Intégration IDP avec SAML

Aperçu général

L'intégration IDP de WalkMe peut utiliser un protocole d'authentification appelé SAML pour authentifier les utilisateurs avec leur fournisseur organisationnel d'IDP et pour obtenir des attributs d'utilisateur qui peuvent être utilisés pour la segmentation et les analyses dans WalkMe. Chaque fournisseur d'IDP qui prend en charge le SAML doit fonctionner avec WalkMe. WalkMe prend en charge le flux initié par SP.

Qu'est-ce que SAML ?

SAML, soit Security Assertion Markup Language (langage de balisage d'assertion de sécurité), est un standard ouvert qui permet aux fournisseurs d'identité (IDP) de transférer les identifiants de l'autorisation aux fournisseurs de services (SP). Cela permet aux clients informatiques de vérifier l'identité d'un utilisateur final en fonction de l'authentification effectuée par un serveur d'autorisation et d'obtenir des informations de profil de base sur l'utilisateur final.

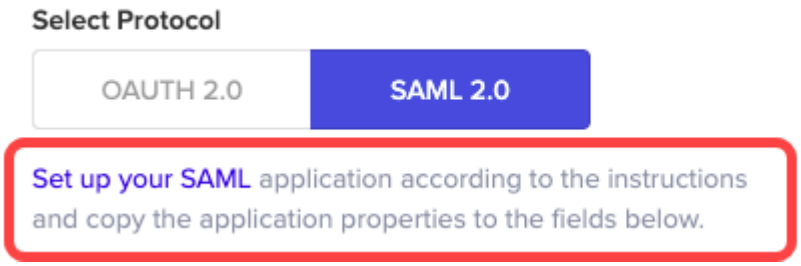
Cas d'utilisation

- 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.

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 le centre d'administration sur l'écran de configuration de l'intégration IDP.



Obtenir des métadonnées et un certificat du fournisseur d'identité

Ces instructions sont génériques. Vous devrez localiser ces informations pour votre fournisseur d'identité spécifique (IdP).

- **URL SSO (Single Sign-On, URL à authentification unique)** : URL envoyée à l'IdP à qui les demandes d'authentification SAML doivent être envoyées. Ce type d'URL se nomme souvent une URL SSO.
- **Certificat de signature X509**: certificat requis par le fournisseur de service pour valider la signature des assertions d'authentification qui ont été signées numériquement par l'IdP. Il doit y avoir un endroit où télécharger le certificat de signature à partir de l'IdP. Si le certificat n'est pas en .pem ou .cer, vous devez le convertir en un de ces formats. plus tard, vous le copierez-collerez sur WalkMe.
  Les méthodes de récupération de ce certificat varient, veuillez donc consulter la documentation de votre IdP si vous avez besoin d'aide supplémentaire.

Remarque :

- Avant de transférer le certificat de signature X.509 sur WalkMe, vous devez convertir le fichier en Base64.
- Pour cela, utilisez un outil en ligne ou exécutez la commande suivante en Bash :
  cat cert.crt | base64.

Ajouter des métadonnées du fournisseur de service WalkMe dans l'IdP

Ajoutez des informations sur le fournisseur de service au fournisseur d'identité pour que l'utilisateur sache comment recevoir et répondre aux demandes d'authentification SAML. Les instructions fournies ici sont génériques. Vous devrez trouver les écrans et les champs appropriés pour le fournisseur d'identité.

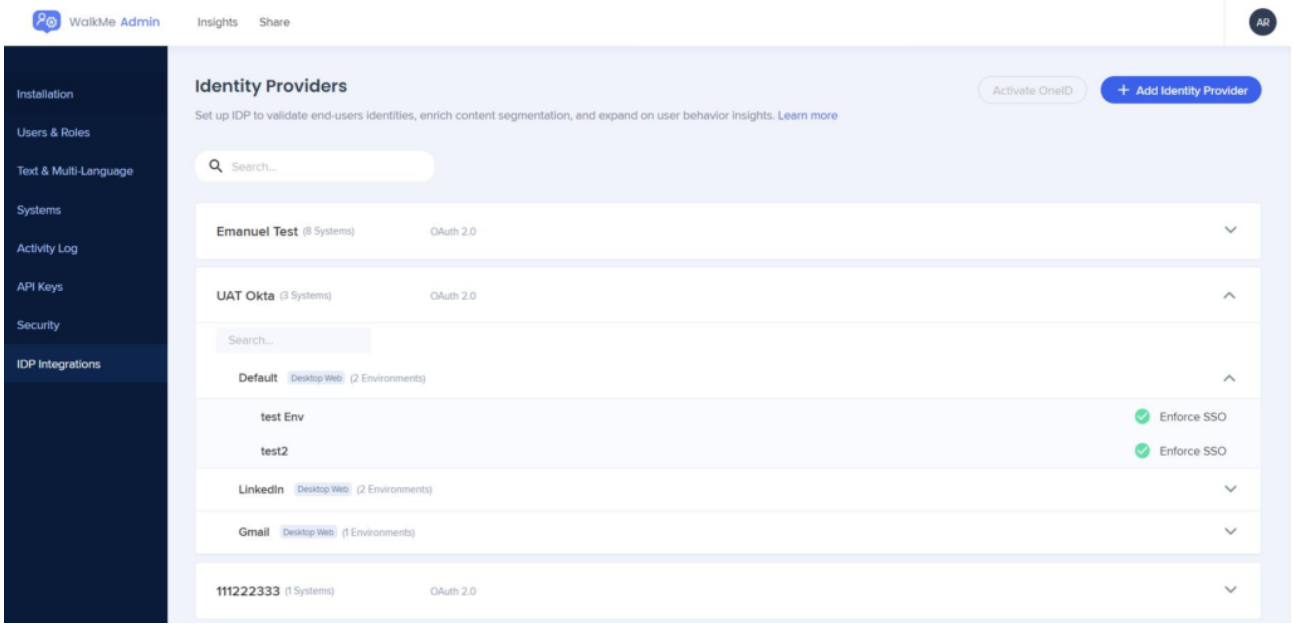
1. Localisez les écrans dans le fournisseur d'identité qui vous permettent de configurer le SAML.

