

# IDPインテグレーション

## 概要

IDプロバイダーはデジタルID情報を保存、管理し、企業が高いセキュリティ基準を維持しながら、アクセスと権限を管理する手段を提供します。

IDPインテグレーションは、その情報を取り入れて、エンドユーザーのID検証、コンテンツのセグメンテーション機能の強化、ユーザーの行動監視の拡張のために利用できます。すべての異なるシステムで利用可能で、信頼でき安全な共通のユーザIDを提供するため、さまざまな変数を使用してシステムごとに一意のユーザIDを定義する必要がありません。

IDPをユーザー識別子として使用することは、すべての新しいシステムの有効な解決策となります。

IDPインテグレーションは、[admin.walkme.com](https://admin.walkme.com)の[管理センター](#)からアクセスできます。

## □ Digital Adoption Institute

- *Digital Adoption Project Management Fundamentals* コースの「[Configure Analytics, Integrations, and Design](#)」のレッスンをご覧ください□
- DAIアカウントはまだお持ちでないですか？ [サインアップはこちら](#)から。

## ユースケース

- エンドユーザーのIDP認証をWalkMeコンテンツ表示の前提条件として使用。
- IDPパラメーター（例えばグループ、地域、部署など）によるコンテンツのセグメンテーションを拡張。
- システム全体で正確なデータ監視。

## サポート対象プラットフォーム

WalkMeのIDPインテグレーションは、**OAuth 2.0**、**OpenID Connect**、**SAML**を含む複数の認証プロトコルの使用をサポートしており、組織のIDPベンダーでユーザーを認証し、後にWalkMeでのセグメンテーションや分析に使用できるユーザー属性を取得します□ WalkMeでは、これらのプロトコルをサポートするすべてのIDPベンダーを利用できるはずですが□ WalkMeは、SPで開始されるフローをサポートしています。

## OAuth 2.0とは？

OAuth 2.0は、[Open Authorization]の略で、ウェブサイトやアプリケーションが、ユーザーに代わって他のウェブアプリケーションがホストするリソースにアクセスできるようにするための規格です。OAuth 2.0は、認証のための業界標準のプロトコルです。

## OpenID Connectとは？

OpenID Connectは、OAuth 2.0プロトコル上のシンプルなアイデンティティレイヤーであり、コンピューティングクライアントは、認証サーバーによって実行される認証に基づいてエンドユーザーのアイデンティティを確認したり、相互運用可能なRESTのような方法でエンドユーザーの基本プロフィール情報を取得したりすることができます。

現在IDPインテグレーションは以下のベンダーをサポートしています。

- Okta
- G-Suite
- ADFS
- AzureAD
- PingID
- OpenIDを使用するIDプロバイダー

OpenID Connect以外の最も一般的な認証プロトコルはSAMLです。SAMLを使用した統合の作成と設定方法については、[SAML IDPインテグレーションの記事](#)を参照してください。

