シングルサインオン（SSO）

概要

管理センターのシングルサインオンページでは、新しい認証基盤に基づいてエンタープライズグレードの**セルフサービスSSO**の設定管理を提供します。

ユースケース

- Onboardingの時間を短縮
- **セルフサービス**の設定と管理の有効化
- 旧式の**プロプライエタリな**SSOの置き換え
- 完全なSSO機能の有効化
- **セキュリティとコンプライアンス**の強化

SSO用語集

アサーション：以下の**サービスプロバイダへのステートメントを1つ**以上提供するIdPが 供給するデータ：

- *Authentication statements（認証ステートメント）*は、アサーションで指定されたユーザーが実際にいつ認証に成功したかを主張します。
- *Attribute（属性）ステートメント*は、ユーザーに係る属性値を与えます（ NameID（名前ID）属性は必須で、ユーザー名を指定しますが、他の属性も手動で設定することができます。
- *Authorization decision（認証の決定）*ステートメントは、アサーション対象者が指定されたリソースへのアクセスを求める要求が承認または拒否されたことを宣言します。

Assertion Consumer Service（アサーションコンシューマーサービス）ACS（SAMLアサーションの受信と分析を担うサービスプロバイダのエンドポイント（URL）） 一部のサービスプロバイダは、ACSに別の用語を使用していることに留意してください（ OktaのSAMLテンプレートでは、こちらを**シングルサインオンのURL**フィールドに入力します。

Attribute（属性）：ユーザーの名前、ファーストネーム（名）、従業員IDなどのユーザーに関するデータセット

Audience Restriction（オーディエンス制限）：SAMLアサーションに含まれる値で、そのアサーションが対象とする人物（*限定可能*）を指定します（ [audience（オーディエンス）]はサービスプロバイダであり、通常はURLですが、技術的には任意の文字列のデータとしてフォーマットすることができます。

この値がSPから提供されない場合は、ACSを使用します。

Default Relay State（デフォルトリレーの状態）：SAMLによる認証が成功した後にユーザーが移動するURL。

エンドポイント：サービスプロバイダとIDプロバイダが互いに通信する際に使用されるURL。

Entity ID（エンティティID）：IDプロバイダまたはサービスプロバイダのグローバルに固有な名前。 固有のOkta Entity IDはアプリケーションごとに生成され、Oktaアプリケーションの設定手順で**Identity Provider Issuer（IDプロバイダの発行者）**と呼ばれています。

Identity Provider（IDプロバイダ）（IdP）：ユーザーのIDと要求されたリソースへのアクセスを検証し、アサートする機関（サービスプロバイダ）。

Metadata（メタデータ）：IdPがSPに提供する、および/またはその逆方向に提供するxmlフォーマットの一連の情報。

- SPのメタデータは、ACS、オーディエンス制限、名前IDフォーマット、およびアーサーションを暗号化する必要がある場合にx.509証明書を提供します。 この場合、SPが提供するメタデータファイルをOktaにインポートすることはできません。
- IdPのメタデータは、シングルサインオンURL、Entity（エンティティ）ID、およびSPがアサーションを復号するために必要とするx.509証明書ファイルを提供します。

