

IDP Integration

Brief Overview

Identity Providers store and manage digital identities, providing a way for companies to manage access and privileges, while maintaining high security standards.

IDP Integration can be used to take that information, 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.

Using IDP as a User Identifier should be the go-to solution for all new systems.

IDP Integrations are accessible from the [Admin Center](#) at admin.walkme.com.

□ Digital Adoption Institute

- View the [Configure Analytics, Integrations, and Design lesson](#) in the *Digital Adoption Project Management Fundamentals* course.
- Don't have a DAI account yet? [Sign up here](#)

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

WalkMe's IDP integration supports the use of several authentication protocol including **OAuth 2.0**, **OpenID Connect**, and **SAML**, in order to authenticate users with their organizational IDP vendor, and to obtain user attributes that can later be used for segmentation and analytics in WalkMe. Every IDP vendor that supports these protocols should work with WalkMe.

WalkMe supports SP initiated flow.

What is OAuth 2.0?

OAuth 2.0, which stands for “Open Authorization”, is a standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user. OAuth 2.0 is the industry-standard protocol for authorization.

What is OpenID Connect?

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner.

IDP Integration currently supports the following vendors:

- **Okta**
- **G-Suite**
- **ADFS**
- **AzureAD**
- **PingID**
- Identity providers that use **OpenID**

Other than OpenID Connect, the most common authentication protocol is SAML. For instructions on how to create and set an integration using SAML, please refer to our [SAML IDP Integration article](#).

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 Admin Center configuration screen for all supported systems.

Select Protocol

OAUTH 2.0

SAML 2.0

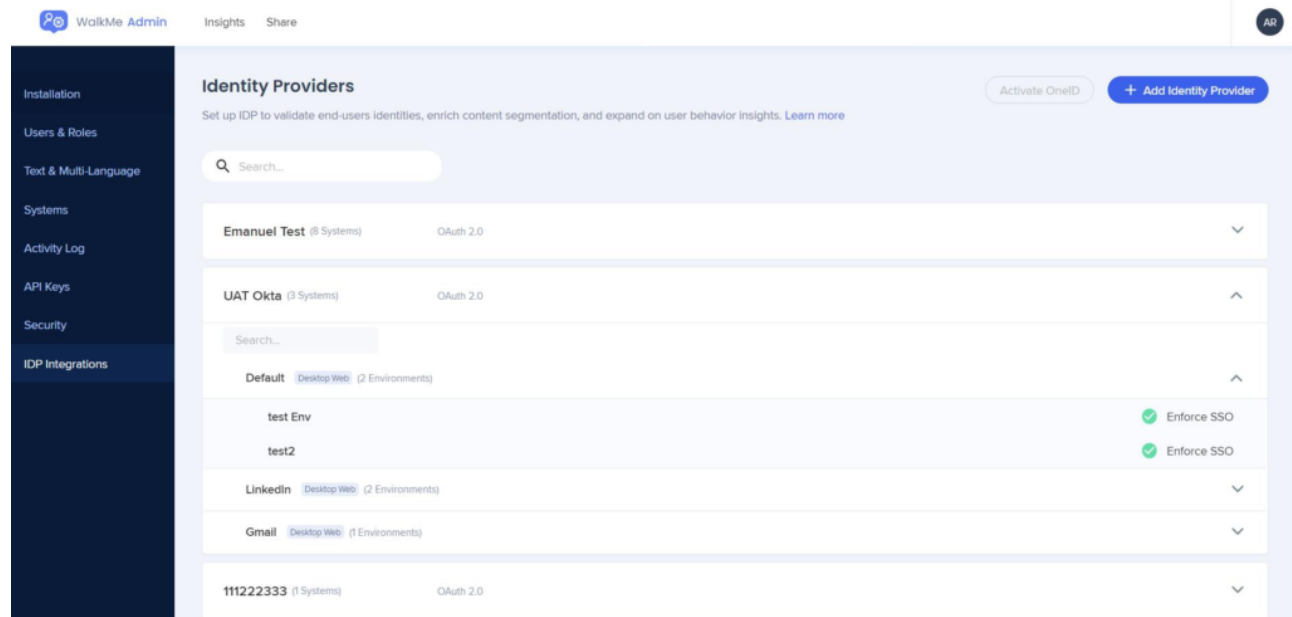
Select Vendor

Okta

Set up your Okta application according to the instructions and copy the application properties to the fields below.

