SAML IDP-Integration

Kurzübersicht

Die IDP-Integration von WalkMe kann ein Authentifizierungsprotokoll namens SAML verwenden, um Benutzer bei ihrem organisatorischen IDP-Anbieter zu authentifizieren und um Benutzerattribute zu erhalten, die später für die Segmentierung und Analyse in WalkMe verwendet werden können. Jeder IDP-Anbieter, der SAML unterstützt, sollte mit WalkMe zusammenarbeiten. WalkMe unterstützt den vom SP initiierten Fluss.

Was ist SAML?

SAML, das für „Security Assertion Markup-Language“ steht, ist ein offener Standard, der es „Identity Providers“ (Identitätsanbietern) (IDP) ermöglicht, Berechtigungsnachweise an Service Provider (SP) weiterzugeben. Es ermöglicht Computer-Clients, die Identität eines Endbenutzers auf der Grundlage der von einem Autorisierungsserver durchgeführten Authentifizierung zu überprüfen und grundlegende Profilinformationen über den Endbenutzer zu erhalten.

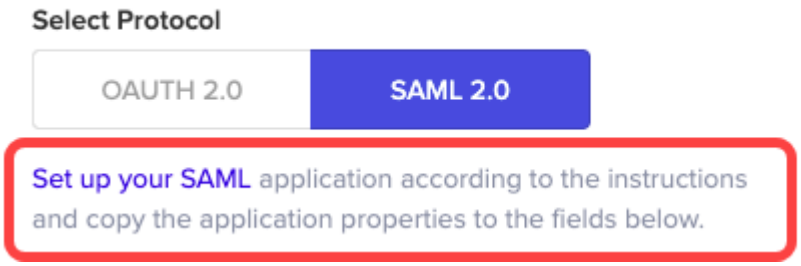
Anwendungsfälle

- IDP-Authentifizierung des Endbenutzers als Voraussetzung für die Darstellung von WalkMe-Inhalten
- Erweiterung der Möglichkeiten zur Segmentierung von Inhalten nach IDP-Parametern (z. B. – Gruppen, Region, Abteilung usw.)
- Genaue Datenüberwachung über Systeme hinweg

Voraussetzungen

Es muss eine IDP-Anwendung erstellt werden, die als „Brücke“ zwischen IDP und dem Integration Center von WalkMe dient.

Eine Anleitung ist im Admin Center auf dem Konfigurationsbildschirm der IDP-Integration verfügbar.



Rufen Sie Metadaten und Zertifikat von Identity Providern ab

Diese Anweisungen sind allgemein. Sie müssen diese Informationen für Ihren spezifischen Identity Provider (IdP) finden.

- **SSO-URL (Single Sign-On URL)** : URL beim IdP, an den SAML-Authentifizierungsanfragen gesendet werden sollen. Dies wird oft als SSO-URL bezeichnet.
- **X509 Signaturzertifikat**: Zertifikat, das der Service Provider benötigt, um die Signatur der vom IdP digital signierten Authentifizierungsaussagen zu validieren. Es sollte einen Platz geben, das Signierzertifikat vom IdP herunterzuladen. Wenn das Zertifikat nicht im .pem oder .cer Format ist, sollten Sie es in eines dieser Formate konvertieren. Später fügen Sie dies in WalkMe ein.
  Die Methoden zum Abrufen dieses Zertifikats sind unterschiedlich, daher sollten Sie die Dokumentation Ihres IdP ansehen, wenn Sie zusätzliche Hilfe benötigen.

Anmerkung:

- Bevor Sie das X.509-Signierzertifikat auf WalkMe hochladen, müssen Sie die Datei in Base64 konvertieren.
- Verwenden Sie dazu entweder ein Online-Tool oder führen Sie den folgenden Befehl in Bash aus:
  cat cert.crt | base64.

Fügen Sie WalkMe Service Provider-Metadaten zum IdP hinzu

Fügen Sie dem Identity Provider Informationen über den Service Provider hinzu, damit der Berechtigte weiß, wie er SAML-Authentifizierungsanforderungen empfangen und beantworten kann. Die hier bereitgestellten Anweisungen sind allgemein. Sie müssen die richtigen Bildschirme und Felder für den Identity Provider finden.

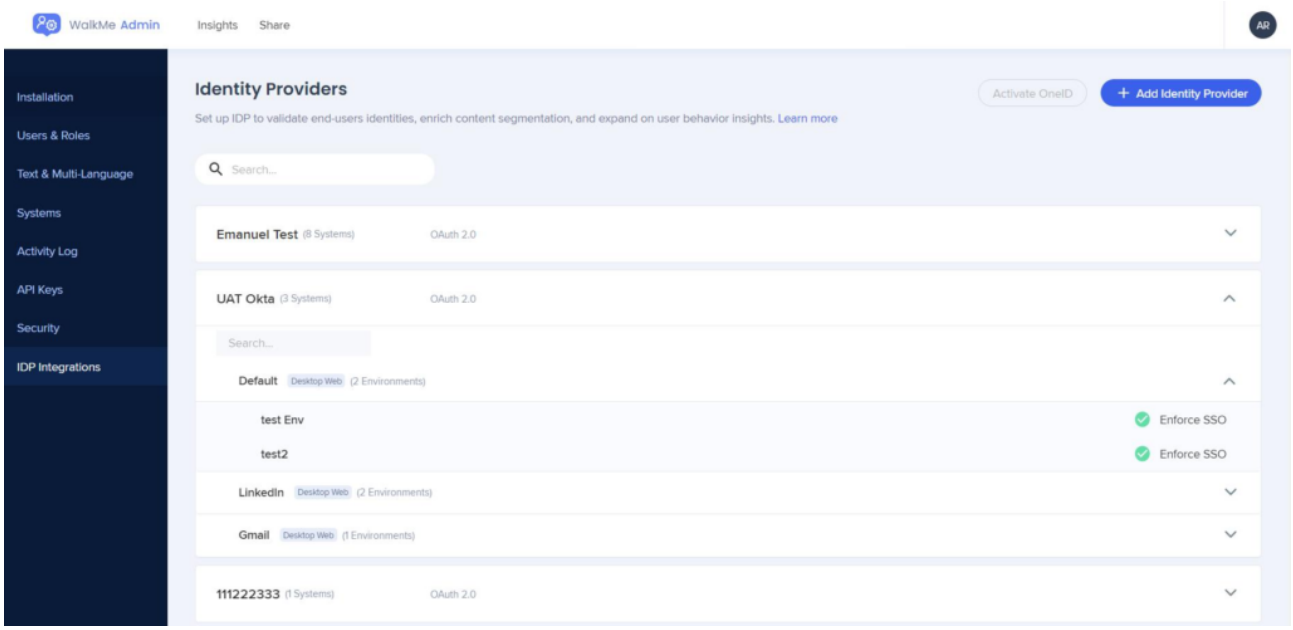
1. Finden Sie die Bildschirme beim Identity Provider, mit denen Sie SAML konfigurieren können.