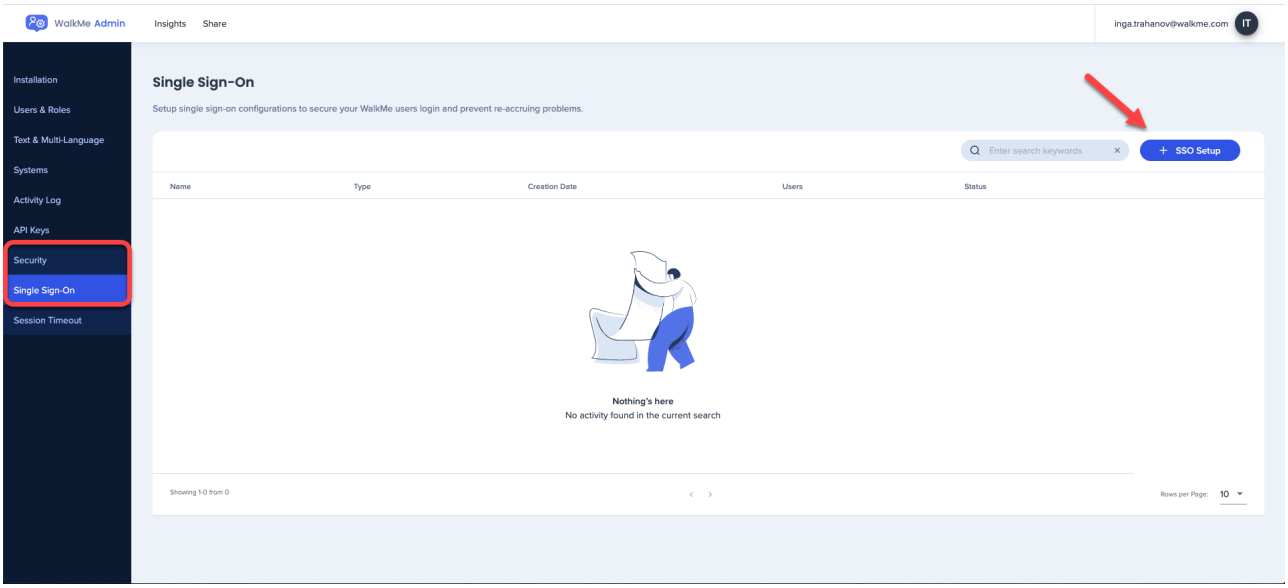
NameID（名前ID）：ユーザーネームを指定するために使用されるアサーション内の属性

Service Provider（サービスプロバイダ）（SP）：Box、Workday、Salesforce、カスタムアプリケーションなど、ユーザーがアクセスしようとするホストリソースまたはサービス。

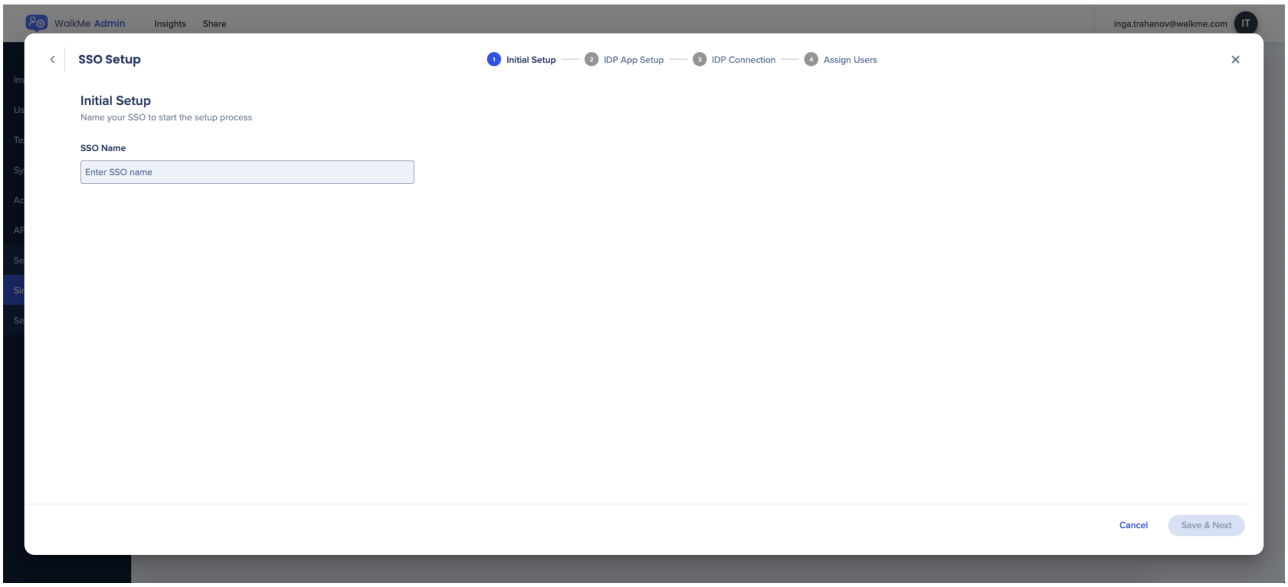
シングルサインオンURL：SAMLトランザクションを処理するためのエンドポイント。 Okta SAMLのテンプレートの設定画面では、SSO URLは**サービスプロバイダの**ACSを参照します。

