SAML IDPの統合

概要

WalkMeのIDP統合では、組織のIDPベンダーによるユーザーの認証を行い、後でWalkMeでのセグメント化や分析に利用するユーザーの属性を取得するため、SAMLと呼ばれる認証プロトコルを利用できます。 WalkMeでは、SAMLに対応するすべてのIDPベンダーが利用可能であるはずです。 WalkMeは、SPで開始されるフローをサポートしています。

SAMLとは何ですか？

SAMLは、”Security Assertion Markup Language”の略であり、アイデンティティプロバイダ（IDP）がサービスプロバイダ（SP）に認証資格情報を渡せるようにするオープン標準です。 これによって、コンピューティングクライアントは認証サーバーが実行する認証に基づきエンドユーザーの本人確認を行い、エンドユーザーの基本プロファイル情報を取得できます。

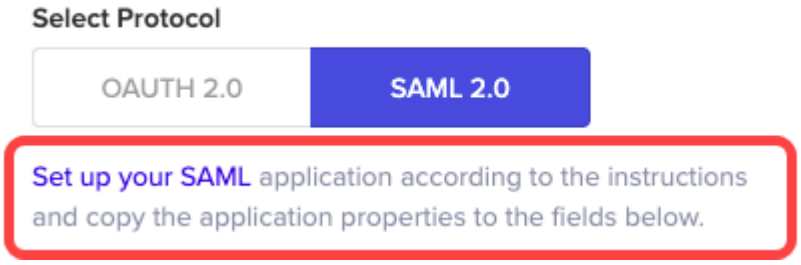
ユースケース

- 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ト化を拡張。
- システム全体で正確なデータ監視。

前提条件

IDPとWalkMeのIntegrationCenter（統合センター）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。

指示ガイドは、IDP統合の設定画面の管理センターで利用できます。



IDプロバイダーからのメタデータと証明書の取得

これらの手順は一般的なものです。 特定のIDプロバイダ（IdP）にこの情報を配置する必要があります。

- **SSO URL（シングルサインオンURL）**：SAML認証要求を送信する必要があるIdPのURL。これはSSO URLと呼ばれることが多いでしょう。
- **X509署名証明書**：サービスプロバイダーがIdPによってデジタル署名された認証アサーションの署名を検証するために必要な証明書。IdPから署名証明書をダウンロードする場所が必要です。証明書が .pemまたは.cer 形式ではない場合、そのいずれかの形式に変換する必要があります。後で、これをWalkMeに貼り付けます。
  この証明書の取得方法は異なるため、追加のサポートが必要な場合は、IdPのドキュメントを参照してください。

注：

- X.509署名証明書をWalkMeにアップロードする前に、ファイルをBase64に変換する必要があります。
- これを行うには、オンラインツールを使用するか、Bashで以下のコマンドを実行します：
  cat cert.crt | base64

IdPへのWalkMeサービスプロバイダーメタデータの追加

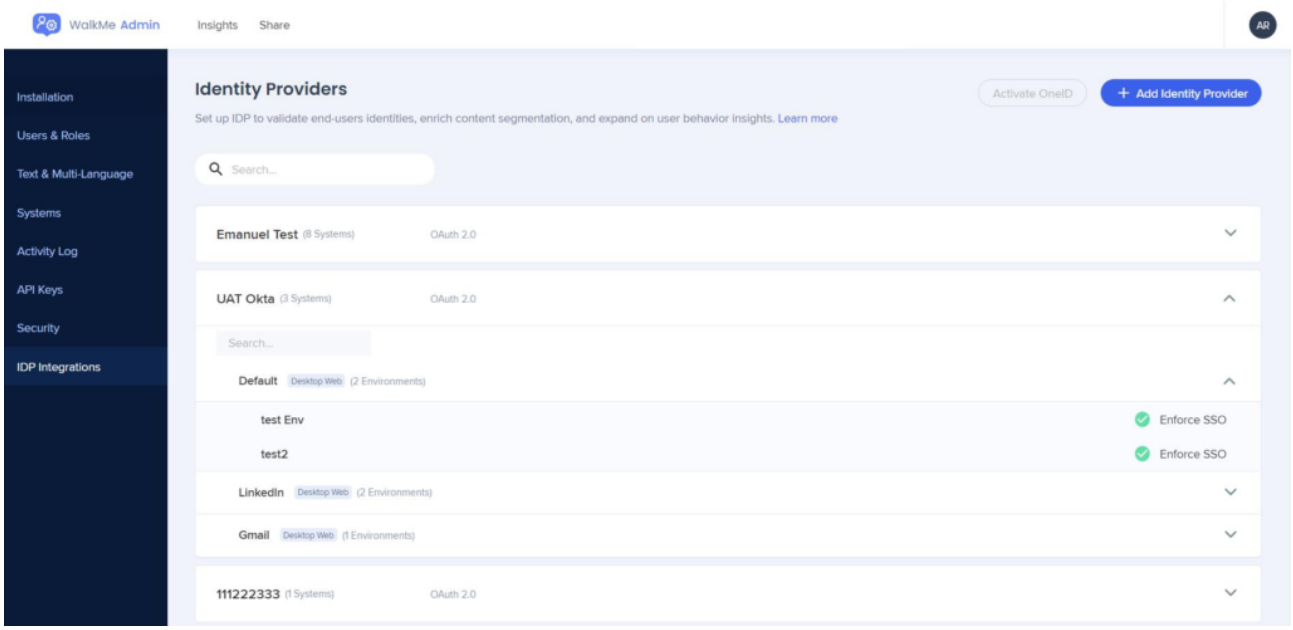
テナントがSAML認証リクエストを受信し、応答する方法を認識できるように、サービスプロバイダーに関する情報をIDプロバイダーに追加します。ここに記載された手順は一般的なものです。IDプロバイダーに適切な画面とフィールドを見つける必要があります。

