

# LinkedIn ラーニングおよび ADFS SSO 設定ガイド

- 2021 年 6 月 18 日
- この文書を読む時間の目安は 4 分です

## ADFS の概要

この文書では、LinkedIn ラーニング管理者が ADFS 3.0 を使用して、シングルサインオンを設定するために必要な手順について説明します。このガイドでは、SSO-ADFS 設定における一般的な問題のトラブルシューティング手順についても説明します。

## この文書の内容

以下の手順では、SSO-ADFS の設定プロセスについて説明します。

1. LinkedIn ラーニングから、SP メタデータをダウンロードします。



2. ADFS で証明書利用者信頼を追加して、証明書をインストールし、セキュアハッシュアルゴリズムを設定します。



3. 組織 SSO を設定 (SAML IdP または LinkedIn SP 経由) して、  
ADFS メタデータを LinkedIn ラーニングにアップロードします。

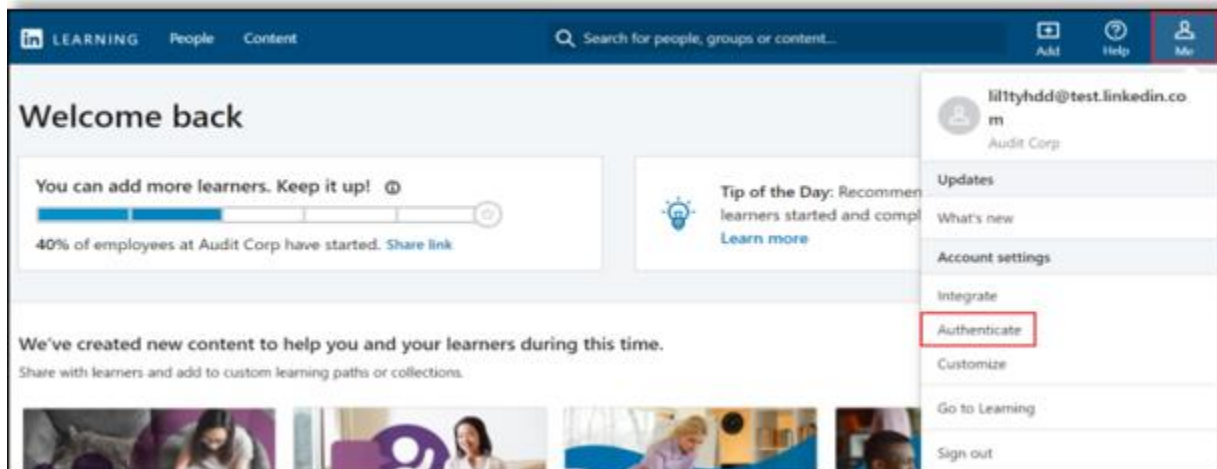


4. 以上で操作は完了です。受講者は、ADFS 経由で LinkedIn ラーニングコンテンツに  
アクセスできるようになりました。

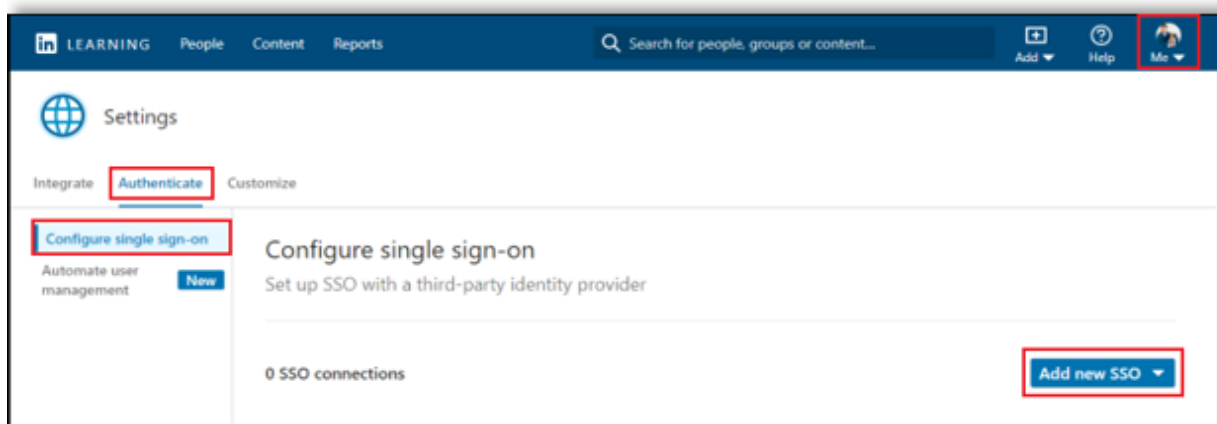


## LinkedIn ラーニングからサービスプロバイダーメタデータをダウンロードする

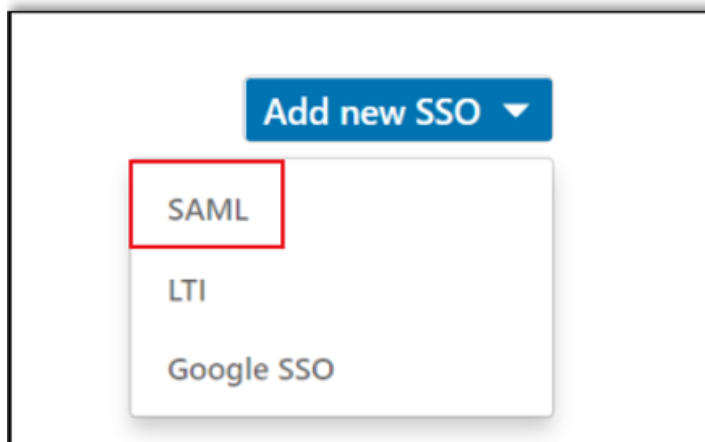
1. ログインした後、[管理者] 画面が表示されていない場合は、[管理者ページ] を選択してから、[プロフィール] > [認証] の順に選択します。



