IDP-Integration

Kurzübersicht

Identitätsdienstleister speichern und verwalten digitale Identitäten und bieten Unternehmen so eine Möglichkeit, Zugang und Nutzungsberechtigungen zu verwalten, bei gleichzeitiger Einhaltung hoher Sicherheitsstandards.

IDP-Integration kann genutzt werden, um anhand dieser Informationen die Identität von Endnutzern zu validieren, die Möglichkeiten der Inhaltssegmentierung zu bereichern oder die Beobachtung des Nutzerverhaltens zu erweitern. Bereitstellung einer zuverlässigen und sicheren Benutzer-ID für jedes System, ohne die Notwendigkeit, die eindeutige Benutzer-ID für jedes System mit verschiedenen Variablen zu definieren.

Die Verwendung von IDP zur Benutzeridentifizierung sollte die primär zu wählende Lösung sein für alle neuen Systeme.

IDP-Integrationen sind vom **Admin Center** aus unter **admin.walkme.com** zugänglich.

Digital Adoption Institute

- Sehen Sie sich die Lektion ***Configure Analytics, Integrations, and Design* im Kurs** *Digital Adoption Project Management Fundamentals* an.
- Sie haben noch kein DAI-Konto? Melden Sie sich hier an.

Verbunden

- 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

Unterstützte Plattformen

Die IDP-Integration von WalkMe unterstützt die Verwendung mehrerer Authentifizierungsprotokolle, einschließlich **OAuth 2.0**, **OpenID Connect** und **SAML**, um Benutzer bei dem IDP-Anbieter ihrer Organisation zu authentifizieren und Benutzer-Attribute zu erhalten, die später bei der Segmentierung und Analyse in WalkMe eingesetzt werden können. Jeder IDP-Anbieter, der diese Protokolle unterstützt, sollte auch mit WalkMe funktionieren. WalkMe unterstützt den vom SP initiierten Fluss.

Was ist OAuth 2.0?

OAuth 2.0 steht für „Open Authorization“, ein Standard, der einer Website oder Anwendung Zugriff auf Ressourcen gewährt, die von anderen Web-Anwendungen für Benutzer gehostet werden. Das Protokoll OAuth 2.0 ist gegenwärtig der Branchenstandard für die Autorisierung.

Was ist OpenID Connect?

OpenID Connect ist eine einfache, dem Protokoll OAuth 2.0 aufgesetzte Identitätsebene, die es Rechen-Clients ermöglicht, auf Basis der durch einen Autorisierungs-Server durchgeführten Authentifizierung die Identität von Benutzern zu verifizieren und Grunddaten des Benutzerprofils zu erhalten, alles auf interoperable und REST-artige Weise.

Die IDP-Integration unterstützt gegenwärtig folgende Anbieter:

- **Okta**
- **G-Suite**
- **ADFS**
- **AzureAD**
- **PingID**
- Identitätsanbieter, die **OpenID** verwenden

Abgesehen von OpenID Connect ist SAML das üblichste Authentifizierungsprotokoll. Anweisungen zur Erstellung und Einrichtung einer Integration von SAML finden Sie in unserem Artikel Integration von SAML.

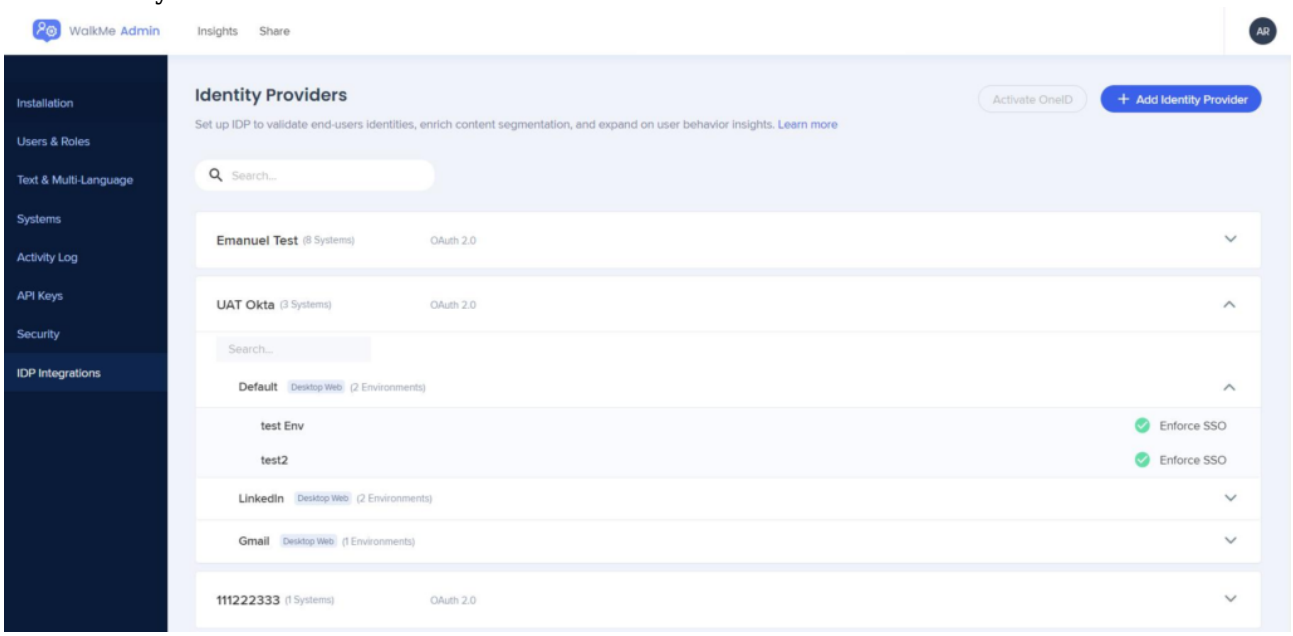
Voraussetzungen

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

Im Konfigurationsbildschirm des Admin Centers ist für alle unterstützten Systeme eine Anleitung verfügbar.