## 前提条件

IDPとWalkMeのIntegration Centerの間の「橋渡し」の役目を果たすIDPアプリケーションを作成する必要があります。

サポートされる全システムについて、指示ガイドが管理センターの設定画面に表示されます。

### Select Protocol

<b>OAuth 2.0</b>	SAML 2.0
------------------	----------

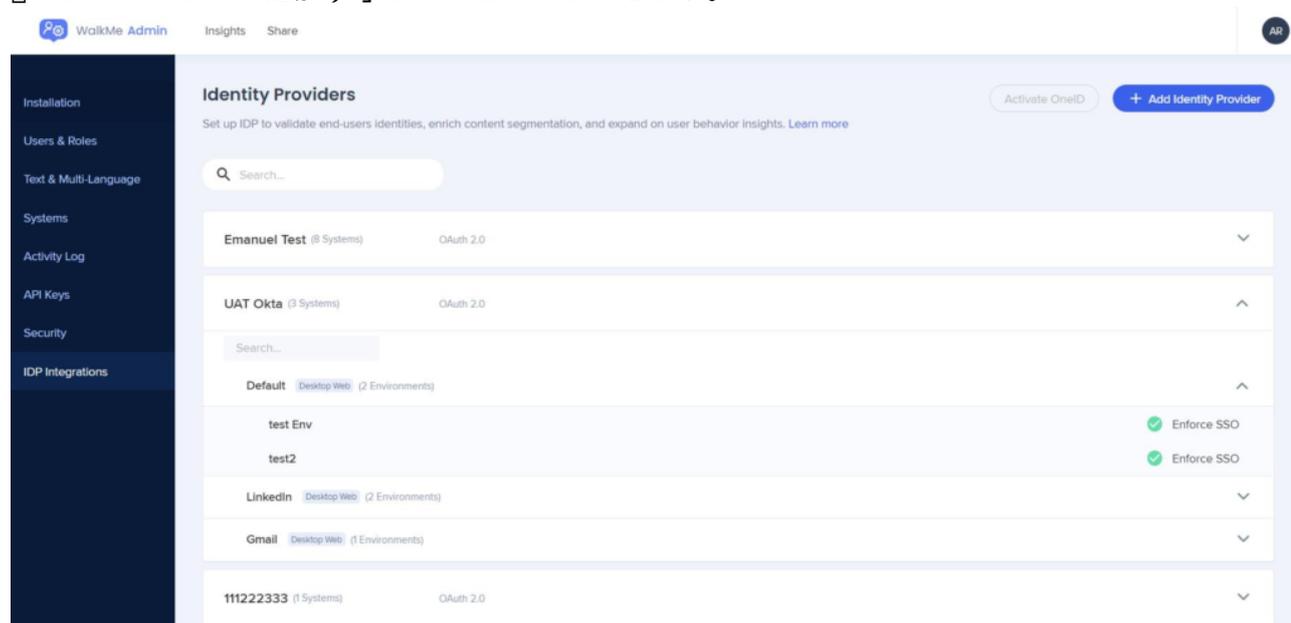
### Select Vendor

Okta	▼
------	---

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

## IDプロバイダーの追加

1. 管理センターの [ IDP Integrations (IDPインテグレーション) ] タブで、 [ + Add Identity Provider (IDプロバイダーの追加) ] ボタンをクリックします。



2. OAuth 2.0プロトコルタイプを選択します

3. 接続に適した構成設定を提供します

1. **IDP vendor** (IDPベンダー) - リストからベンダーを選択します
2. **IDP Name** (IDP名) - 接続名
3. **Client ID** (クライアントID) - アプリの公開識別子
4. **Client Secret** (クライアントシークレット) : アプリケーションと認証サーバーのみに知られている資格情報
5. **IDP Provider Domain** (IDPプロバイダードメイン) - 所属する組織のドメイン

## 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

注：選択したIDPベンダーによってフィールドが異なる場合があります。

- **OpenID Connectの場合：**

1. **IDP vendor** (IDPベンダー) - Oauth2.0ベンダーリストから「OpenID Connect」を選択します。
2. **IDP Name** (IDP名) - 接続名
3. **Client ID** (クライアントID) - アプリの公開識別子
4. **Client Secret** (クライアントシークレット) : アプリケーションと認証サーバーのみに知られている資格情報
5. **IDP Provider Discovery URL** (IDPプロバイダ「Discovery URL」)
6. **IDP Provider Scope** (IDPプロバイダー範囲)
7. **Content Security Policy** (コンテンツセキュリティポリシー)
8. **Your IDP Provider** (利用しているIDPプロバイダー)
9. **Use ID Token For Getting End-Users Properties** (エンドユーザーのプロパティ取得にIDトークンを使用) - 有効にするにはトグルをチェックします

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. 準備ができたら「Save」 「Next」(保存して次へ) をクリックします。

- サインログアウトURLは**必要でない**ことにご注意ください。

5. ユーザーを識別するためのユニークエンドユーザー識別子を選択します。

- 必要な識別子は一つだけです。追加のグループ情報や他の属性は必要ありません。

6. 必要なプロパティを選択し、正しいデータタイプが選択されていることを確認します。

1. String(文字列)
2. 番号
3. Date(日付)

注：ユーザー識別子フィールドは常に文字列タイプに変換されます。

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.

