IDP Integration

Brief Overview

IDP Integration can be used to validate end-users identity, enrich content segmentation capabilities and expand on user behavior monitoring. Providing one reliable and secure User ID across any system without the need of defining the unique user ID for each system with different variables.

Use Cases

- End-user IDP authentication as a prerequisite to present WalkMe content.
- Expanding content segmentation capabilities by IDP parameters (for example - groups, region, department, etc).
- Accurate data monitoring across systems.

Supported Platforms

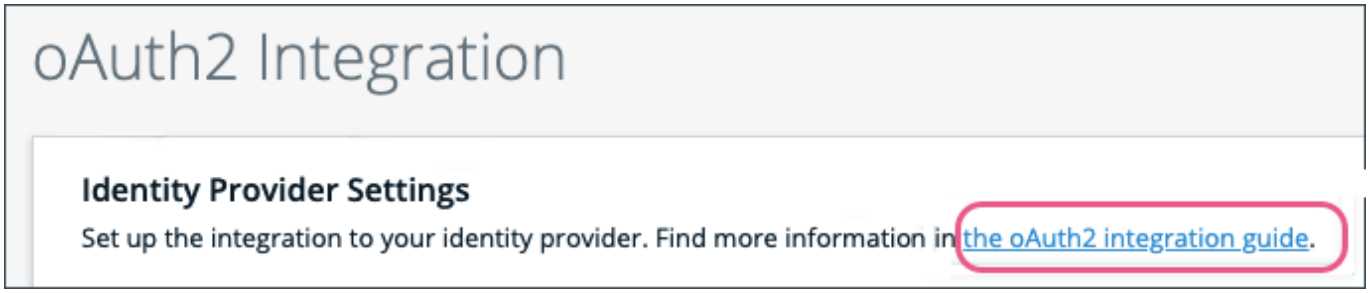
IDP Integration is currently supported on the following systems:

- Okta
- G-Suite
- ADFS
- AzureAD
- PingOne

Pre-requisites

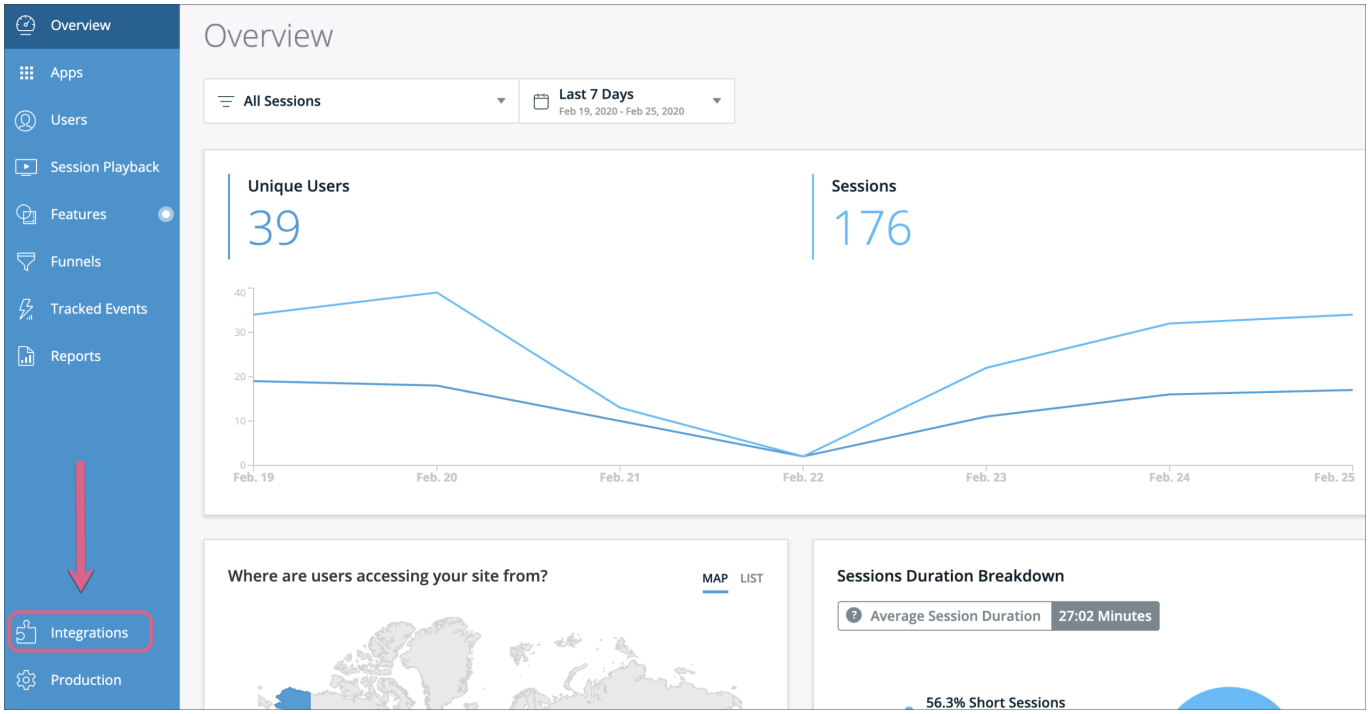
An IDP application needs to be created to serve as the "bridge" between IDP and WalkMe's Integration Center.