1. SAMLの設定を可能にするIDプロバイダーに画面を配置します。IdPがメタデータファイルのアップロードをサポートしている場合、上記の手順で取得したメタデータファイルを指定するだけです。IdPがメタデータのアップロードをしていない場合、以下のように手動で設定できます。
2. ユーザーの認証が済んだ後に、IdPはSAMLアサーションを送信する場所を認識する必要があります。これは **WalkMeのアサーションコンシューマーサービスURL** です。Idpはこの **アサーションコンシューマーサービスURL**または**アプリケーションコールバックURL**を呼び出すことができます。
   米国：https://papi.walkme.com/ic/idp/p/saml/callback
   EU：https://eu-papi.walkme.com/ic/idp/p/saml/callback
3. IdPが**オーディエンス**または**エンティティID**と呼ばれるフィールドを呼び出した場合、そのフィールドにWalkMeから**取得**したエンティティIDを入力します：
   米国：https://papi.walkme.com EU：https://eu-papi.walkme.com
4. IdPがバインディングの選択を提供する場合、**認証リクエストに**HTTP-Redirectを選択する必要があります。

IDプロバイダーの追加

1. 管理センターの［IDP Integrations（IDP統合）］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. SAML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

メタデータファイルをダウンロードする

- 個別にコピー&ペーストすることなくWalkMeの情報をメタデータファイル経由でシステムにアップロードすることができます。

必須フィールド：

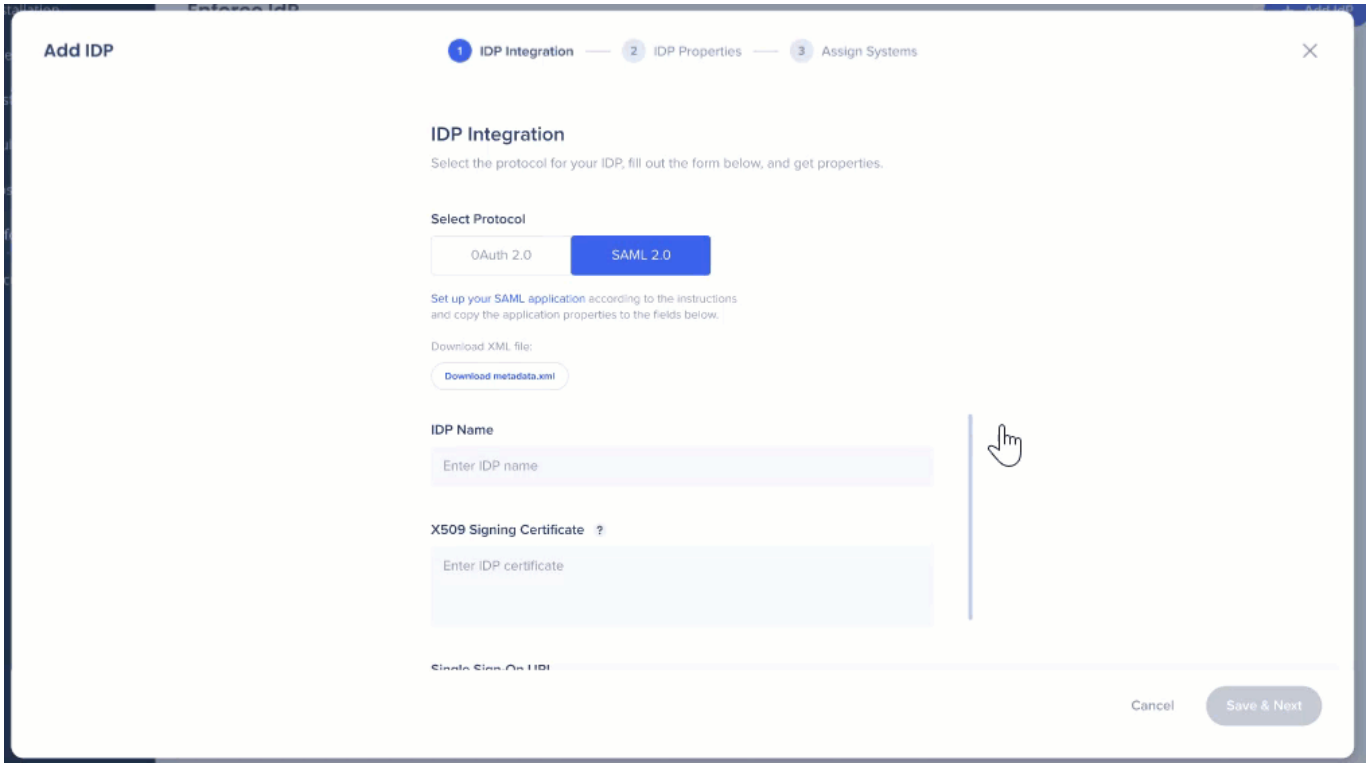
- **IDP Name**（IDP名） – 接続名
- **シングルサインオンURL** – プロバイダーセットアップウィザード から取得したIDプロバイダーシングルサインオンURL
- **X509署名証明書** – プロバイダー からダウンロードした証明書をアップロードします。

オプション – 暗号化設定：

トランザクションのセキュリティを高めるためにSAMLプロトコル内でリクエストと応答の両方に署名または暗号化を実行できます。

まず、アカウントに固有の証明書を生成し、ダウンロードする必要があります。
IDPプロバイダーにアップロードするため、公開鍵が共有されます。

- **AuthnRequest** - プライベートキーを使用してSAML認証リクエストに署名します。
- **アサーション暗号化** – IDプロバイダーから暗号化されたアサーションを受信します。 そのためにはIDPに公開鍵証明書を提供する必要があります IDPは、公開鍵を使用してSAMアサーションを暗号化し、WalkMeに送信しますWalkMeは秘密鍵を使用して、それを復号します。