So fügen Sie einen Identitätsanbieter hinzu

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

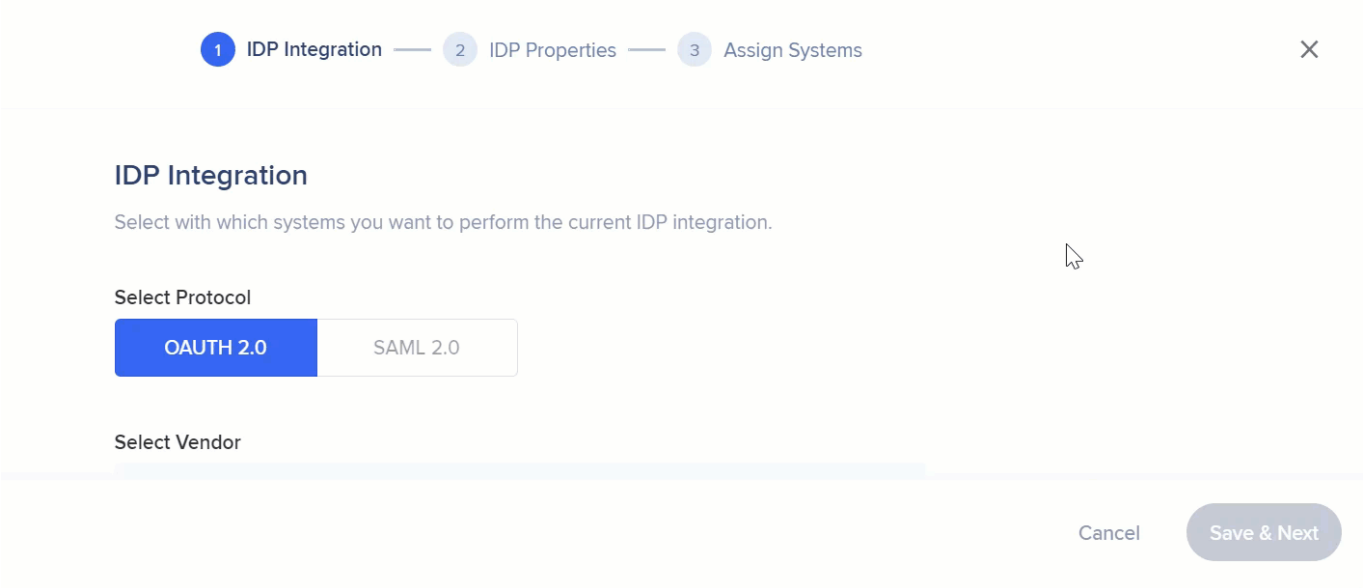


2. Wählen Sie das Protokoll OAuth 2.0 aus

3. Geben Sie die passenden Konfigurationseinstellungen für die Verbindung an

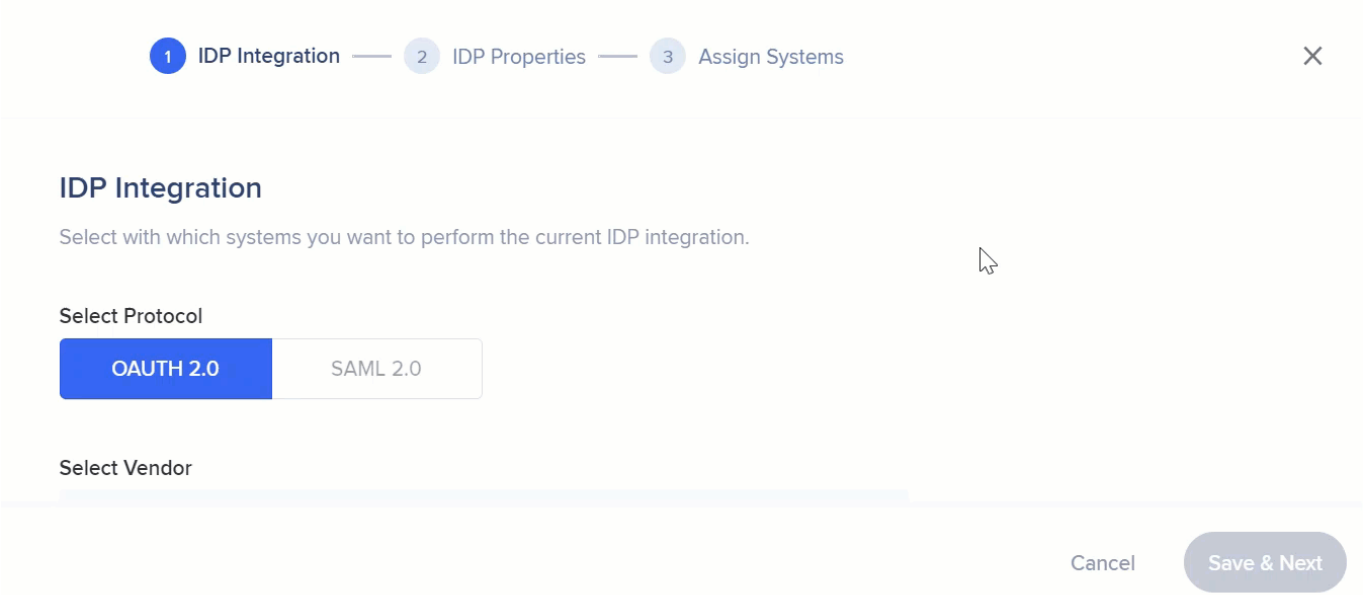
1. **IDP vendor** – Wählen Sie einen Anbieter aus der Liste aus
2. **IDP Name** – Verbindungsname
3. **Client ID** – Öffentlicher Identifikator für Apps
4. **Client Secret** – Eine geheime Angabe, die nur der Anwendung und dem Autorisierungs-

Server bekannt ist
5. **IDP Provider Domain** – Domäne Ihrer Organisation



Anmerkung: Die Felder können je nach gewähltem IDP-Anbieter variieren.

