Single Sign-On (SSO)

Aperçu général

La page Single Sign-On (authentification unique) du **centre d'administration** offre une gestion de niveau entreprise de la configuration de la **SSO en libre-service**, basée sur la nouvelle infrastructure d'authentification.

Cas d'utilisation

- Réduire la durée de l'Onboarding
- Permettre une configuration et une gestion en libre-service
- Remplacer l'ancienne SSO propriétaire
- Accéder aux fonctionnalités complètes de la SSO
- Renforcer la sécurité et la conformité

Glossaire de la SSO

Assertion : données fournies par l'IdP qui fournissent une ou plusieurs des déclarations suivantes à un fournisseur de services :

- *Les déclarations d'authentification* indiquent que l'utilisateur spécifié dans l'assertion a réellement été authentifié avec succès et à quelle heure.
- *Les énoncés d'attributs* fournissent la valeur des attributs de l'utilisateur. L'attribut NameID est requis et spécifie l'utilisateur, mais d'autres attributs peuvent également être configurés manuellement.
- *Les déclarations de décision d'autorisation* indiquent que la demande d'autorisation d'accès à la ressource spécifiée par le sujet de l'assertion a été accordée ou refusée

Assertion Consumer Service (ACS) : le point de terminaison (URL) du fournisseur de services qui est responsable de la réception et de l'analyse d'une assertion SAML. Gardez à l'esprit que certains fournisseurs de services utilisent un autre terme qu'ACS. Dans le modèle SAML Okta, cette donnée est saisie dans le champ **Single Sign On URL**.

Attribut : un ensemble de données sur un utilisateur, comme son nom d'utilisateur, son prénom, son ID d'employé, etc.

Restriction de public : une valeur de l'assertion SAML qui spécifie à qui (et *uniquement* à qui) l'assertion est destinée. La « public » est le fournisseur de services et est généralement une URL, mais il peut techniquement être indiqué sous forme de chaîne de données. Si cette valeur n'est pas fournie par le fournisseur de services, essayez d'utiliser l'ACS

État du relais par défaut : l'URL vers laquelle les utilisateurs sont dirigés après une authentification réussie par SAML

Point de terminaison : les URL qui sont utilisées lorsque les fournisseurs de services et les identity provider communiquent les uns avec les autres.

ID d'entité : nom globalement unique d'un identity provider ou d'un fournisseur de services. Un ID d'entité Okta unique est généré pour chaque application et est désigné comme **Identity Provider Issuer** dans les instructions de configuration de l'application Okta.

Identity Provider (IdP) : l'autorité qui vérifie et confirme l'identité d'un utilisateur et qui accède à une ressource demandée (le « fournisseur de services »)

Métadonnées : ensemble d'informations fournies par l'IdP au fournisseur de services, ou vice-versa, au format xml.

- Les métadonnées fournies par le fournisseur de services fournissent généralement l'ACS, la restriction de public, le format de NameID et un certificat x.509 si l'assertion doit être chiffrée. Actuellement, les fichiers de métadonnées fournies par les fournisseurs de services ne peuvent pas être importés dans Okta.
- Les métadonnées fournies par l'IdP indiquent l'URL du SSO, l'ID d'entité et le fichier du certificat x.509 exigé par le fournisseur de services pour déchiffrer l'assertion.

