

LinkedIn ラーニングシングルサインオン 実装ガイド

2021 年 6 月 18 日

この文書の内容

以下の手順では、LinkedIn ラーニングの SSO の実装プロセスについて説明します。

1. LinkedIn ラーニングで
SSO (SAML、LTI、Google) を設定します。



2. IdP に接続して、.xml ファイルをダウンロードします。



3. IdP に接続して、SSO を有効にします。



4. ユーザーライセンスを自動的に割り当てて、
ユーザー属性を管理します。



5. 以上で操作は完了です。受講者は、
1 つ以上の SSO 方法で、LinkedIn ラーニングコンテンツに
アクセスできるようになりました。



SSO 実装の概要

組織アカウントの管理者は、LinkedIn のエンタープライズプラットフォームに統合されている SSO を使用して LinkedIn ラーニングの認証を受けるように会社を設定できます。

前提条件

- 会社のメールアカウント
- 完全な管理者権限
- ID プロバイダー (IdP) 管理者権限

シングルサインオン (SSO) について

エンタープライズシングルサインオン (SSO) により、自社の従業員が個人の LinkedIn 認証情報の代わりに会社の認証情報を使用して、サポートされる LinkedIn アプリケーションにサインインすることができます。

LinkedIn アプリケーションを使用する場合、SSO の使用や SSO プロバイダーとの統合は必要ありません。SSO が設定されていない場合、従業員は現在利用中の個人の LinkedIn 認証情報を使用して認証するか、メンバーアカウントを新規作成できます。

シングルサインオンを使用する理由

- 会社の既存の認証を活用する
- 自社の従業員が個人アカウントではなく、会社で設定したパスワードプロトコルを使用することで、セキュリティが向上する
- 従業員の退職時のユーザー管理を簡素化する

サポートされている SSO プロトコル

現在サポートされているのは、SAML 2.0、[LTI](#) 1.0、1.1、および [Google SSO](#) です。

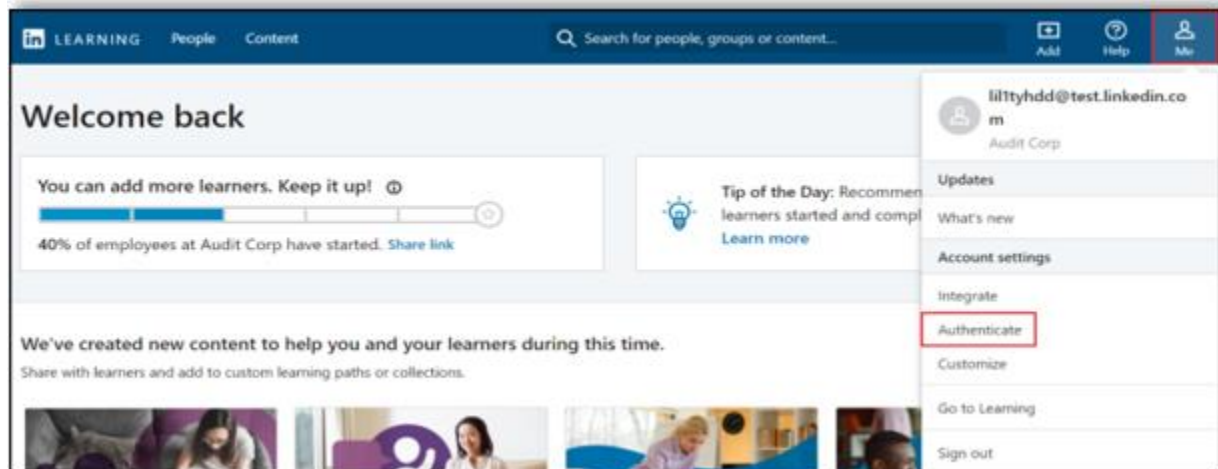
SSO (シングルサインオン) の設定

LinkedIn ラーニングの SSO を設定するには、以下の手順を実行します。

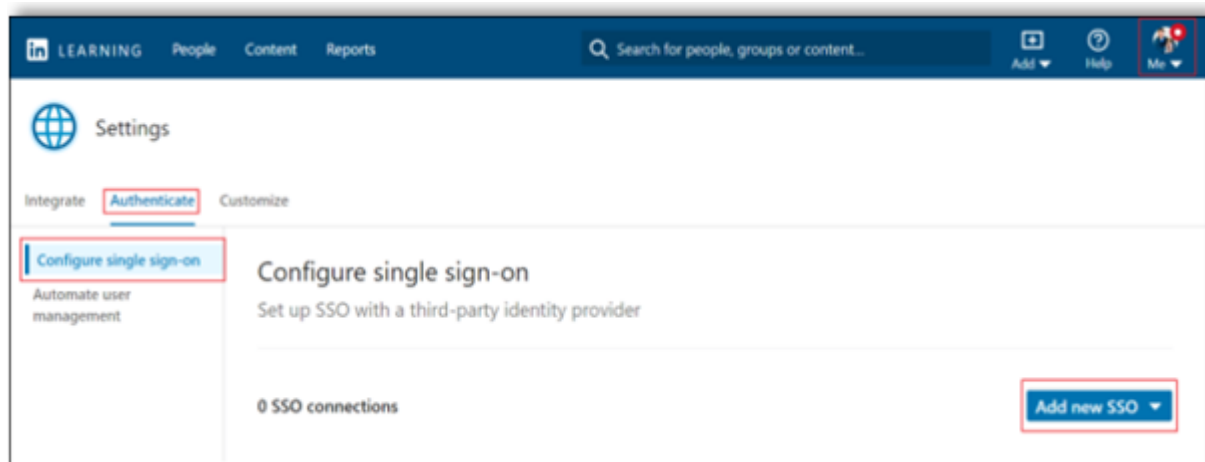
SSO の開始

SSO 設定を開始するには、次の手順を実行します。

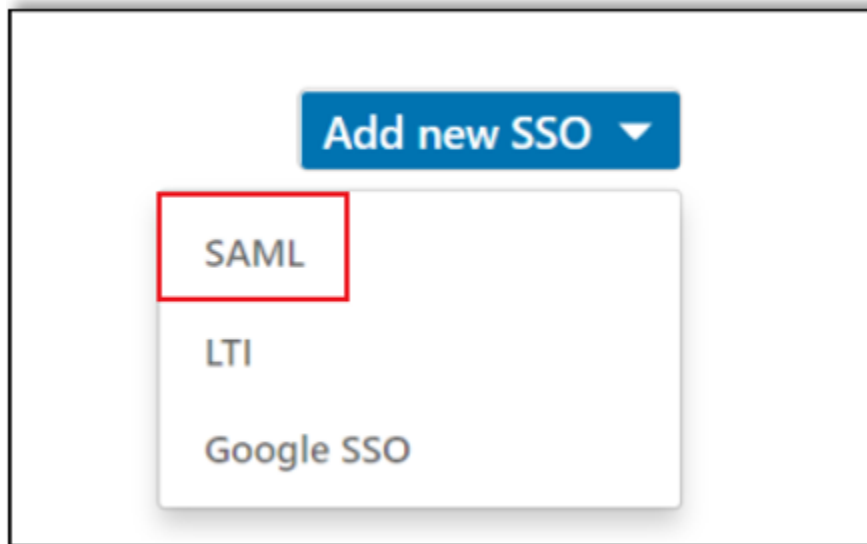
1. ログインした後、[管理者] 画面が表示されていない場合は、[管理者ページ] > [プロフィール] > [認証] の順に選択します。



2. サイドナビゲーションメニューから [シングルサインオンの設定] を選択し、[新規 SSO を追加] をクリックします。



3. SSO 方法を 1 つ選択します (この場合は「SAML」)。



4. SSO 接続に名前を付けます。

A screenshot of a configuration window titled 'Authenticate users with SAML SSO' with a close button (X) in the top right corner. The window has three tabs: 'Basics' (highlighted with a red box), 'Identity provider settings', and 'SSO settings'. Under the 'Basics' tab, there is a text input field for 'SAML Connection Name' with a help icon (i) to its right. The field contains the text 'SAML-1' and has a character count '6/50' to its right. Below this is a toggle switch for 'Automatically provision licenses' with the text 'Grant licenses to your learners automatically when they click an activation link.' and the label 'Off'. At the bottom right of the window are two buttons: 'Cancel' and 'Next' (highlighted with a red box).