Si l'IdP prend en charge le transfert d'un fichier de métadonnées, vous pouvez simplement fournir le fichier de métadonnées obtenu dans l'étape ci-dessus. Si l'IdP ne prend pas en charge le transfert d'un fichier de métadonnées, vous pouvez le configurer manuellement comme suit.

2. L'IdP devra savoir où envoyer les assertions SAML après avoir authentifié un utilisateur. Voici **l'URL d'Assertion Consumer Service (Service ACS)** dans WalkMe. L'IdP peut l'appeler **Assertion Consumer Service URL** ou **Application Callback URL (URL de rappel)**.
   US : https://papi.walkme.com/ic/idp/p/saml/callback
   EU : https://eu-papi.walkme.com/ic/idp/p/saml/callback
3. Si l'IdP dispose d'un champ nommé **Audience** ou **Entity ID (ID d'entité)** , saisissez-y **l'ID d'entité** de WalkMe :
   US : https://papi.walkme.com
   EU : https://eu-papi.walkme.com
4. Si l'IdP vous propose un choix pour les liens, vous devriez sélectionner **HTTP-Redirect** pour les demandes d'authentification.

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 SAML

3. Fournissez les paramètres de configuration appropriés pour la connexion

Téléchargez le fichier de métadonnées

- Vous pouvez télécharger les informations WalkMe sur votre système à l'aide d'un fichier de métadonnées au lieu de devoir copier et coller chaque élément individuellement

Champs obligatoires :

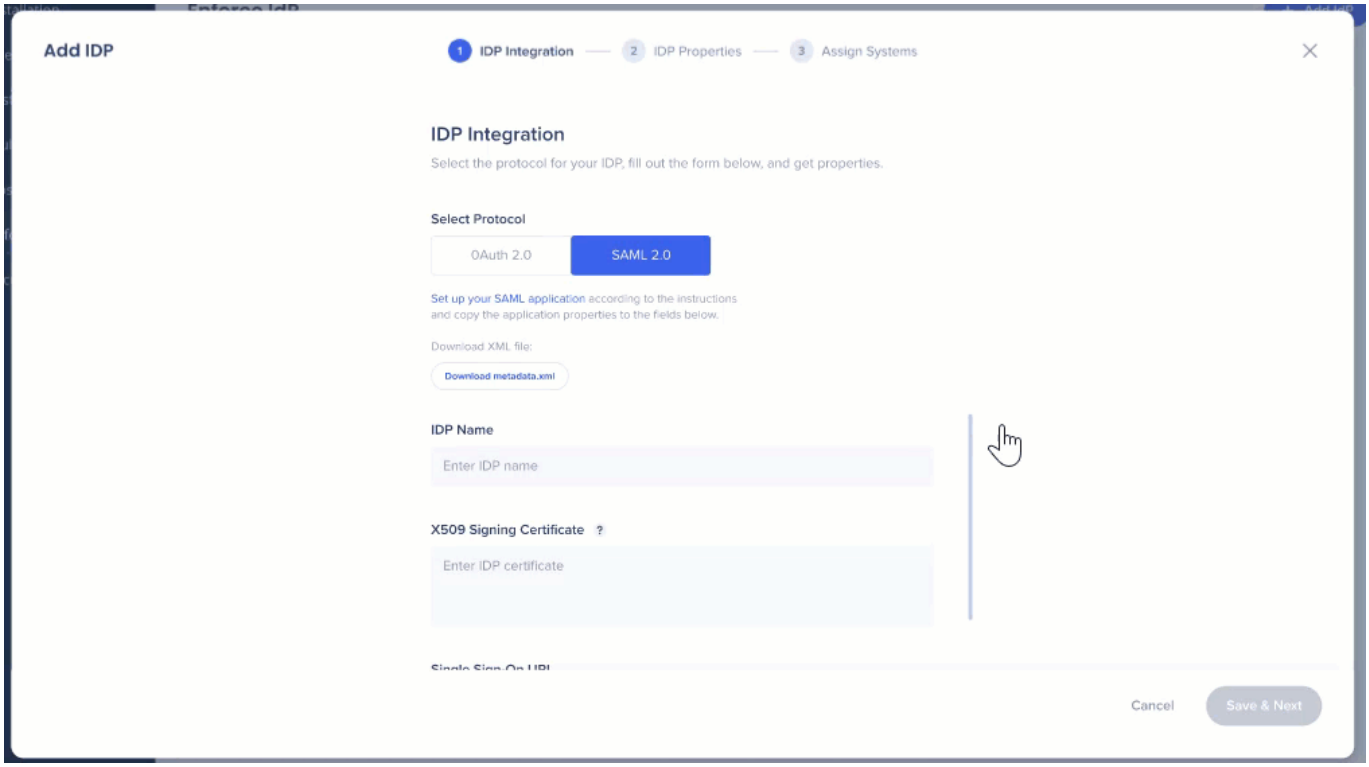
- **Nom de l'IDP** – Nom de la connexion
- **URL à authentification unique** : l'URL à authentification unique du fournisseur d'identité extraite de l'assistant de configuration du fournisseur.
- **Certificat de signature X509** : transférez le certificat que vous avez téléchargé chez votre fournisseur.

Facultatif, paramètres de chiffrement :

Pour accroître la sécurité de vos transactions, vous pouvez signer ou chiffrer vos demandes et vos réponses dans le protocole SAML.