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。

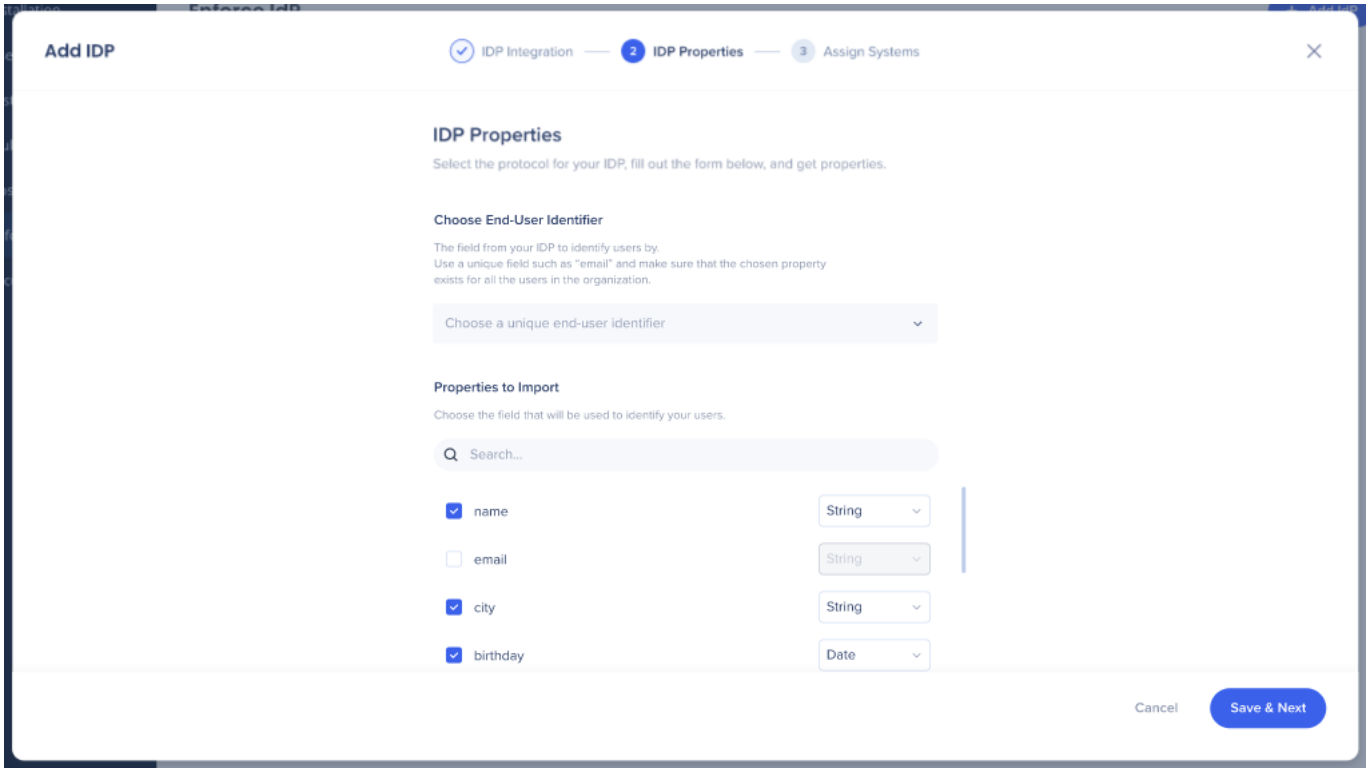
5. ユーザーを識別するためのユニークエンドユーザー識別子を選択します。

- 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。

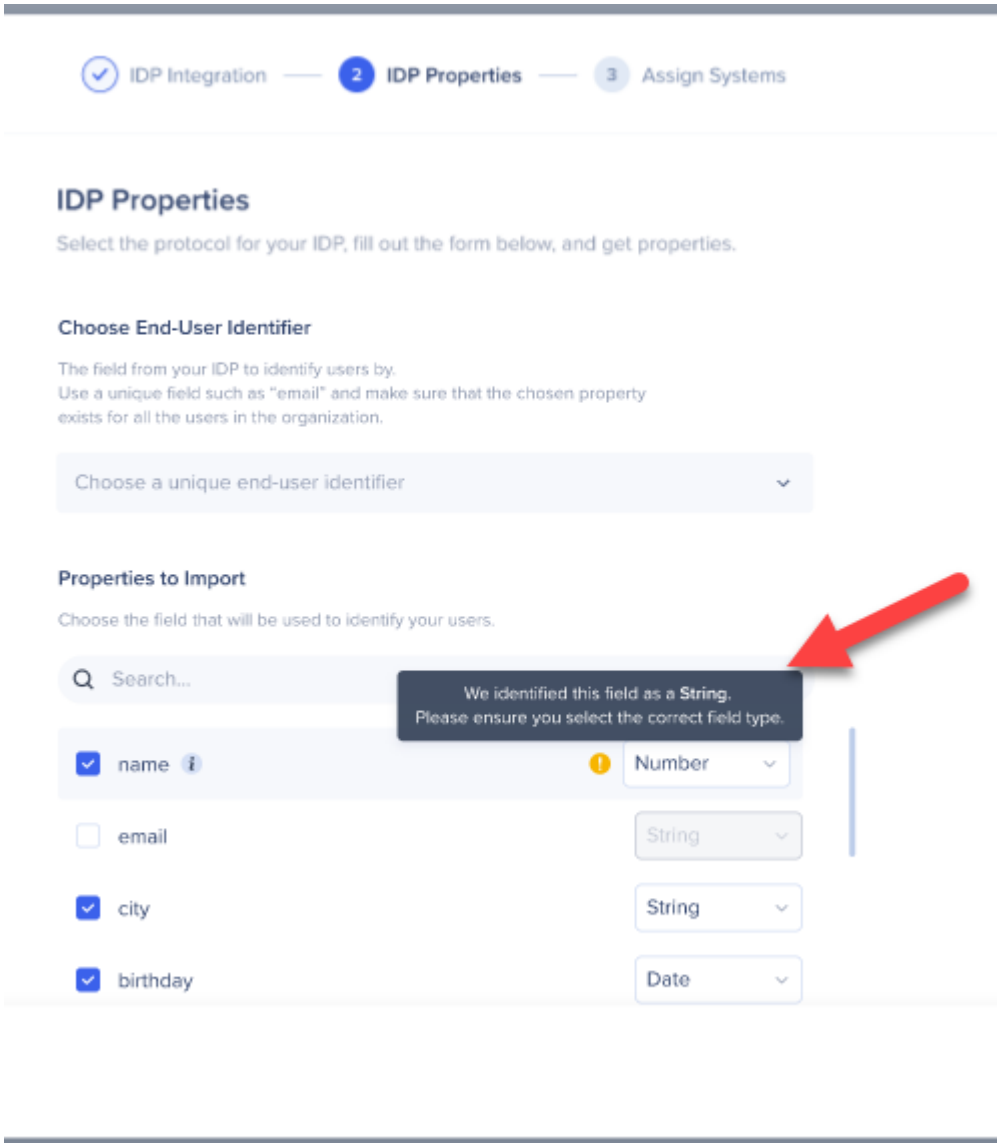
1. 文字列
2. 番号
3. Date (日付)