<input checked="" type="checkbox"/>	name	String
<input type="checkbox"/>	email	String
<input checked="" type="checkbox"/>	city	String
<input checked="" type="checkbox"/>	birthday	Date

Cancel
Save & Next

## ヒント：

- 選択されたデータタイプが適切であることを確認するには ⓘ アイコンの上にカーソルを合わせるとそのプロパティの値を確認できます。
- 選択されたデータタイプがプロパティに適していない場合、オレンジ色の「！」アイコンが表示され、識別されたデータタイプに切り替えることを推奨します。

## 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

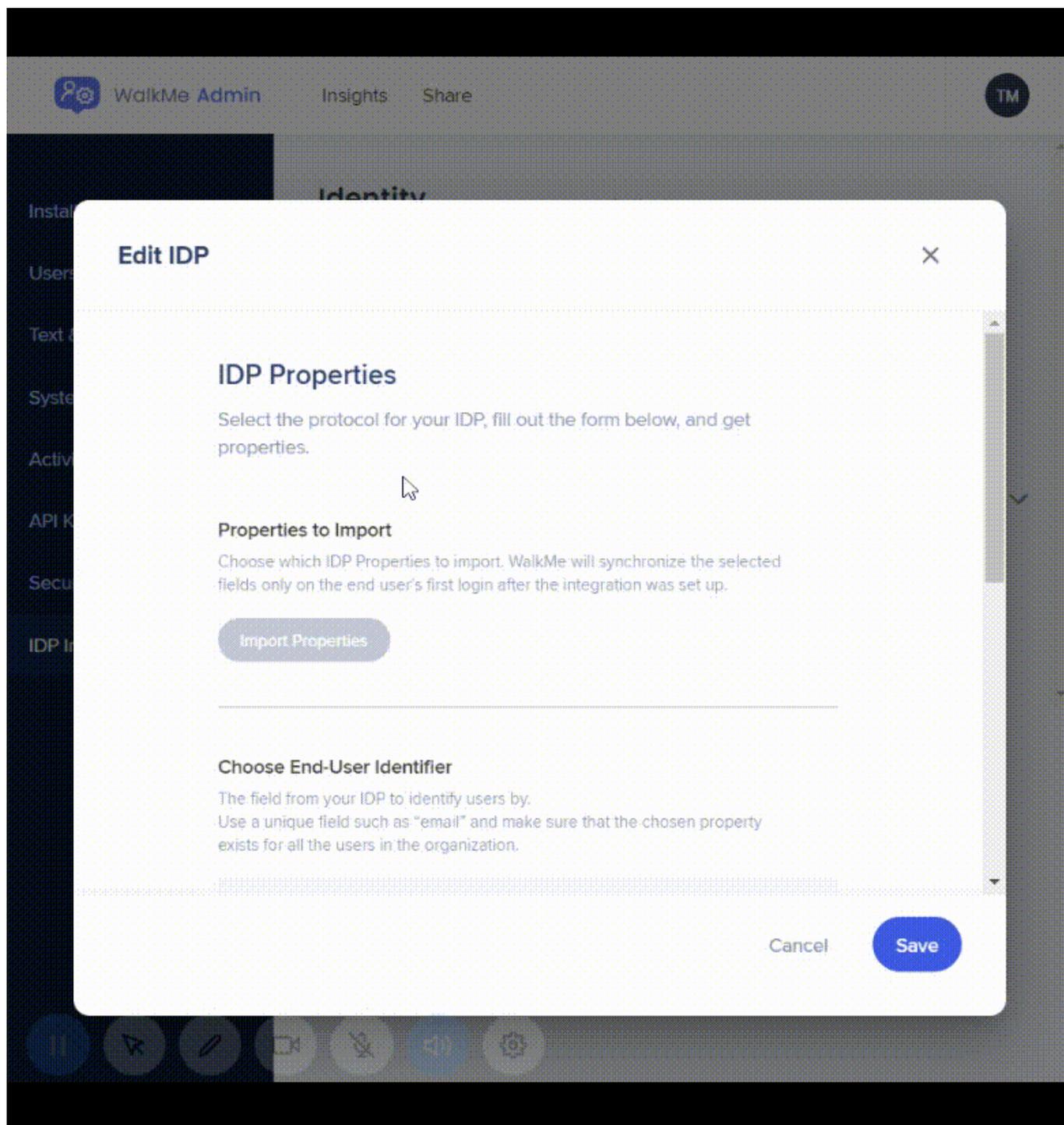
Choose the field that will be used to identify your users.

