

グローバルIDPの統合

概要

グローバルIDPの統合は、マルチシステムアカウントに使用できます。WalkMeのアカウントごとに複数のプロバイダーがサポートされています。アカウントのすべてのシステムは、同じプロバイダーを使用したり、別のプロバイダーを使用したりするように設定できます。統合センターのIDP統合の設定は、いずれかのシステムで1回しか行われません。そして、そのアカウントの他のシステムに自動的にコピーされます。すべてのプロバイダーが設定されたら、システムごとに特定のプロバイダーを選択できます。

IDPを識別方法として使用するには、エディターでIDPを各システムのユーザー識別子として個別に定義する必要があります。これによりIDPが使用されるシステム、およびユーザー識別の別の方法が使用されるシステムを選択できます。ユーザー識別子としてIDPがないシステムはIDPプロバイダーでの認証を必要としないため、ユーザープロパティはこれらのシステムでプルされず、使用もされません。

[IDP統合の詳細については、こちらをご覧ください。](#)

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。

サポート対象プラットフォーム

IDP統合は現在OpenID Connectを使用するIDプロバイダーでサポートされています。

- Okta
- G-Suite
- ADFS(2012バージョン)
- AzureAD
- PingID

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。

サポートされているすべてのシステムの取扱説明書は、統合センターの設定画面で参照できます。

oAuth2 Integration

Identity Provider Settings

Set up the integration to your identity provider. Find more information in [the oAuth2 integration guide](#).

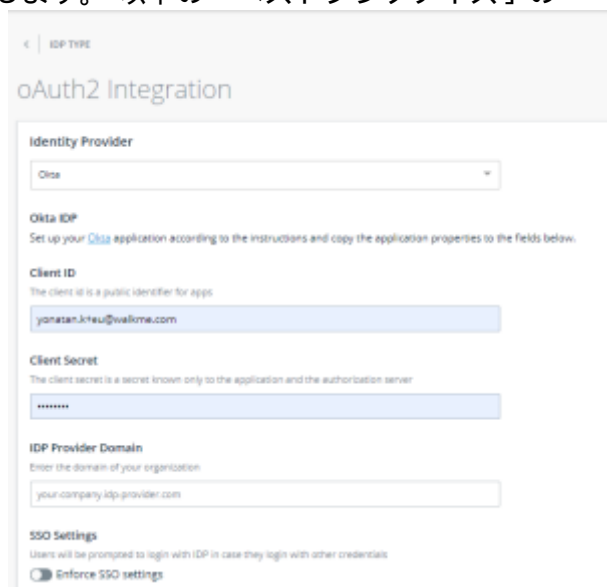
統合の作成と設定



There are no Identity Provider yet

[+ ADD IDENTITY PROVIDER](#)

1. IDプロバイダーを追加します。
2. プロトコルタイプを選択します。
3. IDPベンダータイプを選択します。
4. すべてのIDプロバイダーの詳細を定義し、保存します。以下の「ベストプラクティス」の



oAuth2 Integration

Identity Provider

Okta IDP

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

Client ID

The client id is a public identifier for apps

your-client-id@walkme.com

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

your-company.idp-provider.com

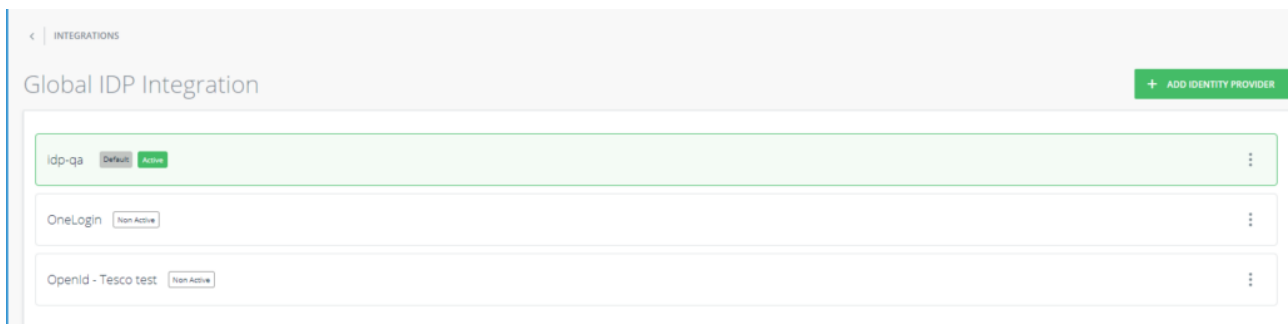
SSO Settings

Users will be prompted to login with IDP in case they login with other credentials

