シングル サインオン（製品共通）

設定ガイド

最終更新日: 2022 年 1 月 19 日

以下の SAP Concur ソリューションに適用されます。

- ☒ Expense
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Travel
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Invoice
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Request
  - ☒ Professional/Premium edition
  - ☒ Standard edition

目次

セクション 1: アクセス許可 1

セクション 2: 概要 1

機能の利点 1

必要事項 1

セクション 3: 必要なアクセス許可の取得 2

Professional Edition をお使いで Concur Travel をお持ちのお客様 2

Professional Edition をお使いで Concur Travel をお持ちでないお客様 Standard Edition をお使いのすべてのお客様 2

セクション 4: 設定 – Web ベース サービス向けの 2 つの設定方法 2

重要事項 3

アイデンティティ プロバイダ (IdP) 固有のプロセス 3

一般的なプロセス 4

セクション 5: Web ベース サービスの設定 – 一般的なプロセス 4

[シングル サインオンの管理] ページへのアクセス 5

暗号化を使用しない SSO アプリ/コネクタの設定 7

ステップ 1: エンティティ ID および ACS エンドポイントを入手する 7

ステップ 2: エンティティ ID および ACS エンドポイントを提供する 8

ステップ 3: 受信者 URL および宛先 URL を提供する 9

ステップ 4: NameID (IdP) がユーザーの Login_ID（SAP Concur ソリューション）と一致することを確認する 10

ステップ 5: IdP メタデータを入手する 11

ステップ 6: IdP メタデータを Concur にアップロードする 12

ステップ 7: IdP-Initiated SSO をテストする 15

ステップ 8: SP-Initiated SSO をテストする 17

ステップ 9: 任意または必須として SSO を有効化する 17

SSO 設定の編集 18

以前の変更を表示 19

暗号化を使用する SSO アプリ/コネクタの設定（オプション） 23

ステップ 1: 暗号化キーを入手して保存する 23

ステップ 2: IdP に encryption.crt をアップロードする 24

セクション 6: よくある質問 25

セクション 7: 付録: ADFS の設定 27

はじめに 27

ADFS の設定 29

SAP Concur サイトを設定する 37

SSO ログインのテスト 40

IdP 主導型の SSO をテストする 40
SP-Initiated SSO をテストする 40
Mobile シングル サインオン（SSO） 42
メール通知 42
展開 42
セクション 8: 付録 - Microsoft Azure AD の設定 43
はじめに 43
Azure AD アプリケーションを設定する 45
ステップ 1: ギャラリー アプリケーションを作成する 45
ステップ 2: ID および 応答 URL と Azure iD を提供する 46
ステップ 3: 一意のユーザー ID の変更 47
ステップ 5: Azure AD メタデータ ファイルをダウンロードする 48
SAP Concur サイトを設定する 49
SSO ログインをテストする 51
IdP-initiated SSO をテストする 51
SP-initiated SSO をテストする 52
モバイル シングル サインオン（SSO） 54
メール通知 54
展開 54
セクション 9: 付録- Idaptive の設定 55
はじめに 55
Idaptive アプリケーションを設定する 57
ステップ 1: Idaptive アプリを作成する 57
SAP Concur サイトを設定する 60
SSO ログインをテストする 61
IdP-initiated SSO をテストする 61
SP-initiated SSO をテストする 61
モバイル シングル サインオン（SSO） 63
メール通知 63
展開 64
セクション 10: 付録- Okta の設定 64
はじめに 64
Okta アプリケーションを設定する 66
ステップ 1:SAP Concur メタデータを入手する 66
ステップ 2: Okta でアプリケーションを作成する 68
ステップ 3: 名前 ID の構成 70
ステップ 4:（オプション）アプリケーションを暗号化する 71
ステップ 5: 設定の完了 73

ステップ 6: メタデータ ファイルをダウンロードする 74
SAP Concur サイトを設定する 75
SSO ログインをテストする 78
IdP-initiated SSO をテストする 78
SP-Initiated SSO をテストする 79
モバイル シングル サインオン（SSO） 79
メール通知 81
展開 81
以前の変更を表示 82
セクション 11: 付録- PingOne の設定 83
はじめに 83
PingOne アプリケーションを設定する 85
ステップ 1: 非ギャラリー SAML アプリケーションを作成する 85
ステップ 2: アプリケーションの詳細 85
ステップ 3: アプリケーションの設定 86
ステップ 4: 属性マッピング 88
ステップ 5: ユーザー グループにアクセスを付与する 89
ステップ 6: 見直しと完了 89
SAP Concur サイトを設定する 90
SSO ログインをテストする 91
IdP-Initiated SSO のテスト 91
SP-Initiated SSO のテスト 92
モバイル シングル サインオン（SSO） 93
メール通知 93
展開 93
セクション 12: 付録 - SAP Identity Authentication Service (IAS) 設定 95
はじめに 95
SAP IAS アプリケーションを設定する 97
ステップ 1:SAP Concur メタデータを入手する 97
ステップ 2: SAP IAS でアプリケーションを作成する 98
ステップ 3: [Subject Name Identifier] を変更する 101
ステップ 4: [Default Name ID Format] を変更する 102
ステップ 5: メタデータをダウンロードする 103
SAP Concur サイトを設定する 105
SSO ログインのテスト 108
IdP-initiated SSO のテスト 108
SP-Initiated SSO のテスト 109
モバイル シングル サインオン（SSO） 110