使用方法

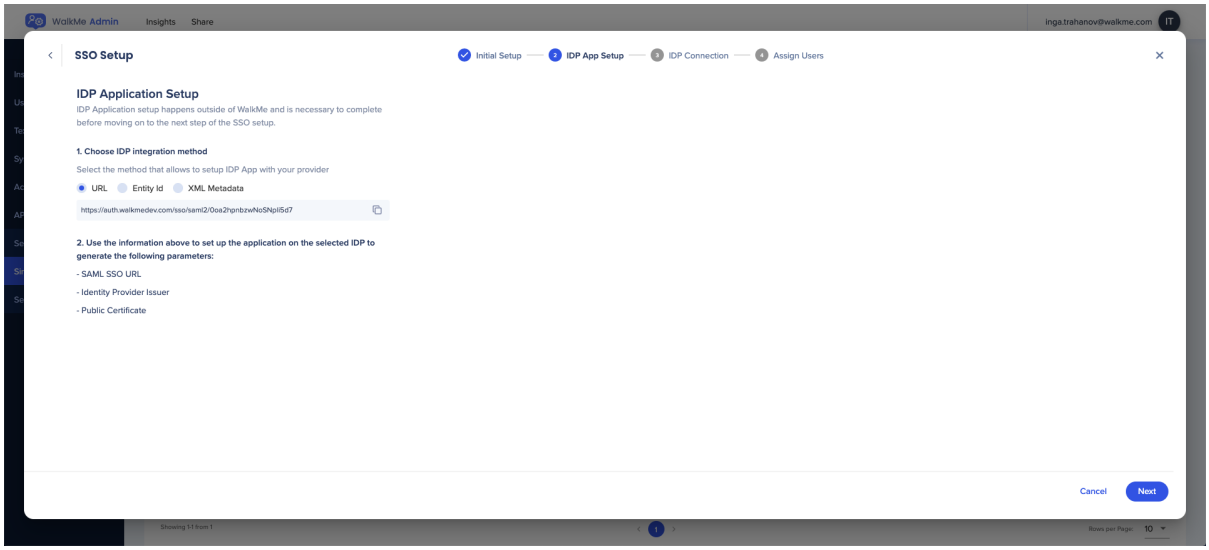
1. admin.walkme.comからAdmin Center（管理センター）を開きます
    1. EUユーザーについては、eu-admin.walkme.comに移動します
2. **セキュリティ**ページに移動し、**シングルサインオンをします**
3. **+ SSOセットアップ**ボタンをクリックします



