

IDP Integration

Aperçu général

Les fournisseurs d'identité stockent et gèrent les identités numériques, offrant aux entreprises un moyen de gérer l'accès et les privilèges, tout en maintenant des normes de sécurité élevées.

L'intégration IDP peut être utilisée pour récupérer ces informations, valider l'identité des utilisateurs finaux, enrichir les capacités de segmentation du contenu et étendre la surveillance du comportement des utilisateurs. Cette fonctionnalité fournit un identifiant utilisateur fiable et sécurisé sur n'importe quel système sans avoir besoin de définir l'identifiant utilisateur unique pour chaque système avec des variables différentes.

L'utilisation d'IDP comme identifiant d'utilisateur devrait être la solution de prédilection pour tous les nouveaux systèmes.

Les intégrations IDP sont accessibles depuis le [centre d'administration](#) sur admin.walkme.com .

▣ Institut d'adoption numérique

- Consultez la leçon [Configurer Analytics, Integrations and Design](#) du cours *Fondements de gestion de projet pour l'adoption numérique* .
- Vous n'avez pas encore de compte DAI ? [Inscrivez-vous ici](#)

Cas d'utilisation

- L'authentification IDP de l'utilisateur final est un prérequis pour présenter le contenu WalkMe.
- Étendre les capacités de segmentation du contenu par les paramètres IDP (par exemple, les groupes, la région, le service, etc.).
- Surveillance précise des données sur l'ensemble des systèmes.

Plateformes prises en charge

L'intégration IDP de WalkMe prend en charge l'utilisation de plusieurs protocoles d'authentification, notamment **OAuth 2.0**, **OpenID Connect** et **SAML**, afin d'authentifier les utilisateurs auprès de leur fournisseur IDP organisationnel et d'obtenir des attributs utilisateur pouvant être utilisés ultérieurement pour la segmentation et l'analyse dans WalkMe. Chaque fournisseur IDP qui prend en charge ces protocoles doit fonctionner avec WalkMe. WalkMe prend en charge le flux initié par SP.

Qu'est-ce qu'OAuth 2.0 ?

OAuth 2.0, qui représente « Open Authorization » (ouvrir l'autorisation), est une norme conçue pour permettre à un site ou une application d'accéder aux Ressources hébergées par d'autres applications Web au nom d'un utilisateur. OAuth 2.0 est le protocole d'autorisation standard de l'industrie.

Qu'est-ce qu'OpenID Connect ?

OpenID Connect est une simple couche d'identité au-dessus du protocole OAuth 2.0, qui permet aux clients informatiques de vérifier l'identité d'un utilisateur final sur la base de l'authentification effectuée par un serveur d'autorisation, ainsi que d'obtenir des informations de profil de base sur l'utilisateur final dans une manière interopérable et de type REST.

L'intégration IDP prend actuellement en charge les fournisseurs suivants :

- **Okta**
- **G-Suite**
- **ADFS**
- **AzureAD**
- **PingID**
- Fournisseurs d'identités qui utilisent **OpenID**

Outre OpenID Connect, le protocole d'authentification le plus courant est SAML. Pour obtenir des instructions sur la création et la configuration d'une intégration à l'aide de SAML, veuillez vous reporter à notre [article sur l'intégration IDP SAML](#).

Prérequis

Une application IDP doit être créée pour servir de pont entre l'IDP et le Centre d'intégration WalkMe.

Un guide d'instructions est disponible dans l'écran de configuration du Centre d'administration pour tous les systèmes pris en charge.

Select Protocol

OAUTH 2.0 SAML 2.0

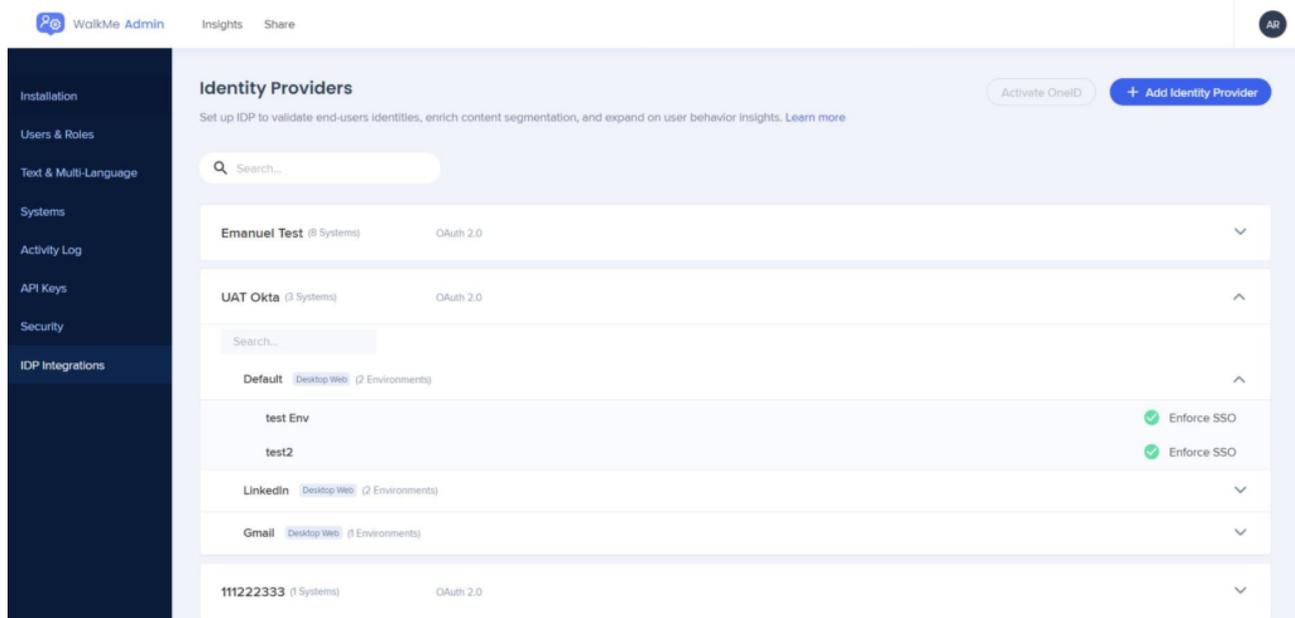
Select Vendor

Okta

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

Ajouter un fournisseur d'identité

1. Dans l'onglet Intégrations IDP du Centre d'administration, cliquez sur le bouton « + Ajouter un fournisseur d'identité »