Adding an Identity Provider

1. In the IDP Integrations tab of the Admin Center, click on the “+ Add Identity Provider” button



2. Select the OAuth 2.0 protocol type
3. Provide the appropriate configuration settings for the connection

1. **IDP vendor** – Select a vendor from the list
2. **IDP Name** – Connection name
3. **Client ID** – Public identifier for apps
4. **Client Secret** – Secret known only to the application and the authorization server
5. **IDP Provider Domain** – Domain of your organization

1 IDP Integration
2 IDP Properties
3 Assign Systems
X

IDP Integration

Select with which systems you want to perform the current IDP integration.

Select Protocol

OAUTH 2.0
SAML 2.0

Select Vendor

Cancel
Save & Next

Note: Fields may vary pending on the IDP vendor selected.

- **For OpenID Connect:**

1. **IDP vendor** - Select OpenID Connect from the Oath2.0 vendor list
2. **IDP Name** - Connection name
3. **Client ID** - Public identifier for apps
4. **Client Secret** - Secret known only to the application and the authorization server
5. **IDP Provider Discovery URL**
6. **IDP Provider Scope**
7. **Content Security Policy**
8. **Your IDP Provider**
9. **Use ID Token For Getting End-Users Properties** - Check the toggle to enable

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

OAUTH 2.0

SAML 2.0

Select Vendor

Cancel

Save & Next

4. Click “Save & Next” once ready

- Note that we **do not** require a Sign Logout URL

5. Choose a unique end-user identifier to identity users by

- You only need one identifier; we do not require any additional group information or other attributes

6. Select the desired properties and ensure the correct data type was chosen:

1. String
2. Number
3. Date

Please note: The User Identifier field will be always converted to type String.

Add IDP

1 IDP Integration
2 IDP Properties
3 Assign Systems

IDP Properties

Select the protocol for your IDP, fill out the form below, and get properties.

Choose End-User Identifier

The field from your IDP to identify users by.
Use a unique field such as "email" and make sure that the chosen property exists for all the users in the organization.

Choose a unique end-user identifier

Properties to Import

Choose the field that will be used to identify your users.

☒ name
String
☐ email
String
☒ city
String
☒ birthday
Date

Cancel
Save & Next

Tip:

- To make sure the selected data type is suitable, you can hover above the "i" icon and check the value of that property.
- If the selected data type isn't suitable for the property, an orange "!" icon will appear recommending to switch back to the identified data type.

IDP Properties

Select the protocol for your IDP, fill out the form below, and get properties.

Choose End-User Identifier

The field from your IDP to identify users by.
Use a unique field such as "email" and make sure that the chosen property exists for all the users in the organization.