D'abord, nous devons générer et télécharger un certificat qui sera unique pour votre compte.
La clé publique vous sera partagée pour qu'elle soit transférée sur votre fournisseur d'identité.

- **Requête d'authentification :** signez la demande d'authentification SAML à l'aide de la clé privée.
- **Chiffrage d'assertion :** recevez les assertions chiffrées d'un fournisseur d'identité. Pour ce faire, vous devez fournir le certificat de clé public au fournisseur d'identité. Le fournisseur d'identité chiffre l'assertion SAML à l'aide de la clé publique et l'envoie à WalkMe qui la déchiffre à l'aide de la clé privée.



4. Cliquez sur « Save Next » (enregistrer et aller sur la page suivante) une fois prêt.

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

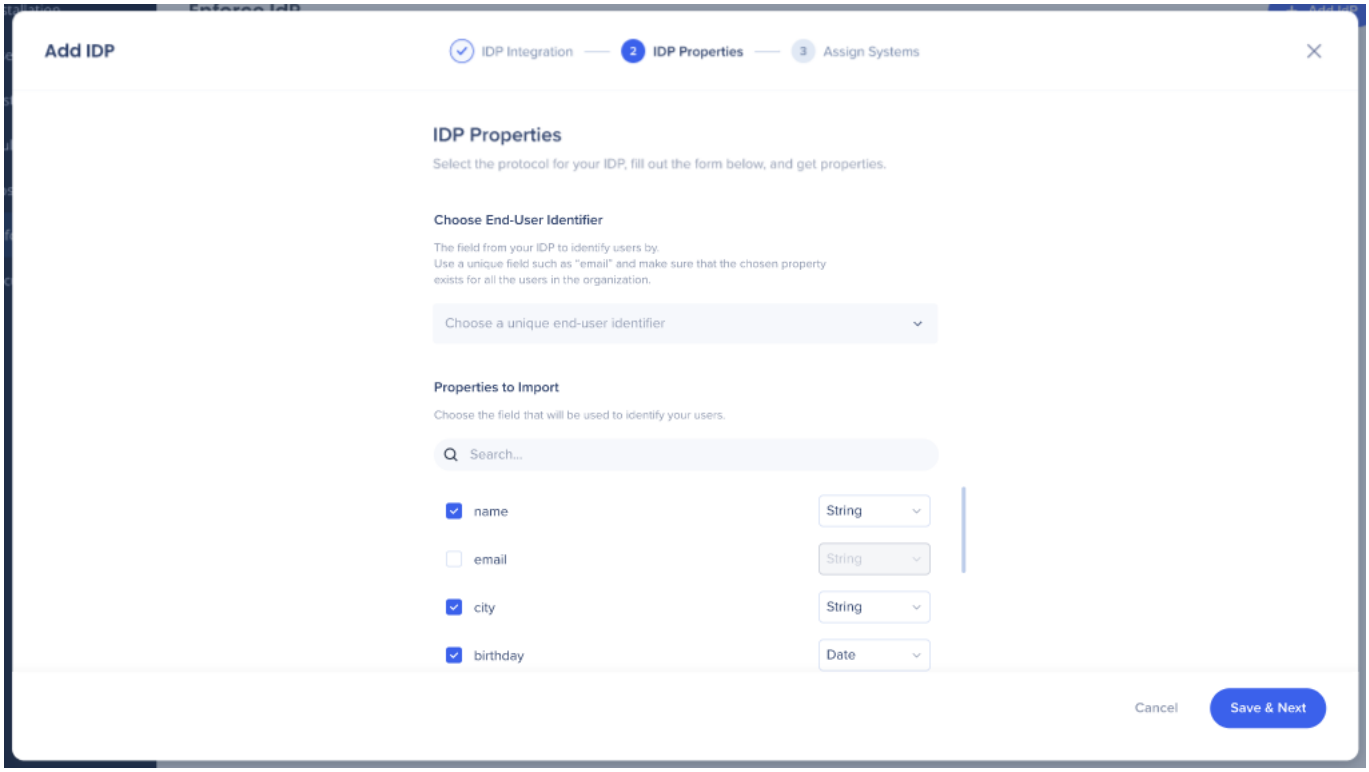
5. Choisissez un identifiant d'utilisateur final unique pour identifier les utilisateurs

- 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 :