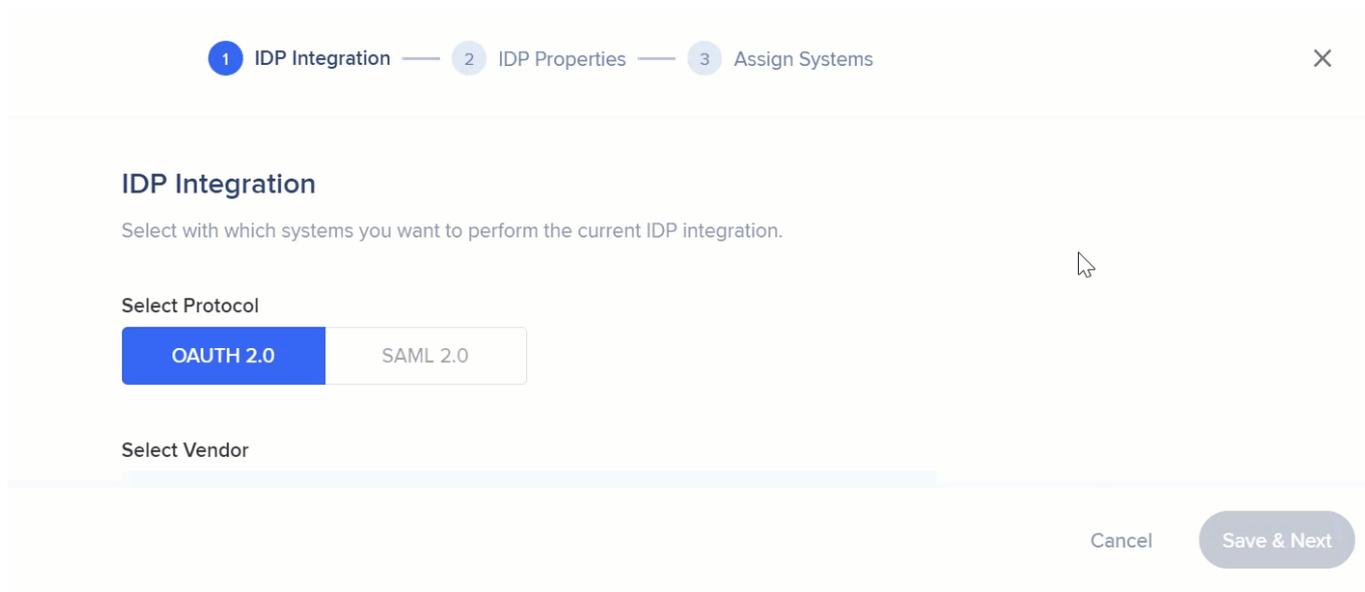


2. Sélectionnez le type de protocole OAuth 2.0

3. Fournissez les paramètres de configuration appropriés pour la connexion

1. **Fournisseur IDP** : sélectionnez un fournisseur à partir de la liste
2. **Nom de l'IDP** - Nom de la connexion
3. **ID client** - Identifiant public des applications
4. **Secret client** - Secret connu uniquement de l'application et du serveur d'autorisation

5. **Domaine du fournisseur IDP** : domaine de votre organisation



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

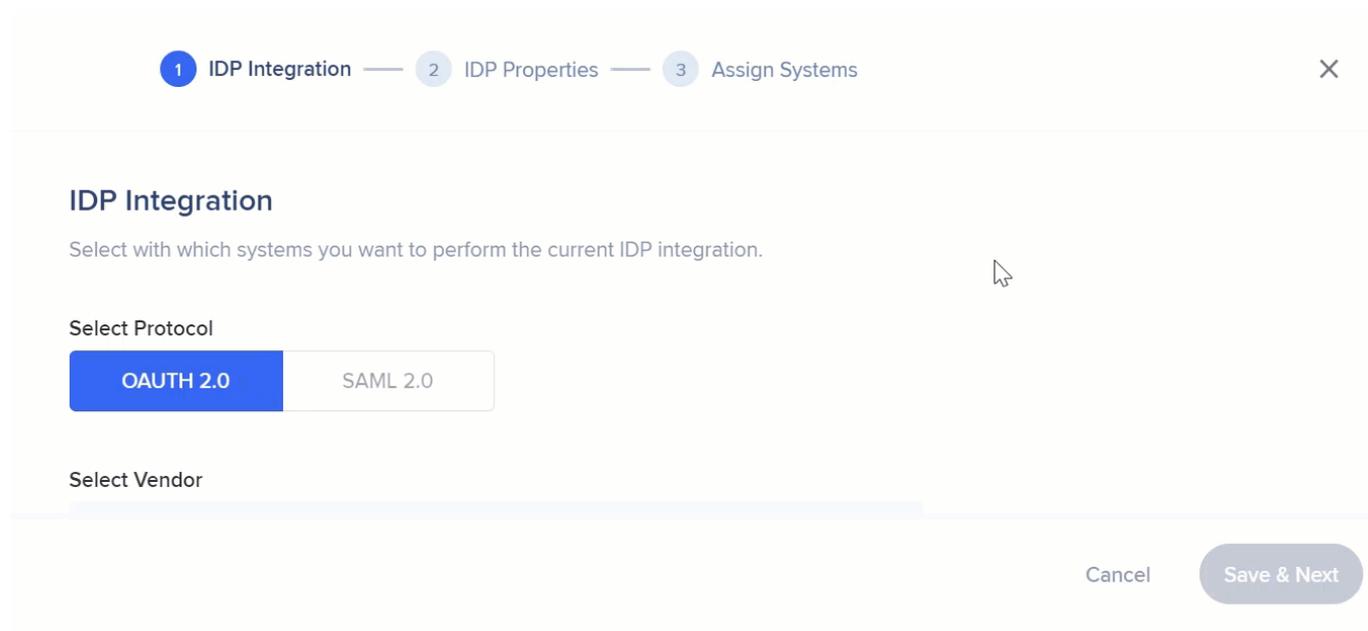
Select Vendor

Cancel Save & Next

Remarque : les champs peuvent varier en fonction du fournisseur IDP sélectionné.