Wenn der IdP das Hochladen einer Metadaten-Datei unterstützt, können Sie einfach die im obigen Schritt erhaltene Metadaten-Datei bereitstellen. Wenn der IdP das Hochladen einer Metadaten-Datei nicht unterstützt, können Sie sie wie folgt manuell konfigurieren.

2. Der IdP muss wissen, wohin er die SAML-Assertionen senden kann, nachdem er einen Benutzer authentifiziert hat. Dies ist die **Assertion Consumer Service URL** in WalkMe. Der IdP kann dies bezeichnen als **Assertion Consumer URL** oder **Application Callback URL** .
   US: https://papi.walkme.com/ic/idp/p/saml/callback
   EU: https://eu-papi.walkme.com/ic/idp/p/saml/callback
3. Wenn der IdP ein Feld namens **Audience** oder **Entity ID** hat, geben Sie in dieses Feld die **Entity ID** von WalkMe :
   US: https://papi.walkme.com
   EU: https://eu-papi.walkme.com ein
4. Wenn der IdP eine Auswahl für Bindungen anbietet, sollten Sie **HTTP-Redirect** für Authentifizierungsanfragen auswählen.

So fügen Sie einen Identity Provider hinzu

1. Klicken Sie auf der Registerkarte „IDP-Integrations“ des Admin Centers auf die Schaltfläche „+ Add Identity Provider“



2. Wählen Sie den SAML-Protokolltyp

3. Geben Sie die passenden Konfigurationseinstellungen für die Verbindung an

Laden Sie die Metadaten-Datei herunter

- Sie können die WalkMe-Informationen über eine Metadaten-Datei in Ihr System hochladen,

anstatt jedes einzelne Teil kopieren und einfügen zu müssen.

Pflichtfelder:

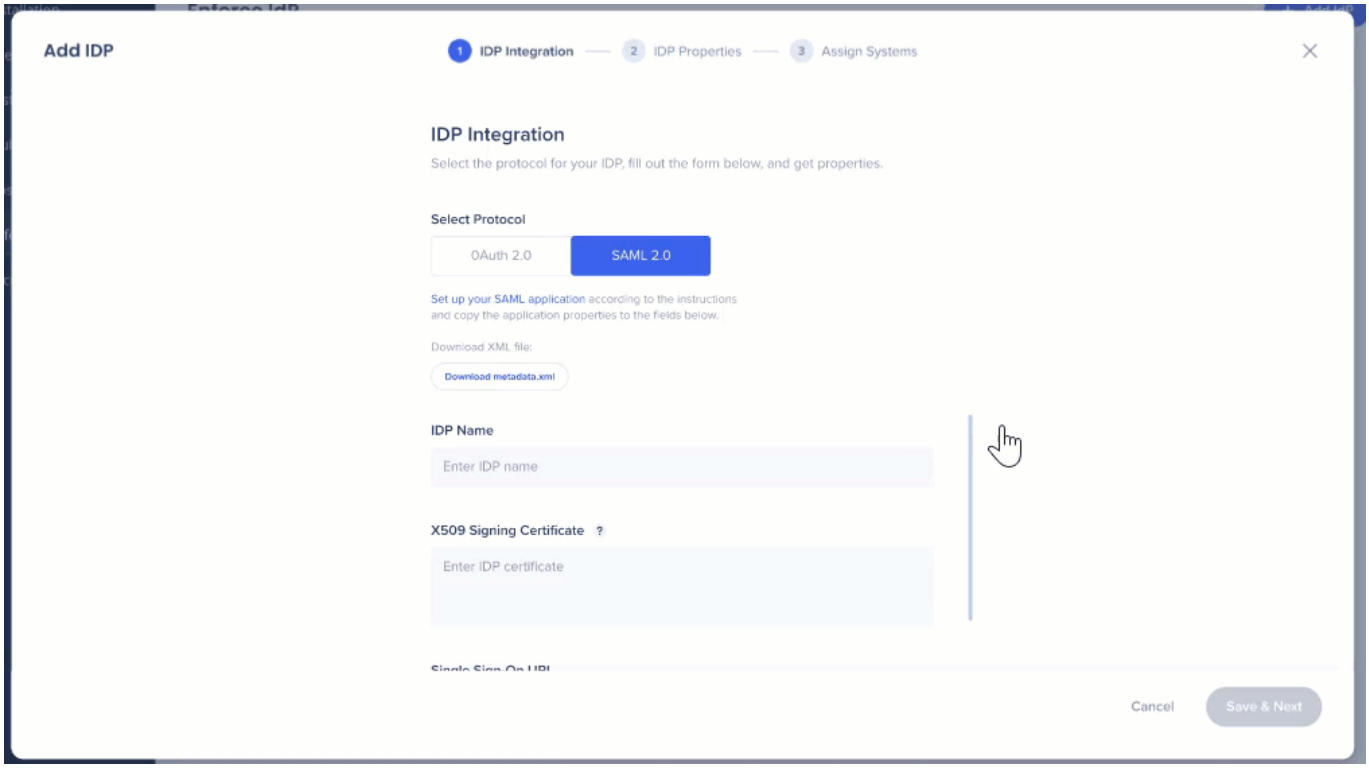
- **IDP Name** – Verbindungsname
- **Single Sign-On URL** – Die Identity Provider Single Sign-On URL vom Installationsassistenten
- **X509 Signierzertifikat** – Laden Sie das Zertifikat hoch, das Sie von Ihrem Anbieter heruntergeladen haben.

Optional – Verschlüsselungseinstellungen:

Um die Sicherheit Ihrer Transaktionen zu erhöhen, können Sie sowohl Ihre Anfragen als auch Ihre Antworten im SAML-Protokoll signieren oder verschlüsseln.

Zunächst müssen wir ein Zertifikat erstellen und herunterladen, das für Ihr Konto eindeutig ist. Der öffentliche Schlüssel wird Ihnen mitgeteilt, damit Sie ihn bei Ihrem IDP-Anbieter hochladen können.

- **AuthnRequest –** Signieren Sie die SAML-Authentifizierungsanfrage mit dem privaten Schlüssel.
- **Assertion Encryption –** Empfangen Sie verschlüsselte Assertionen von einem Identity Provider. Dazu müssen Sie dem IDP das öffentliche Schlüsselzertifikat bereitstellen. Der IDP verschlüsselt die SAML Assertion mit dem öffentlichen Schlüssel und sendet sie an WalkMe, das es mit dem privaten Schlüssel entschlüsselt.



4. Klicken Sie auf „Save & Next“ (Speichern und Weiter), sobald Sie fertig sind

- Beachten Sie, dass wir **keine** Sign Logout URL benötigen.

