job online!