- **Pour OpenID Connect :**

1. **Fournisseur IDP** : sélectionnez OpenID Connect à partir de la liste des fournisseurs Oauth2.0
2. **Nom de l'IDP** - Nom de la connexion
3. **ID client** - Identifiant public des applications
4. **Secret client** - Secret connu uniquement de l'application et du serveur d'autorisation
5. **URL de découverte du fournisseur IDP**
6. **Portée du fournisseur IDP**
7. **Politique de sécurité du contenu**
8. **Votre fournisseur IDP**
9. **Utiliser le jeton d'identification pour obtenir les propriétés des utilisateurs finaux** - Cochez le bouton bascule pour l'activer



4. Cliquez sur « Enregistrer et suivant » une fois prêt

- Notez que nous n'exigeons **pas** d'URL de déconnexion

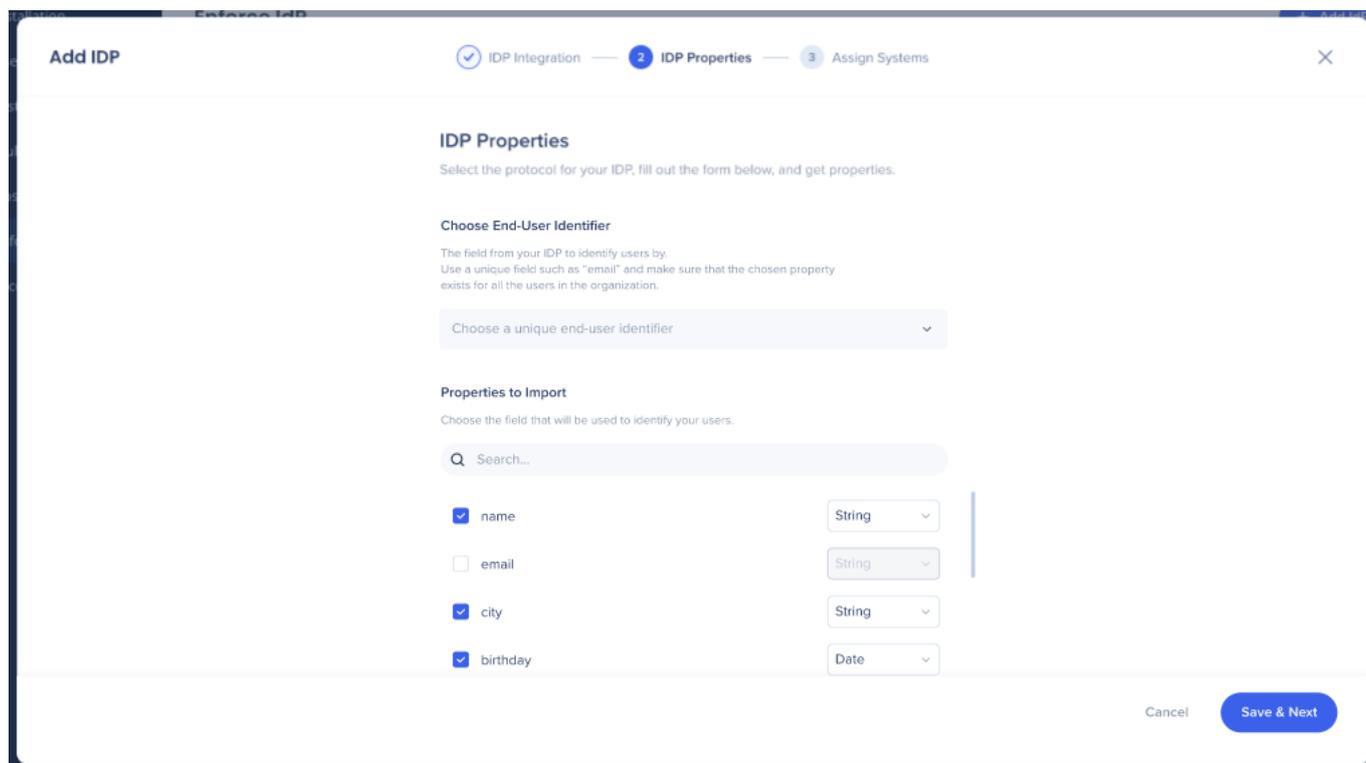
5. Choisissez un identifiant d'utilisateur final unique pour identifier les utilisateurs

- Vous n'avez besoin que d'un seul identificateur ; nous n'avons ni besoin d'informations supplémentaires sur le groupe ni d'autres attributs

6. Sélectionnez les propriétés souhaitées et assurez-vous que le type de données correct a été choisi :

1. Chaîne
2. Numéro
3. Date

Remarque : le champ d'identificateur d'utilisateur sera toujours converti en type chaîne.



Add IDP 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.

Search...

<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

Conseil :

- Pour vous assurer que le type de données sélectionné convient, vous pouvez passer la souris sur l'icône « i » et vérifier la valeur de cette propriété.
- Si le type de données sélectionné ne convient pas pour la propriété, une icône « ! » orange apparaîtra pour recommander de revenir au type de données identifiés.