メール通知 111
展開 111
以前の変更を表示 112
セクション 13: 付録: SAP NetWeaver の設定 115
概要 115
SAP NetWeaver アプリケーションを設定する 117
ステップ 1:SAP Concur メタデータを入手する 117
ステップ 2: SAP NetWeaver でアプリケーションを作成する 118
ステップ 3: 名前 ID 設定 120
ステップ 4: アプリケーションを有効化する 121
ステップ 5: メタデータ ファイルをダウンロードする 122
SAP Concur サイトを設定する 122
SSO ログインをテストする 125
IdP-initiated SSO のテスト 125
SP-Initiated SSO をテストする 126
モバイル シングル サインオン（SSO） 126
メール通知 128
展開 128
以前の変更を表示 129

改訂履歴

日付	注意事項 / コメント / 変更内容
2022 年 1 月 19 日	*Web* ベース サービスの設定 内の、*Concur* への *IdP* メタデータのアップロード の説明を更新しました。
2021 年 07 月 27 日	SSO 設定に関するインストラクションの付録を複数追加しました。
2021 年 04 月 15 日	著作権を更新しました。その他の変更はありません。表紙の日付は更新されていません。
2021 年 03 月 26 日	新しい「以前の変更を表示」機能に関する情報を追加しました。
2020 年 12 月 2 日	誤字を修正しました。。（表紙の日付は変更されていません。）
2020 年 11 月 14 日	初版発行

シングル サインオンの管理

セクション 1: アクセス許可

この機能を使用する際は、管理者のアクセス許可が必要です。

このガイドに記載されている作業は SAP Concur サポートにのみ許可されているものもあります。必要に応じて SAP Concur サポートにご依頼ください。

セクション 2: 概要

シングル サインオン（SSO）により、ユーザーは一組のサインイン資格情報を使用して複数のアプリケーションにアクセスすることができます。SSO を設定するためのセルフサービス オプションを提供します。

現在、SAP Concur ソリューションには、ユーザー名およびパスワードの使用、**または**ユーザーの組織のサインイン資格情報などのアイデンティティ プロバイダ（IdP）の資格情報のある SSO の使用、という 2 つのサインイン方法があります。SSO は現在、経費精算、請求書処理、事前申請、および出張予約でサポートされています。

この機能を設定することで、組織のユーザーにシングル サインオンを設定することができます。

機能の利点

シングル サインオンの管理機能では、次の機能が提供されます。

- 組織管理者が Web とモバイルの両方のプラットフォームに IdP-initiated SSO と SP-initiated SSO を組織に設定することができるセルフサービス オプション
- 既存の SSO 機能を現在使用している企業が、新しいシングル サインオンの管理機能も活用できる機能（両方の SSO オプションが同時に機能します）
- すべてのユーザーに SSO を要求する機能
- ユーザーのサインイン方法の改善
- ユーザーのサインイン成功率の向上

本ガイドでは、SAP Concur サービスのシングル サインオンの管理を有効化し、設定する方法を説明しています。

必要事項

この機能を使用するには、SAML 2.0 標準をサポートする IdP（アイデンティティ プロバイダ）

を利用しており、IdP メタデータを生成できる必要があります。

セクション 3:　必要なアクセス許可の取得

ユーザーが **[シングル サインオンの管理]** ページにアクセスするには、組織管理（Travel）権限が割り当てられている必要があります。

ユーザーは必要なアクセス許可が割り当てられると、**[シングル サインオンの管理]** ページにアクセスすることができるようになります。SAP Concur Professional Edition と Standard Edition では、ページを移動する方法が異なります。

📖 SAP Concur Professional Edition および Standard Edition でページにアクセスする方法の説明については、本ドキュメントのセクション 5 に記載された「シングル サインオンの管理ページへのアクセス」をご参照ください。

Professional Edition をお使いで Concur Travel をお持ちのお客様

Professional Edition をお使いで Concur Travel をお持ちのお客様の場合、組織管理（Travel）権限を持つすべてのユーザーに対して、**[認証管理]** メニューが自動的に表示されます。

追加のユーザーにアクセスを提供するために、顧客は **[管理] > [会社] > [組織管理] > [ロール管理]**（左側メニュー）で組織管理（Travel）権限を割り当て、**[出張予約]** タブをクリックします。

📖 ロールと権限の割り当てに関する詳細情報は、ユーザー ガイド「ユーザー管理（製品共通）」をご参照ください。

Professional Edition をお使いで Concur Travel をお持ちでないお客様
Standard Edition をお使いのすべてのお客様