5. [次へ] をクリックし、[こちら](#)に表示される手順に従います。

6. [SSO の設定] で、SSO オプションを選択します。

- AuthnRequest 署名:
 - はい

- いいえ (デフォルト)
- SAML リクエストバインディング:
 - HTTP リダイレクト (デフォルト)
 - HTTP-Post
- アサーションコンシューマーサービスの URL を含める:
 - はい
 - いいえ (デフォルト)
- 認証リクエスト署名アルゴリズム:
 - SHA1 (デフォルト)
 - SHA256
- AuthnContextClassRef - 使用する値が不明の場合は、「デフォルト値 (この値を送信しません)」を使用します。

7. [保存] をクリックします。

Sign AuthnRequest
☒ No (default) ☐ Yes

Include Assertion Consumer Service URL
☒ No (default) ☐ Yes

AuthnContextClassRef
Don't send this value (default) ▼

SAML Request Binding
☒ HTTP-Redirect (default) ☐ HTTP-Post

Authentication Request Signing Algorithm
☒ SHA1 (default) ☐ SHA256

Cancel Save

ID プロバイダーへの接続

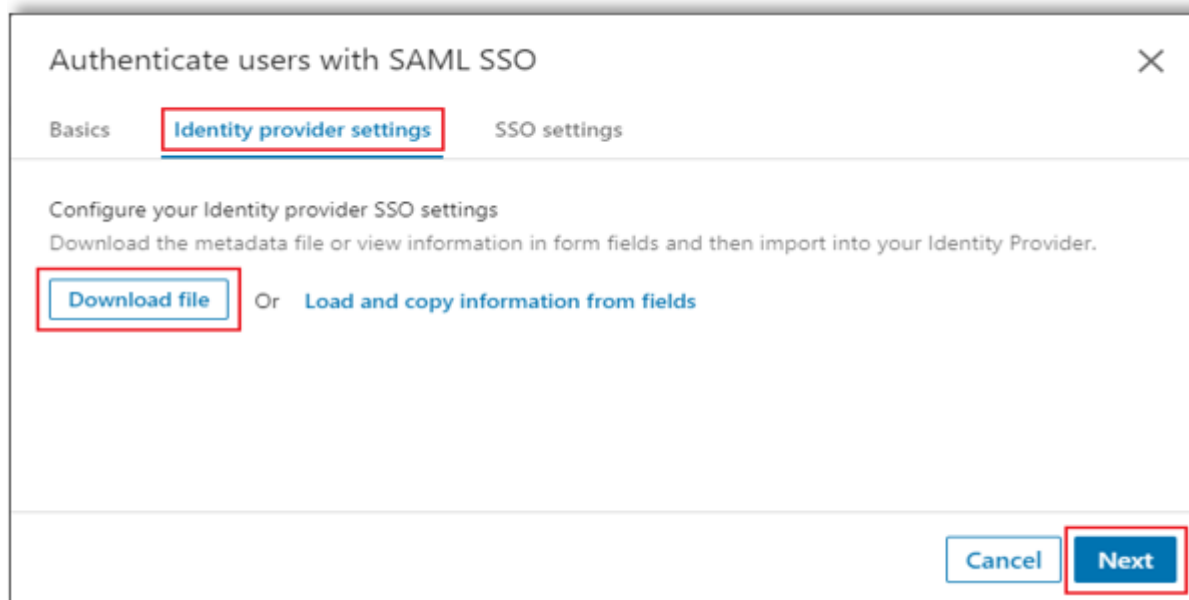
ID プロバイダーがメタデータの読み込みをサポートしている場合、XML 設定ファイルをダウンロードして ID プロバイダーに送信できます。ID プロバイダーは、LinkedIn ラーニングに接続するための設定を指定して、XML 設定ファイルをアップロードできます。

メタデータファイルをダウンロードできるかどうか、または各フィールドで作業する必要があるかどうかを確認し、次のセクションのいずれかの手順を実行します。

ファイルのダウンロード

メタデータファイルを使用して IdP を設定するには、次の手順を実行します。

1. [ID プロバイダー設定] タブで、[ファイルをダウンロード] をクリックして、ID プロバイダーシステムで使用できるメタデータファイルをダウンロードします。 metadata.xml ファイルがコンピューターにダウンロードされます。



2. ID プロバイダーシステムにアクセスします。
3. メタデータファイルをアップロードします。

注: このファイルは、ID プロバイダーにインポートできない場合があります。例えば、Okta にはこの機能はありません。構成要件に一致する場合は、[各フィールドでの操作](#)を続行します。

4. [次へ] をクリックします。

詳しくは、[ID プロバイダーの設定](#)を参照してください。

各フィールドでの操作

LinkedIn ラーニングアプリケーションインターフェイスの各フィールドで IdP を設定するには、次の手順を実行します。

1. [ID プロバイダー設定] タブで、[フィールドから情報を読み込んでコピー] をクリックします。

The screenshot shows a configuration window titled "Authenticate users with SAML SSO". It has three tabs: "Basics", "Identity provider settings" (which is selected and highlighted with a red box), and "SSO settings". Below the tabs, there is a section titled "Configure your Identity provider SSO settings" with the instruction "Download the metadata file or view information in form fields and then import into your Identity Provider." and a "Download file" button. Below this, there are three input fields: "Entity ID" with the value "https://www.linkedin.com/learning/ABEAAAAA", "Assertion Consumer Service (ACS) URL" with the value "https://www.linkedin.com/checkpoint/enterprise", and "SP X.509 Certificate (signing)" with a long base64-encoded string. At the bottom right, there are "Cancel" and "Next" buttons, with the "Next" button highlighted by a red box.

2. 含めるフィールドをコピーして貼り付けます。
3. [次へ] をクリックします。

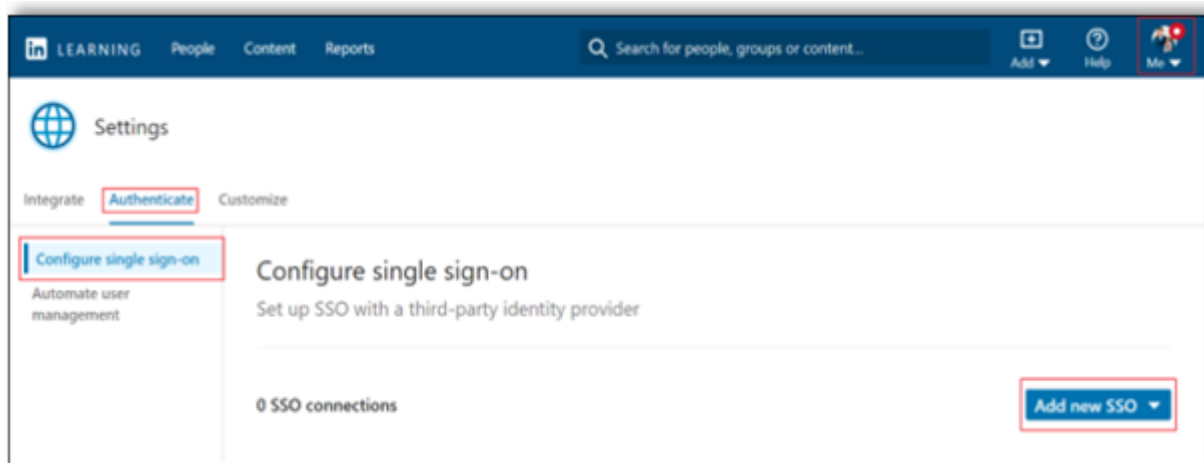
ID プロバイダーの設定

LinkedIn のプラットフォームと通信できるように ID プロバイダーを設定します。ID プロバイダーからメタデータファイルをアップロードできるかどうか、または手動で値を入力する必要があるかどうかを判断し、次のセクションのいずれかの手順を実行します。