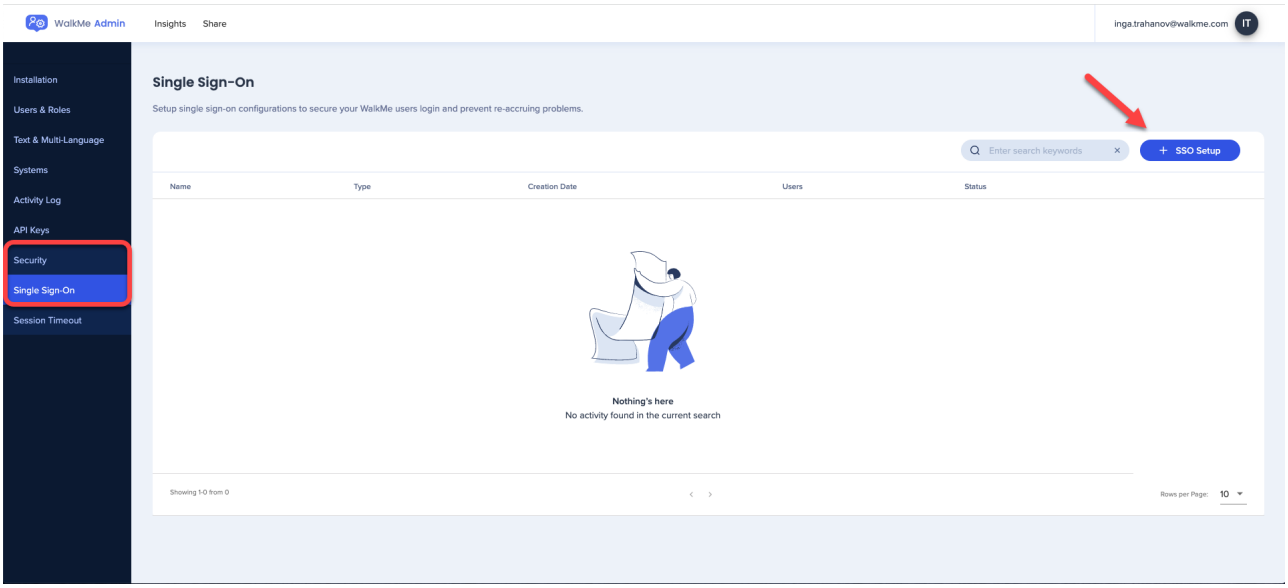
ID du nom : un attribut de l'assertion qui est utilisé pour spécifier le nom de l'utilisateur.

Fournisseur de services (SP) : la ressource hébergée ou le service auquel l'utilisateur a l'intention d'accéder, comme Box, Workday®, Salesforce, une application personnalisée, etc.

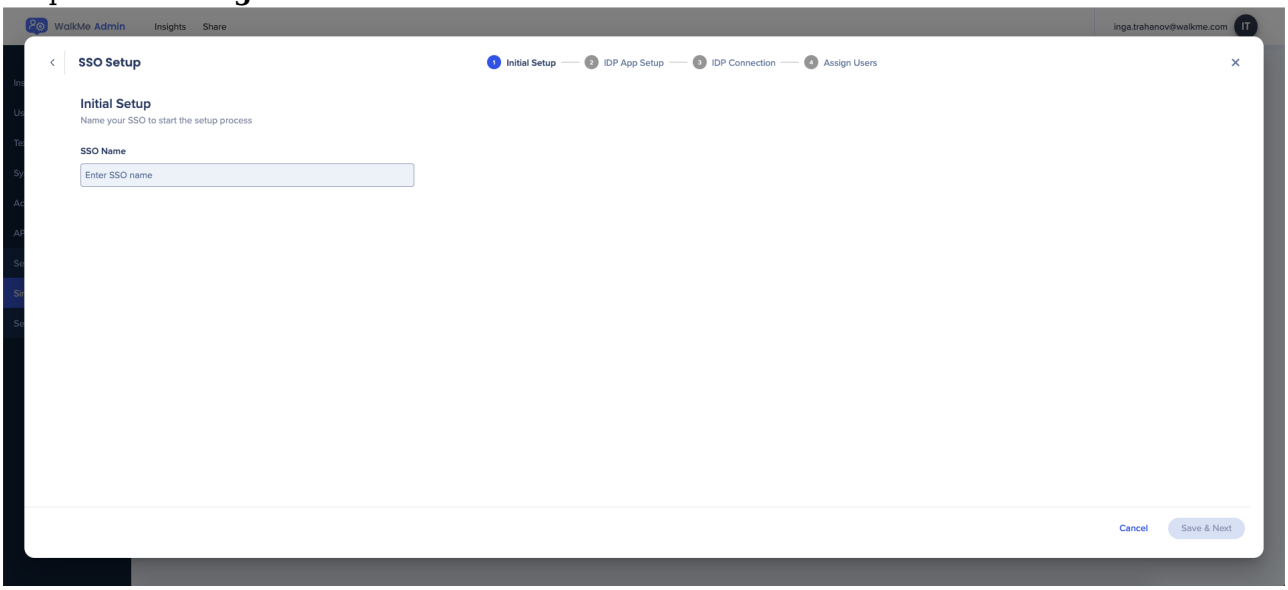
URL de SSO : le point de terminaison dédié à la gestion des transactions SAML. Sur l'écran de configuration du modèle SAML Okta, l'URL du SSO se rapporte à l'**ACS** du fournisseur de services.