Q Search...

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

<input checked="" type="checkbox"/> name ⓘ	<span>!</span> Number <span>▼</span>
<input type="checkbox"/> email	String <span>▼</span>
<input checked="" type="checkbox"/> city	String <span>▼</span>
<input checked="" type="checkbox"/> birthday	Date <span>▼</span>

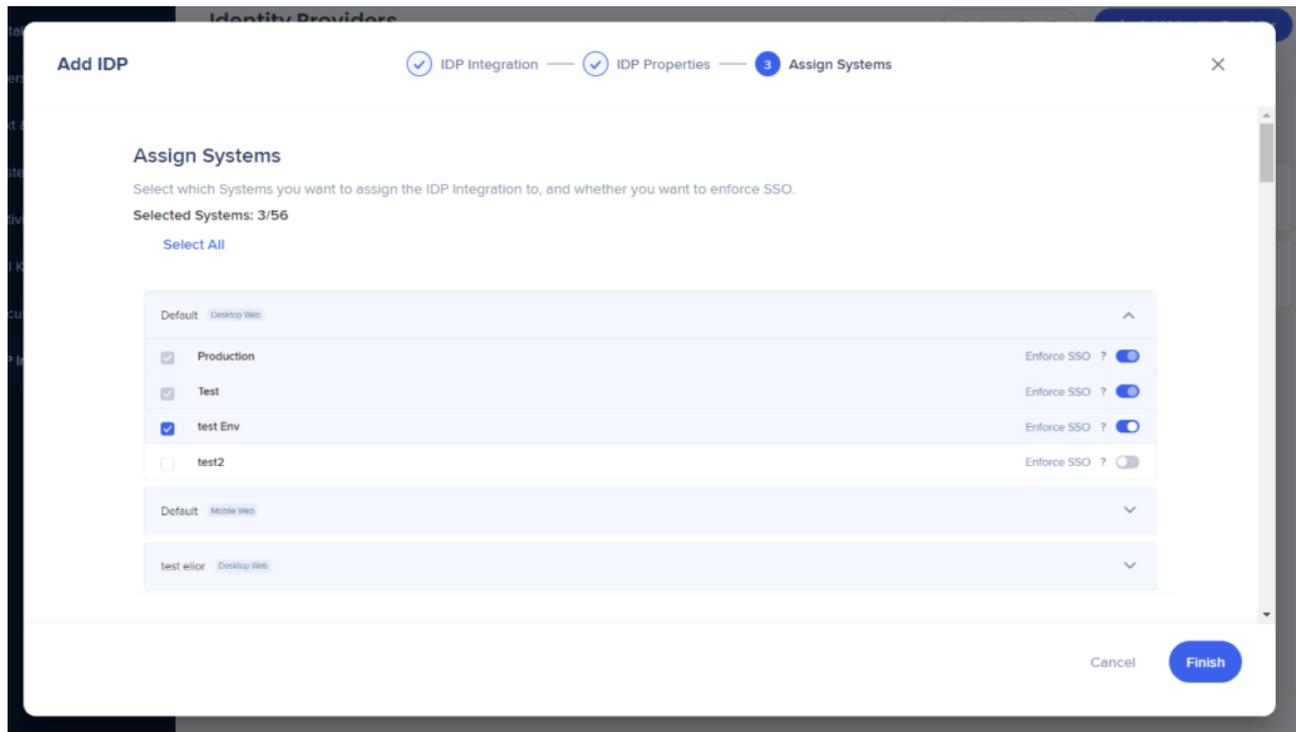
選択されたプロパティの名前の変更、元の値と名前の表示、上書きされた場合には元の値へ戻すこともできます。