An instruction guide is available in the Integration Center on the configuration screen for all supported systems.

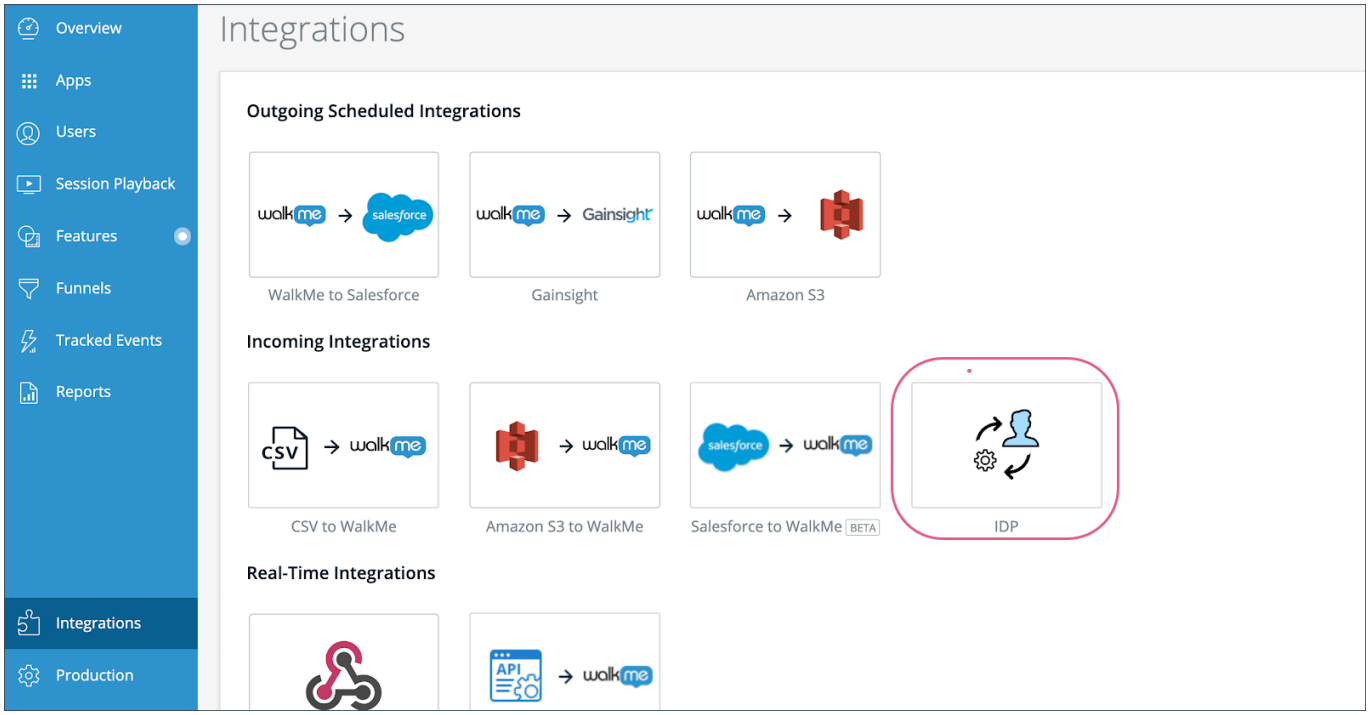


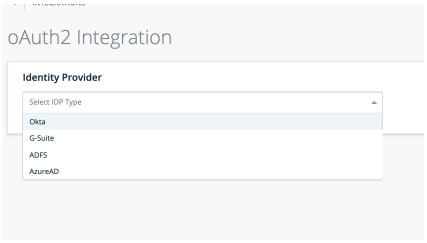