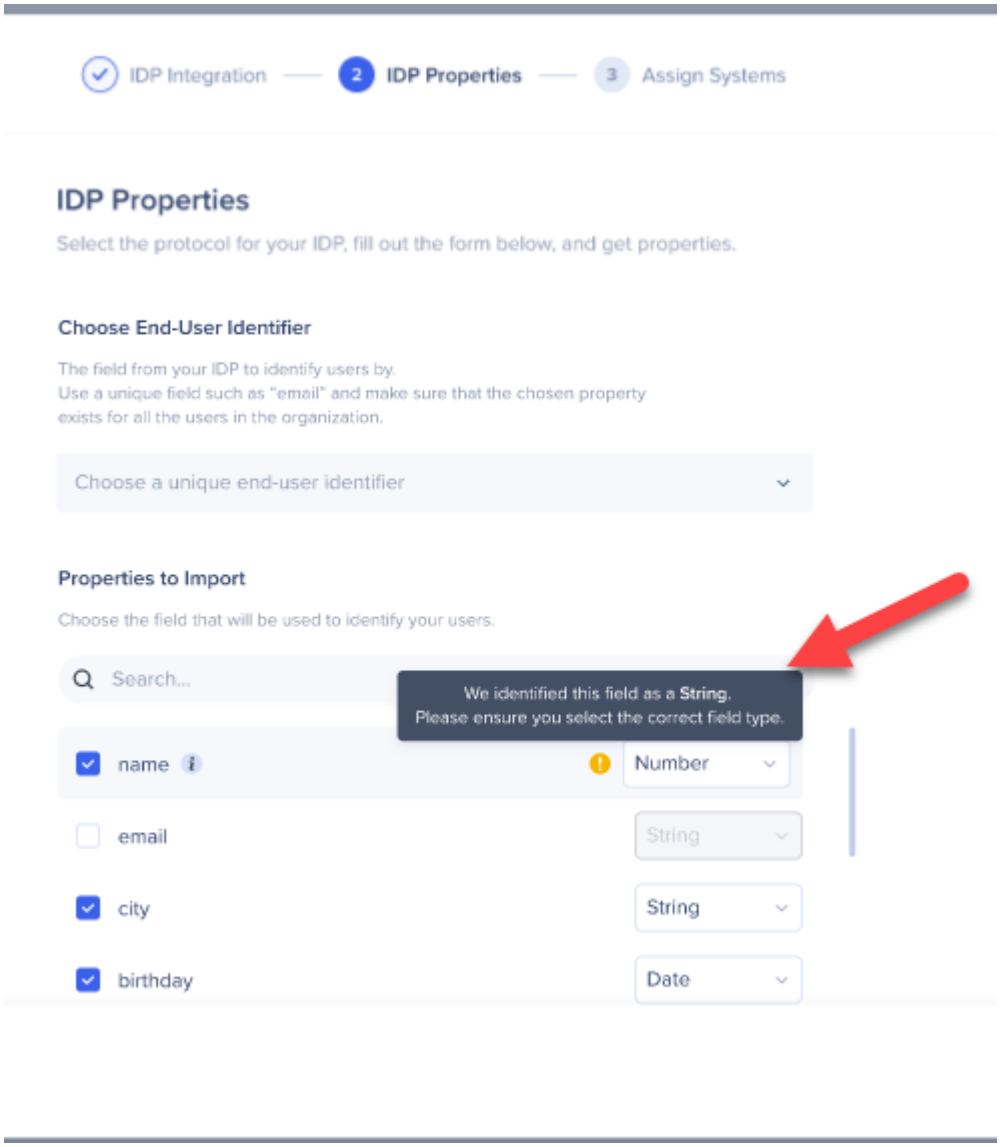
1. Chaîne
2. Numéro
3. Date

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



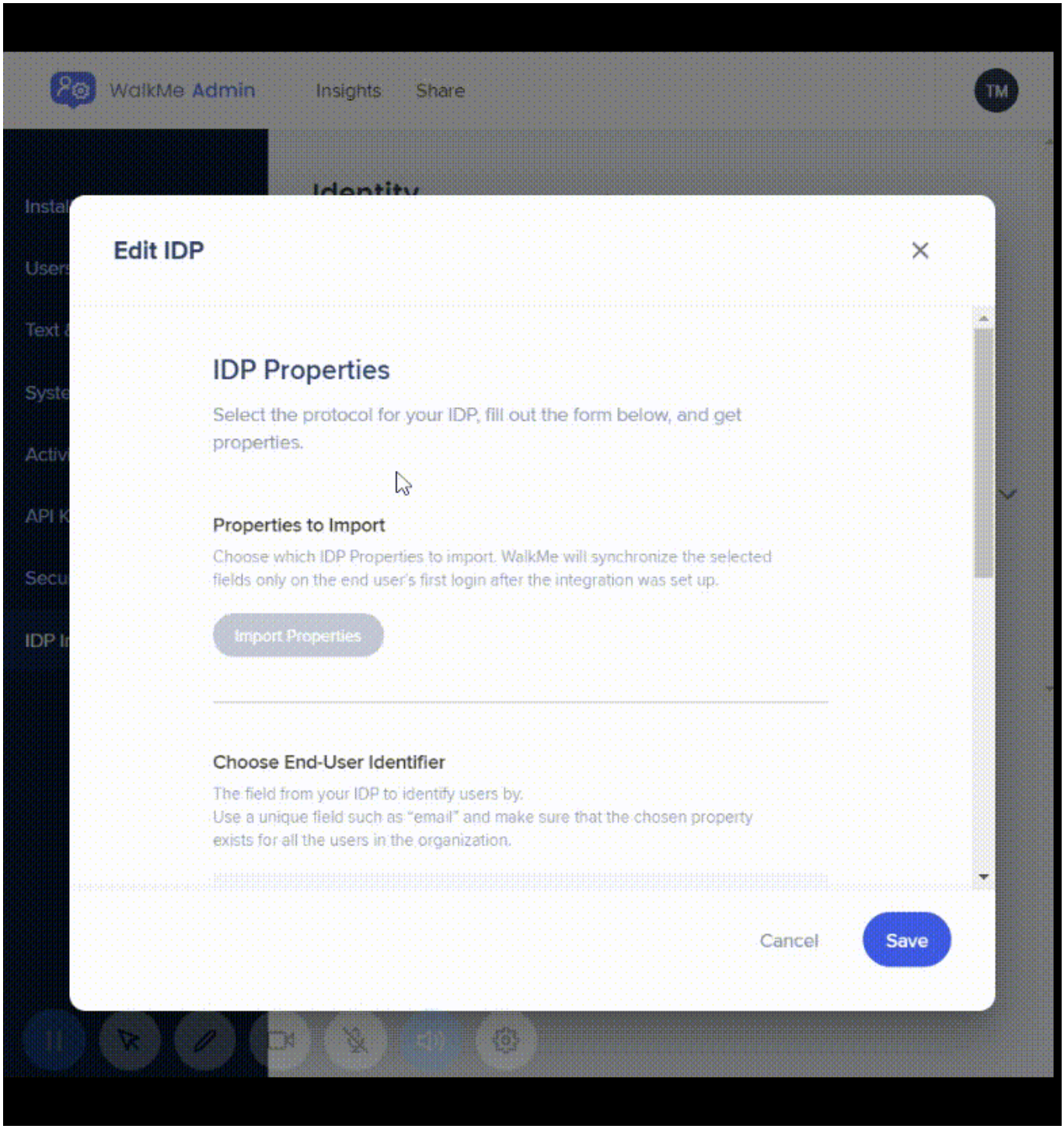
Conseil :

- 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.