Professional Edition をお使いで Concur Travel をお持ちでないお客様や Standard Edition をお使いのお客様は、必要なアクセス権限の取得について SAP Concur サポートにお問い合わせください。SAP Concur サポートが目的のユーザーに権限を割り当てます。

セクション 4:　設定 – Web ベース サービス向けの 2 つの設定方法

SSO の設定には次の 2 つの方法があります。

- アイデンティティ プロバイダ（IdP）固有のプロセスに従う

  - または -

- 一般的なプロセスに従う（下記に記載）

重要事項

両方の方法を下記に記載します。ただし、**個々の管理者は一般的なプロセスの情報を精査する必要があります。**場合によっては、IdP が提供する情報を使用しても、一般的なプロセスのステップが必要になることがあります。

アイデンティティ プロバイダ（IdP）固有のプロセス

SAP Concur は信頼性の高い統合プロセスを構築するために、複数の IdP と連携しました。以下の IdP のいずれかをお使いの場合、最良の方法として、SSO を設定する際に、以下の表で該当するリンクをクリックして説明に従ってください。

NOTE: このセクションの説明はサード パーティー プロバイダにより提供されており、 SAP Concur はその正確性を保証することはできません。

問題が発生した場合は、サード パーティー プロバイダのサポートにご連絡ください。

アイデンティティ プロバイダ	設定 URL
ADFS	本ガイドの付録を参照してください。
Azure AD	本ガイドの付録を参照してください。詳細はこちらをご覧ください: https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/concur-travel-and-expense-tutorial
Idaptive	本ガイドの付録を参照してください。
JumpCloud	https://jumpcloud-support.force.com/support/s/article/Single-Sign-On-SSO-with-Concur-Travel-and-Expense
Okta	本ガイドの付録を参照してください。詳細はこちらをご覧ください: https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Concur-Travel-and-Expense.html

アイデンティティ プロバイダ	設定 URL
OneLogin	次のいずれかを選択します。 • アメリカ（北米）のデータ センターをお使いの SAP Concur お客様の場合: htpps://{subdomain}.onelogin.com/apps/new/124919 • EMEA のデータ センターをお使いの SAP Concur お客様の場合: https://{subdomain}.onelogin.com/apps/new/125208 • 中国 のデータ センターをお使いの SAP Concur お客様の場合: https://{subdomain}.onelogin.com/apps/new/127148 次の点にご注意ください。 • 記載されているように、お使いの OneLogin ドメインを上記の URL に追加する必要があります。 • 上記の URL を使用して SAP Concur アプリを OneLogin に追加すると、**[設定]** タブが表示されます。SAP Concur への OneLogin メタデータのアップロードに関する説明については、そのタブにアクセスする必要があります。
Ping Identity	本ガイドの付録を参照してください。
SAP Identity Authentication Service (IAS)	本ガイドの付録を参照してください。
SAP NetWeaver	本ガイドの付録を参照してください。

一般的なプロセス

上記の表に記載されていない IdP をお使いの場合、セクション 5 の該当する手順に従います。セクション 5 には、以下の設定に関する手順が記載されています。

- 暗号化を**使用しない** SSO アプリ/コネクタ
- 暗号化を**使用する** SSO アプリ/コネクタ

セクション 5: Web ベース サービスの設定 – 一般的なプロセス

適切なアクセス許可が割り当てられると、SSO を設定できるようになります。以降のページでは、以下について説明します。

- **シングル サインオンの管理** ページへのアクセス
- 暗号化を使用しない SSO アプリ/コネクタの設定
- 暗号化を使用する SSO アプリ/コネクタの設定（オプション）