Creating and Setting an Integration

1. Navigate to Integration Center within Insights



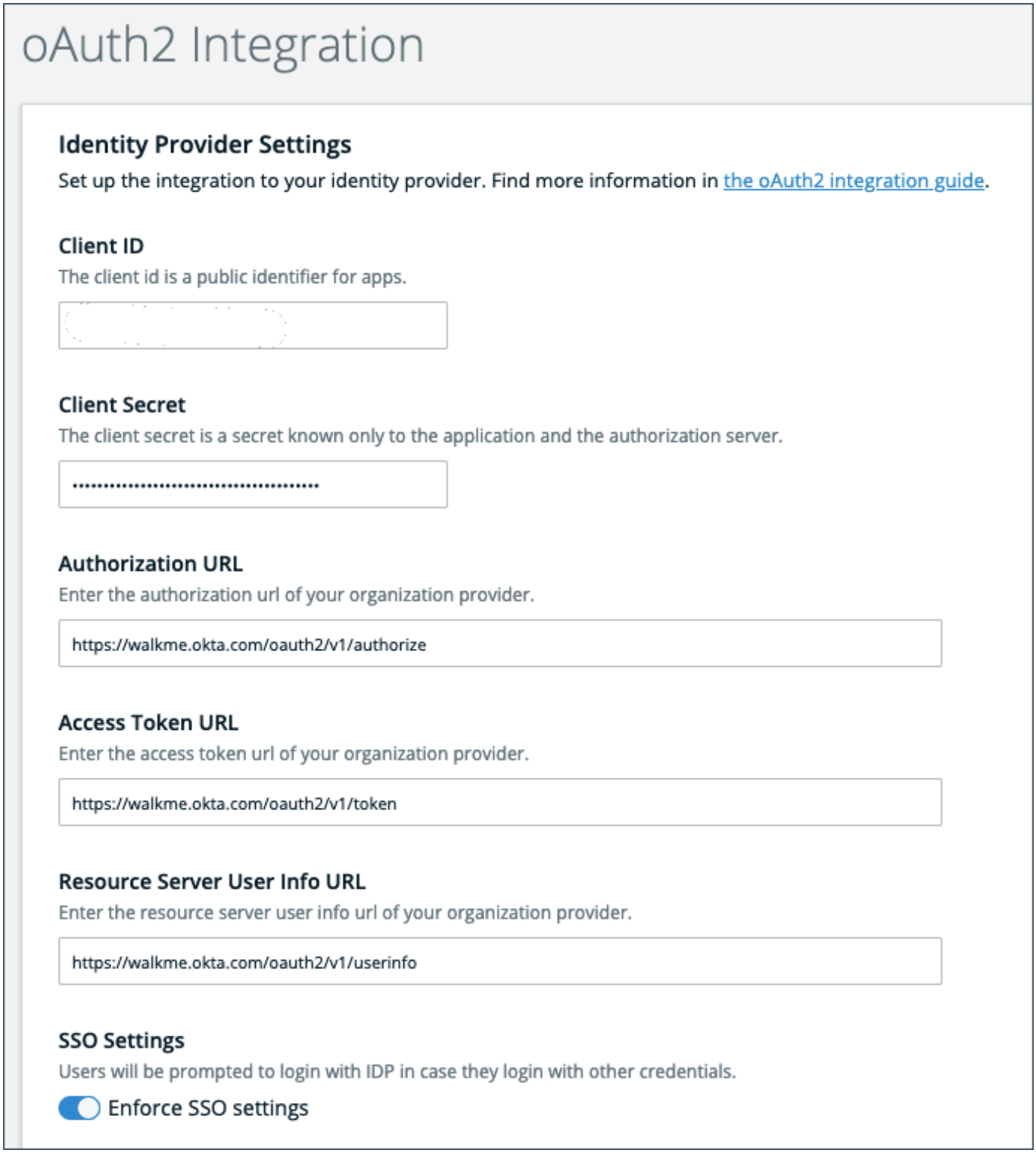
2. Choose "IDP Integration"