Comment ça marche

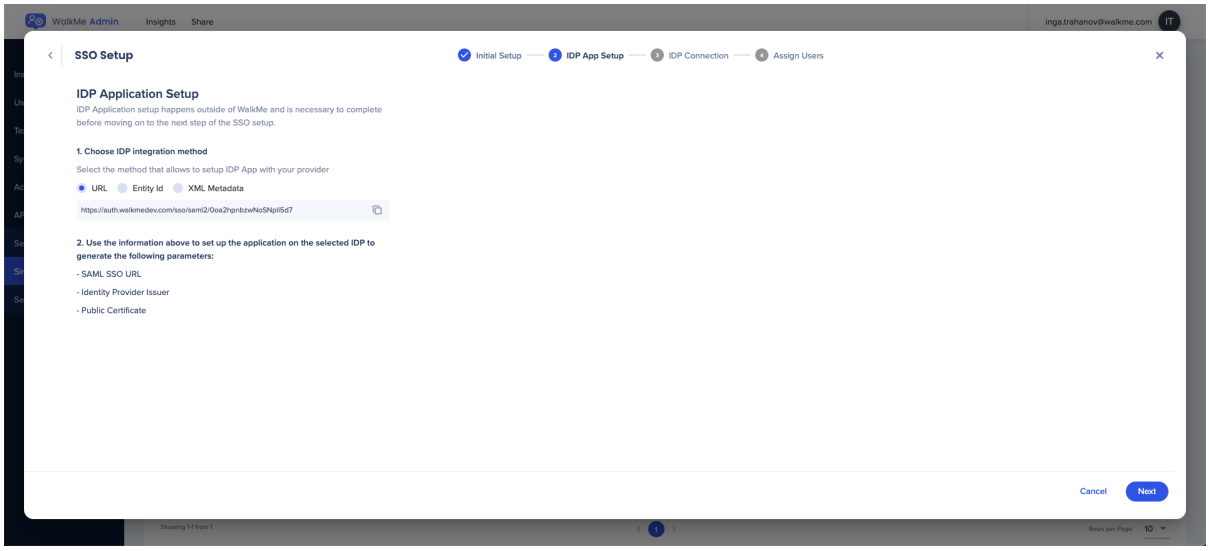
1. Ouvrez le **Centre d'administration** à l'adresse suivante **admin.walkme.com**
    1. Pour les utilisateurs de l'UE, rendez-vous sur **eu-admin.walkme.com**
2. Accédez à la page **Sécurité**, puis à **Authentification unique**
3. Cliquez sur le bouton **Configuration de + SSO**



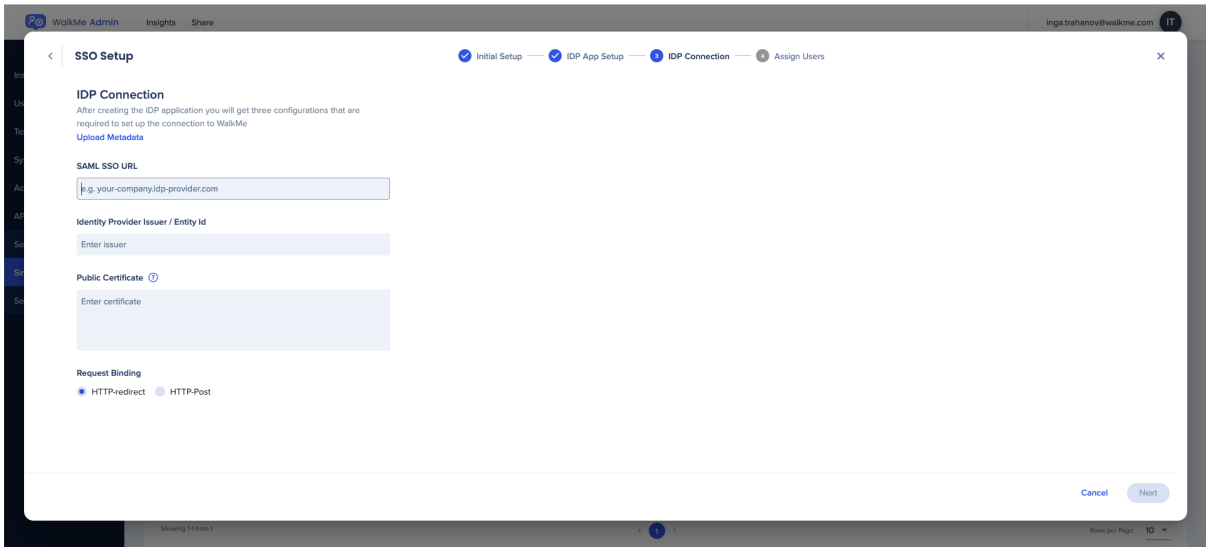
4. Saisissez le nom du SSO
5. Cliquez sur **Enregistrer et Suivant**