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

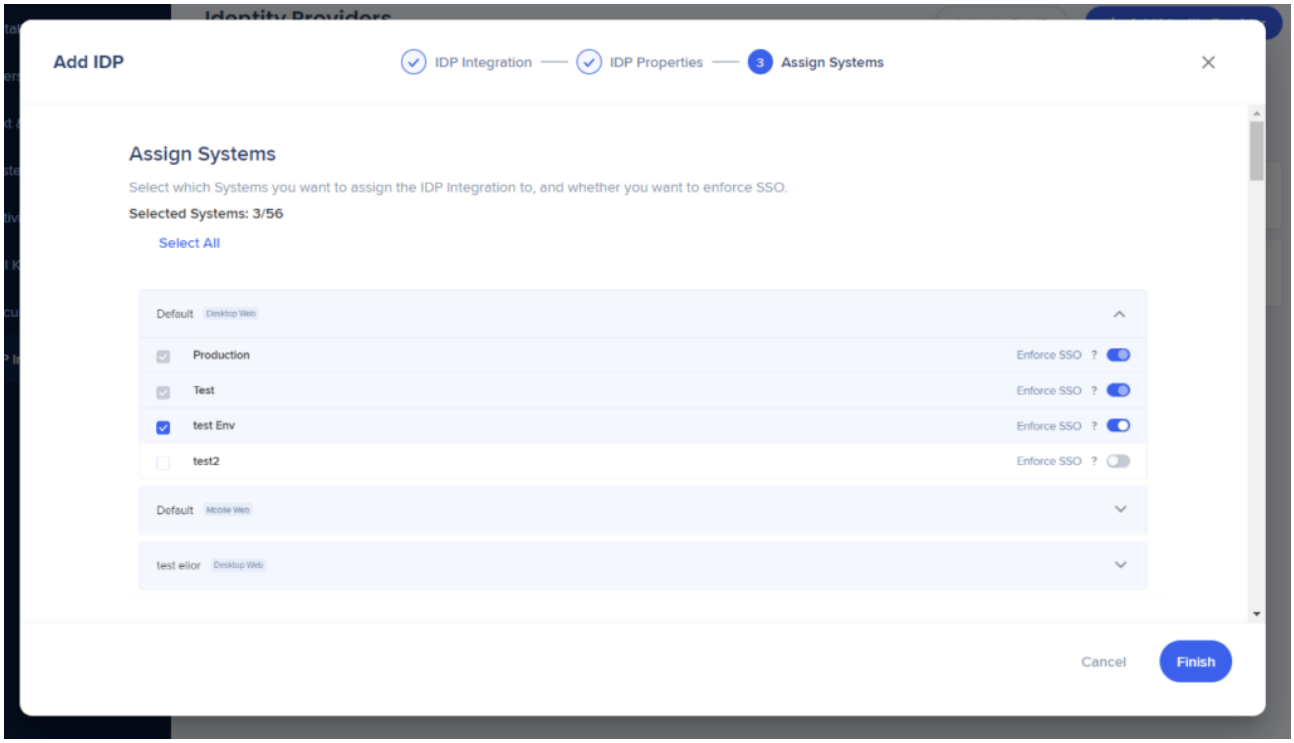
Vous pouvez également renommer toute propriété sélectionnée, afficher sa valeur et son nom d'origine et retourner à sa valeur d'origine si elle est remplacée.



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).

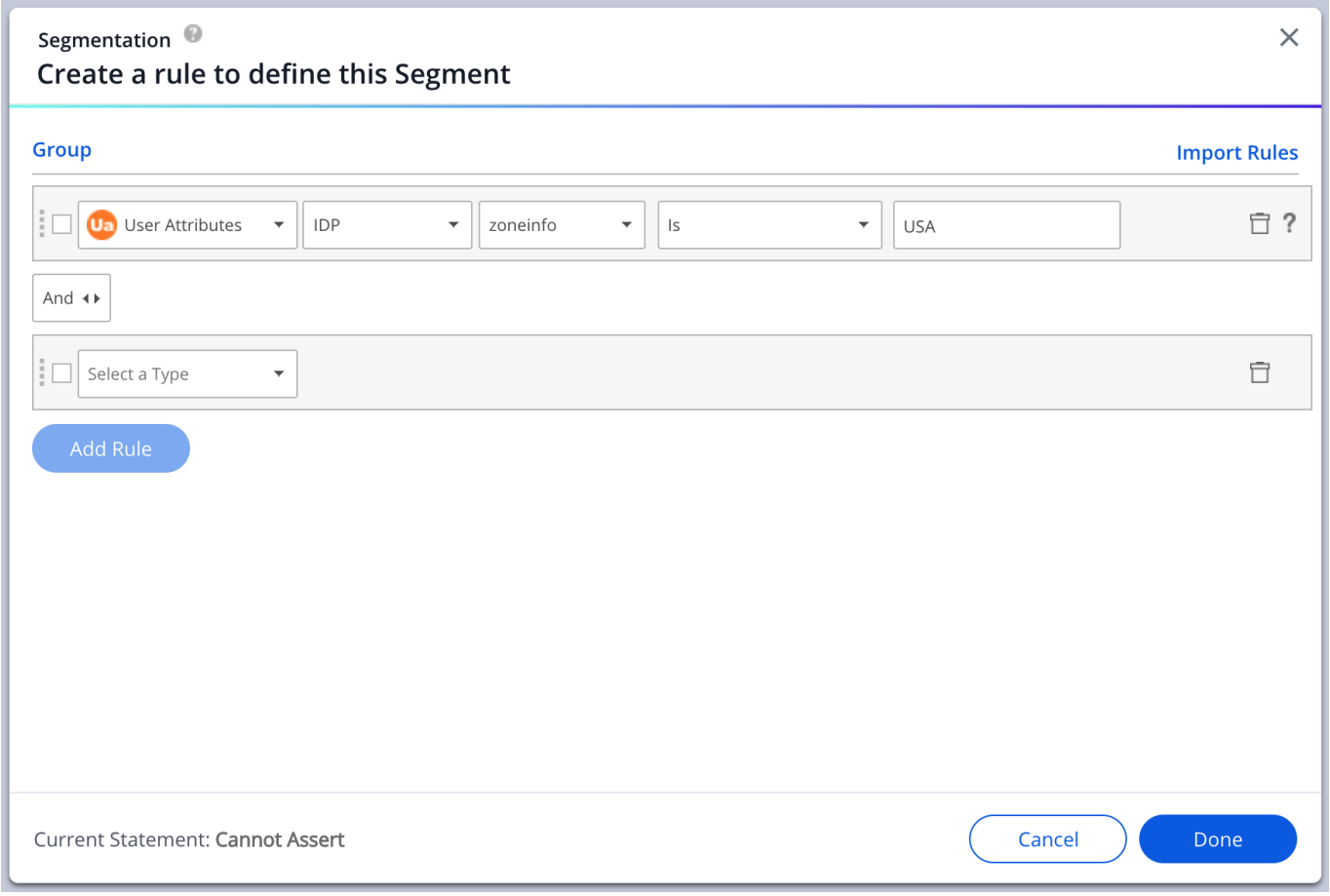
10. Un message apparaîtra vous indiquant si votre IDP a été ajouté avec succès ou pas