7. IDPインテグレーションを割り当てたいシステムを選択します。

- 各システムごとに、目的の環境においてIDPインテグレーションを別々に有効にすることができます。

8. トグルを使用して「Enforce SSO」を設定します。



注：

- IDPは最も正確なユーザー識別情報を提供するはずですが「[Enforce SSO(SSOの強制)]が無効になっている場合、その数値は正確ではない可能性があります。
- 「[Enforce SSO(SSOの強制)]」を無効にすると、ユーザーはIDPプロバイダーの認証を受けずにアプリケーションを利用することができ「WalkMe Idが生成されてユーザー識別子として使用されます。
- ユーザーは、認証を全く必要としないアプリケーションを使用するか「IDPのログインフローを経由せずにユーザー名とパスワードで直接アプリケーションにログインすることで「IDPの認証を「スキップ」することができます。

9. 「Finish(終了)」をクリックします。

10. IDPが正常に追加されたかどうかのメッセージが表示されます。



注：

- システムを割り当てた後は、割り当てたシステムのUUID設定が自動的にIDPに設定され、パブリック化されるので、以降の作業は必要ありません。
- ベンダーからシステムの割り当てを解除することがUUIDを変更する唯一の方法です（以下の「システム割り当ての管理」の項を参照）。
- インサイトやエディタの [ User Attributes<ユーザー属性>>IDP<IDP>で、インポートされた属性を使い、設定したデータフィールドタイプに応じた適切なフィルター条件でコンテンツをセグメント化できるようになりました。
- [詳細については、こちらをご覧ください](#)

Segmentation ⓘ
×

### Create a rule to define this Segment

Group
Import Rules

Ua

User Attributes

IDP

zoneinfo

Is

USA

🗑️ ?

And ↔

Select a Type

🗑️

Add Rule

Current Statement: Cannot Assert

Cancel

Done

ヒント：

- インテグレーションによってユーザーが識別され、要求されたすべての属性が収集されていることを検証するために、すべてのユーザーデータが表示される [insights.walkme.com](https://insights.walkme.com) の [インサイト](#)

のユーザーページを表示することをお勧めします。

- ユーザーはセッションが終了した後にテーブルに追加されるためIDPを設定した後にユーザーが追加されるまで時間がかかる場合があります。

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	Agostini
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. 27, 2020	4 hours ago Nov. 10, 2020	5 hours	3 hours	1148	-	Hale

## IDプロバイダーの管理

IDプロバイダーの行にカーソルを合わせると、いくつかのオプションが表示されます。

- 削除
- システム割り当ての管理
- プロパティのインポート
- 編集
- 展開

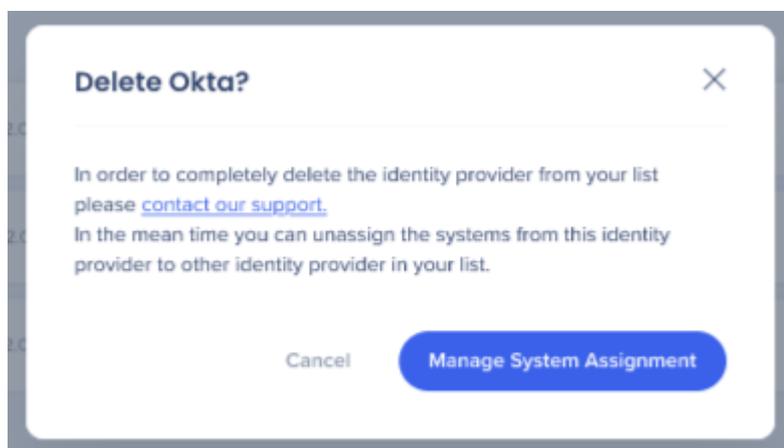
Search...	Systems	OAuth 2.0	Actions
Test IDP	(2 Systems)	OAuth 2.0	<ul style="list-style-type: none"> <li>🗑️</li> <li>⊕</li> <li>📄</li> <li>✎</li> <li>⬆️</li> </ul>
Search...			
default	Desktop Web (8 Environments)		⌵
default	Mobile Web (2 Environments)		⌵

## 削除

- ごみ箱のアイコンをクリックしてIDプロバイダーを「削除」します

### 重要な注意事項：

- サポートに連絡することなくIDプロバイダーを完全に削除することはできません。
- 削除が可能になる前に、IDプロバイダーは [ Manage System Assignment(システム割り当ての管理) ] 画面を使用して全てのシステムへの割り当てを解除されている必要があります。