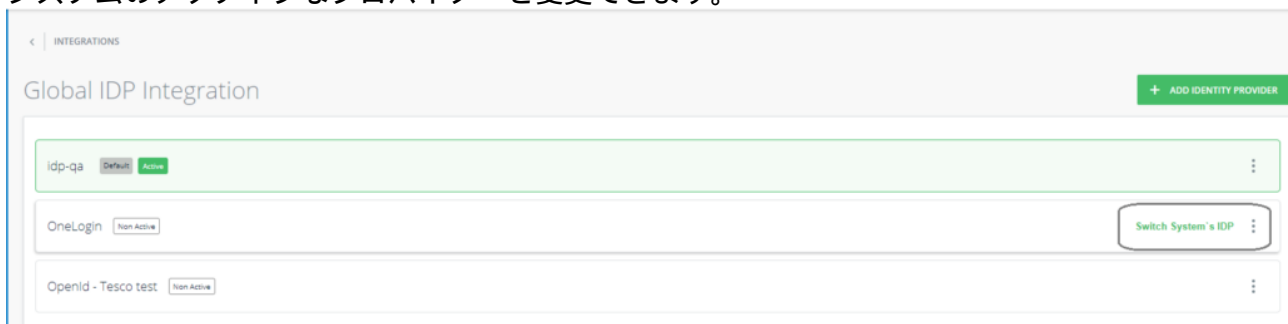
☐ Enforce SSO settings

「Enforce SSO」の設定の詳細をご覧ください。

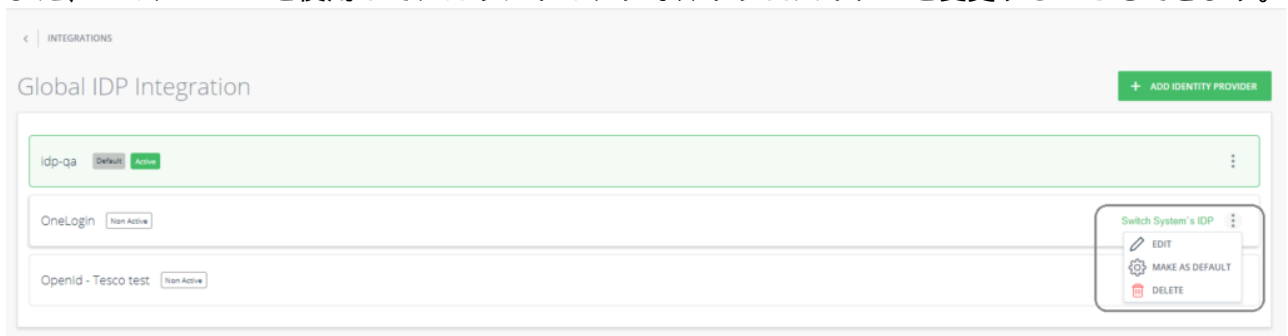
5. 最初のIDPが設定されたら、アカウントのすべてのシステムのデフォルトプロバイダーになります。デフォルトのプロバイダーとは、アカウントごとに複数のプロバイダーが存在する場合、設定が変更されるまではこれがデフォルトでアクティブなプロバイダーになるという意味です。必要に応じて、プロバイダーを追加できます（オプション）。



6. これで「Switch systems' IDP (システムのIDPを変更)」をクリックすることで、アカウントの各システムのアクティブなプロバイダーを変更できます。