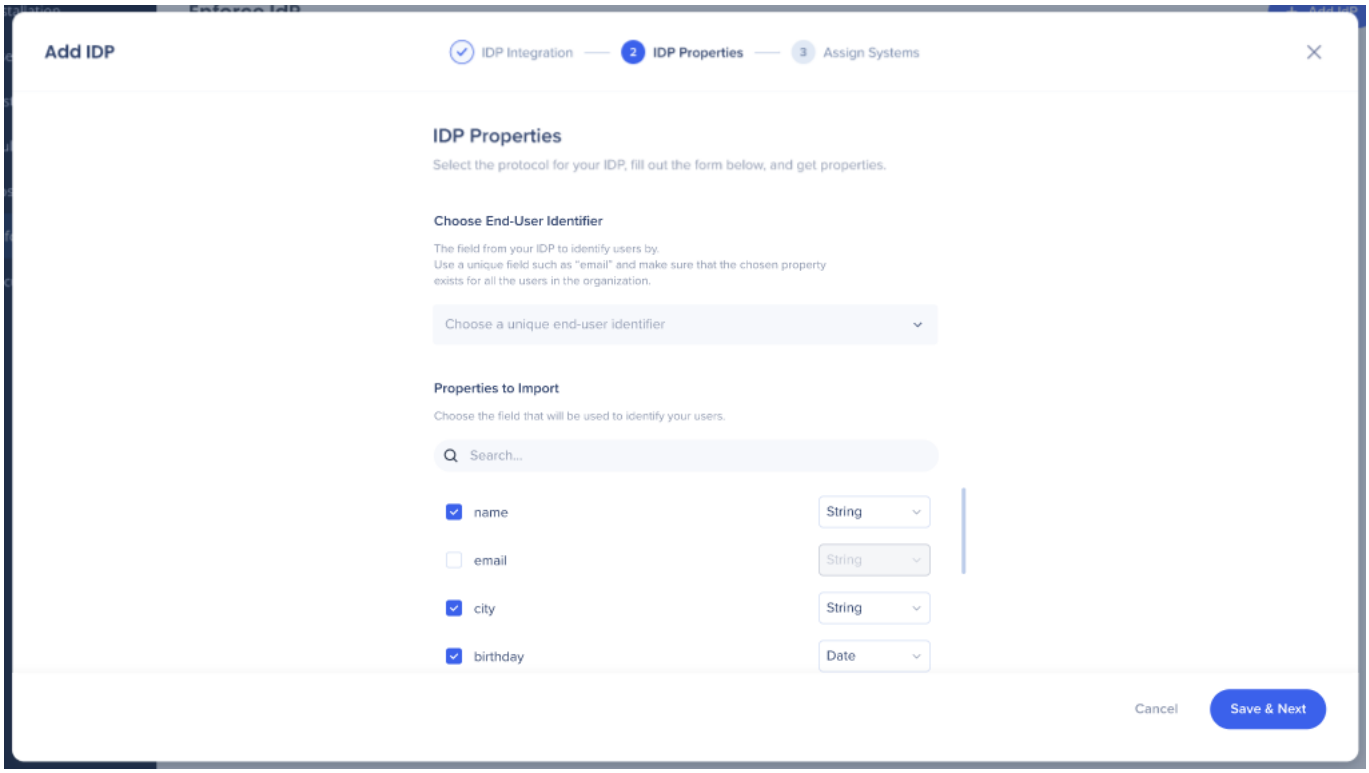
5. Wählen Sie einen eindeutigen Endbenutzerkenner, um die Benutzer zu identifizieren

- Sie benötigen nur eine Kennung. Wir benötigen keine zusätzlichen Gruppeninformationen oder andere Attribute.

6. Wählen Sie die gewünschten Eigenschaften und vergewissern Sie sich, dass Sie den richtigen Datentyp ausgewählt haben:

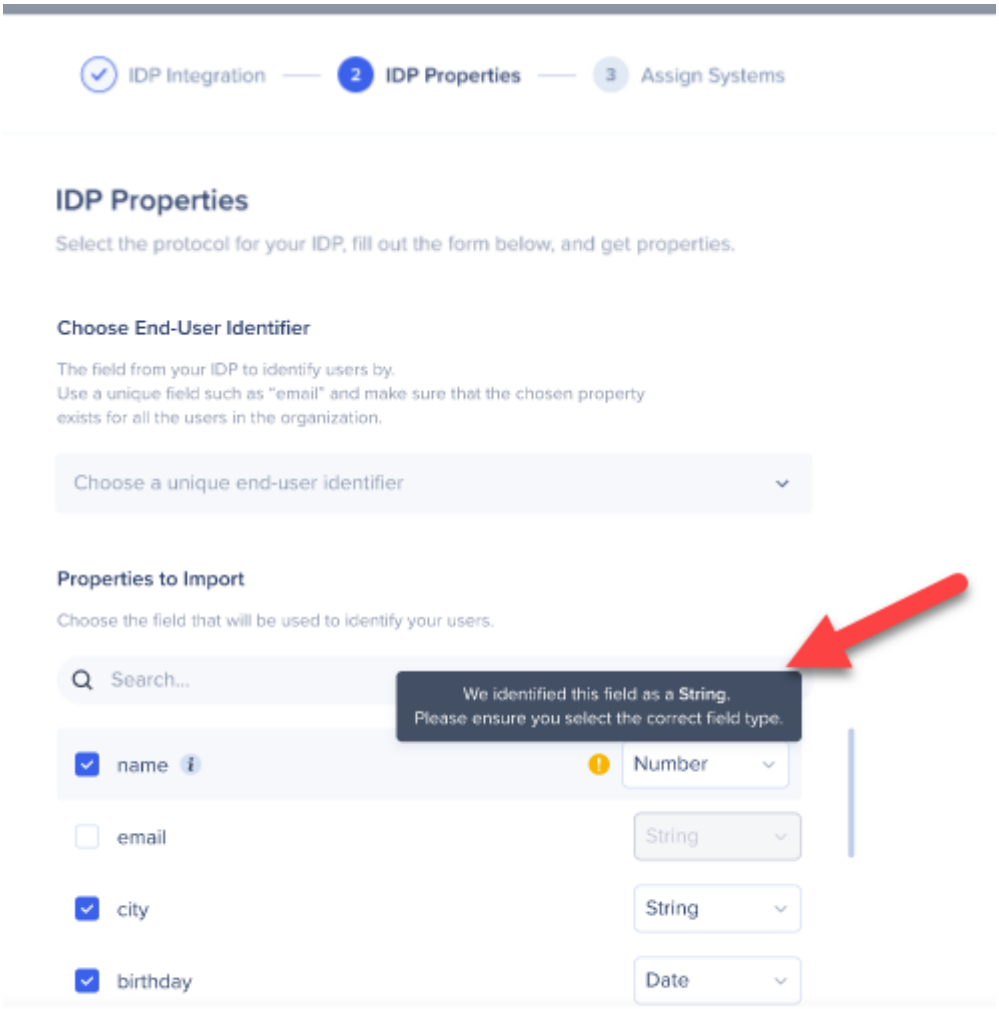
1. String (Zeichenfolge)
2. Number (Nummer)
3. Date (Datum)

Hinweis: Das Feld „User Identifier“ (Benutzer-ID) wird immer in den Typ „String“ (Zeichenfolge) umgewandelt.