- **Für OpenID Connect:**
  1. **IDP vendor** – Wählen Sie OpenID Connect aus der Liste „Oath2.0 vendor“ aus
  2. **IDP Name** – Verbindungsname
  3. **Client ID** – Öffentlicher Identifikator für Apps
  4. **Client Secret** – Eine geheime Angabe, die nur der Anwendung und dem Autorisierungs-Server bekannt ist
  5. **IDP Provider Discovery URL – Dicovery URL des IDP-Anbieters**
  6. **IDP Provider Scope – Bereichsumfang beim IDP-Anbieter**
  7. **Content Security Policy – Vorgaben für die Inhaltssicherheit**
  8. **Ihr IDP-Anbieter**
  9. **Use ID Token For Getting End-Users Properties** – Verwendung des ID-Tokens zum Einholen der Endnutzereigenschaften. Verwenden Sie den Schalter, um dies zu aktivieren.



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

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

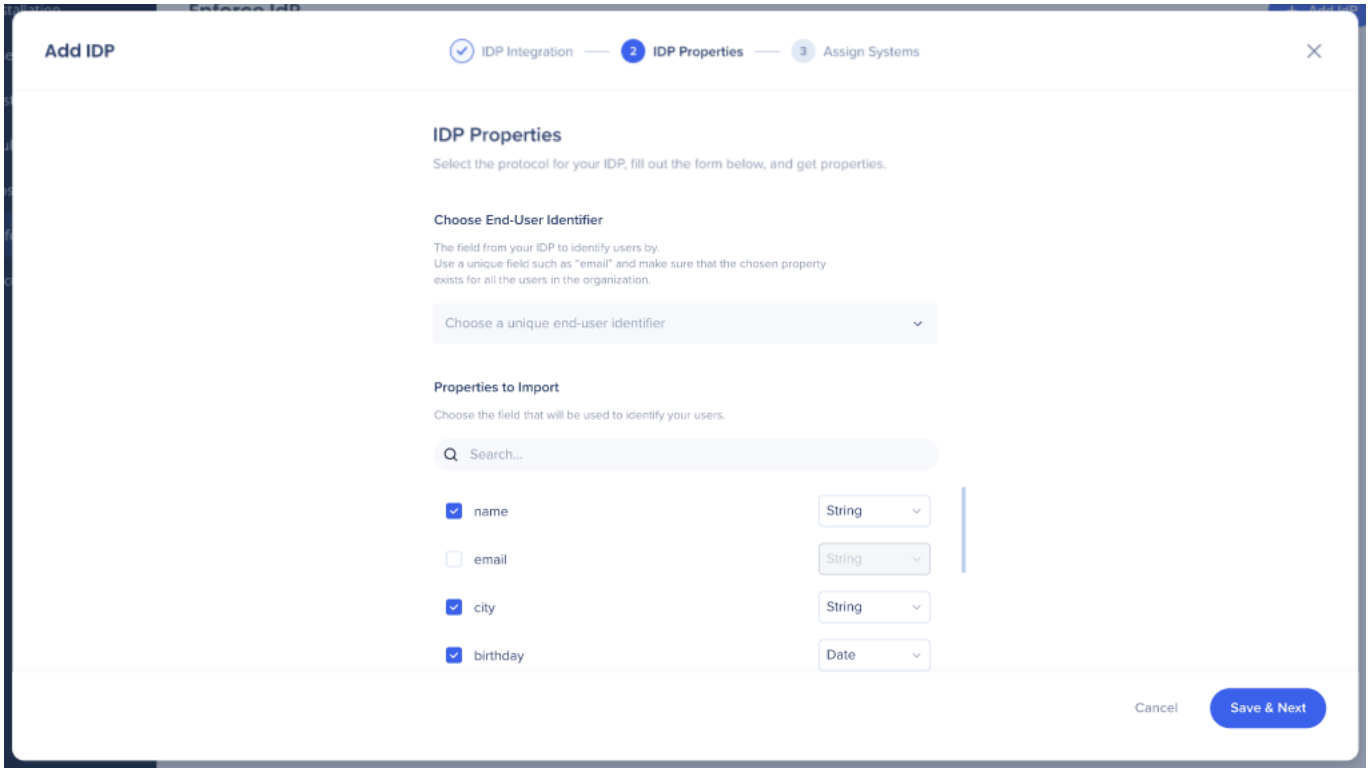
5. Wählen Sie einen eindeutigen Endbenutzerkenner, um die Benutzer zu identifizieren

- 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:

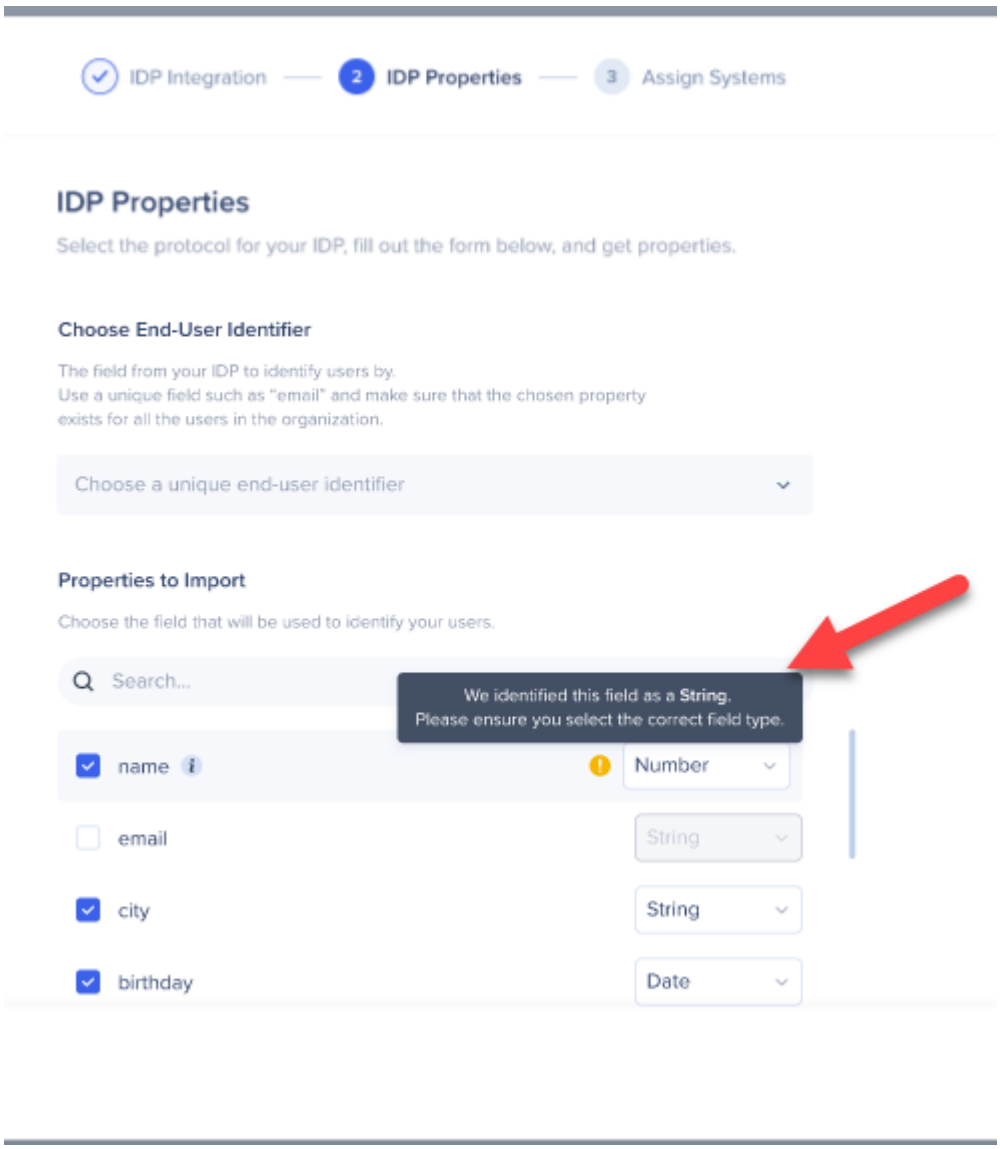
1. String (Zeichenfolge)
2. Number (Nummer)
3. Date (Datum)

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

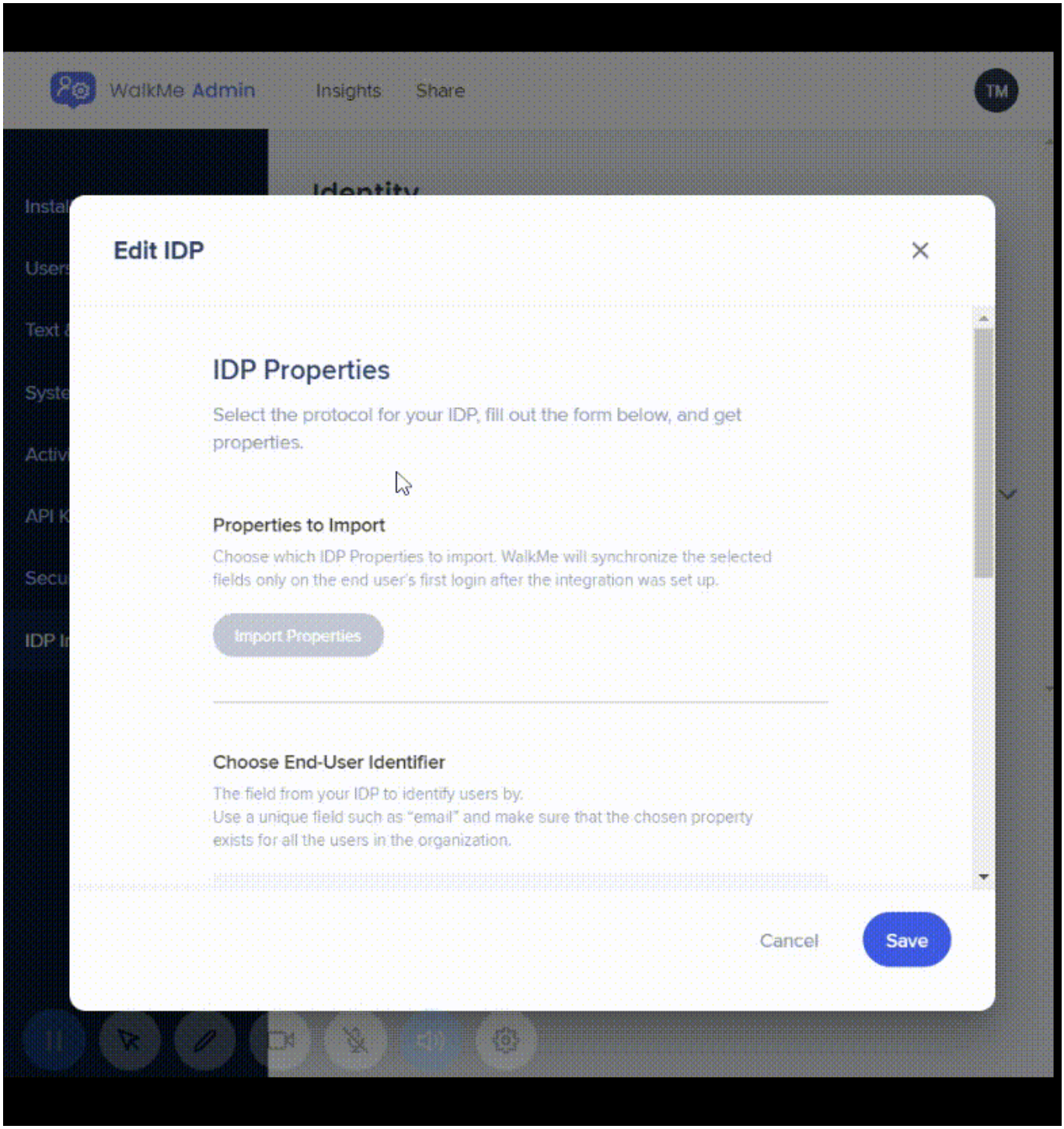


Tipp:

- 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.