Choose a unique end-user identifier

Properties to Import

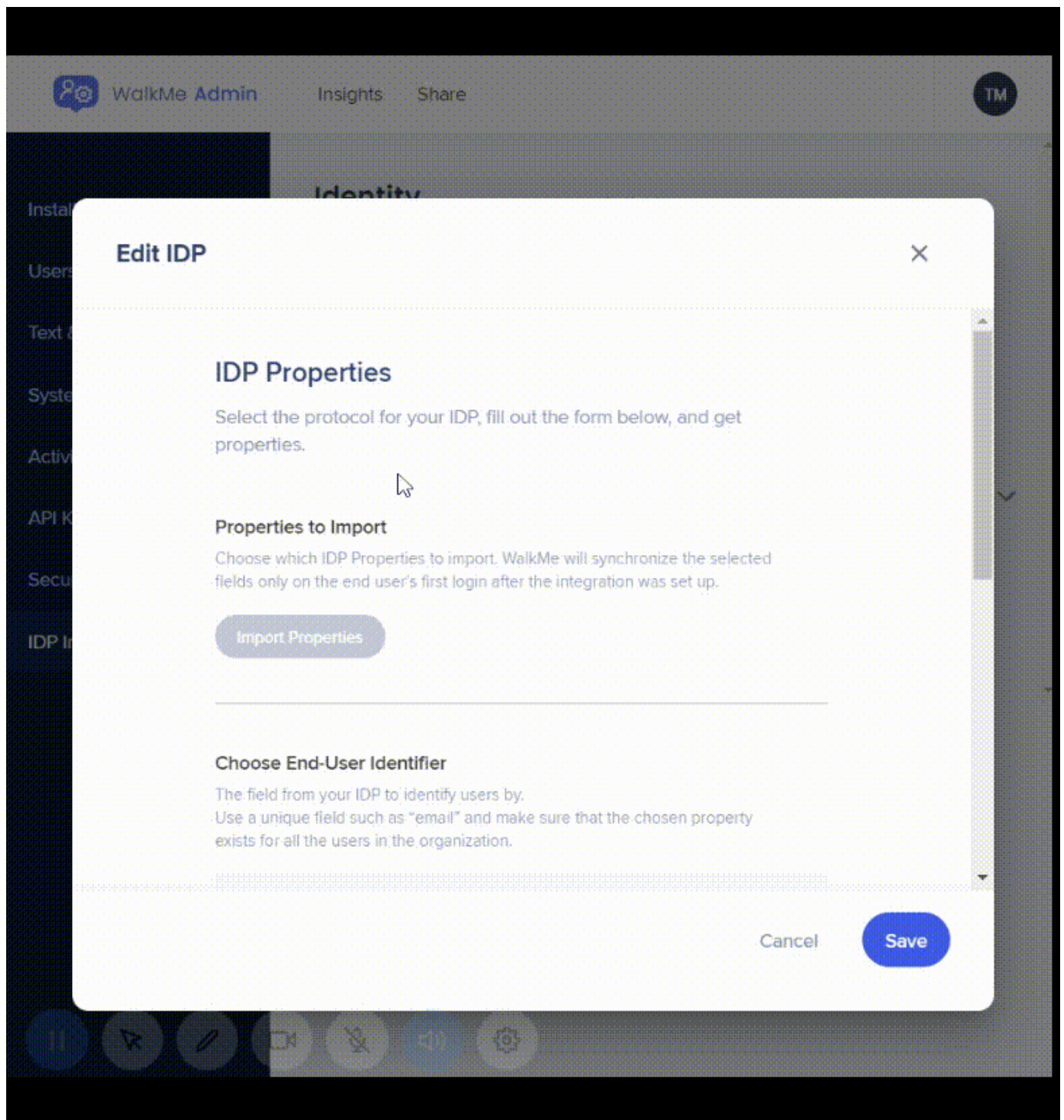
Choose the field that will be used to identify your users.

Q Search...

We identified this field as a String.
Please ensure you select the correct field type.

| | | | | | |
|-------------------------------------|----------|---|---|--------|---|
| <input checked="" type="checkbox"/> | name |  |  | Number | ▼ |
| <input type="checkbox"/> | email | | | String | ▼ |
| <input checked="" type="checkbox"/> | city | | | String | ▼ |
| <input checked="" type="checkbox"/> | birthday | | | Date | ▼ |