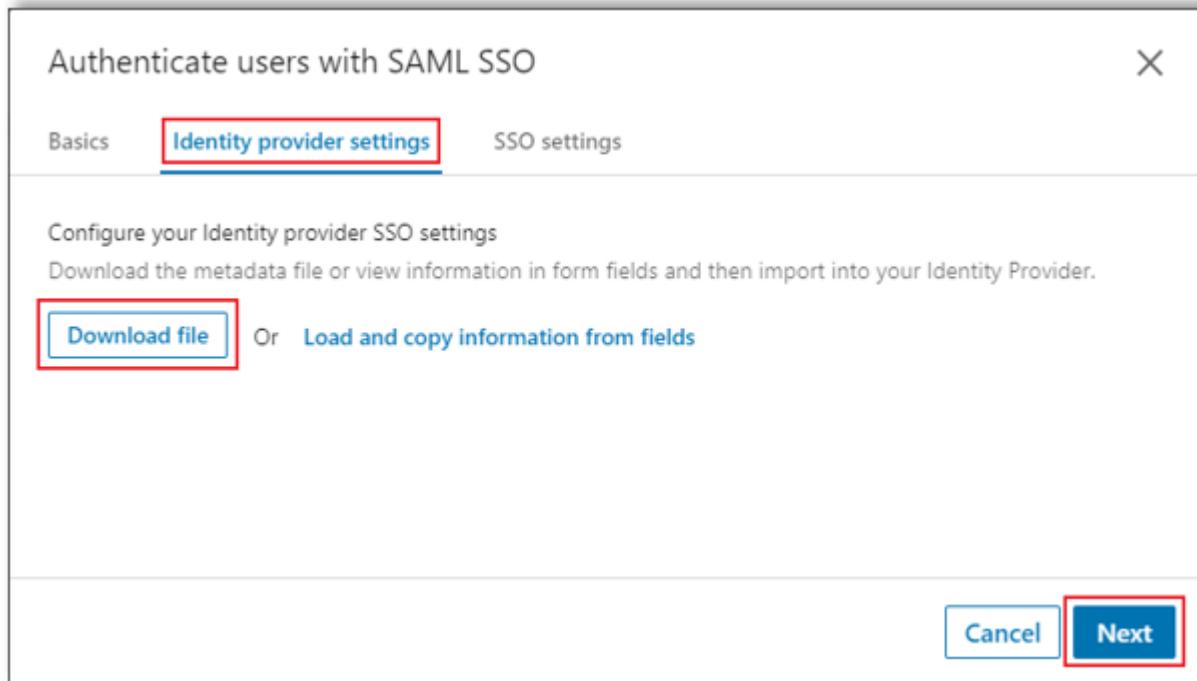
2. サイドナビゲーションメニューから [シングルサインオンの設定] を選択し、[新規 SSO を追加] をクリックします。



3. [新規 SSO を追加] をクリックし、[SAML] を選択します。



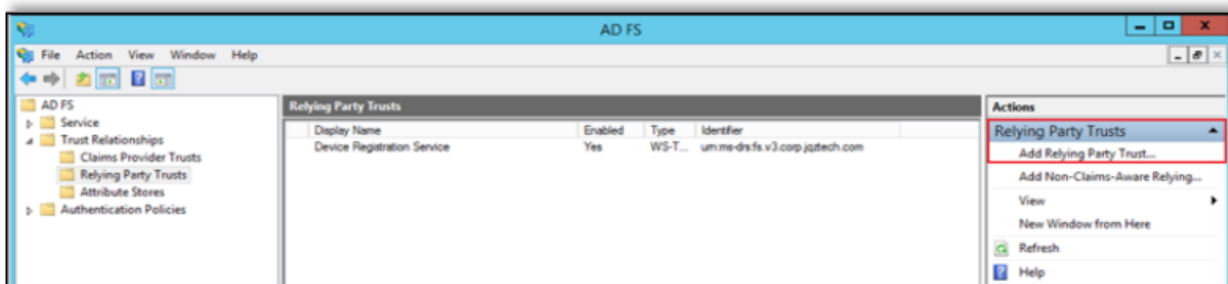
4. [SAML SSO でユーザーを認証] 画面の [ID プロバイダー設定] で、[ファイルをダウンロード] をクリックします。



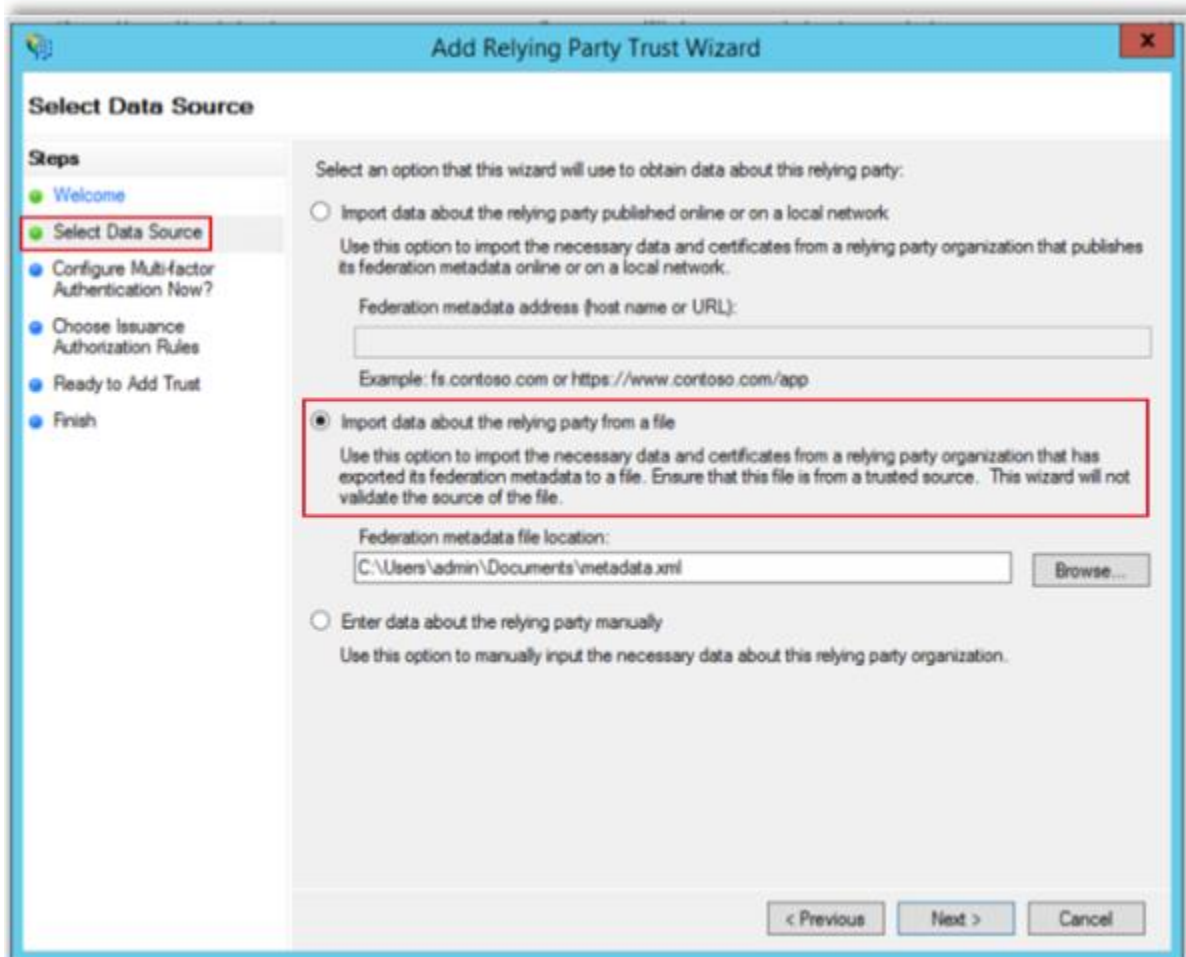
LinkedIn ラーニングは、SP メタデータを XML ファイルとしてダウンロードします。このファイルは、次のセクションで必要となります。

