

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

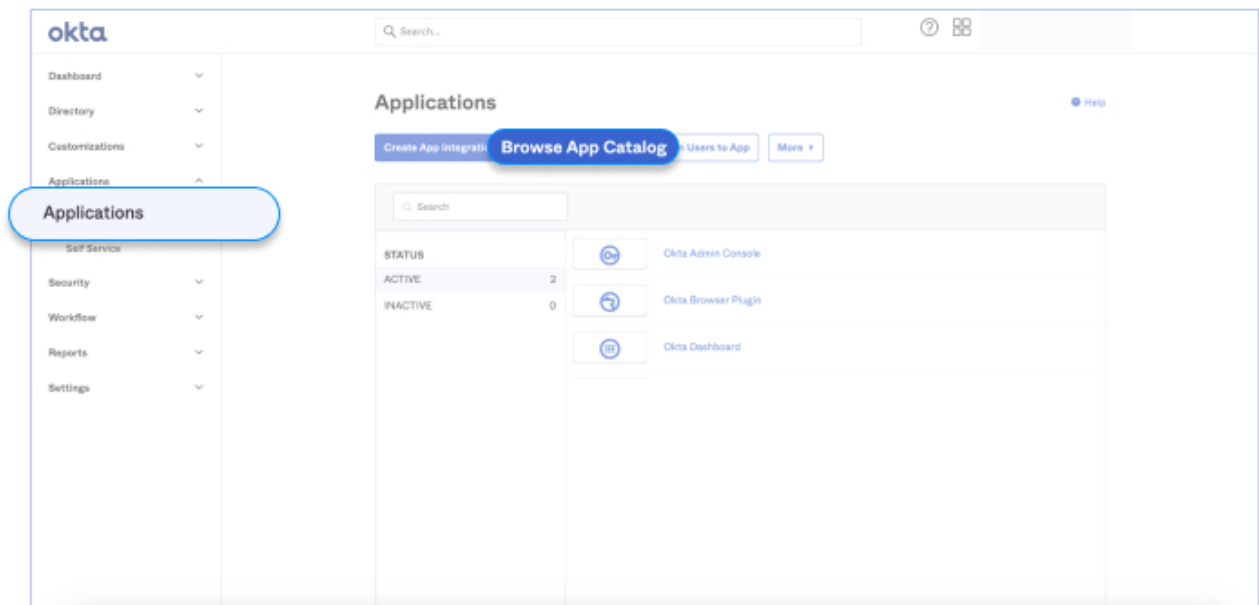
Setup

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.

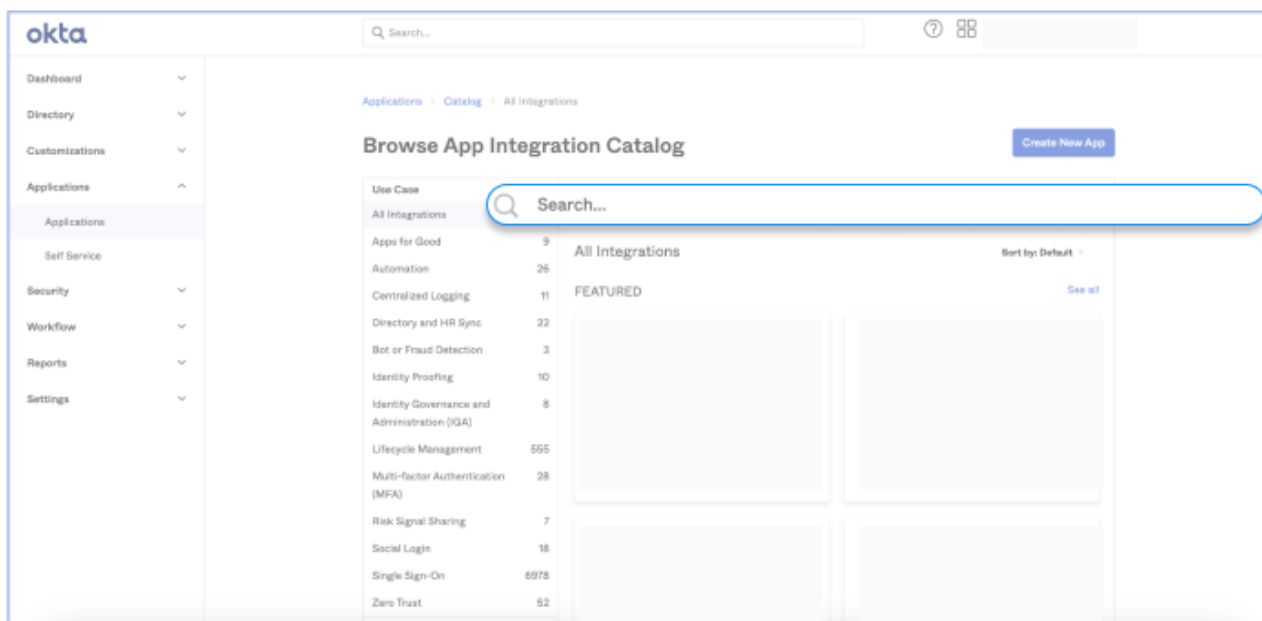
Phase 1 – Install the WalkMe app via Okta App Integration Catalog

