

LinkedIn ラーニング SSO 複数認証ガイド

2021 年 6 月 28 日

この文書の内容

以下の手順では、LinkedIn ラーニングの SSO 複数認証プロセスについて説明します。

1. SAML IdP または LTI を使用し、SAML SSO を有効にします。



2. ドメイン検証を有効にする (受講者はセルフサービスで実行できます)。



3. ユーザー認証の方法を管理します (CSV のダウンロード、個々のユーザー管理)。



4. 以上で操作は完了です。受講者は、複数の認証方法を

利用して 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 複数認証の概要

LinkedIn ラーニングでは、ユーザー向けに複数の認証方法をサポートできるようになりました。これにより LinkedIn ラーニングと統合した新しいユーザー/管理者は、受講者が SSO など、1 つの認証方法を使用して認証することを可能にしたり、また、それを行わない受講者がメールアドレスやパスワード、LTI、セカンダリーSSO 接続など他の認証方法を使用して認証できるようにしたりすることができます。

このガイドでは、統合中に使用できるさまざまな認証方法、認証方法の設定の仕方、各ユーザーが希望する認証方法の管理方法について説明します。

前提条件

- 会社のメールアカウント
- LinkedIn ラーニングのすべての管理者権限
- 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。

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。

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

複数認証の方法とは？

LinkedIn ラーニングは、認証方法を使用して、受講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。

認証方法には、SAML シングルサインオン、LTI、または非 SSO (ユーザー名とパスワード) を使用できます。

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。例を上げましょう。

- Okta (SAML SSO) + Ping (SAML SSO)
- Okta + メールドメインの検証

- Okta + LTI + メールドメインの検証
- Okta + 手動ユーザーアップロード
- Okta + Ping + メールによる招待

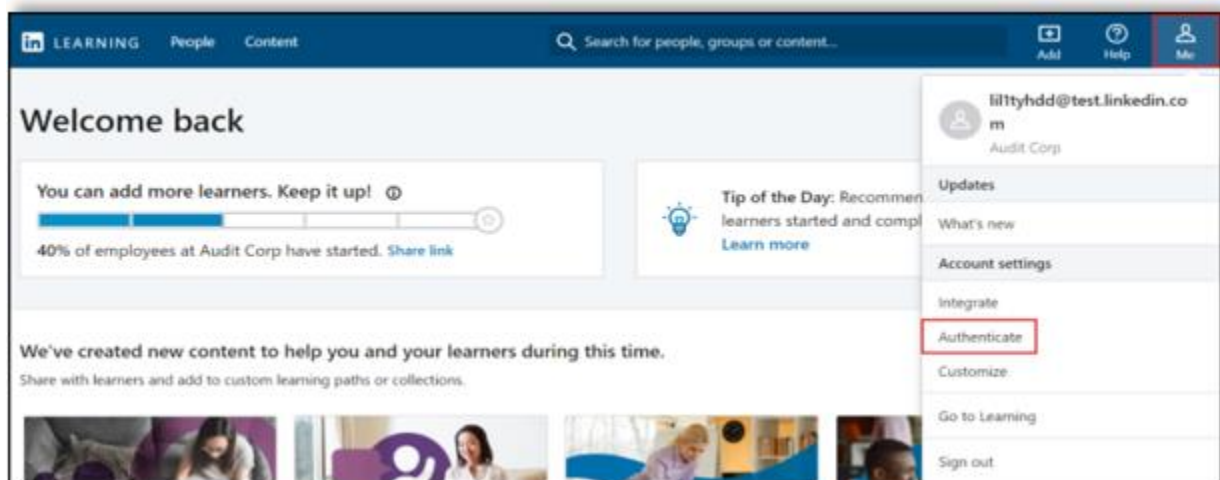
複数の認証方法を使用する場合、次の 3 つの認証シナリオが考えられます。

- 「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」

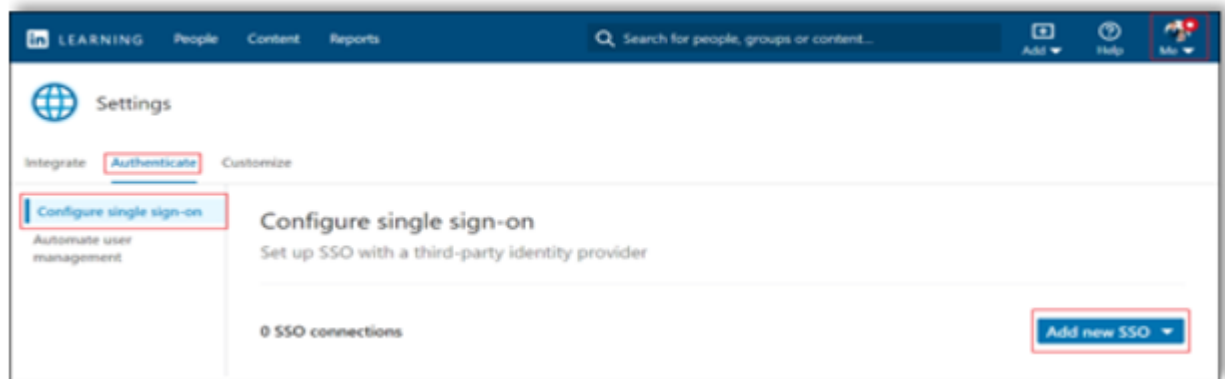
SAML SSO 接続の追加

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。この SSO を設定する手順は以下のとおりです。

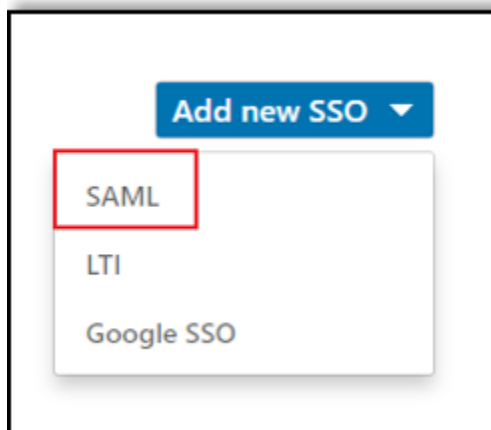
1. ログインした後、[管理者] 画面が表示されていない場合は、[管理者ページ] > [プロフィール] > [認証] の順に選択します。