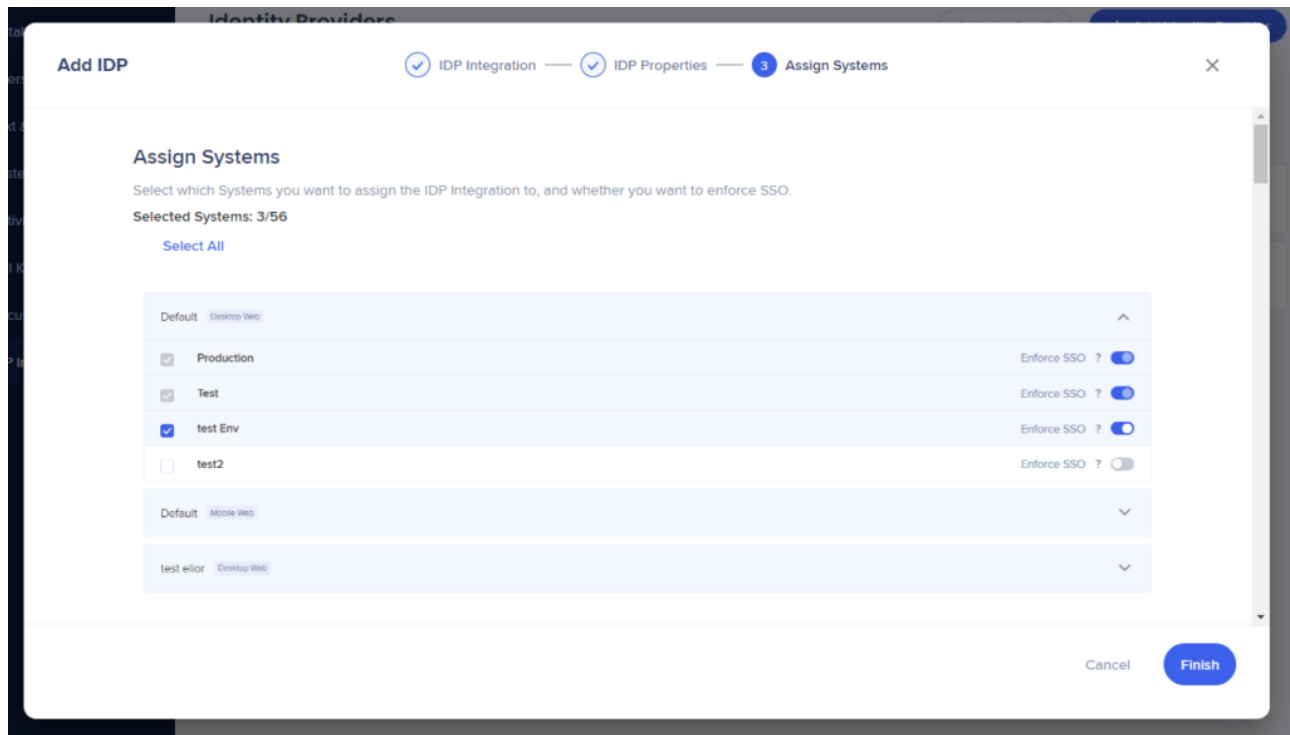
You may also rename any selected property, view its original value and name, and revert back to its original value if it is overridden.



7. Select which systems you want to assign the IDP Integration to

- For each system, you can separately enable IDP Integration on the desired environments

8. Use the toggle to Enforce SSO

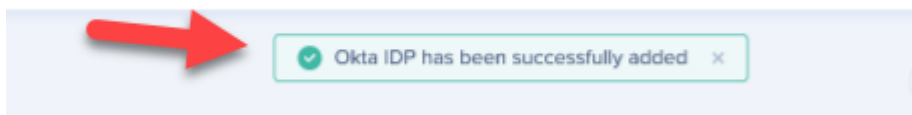


Note:

- IDP should provide the most accurate user identification, but the numbers may be not accurate when Enforce SSO is disabled.
- When enforce SSO is disabled, users can use applications without authenticating to their IDP provider, and a WalkMe Id will be generated and used as user identifier.
- Users can “skip” the IDP authentication by either using apps that don’t require authentication at all, or by logging into the application directly via user/password, without going through the IDP login flow.

9. Click “Finish”

10. A message will appear telling you whether your IDP was successfully added or not



Note:


- After assigning systems, the **UUID setting** for the assigned systems is automatically set to IDP and settings are published so no further action is required.
- The only way to change the UUID is by unassigning the system from the vendor (see “**Manage System Assignment**” section below).
- You can now segment content using the imported attributes in Insights and in the Editor under User Attributes > IDP with the suitable filter conditions according to the set data field type.
- [Read more here](#).

Segmentation ?
×

Create a rule to define this Segment

Group
Import Rules

☐


User Attributes

IDP

zoneinfo

Is

USA

✕ ?