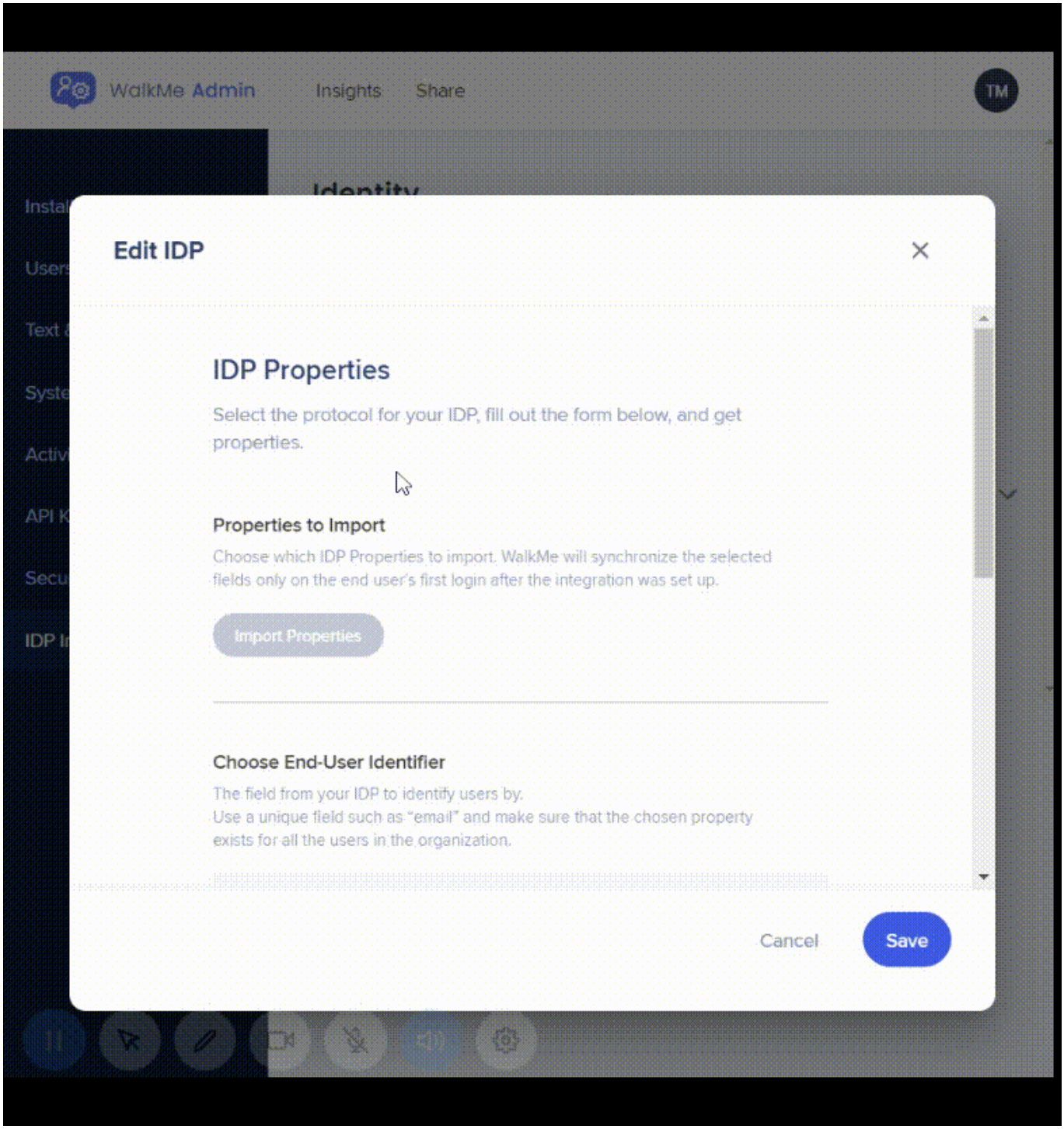
Tipp:

- Um sicherzustellen, dass der ausgewählte Datentyp geeignet ist, können Sie den Mauszeiger über das „i“-Symbol bewegen und den Wert dieser Eigenschaft überprüfen.
- Wenn der gewählte Datentyp nicht für die Eigenschaft geeignet ist, erscheint ein oranges „!“-Symbol mit der Empfehlung, wieder zum identifizierten Datentyp zu wechseln.



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

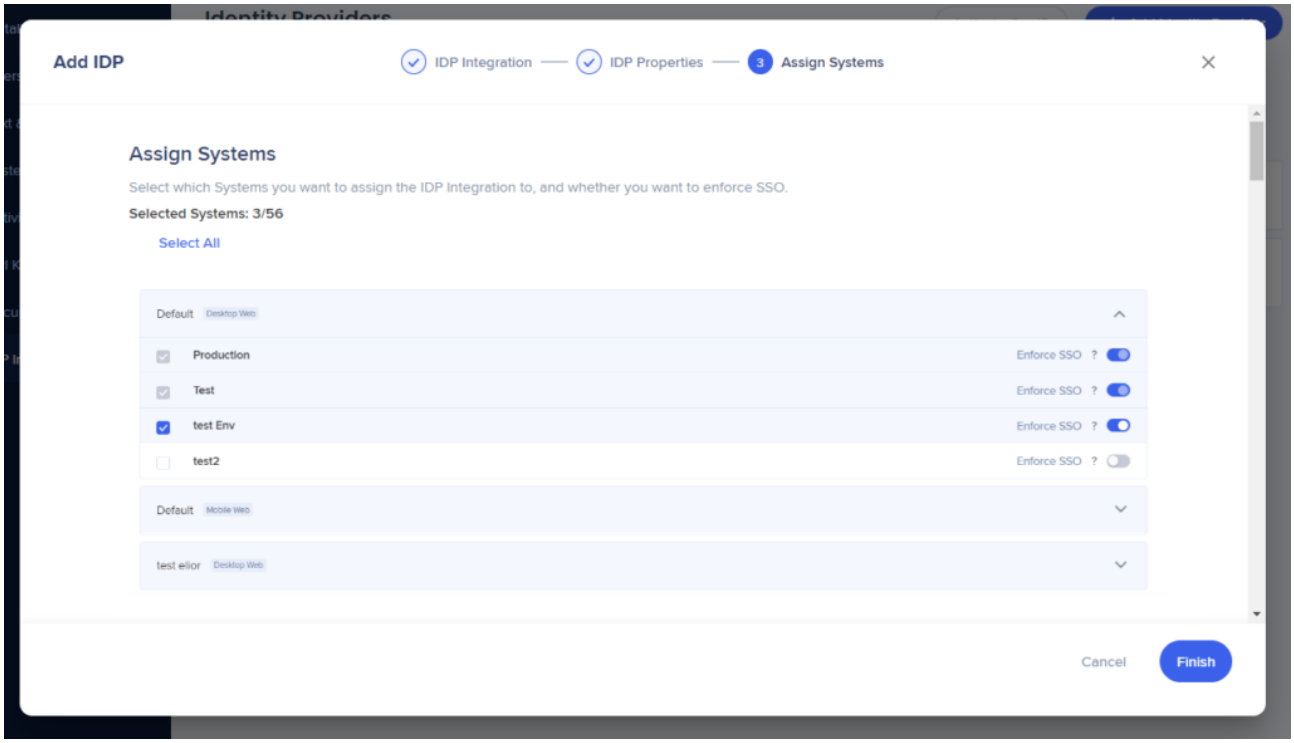
Sie können auch jede ausgewählte Eigenschaft umbenennen, ihren ursprünglichen Wert und Namen anzeigen und zu ihrem ursprünglichen Wert zurückkehren, wenn sie überschrieben wird.