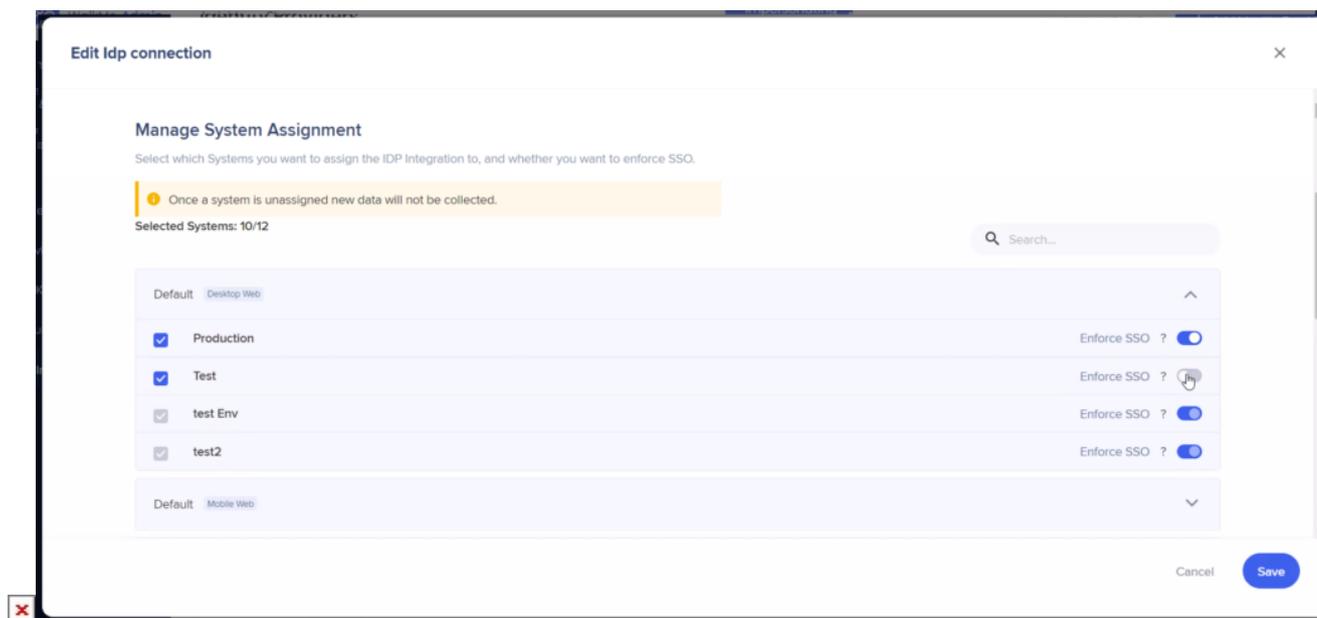


## システム割り当ての管理

- [ + ] のアイコンをクリックすると [ Manage System Assignment(システム割り当ての管理) ] 画面が表示されます。
- IDプロバイダーに割り当てたいシステムを選択または解除します
- また、トグルで [ Enforce SSO(SSOを強制) ] の設定にすることもできます。
- 完了したら [ Save Changes(変更を保存) ] ボタンをクリックします。

### 注：

- ユーザーは、インポートされたプロパティを持たないベンダーのシステム割り当て管理することはできません。プロパティを最初にインポートする必要があります。
- システムを割り当てた後は、割り当てたシステムのUUID設定が自動的にIDPに設定され、パブリッシュされるので、以降の作業は必要ありません。