These steps must be done by an Okta Admin

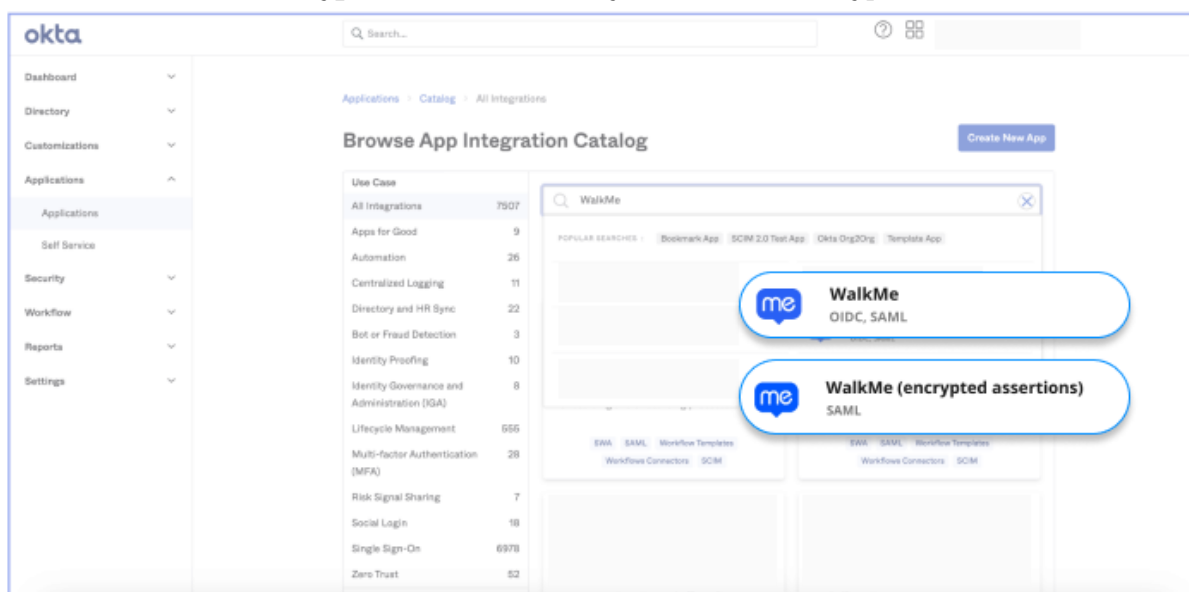
1. In the Okta App Integration Catalog, click **Applications** in the left side menu and then click on **Browse App Catalog**