7. Wählen Sie aus, welches der Systeme Sie der IDP-Integration zuweisen möchten

- Für jedes System können Sie die IDP-Integration für die gewünschten Umgebungen separat aktivieren.

8. Verwenden Sie den Umschalter, um SSO zu erzwingen.



Anmerkung:

- IDP sollte eigentlich die akkurateste Benutzeridentifizierung liefern, aber die Zahlen können inakkurat sein, wenn „Enforce SSO“ deaktiviert ist.
- Wenn „Enforce SSO“ deaktiviert ist, können die Benutzer Anwendungen verwenden, ohne sich bei ihrem IDP-Anbieter zu authentifizieren. Stattdessen wird eine WalkMe-ID erstellt und zur Benutzeridentifikation verwendet.
- Benutzer können die IDP-Authentifizierung „überspringen“, indem sie entweder Anwendungen verwenden, die überhaupt keine Authentifizierung erfordern, oder indem sie sich direkt über Benutzer/Passwort bei der Anwendung anmelden, ohne den IDP-Anmeldevorgang zu durchlaufen.

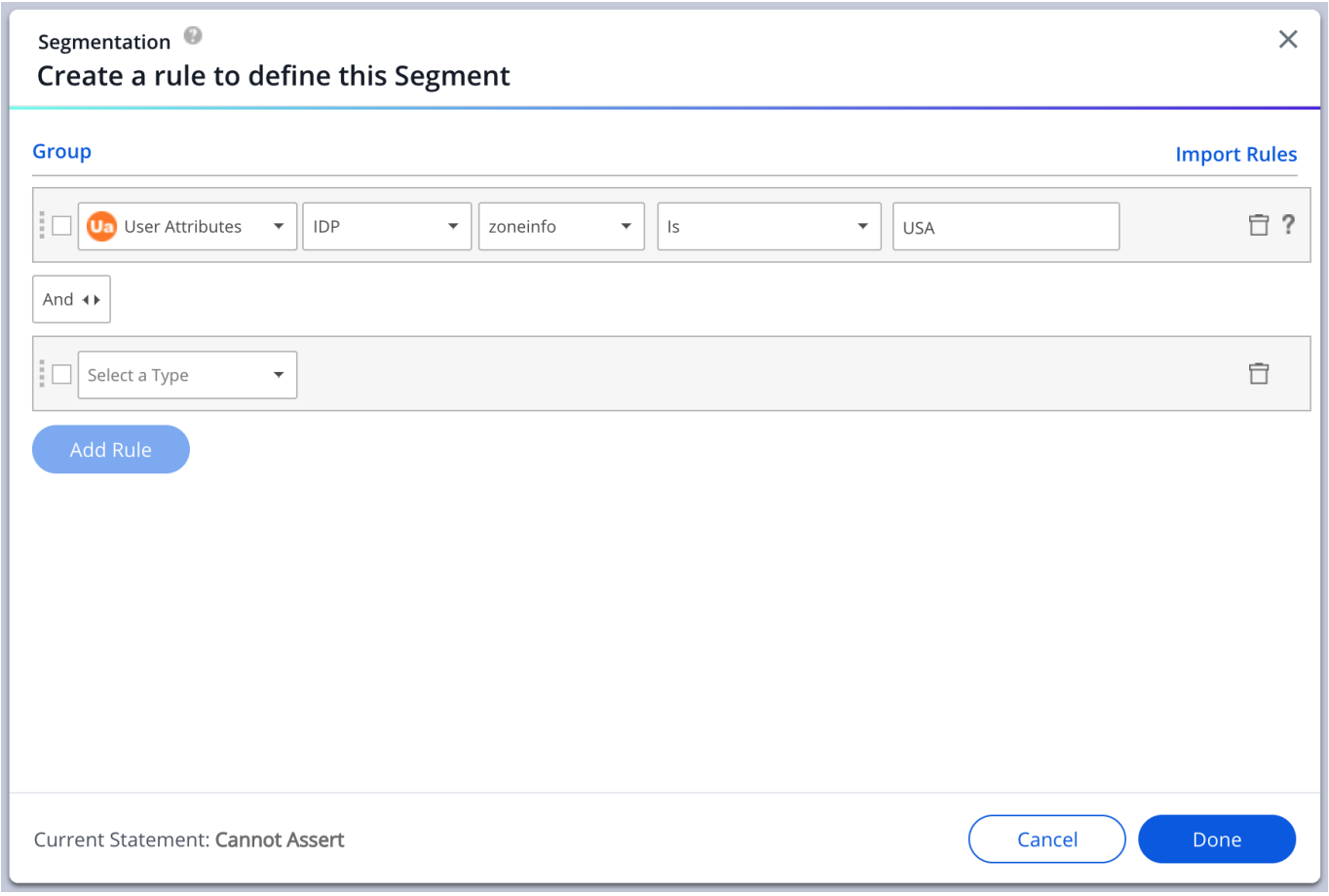
9. Klicken Sie auf „Finish“ (Beenden)

10. Es wird eine Meldung angezeigt, die Ihnen mitteilt, ob Ihr IDP erfolgreich hinzugefügt wurde oder nicht

Anmerkung:

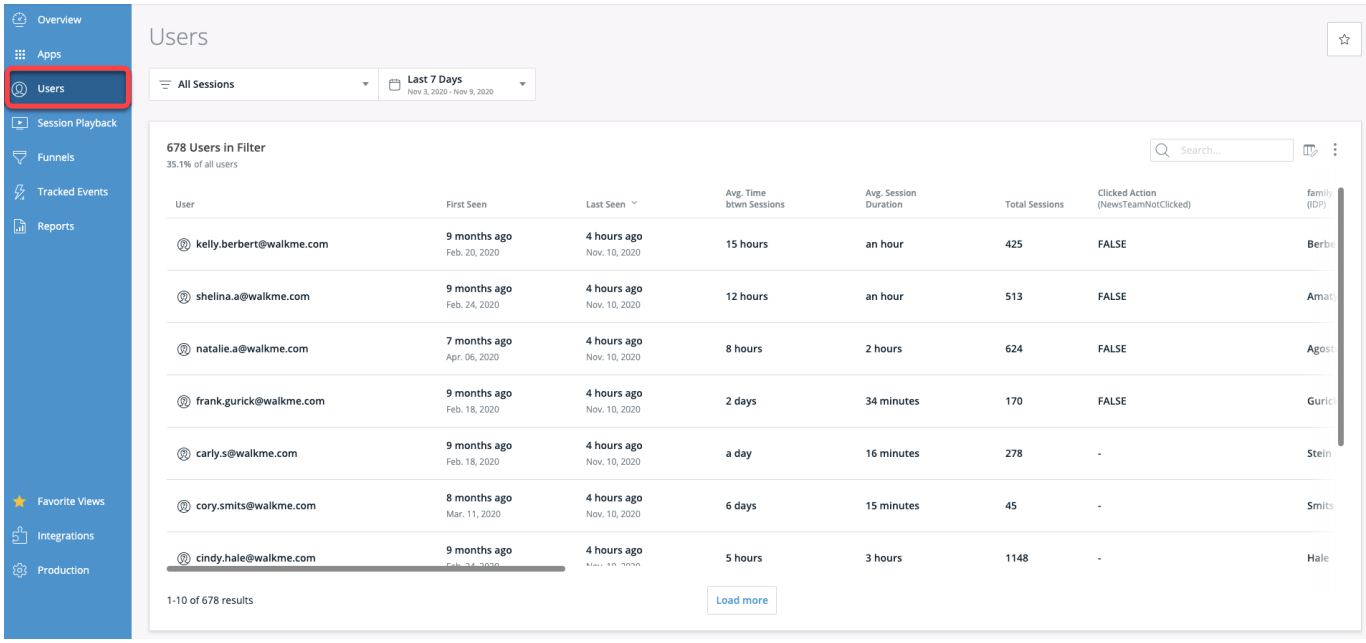
- Nach der Zuordnung von Systemen wird deren **UUID-Einstellung** automatisch auf IDP gesetzt und die Einstellungen werden veröffentlicht, sodass keine weiteren Maßnahmen erforderlich sind.
- Die einzige Möglichkeit, die UUID zu ändern, besteht darin, die Zuordnung des Systems zum Anbieter aufzuheben (siehe unten den Abschnitt **Manage System Assignment** (Verwaltung der Systemzuordnung)).