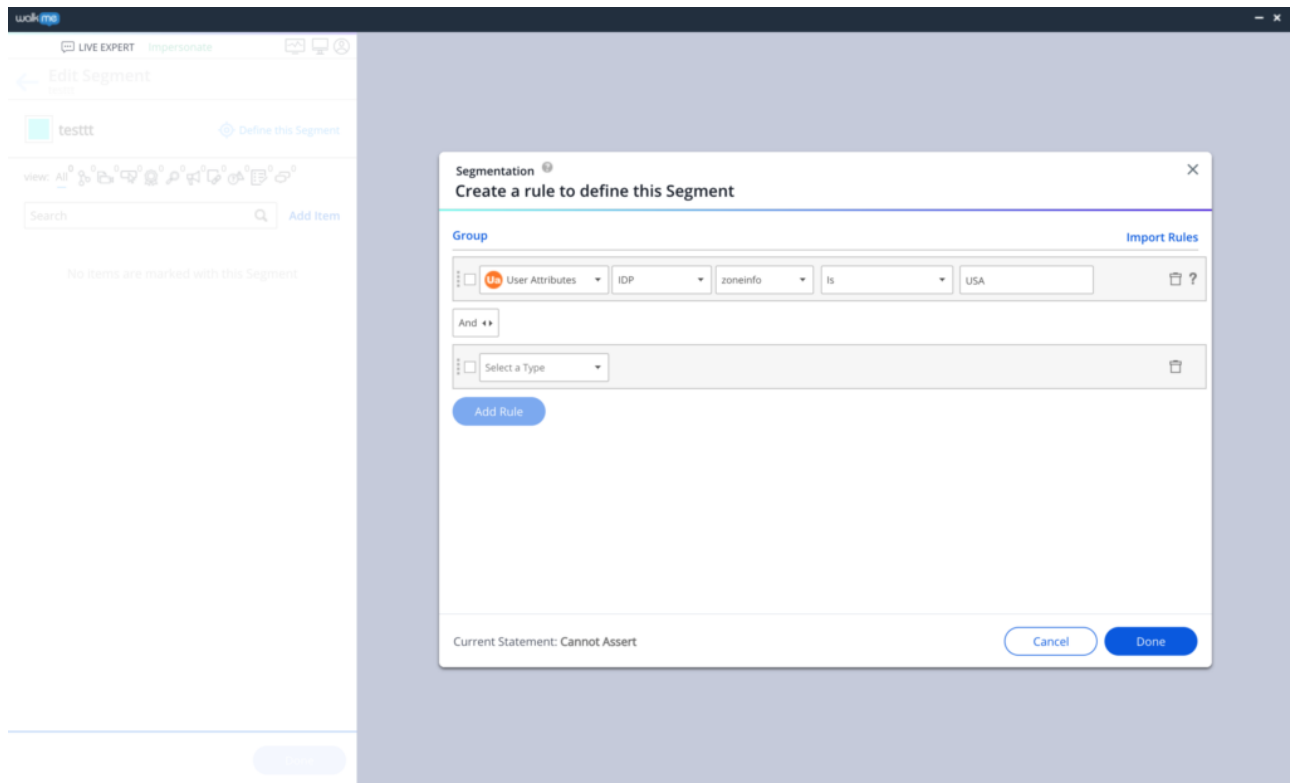


7. また、このメニューを使用してアカウントのデフォルトプロバイダーを変更することもできます。



11. 該当する環境の新しい設定を公開します。

12. これで「Segmentation Center (セグメント化センター)」を介してUser Attributes (ユーザー属性) > IDPの下の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。



注：IDP統合は、統合センターの段階でアカウントレベルで設定されます。ユーザー識別子のパラメーターの変更はシステムレベルで行われます。

ワークステーションユーザー

上記の手順を完了したら、アカウントマネージャーに連絡して、手順の続きを行ってください。

ベストプラクティス

- [Enforce SSO]設定 –
 - 有効 – 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、SSOは1時間無効になります。ユーザーIDは設定に応じて、フォールバックとして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が読み込みを行いません。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。
 - 無効 – ページの読み込み時にIDP認証が試行されますがIDP用の有効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。そのユーザーIDは「WalkMe ID」メソッドに自動的にダウンスケールされます。

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、ユーザーの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。

- 利用できるIDP統合は、アカウント当たり1つのみです。