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。



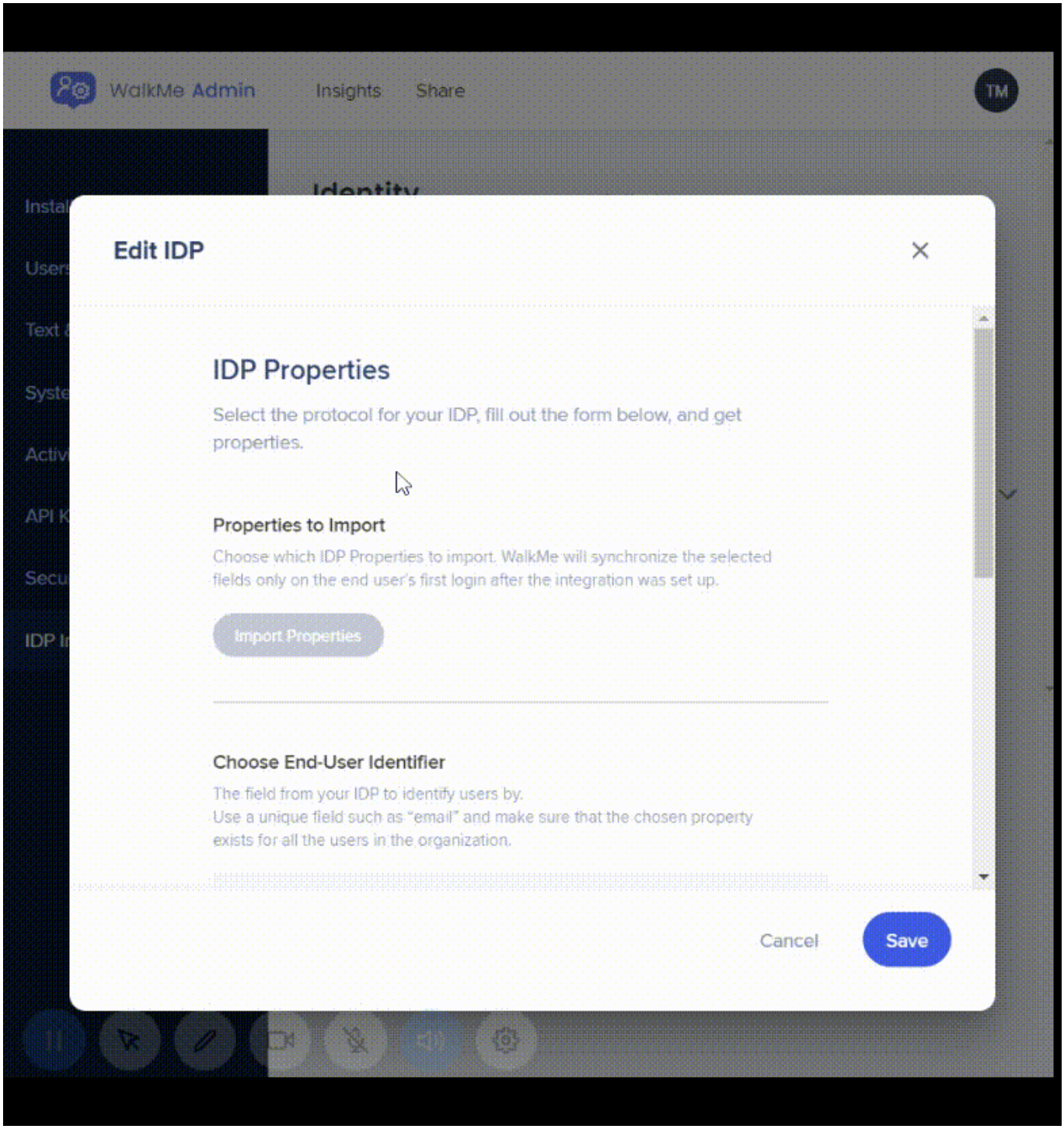
ヒント：

- 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□□i□アイコンの上にカーソルを合わせることでそのプロパティの値を確認することができます。
- 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「i□アイコンが表示され、識別されたデータタイプに戻ることを推奨します。



[ht_message mstyle="info" title="" show_icon="" id="" class="" style=""]