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

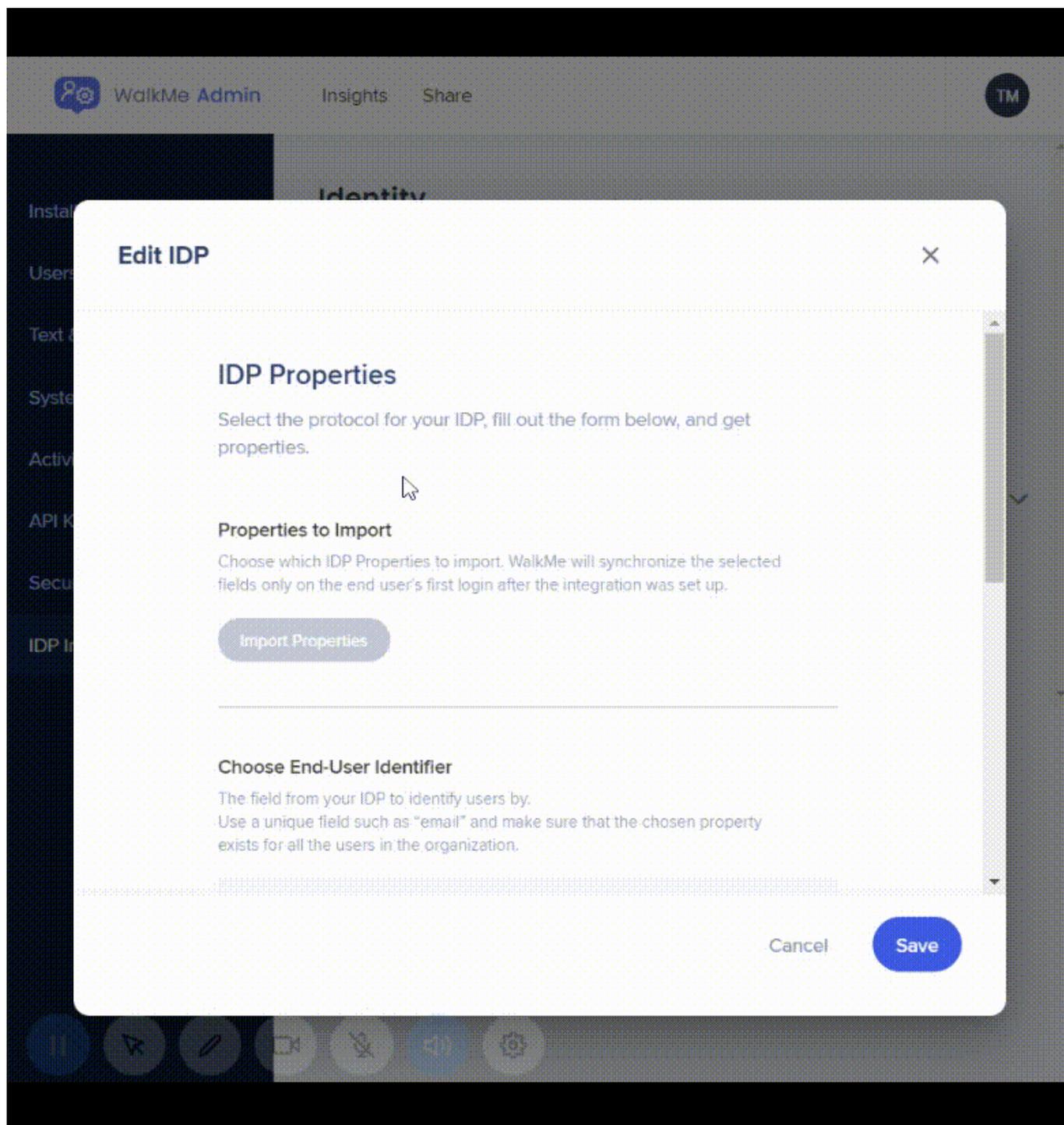
Choose the field that will be used to identify your users.

Q Search...

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

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

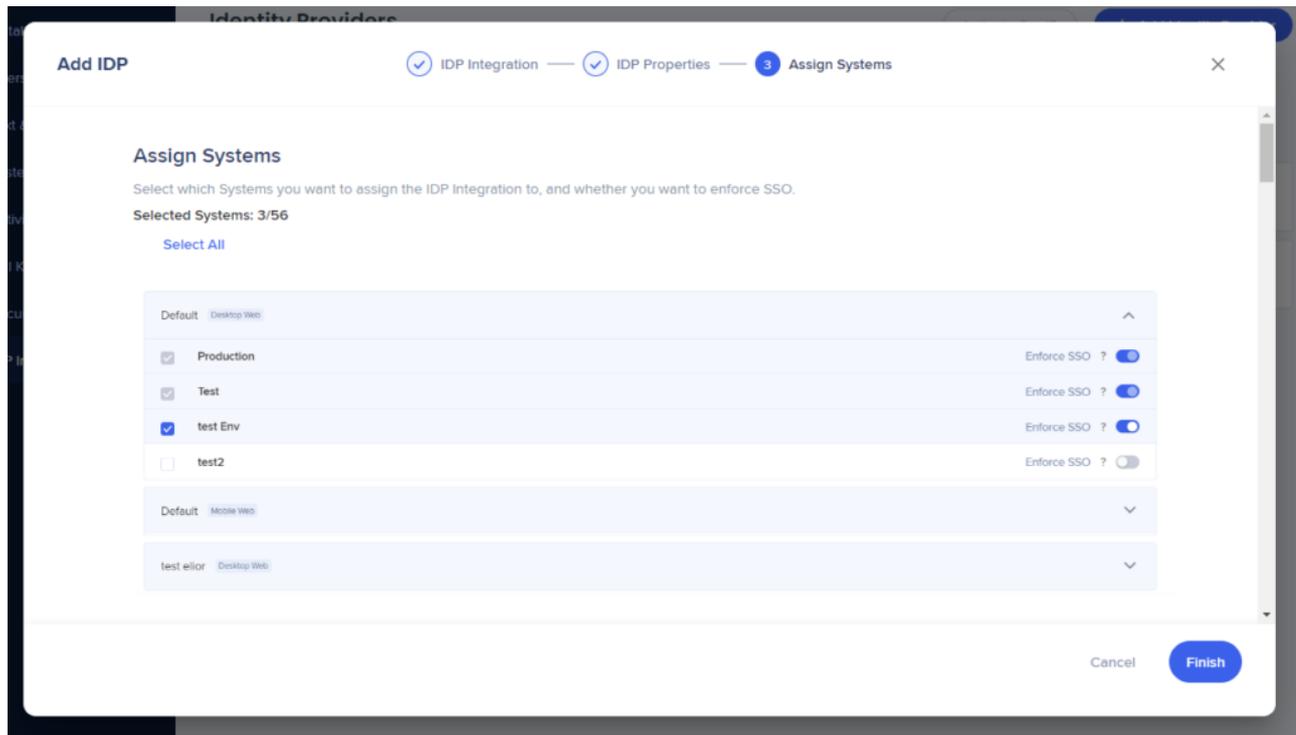
Vous pouvez également renommer toute propriété sélectionnée, afficher sa valeur et son nom d'origine et retourner à sa valeur d'origine si elle est remplacée.