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 の方法を 1 つ選択します (この場合は「SAML」)。



4. [SAML SSO でユーザーを認証] 画面で、SSO 接続の名前を入力し、[次へ] をクリックします。

Authenticate users with SAML SSO

Basics Identity provider settings SSO settings

SAML Connection Name ⓘ

SAML-1 6/50

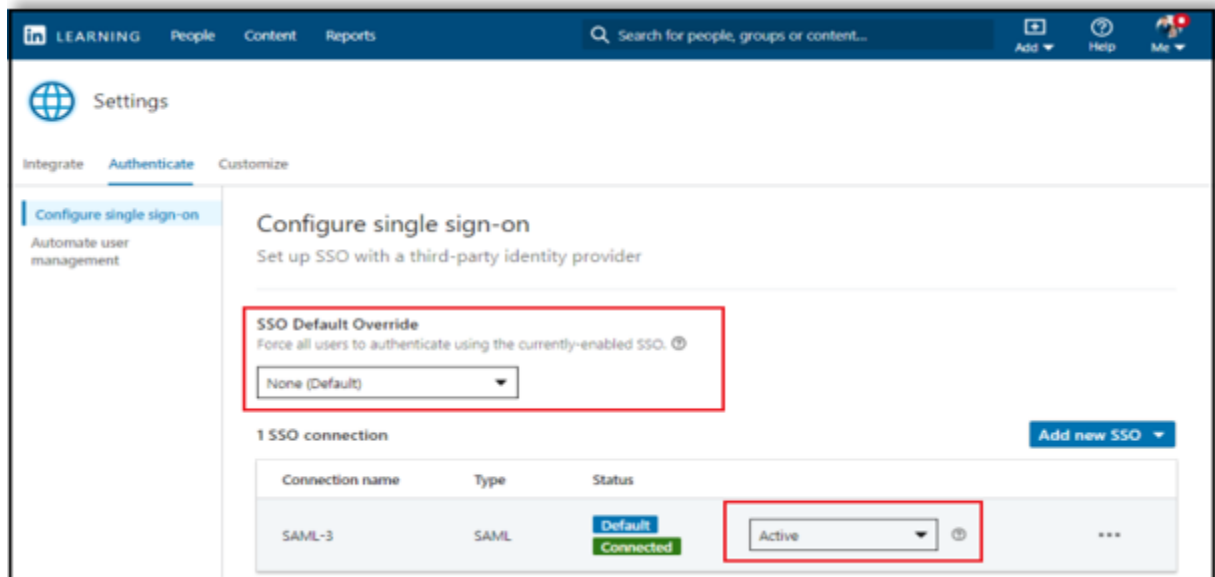
Automatically provision licenses

Grant licenses to your learners automatically when they click an activation link. Off

Cancel Next

SAML SSO 接続の設定の詳細については、[こちら](#)をクリックしてください。

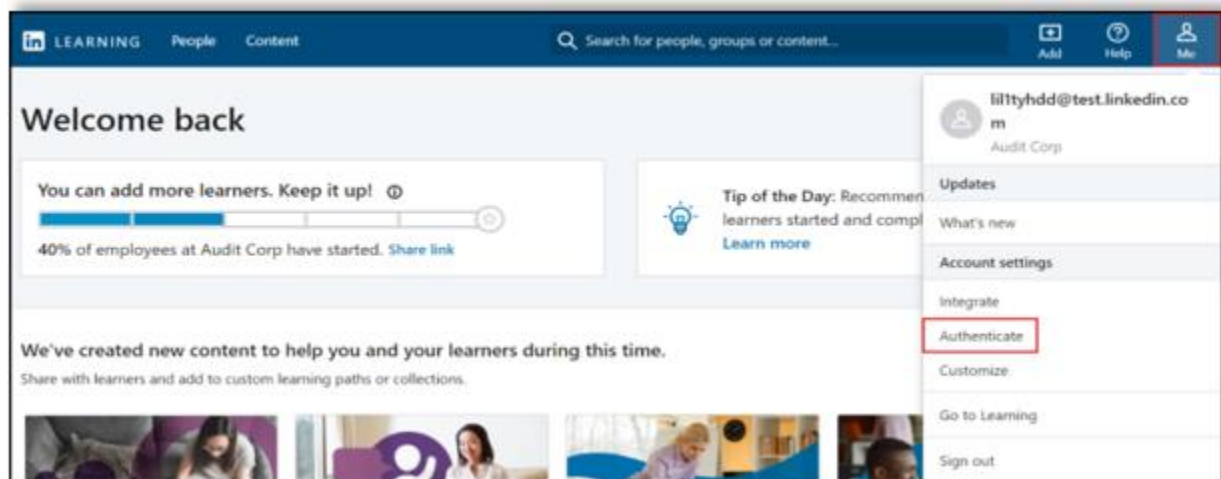
5. 接続のステータスを「有効」に切り替えます。
6. SSO 接続を設定した後、SSO の外部で学習プラットフォームへのアクセスをユーザーに許可する場合は、[SSO のデフォルトを変更] の下で、[いいえ (デフォルト)] を選択します。このアクションにより、管理者は SSO を使用して認証する必要があるユーザーと、メールアドレス検証またはメールによる招待 (ユーザーによる手作業のアップロード) を使用して認証する必要があるユーザーを選択できます。