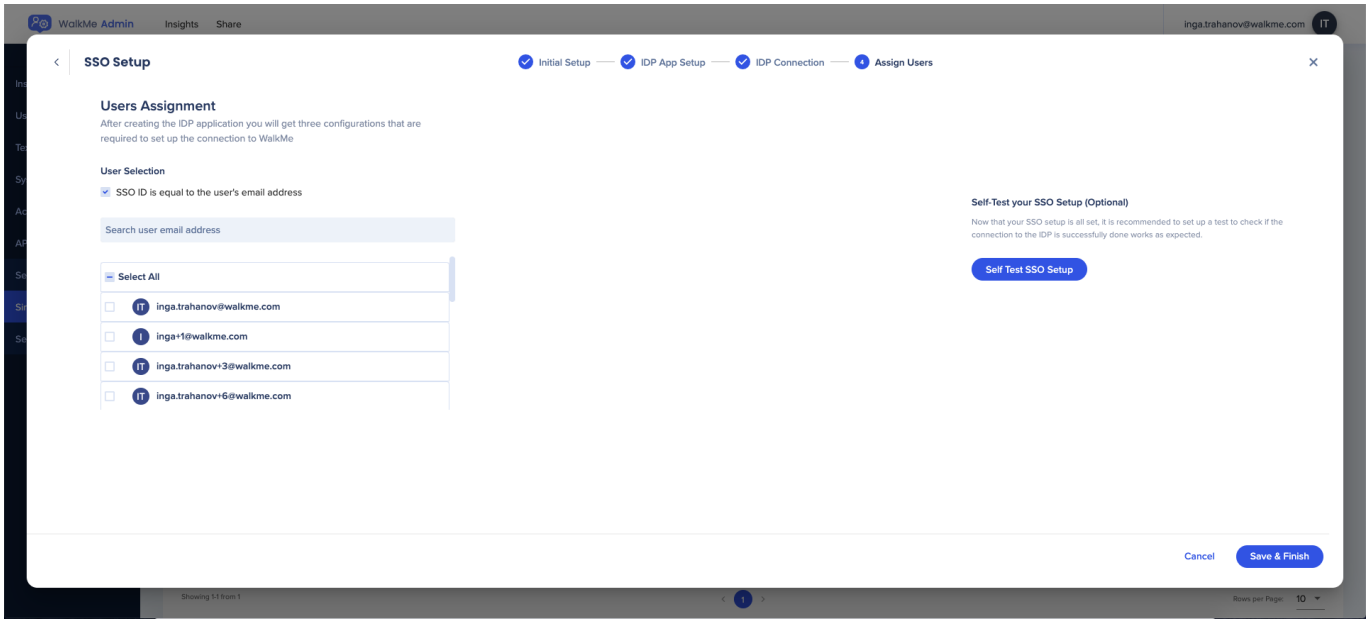
6. Choisissez la méthode d'intégration IDP :
    - **URL**
    - **ID d'entité**
    - **Métadonnées XML** : lorsque vous choisissez cette méthode, vous pouvez télécharger le contenu xml sous forme de fichier