7. Sélectionnez les systèmes auxquels vous souhaitez affecter l'intégration IDP

- Pour chaque système, vous pouvez activer séparément l'intégration IDP sur les environnements souhaités

8. Utilisez le bouton bascule pour appliquer la SSO



Remarque :

- IDP doit fournir l'identification d'utilisateur la plus précise, mais les chiffres peuvent ne pas être exacts lorsque Enforce SSO est désactivé.
- Lorsque l'application SSO est désactivée, les utilisateurs peuvent utiliser des applications sans s'authentifier auprès de leur fournisseur IDP, et un identifiant WalkMe sera généré et utilisé comme identifiant utilisateur.
- Les utilisateurs peuvent « ignorer » l'authentification IDP soit en utilisant des applications qui ne nécessitent aucune authentification, soit en se connectant directement à l'application via utilisateur/mot de passe, sans passer par le flux de connexion IDP.

9. Cliquez sur « Finish » (finir).

10. Un message apparaîtra vous indiquant si votre IDP a été ajouté avec succès ou pas



Remarque :

- Après l'attribution des systèmes, le **paramètre UUID** des systèmes attribués est automatiquement défini sur IDP et les paramètres sont publiés de sorte qu'aucune autre action n'est requise.
- La seule façon de modifier l'UUID est de désaffecter le système du fournisseur (voir la section « **Gérer l'affectation du système** » ci-dessous).
- Vous pouvez désormais segmenter le contenu à l'aide des attributs importés dans Insights et dans l'éditeur sous Attributs utilisateur > IDP avec les conditions de filtrage appropriées en fonction du type de champ de données défini.
- [Pour en savoir plus, cliquez ici.](#)

Segmentation ⓘ
Create a rule to define this Segment

Group Import Rules

<input type="checkbox"/>	Ua User Attributes	IDP	zoneinfo	Is	USA	<input type="checkbox"/>	?
--------------------------	--------------------	-----	----------	----	-----	--------------------------	---

And ↔

<input type="checkbox"/>	Select a Type					<input type="checkbox"/>	
--------------------------	---------------	--	--	--	--	--------------------------	--

Current Statement: Cannot Assert

Conseil :

- Pour valider l'identification des utilisateurs par l'intégration et que tous les attributs

demandés sont collectés, il est recommandé de consulter la page des utilisateurs dans [Insights](https://insights.walkme.com) à insights.walkme.com, où toutes les données utilisateur sont affichées.

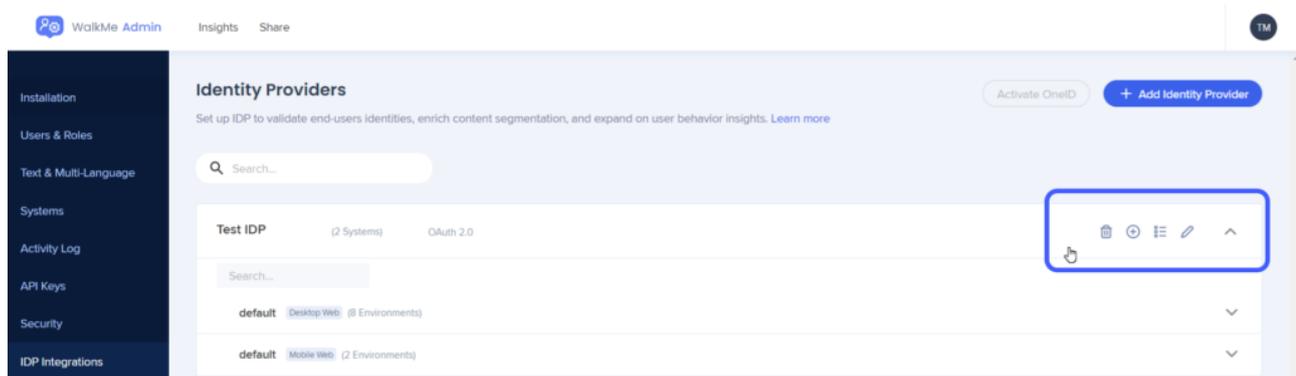
- Les utilisateurs sont ajoutés au tableau uniquement après la fin de la session. L'ajout des utilisateurs prendra donc un peu de temps après la configuration IDP.