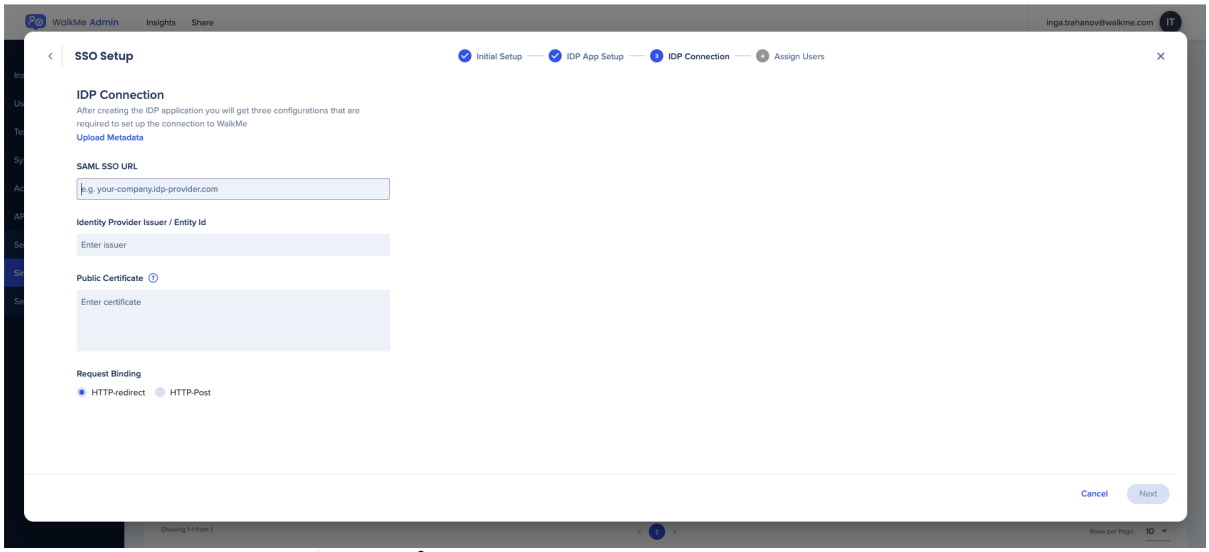
4. SSOの名前を入力します
5. **保存して次へをクリックします**



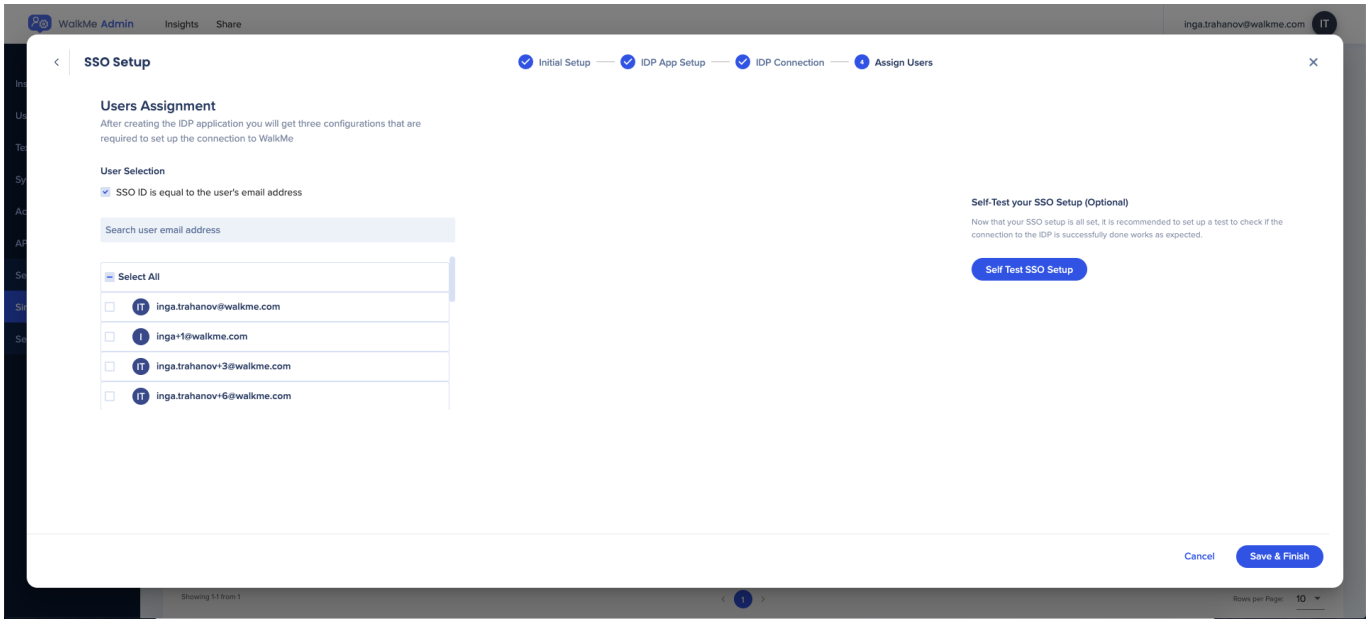
6. IDPの統合方法を選択します：
    - **URLの基になるURLルールは、**
    - **Entity ID（エンティティID）**
    - **XMLメタデータ** – この 方法を選択すると（xmlをファイルとしてダウンロードすることができます