## 証明書利用者信頼の追加

1. ADFS で、[Trust Relationships] > [Relaying Party Trusts] の順に移動します。以前に追加したすべての証明書利用者信頼が表示されます。
2. 右側の列で、[Add Relying Party Trust] を選択します。



3. 左側のサイドナビゲーションで [Select Data Source] をクリックしてから、[Import data about the relying party from a file] を選択して、LinkedIn ラーニングからダウンロードした SP メタデータファイルを選択します。



4. [Specify Display Name] を選択してから、[Display name] フィールドに表示名 (例: 「LinkedIn Learning」) を入力します。

**Add Relying Party Trust Wizard**

**Specify Display Name**

Enter the display name and any optional notes for this relying party.

**Steps**

- Welcome
- Select Data Source
- Specify Display Name**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Display name: LinkedIn Learning

Notes: Enter your notes here

5. [Configure Multi-factor Authentication Now?] をクリックし、[I do not want to configure multi-factor authentication settings for this relying party trust at this time] を選択します。

**Add Relying Party Trust Wizard**

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?**
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

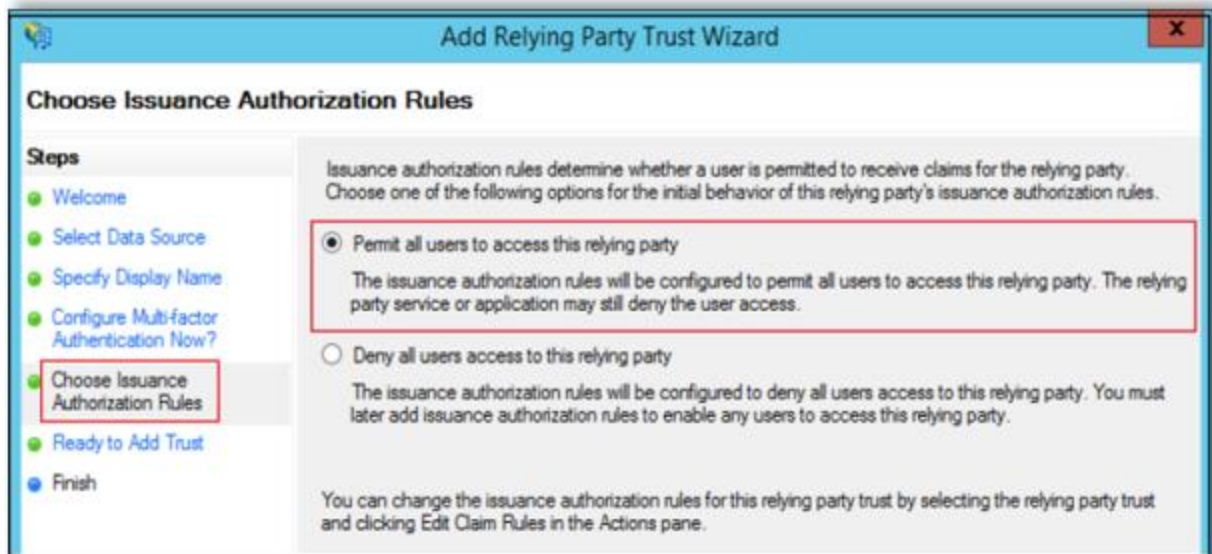
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.
   
☐ Configure multi-factor authentication settings for this relying party trust.

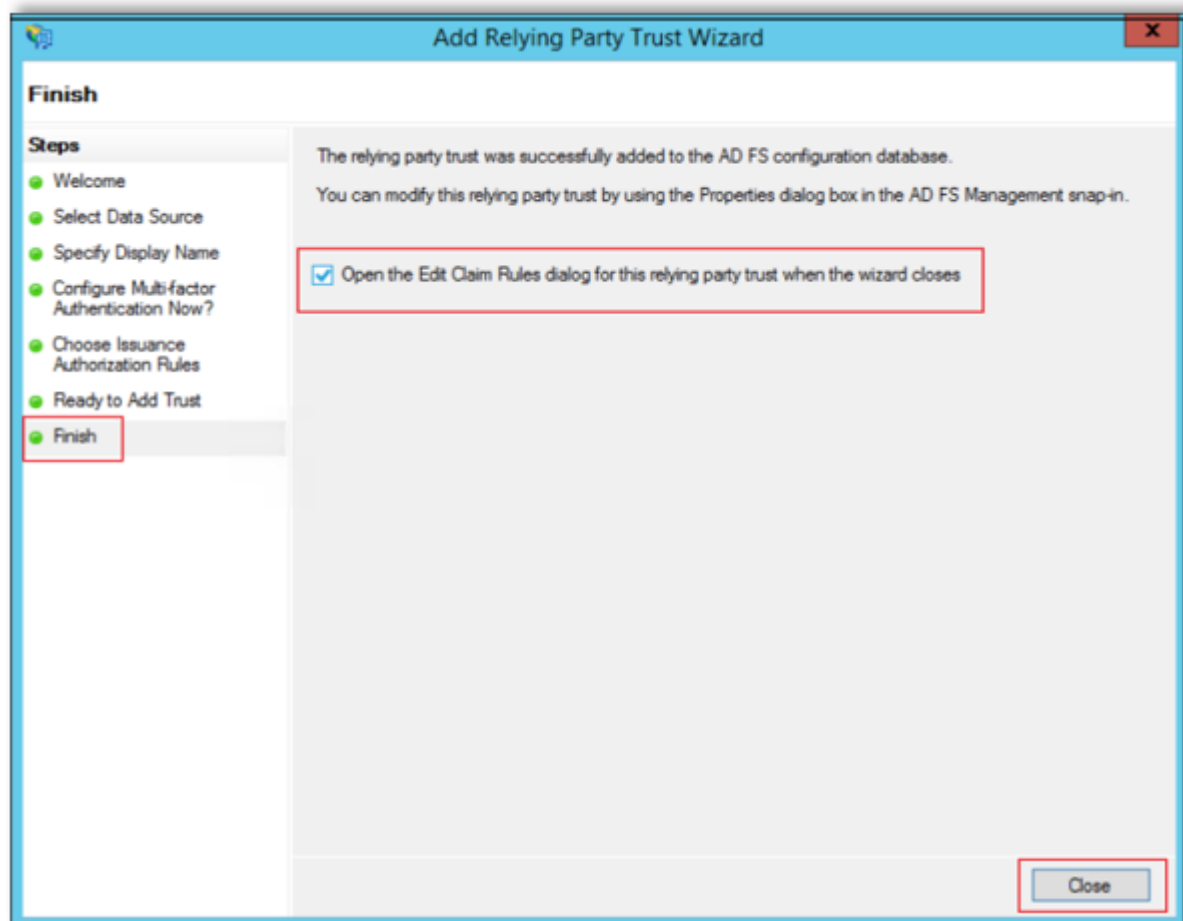
You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous   Next >   Cancel