And

☐

Select a Type

✕

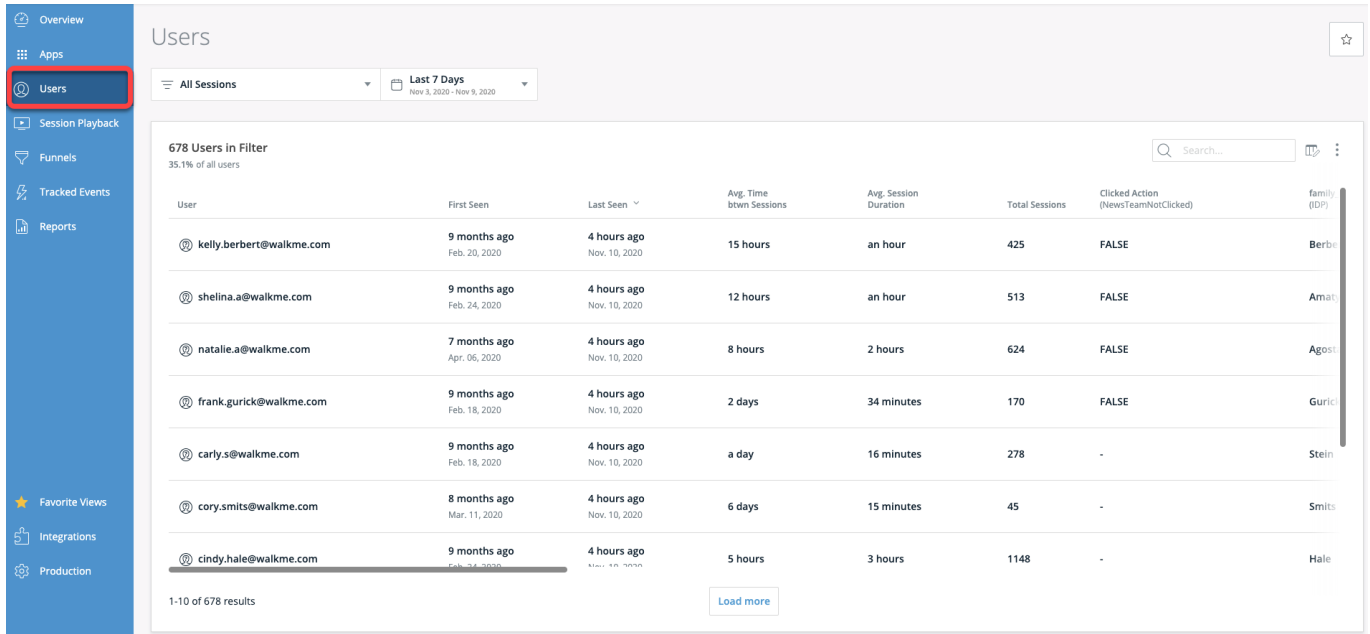
Add Rule

Current Statement: Cannot Assert
Cancel Done

Tip:

- In order to validate that users are being identified by the integration and that all the requested attributes are collected, it is recommended to view the Users page in [Insights](#) at insights.walkme.com, where all user data is displayed.

- Users are added to the table only after their session has ended, so after setting up IDP it will take some time for users to be added.