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.

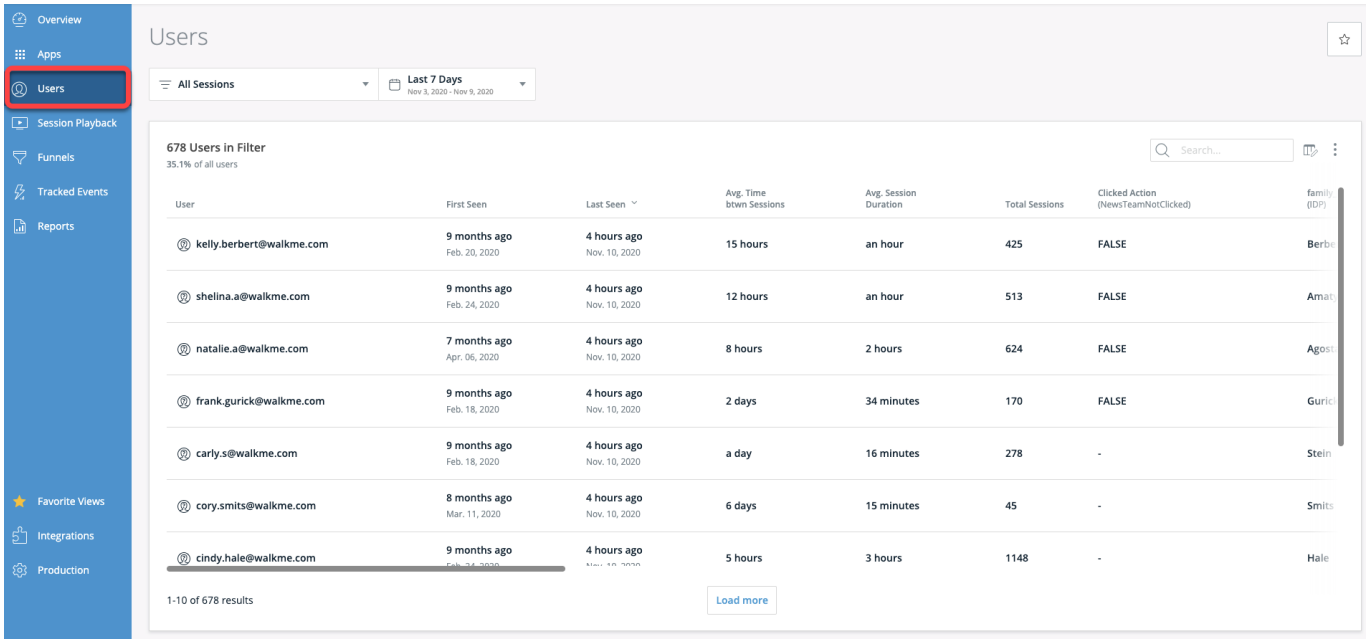


Conseil :

- 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** à **insights.walkme.com**, où toutes les données utilisateur sont affichées.

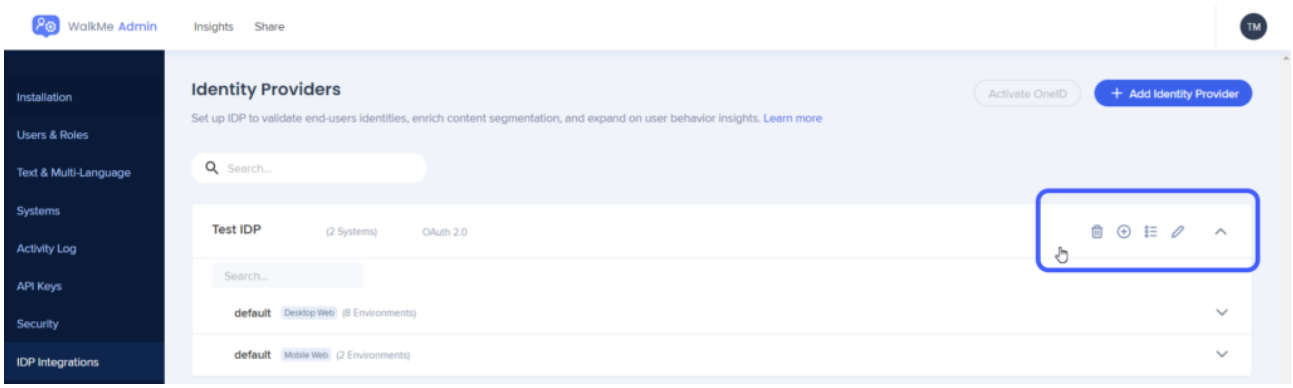
- Les utilisateurs sont ajoutés au tableau uniquement après la fin de la session. L'ajout des utilisateurs prendra donc un peu de temps après la configuration IDP.