6. [Choose Issuance Authorization Rules] を選択してから、[Permit all users to access this relying party] を選択します。



7. [Finish] を選択してから、[Open the Edit Claim Rules dialog for this relying party trust when the wizard closes] を選択して、[Close] をクリックします。

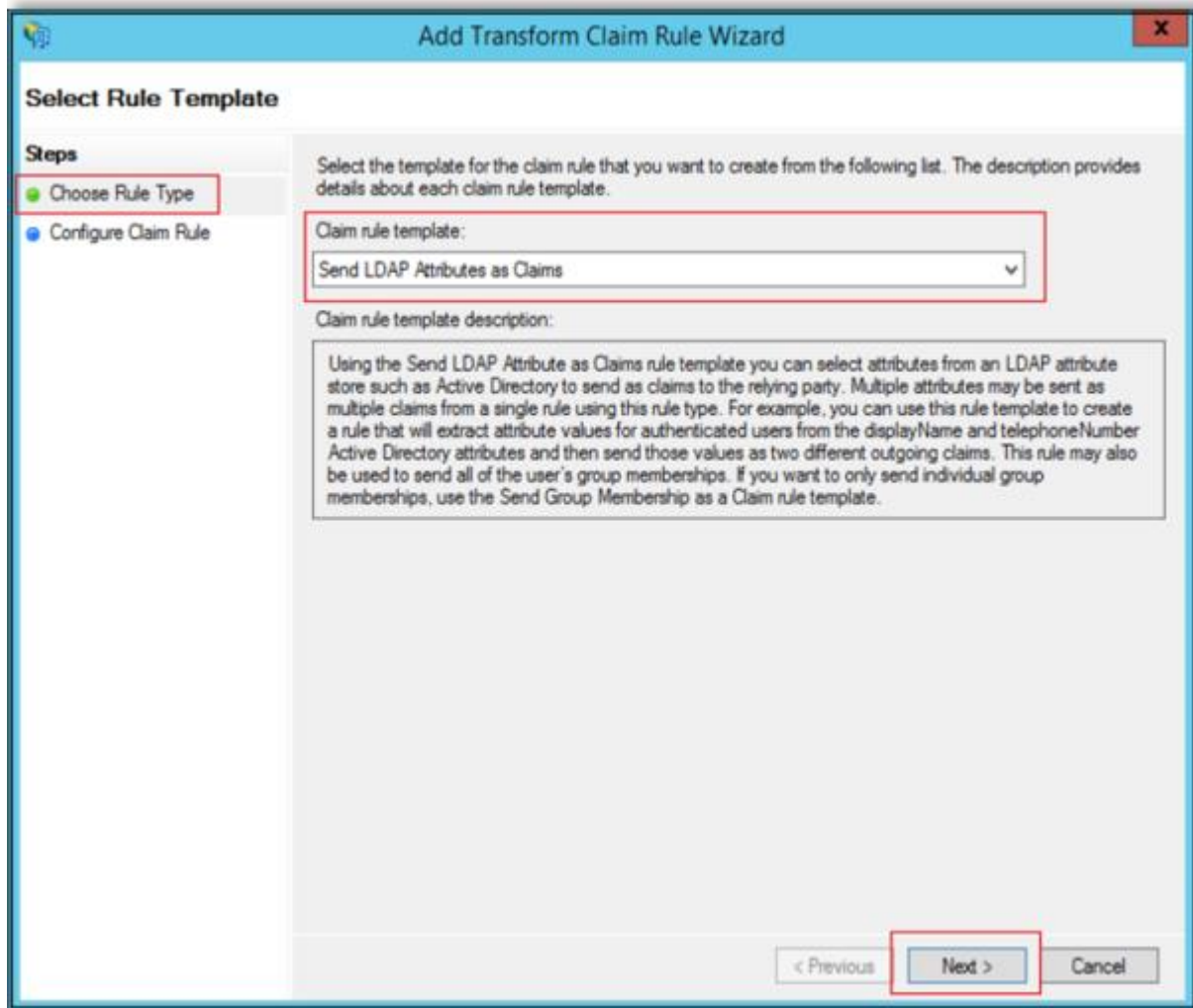


8. [Issuance Transform Rules] タブで [Add Rule...] を選択してから、[OK] をクリックします。





9. [Add Transform claim Rule Wizard] ウィンドウで、[Choose Rule Type] を選択します。
10. ドロップダウンから [Send LDAP Attributes as Claims] を選択し、[Next] をクリックします。



11. [Configure Claim Rule] を選択してから、[Claim rule name] フィールドに名前を入力します。
12. [Attribute Store] ドロップダウンで [Active Directory] を選択します。
13. マッピングを選択します。以下に示す値を推奨しますが、組織のニーズに適した値を選択することもできます。

**認証を成功させるには、一意の識別子を名前 ID の要求の種類にマッピングする必要があります。**この値は、LinkedIn ラーニングのユーザーを識別するために使用され、従業員 ID や UPN など、一意かつ不変である必要があります。

**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule**

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Test App Claim

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	Name ID
E-Mail-Addresses	E-Mail Address
Given-Name	Given Name
Surname	Surname
...	...

