Setting up Okta SAML Account Identity Provider

This topic describes how to set up Okta SAML as an account identity provider (IdP).

Prerequisites:

- Okta account
- Proofpoint Information Protection Platform ITM account
- From the **Proofpoint Information Protection Platform**, select the **Administration** app. Select **Settings** and complete the following settings (see IdP Configuration):
 - Kind: Select saml
 - Alias: Choose an Alias. You'll use this when you setup Okta SAML.
 - Name: Choose a Name. This will appear in the **Proofpoint Information Protection Platform** login page.
- Open both the **Proofpoint Information Protection Platform** and Okta dashboard so you will be able to copy/paste between them.

Important: This document was last update February 2021 and is accurate to that date.

Setting up from the Okta dashboard

- 1. Log in to your Okta account.
- 2. Select the Applications tab and in the Applications screen, click Add Application.
- 3. In the Add Application screen, select Create New App.

Q Search pe	eople, apps							observeit	Help and Support	Sign out
okta	Get Started		ory Applications						Му	Apps 🕣
Add Application More •										
Q Search										
STATUS	40	Confluence	Atlassian Confluen	ice Cloud						¢ •
INACTIVE	20	📲 Jira	Atlassian Jira Clou	d						¢ •
		AWS	BI @ ADMINS @ A\	WS						¢ •
		AWS	BI @ TroubleShoot	ing @ AWS						¢ •

- 4. In the Create a New Application Integration dialog box, do the following:
 - In the **Platform** field, select **Web** from the dropdown.
 - In the Sign on method, select SAML 2.0.
 - Click Create.

Create a New Application Integration	×
Platform	Web
Sign on method	 Secure Web Authentication (SWA) Uses 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 Cancel

5. In the Create SAML Integration screen, in General Settings tab provide an App name and optionally set up an App logo. Click Next.

6. In **Configure SAML** tab, fill in the following fields as shown:

Single sign on URL		Callba	ck URL				
	-	Use t	his for Recipient URL and Destination URL				
			this app to request other SSO URLs				
Recipient URL 🔘		Login URL					
Destination URL 🔞		Callba	Callback URL				
Audience URI (SP En	tity ID) 🌍	Alias					
Default RelayState	D						
o eroon newyonare q		If no value	e is set, a blank RelayState is sent				
			- na anna ar anna an tha na fanana na antar				
Name ID format 🔞		EmailAd	EmailAddress 👻				
Application usernam	e 🚯	Email •					
Update application u	sername on	Create and update *					
			Show Advanced Settings				
Name	Name format (optional)	Value				
Jane	Unspecified	i v	user.firstName •				
Doe	Unspecified	i v	user.lastName ×				
	STATEMENTS (OPT						
GROUP ATTRIBUTE	STATEMENTS (OPT	IONAL)					
Name	Name format	(optional)	Filter				
	Unspecifie	d v	Starts with v				

- Single Sign on URL: Copy Callback URL from the Create Provider dialog box in Proofpoint Information Protection Platform. Leave the check boxes blank.
- Recipient URL: Copy Login URL from the Create Provider dialog box in Proofpoint Information Protection Platform. (This field appears only after you have filled in the Single sign on URL.

- Destination URL: Copy Callback URL from the Create Provider dialog box in Proofpoint Information Protection Platform. (This field appears only after you have filled in the Single sign on URL.
- Audience URI: Copy the Alias you provided in the Create Provider dialog box in Proofpoint Information Protection Platform.
- Name ID format: Select EmailAdress from the dropdown.
- Application username: Select Email from the dropdown.
- Name: Complete the user firstName and user lastName values.
- Click Next
- 7. Provide the required feedback and click Finish.
- 8. From the Sign On tab, in the Settings, click View Setup Instructions.

Settings	Edit
SIGN ON METHODS	
The sign-on method determines how a user signs into and manages their credentials for an application on methods require additional configuration in the 3rd party application.	ion. Some sign-
Application username is determined by the user profile mapping. Configure profile mapping	
SAML 2.0	
Default Relay State	
SAML 2.0 is not configured until you complete the setup instructions.	
View Setup Instructions	
Identity Provider metadata is available if this application supports dynamic configuration	1.

