

WalkMe SAML Integration with Okta

Brief Overview

Use the Okta IDP Integration to easily validate end-user identities, enhance WalkMe content segmentation, and extend user behavior monitoring capabilities.

Use Cases

Connect WalkMe to Okta to:

- Identify users across applications for full visibility of digital usage trends at a large enterprise
- Segment DAP content by employee attributes so users only receive DAP guidance where it is relevant to them

Before You Get Started

Integration Requirements

To set up Okta integration for your organization, you must have the following:

- Be the Okta administrator of your company's Okta organization account
- Your company is currently using Okta as an identity provider
- You are able to install a new Okta application via Okta App Integration Catalog

Supported Features

The Service Provider (SP) Initiated Authentication Flow occurs when the end user attempts to interact with every website WalkMe is enabled on.

Supported Attributes

The following SAML attributes are supported:

Name	Value
email	user.email



Setup

Follow the below steps to install the WalkMe app via Okta App Integration Catalog. Once you install the WalkMe app, you will have to copy and paste the relevant information in the WalkMe Admin Center to complete the integration setup process.

Phase 1 - Install the WalkMe app via Okta App Integration Catalog

These steps must be done by an Okta Admin

1. In the Okta App Integration Catalog, click **Applications** in the left side menu and then click on **Browse App Catalog**

okta		Q Search			0 12	
Dashboard Directory	~	Applica	tions		Help	
Customizations	Ý	Create App	megnetic Browse A	pp Cata	alog In Users to App More *	
Applications	^	Q. Searc	h			
Self Service		STATUS		0	Okta Admin Console	
Security	Ý	ACTIVE INACTIVE	2	0	Okta Browser Plagin	
Workflow Reports	÷				Cikta Deehboard	
Settings	~					

2. Type WalkMe in the search bar under Browse App Integration Catalog



okta		Q Search	0 88
Dashboard	~		
Directory	~	Applications > Catalog > All Integrations	
Customizations	~	Browse App Integration Catalog	Create New App
Applications	^	Al Integrations Q Search	
Appecations Self Service		Apps for Good 9 All Integrations	Sort by: Default
Security	÷	Automation 26 Centralized Logging 11 FEATURED	See all
Workflow	~	Directory and HR Sync. 22	
Reports		Bot or Fraud Detection 3	
Settings	÷	Identity Proceiling 1D Identity Governance and 8 Administration (IGA)	
		Lifecycle Management 555	
		Multi-factor Authentication 28 (MFA)	
		Risk Signal Sharing 7	
		Social Login 18	
		Single Sign-On 6978	
		Zero Trust 52	

- 3. Select **WalkMe** from the list of suggested integrations
 - $\circ\,$ If "WalkMe" is not visible in the list, click See All Results to find WalkMe $\,$
 - Choose WalkMe (encrypted assertions) if you need the encrypted version

okta		Q Search		0 88
Dashboard	~			
Jirectory	~	Applications > Catalog > A	II Integrations	
Sustomizations	~	Browse App Int	tegration Ca	Creste New App
pplications	~	Use Case		
Applications		All Integrations	7907 Q Wa	alkMe 🛞
Relf Remise		Apps for Good	9 POPULAR	IEARCHES : Bookmark App SCIM 2.0 Test App Okts Org2Org Template App
Self Service		Automation	26	
ecurity	~	Centralized Logging	11	Wellate
orkflow	~	Directory and HR Sync	22	
		Bot or Fraud Detection	з	onde, anne
aporta	~	Identity Proofing	10	
ettings	Ý	Identity Governance and Administration (IGA)	8	WalkMe (encrypted assertion
		Lifecycle Management	655	and a state of
		Multi-factor Authentication (MFA)	28	EAM EAUL Monthow Templates EAM SUAL Menvilies Templates Workflows Connectors SCM Workflows Connectors SCM
		Risk Signal Sharing	7	
		Social Login	18	
		Single Sign-On	6978	
		Zero Trust	52	

4. Click Add Integration



okta		Q, Sarch	0 #
Dashboard	÷		
Directory	÷	Applications > Catalog > Single Sign-On > Walking	
Customizations	~		Cast updated: March 7, 2023
Applications	^		 Add Integration
Applications			
Self Service		me	WalkMe
Security	~		DIDC SAML
Workflow	~		
Reports	~		
Settings	Ň	Oixta Verified 👳	Overview
		The integration was either created by Okta or by Okta community users and then tested and verified by Okta	WalkMe is a powerful cloud-based Digital Adoption Platform that helps organizations to measure, drive, and maximize the value of their software investments. Use the Okta IDP Integration to early validate end-user identities,
		Use Case	enhance WalkMe content segmentation, and extend user
		Single Sign-On	behavior monitoring capacitities.