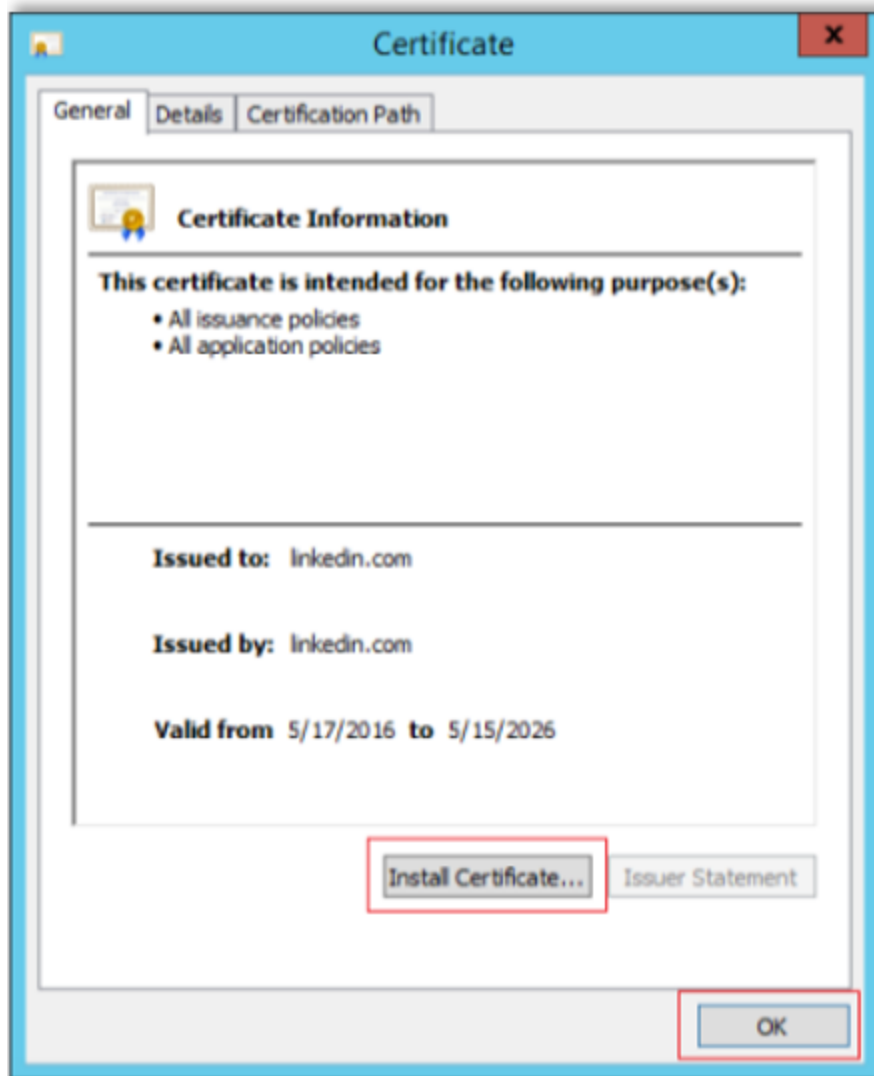
< Previous **Finish** Cancel

**注:** レポート作成またはグループ化のために、「役職」や「部門」などの追加の要求規則を作成することができます。

14. [Finish] をクリックして、次の画面で [OK] をクリックします。

## 証明書のインストール

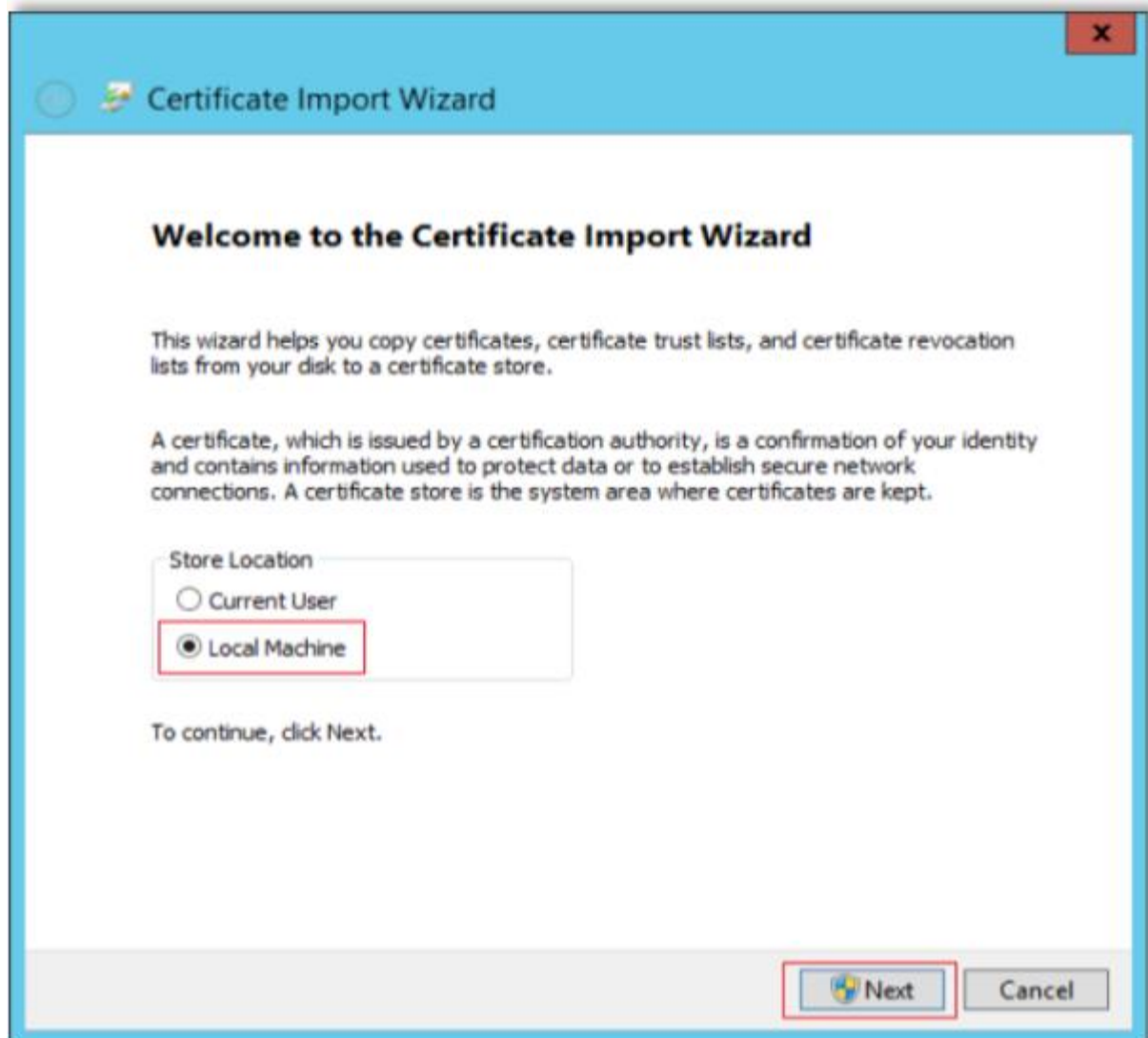
1. ADFS で、作成した証明書利用者信頼のプロパティに移動し、[Signature] タブをクリックします。証明書をダブルクリックします。ウィンドウがこのように表示される場合は、次のセクションに進みます。