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



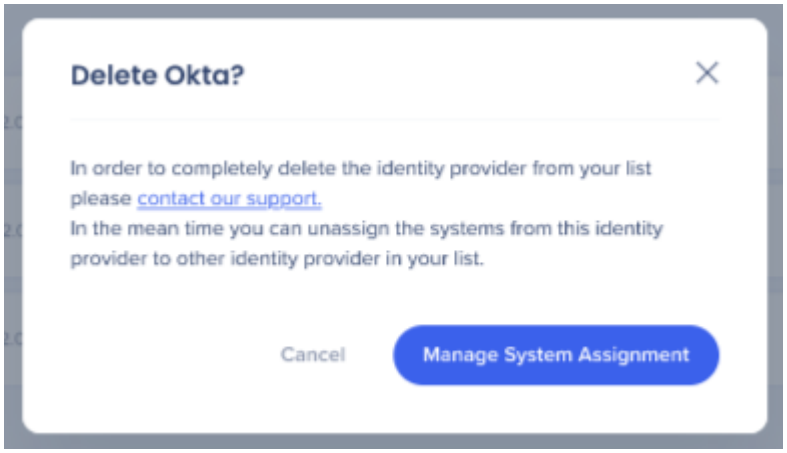
Supprimer

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

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

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.



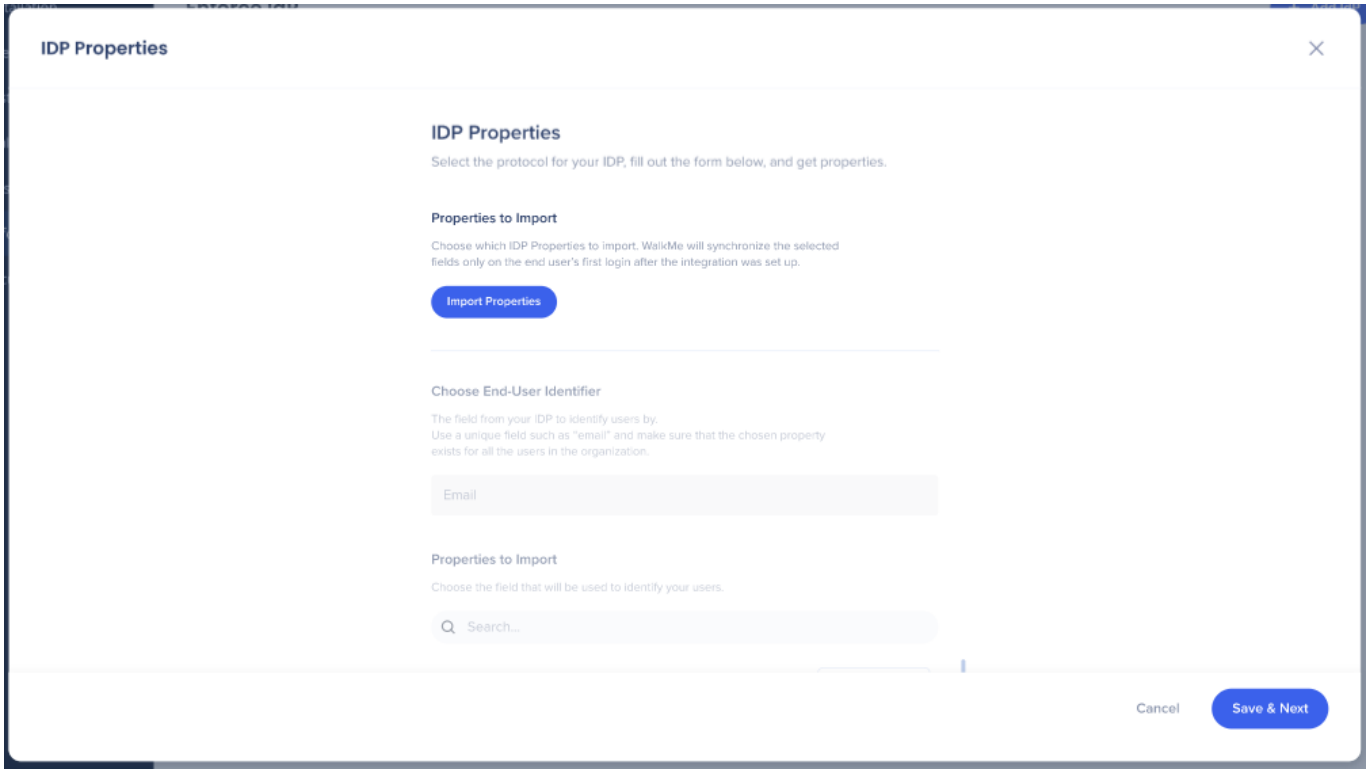
Importer des propriétés

- 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.