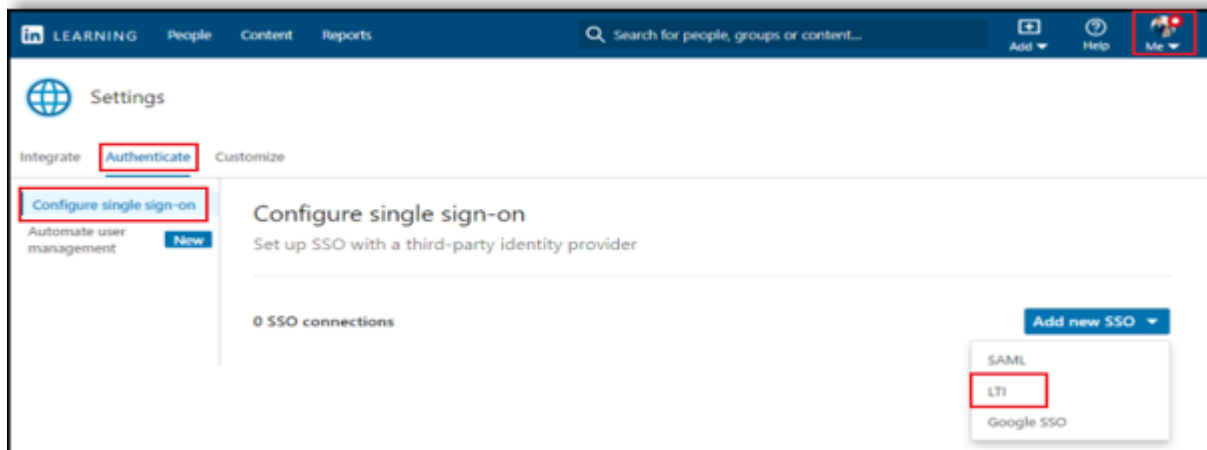
LTI 接続の追加

LTI SSO 接続を追加するには、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. [新規 SSO を追加] をクリックし、「LTI」を選択します。



4. SSO 接続に名前を付けます。スペースや特殊文字は使用できません。
5. 講師のサブ管理者権限を自動的にプロビジョニングする場合は、[講師に対して自動役割プロビジョニングを有効にする] を [オン] に切り替えます。
6. [外部 ID パラメーター名] ドロップダウンで、ユーザーの識別に使用するパラメーターを選択します。どの値を使用するかわからない場合は、「ユーザーID」のままにしておいてください。

注: 設定された「ユーザーID」の値は、LMS から LinkedIn ラーニングに送信される値と一致する必要があります。値が一致しない場合は、プロフィールが重複して作成されてしまう可能性があります。選択する値がわからない場合は、LinkedIn ラーニング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。

7. お使いの LMS が、ツールプロバイダーが開始する認証をサポートしている場合は、SP 起点のリダイレクト URL を入力します。使用する URL がわからない場合は、フィールドを空白のままにしておいてください。
8. [キーを生成する] をクリックします。この情報は、お使いの学習管理システムにアクセスする際に必要です。

Authenticate users with LTI SSO

LTI Connection Name ⓘ

5/50

LMS Login URL ⓘ

Enable automatic role provisioning for instructors ⓘ
On ☒

External ID Parameter Name

SP-initiated redirect URL

Cancel Generate Keys

9. 接続のステータスを「有効」に切り替えます。統合プロセス中に 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。

LEARNING People Content Reports
Search for people, groups or content...
Add Help Me

Settings

Integrate Authenticate Customize

Configure single sign-on
Automate user management

Configure single sign-on
Set up SSO with a third-party identity provider

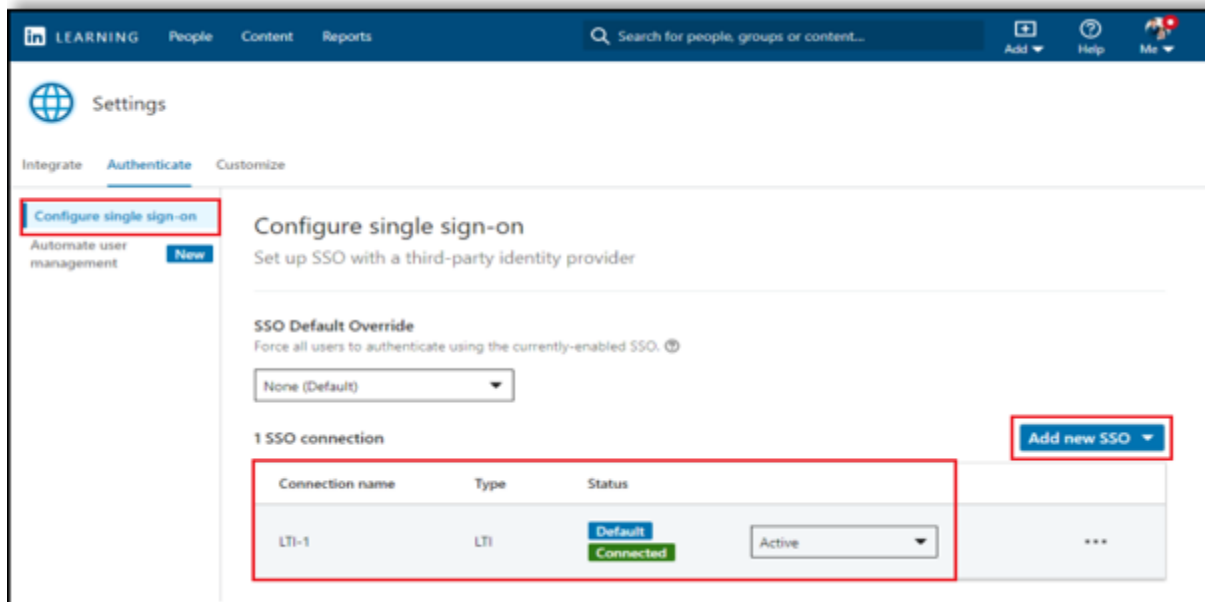
SSO Default Override
Force all users to authenticate using the currently-enabled SSO. ⓘ

1 SSO connection
Add new SSO

Connection name	Type	Status	
SAML-3	SAML	Default Connected	<input type="text" value="Active"/> ⓘ

SAML または LTI SSO 接続の追加

上記の手順を必要に応じて繰り返し、SSO 接続を追加します。



SSO 起動の URL の作成

複数の SAML SSO 接続を使用する場合は、接続ごとに一意のサービスプロバイダー開始の URL を作成することができます。SSO ユーザーは、この URL を使用することで LinkedIn ラーニングにすばやくアクセスできるようになります。この SSO 起動の URL を設定する手順は以下のとおりです。

1. ブラウザーで URL からアカウント ID を検索します。
例: <https://www.linkedin.com/learning-admin/settings/global?account=2108666>
2. 接続のセットアップ時に設定した SSO 接続名を見つけます。
3. 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