上記のウィンドウが表示されない場合は、証明書をインストールします。

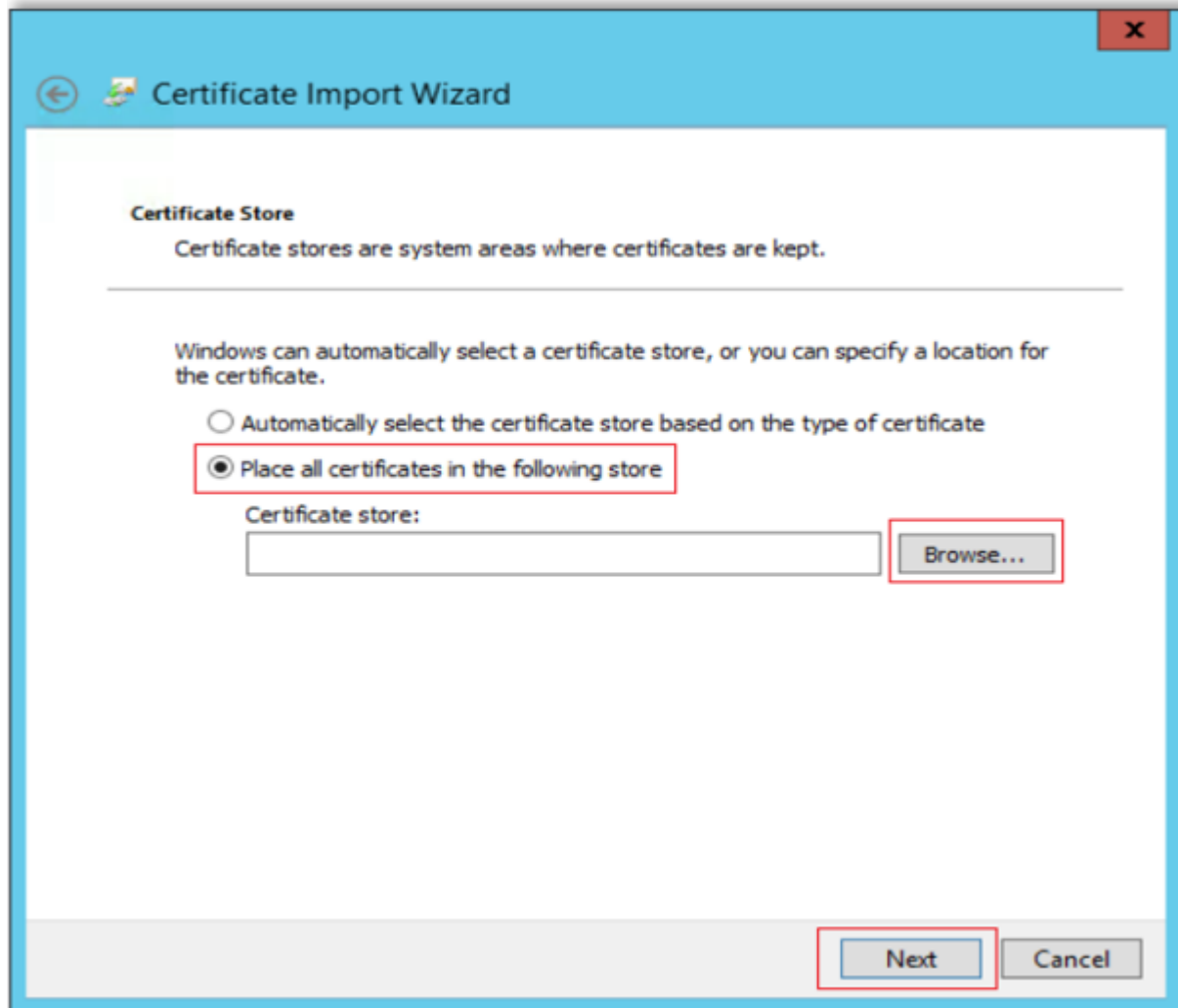
15. [Install Certificate...] をクリックして、ウィザードを開きます。

16. [Store Location] には、[Local Machine] を選択します。

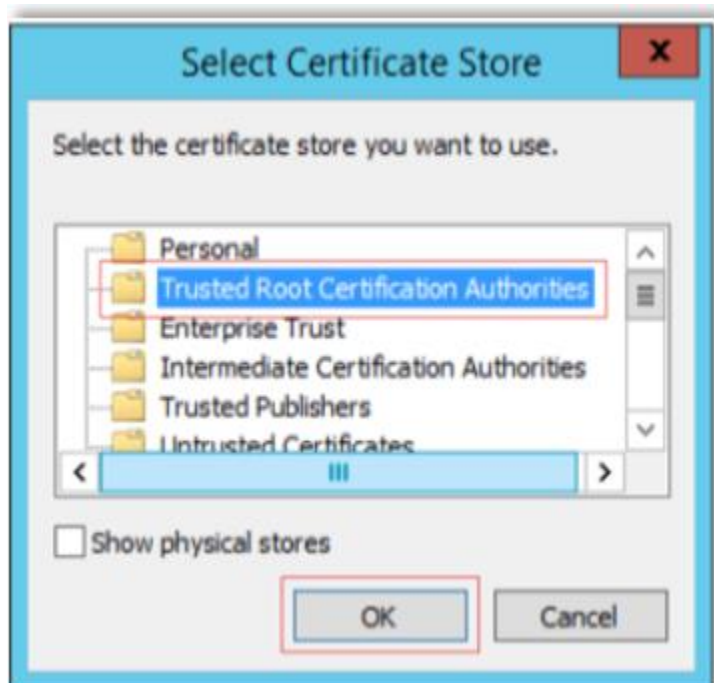


17. [Next] をクリックします。

18. 次の画面で、[Place all certificates in the following store] を選択し、[Browse] をクリックします。