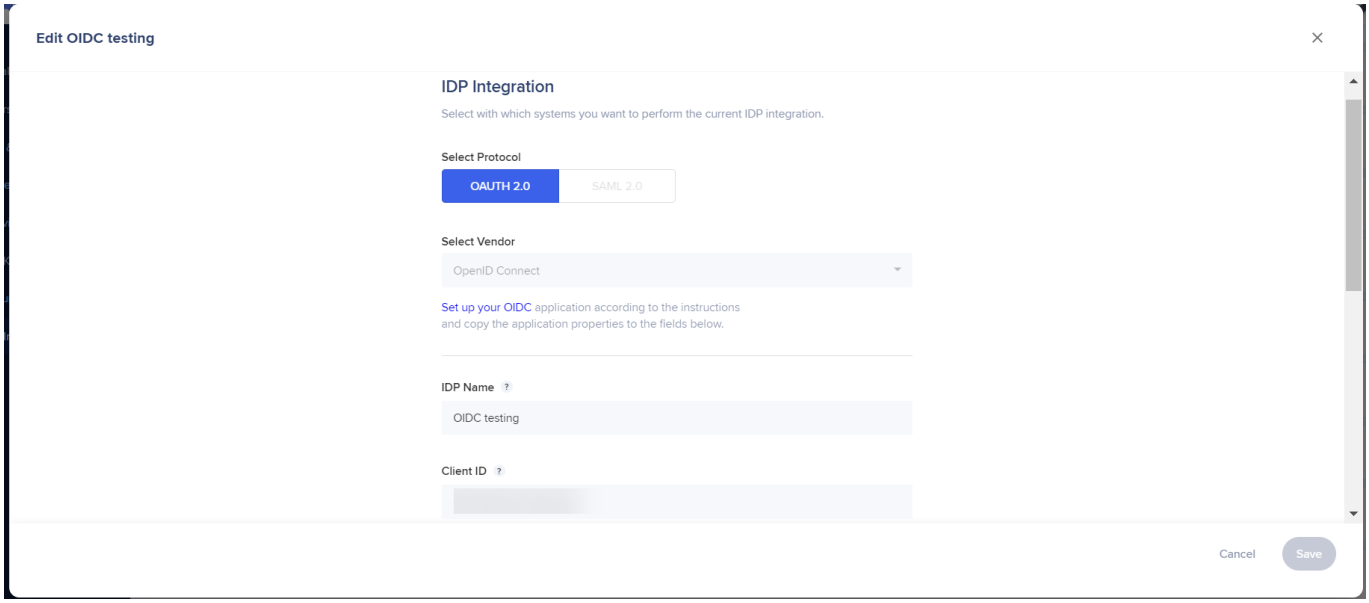


Modifier

- 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

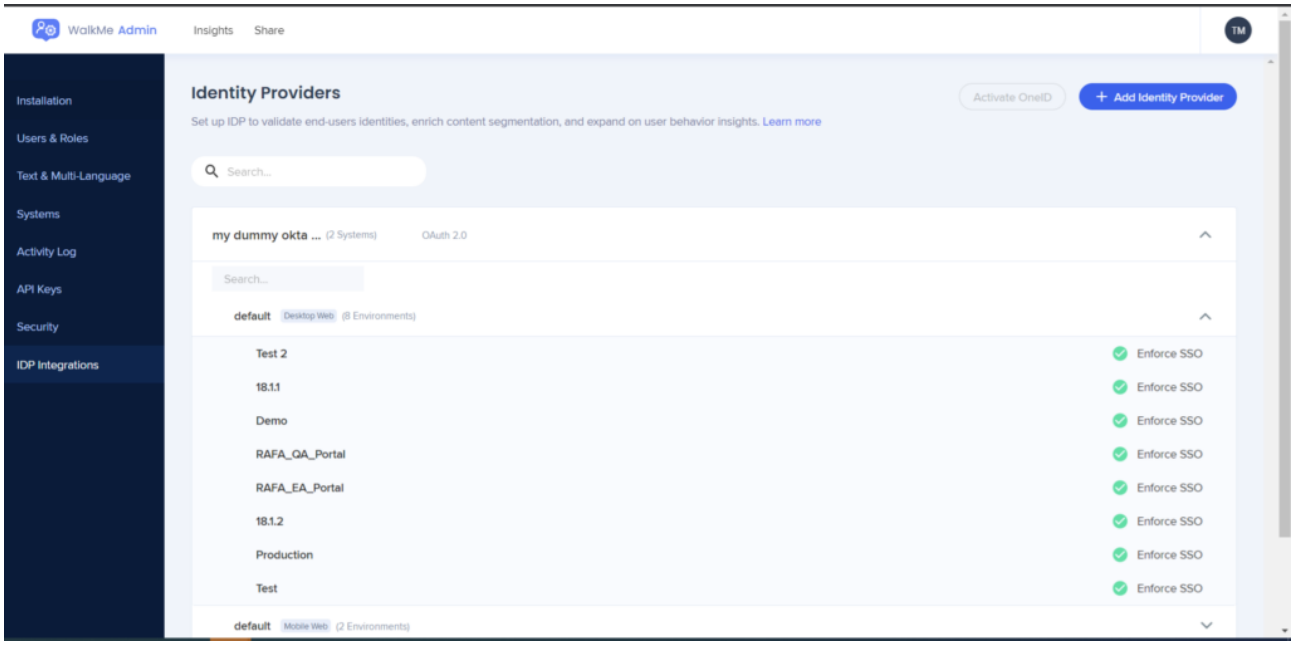
Remarque :

- 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 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 :** Modifier l'identificateur d'utilisateur a un impact sur la façon dont WalkMe identifie les utilisateurs finaux et peut réinitialiser les configurations de « Play once » (lecture unique).

Veuillez noter que votre implémentation est déjà en vigueur, modifier l'identificateur d'utilisateur a des répercussions sur la façon 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.

- Le navigateur Safari ne prend pas en charge l'IDP
- 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 une 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

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

[/ht_message][/ht_message]