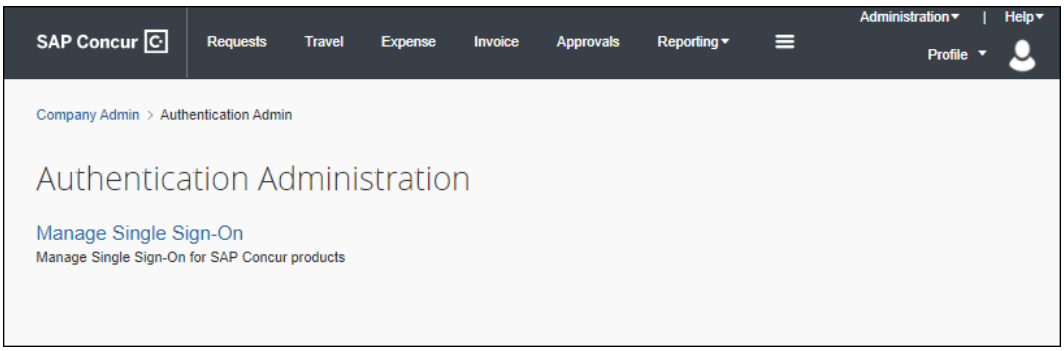
[シングル サインオンの管理] ページへのアクセス

ユーザーが **[シングル サインオンの管理]** ページにアクセスするには、組織管理（Travel）権限が割り当てられている必要があります。

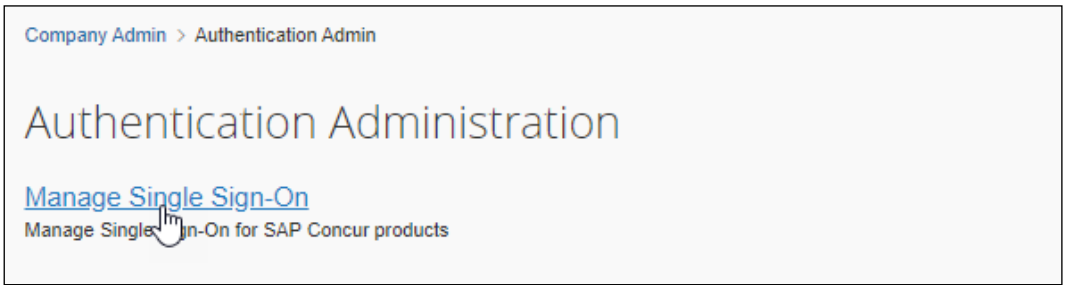
📖 必要な権限の取得については、セクション 3 をご参照ください。

Professional または Standard Edition の [シングル サインオンの管理] ページにアクセスするには:

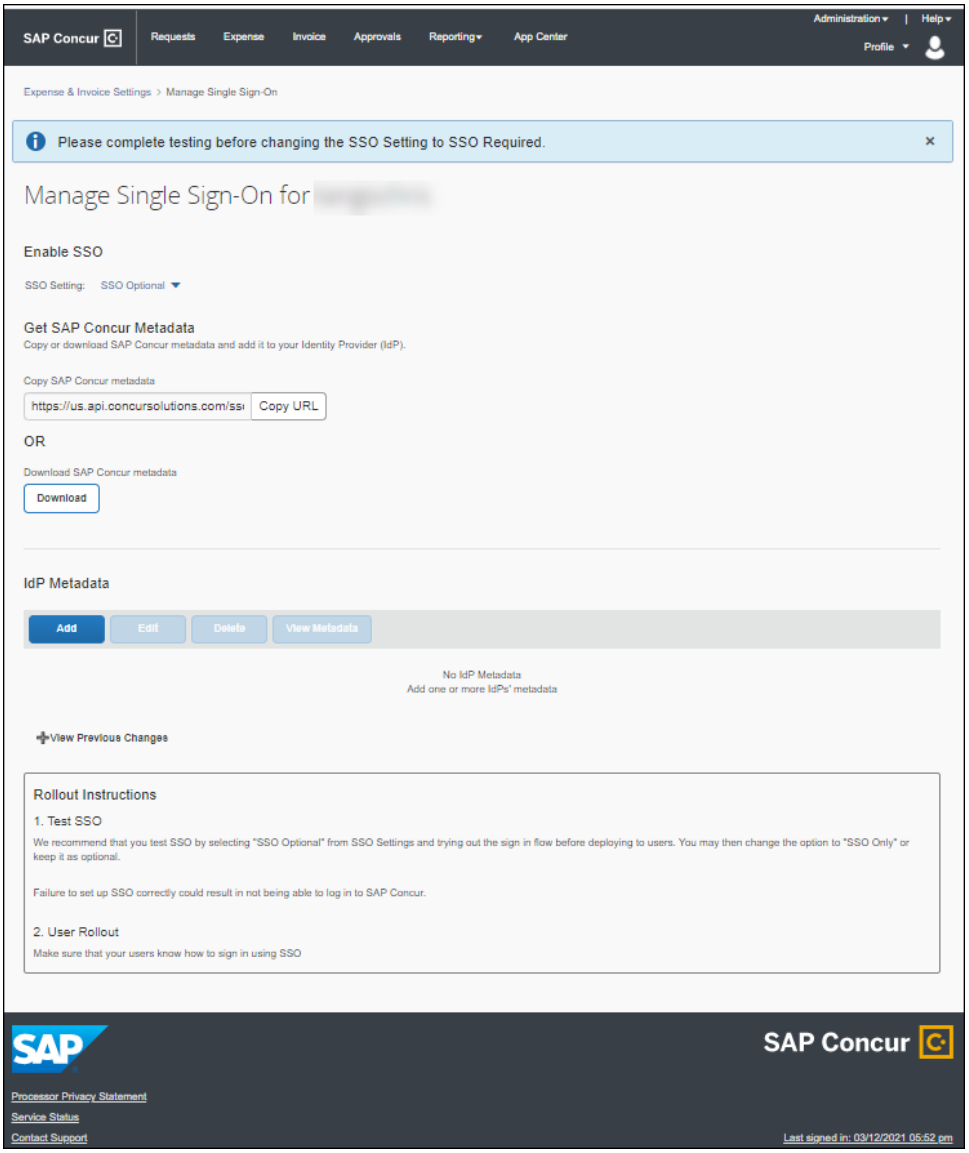
1. **[管理]** > **[会社]** > **[認証管理]** をクリックします。**[認証管理]** ページが表示されます。