User	First Seen	Last Seen	Avg. Time btwn Sessions	Avg. Session Duration	Total Sessions	Clicked Action (NewTeamNotClicked)	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	Amato
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. 27, 2020	4 hours ago Nov. 10, 2020	5 hours	3 hours	1148	-	Hale

Gestion d'un fournisseur d'identité

En survolant la ligne d'un fournisseur d'identité, plusieurs options s'offrent à vous :

- Supprimer
- Gérer l'affectation du système
- Importer des propriétés
- Modifier
- Développer

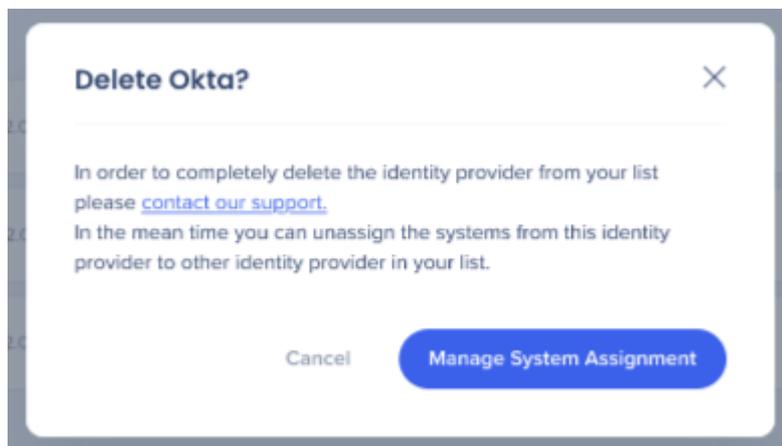


Supprimer

- Cliquez sur l'icône de la corbeille pour « supprimer » un fournisseur d'identité.

Remarque importante :

- Il n'est pas possible de supprimer complètement un fournisseur d'identité sans contacter le support.
- Avant que la suppression ne soit possible, le fournisseur d'identité doit être désaffecté à tous les systèmes à l'aide de l'écran Gérer l'affectation du système.



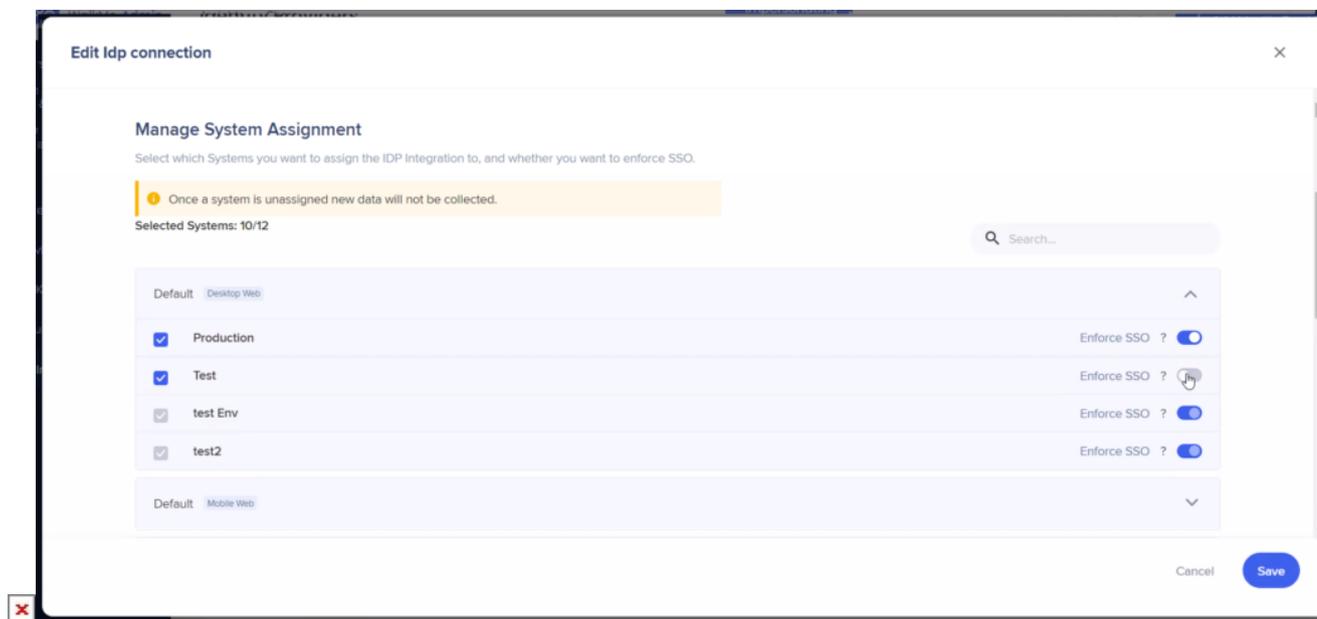
Gérer l'affectation du système

- Cliquez sur l'icône « + » pour ouvrir l'écran de gestion de l'affectation du système.
- Sélectionnez ou désélectionnez les systèmes que vous souhaitez affecter au fournisseur d'identité
- Vous pouvez également utiliser la bascule pour appliquer la SSO
- Cliquez sur le bouton « Save Changes » (enregistrer les changements) une fois que vous avez fini

Remarque :

- Les utilisateurs ne peuvent pas gérer l'affectation du système pour les fournisseurs qui n'ont pas de propriétés importées. Les propriétés devront d'abord être importées.
- Après l'attribution des systèmes, le **paramètre UUID** des systèmes attribués est

automatiquement défini sur IDP et les paramètres sont publiés de sorte qu'aucune autre action n'est requise.