Overview
Apps
Users
Session Playback
Features
Funnels
Tracked Events
Reports
Integrations
Production
Integrations
Outgoing Scheduled Integrations
WalkMe to Salesforce
Gainsight
Amazon S3
Incoming Integrations
CSV to WalkMe
Amazon S3 to WalkMe
Salesforce to WalkMe BETA
IDP
Real-Time Integrations



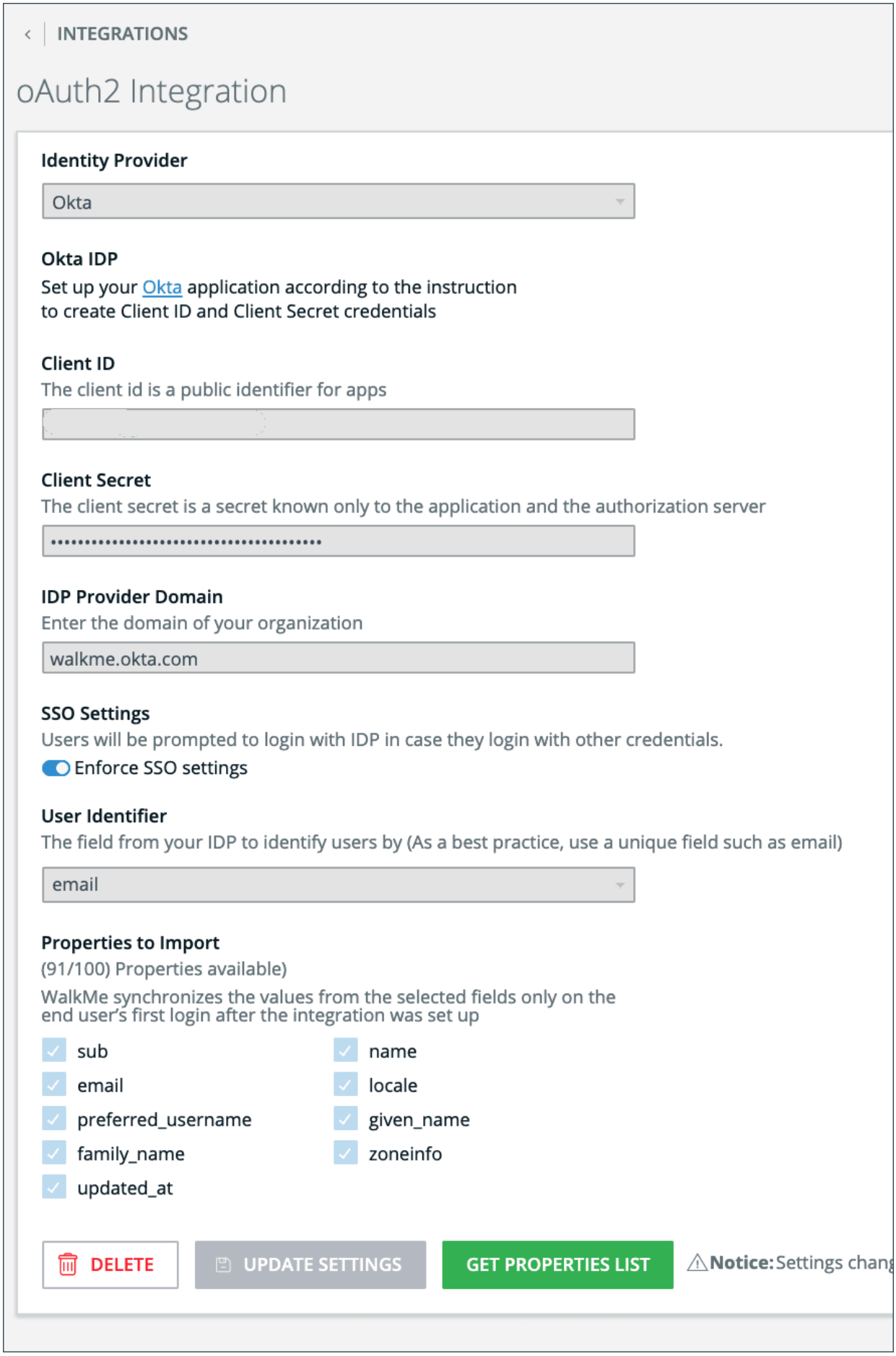
3. Choose your IDP type from the Identity Provider dropdown:

4. Fill the fields according to the instructions guide (instructions may vary pending the IDP provider type).

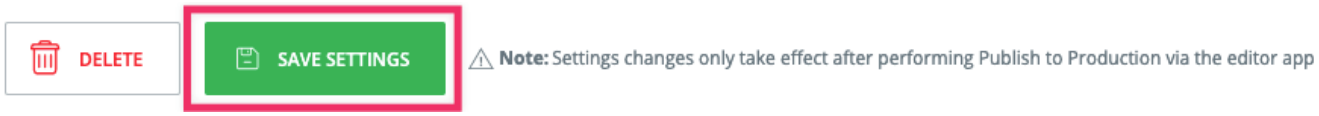


5. Click Get Properties list

6. Choose which IDP attributes should be imported for content segmentation and reporting to Insights:

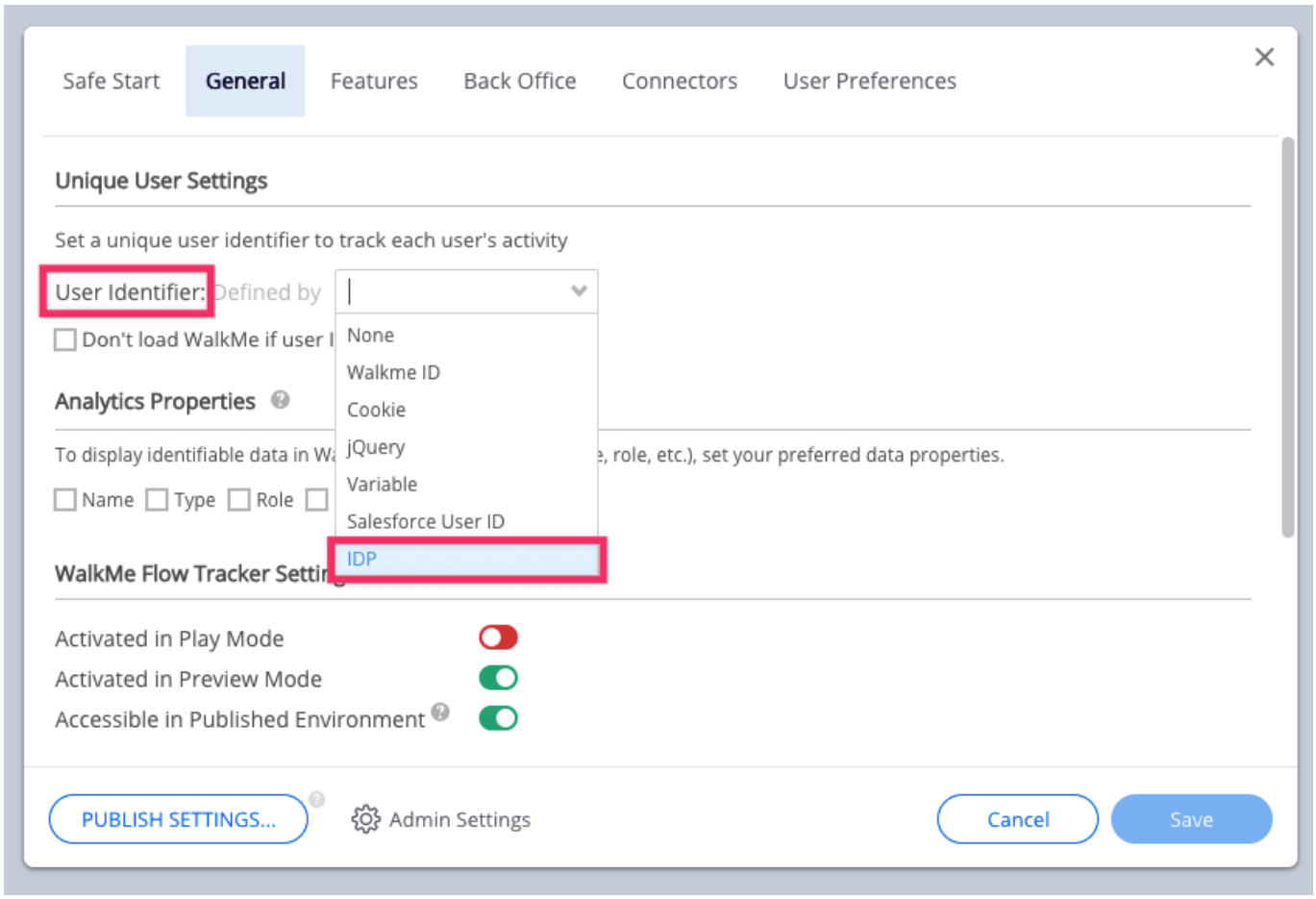

INTEGRATIONS
oAuth2 Integration
Identity Provider
Okta
Okta IDP
Set up your Okta application according to the instruction
to create Client ID and Client Secret credentials
Client ID
The client id is a public identifier for apps
Client Secret
The client secret is a secret known only to the application and the authorization server
IDP Provider Domain
Enter the domain of your organization
walkme.okta.com
SSO Settings
Users will be prompted to login with IDP in case they login with other credentials.
Enforce SSO settings
User Identifier
The field from your IDP to identify users by (As a best practice, use a unique field such as email)
email
Properties to Import
(91/100) Properties available)
WalkMe synchronizes the values from the selected fields only on the
end user's first login after the integration was set up
sub
email
preferred_username
family_name
updated_at
name
locale
given_name
zoneinfo
DELETE
UPDATE SETTINGS
GET PROPERTIES LIST
Notice: Settings chang