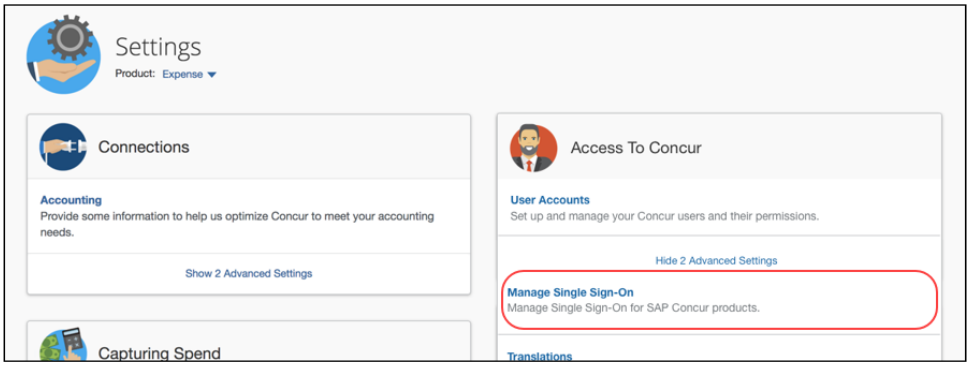
2. **[シングル サインオンの管理]** をクリックします。



[シングル サインオンの管理] ページが表示されます。



SAP Concur Standard Edition では、[製品設定] からも **[シングル サインオンの管理]** ページにアクセスすることができます。



暗号化を使用しない SSO アプリ/コネクタの設定

ステップ 1 およびステップ 6 は SAP Concur サービスで処理を行います。SAP Concur サポートにお問い合わせください。

ステップ 2 からステップ 5 はご利用の IdP で処理を行います。ご不明な点がありましたら、ご利用のアイデンティティプロバイダにお問い合わせください。

ステップ *1:* エンティティ *ID* および *ACS* エンドポイントを入手する

エンティティ ID とは SAP Concur SSO の一意識別子であり、ACS エンドポイントはご利用の IdP が SAP Concur ソリューションに POST SAML アサーションを行うために使用するエンドポイントです。どちらも IdP で必要になります。

SAP Concur SP メタデータを確認することで、エンティティ ID および ACS エンドポイントを入手することができます。本ドキュメントに記載された該当地域（データ センター）の URL をクリックする、または **[シングル サインオンの管理]** ページからメタデータを確認することができます。

- **お使いのデータ センターが所在する地域の *URL* をクリックして、エンティティ *ID* および *ACS* エンドポイントを取得するには*:***
  - エンティティがホストされている地域（データ センター）の後の URL をクリックし、SAP Concur SP メタデータを確認します。

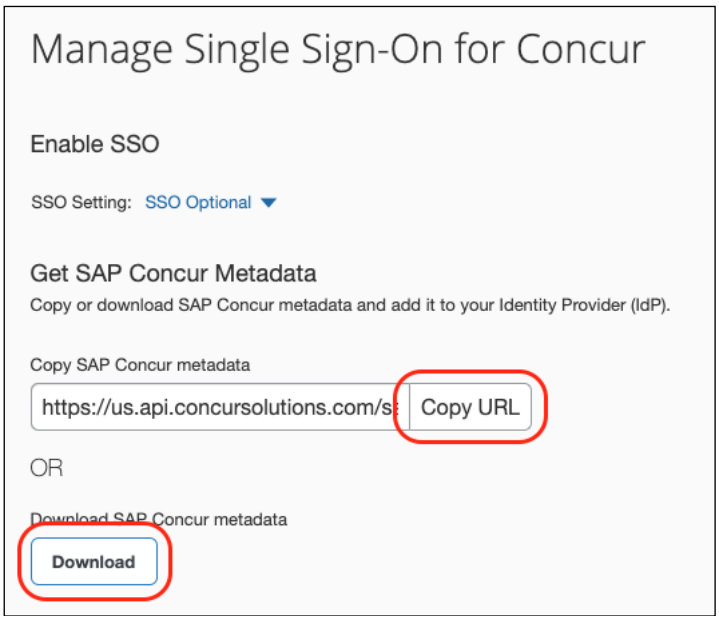
    NOTE: 推奨ブラウザは Google Chrome です。

    - **アメリカ（北米）:** https://www-us.api.concursolutions.com/sso/saml2/V1/sp/metadata/
    - **EMEA:** https://www-emea.api.concursolutions.com/sso/saml2/V1/sp/metadata/
    - **中国:** https://www-cn.api.concurcdc.cn/sso/saml2/V1/sp/metadata

- ***[シングル サインオンの管理] ページからメタデータを表示するには*:**

  1. **[管理]** > **[会社]** > **[認証管理]** をクリックしてから、**[シングル サインオンの管理]** をクリックします。

2. **[URL コピー]** または **[ダウンロード]** をクリックします。



以下は、https://www-us.api.concursolutions.com/sso/saml2/V1/sp/metadata/ の SAP Concur US SP メタデータのサンプルです。