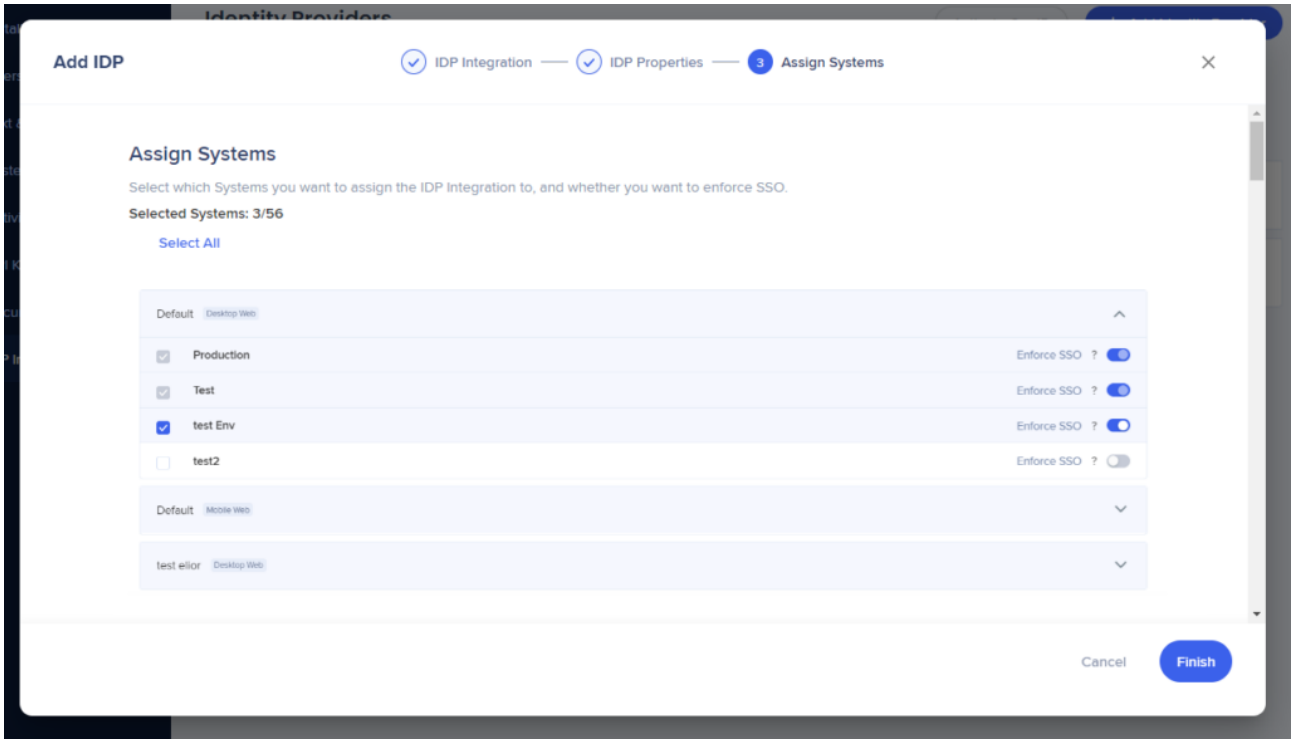
Sie können auch jede ausgewählte Eigenschaft umbenennen, ihren ursprünglichen Wert und Namen anzeigen und zu ihrem ursprünglichen Wert zurückkehren, wenn sie überschrieben wird.



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.

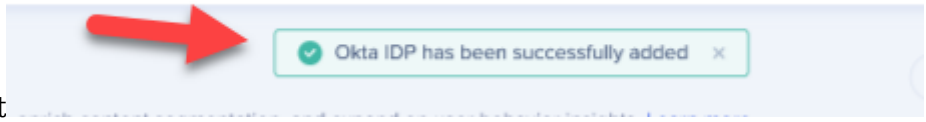


Anmerkung:

- 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)

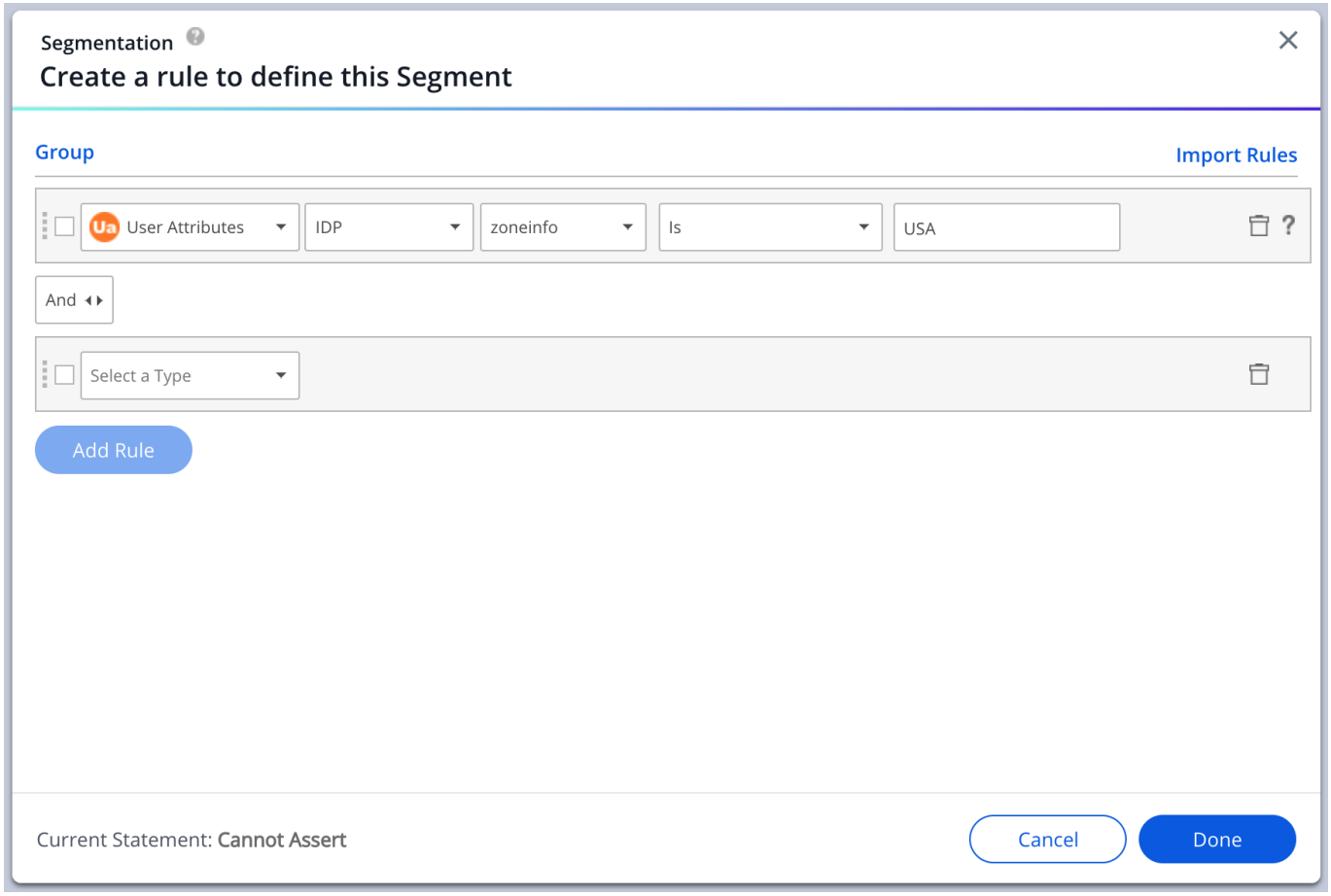
10. Es wird eine Meldung angezeigt, die Ihnen mitteilt, ob Ihre IDP erfolgreich hinzugefügt wurde oder nicht