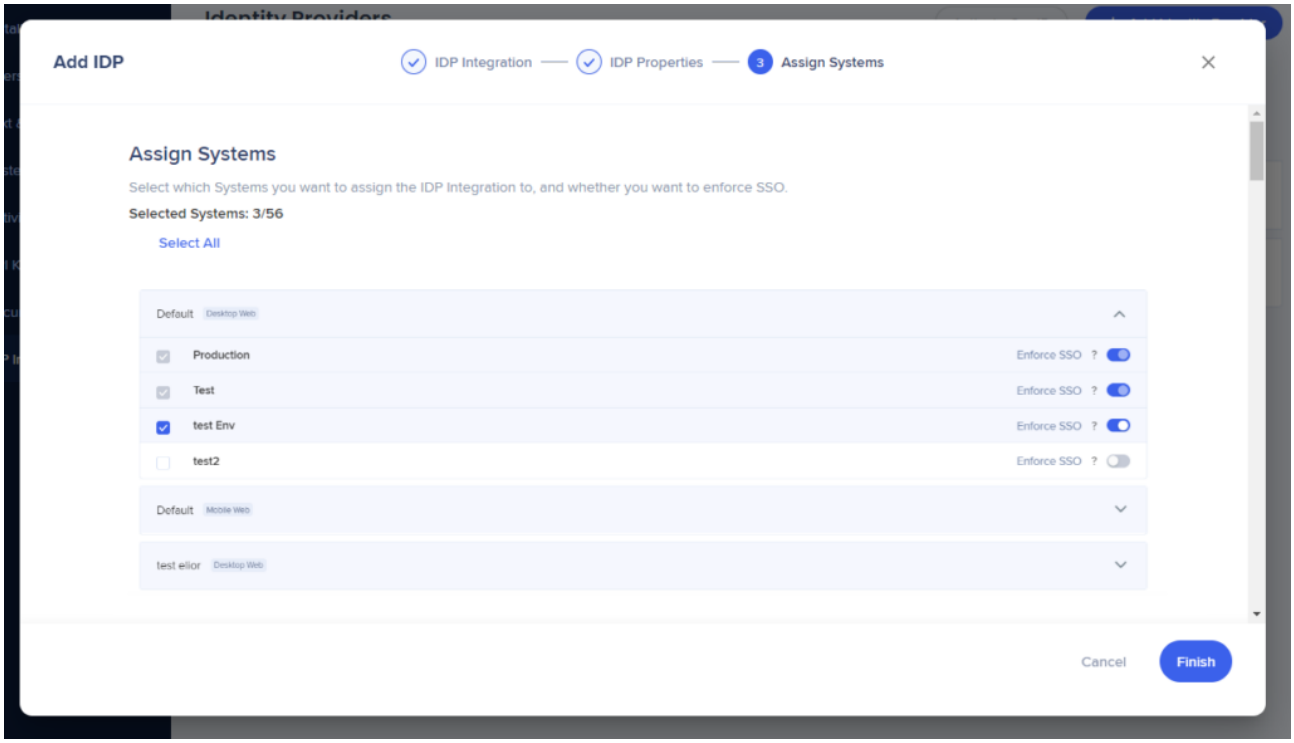
選択されたプロパティの名前の変更、元の値と名前の表示、上書きされた場合には元の値へ戻すこともできます。



7. IDP統合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。

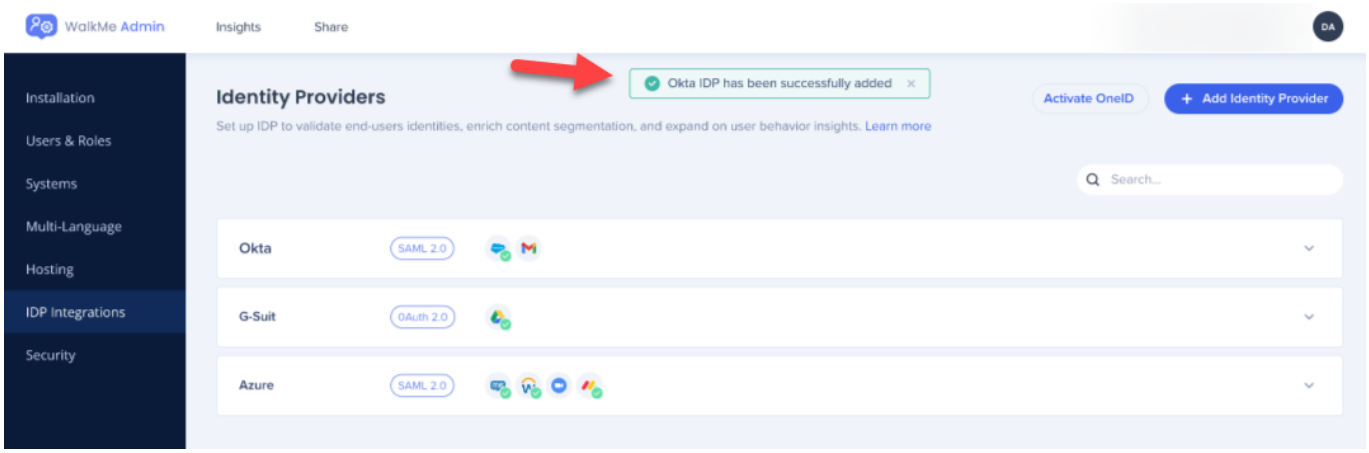


注：

- 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/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。