ファイルのアップロード

.xml ファイルのアップロードを介して SSO を設定するには、次の手順を実行します。

1. ログインした後、[管理者] 画面が表示されていない場合は、[管理者ページ] を選択してから、[プロフィール] > [認証] の順に選択します。
2. [シングルサインオンの設定] を選択します。
3. [新規 SSO を追加] をクリックします。
4. SSO プロトコル ([上記参照](#)) を選択します。



5. [ダウンロード] をクリックします。 metadata.xml ファイルによって LinkedIn ラーニングのメタデータがコンピューターにダウンロードされます。
6. [次へ] をクリックします。

The screenshot shows a dialog box titled "Authenticate users with SAML SSO" with a close button (X) in the top right corner. Below the title bar are three tabs: "Basics", "Identity provider settings" (which is selected and highlighted with a red box), and "SSO settings". The main content area contains the text "Configure your Identity provider SSO settings" and "Download the metadata file or view information in form fields and then import into your Identity Provider." Below this text are two options: a button labeled "Download file" (highlighted with a red box) and the text "Or Load and copy information from fields". At the bottom right of the dialog are two buttons: "Cancel" and "Next" (highlighted with a red box).

7. [SSO の設定] ボックスで、[XML ファイルをアップロード] をクリックし、ID プロバイダーからメタデータファイルを追加します。

The screenshot shows the same dialog box, but now the "SSO settings" tab is selected and highlighted with a red box. The "Identity provider settings" tab is still visible. The main content area contains the text "Configure the LinkedIn service provider SSO settings." and "Get a metadata file from your identity provider and upload it here, or manually enter the values." Below this text are two radio button options: "Upload XML file" (which is selected and highlighted with a red box) and "Manually enter values". Below the "Upload XML file" option is a button labeled "Upload XML file" (highlighted with a red box).

8. ダウンロードしたファイルに移動して選択し、[開く] をクリックします。成功すると、メタデータが入力されたフィールドが表示されます。

値の手動入力

SSO を手動で構成するには、次の手順を実行します。

1. [SSO の設定] タブから [手動で値を入力] ラジオボタンを選択して、データを手動で追加します。
2. 次のフィールドにデータを入力します。

- **発行元の文字列またはエンティティ ID:** [md:EntityDescriptor entityID] フィールドと一致する必要があります。
- **予算グループ:** デフォルトオプションを選択するか、空白のままにします。
- **IdP リダイレクトエンドポイント:** [md:SingleSignOnService location] フィールドと一致する必要があります。**注:** LinkedIn は現在、urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect binding のみをサポートしています。
- **SAML サブジェクト識別属性名:** 従業員の識別に使用される SAML 認証応答の属性名です。LinkedIn は、以下のルールを使用して従業員を特定しています。
 - SAML 認証応答が属性のセットを含む SAML アサーションを提供する場合、このテキストフィールドに従業員の ID を含む属性の SAML 属性名を指定できます。例えば、employeeId という SAML 属性に整数の employeeId が送信された場合、[SAML サブジェクト識別属性名] フィールドに employeeId を入力できます。LinkedIn は各アサーションに送信された employeeId を使用して従業員 ID を検索します。
 - このフィールドに何も指定されていない場合、LinkedIn は <saml:Subject> に送信された NameId の値で従業員を検索します。このフィールドは一意的 ID でなければなりません。この値がメールアドレスでない場合、追加属性としてメールアドレスを指定することを強くお勧めします。
 - [SAML サブジェクト識別属性名] フィールドに設定された属性でユーザーを検索できない場合、または <saml:Subject> で NameID として設定された一意の識別子でユーザーを検索できない場合、LinkedIn はそのユーザーを認証しません。自動ライセンスプロビジョニングが有効になっていて、ユーザーが見つからない場合は、この値を使用してユーザープロフィールが新規作成されます。

- 公開証明書: LinkedIn は、ID プロバイダーが署名に使用する x.509 証明書を使用して、SAML 認証応答で送信された SAML アサーションの妥当性を検証します。認証応答の署名を検証できない場合、ユーザーは認証されません。

Authenticate users with SAML SSO

Basics Identity provider settings **SSO settings**

Configure the LinkedIn service provider SSO settings.
Get a metadata file from your identity provider and upload it here, or manually enter the values.

☐ Upload XML file ☒ Manually enter values

Issuer String or Entity ID ⓘ

Budget group ⓘ

IdP redirect endpoint ⓘ

SAML Subject Identity attribute name ⓘ

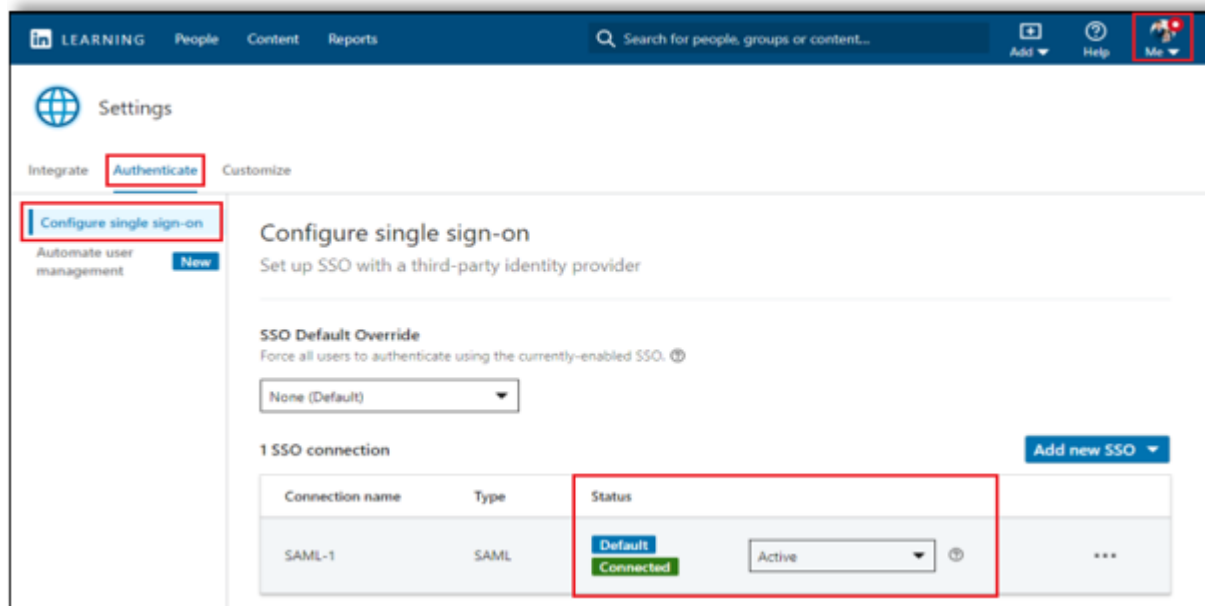
X.509 Public certificate ⓘ

+ Add another certificate

3. [保存] をクリックします。

シングルサインオンの有効化

設定が完了したら、[SSO ステータス] ドロップダウンから [有効] を選択して、SSO を有効にします。使用可能なオプションを使用するタイミングについては、以下の[有効なオプション](#)の表を参照してください。