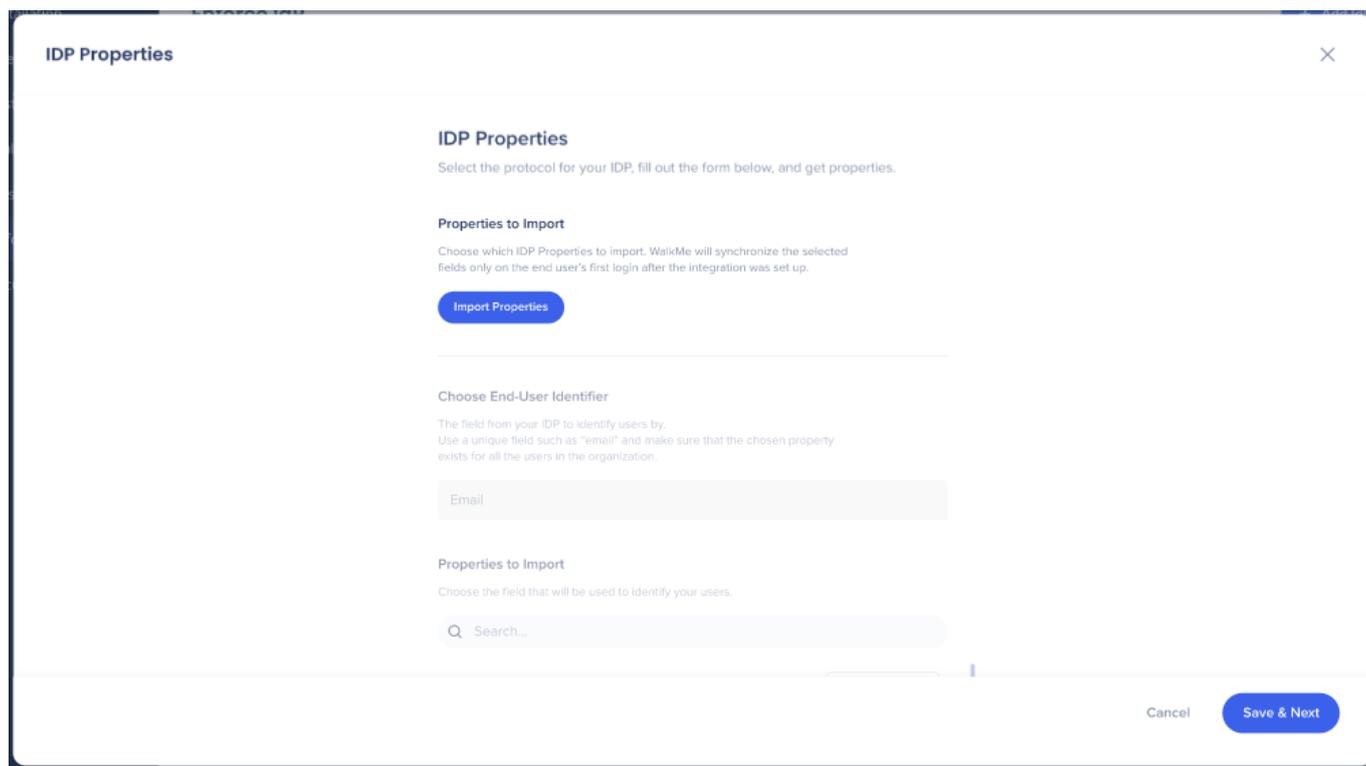
Importer des propriétés

- Cliquez sur l'icône de la liste et puis sur le bouton « Import Properties » (importer les propriétés) pour modifier ou ajouter des propriétés importées supplémentaires

Ces attributs seront utilisés pour la segmentation du contenu et la création de rapports dans Insights.

Remarque :

- Pour ce faire, il est nécessaire de s'authentifier auprès d'un utilisateur affecté à l'application WalkMe du côté du fournisseur.

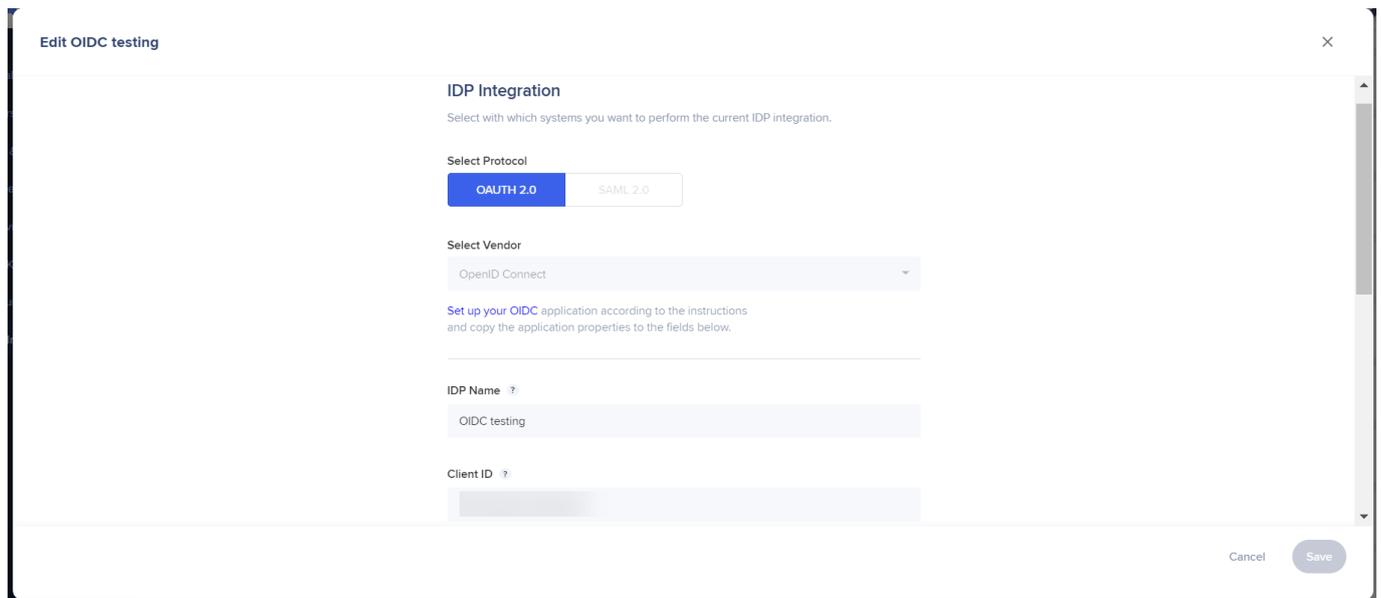


Modifier

- Cliquez sur l'icône en forme de crayon pour modifier les paramètres du fournisseur d'identité
- Vous serez en mesure de modifier tous les champs renseignés dans la configuration initiale du fournisseur d'identité

Remarque :

- Les utilisateurs ne peuvent pas gérer l'affectation du système pour les fournisseurs qui n'ont pas de propriétés importées. Les propriétés devront d'abord être importées.