赤枠はそれぞれエンティティ ID と ACS エンドポイントを示しています。

ステップ *2:* エンティティ *ID* および *ACS* エンドポイントを提供する

ご利用の IdP のカスタム アプリ/コネクタにエンティティ ID および ACS エンドポイントを提供します。

! **重要:** 本ガイドの「アイデンティティ プロバイダ (IdP) -固有のプロセス」セクションの表にご利用の IdP が記載されていない場合、IdP の ギャラリーや事前に構成された SAP Concur アプリ/コネクタを使用しないでください。従来のエンドポイントを持つ従来のアプリ/コネクタであるため、新しい SAP Concur SSO サービスと連携しません。その代わりに、IdP の**カスタム** アプリまたはコネクタを使用します。頻繁に「アイデンティティ プロバイダ (IdP) -固有のプロセス」セクションに戻り、ご利用の IdP が表に追加されているかどうかを確認してください。

様々な IdP がエンティティ ID や ACS エンドポイントに異なる名称を使用しています。下表は、多くの一般的な IdP のフィールド名を記載しています。

IdP	エンティティ ID の名前	ACS エンドポイントの名前
Okta	Audience URI (SP EntityID)	Single sign on URL
Azure AD	ID（エンティティ ID）	応答 URL（アサーション コンシューマー サービス URL）
OneLogin	対象	ACS (Consumer) URL
Ping	SP entityID	ACS URL
JumpCloud	SP Entity ID / SP Issuer / Audience	Assertion Consumer Service (ACS) URL

エンティティ ID や ACS エンドポイントの追加先が分からない場合は、ご利用のアイデンティティ プロバイダにお問い合わせください。

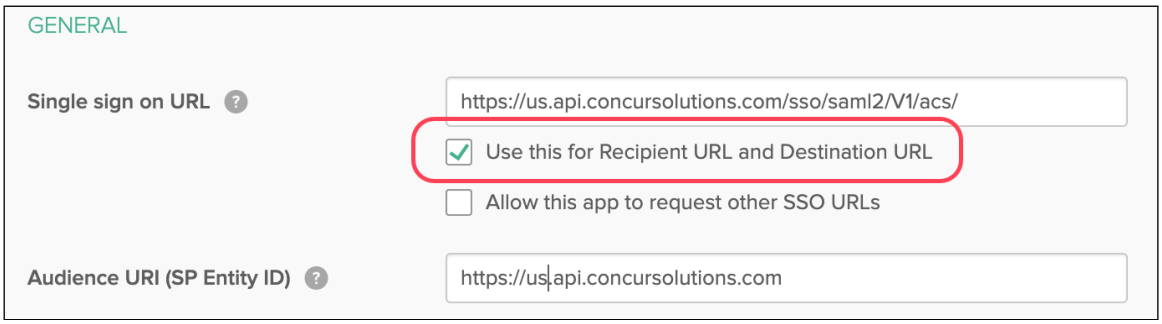
ステップ 3: 受信者 URL および宛先 URL を提供する

受信者 URL および宛先 URL を IdP のカスタム アプリ/コネクタに提供します。

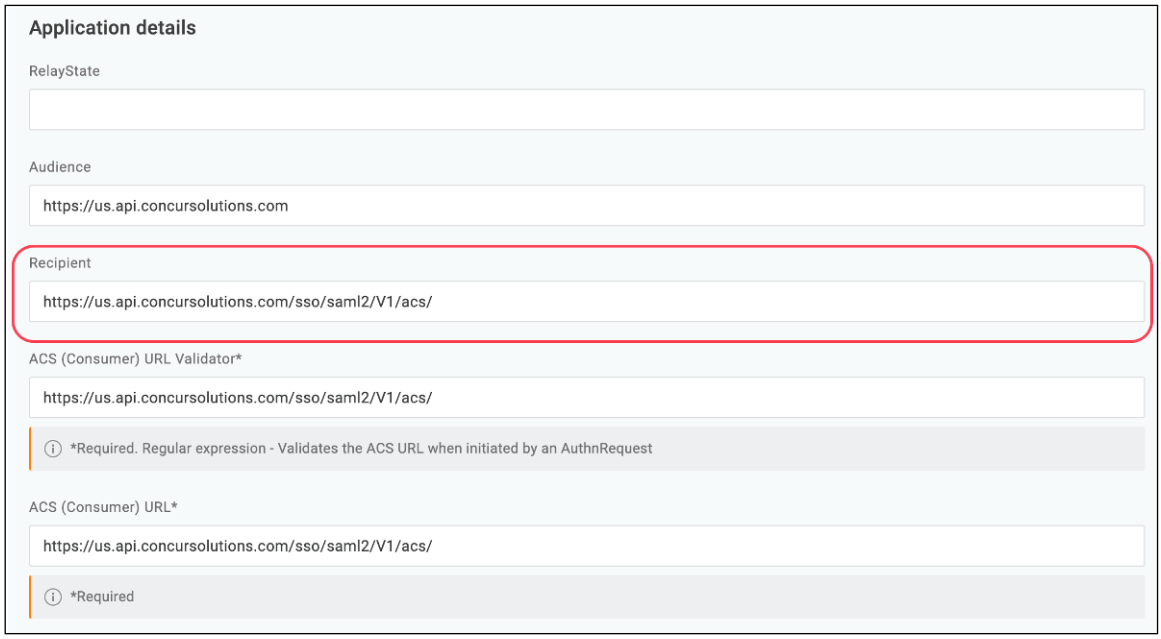
NOTE: このステップは一部の IdP では任意ですが、他の IdP では必須になります。IdP で受信者 URL および宛先 URL が必要な場合、SAP Concur SP メタデータから入手した ACS エンドポイントを使用してそれらのフィールドに記入することができます。