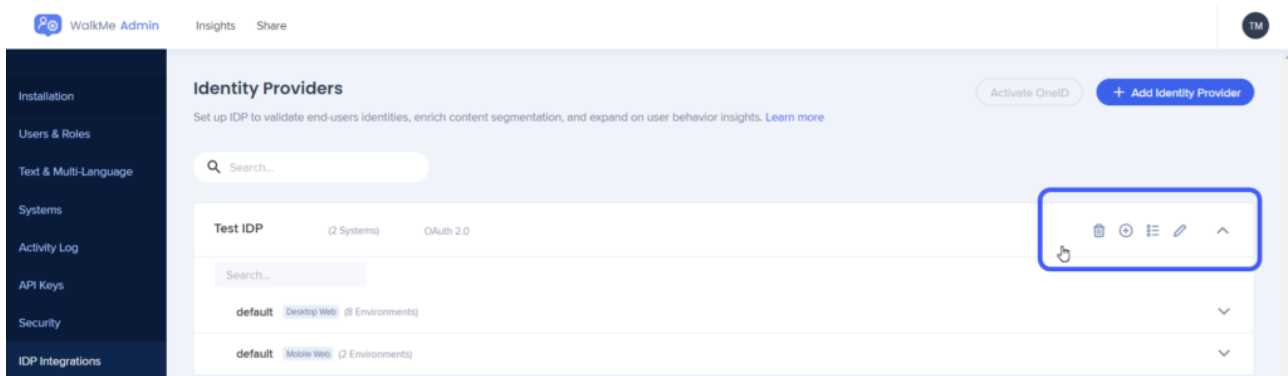
The screenshot shows the 'Users' page in the WalkMe interface. The left sidebar has a red box around the 'Users' link. The main content area shows a table of users with the following columns: User, First Seen, Last Seen, Avg. Time btwn Sessions, Avg. Session Duration, Total Sessions, Clicked Action (NewsTeamNotClicked), and family (IDP). The table lists 678 users in filter, with 35.1% of all users. The first 10 users are shown, with a 'Load more' button at the bottom.

| User | First Seen | Last Seen | Avg. Time btwn Sessions | Avg. Session Duration | Total Sessions | Clicked Action (NewsTeamNotClicked) | family (IDP) |
|--------------------------|-------------------------------|------------------------------|-------------------------|-----------------------|----------------|-------------------------------------|--------------|
| kelly.berbert@walkme.com | 9 months ago Feb. 20, 2020 | 4 hours ago Nov. 10, 2020 | 15 hours | an hour | 425 | FALSE | Berbert |
| shelina.a@walkme.com | 9 months ago Feb. 24, 2020 | 4 hours ago Nov. 10, 2020 | 12 hours | an hour | 513 | FALSE | Amari |
| natalie.a@walkme.com | 7 months ago Apr. 06, 2020 | 4 hours ago Nov. 10, 2020 | 8 hours | 2 hours | 624 | FALSE | Agosti |
| frank.gurick@walkme.com | 9 months ago Feb. 18, 2020 | 4 hours ago Nov. 10, 2020 | 2 days | 34 minutes | 170 | FALSE | Gurick |
| carly.s@walkme.com | 9 months ago Feb. 18, 2020 | 4 hours ago Nov. 10, 2020 | a day | 16 minutes | 278 | - | Stein |
| cory.smits@walkme.com | 8 months ago Mar. 11, 2020 | 4 hours ago Nov. 10, 2020 | 6 days | 15 minutes | 45 | - | Smits |
| cindy.hale@walkme.com | 9 months ago Feb. 24, 2020 | 4 hours ago Nov. 10, 2020 | 5 hours | 3 hours | 1148 | - | Hale |

Managing an Identity Provider

Hovering over the row of an Identity Provider will provide you with several options:

- Delete
- Manage System Assignment
- Import Properties
- Edit
- Expand

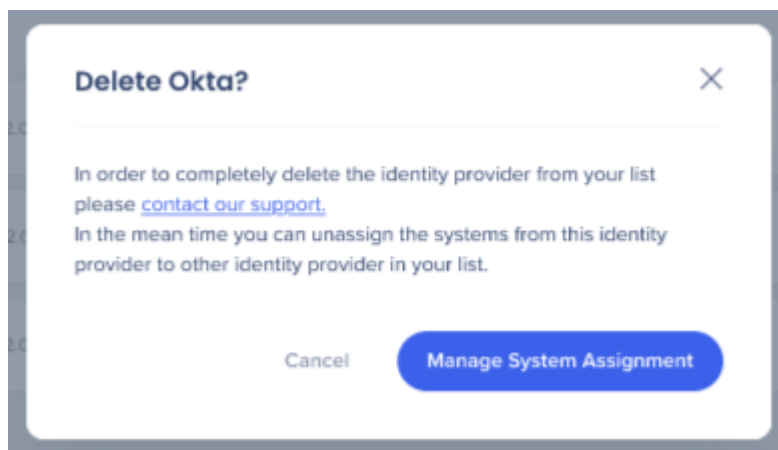


Delete

- Click on the trash icon to “delete” an identity provider

Important Note:

- It is not possible to completely delete an identity provider without contacting Support.
- Before deleting is possible the identity provider must be unassigned to any systems using the Manage System Assignment screen.