Anmerkung:

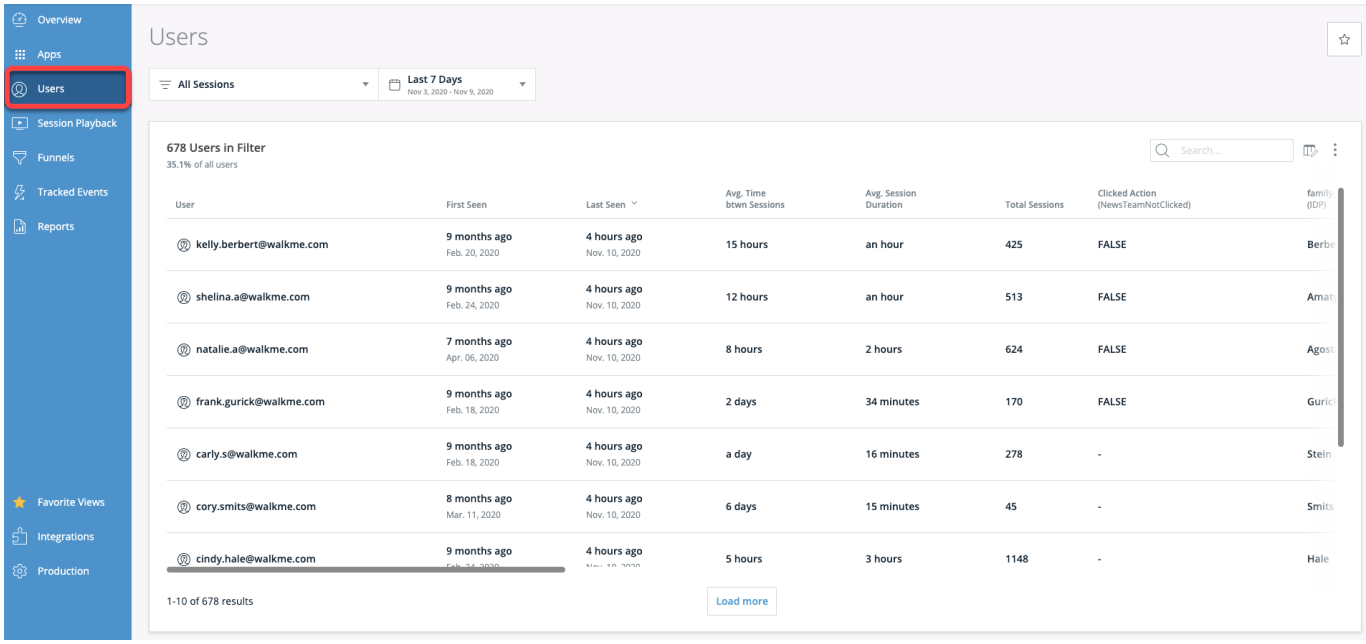
- Nach der Zuordnung von Systemen wird deren **UUID-Einstellung** automatisch auf IDP gesetzt und die Einstellungen werden veröffentlicht, sodass keine weiteren Maßnahmen erforderlich sind.
- Die einzige Möglichkeit, die UUID zu ändern, besteht darin, die Zuordnung des Systems zum Anbieter aufzuheben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

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



Tipp:

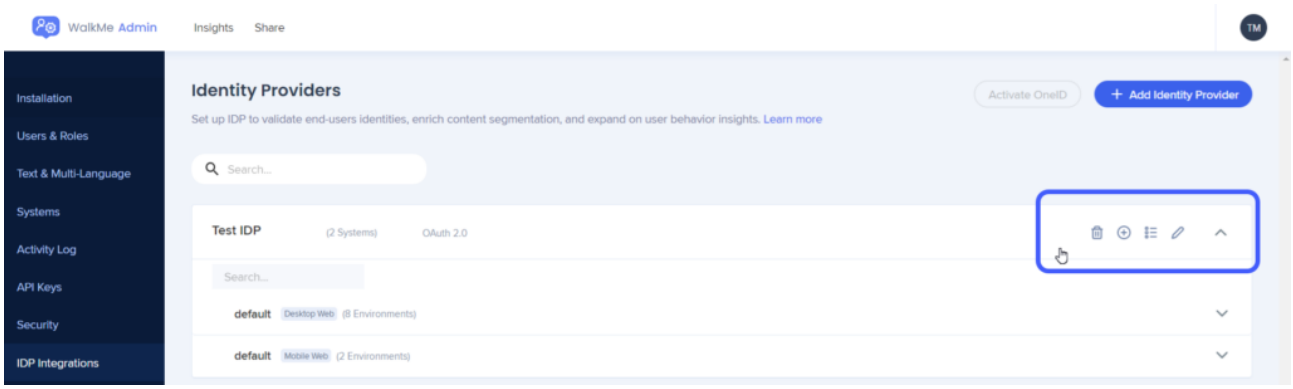
- Um zu validieren, dass die Benutzer von der Integration identifiziert und alle angeforderten Attribute erfasst werden, wird empfohlen, die Seite „Users“ (Benutzer) in **Insights** aufzurufen unter **insights.walkme.com**, wo alle Benutzerdaten angezeigt werden.
- Benutzer werden der Tabelle erst nach 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
- Erweitern