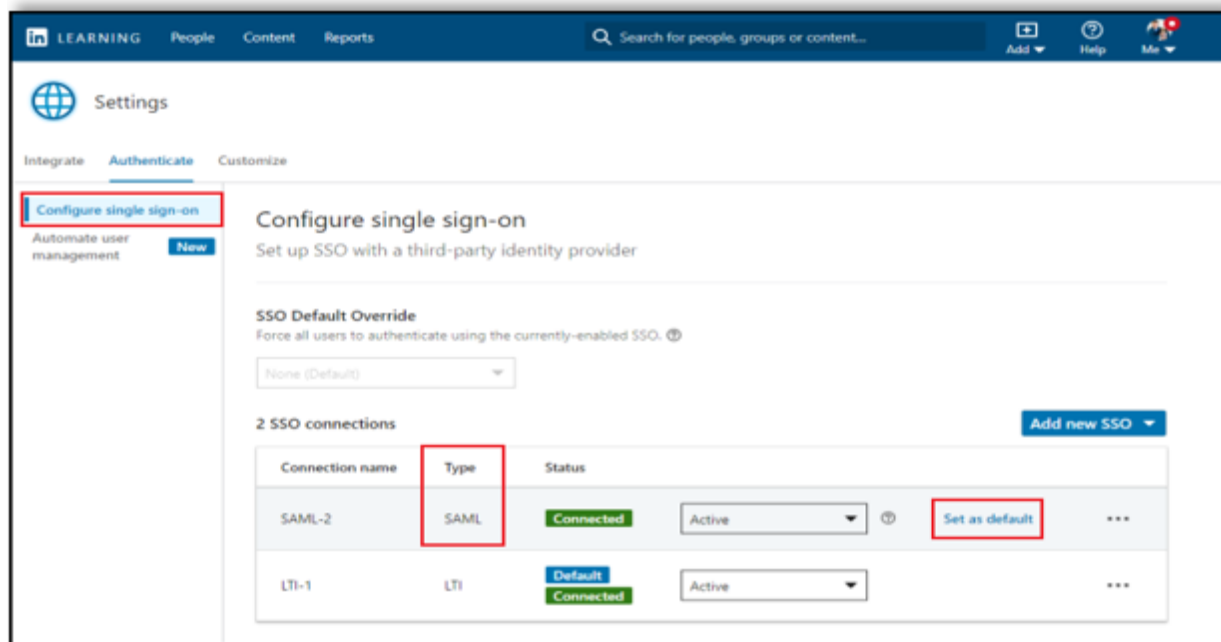
自動ライセンスプロビジョニングを有効にすると、SP 起点の URL を使用して新しいユーザーをアクティブ化できます。

注: SSO 接続の名前を変更すると、SSO URL は機能しなくなります。

デフォルトの SSO の選択

必要な数だけ SSO 接続の設定をすることができますが、デフォルト接続に設定できる SSO は 1 つのみです。LinkedIn ラーニングコンテンツを学習管理システム (LMS) に統合する場合は、すべてのコースのスタート時にデフォルトの SSO 接続が使用されます。

デフォルトを指定するには、使用する SSO 接続を指定し、[デフォルトとして設定] を選択します。



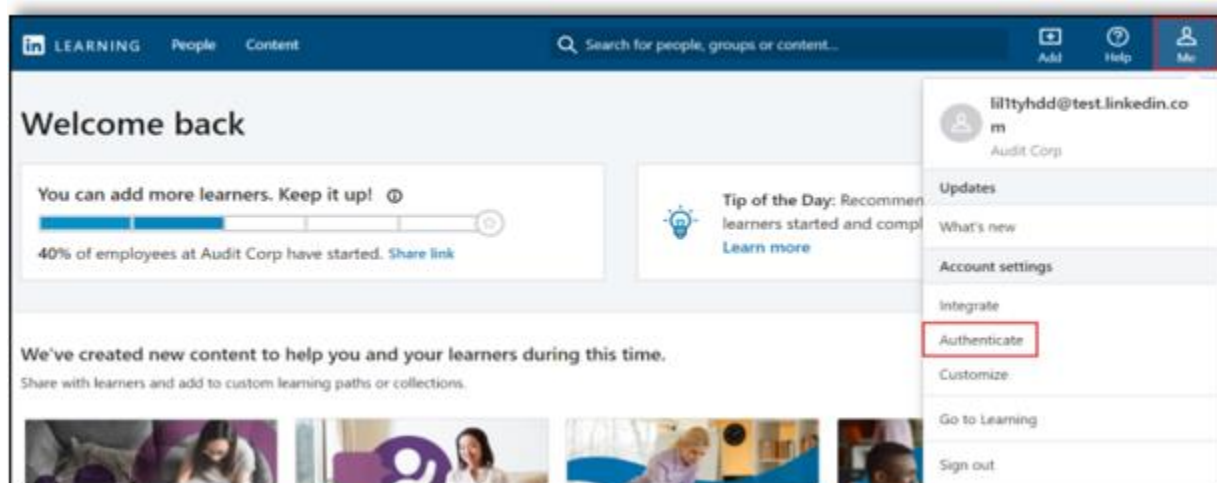
注: SAML SSO と LTI の両方を使用する場合は、LTI をデフォルトの認証方法として設定しないでください。LTI は、SP 起点のログインを常にサポートしているわけではなく、LTI をデフ

オルトで使用することで、アカウントで使用されている他の認証方法が壊れる恐れがあります。そうすると、ユーザーは LMS からログインする以外に選択肢がなくなります。