- Sie können nun anhand der importierten Attribute Inhalte segmentieren in Insights und im Editor unter User Attributes >IDP, mit den zum eingestellten Datenfeldtyp passenden Filterbedingungen.
- Lesen Sie hier mehr darüber.



Tipp:

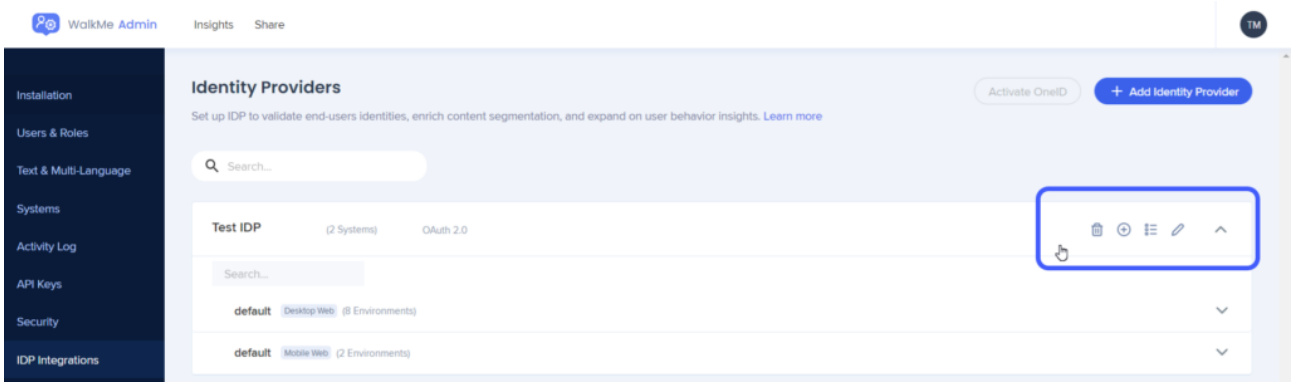
- Um zu validieren, dass die Benutzer von der Integration identifiziert und alle angeforderten Attribute erfasst werden, wird empfohlen, die Seite „Users“ (Benutzer) in **Insights** aufzurufen unter **insights.walkme.com**, wo alle Benutzerdaten angezeigt werden.
- Benutzer werden der Tabelle erst nach Beendigung ihrer Sitzung hinzugefügt, daher dauert es nach dem Einrichten von IDP einige Zeit, bis Benutzer in der Tabelle angezeigt werden.



So verwalten Sie einen Identity Provider

Wenn Sie den Mauszeiger über die Zeile eines Identity Providers bewegen, werden Ihnen mehrere Optionen angezeigt:

- Löschen
- Manage System Assignment (Verwalten der Systemzuordnung)
- Import Properties (Importieren von Eigenschaften)
- Bearbeiten
- Expand (Erweitern)



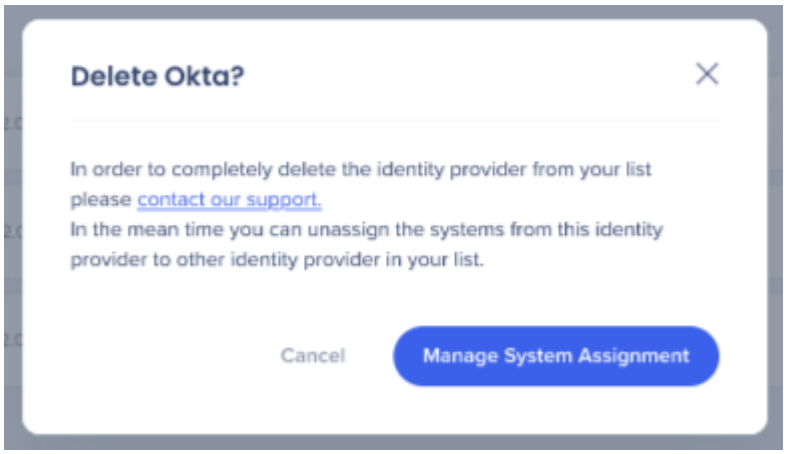
Löschen

- Klicken Sie auf das Papierkorbsymbol, um einen Identity Provider zu „löschen“

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

Wichtige Anmerkung:

- Es ist nicht möglich, einen Identity Provider vollständig zu löschen, ohne den Support zu kontaktieren.
- Bevor das Löschen möglich ist, muss der Identity Provider über den Bildschirm „Manage System Assignment“ (Systemzuordnung verwalten) von der Zuordnung zu Systemen gelöst werden.



Manage System Assignment (Verwalten der Systemzuordnung)

- Klicken Sie auf das Symbol „+“, um den Bildschirm „Manage System Assignment“ zu öffnen.
- Wählen Sie die Systeme aus, die Sie dem Identity Provider zuweisen möchten, oder heben Sie die Auswahl auf.
- Sie können auch umschalten auf „Enforce SSO“ (SSO erzwingen)
- Klicken Sie auf die Schaltfläche „Save Changes“ (Änderungen speichern), sobald Sie fertig sind

Anmerkung:

- Benutzer können keine Systemzuweisung für Anbieter verwalten, die keine importierten Eigenschaften haben. Eigenschaften müssen zuerst importiert werden.
- Nach der Zuordnung von Systemen wird deren **UUID-Einstellung** automatisch auf IDP gesetzt und die Einstellungen werden veröffentlicht, sodass keine weiteren Maßnahmen erforderlich sind.