有効なオプション

ステータス	説明
無効	<ul style="list-style-type: none"> SSO 実装の設定は不要です。 ユーザーは、LinkedIn ベースのロジックを使用して、割り当てられたライセンスにサインインできます。
パイロットモード (IdP のみ)	<ul style="list-style-type: none"> SSO が設定され、構成されています。 パイロットモードでは、IdP を介してアクセス権を付与された従業員の IdP 起点のフローに対して SSO が強制されますが、SP 起点のフローの場合は通常の LinkedIn ベースのサインインが可能です。ユーザーがサインインするために、IdP を使用して認証を受ける必要はありません。LinkedIn から直接アプリケーションにアクセスできます。 このモードは、SSO を初めて設定する場合に便利ですが、テストが完了した後は使用しないようにしてください。 SSO がパイロットモードの場合、新規ユーザーは追加できません。これは、アクティブにテストを実行してい

	るときに、SSO 管理者が一時的に使用する必要があります。
有効	<ul style="list-style-type: none"> SSO が設定され、有効になっています。 ユーザーは、IdP 起点のフローまたは SP 起点のフローを介してサインインする必要があります (IdP が IdP 起点のフローのみをサポートしている場合を除き、SP 起点のフローはサポートされません)。どの方法を使用するかに関係なく、認証が必要です。
警告:	初回設定後に [有効] を選択する場合は、SSO が正常に機能していることを確認するまでウィンドウを閉じないでください。閉じてしまうと、アカウントで SSO を無効にするためにカスタマーサポートへの連絡が必要になります。SSO を [有効] にする前に、[パイロット] オプションを使用して IdP 起点のフローを検証することをお勧めします。

- IdP 起点のフロー: ユーザーが ID プロバイダー (Okta、Azure、Ping など) でアプリケーションにアクセスする場合。
- SP 起点のフロー: ユーザーが LinkedIn ラーニング (サービスプロバイダー) に直接移動してライセンスにアクセスする場合。

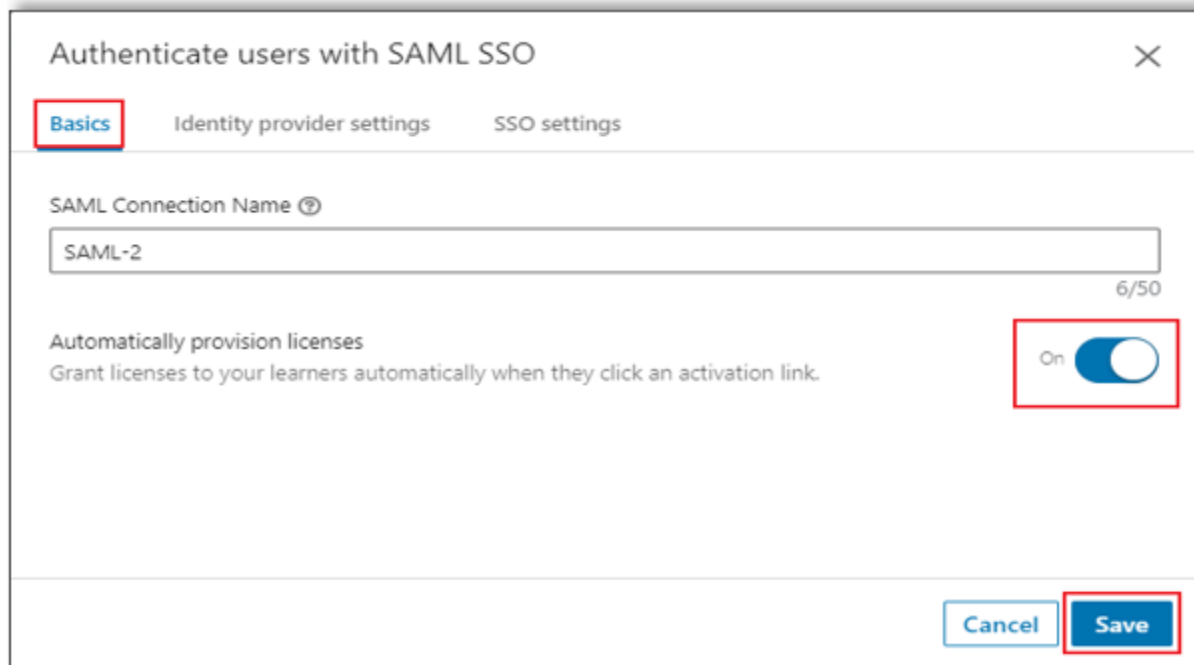
ライセンスの割り当て

SSO が有効になると、[ライセンスの自動割り当て] を [オン] に切り替えて、従業員にライセンスを自動的に割り当てることができます。このオプションを有効にすると、ユーザーは初めて認証されたときに、自動的にライセンスが付与されます。

ライセンスの割り当てを自動化するには、次の手順を実行します。

- [その他のオプション] (「...」) アイコンをクリックし、[編集] を選択します。
- [ライセンスの自動プロビジョニング] の切り替えを [オン] に設定します。

3. [保存] をクリックします。



注:

- このオプションを有効にしない場合、[ユーザー] タブで、管理者が手動でユーザーを追加する必要があります。LinkedIn ラーニングは、ユーザーをメールアドレスで識別します。
- このオプションを有効にすると、一致する識別子を持つ既存のユーザーが見つからない場合、認証時に新しいユーザープロフィールが自動的に作成されます。

NameID (フィールド)

LinkedIn ラーニングはデフォルトで、SAML 応答の NameID フィールドに送信された値を、ユーザーの一意の ID として使用します。この値は、サービスプロバイダーが一般的に使用するものなら何でもかまいません。LinkedIn ラーニングに統合されている学習管理システム (LMS) を使う予定の場合は、具体的な SSO ID を LinkedIn ラーニングに送信する必要があります。この ID はユーザーの LMS ID と一致している必要があり、LinkedIn ラーニングがレポートメッセージを LMS に送信できる必要があります。

ライセンスを自動的に割り当てるための要件

SAML 2.0 が普及した理由の 1 つは、サービスプロバイダーに追加情報を送信する際の柔軟性です。ID プロバイダーがアサーションを送信する場合、ユーザーを説明する属性が含まれます。これらの属性により、LinkedIn はユーザーを特定し、ユーザーを自動的にプロビジョニングすることができます。このセクションでは、いくつかの使用可能な属性について説明します。

メールアドレス (強く推奨)

EmailAddress は、SSO の有無に関係なくユーザーを識別するために使用できます。メールアドレスはユーザーのメイン識別子として使用できますが、変更されることのない従業員 ID やその他の一意の値を使用して、追加属性としてメールを含めることを推奨します。

ID プロバイダーは異なる命名規則を使用しているため、LinkedIn は次の属性名でメールアドレスを順番に検索します。

- EmailAddress
- email
- Email
- Mail
- emailAddress
- User.email

ID プロバイダーが別の命名規則を使用している場合、次のセクションで命名規則を設定できます。

名前 (オプション)

ID プロバイダーは、メールアドレスと同様に、複数の共通フィールドに名前を送信場合があります。LinkedIn は、ほとんどの ID プロバイダーとの互換性を即座に提供するため、以下の属性名で名前を検索します。

- FirstName
- first_name
- firstname
- firstName
- User.FirstName

姓 (オプション)