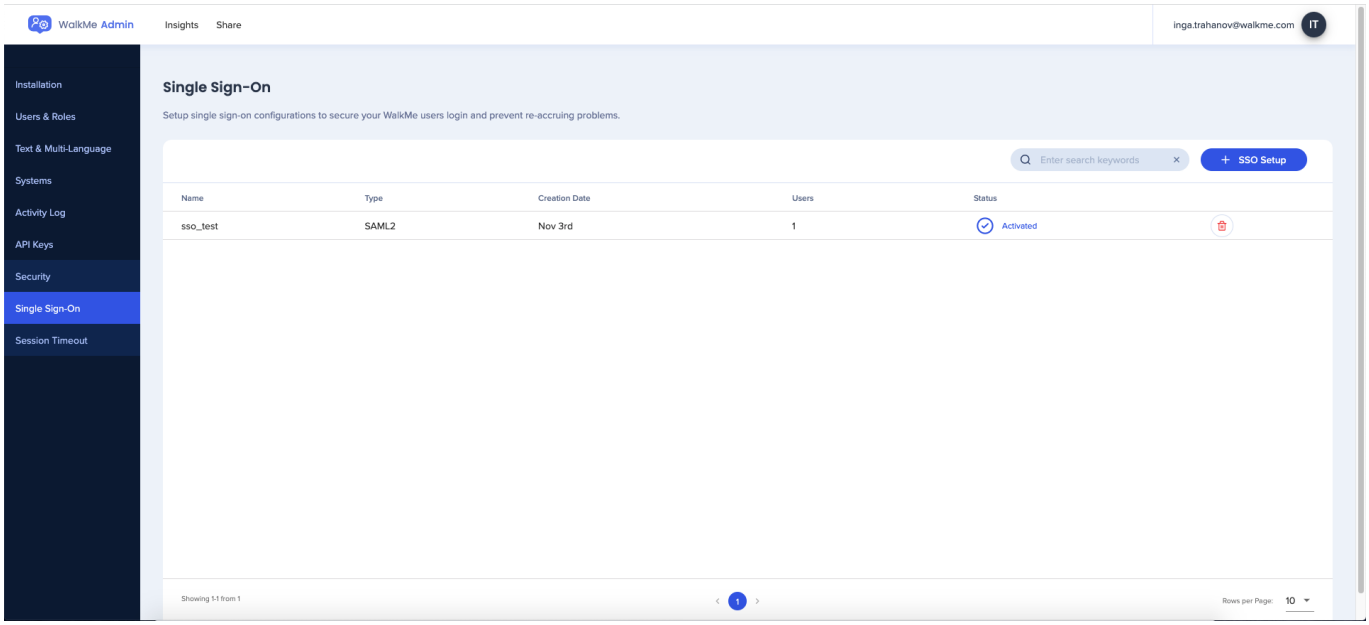
7. 必要な情報を入力して、SSOの設定を完了します：
   - **SAML SSOのURL**
   - **Identity Provider Issuer（IDプロバイダの発行者）/Entity ID（エンティティID）**
   - **公開証明書**
8. 関連するリクエストバインディングを選択します
   - **HTTPリダイレクト**
   - **HTTPポート**



   - **ヒント： メタデータをアップロード**をクリックして、関連するすべてのフィールドを自動的に入力します
9. SSOに割り当てるユーザーを選択します
   - 特定のユーザーを検索およびアサインするか、**すべてを選択**できます
   - デフォルトのSSO IDはメールアドレスですが、必要に応じて変更することができます
   - **テストSSOのセットアップ**ボタンを使用して、SSOのセットアップを確認します
10. **保存して終了**をクリックします。



SSO接続が正常に追加されたら、管理センターの［Single Sign-On（シングルサインオン）］ページで確認することができます。



Azure ADのSSOを設定する方法の詳細については、次の記事を参照してください：[Microsoftチュートリアル]