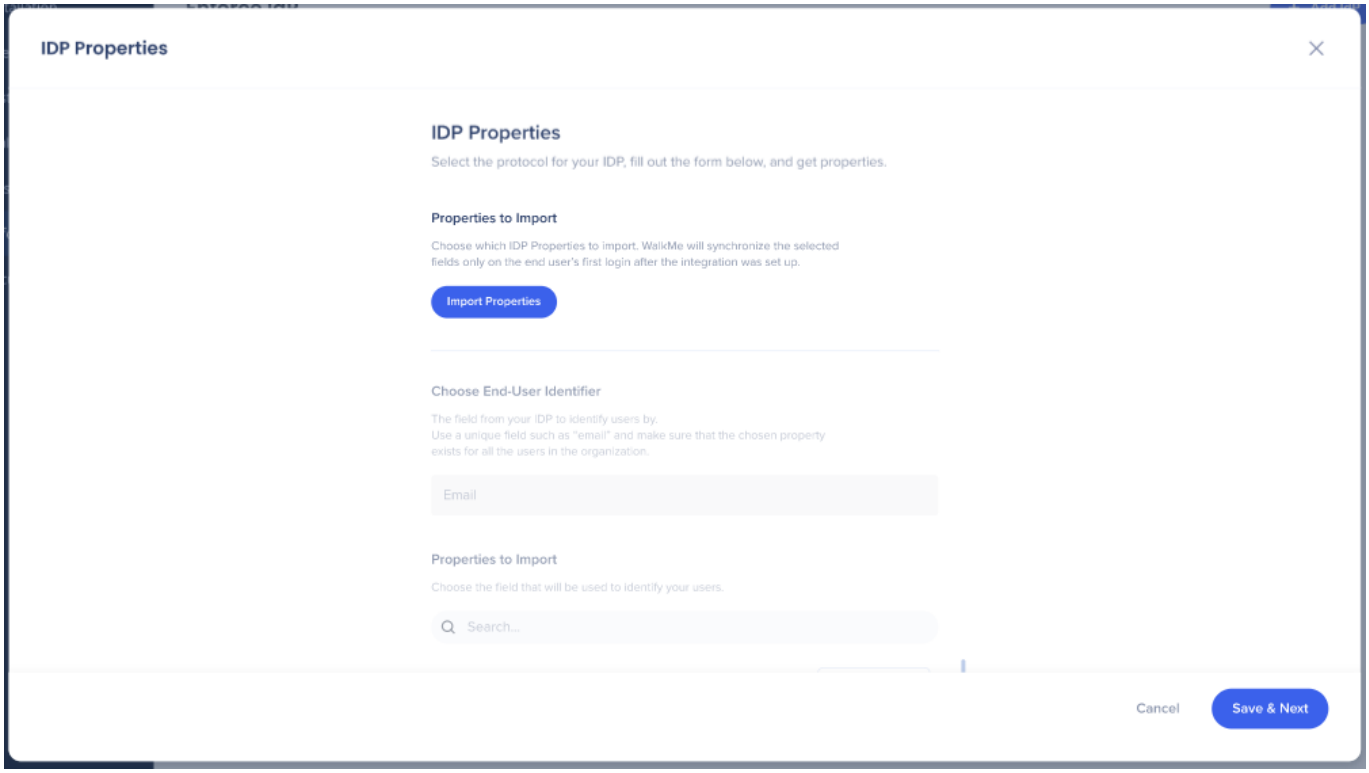
Import Properties (Importieren von Eigenschaften)

- Klicken Sie auf das Listensymbol und dann auf die Schaltfläche „Import Properties“, um zusätzliche importierte Eigenschaften zu bearbeiten oder hinzuzufügen.

Diese Attribute werden für die Segmentierung von Inhalten und die Berichterstattung in Insights verwendet.

Anmerkung:

- Dazu ist es erforderlich, sich als Benutzer zu authentifizieren, der auf Anbieterseite der WalkMe-Anwendung zugeordnet ist.

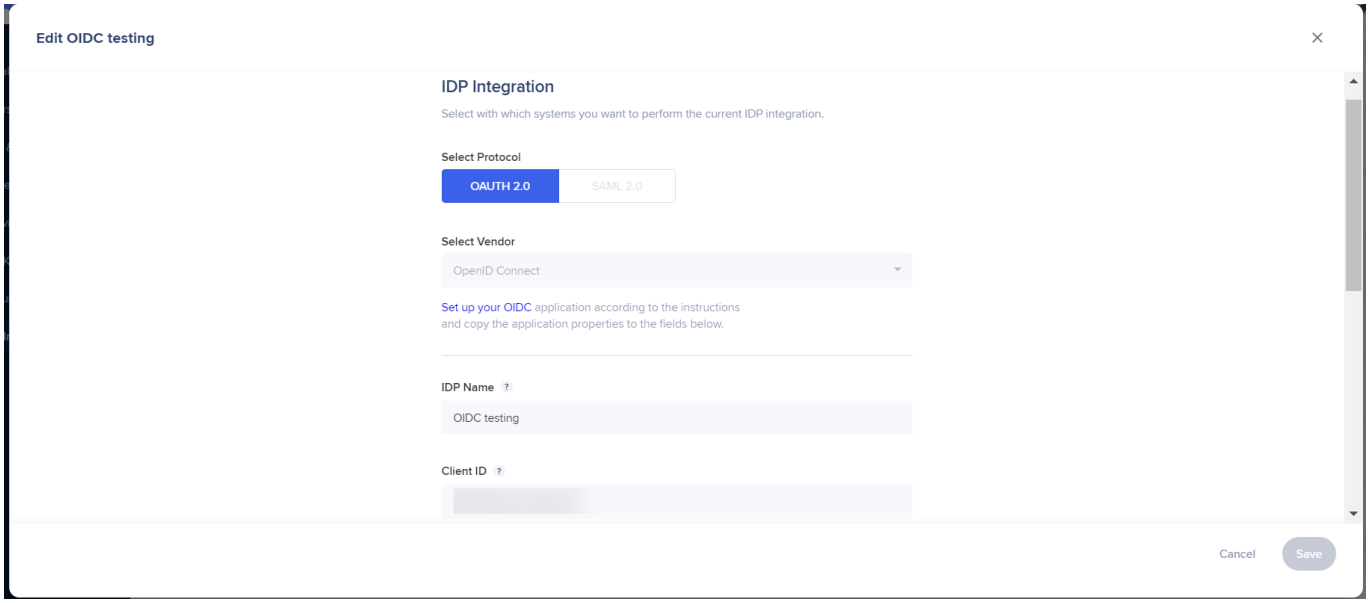


Bearbeiten

- Klicken Sie auf das Stiftsymbol, um die Einstellungen des Identity Providers zu bearbeiten
- Sie können alle Felder bearbeiten, die Sie bei der ersten Konfiguration des Identity Providers ausgefüllt haben