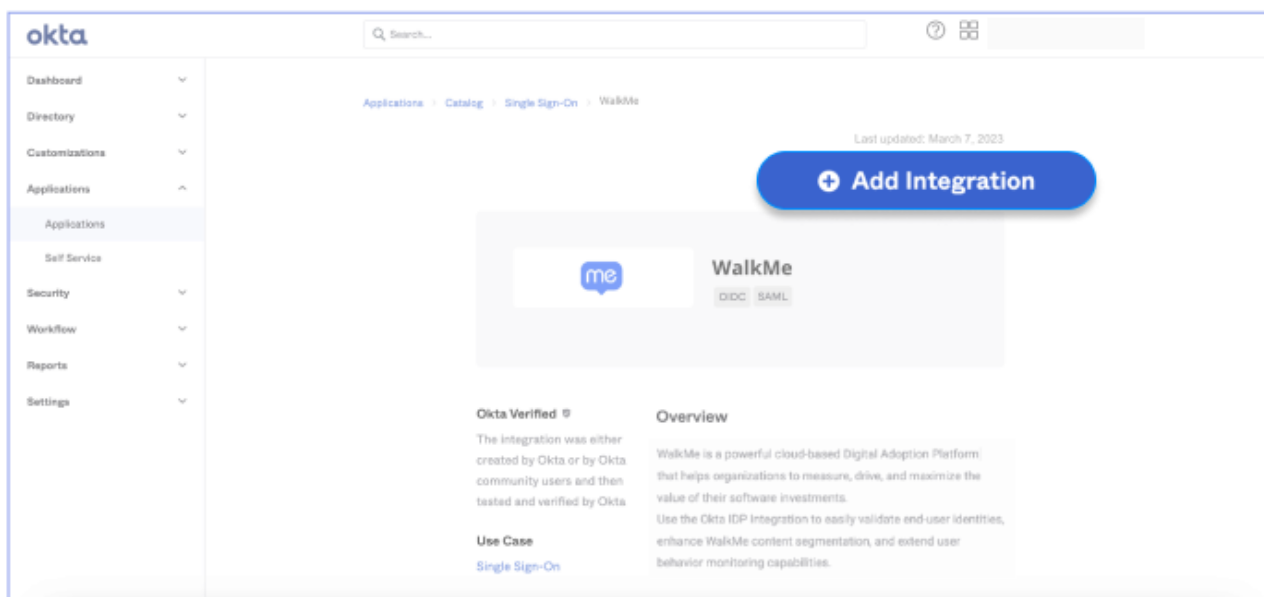
2. Type **WalkMe** in the search bar under **Browse App Integration Catalog**



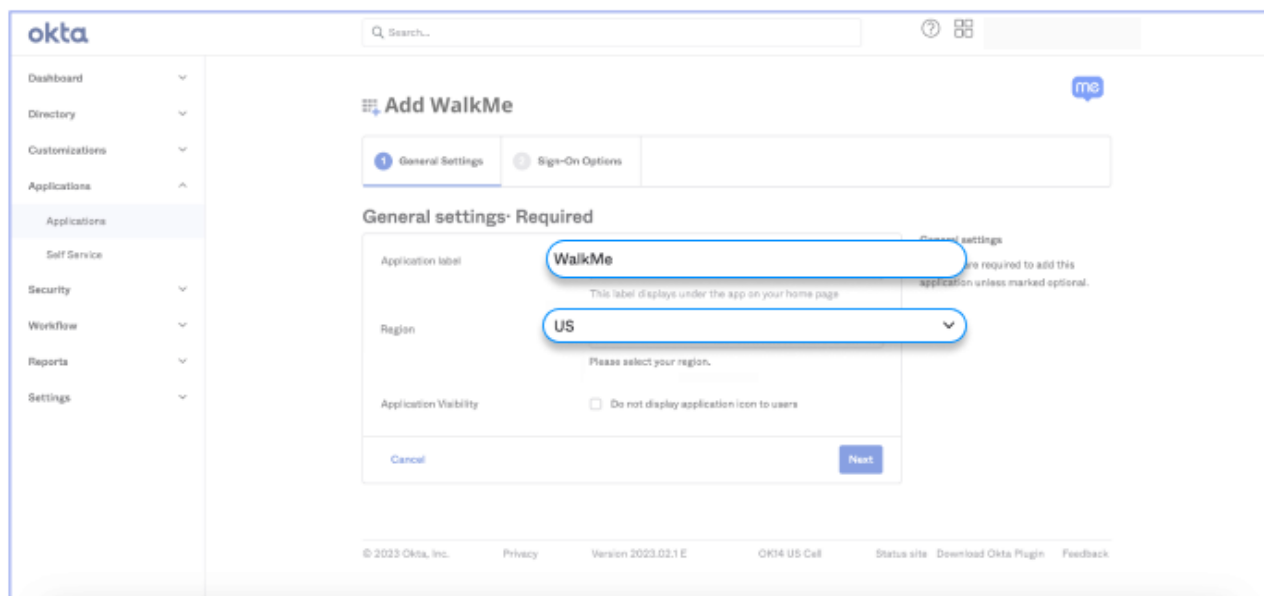
3. Select **WalkMe** from the list of suggested integrations
 - If "WalkMe" is not visible in the list, click **See All Results** to find WalkMe
 - Choose **WalkMe (encrypted assertions)** if you need the encrypted version



4. Click **Add Integration**



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



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

okta

Search for people, apps and groups

?