7. Press "Save"



8. Open WalkMe Editor within the system you would like to use IDP as User Identifier on

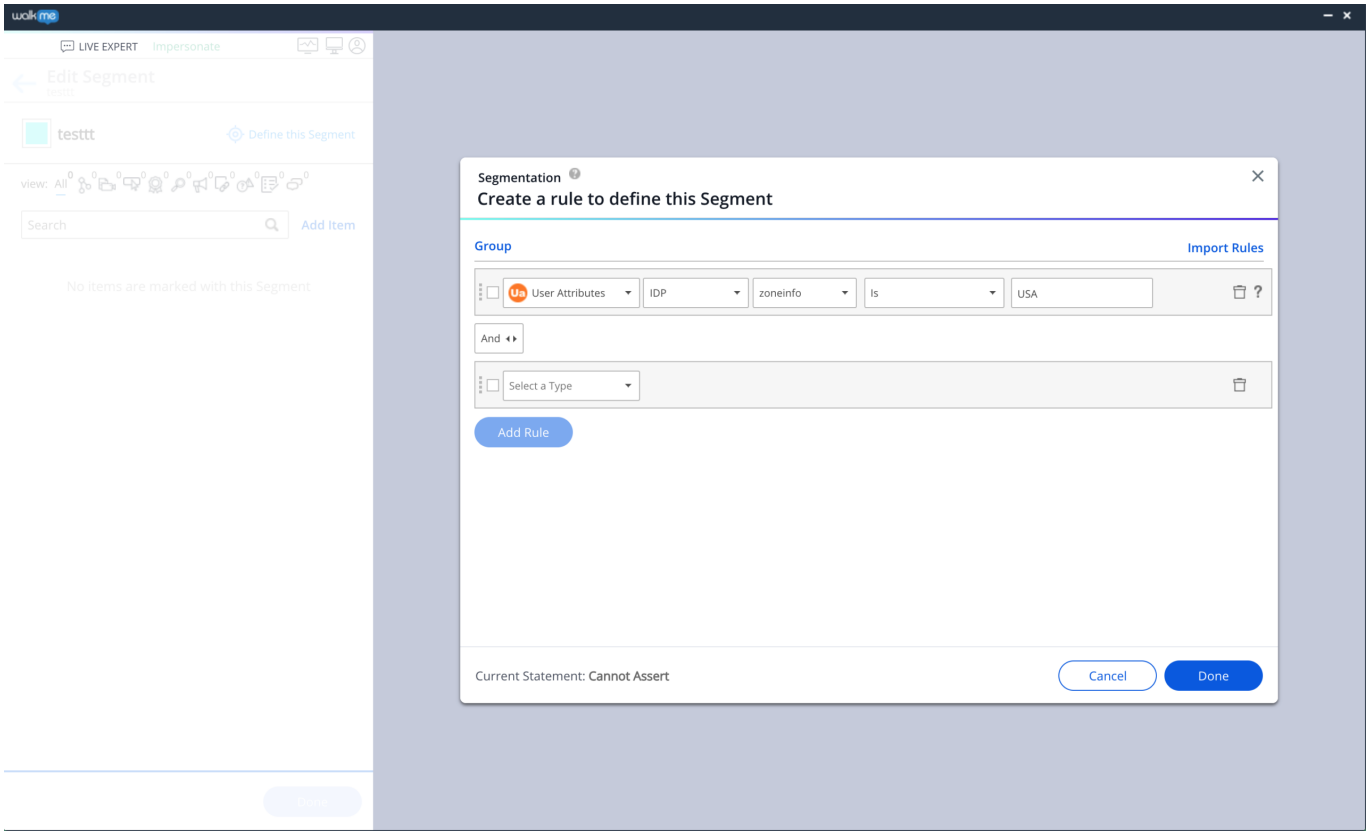
9. Click "Settings" and set the User Identifier parameter to "IDP" (This option will be available to any system under the configured account)



10. Save settings

11. Publish the new settings for the relevant environment

12. You can now segment content using the imported attributes and through Segmentation Center, under User Attributes > IDP:



Note: IDP Integration is configured on account-level on Integration Center phase. Changing the User Identifier parameter is done on the system-level.

Workstation Users

After completing the steps above, please contact your Account Manager to continue

Best Practices

- "Enforce SSO" configuration -
  - Enabled - IDP authentication must occur before opening a web page to end-user, if IDP token is not recognized then the end-user will be

redirected to its IDP login page.
- Disabled - IDP authentication is attempted upon page load, but if there's is not an active token for IDP then end-user won't be redirected to IDP. Its User Identifier will be downscaled automatically to "WalkMe ID" method.

Limitations

- Important: Changing User Identifier impacts the way WalkMe identifies end-users and may reset "Play once" configurations.

Please be aware that, if your implementation is already live, changing the User Identifier impacts the way WalkMe identifies end-users. This could result in resetting auto-play rules (ie. Play Once settings) or users seeing their Onboarding tasks marked as uncomplete, due to their unique user identifier (UUID) being changed. There is no way around this limitation, as each user is being recognized as a new user, tied to their new UUID value.

- Only one IDP Integration is available per account.