5. Enter the desired label for your app (we recommendleaving it as **WalkMe**), select the relevant region (US/EU), and click **Next**

ard V ry V textform V textform Active Conserval Settings Sign-On Options textform Conserval Settings Required Conserval Settings Required	
ry V Bis Add Walkie	
izations	
Itana A General settings Required	
Service Application label WalkMe	
	re required to add this
This label displays under the app on your home page	in unless marked optiona
~ Region US ~)
V Please select your region.	
Application Wability Do not display application icon to users	
Cancul Next	
© 2023 Okta, Inc. Privacy Version 2023.02.1 E OK14 US Cell Status site Downi	iond Okta Plusin - Fee

6. Go to the Sign On tab and select the required Sign on method: SAML 2.0



okta		Q. Search for people, apps and groups	0 == ·
Dashboard Directory	~ ~	₩. Add WalkMe	me
Customizations	~	General Settings 2 Sign-On Options	
Applications	^		
Applications		Sign-On Options. Required	About
Self Service API Service Integrations Security	~	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 3 rd party application. Application username is determined by the user profile mapping. Configure profile mapping	SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd
Paports		SAML 2.0	ty application may be required to
Reports	v (Default Relay State All IDP-initiated requests will include this RelayState.	Application Username Choose a format to use as the default username value when assigning the application to users.
		Attributes (Optional) Learn More Disable Force	If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.
		Authentication Never prompt user to re-authenticate. Preview SAML	
		Metadata details Metadata URL https://walkme.oktapreview.com/app/exk1lv7ta58rw K69q0h8/sso/saml/metadata Copy	
		More details	
		 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. 	
		O OpenID Connect	
		Credentials Details	
		Application username format Okta username 🗸	
		Update application username on Create and update ~	
		Password reveal Allow users to securely see their password (Recommended)	
		• Password reveal is disabled, since this app is using SAML with no password.	
		Previous Cancel Done	

Default Relay Field is Optional

Please note that the Default Relay State field in Okta IDP setup is not required and can be left



SAML 2.0	
Default Relay State	
	All IDP-initiated requests will include this RelayState.

empty for WalkMe's integration.

- If you selected **WalkMe (encrypted assertions):**
 - 1. Click Edit
 - Upload the encryption certificate generated from the <u>WalkMe Admin</u> <u>Center</u> (IDP integrations → Add Identity provider → SAML → Setup Encryption Settings → Generate Certificate → Download Certificate)

Add IDP	1 IDP Integration — 2 IDP Properties — 3 Assign Systems	×
	IDP Integration	
	Select with which systems you want to perform the current IDP integration.	
	Select Protocol	
	CAUTH 2.0 SAML 2.0	
	Set up your SAML application according to the instructions	
	and copy the application properties to the fields below.	
	Deveload metaliata.col	
	IDP Name 1	
	Enter the IDP name	
	X509 Signing Certificate 1	
	Single Sign-On URL 1	
	Setup Encryption Settings -	
	To setup the encryption of the integration please generate the certificate first, And	
	there enter the extension below.	
	Generate Certificate	
	AuthnRequest	
	Sign the SAML AuthnRequest	
	Assertion Encryption	

- Under "more details" you can copy the required URLs and copy or download the certificate
- 7. Click Done
 - 1. You'll be directed to your WalkMe app page in Okta. Click on the **Sign On** tab to copy the relevant parameters to complete the IDP integration with WalkMe.
- 8. Go to the Assignments tab to assign a user to the app

Phase 2 - Complete the IDP integration on WalkMe Admin Center

Follow these steps for SAML 2.0 protocol.

⁷¹ Stevenson Street, Floor 20 San Francisco, CA 94105 | 245 Fifth Avenue, STE 1501 New York, NY, 10016 | 421 Fayetteville St STE 215 Raleigh, NC 27601 www.walkme.com



Without encryption:

- 1. Log in to the WalkMe Admin Center, navigate to IDP Integrations in the left side menu, and click **Add Identity Provider**
- 2. Select the relevant protocol: SAML 2.0
- 3. For **SAML 2.0** you will have to provide the following information:
 - $\circ~$ Set a name for the configuration
 - **SSO URL (Single Sign-On URL):** URL of the IDP to which SAML authentication requests should be sent
 - **X509 Signing certificate:** Certificate needed by the service provider to validate the signature of the authentication assertions that have been digitally signed by the IDP. There should be a place to download the certificate from the IDP. If the certificate is not in .pem or .cer format, you can convert it to one of these formats so we can copy and paste it into WalkMe later.
- 4. Click Save & Next
- 5. An authorization flow will run in order to check the configured connection to Okta
- 6. Select End User Identifier (EUID) and import properties to leverage IDP integration to identify users and segmentation
- 7. Assign systems: select which WalkMe systems will be utilizing IDP for users identification and segmentation
- 8. Click **Finish** to complete the configuration

With encryption: (supports assertion encryption only)

- 1. Log in to the WalkMe Admin Center, navigate to IDP Integrations in the left side menu, and click **Add Identity Provider**
- 2. Select the relevant protocol: SAML 2.0
- 3. For **SAML 2.0** you will have to provide the following information:
 - $\circ\,$ Set a name for the configuration
 - $\circ~$ SSO URL (Single Sign-On URL): URL of the IDP to which SAML authentication requests should be sent
 - **X509 Signing certificate**: Certificate needed by the service provider to validate the signature of the authentication assertions that have been digitally signed by the IDP. There should be a place to download the signing certificate from the IDP. If the certificate is not in .pem or .cer format, convert it to one of these formats so we can copy and paste it into WalkMe later.
- 4. Click Setup Encryption Settings
- 5. Click the **Generate Certificate** button. A new certificate will be generated for this configuration.
- 6. **Download** the generated certificate
- 7. In Okta, set the Assertion Encryption as Encrypted, then upload the certificate you downloaded earlier to the Encryption Certificate field
- 8. In WalkMe, toggle on Assertion Encryption
- 9. Click **Save & Next.** An authorization flow will run in order to check the configured connection



to Okta.

- 10. Select End User Identifier (EUID) and import properties to leverage IDP integration to identify users and segmentation
- 11. Assign systems: select which WalkMe systems will be utilizing IDP for users identification and segmentation
- 12. Click **Finish** to complete the configuration