Dashboard

Directory

Customizations

Applications

Applications

Self Service

API Service Integrations

Security

Workflow

Reports

Settings

me

Add WalkMe

1 General Settings

2 Sign-On Options

Sign-On Options Required

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

All IDP-initiated requests will include this RelayState.

Attributes (Optional)

[Learn More](#)

Disable Force Authentication

☒

Never prompt user to re-authenticate.

Preview SAML

Metadata details

Metadata URL

<https://walkme.oktapreview.com/app/exk1lv7ta58rw/K69qOH8/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.

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

About

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 party application may be required to complete the integration with Okta.

Application Username

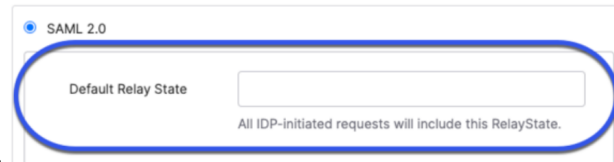
Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

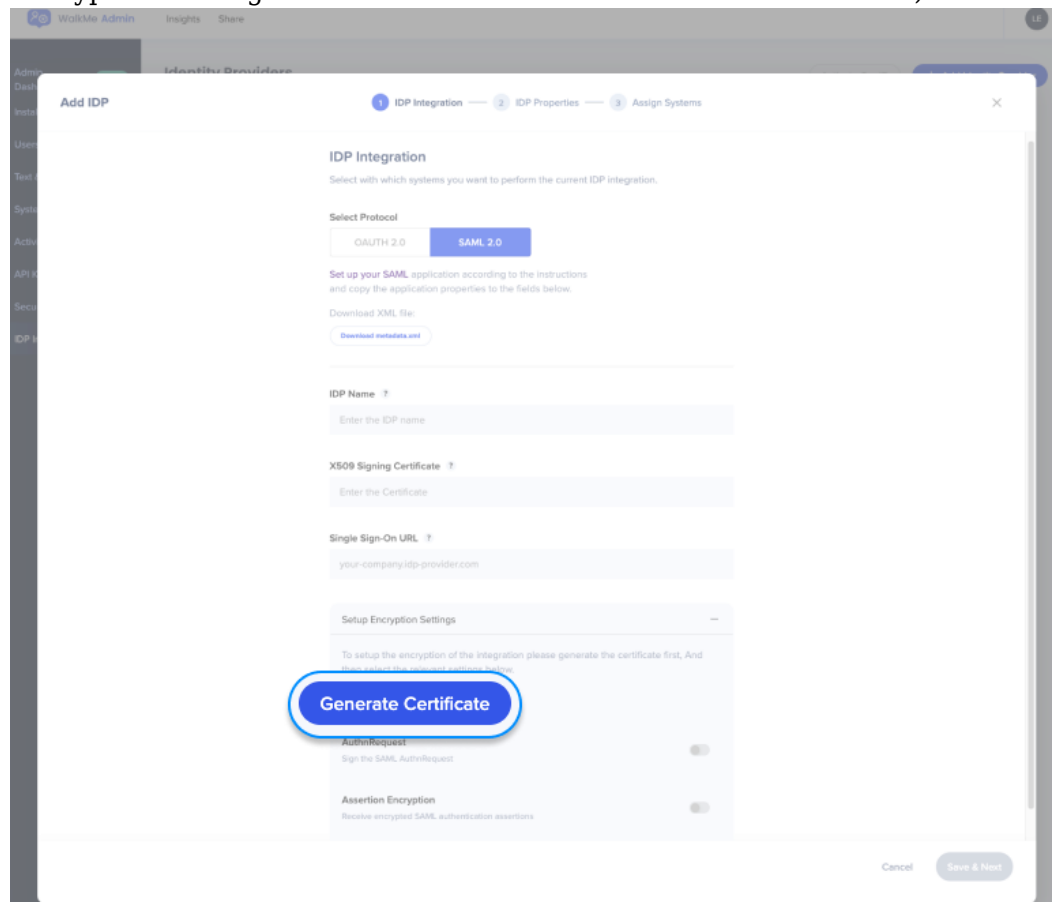
Default Relay Field is Optional

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

empty for WalkMe's integration.



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



- 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.

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:
 - 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:
 - 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 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