LinkedIn は、以下の属性名で姓を検索します。

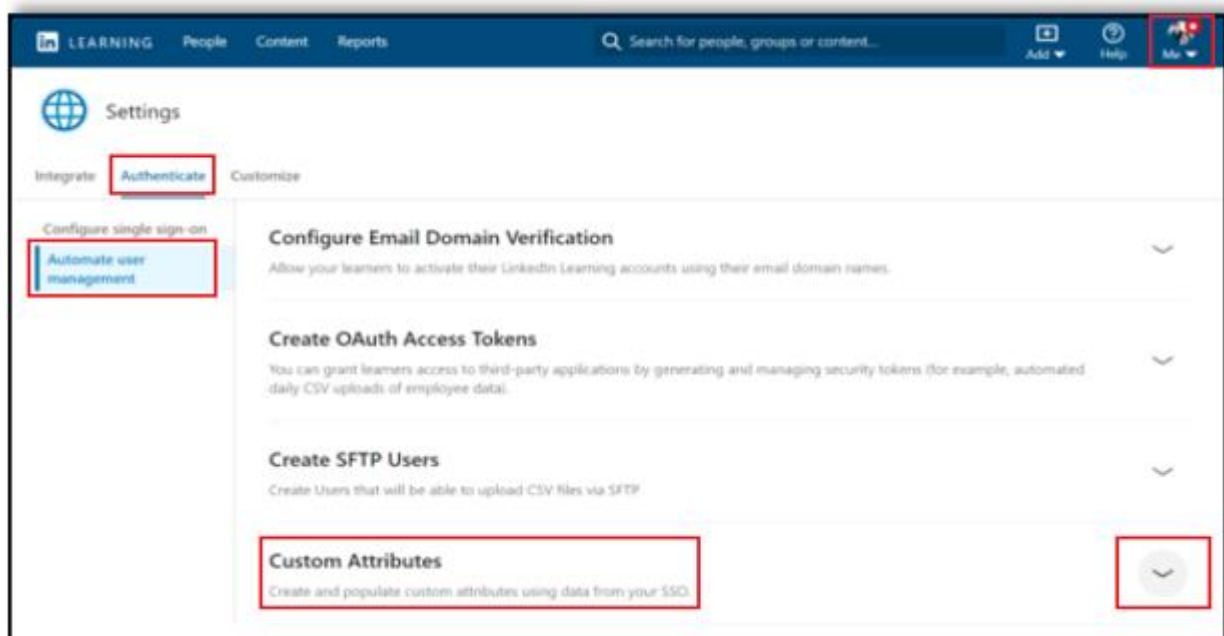
- LastName
- last_name
- lastname
- lastName
- User.LastName

カスタム属性

カスタム名マッピングを指定して、IdP 設定に対応させることができます (デフォルトのマッピングは使用しない)。カスタム属性名を入力し、マッピング先の属性を選択します。

SSO を通じてカスタム属性を追加するには、以下の手順を実行します。

1. [プロフィール] > [認証] > [ユーザー管理の自動化] の順に選択します。
2. [カスタム属性] を選択します。



3. [属性の追加] をクリックします。「属性名」というタイトルのドロップダウンメニューが表示されます。

Custom Attributes
Create and populate custom attributes using data from your SSO.

Attributes
First, choose a name for the attribute in LinkedIn Learning. Then, choose how to populate that attribute from your SSO.

Add Attribute

Primary Email Address ✕

Map to SSO attribute name
jdoe@generic.com ✎ 🗑

Add Mapping

Access Rule Redirect URL
Redirect users who are not allowed access to a URL of your choice.

Add Redirect URL

4. メニューから該当する属性名 (例: 「プライマリメールアドレス」) を選択するか、「カスタム名」を選択し、独自の属性名を入力します。

注: 選択した属性名で受講者を自動グループ化するには、[グループの割り当て] チェックボックスをオンにします。

5. [保存] をクリックします。

Add Attribute

Attribute Name

Custom name

Enter a custom name

JobTitle

☐ Assign groups

Cancel

Save

6. 作成した属性で、[マッピングの追加] をクリックします。

Custom Attributes

Create and populate custom attributes using data from your SSO.

Attributes

First, choose a name for the attribute in LinkedIn Learning. Then, choose how to populate that attribute from your SSO.

Add Attribute

JobTitle

Groups Assigned

Primary Email Address

Map to SSO attribute name

jdoe@generic.com

Add Mapping

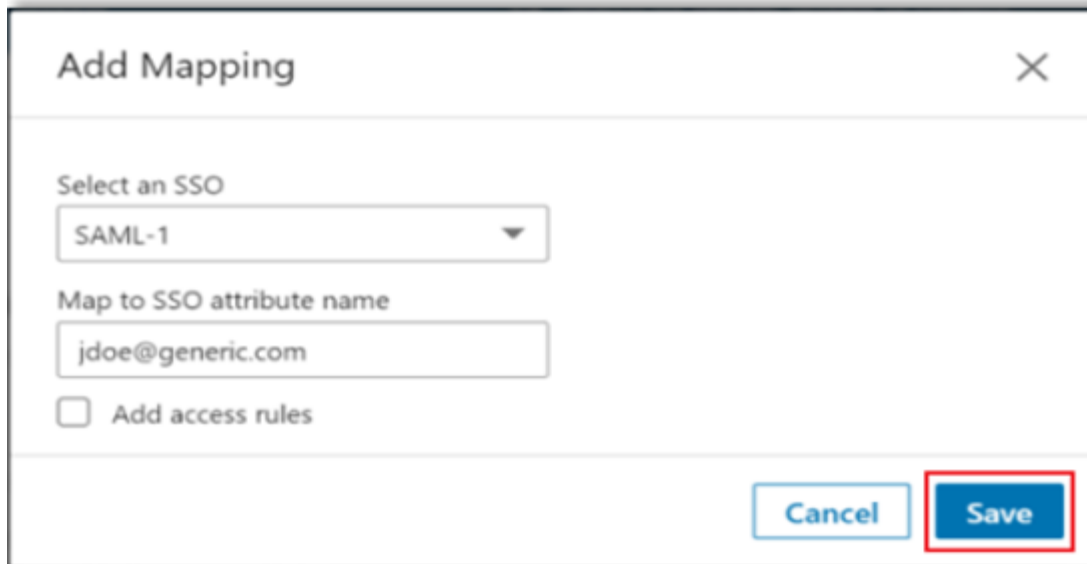
Access Rule Redirect URL

Redirect users who are not allowed access to a URL of your choice.

Add Redirect URL

7. マッピングの SSO 接続を選択します。

8. 「SSO 属性名にマップ」で、SAML 応答にある属性名を入力します。実際の属性名は、分かりやすいように任意に付けた名前ではなく、SAML 応答に表示されるとおりのものを使用します。
9. [保存] をクリックします。



The screenshot shows a dialog box titled "Add Mapping". It contains the following elements:

- A dropdown menu labeled "Select an SSO" with "SAML-1" selected.
- A text input field labeled "Map to SSO attribute name" containing the text "jdoe@generic.com".
- An unchecked checkbox labeled "Add access rules".
- At the bottom right, there are two buttons: "Cancel" and "Save". The "Save" button is highlighted with a red rectangular border.