19. [Trusted Root Certification Authorities] を選択します。

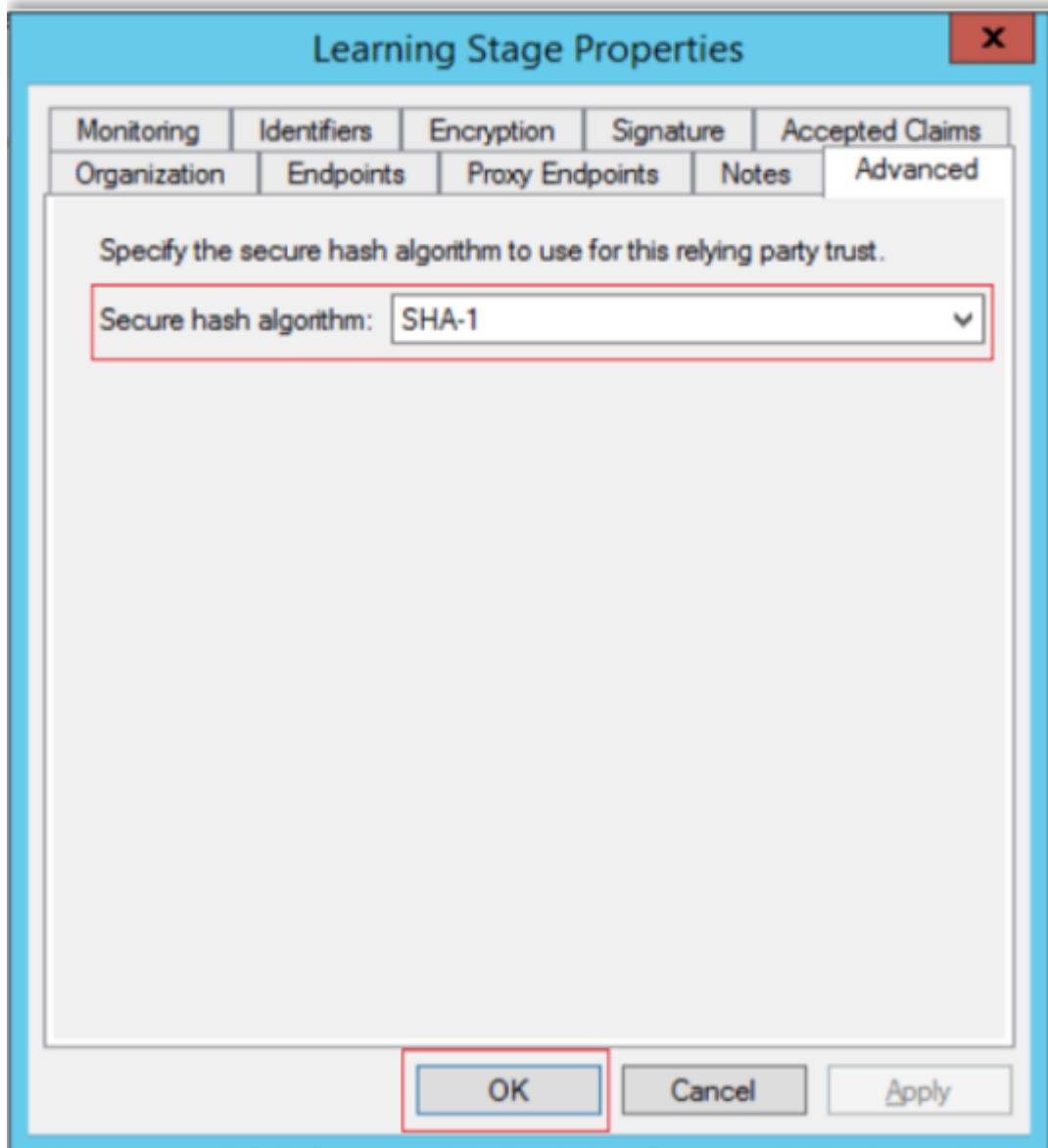


20. [OK] の次に [Finish] をクリックします。これで、証明書ウィンドウは上記と同様な外観になります。

## セキュアハッシュアルゴリズムの設定

1. 作成した証明書利用者信頼のプロパティで、[Advanced] タブに移動します。
21. セキュアハッシュアルゴリズムセクションで、[SHA-1] または [SHA-256] を選択します。

**注:** LinkedIn ラーニングのデフォルト設定は「SHA-1」です。[SHA-256] を選択した場合は、LinkedIn ラーニングで構成を完了する際に [SHA-256] も選択してください。



## SAML SSO の設定

ADFS と LinkedIn ラーニングで SAML SSO を設定するには、次の手順を実行します。

1. ADFS で [Endpoints] タブに移動します。
2. LinkedIn ラーニングからダウンロードした SP メタデータ XML ファイルを開いて、AssertionConsumerService URL を見つけて、エンドポイントに貼り付けます。

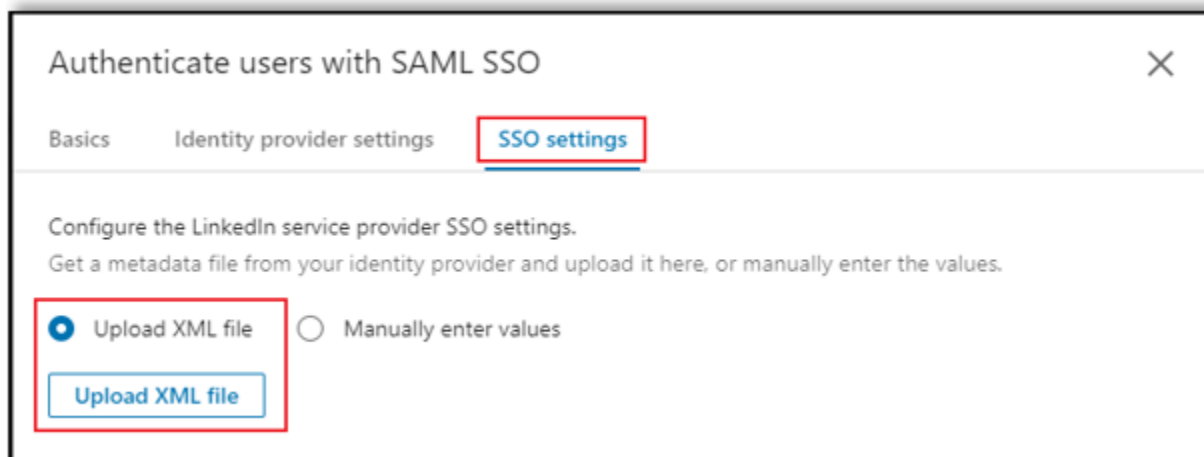


例: <https://www.linkedin.com/checkpoint/enterprise/saml/1234567?application=learning&appInstanceId=1234567&authModeId=1234567>