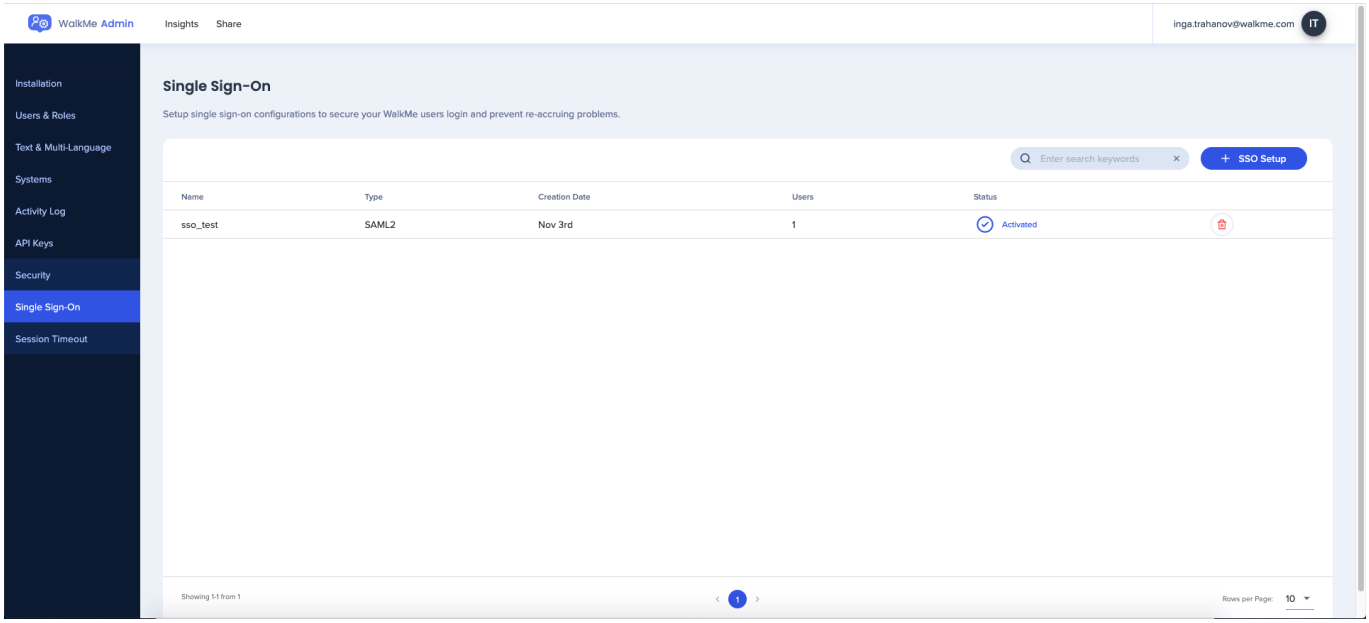
7. Saisissez les détails requis pour terminer la configuration de la SSO :
    - **SAML SSO URL**
    - **Identity Provider Issuer / Entity ID**
    - **Public Certificate**
8. Choisissez une liaison pertinente pour la demande
    - **HTTP-redirect**
    - **HTTP-Port**



    - **Astuce :** cliquez sur **Télécharger les métadonnées** pour compléter tous les champs pertinents automatiquement
9. Sélectionnez les utilisateurs à affecter à la SSO
    - Vous pouvez rechercher et affecter des utilisateurs spécifiques ou **Tout sélectionner**
    - L'ID SSO par défaut est une adresse e-mail, mais il peut être modifié si vous le souhaitez
    - Utilisez le bouton **Tester la configuration du SSO** pour contrôler le paramétrage du SSO
10. Cliquez sur **Enregistrer et Terminer**



Une fois que la connexion SSO a été ajoutée avec succès, vous pouvez la voir sur la page Single Sign-On du centre d'administration.



Pour plus d'informations sur la configuration du SSO d'Azure AD, veuillez vous reporter à l'article suivant : **[Tutoriel Microsoft]**

Certificat SSO

Remarque :

- WalkMe passe à une nouvelle solution SSO fournie par Okta, leader de la gestion de l'identité. Elle offre plus de disponibilités et de performances, ainsi que de meilleures capacités de surveillance et de journalisation.
- Si votre compte est actuellement enregistré avec l'ancien SSO de WalkMe, veuillez contacter la personne qui gère votre Authentification unique en interne. Il s'agit généralement de l'équipe chargée de la gestion de l'identification et de l'accès ou de l'équipe informatique. Demandez-leur de suivre le processus décrit ci-après.
- Ils sauront quelles informations doivent être saisies pour configurer le SSO.