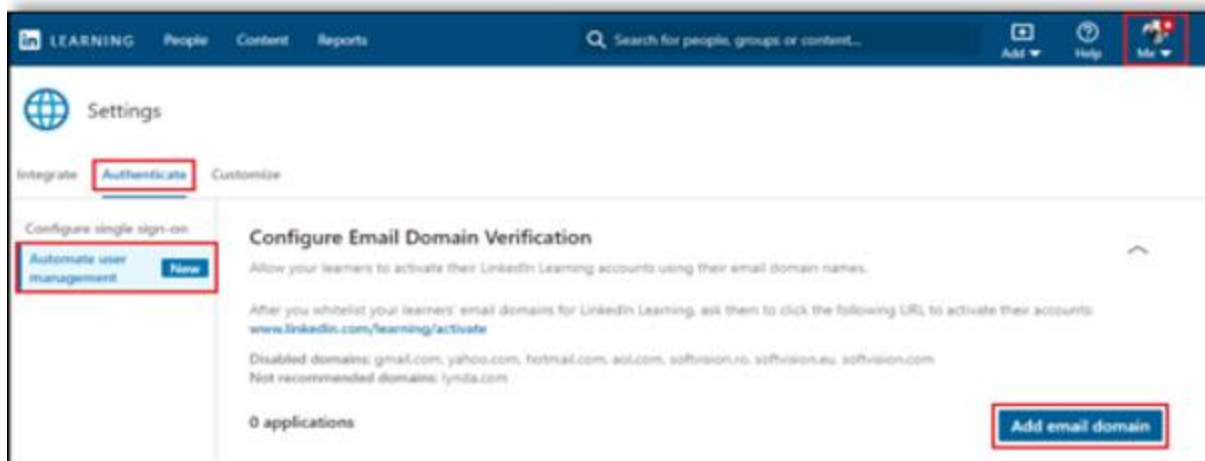
メールドメインの検証

メールドメインの検証を使用すると、承認済みのメールドメインを指定することができます。これにより、管理者が手作業で追加することなく、受講者が自分自身で登録を行うことができるようになります。メールドメインの検証を有効にすると、ユーザーは自分の仕事用または組織のアドレスを使用して自分で SSO を有効にすることができます。ユーザーは有効化メールを受信し、SSO 経由でルーティングされるか、[ドメイン検証の SSO] が「いいえ」に設定されている場合はパスワードの作成を求められます。メールドメインの検証を有効にするには、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. 左側のナビゲーションメニューから [ユーザー管理の自動化] を選択し、[メールドメインの検証の設定] を展開します。
3. [メールドメインを追加する] をクリックします。



4. [新しいメールアドレスを追加] 画面で、電子メールアドレス名 (該当する場合は AMD サブドメイン名) を入力します。
5. 電子メールで SSO 接続を有効にする場合は、[ドメイン認証の SSO] ドロップダウンで [いいえ] を選択します (上記を参照してください)。それ以外の場合は、選択した認証方法を選択します。
6. [保存] をクリックします。

The screenshot shows the 'Add a new email domain' dialog box. It has a title bar with a close button (X). The 'Email domain' field contains 'email.lms.com'. Below it, the 'SSO for domain verification' dropdown menu is set to 'No', which is highlighted with a red box. At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a red box.