Développer/Réduire la vue

- Utilisez l'icône de la flèche pour ouvrir et réduire la vue élargie
- Une fois développé, vous verrez tous les systèmes attribués à un fournisseur d'identité et si Enforce SSO a été activé ou pas



Les meilleures pratiques

Configuration « Enforce SSO » (Appliquer l'authentification unique)

- Lorsque l'authentification IDP doit être **activée** avant d'ouvrir la page Web à l'utilisateur final, si le jeton IDP n'est pas reconnu, l'utilisateur final sera redirigé vers sa page de connexion IDP.
 - Chaque fois que l'utilisateur final ne parvient pas à s'authentifier auprès de l'IDP pour des raisons diverses telles que l'IDP était en panne, le client a oublié les informations d'identification ou l'utilisateur final n'a pas été affecté à l'application de l'IDP, l'authentification unique sera désactivée pendant 1 heure et l'identifiant de l'utilisateur sera automatiquement réduit à la méthode « WalkMe ID » en tant que fallback, ou WalkMe ne se chargera pas, selon la configuration du client.
 - Après 1 heure - si le jeton IDP n'est toujours pas reconnu, l'utilisateur final sera à nouveau redirigé vers sa page de connexion IDP, sinon, la connexion à l'IDP ne sera pas nécessaire. Il est important de s'assurer que cela est absolument clair pour le client. Sinon, N'activez PAS cette option.
- Lorsque **désactivé** - L'authentification IDP est tentée lors du chargement de la page, mais s'il n'y a pas de jeton actif pour IDP, l'utilisateur final ne sera pas redirigé vers IDP. L'identifiant

de l'utilisateur sera automatiquement réduit à la méthode « ID WalkMe » ou WalkMe ne se chargera pas, selon la configuration du client.

Limites

Important : veuillez noter que si votre implémentation est déjà en vigueur, la modification de l'identificateur d'utilisateur affecte la manière dont WalkMe identifie les utilisateurs finaux. Cela pourrait entraîner la réinitialisation des règles de lecture automatique (c'est-à-dire les paramètres de lecture unique) ou les utilisateurs voient leurs tâches d'intégration précédemment terminées marquées comme inachevées, en raison de la modification de leur identifiant utilisateur unique (UUID). Il n'y a aucun moyen de contourner cette limite, car chaque utilisateur est reconnu comme un nouvel utilisateur, lié à sa nouvelle valeur D'UUID.

- L'extension du navigateur Safari n'est pas prise en charge par IDP
- La modification de l'identificateur d'utilisateur affecte la manière dont WalkMe identifie les utilisateurs finaux et peut réinitialiser les configurations « Play once » (lecture unique)
- L'utilisateur doit avoir des autorisations d'administrateur pour le centre d'administration
- IDP doit être configuré sur le système requis
- Les utilisateurs finaux doivent utiliser IDP pour s'authentifier auprès de ce système
- Si votre entreprise a CSP (Content Security Policy ou Politique de sécurité du contenu), elle bloquera les appels vers le fournisseur IDP
 - Afin de surmonter cela, la bonne URL doit être ajoutée dans les paramètres CSP de la configuration de l'extension
- Après l'attribution des systèmes, le **paramètre UUID** des systèmes attribués est automatiquement défini sur IDP et les paramètres sont publiés de sorte qu'aucune autre action n'est requise
 - Pour que les modifications de l'IDP prennent effet, les systèmes du client doivent être mis à jour vers la dernière version de WalkMe (cela peut être réalisé en publiant les paramètres)
 - Pour les comptes d'entreprise, vous devez cocher « Mettre à jour vers la dernière version de WalkMe » lors de la publication
- Lors de l'importation d'une propriété de type de date, seuls les formats suivants sont pris en charge :
 - 2018-02-20
 - 2018-02-20T14:32:00
 - 12/30/2018
 - L'importation d'une chaîne ou d'un nombre en tant que date ne fonctionnera pas dans la segmentation du filtrage/de l'Éditeur d'Insights

Mobile Web :

- Mobile Web sera automatiquement activé une fois que la configuration IDP est terminée.
- Si Mobile Web est ajouté après IDP / OneID a déjà été activé, les utilisateurs devront désactiver puis réactiver IDP pour la prise en charge de Mobile Web

Résolution des problèmes communs

L'utilisateur n'est pas assigné

Pour empêcher que cela se produise, tous les employés doivent être assignés à WalkMe. La personne du département informatique de votre entreprise devrait être en mesure de vous aider avec cela en modifiant le paramètre d'accès à l'**application WalkMe** dans votre fournisseur IDP pour tous les employés.

EUID n'a pas été trouvé dans le profil de l'utilisateur

Pour remédier à cela, vous pouvez soit sélectionner un EUID différent, qui est disponible pour tous les employés affectés à WalkMe, ou vous pouvez individuellement ajouter les informations manquantes aux utilisateurs concernés.

Client **expiré** / Clés secrètes **expirées**

Si la clé est expirée, vous devrez la recréer et ensuite mettre à jour les nouvelles clés dans la connexion IDP concernée dans la page **Intégrations** IDP dans le Centre d'administration WalkMe.

Client **invalide** / Clés secrètes **invalides**

Assurez-vous que vous avez copié les clés correctes et ensuite, collez-les dans la connexion IDP concernée dans la page **Intégrations** IDP dans le Centre d'administration WalkMe.