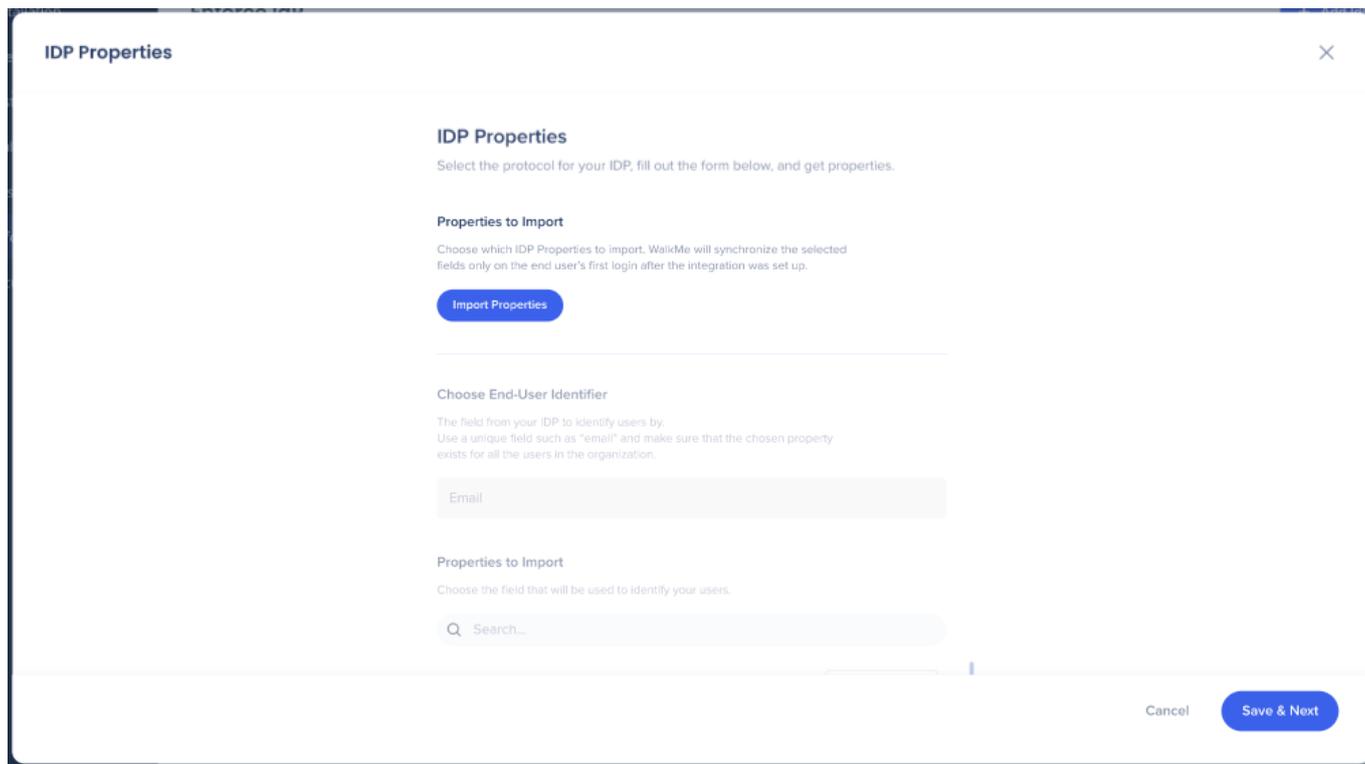
## プロパティのインポート

- リストのアイコンをクリックし、[Import Properties(プロパティのインポート)] ボタンをクリックして、新たにインポートしたプロパティを編集または追加します。

これらの属性は、インサイトでのコンテンツのセグメンテーションとレポートに使用されます。

### 注：

- そのためには、プロバイダー側のWalkMeアプリに割り当てられたユーザーでの認証が必要になります。



## 編集

- 鉛筆のアイコンをクリックしてIDプロバイダーの設定を編集します。
- IDプロバイダーの初期設定で入力したすべてのフィールドを編集することができるようになります。

## 注：

- ユーザーは、インポートされたプロパティを持たないベンダーのシステム割り当て管理することはできません。プロパティを最初にインポートする必要があります。

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

## 展開 / 折りたたみ表示

- 矢印アイコンを使って、拡大表示を展開したり、折りたたんだりします。
- 展開すると「IDプロバイダーに割り当てられているすべてのシステムと、[Enforce SSO]（SSOを強制）」が有効になっているかどうかが表示されます。