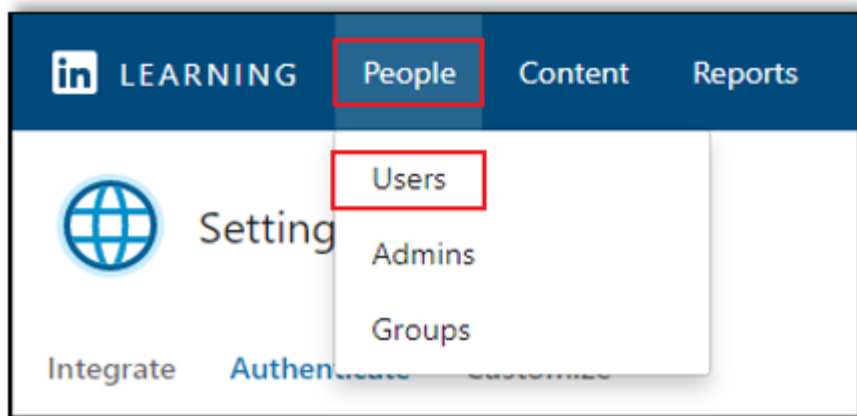
ユーザーの認証方法の管理

ユーザーの認証方法は、個別に指定することも、CSV を使用して一括で指定することもできます。

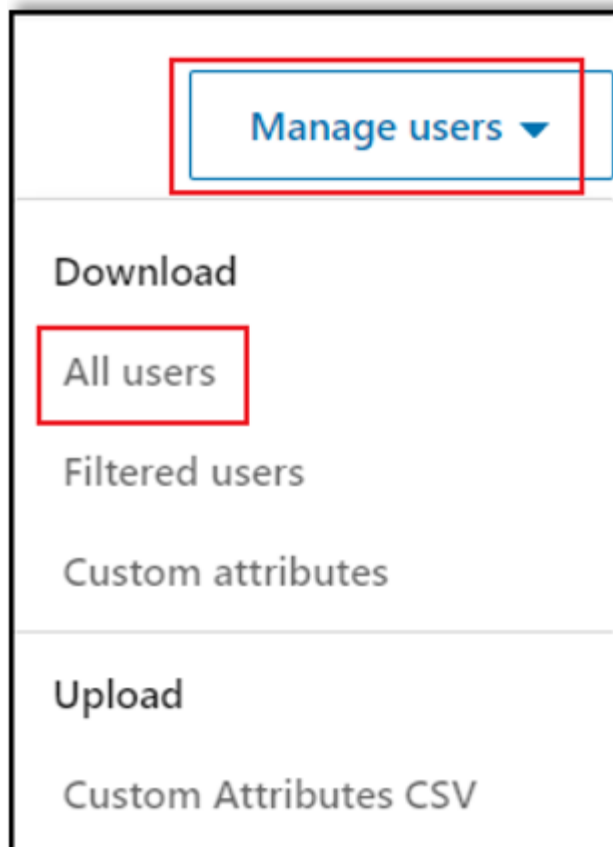
ユーザーリスト CSV ファイル管理

ユーザーリストを使用して、ユーザーグループの認証方法を一括で編集できます。

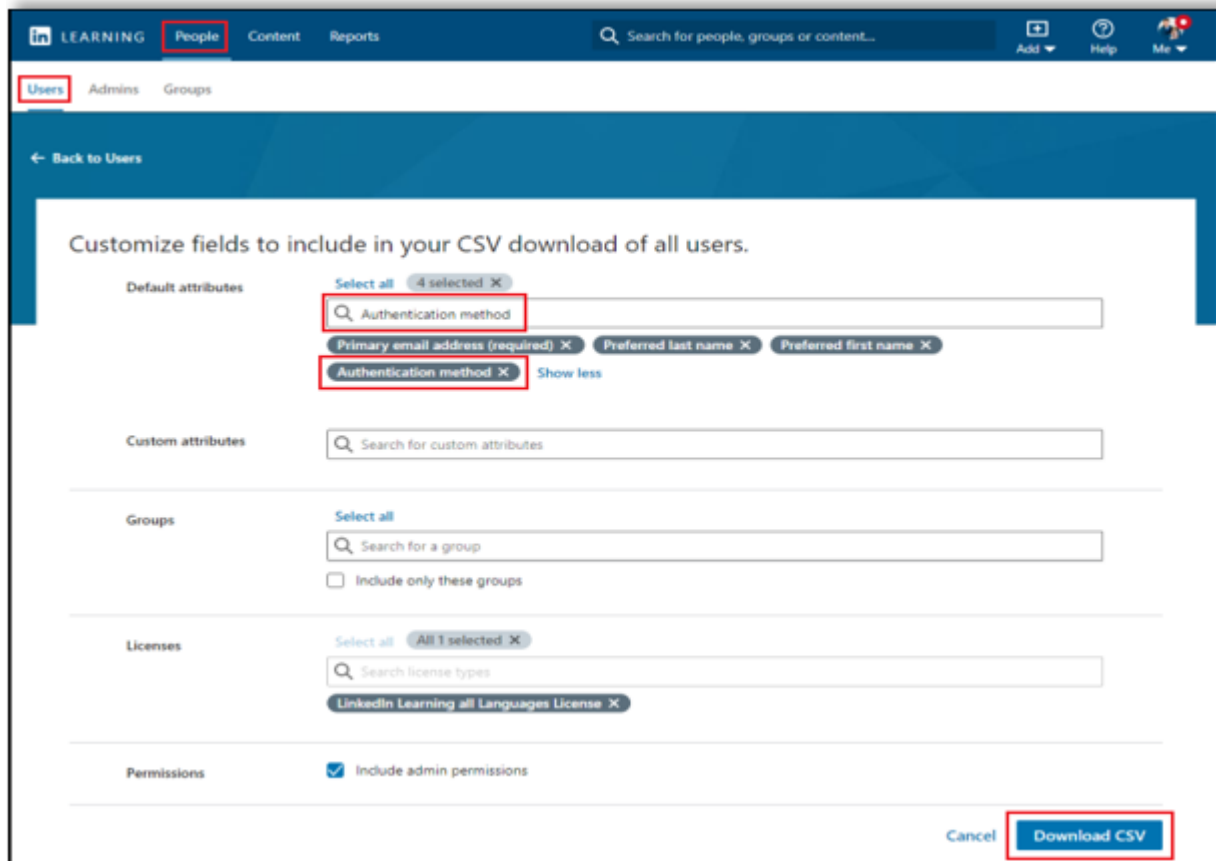
1. LinkedIn ラーニングの [管理者] 設定で、[ユーザー] > [ユーザー] の順に選択します。



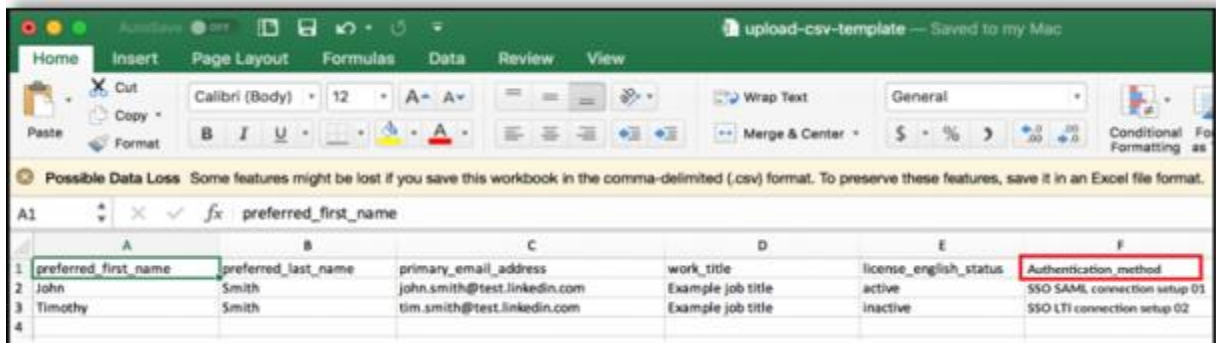
2. [ユーザーを管理する] > [ダウンロード] > [すべてのユーザー] を選択します。



3. [全ユーザーの CSV ダウンロードのフィールドをカスタマイズします] 画面で、[デフォルト属性] フィールドに「認証方法」を追加します。
4. [CSV ファイルをダウンロード] をクリックします。

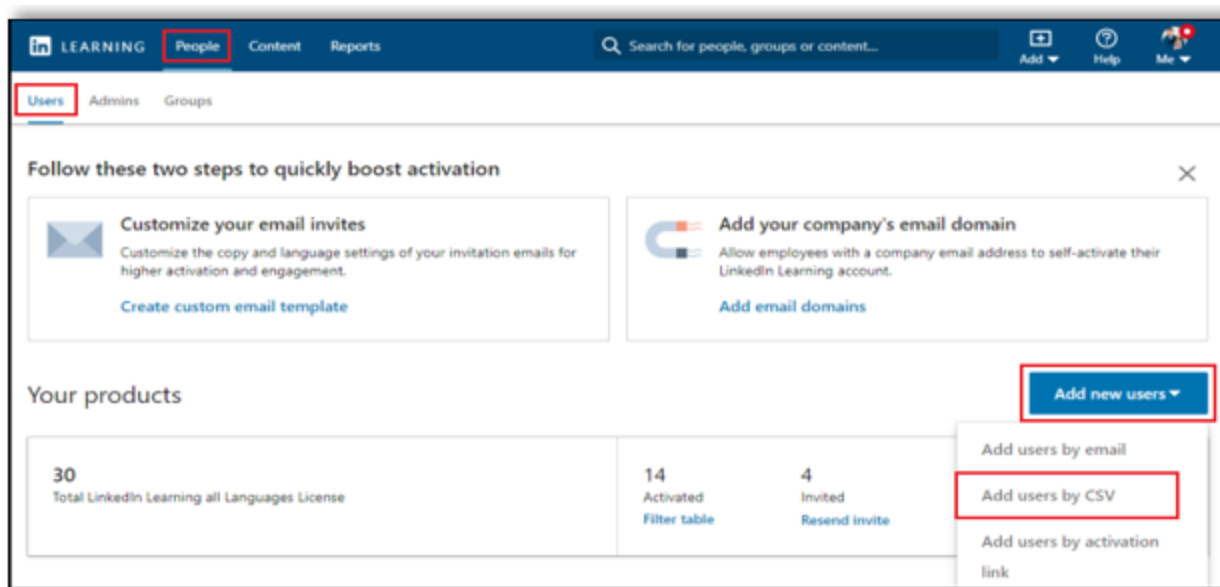


5. ダウンロードした CSV ファイルを開きます。
6. 「authentication_method」列を使用して、各受講者が使用する認証方法を選択します。



7. 手順 1～3 でそれぞれの SSO 接続用に作成した名前に基づいて、各受講者の「authentication_method」列に SSO 接続名を入力します。