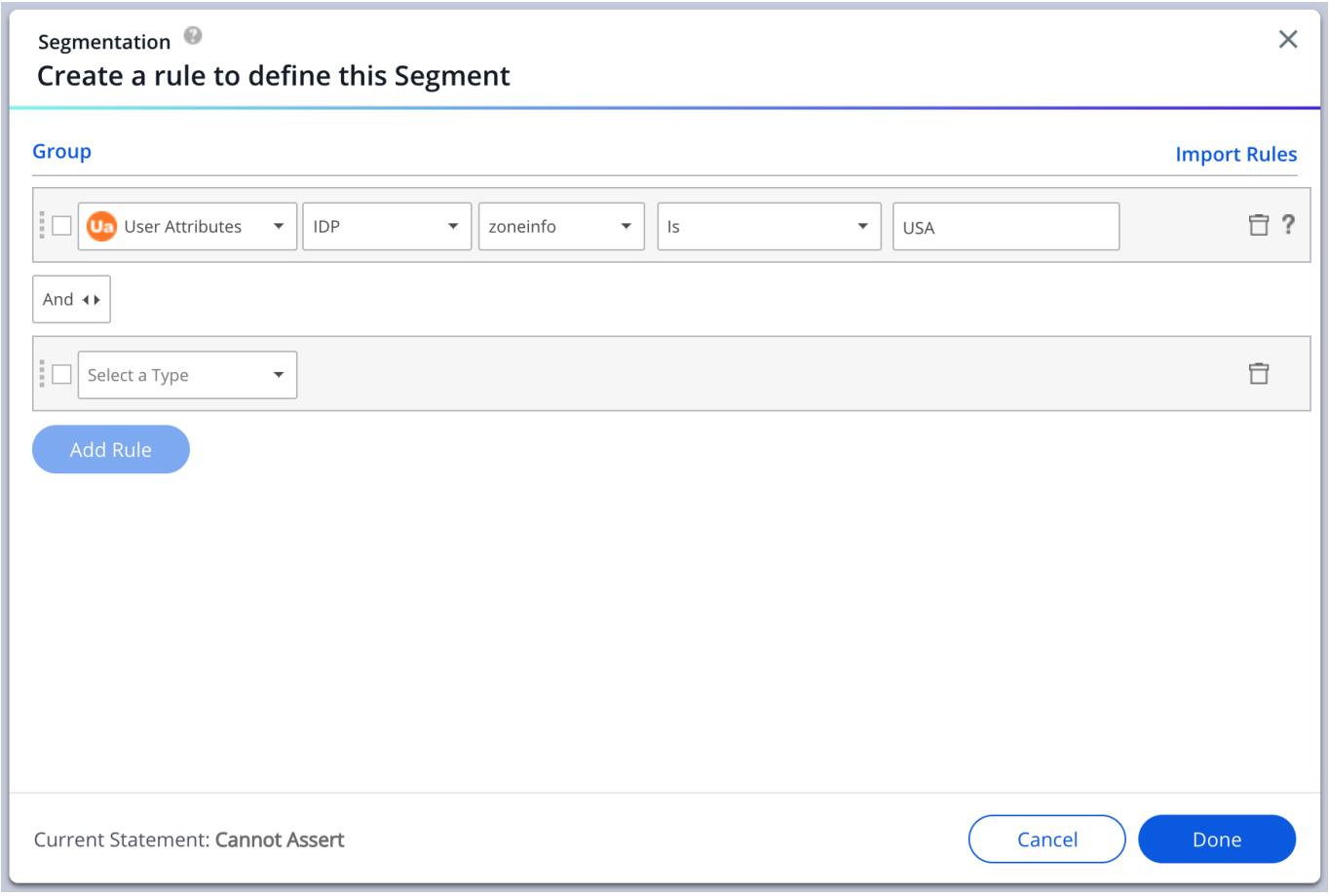
10. IDPが正常に追加されたかどうかのメッセージが表示されます。



注：

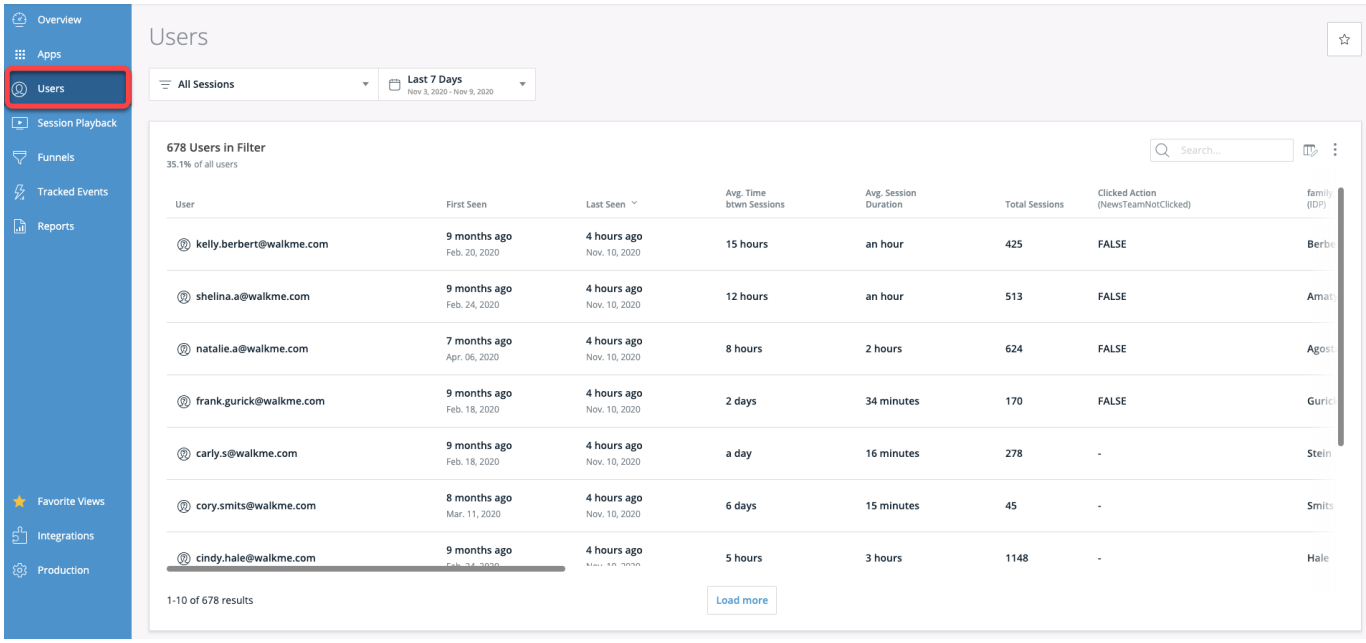
- **システムを割り当てた後は、割り当てたシステムのUUID設定が自動的にIDPに設定され、公開されるので、以降の作業は必要ありません。**
- **ベンダーからシステムの割り当てを解除することが**UUIDを変更する唯一の方法です（以下の「**システム割り当ての管理**」の項を参照）。

- 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、InsightsやUser Attributes（ユーザー属性）>>IDPのEditorでインポートされた属性を使って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