以下の名称は、ユーザー提供のカスタム属性にマッピングできる標準ラベルの一部です。

- 建物コード
- 部署
- デスクの場所
- 職務タイプ
- 職務レベル
- マネージャー (プレーンテキストのみ。例: 「マネージャー」)
- 携帯番号
- プライマリメールアドレス
- 名
- 姓
- 作業者のステータス (アクティブまたは非アクティブ)
- 作業者の種類 (従業員、請負業者、またはその他)
- 役職

- 会社電話番号

SSO カスタム属性について詳しくは、[こちら](#)をクリックしてください。

設定の確認

ID プロバイダーと正常に統合されていること、および次の条件が満たされていることを確認します。

- SSO が有効で、[有効] に設定されている。
- LinkedIn ラーニングアプリケーションが ID プロバイダーで以前に指示された手順に従って設定されている。
- IdP で設定されている LinkedIn ラーニングアプリケーションが適切なユーザーにプロビジョニングされている。
- SAML サブジェクト NameID 値が SAML 応答で送信されるか、SAML サブジェクト ID が識別子として代替属性名を使用するために [LinkedIn サービスプロバイダーの SSO の設定] で定義されている。

次のログイン情報を使ってテストします。

- ID プロバイダーが開始するログインの場合
 - ID プロバイダーから直接 LinkedIn ラーニングを起動する。
- サービスプロバイダーが開始するログインの場合
 - 最初に、ブラウザで URL からアカウント ID を検索する。例:

<https://www.linkedin.com/learning-admin/settings/global?account=2108666>

- SP 起点の URL を作成するには、次の形式を使用します。

形式:

<https://www.linkedin.com/checkpoint/enterprise/login/accountid/?application=learning>

例:

<https://www.linkedin.com/checkpoint/enterprise/login/2108666?application=learning>

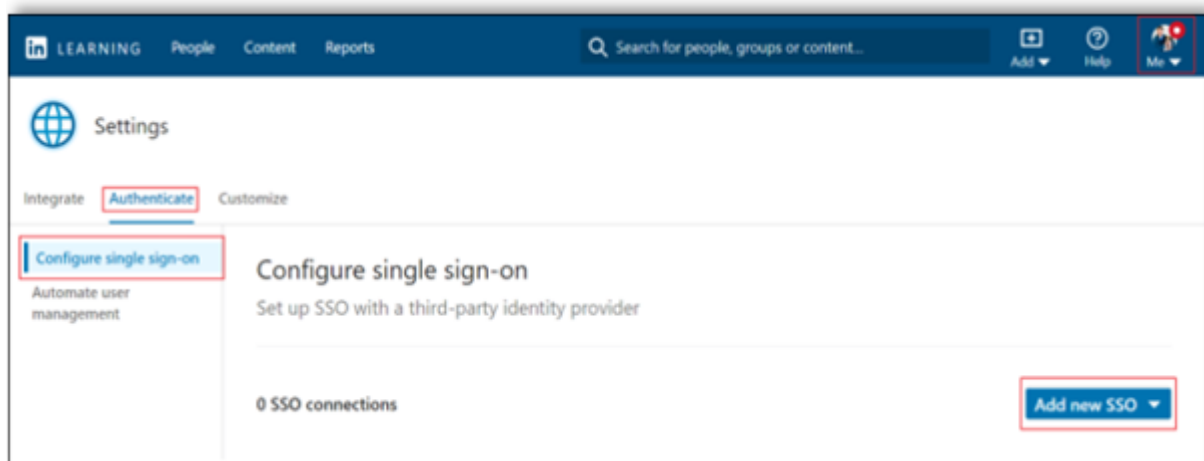
- この SP 起点の URL は、自動ライセンスプロビジョニングが有効になっている場合に新規ユーザーを有効にするために使用できます。
- すでに自分の LinkedIn プロフィールを LinkedIn ラーニングに接続している場合は、<https://www.linkedin.com/learning/login> にアクセスして、LinkedIn 資格情報を使ってログインします。IdP に移動して認証を受けた後、LinkedIn ラーニングにリダイレクトされます。

注: LinkedIn プロフィールを LinkedIn ラーニングに関連付けていても、ブラウザで LinkedIn セッションを開いていない場合、SSO での認証後、個人の資格情報で LinkedIn にログインするように求められる場合があります。これは SSO とは別の動作のため、SSO が破損しているわけではありません。

複数の SSO 接続の設定

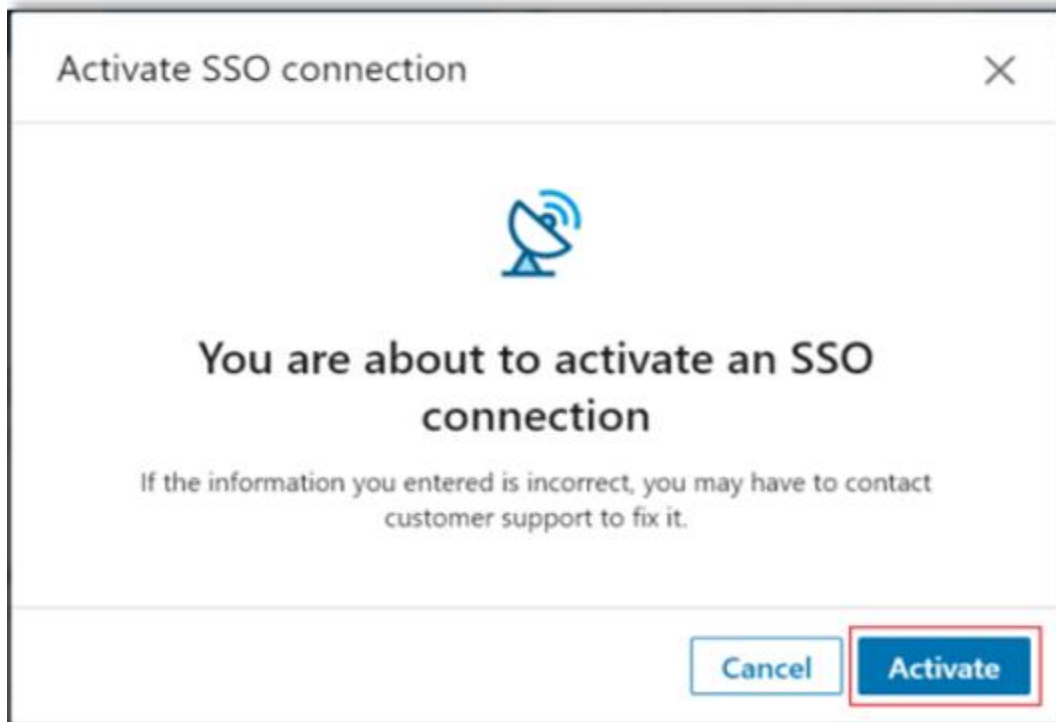
LinkedIn ラーニングは、複数の SSO 接続をサポートしており、テスト-QA 接続や複数の ID プロバイダーを利用できます。新しい SSO 接続を作成するには、以下の手順を実行します。