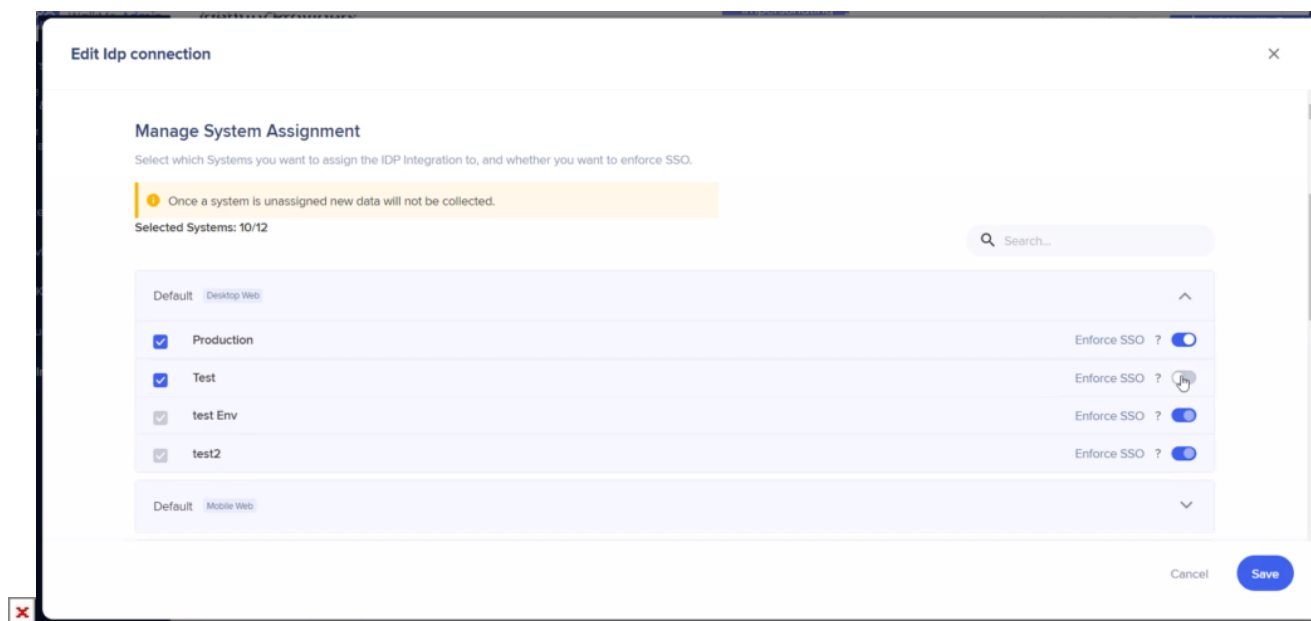


Manage System Assignment

- Click on the “+” icon to open the Manage System Assignment screen
- Select or deselect the systems you want assigned to the identity provider
- You can also use the toggle to Enforce SSO
- Click on the “Save Changes” button once you are finished

Note:

- Users cannot manage system assignment for vendors that have no imported properties. Properties will have to be imported first.
- After assigning systems, the **UUID setting** for the assigned systems is automatically set to IDP and settings are published so no further action is required.



Import Properties

- Click on the list icon and then the “Import Properties” button to edit or add additional imported properties

These attributes will be used for content segmentation and reporting in Insights.

Note:

- In order to do this it is required to authenticate with a user that is assigned to the WalkMe app on the provider side.

IDP Properties

IDP Properties

Select the protocol for your IDP, fill out the form below, and get properties.