ヒント：

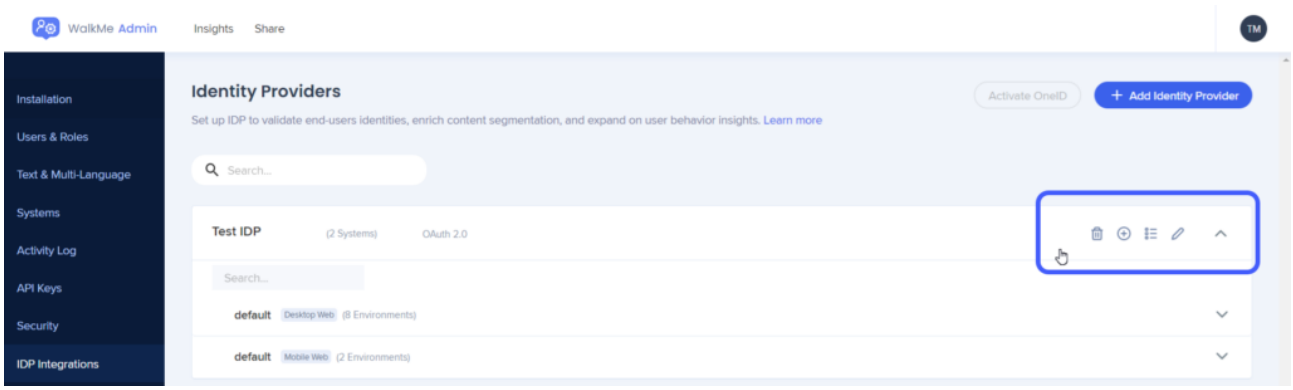
- 統合によってユーザーが識別され、要求されたすべての属性が収集されていることを検証するために、すべてのユーザーデータが表示される**insights.walkme.com**の**インサイト**のユーザーページを表示することをお勧めします。
- **ユーザーはセッションが終了した後にテーブルに追加されるため**IDPを設定した後にユーザーが追加されるまで時間がかかる場合があります。



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
- プロパティーのインポート
- 編集
- 展開



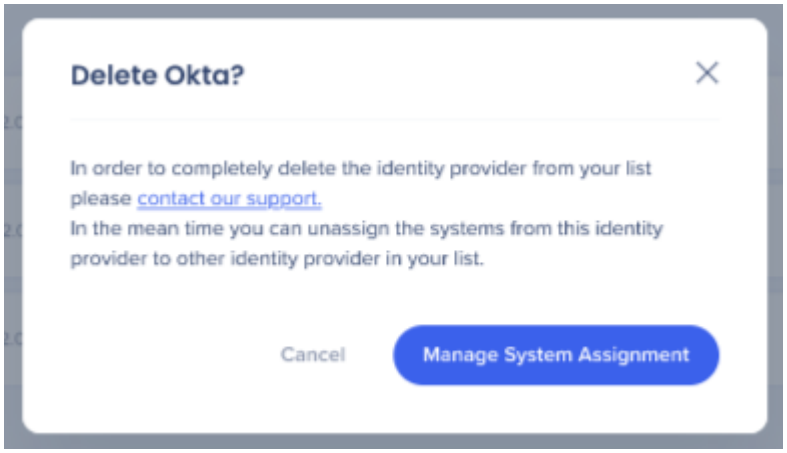
削除

- ゴミ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

[ht_message mstyle="info" title="" show_icon="" id="" class="" style=""]

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しま**
- **また、トグルで「Enforce SSO」に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ー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。 プロパティー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、公開されるので、以降の作業は必要ありません。**

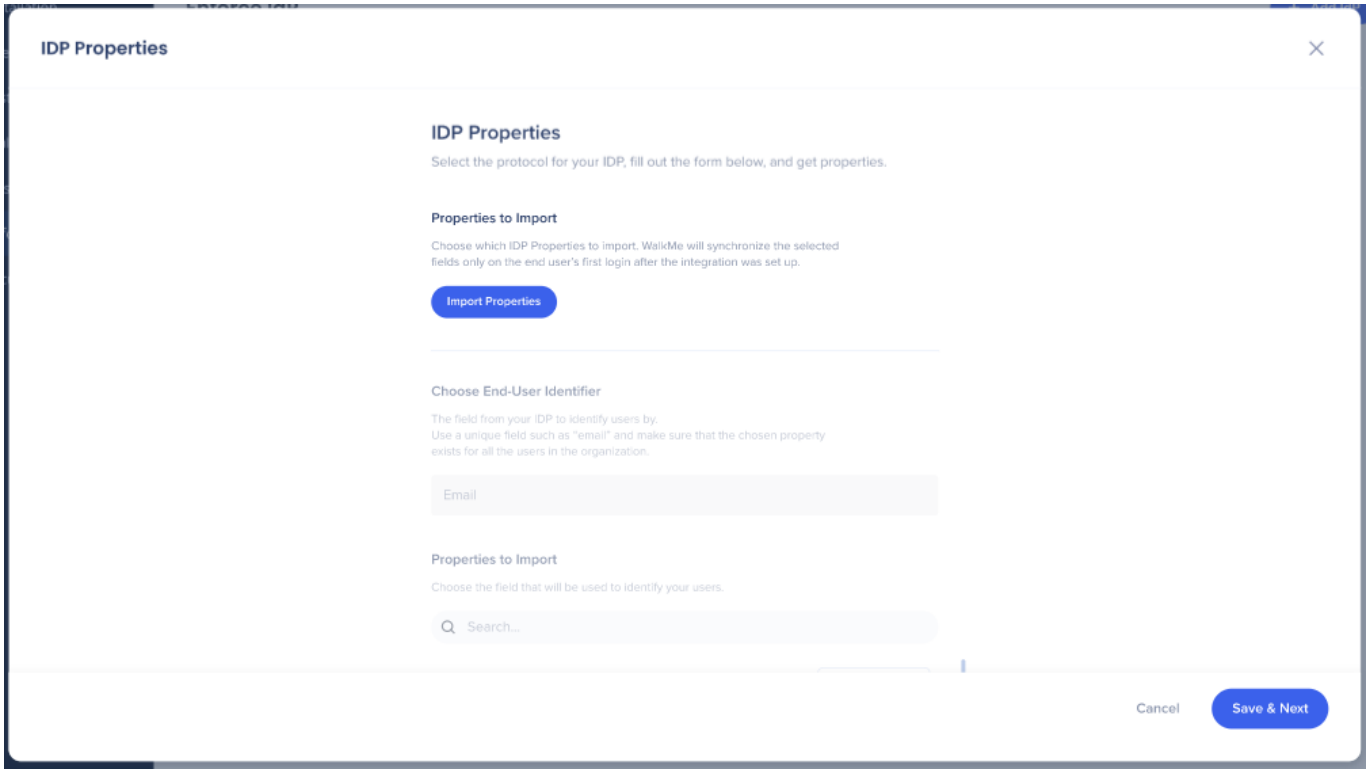
プロパティーのインポート

- リストのアイコンをクリックし、[Import Properties[プロパティーのインポート）］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ーを編集または追加します。