9. Scroll down and you can see the fields you will need to copy.

he	following is needed to configure Sample SAML
0	Identity Provider Single Sign-On URL:
	https://proofpointtechwriter.okta.com/app/proofpointtechwriter_samplesaml_1/exk4ww1mjfnrr3Hkc5d6/sso/saml
2	Identity Provider Issuer:
	http://www.okta.com/exk4wwimjfnrr3Hkc5d6
3	X.509 Certificate:
	BEGIN CERTIFICATE
	A1UECAwKQ2FsaWZvcmöpYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
	MBIGA1UECwwLU1NPUHJvdm1k2XIXHTAbBgNVBAMMFHByb29mc09pbnR02vNod3Jpd0VyMRww0gYJ KoZIbycNACkBFo1obw2vCQC9yd0EvY29tMB4XDT1xMD1wM1A3NDc1MVoXDTNxMD1wM1A3NDc1MFow
	g2wstCzAJBgNVBAYTAIVTNRH#EQYDVQQIDApDYWxp2m9ybm1hMRY#FAYDVQHDAITY¥4g8nJhbmNp
	c2NvMQ0wCwYDVQQKDARPa3RhMRQwEgYDVQQLDAtTU09Qcm92aWR1cjEdMBsGA1UEAwwUcHJvb2Zw
	b21udHR1Y2h3cm10ZXIxHDAaBgkqhkiG9w08CQEWDW1uZm9Ab2t0YS5jb20wggEiMA0GCSqGSIb3
	DQEBAQUAA4IBDmAwggEKA0IBAQCMRIzxx03wc7yAYy1x1KfWmZx5Pby88WsznDDMAkyAgCh82FBb6 DQF///WWWJX4A#EE864C9-act/wEEX60DHBT/bcc//WUWUMDB10C/WWTEWDB2/wC20FFFFF
	00C//jkuma.dar.tom.box/star.tom.box/star.tom.tom.tom.tom.tom.tom.tom.tom.tom.tom
	QzuGzXIPusvWtXwGwzv7Gd1bUC11wXBVuPOvbtxHhLOSY/M1EusgcfufXoBgrZmTmXZCVHNh+1AX
	kNzjUkEW2f0d/uDCD9x2ycUIyQWkkv1ih2TEThqfQm5Wyd1310HiFiySjH1gqwzHAgMBAAEwDQYJ
	KoZIhvcNAQELBQADggEBAFonS14J5/vhzusPPeVBc15wJxbYilwz1LX0qebEXM0yewwxJpNimAg6
	nCU5cxBAMK7jtUVIIIAqRKEFNKMoPEPhwWi5dpYLZtZINDJd0YUmg5+W9L88gwwdup19jodiGwWR
	WXt1WYdg15/jpqQnKEc4ijxwQOOmFMxmmXtnkrYfSgA8LOwwJVBGzA8E1Fe3HsBJBg/XsOOE814b
	RfphAmTX21UDLEez4TINvDXWMZ1DayvpBn0oQx1z1jYV0/PavpNjaOLwMsByFuem8cw11LeJFV43
	7TK013NOMtt0P/EHFuJjYY0dau11d39IYmBmwemApOsVE+KHKQSCAYCVFyA=

10. Complete the following fields in the he **Create Provider** dialog box in Proofpoint Information Protection Platform from the Okta Settings as shown:

Create F	Provider
----------	----------

Kind

saml

Alias

sample-alias

Use only lowercase characters, dashes and underscores

Name

Sample IdP

Issuer

Identity Provider Issuer

Entry Point

Identity Provider Single Sign-On URL

Certificate

Certificate

Callback URL

https://app.us-east-1-ci1.dev.oit.proofpoint.com/v2/apis/auth/logins/san

Initiate Login URL

https://app.us-east-1-ci1.dev.oit.proofpoint.com/v2/apis/auth/logins/san



×

- Issuer: Copy Identity Provider Issuer.
- Entry Point: Copy Identity Provider Single Sign-On URL.
- Certificate: Copy the Certificate.

Click Save.