SSO証明書

注：

- WalkMeは、ID管理のグローバルリーダーであるOktaによって提供される新しいSSOソリューションに移行し、より高い可用性、パフォーマンス、および優れた監視とロギング機能を提供します。
- アカウントが現在WalkMeのレガシSSOで登録されている場合は、シングルサインオンの組織内部の管理者（通常はIDおよびアクセス管理またはITチームです）に連絡し、以下のプロセスに従ってもらってください。
- 管理者は、SSOを設定するために入力が必要な情報について理解することになります。

1. 上記の手順に従って、新しいSSO接続を作成します
2. 3番目のステップでは、新しい証明書をアップロードし、セットアップを完了する必要があります
3. 新しいSSO接続が作成されると、古いSSOを使用しているすべての関連するリンクは、セットアップで作成された新しいリンクに変更する必要があります

SSOのトラブルシューティング

SAMLエラーの原因は何ですか？

SAMLエラーは通常SAML設定中に入力された情報が欠落したか、または不正確な場合に発生します。これらの問題のほとんどはIDP設定から解決することができますが、一部の問題はWalkMeでSSO設定を同様に更新する必要があります。

SAMLエラーメッセージ

エラーメッセージ	修正方法
SAMLレスポンスには、正しいIdentity Provider IssuerIDプロバイダの発行者）が含まれていません [IDP]設定の発行者URLが、以下のIdentity Provider IssuerIDプロバイダの発行者）と一致していることを確認してください。	IDP設定を確認して、管理センターのSSO設定に適切な値がコピーされていることを確認します.IDPのイシュアー値は通常、 **発行者のURL** または **エンティティURL/IDと呼ばれます**
SAMLレスポンスは署名されていません IDP設定をご確認ください。	有効化 **[signing responses署名付き応答）]** を有効化してください。これらのオプションが表示されない場合は、IDPに連絡してください。

SAMLレスポンスに正しいオーディエンスが含まれていません。[IDP]設定のService Provider（サービスプロバイダ）のURLが、以下の高度なオプションのService Provider Issuer（サービスプロバイダの発行者）と一致していることを確認してください。	Service Provider Issuer（サービスプロバイダの発行者）が **IDP設定** の **オーディエンス** を有効化してください。 The **オーディエンス** は、 **SPエンティティID** または **Relying Party Identifier**（証明書利用者の識別子）と呼ばれることもあります。
SAMLレスポンスのアサーションが署名されていません。（IDP）設定をご確認ください。	有効化**レスポンスのサインアサーション** を有効化してください。 これらのオプションが表示されない場合は、IDPに連絡してください。
SAMLレスポンスには、https://auth.walkme.com/sso/saml2 のような正しい送信先が含まれていません。. （IDP）設定をご確認ください。	IDPで**送信先**を更新します。 値の名前は変わる場合がありますが、通常は以下のうちの1つです：Reply URL、ACS URL、Assertion Consumer Service URL、Trusted URL、またはEndpoint URL
SAMLレスポンスにはID属性がありません。 （IDP）設定をご確認ください。	**NameID**（名前ID）が、IDPで送信されたクレームとして正しい（永続的な）フォーマットであることを確認してください。
SAMLレスポンスとSAMLレスポンスのアサーションのどちらも署名されていません。 （IDP）設定をご確認ください。	IDPの設定から、**レスポンス**、**レスポンスのアサーション**、またはその両方の署名を有効にします。 これらのオプションが表示されない場合は、IDPに連絡してください。
SAMLレスポンスは署名されていません（しかし、EncryptedId で署名と暗号化されたアサーションが存在します。 Apologies（アポロジー）ですが、WalkMeはこのフォーマットをサポートしていません。 （IDP）設定をご確認ください。	このフォーマットをサポートしていません。 **レスポンスへの署名**を有効にして、SSOを正しく設定するためのガイドラインに従っていることを確認してください。
SAMLレスポンスがバージョン2.0ではありません。 （IDP）設定をご確認ください。	IDPで**SAML 2.0**を使用していることを確認します。
署名の検証に失敗したようです。 [IDP]設定で、署名証明書を確認してください。	管理センターのSSO設定で**証明書**を更新して、IDPから送信された証明書と照合します。