IdP による受信者 URL および宛先 URL の追加処理の例を以下に示します。

Okta の場合、受信者 URL と宛先 URL として ACS エンドポイントを使用するオプションがあります。



OneLogin の場合、受信者 URL を入力するフィールドがあります（宛先 URL のオプションはありません）。



ステップ *4: NameID (IdP)* がユーザーの *Login_ID*（*SAP Concur* ソリューション）と一致することを確認する

NameID フィールドの値が SAP Concur ユーザーの Login_ID と一致することを確認します。IdP は SAMLResponse XML ファイルを SAP Concur ソリューションに送信しますが、次の例に示すとおり、その SAMLResponse ファイル内には NameID フィールドがあります。

```
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">username@domain.com</saml2:NameID>
```

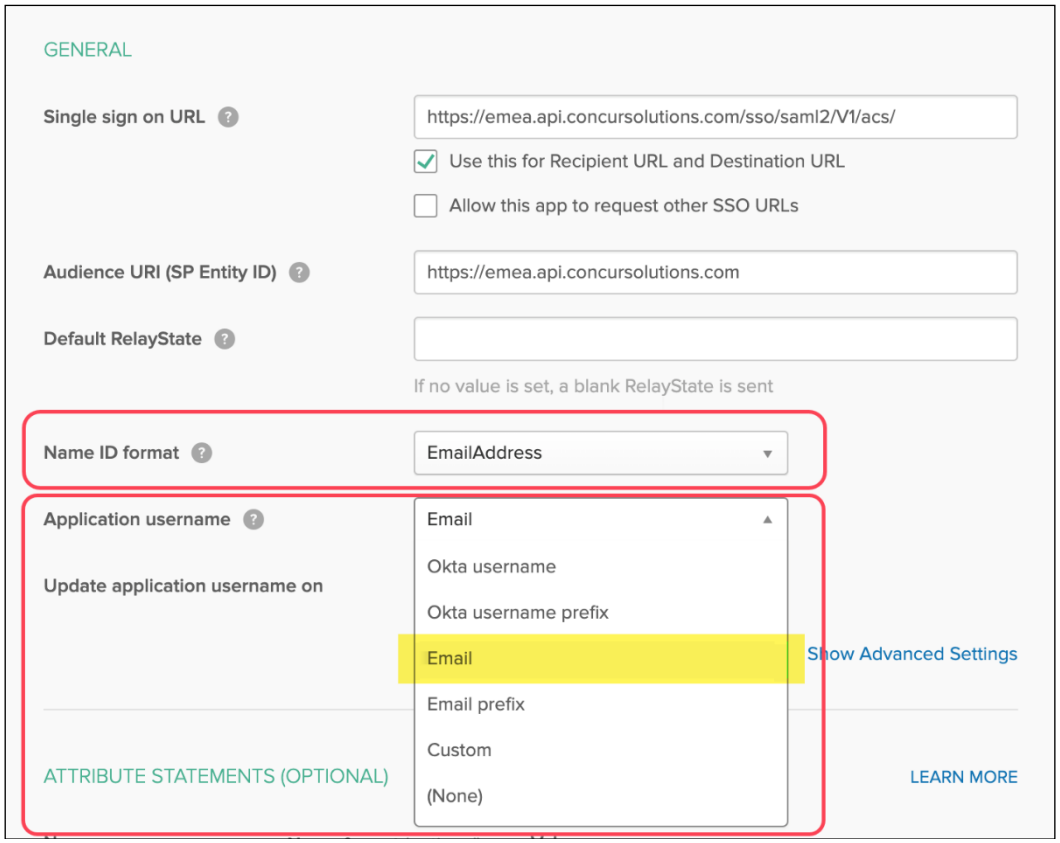
SAP Concur は、NameID フィールドから Login_ID まで *username@domain.com* を照合します。一致しない場合、SAP Concur ソリューションは正しいユーザーを特定することができないため、サインインは失敗します。

NOTE: ご利用の IdP でお使いのメール アドレスが SAP Concur Login_ID と一致しない場合、カスタム ルールを使用して Concur で Login_ID と一致するメール アドレスまたはユーザー名を作成します。