## ベストプラクティス

### [Enforce SSO] の設定

- **有効の場合** - エンドユーザーにWebページを開く前に、IDP認証を行う必要があります。IDPトークンが認識されない場合、エンドユーザーはIDPログインページにリダイレクトされます。
  - IDPがダウンした、お客様が認証情報を忘れた、エンドユーザーがIDPのアプリに割り当てられていない、などの理由でエンドユーザーがIDPへの認証に失敗するたびに[SSO]は1時間無効になります。ユーザー識別子はお客様の設定により、フォールバックとして[WalkMe ID]方式に自動的にダウンスケールされるか[WalkMe]が読み込まれません。
  - 1時間後 - IDPトークンがまだ認識されない場合、エンドユーザーは再びIDPログインページにリダイレクトされますが、そうでない場合はIDPへのログインは必要ありません。この点をお客様にしっかりと伝えることが大切です。そうでない場合は、このオプションを有効にしないでください。
- **無効の場合** - ページの読み込み時にIDP認証が試行されますがIDP用のアクティブなトークンがない場合は、エンドユーザーはIDPにリダイレクトされません。ユーザー識別子は、お客様の設定に応じて[WalkMe ID]メソッドに自動的にダウンスケールされるか、またはWalkMeが読み込まれません。

## 制限

**重要：**実装が本番環境で稼働している場合、ユーザー識別子の変更によってWalkMeがエンドユーザーを識別する方法に影響が出ることに注意してください。これにより、一意のユーザー識別子「UUID」が変更されたために、自動再生ルール（例えば「一度だけ再生」の設定）がリセットされたり、ユーザーが以前設定したオンボーディングタスクが未修了となったりする可能性があります。各ユーザーが、新しい一意のユーザー識別子の値に関連づけられた新規のユーザーとして認識されるため、この制限を回避する方法はありません。

- IDPではSafariブラウザー拡張がサポートされていません
- ユーザー識別子の変更は、WalkMeによるエンドユーザー識別の方法に影響を与えるため「Play once（一度だけ再生）」の設定がリセットされる場合があります。
- ユーザーは管理センターの管理者権限を持っている必要があります。
- IDPは、必要なシステム上で設定する必要があります。
- エンドユーザーは、IDPを使ってそのシステムに認証を行う必要があります。
- 会社がCSP（コンテンツセキュリティポリシー）を導入している場合「IDPプロバイダーへのコールがブロックされます」。
  - この問題を解決するには、エクステンションのCSP設定で正しいURLを追加する必要があります。
- システムを割り当てた後は、割り当てたシステムのUUID設定が自動的にIDPに設定され、パブリッシュされるので、以降の作業は必要ありません。
  - IDPの変更を有効にするためには、お客様のシステムをWalkMeの最新バージョンにアップデートする必要があります（これは設定のパブリッシュにより実行できます）。
  - エンタープライズアカウントの場合、パブリッシュ時に「Update to the latest WalkMe version（WalkMeの最新バージョンに更新する）」をチェックする必要があります。
- 日付タイプのプロパティをインポートすると、次のフォーマットのみがサポートされます。
  - 2018-02-20
  - 2018-02-20T14:32:00
  - 12/30/2018
  - 日付として文字列または数字をインポートすると、インサイトフィルタリング/エディタセグメンテーションでは動作しません

### Mobile Web

- IDPの設定が完了すると、自動的にMobile Webが有効になります。
- IDP / OneIDを有効化した後にMobile Webを追加した場合「Mobile WebをサポートするにはIDPを無効化してから再度有効化する必要があります」。

## 共通の問題の解決

### ユーザーが割り当てられていません

これを防止するには、すべての従業員をWalkMeに割り当てる必要があります。御社のIT担当者は、IDPプロバイダのWalkMeアプリへのアクセス設定をすべての従業員に変更することで、これをサポートできるはずですが。

### ユーザープロフィールでEUIDが見つかりません

これに対処するには、WalkMeに割り当てられたすべての従業員が使用できる別のEUIDを選択するか、不足している情報を関連するユーザーに個別に追加します。

### 期限切れのクライアント/秘密キー

キーの有効期限が切れている場合は、キーを再作成し、WalkMe管理センターの「IDP統合」ページにある関連するIDP接続の新しいキーを更新する必要があります。

### 無効なクライアント/秘密キー

正しいキーがコピーされていることを確認し、WalkMe管理センターの「IDP統合」ページで関連するIDP接続に貼り付けます。