1. [SSO (シングルサインオン)] パネルを開き、[新規 SSO を追加] をクリックします。

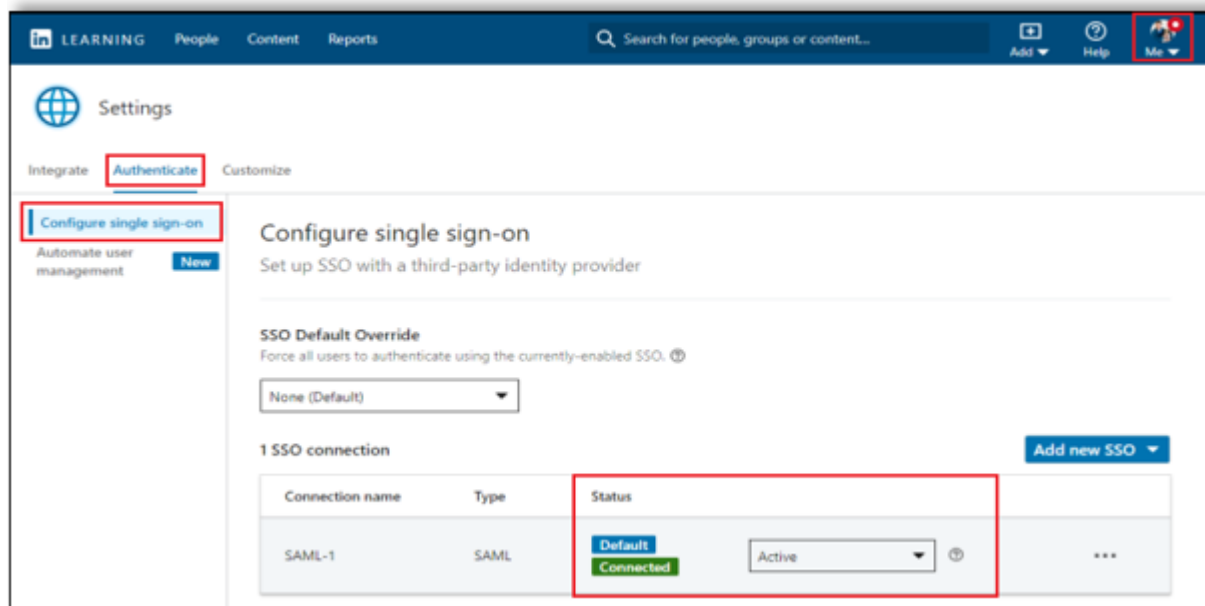


2. 新しい SSO 接続に名前を付けます。スペースは使用できません。

3. 前述の手順に従って、新しい SSO 接続を設定し、有効にします。接続が「有効」になっていることを確認し、ポップアップで [有効にする] を選択します。



4. この接続をデフォルトの認証方法にする場合、[デフォルトとして設定] を選択します。選択しない場合は、SP 起点の特定の URL を作成して、LinkedIn ラーニングの認証を受ける必要があります。



注: 複数の SSO 接続を使用するときは、1 つをデフォルトの接続にする必要があります。デフォルトの接続は、すべての LMS 統合に使用されます。

SP 起点の URL の作成

複数の SSO 接続を使用する場合、デフォルト以外の接続ごとに、SP 起点の特別な URL を作成する必要があります。この URL を生成する手順は以下のとおりです。

1. 最初に、ブラウザーで URL からアカウント ID を検索する。例:

<https://www.linkedin.com/learning-admin/settings/global?account=2108666>

2. SP 起点の URL を作成するには、次の形式を使用します。

形式:

https://www.linkedin.com/checkpoint/enterprise/login/accountid/?application=learning&authModeName=SSO_Connection_Name

- 例:
https://www.linkedin.com/checkpoint/enterprise/login/2108666?application=learning&authModeName=OneLogin-Attribute_test
- この SP 起点の URL は、自動ライセンスプロビジョニングが有効になっている場合に新規ユーザーを有効にするために使用できます。

複数の認証方法の使用

LinkedIn ラーニングは、複数の認証方法を使用して、学習者がプラットフォームへのアクセス権を持っているかを識別します。

LinkedIn ラーニングが現在サポートしているシングルサインオンは次の 3 種類です。

- SAML 2.0
- [LTI \(1.0 および 1.1\)](#)
- [Google を使ったサインイン](#)

複数認証では、自社のニーズに基づいて認証方法を組み合わせて使用できます。

考えられる認証のシナリオは 3 つあります。

- 「1 つの SSO 接続を全員に適用したい」
- 「必要な SSO 接続は 1 つだが、SSO は使いたくないというユーザーがいる」
- 「複数の SSO 接続が必要で、ユーザーによって使う接続が異なる」

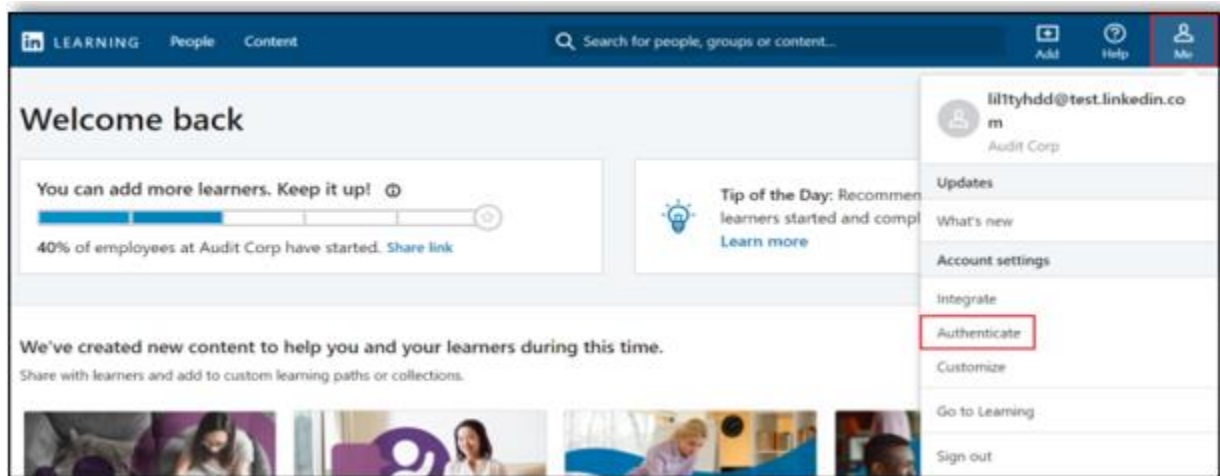
複数の認証方法の使用に関して詳しくは、[複数の認証 SSO](#) のドキュメントを参照してください。

SSO 接続の追加

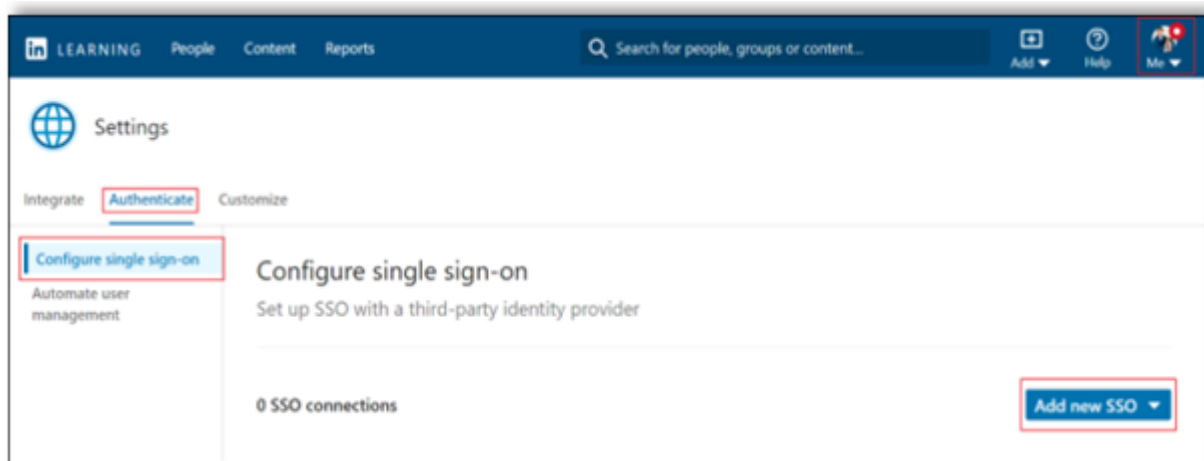
複数の認証方法を設定するには、まずシングルサインオン接続を設定する必要があります。