- セルを空白のままにすると、受講者はあなたが設定したデフォルトの SSO 接続を使用する必要があります。
 - メールの招待またはメールドメイン検証を介して有効化するユーザーには、「no_sso」と入力します。
8. 更新した CSV ファイルを自分のコンピューターに保存します。
 9. [ユーザー] タブに戻り、[ユーザー] > [新しいユーザーの追加] > [CSV でユーザーを追加する] の順に選択します。




10. [CSV でユーザーを追加する] 画面で、[CSV ファイルをアップロード] を選択します。

Add users by CSV


×

Is your CSV file ready to upload?



No, I need help creating one

Get started



Yes, I'm ready to upload

Upload CSV

11. [CSV を使ってユーザーをアップロードする] 画面で、[コンピューターからアップロード] をクリックします。
12. CSV ファイルを選択し、[開く] をクリックします。


Upload users via CSV

×

CSV

metadata (12).xml

2kB



Learner invitation email

Create a new custom email template with customized messaging and language settings. If license information isn't added to the CSV, the invitation email will not be sent.

☒ Default invitation email

☐ Custom email template

Back

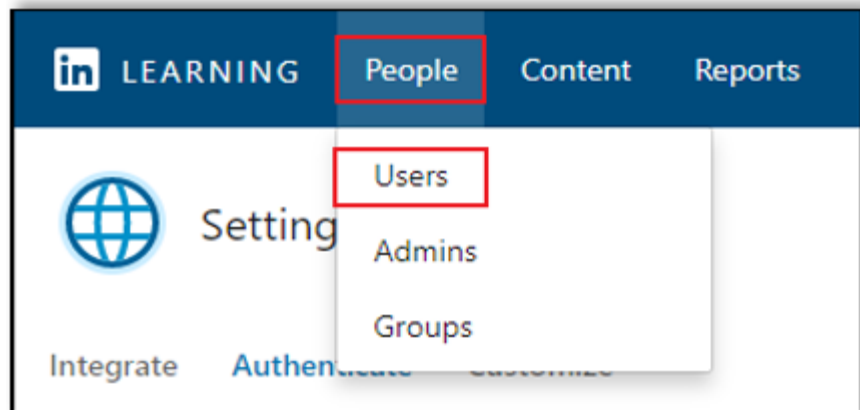
Cancel

Upload

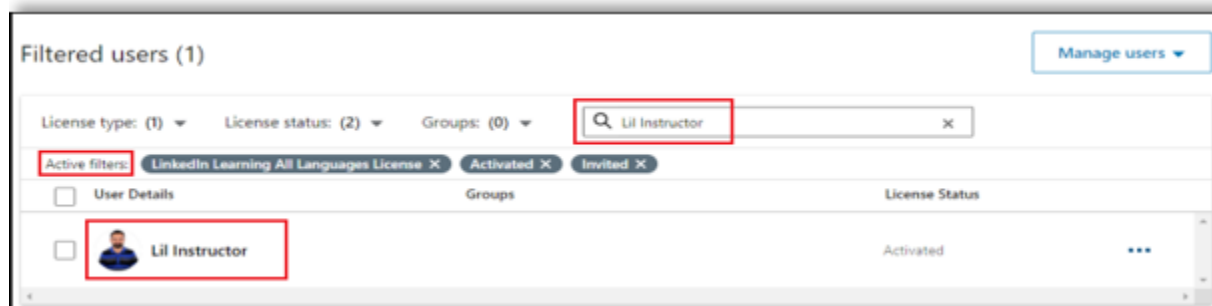
個々のユーザー管理

個々のユーザーの認証方法を管理するには、次の手順を実行します。

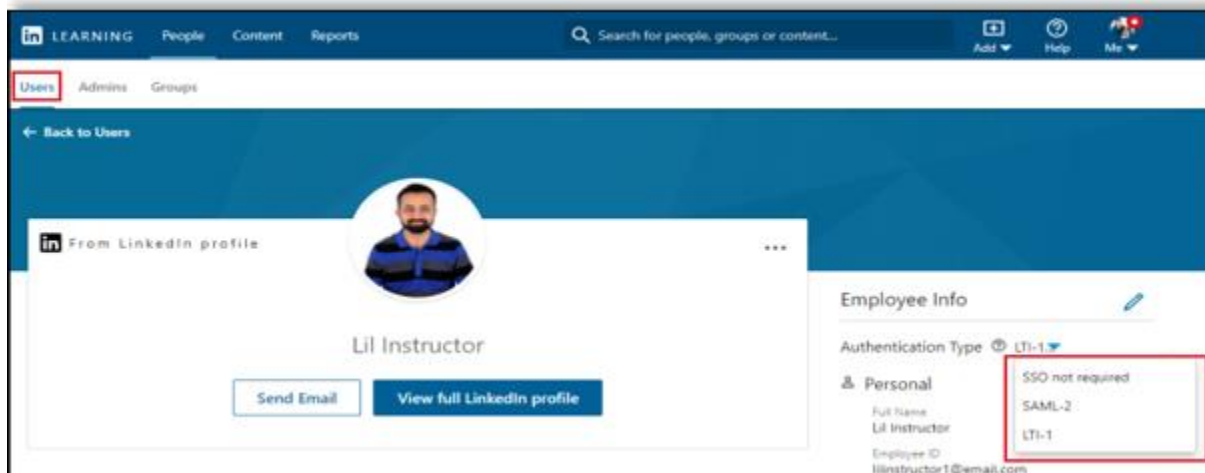
1. LinkedIn ラーニングの [管理者] 設定で、[ユーザー] > [ユーザー] の順に選択します。