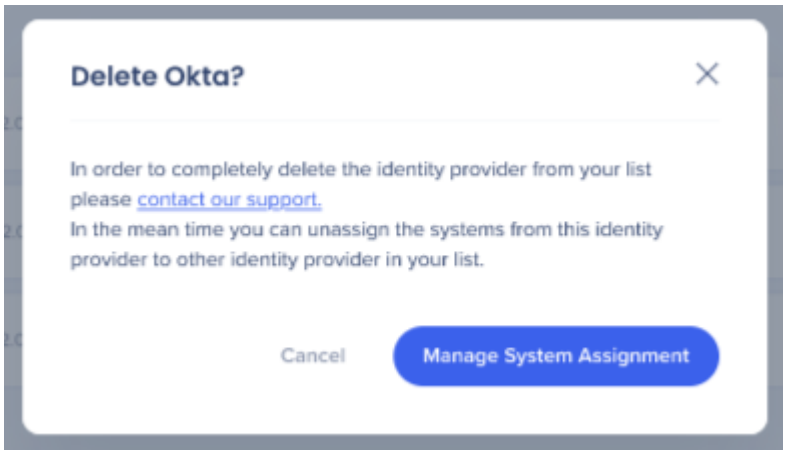


Löschen

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

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.



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 Lieferanten verwalten, die keine importierten Eigenschaften haben. Eigenschaften müssen zuerst importiert werden.
- Nach der Zuordnung von Systemen wird die **UUID setting** (UUID-Einstellung) für die zugewiesenen Systeme automatisch auf IDP gesetzt und die Einstellungen werden veröffentlicht, sodass keine weiteren Maßnahmen erforderlich sind.

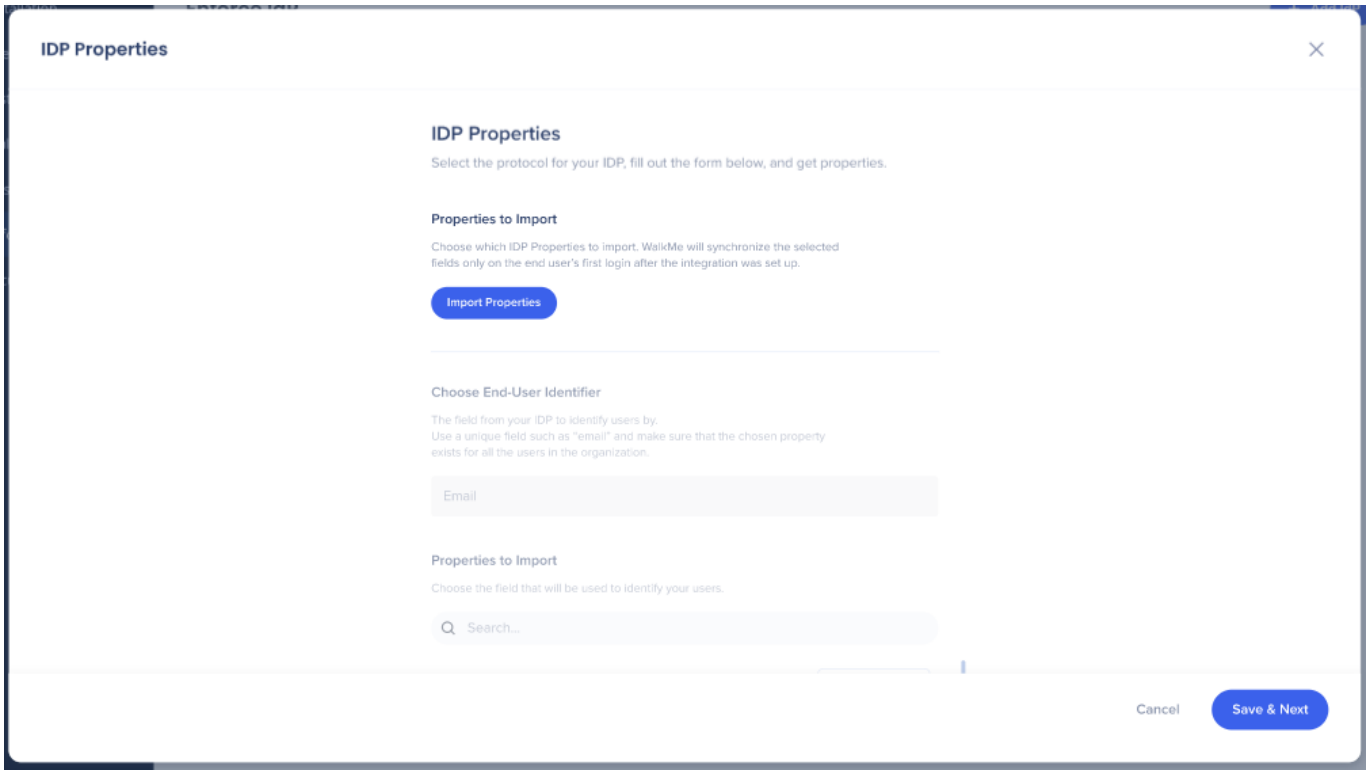
Import Properties (Importieren von Eigenschaften)

- 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 mit einem Benutzer zu authentifizieren, der auf der Anbieterseite der WalkMe-App zugewiesen ist.