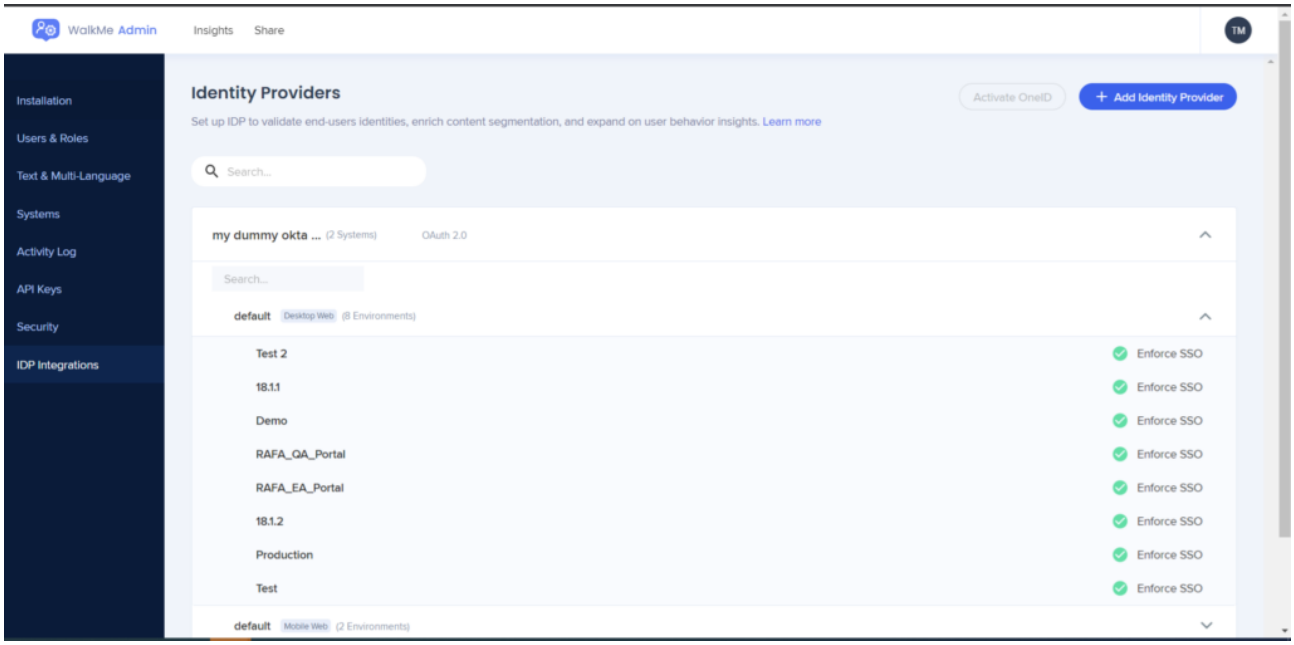
Anmerkung:

- Benutzer können keine Systemzuweisung für Anbieter verwalten, die keine importierten Eigenschaften haben. Eigenschaften müssen zuerst importiert werden.



Ansicht erweitern/verkleinern

- Verwenden Sie das Pfeilsymbol, um die erweiterte Ansicht zu öffnen oder zu schließen
- Im erweiterten Zustand sehen Sie alle Systeme, die einem Identity Provider zugewiesen sind, und ob „Enforce SSO“ aktiviert wurde oder nicht



Bewährte Verfahren

Konfiguration von „Enforce SSO“ (SSO erzwingen)

- Falls ***aktiviert*** – Die IDP-Authentifizierung muss erfolgen, bevor die Webseite für die Endbenutzer geöffnet wird. Wenn das IDP-Token nicht erkannt wird, werden die Endbenutzer auf ihre IDP-Anmeldeseite umgeleitet.
    - Jedes Mal, wenn Endbenutzer sich nicht bei der IDP authentifizieren können, z. B. weil der IDP ausgefallen ist, die Kunden ihre Anmeldedaten vergessen haben oder die Endbenutzer nicht der IDP-Anwendung zugewiesen wurden, wird SSO für eine Stunde deaktiviert und die Benutzerkennung wird automatisch auf die „WalkMe-ID“-Methode als Ausweichmöglichkeit herunterskaliert, oder WalkMe wird nicht geladen, je nach Konfiguration der Kunden.
    - Nach einer Stunde – Wenn das IDP-Token immer noch nicht erkannt wird, werden die Endbenutzer erneut auf ihre IDP-Anmeldeseite weitergeleitet. Andernfalls ist eine Anmeldung bei der IDP nicht erforderlich. Es ist wichtig, dass das für die Kunden absolut klar verständlich passiert. Andernfalls sollten Sie diese Option NICHT aktivieren.
- Falls ***deaktiviert*** – Die IDP-Authentifizierung wird beim Laden der Seite versucht, aber wenn es kein aktives Token für den IDP gibt, werden Endbenutzer nicht zum IDP weitergeleitet. Der User Identifier wird automatisch auf die Methode „WalkMe-ID“ herunterskaliert oder WalkMe wird nicht geladen, je nach Konfiguration der Kunden.

Einschränkungen

- **Wichtig:** Das Ändern des User Identifier hat Auswirkungen auf die Art, wie WalkMe die Endbenutzer identifiziert und kann die „Play once“ (Einmal abspielen)-Konfigurationen zurücksetzen.

Bitte beachten Sie, dass die Änderung des User Identifier Auswirkungen auf die Art hat, wie WalkMe die Endbenutzer identifiziert, wenn Ihre Implementierung bereits in Betrieb ist. Dies kann dazu führen, dass Auto-Play-Regeln zurückgesetzt werden (z. B. Einstellungen für „Einmal abspielen“) oder dass Benutzer ihre zuvor abgeschlossenen Onboarding-Aufgaben als unvollständig markiert sehen, weil ihre „Unique User Identifier“ (eindeutige Benutzerkennung) (UUID) geändert wurde. Es gibt keine Möglichkeit, diese Einschränkung zu umgehen, da jeder Benutzer als neuer Benutzer erkannt wird, der an seinen neuen UUID-Wert gebunden ist.

- Der Safari-Browser unterstützt keinen IDP
- Benutzer sollten Administratorenberechtigungen für das Admin Center haben
- IDP muss auf dem erforderlichen System konfiguriert werden
- Endbenutzer sollten den IDP verwenden, um sich für dieses System zu authentifizieren
- Wenn Ihr Unternehmen eine aktive CSP (Content Security Policy) hat, blockiert es Anrufe an den IDP-Anbieter
    - Um dies zu umgehen, sollte die richtige URL in den CSP-Einstellungen der Erweiterungskonfiguration hinzugefügt werden

- Nach der Zuordnung von Systemen wird die **UUID-Einstellung** für die zugewiesenen Systeme automatisch auf IDP gesetzt und die Einstellungen werden veröffentlicht, sodass keine weiteren Maßnahmen erforderlich sind.
    - Damit die IDP-Änderungen wirksam werden, müssen die Systeme der Kunden auf die neueste WalkMe-Version aktualisiert werden (das kann durch Veröffentlichung der Einstellungen erreicht werden)
    - Bei Enterprise-Konten müssen Sie beim Veröffentlichen „Update to the latest WalkMe version“ (auf die neueste WalkMe-Version aktualisieren) einschalten

Mobile Web:

- Mobile Web wird automatisch aktiviert, nachdem die IDP-Einrichtung abgeschlossen ist
- Mobile Web wird hinzugefügt, nachdem der IDP / die OneID bereits aktiviert wurde. Die Benutzer müssen IDP für den Support von Mobile Web deaktivieren und dann wieder aktivieren

[/ht_message][/ht_message]