2. ユーザー検索フィルターを選択するか、ユーザー名で検索します。



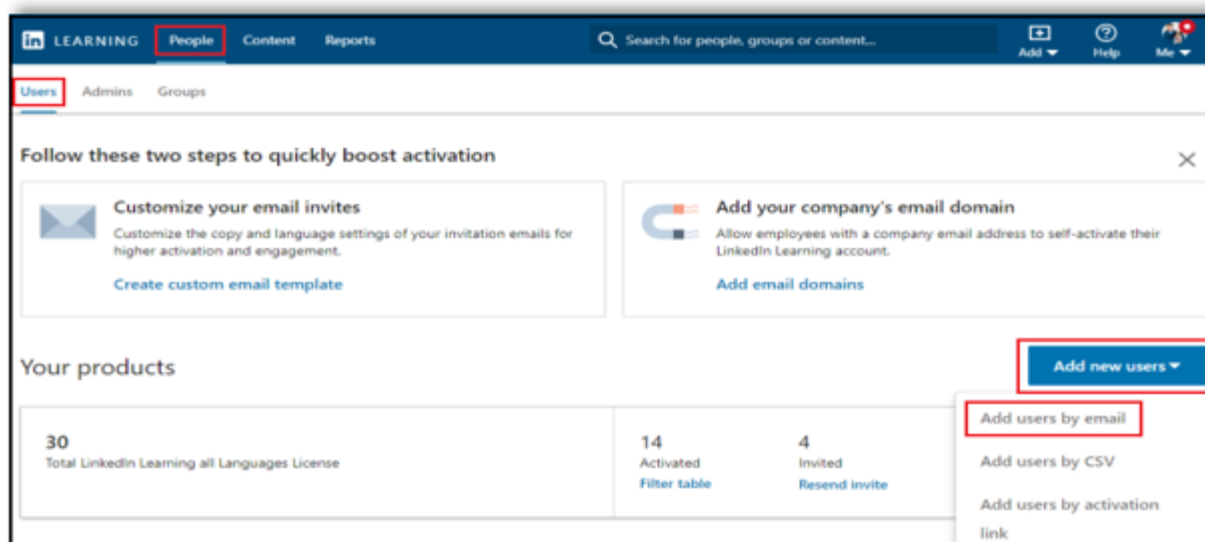
3. [認証タイプ] ドロップダウンを選択し、ユーザーの (新しい) 認証方法を選択します。



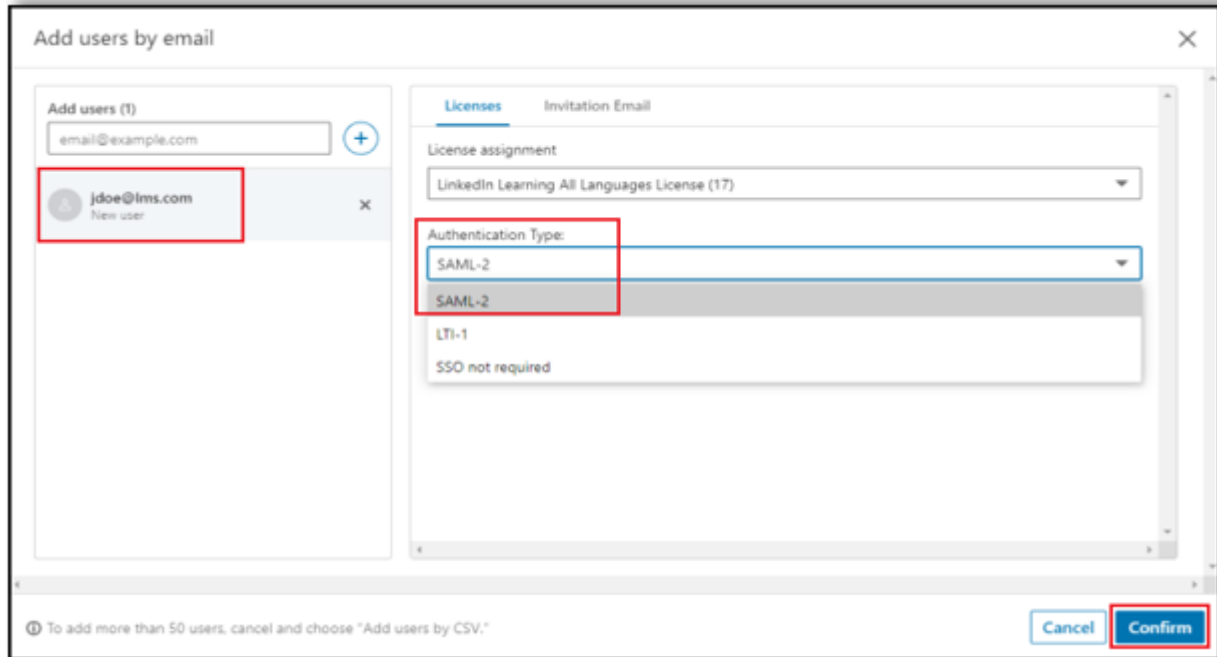
メールアドレスによる新規ユーザーの追加

新規ユーザーをメールで追加する場合は、その認証方法を設定できます。メールでユーザーを追加するには、次の手順を実行します。

1. [ユーザー] タブより、[ユーザー] > [新しいユーザーの追加] > [メールでユーザーを追加する] の順に選択します。



2. [メールでユーザーを追加する] 画面で、[ユーザーを追加] フィールドにユーザーのメールアドレスを入力します。
3. [認証タイプ] で、ユーザーの希望する認証方法を選択します。
4. [確認] をクリックします。システムが、ユーザーにアクティベーションメールを送信し、ユーザーは直接または選択した SSO 方法でログインします。



The screenshot shows the 'Add users by email' interface. On the left, a list of users to be added is shown, with 'jdoe@lms.com' (New user) highlighted. The main area is divided into two tabs: 'Licenses' and 'Invitation Email'. Under the 'Licenses' tab, the 'License assignment' dropdown is set to 'LinkedIn Learning All Languages License (17)'. The 'Authentication Type' dropdown is open, showing 'SAML-2' as the selected option, with 'SAML-2', 'LTI-1', and 'SSO not required' as other options. At the bottom right, there are 'Cancel' and 'Confirm' buttons. A note at the bottom left states: 'To add more than 50 users, cancel and choose "Add users by CSV."'

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](#)
- [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。