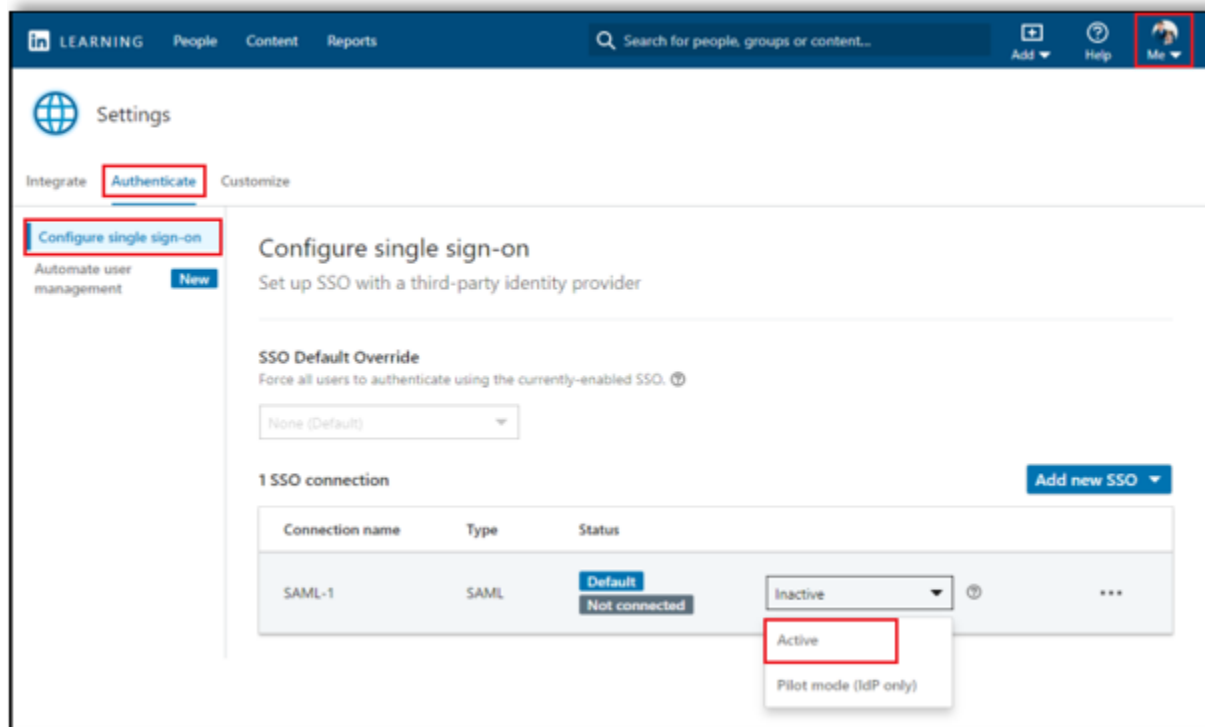
このフィールドは Assertion Consumer Service URL にマッピングされ、SAML 応答はユーザーエージェント経由で「POST」を送信します。つまり管理者は、このエンドポイントに応答を送信することで、IdP 起点のフローをトリガーします。

## ADFS メタデータの LinkedIn ラーニングへのアップロード

1. 次の形式を使用して、ADFS メタデータをダウンロードします (your.adfsserver.com を自分のサーバー名で置き換えます):  
<https://your.adfsserver.com/FederationMetadata/2007-06/FederationMetadata.xml>
2. XML ファイルをコンピューターに保存します。
3. [SAML SSO でユーザーを認証] 画面で [SSO の設定] を選択します。
4. [XML ファイルをアップロード] をクリックします。



5. ダウンロードした ADFS メタデータ XML ファイルを選択します。
6. ADFS で証明書利用者信頼を設定する際に、[SHA-256] を選択した場合は、[認証リクエスト署名アルゴリズム] に同じ値を選択します。[SHA-256] を選択しなかった場合は、SSO オプションをデフォルト値のままにします。
7. [保存] をクリックします。
8. 接続を [有効] に切り替えます。



## IdP 起点の認証フローをトリガーする

ID プロバイダーが開始する SSO をテストするには、次の形式を使用します (your.adfsserver.com を自分のサーバー名で置き換えます)。

<https://your.adfsserver.com/adfs/ls/IdpInitiatedSignOn.aspx>

## SP 起点の認証フローをトリガーする

1. 最初にブラウザーで、SSO を設定した 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=1234567>
2. サービスプロバイダーが開始する URL を作成するには次の形式を使用します。

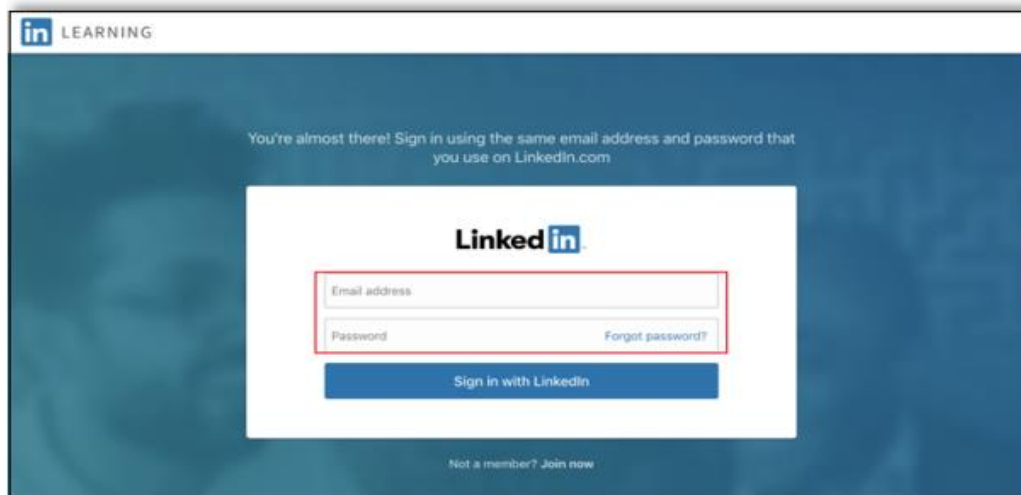
形式:

[https://www.linkedin.com/checkpoint/enterprise/login/\[accountid\]?application=learning](https://www.linkedin.com/checkpoint/enterprise/login/[accountid]?application=learning)

例:

<https://www.linkedin.com/checkpoint/enterprise/login/1234567?application=learning>

**注:** LinkedIn ラーニングアカウントで LinkedIn プロフィールのバインディングが有効になっている場合は、SSO 認証が成功した後に LinkedIn にログインするように求められることがあります。このログイン情報は、LinkedIn ラーニングのログイン情報を個人の LinkedIn アカウントに関連付けて、おすすめのコンテンツを促進するために使用されます。このプロンプトについて質問がある場合は、LinkedIn ラーニング専任のカスタマーサクセスマネージャーにお問い合わせのうえ、詳細をご確認ください。



以上で操作は完了です。受講者は、ADFS を使用して LinkedIn ラーニングの認証を受けることが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

- [SSO 実装ガイド](#)
- [Google SSO](#)
- [LTI 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](mailto:security@linkedin.com)までお問い合わせください。