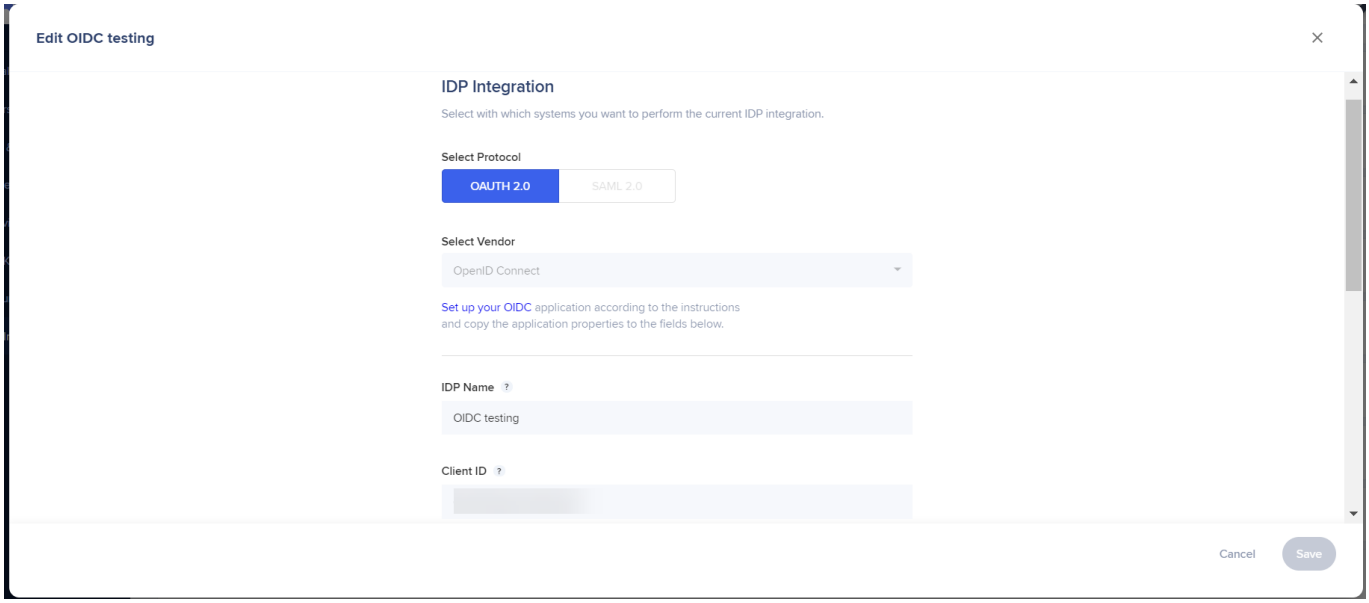


Bearbeiten

- 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 Lieferanten 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)

- Wenn ***aktiviert*** – Die IDP-Authentifizierung muss erfolgen, bevor die Webseite für den Endbenutzer geöffnet wird. Wenn das IDP-Token nicht erkannt wird, wird der Endbenutzer auf seine IDP-Anmeldeseite umgeleitet.
    - Jedes Mal, wenn der Endbenutzer sich nicht bei der IDP authentifizieren kann, z. B. weil die IDP ausgefallen ist, der Kunde seine Anmeldedaten vergessen hat oder der Endbenutzer nicht der IDP-App zugewiesen wurde, 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 des 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 dies für den Kunden absolut klar ist. 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 des Kunden.

Einschränkungen

Wichtig: Bitte beachten Sie, dass eine Änderung von User Identifier die Art und Weise beeinflusst, wie WalkMe Endbenutzer identifiziert, wenn Ihre Implementierung bereits aktiv 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.

- Die Browsererweiterung für Safari wird nicht mit IDP unterstützt.
- Wichtig: Das Ändern des User Identifier hat Auswirkungen auf die Art, wie WalkMe die Endbenutzer identifiziert und kann die Konfigurationen von „Play once“ zurücksetzen.

- 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
- Beim Import einer Datums-Eigenschaft werden nur die folgenden Formate unterstützt:
    - 2018-02-20
    - 2018-02-20T14:32:00
    - 12/30/2018
    - Der Import einer Zeichenfolge oder Nummer als Datum funktioniert bei der Insights-Filterung/Editor-Segmentierung nicht.

Mobile Web:

- Mobile Web wird automatisch aktiviert, nachdem die IDP-Einrichtung abgeschlossen ist
- Wenn Mobile Web hinzugefügt wird und der IDP / OneID bereits aktiviert ist, müssen die Benutzer die Unterstützung des IDP für Mobile Web deaktivieren und erneut aktivieren

Lösen häufiger Probleme

Benutzer wird nicht zugewiesen

Um dies zu verhindern, müssen alle Mitarbeiter WalkMe zugewiesen werden. Der IT-Mitarbeiter in Ihrem Unternehmen sollte Ihnen dabei helfen können, indem er die Zugriffseinstellungen für die **WalkMe-App** in Ihrem IDP-Anbieter für alle Mitarbeiter ändert.

EUID wurde im Benutzerprofil nicht gefunden

Um dies zu beheben, können Sie entweder eine andere EUID auswählen, die allen WalkMe zugewiesenen Mitarbeitern zur Verfügung steht, oder Sie können die fehlenden Informationen individuell für die entsprechenden Benutzer hinzufügen.

Abgelaufener Client/geheime Schlüssel

Wenn der Schlüssel abgelaufen ist, müssen Sie ihn neu erstellen und dann die neuen Schlüssel in der entsprechenden IDP auf der Seite **IDP-Integrationen** im WalkMe Admin Center aktualisieren.

Ungültiger Client/geheime Schlüssel

Stellen Sie sicher, dass Sie die richtigen Schlüssel kopiert haben, und fügen Sie sie dann in die entsprechende IDP-Verbindung auf der IDP-**Integrationsseite** im WalkMe Admin Center ein.