1. Créer une nouvelle connexion SSO en suivant les étapes ci-dessus
2. Dans la 3e étape, vous devrez télécharger le nouveau certificat et terminer la configuration
3. Après la création de la nouvelle connexion SSO, tous les liens pertinents qui utilisent l'ancien SSO doivent être remplacés par le nouveau créé dans la configuration

Aide au dépannage de la SSO

Quelle est la cause des erreurs SAML ?

Les erreurs SAML se produisent généralement lors de la configuration de votre SAML, lorsque des informations incorrectes sont saisies ou manquantes. Vous pouvez résoudre la plupart de ces problèmes depuis vos paramètres IDP, mais pour certains, vous devrez aussi mettre à jour les paramètres SSO de WalkMe.

Messages d'erreur SAML

Message d'erreur	**Comment la corriger**
La réponse SAML ne contient pas l'émetteur Identity Provider correct. Vérifiez que l'URL de l'émetteur indiquée dans vos paramètres [IDP] correspond à l'émetteur Identity Provider ci-dessous.	Vérifiez vos paramètres IDP pour vous assurer que la valeur correcte est copiée dans votre configuration SSO du centre d'administration. La valeur de l'émetteur d'un IDP est généralement appelée une **URL d'émetteur** Ou **URL/ID d'entité** .

La réponse SAML n’est pas signée. Vérifier vos paramètres [IDP].	Activer **la signature des réponses** dans vos paramètres IDP. Si vous ne voyez pas ces options, contactez votre IDP.
La réponse SAML ne contient pas le public correct. Vérifiez que l’URL du fournisseur de services de vos paramètres [IDP] correspond à l’émetteur du fournisseur de services dans les options avancées ci-dessous.	Assurez-vous que **l’émetteur du fournisseur de services** correspond au **Public** dans vos paramètres IDP. La page de téléchargement du **Public** peut également être appelé **ID d’entité du fournisseur de services** Ou **Identifiant de la partie de confiance** .
L’assertion de la réponse SAML n’est pas signée. Vérifier vos paramètres [IDP].	Activer **la signature des assertions de réponses** dans vos paramètres IDP. Si vous ne voyez pas ces options, contactez votre IDP.
La réponse SAML ne contient pas la destination correcte qui doit ressembler à https://auth.walkme.com/sso/saml2. Vérifier vos paramètres [IDP].	Mettez à jour la **destination** dans votre IDP. Le nom de la valeur peut varier, mais c’est généralement un des suivants : Reply URL, ACS URL, Assertion Consumer Service URL, Trusted URL, ou Endpoint URL.
L’attribut ID est manquant dans la réponse SAML. Vérifier vos paramètres [IDP].	Veillez à inclure le **NameID** sous forme de demande envoyée dans votre IDP dans le format correct (Persistent).
La réponse SAML et l’assertion de la réponse SAML ne sont signées ni l’une, ni l’autre. Vérifier vos paramètres [IDP].	Depuis vos paramètres IDP, activez la **signature de la réponse**, l’**assertion de la réponse** ou des deux. Si vous ne voyez pas ces options, contactez votre IDP.
La réponse SAML n’est pas signée (bien qu’il y ait une assertion signée et chiffrée avec un EncryptedId). Nous sommes désolés, mais WalkMe ne prend pas en charge ce format. Vérifier vos paramètres [IDP].	Nous ne prenons pas en charge ce format. Autorisez la **signature des réponses** et veillez à suivre les directives pour configurer correctement votre SSO.
La réponse SAML n’est pas de la version 2.0. Vérifier vos paramètres [IDP].	Veillez à utiliser **SAML 2.0** dans votre IDP.

Hmm, il ressemble que la validation de la signature a échoué. Vérifiez les certificats de signature dans vos paramètres [IDP].	Mettez à jour le **certificat** dans la configuration SSO de votre centre d'administration pour qu'il corresponde au certificat envoyé par votre IDP.