Properties to Import

Choose which IDP Properties to import. WalkMe will synchronize the selected fields only on the end user's first login after the integration was set up.

Import Properties

Choose End-User Identifier

The field from your IDP to identify users by.
Use a unique field such as "email" and make sure that the chosen property exists for all the users in the organization.

Email

Properties to Import

Choose the field that will be used to identify your users.

Q Search...

Cancel

Save & Next

Edit

- Click on the pencil icon to edit identity provider settings
- You will be able to be able to edit all of the fields filled out in the initial identity provider configuration

Note:

- Users cannot manage system assignment for vendors that have no imported properties. Properties will have to be imported first.

Edit OIDC testing

IDP Integration

Select with which systems you want to perform the current IDP integration.

Select Protocol

OAuth 2.0

SAML 2.0

Select Vendor

OpenID Connect

Set up your OIDC application according to the instructions and copy the application properties to the fields below.

IDP Name ?

OIDC testing

Client ID ?

Cancel

Save

Expand / Collapse View

- Use the arrow icon to open and collapse the expanded view
- When expanded you will see all of the systems assigned to an identity provider and whether or not Enforce SSO has been enabled



Best Practices

“Enforce SSO” Configuration

- When **Enabled** – IDP authentication must occur before opening web page to end-user, if IDP token is not recognized then the end-user will be redirected to their IDP login page.
 - Each time the end-user fails to authenticate to the IDP due to reasons such as, IDP was down, customer forgot credentials, or end-user was not assigned to the IDP’s app, SSO will be disabled for 1 hour and the User Identifier will be automatically downscaled to “WalkMe ID” method as fallback or WalkMe will not load, depending on the customer’s configuration.
 - After 1 hour – if IDP token is still not recognized then the end-user will be redirected again to their IDP login page, otherwise, login to the IDP will not be needed. It is important to make sure this is absolutely clear to the customer. Otherwise, DO NOT enable this option.
- When **Disabled** – IDP authentication is attempted upon page load, but if there is no active token for IDP then the end-user won’t be redirected to IDP. The User Identifier will be downscaled automatically to “WalkMe ID” method or WalkMe will not load, depending on the customer’s configuration.

Limitations

Important: 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 previously completed 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.

- Safari browser extension is not supported with IDP
- Changing User Identifier impacts the way WalkMe identifies end-users and may reset “Play once” configurations
- User should have Admin permissions for Admin Center
- IDP must be configured on the required system
- End users should be using IDP to authenticate to that system
- If your company has CSP (Content Security Policy) it will block calls to the IDP provider
 - In order to overcome this, the right URL should be added in the CSP settings of the extension configuration
- After assigning systems, the **UUID setting** for the assigned systems is automatically set to IDP and settings are published so no further action is required
 - For the IDP changes to take effect, the customer’s systems must be updated to the latest WalkMe version (this can be achieved by doing a settings publish)
 - For Enterprise accounts you must check “Update to the latest WalkMe version” when publishing
- When importing a date type property, only the following formats are supported:
 - 2018-02-20
 - 2018-02-20T14:32:00
 - 12/30/2018
 - Importing a string or number as a date will fail to work in Insights filtering/Editor segmentation

Mobile Web:

- Mobile Web will be automatically activated after IDP setup is complete
- If Mobile Web is added after IDP / OneID has already been activated, users will need to deactivate and then reactivate IDP for Mobile Web support

Solving Common Issues

User is not assigned

To prevent this from occurring, all employees need to be assigned to WalkMe. The IT person at your company should be able to assist you with this by modifying the access setting to the **WalkMe app** in your IDP provider to all employees.

EUID was not found in the user profile

To address this, you can either select a different EUID, which is available to all employees assigned to WalkMe, or you can individually add the missing information to the relevant users.

Expired Client / Secret Keys

If the key is expired, you will have to recreate it and then update the new keys in the relevant IDP connection in the **IDP Integrations** page in the WalkMe Admin Center.

Invalid Client /Secret Keys

Ensure that you have copied the correct keys and then paste them in the relevant IDP connection in the **IDP Integrations** page in the WalkMe Admin Center.