SSO 接続を追加するには、次の手順を実行します。

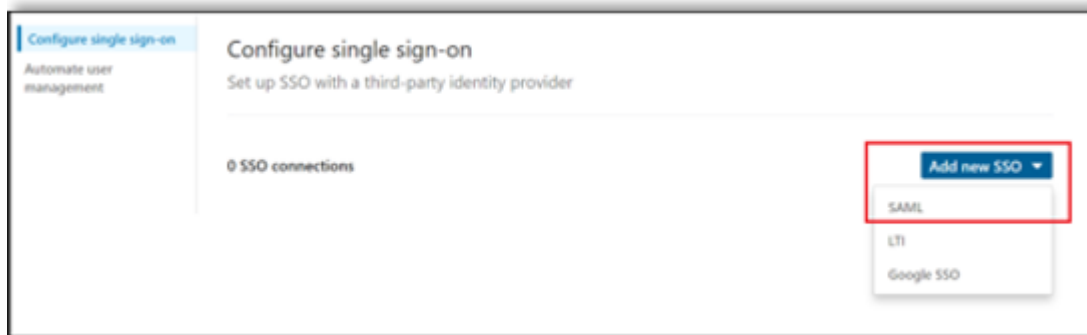
1. LinkedIn ラーニングの [管理者] 設定で、[プロフィール] > [認証] の順にクリックします。



2. サイドナビゲーションメニューから [シングルサインオンの設定] を選択し、[新規 SSO を追加] をクリックします。



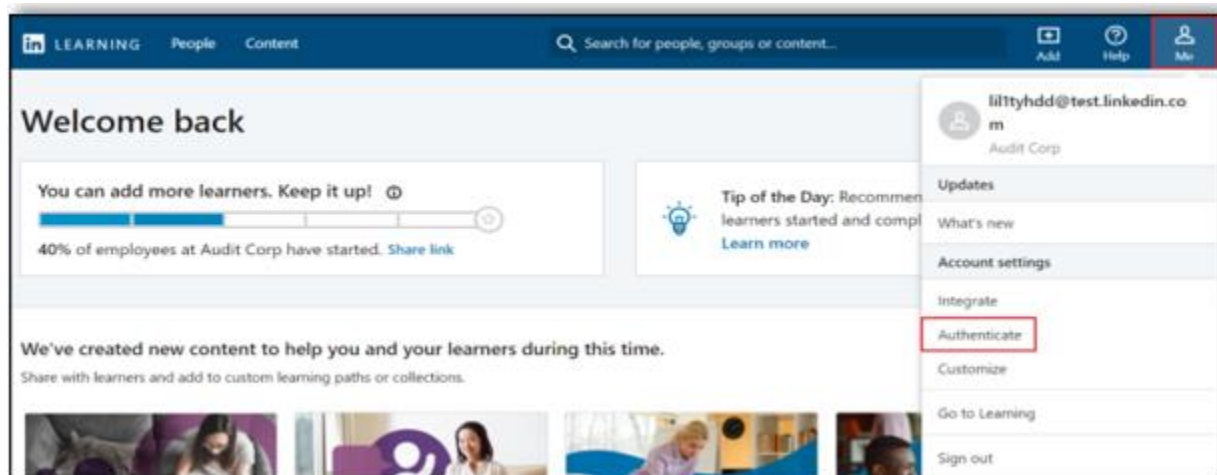
3. [SSO (シングルサインオン)] セクションを展開します。
4. [新規 SSO を追加] をクリックし、[SAML] を選択します。
5. 前述の手順に従い、追加のシングルサインオン接続を有効にします。



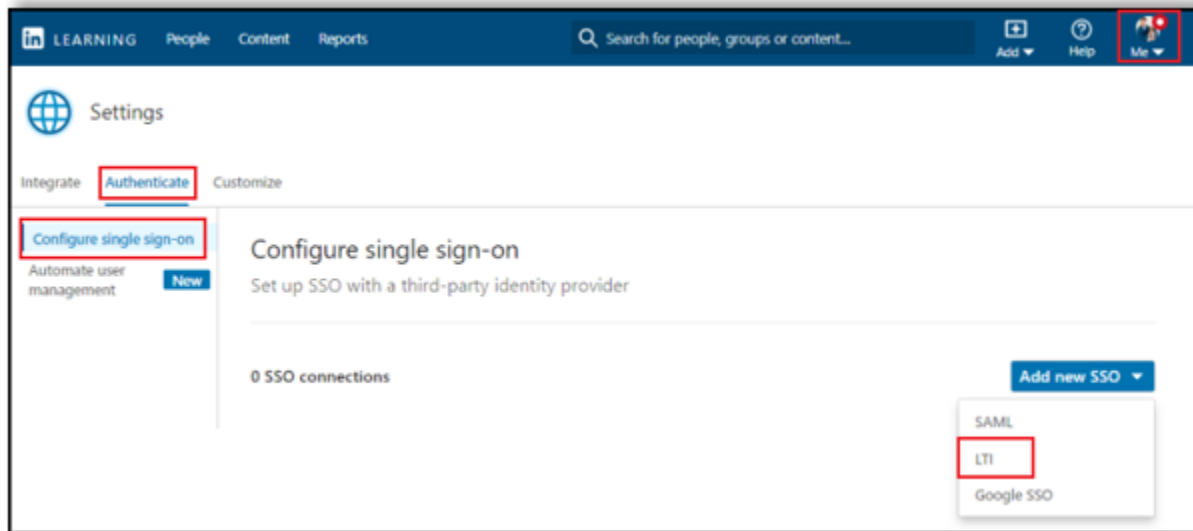
LTI 接続の追加

LTI 接続を追加するには、次の手順を実行します。

1. LinkedIn ラーニングの [管理者] 設定で、[プロフィール] > [認証] の順にクリックします。



2. サイドナビゲーションメニューで [シングルサインオンの設定] を選択し、[SSO (シングルサインオン)] セクションを展開します。
3. [新規 SSO を追加] をクリックし、「LTI」を選択します。



4. SSO 接続の名称を設定し、設定を終了します。
5. [キーを生成する] をクリックします。(LMS に入力するには、この情報が必要です)。[保存] をクリックします。

Authenticate users with LTI SSO

LTI Connection Name ⓘ
LTI-1
5/50

LMS Login URL ⓘ
https://examplecompany.lms.com

Enable automatic role provisioning for instructors ⓘ
On ☒

External ID Parameter Name
User ID ▼

SP-initiated redirect URL
Enter your SP-initiated redirect URL

Cancel

Generate Keys

6. 接続ステータスドロップダウンメニューから [有効] を選択します。

認証プロセス中に LTI 接続を追加する手順について詳しくは、[こちら](#)をクリックしてください。

アカウントで複数の認証方法を使用する際の詳細については、カスタマーサクセスマネージャーにお問い合わせください。

注: 受講者に、LinkedIn ラーニングアカウントの SSO 認証としてメールドメイン認証を使用可能にすることもできます。詳しくは、[こちら](#)をクリックしてください。

以上で操作は完了です。受講者は、複数のシングルサインオン (SSO) 方法で、LinkedIn ラーニングコンテンツにアクセスできるようになりました。

サポート

サポートドキュメントおよびその他のリソースは、以下から入手できます。

サポートドキュメント

- [ADFS SSO](#)
- [Azure Active Directory SSO](#)
- [Google SSO](#)
- [複数の認証 SSO](#)
- [Okta SSO](#)
- [CSV Org Sync を使用したユーザーの一括追加と管理](#)
- [プライバシーとセキュリティに関するホワイトペーパー: アカウントセンターの従業員データベース統合 \(EDI\) とシングルサインオン \(SSO\)](#)

技術的な問題

SSO の設定で技術的な問題が発生した場合、[LinkedIn ラーニングのヘルプセンター](#)を通じてアカウントチームまたはアプリケーションサポートチームにお問い合わせください。

LinkedIn のプライバシーおよびデータセキュリティポリシー

<https://www.linkedin.com/legal/privacy-policy>

LinkedIn のセキュリティに関する連絡先

セキュリティに関するご質問がある場合や、セキュリティ上の問題を報告する場合は、security@linkedin.com までお問い合わせください。