これらの属性は、Insights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。

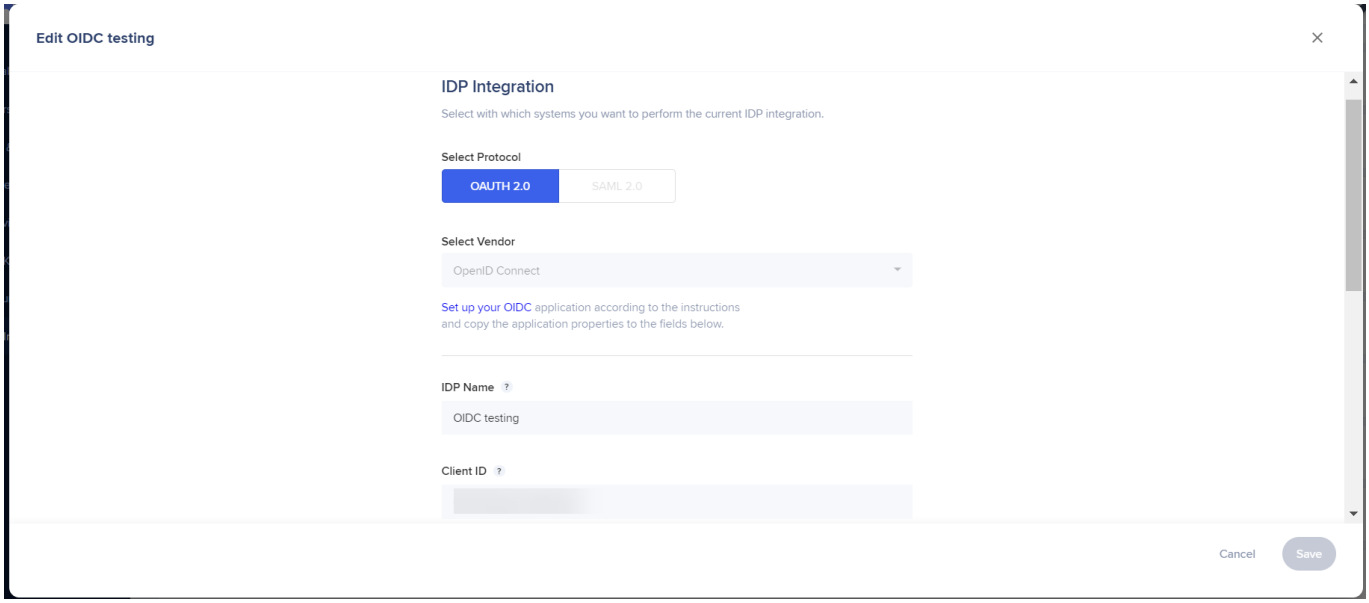


編集

- 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。

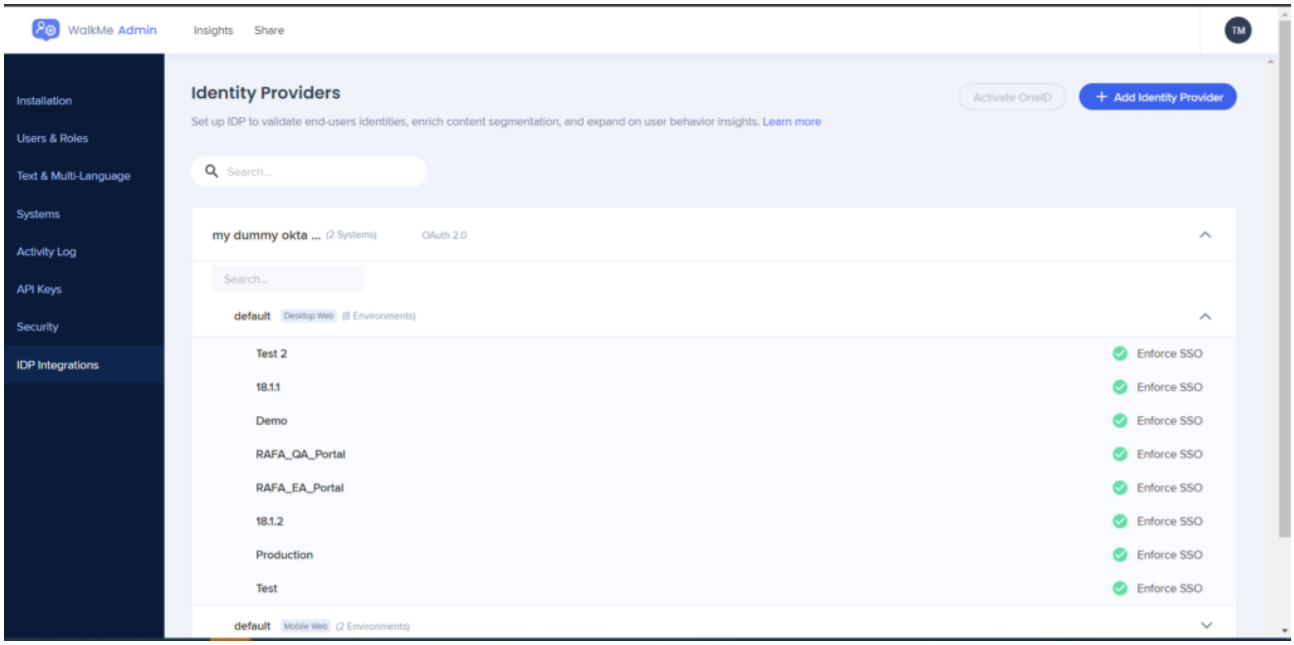
注：

- **ユーザーは、インポートされたプロパティー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。 プロパティーを最初にインポートする必要があります。**



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、EnforceSSO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

- ***有効な場合***–エンドユーザー にウェブページを開く前に、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。
- ***無効な場合*** – 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：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。

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Onboarding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。

- Safariブラウザーは**IDPをサポートしていません。**
- 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・セキュリティー・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、拡張機能設定の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、公開されるので、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、公開時に［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。

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。

[/ht_message][/ht_message]