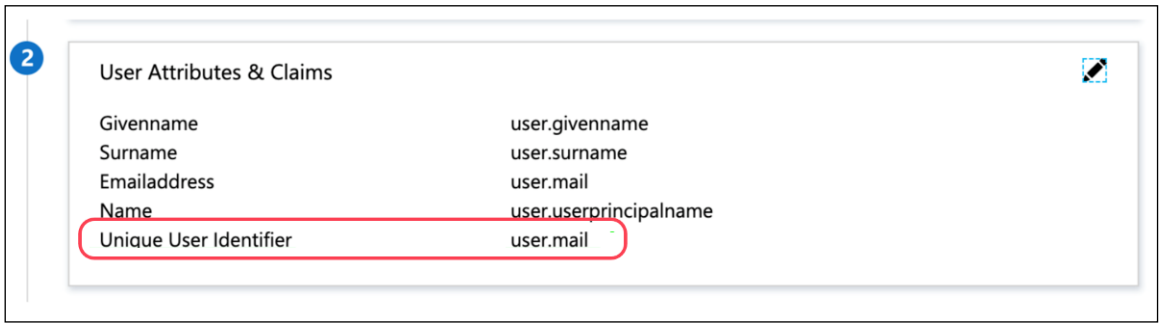
IdP からのメール アドレスが SAP Concur の Login_ID と異なっているのはよくあることです。このような場合は、IdP 側で可能な設定の例を以下に示します。

Okta の場合:

- **[Name ID format]** フィールドで、**[EmailAddress]** を選択します。
- **[Application username]** フィールドで、**[Email]** を選択します。



Azure AD の場合、**[Unique User Identifier]** フィールドを「user.mail」に編集します。



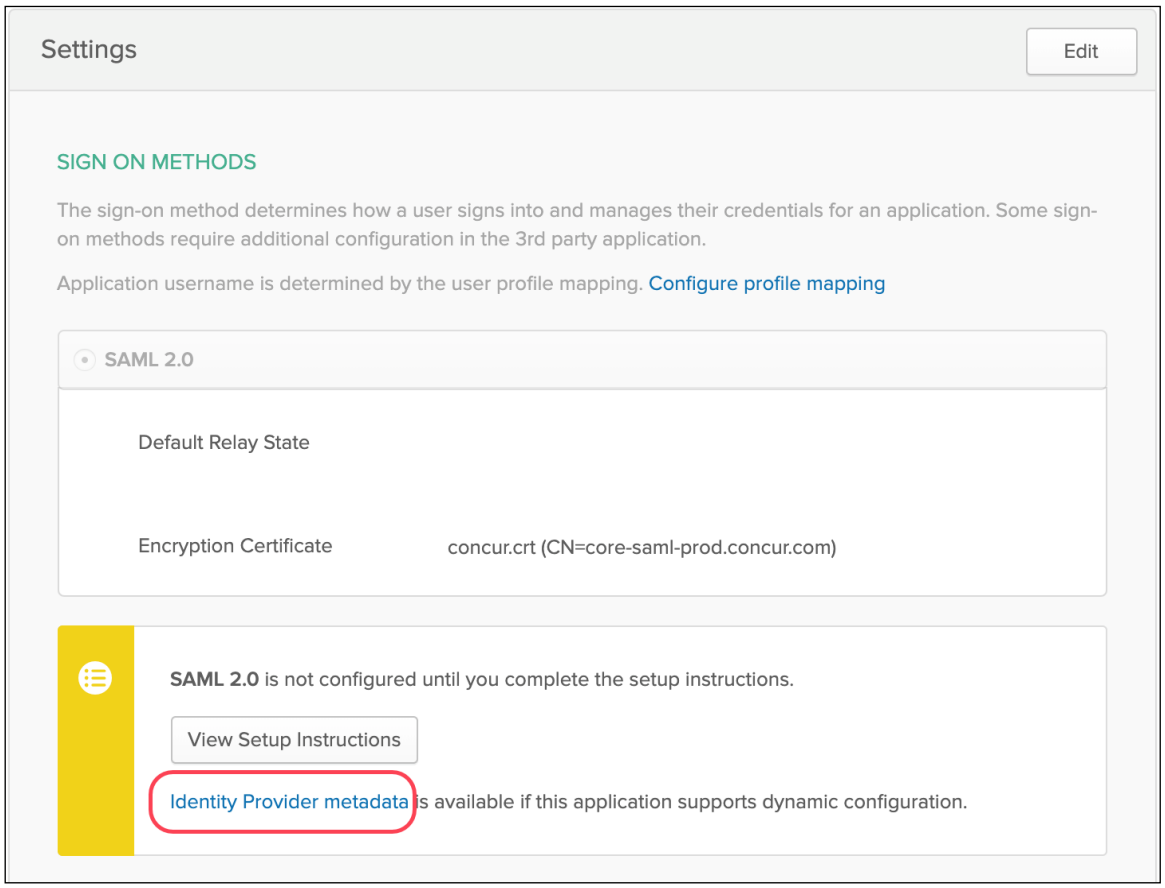
NameID フィールドの設定方法が分からない場合は、ご利用のアイデンティティ プロバイダにお問い合わせください。

ステップ 5: IdP メタデータを入手する

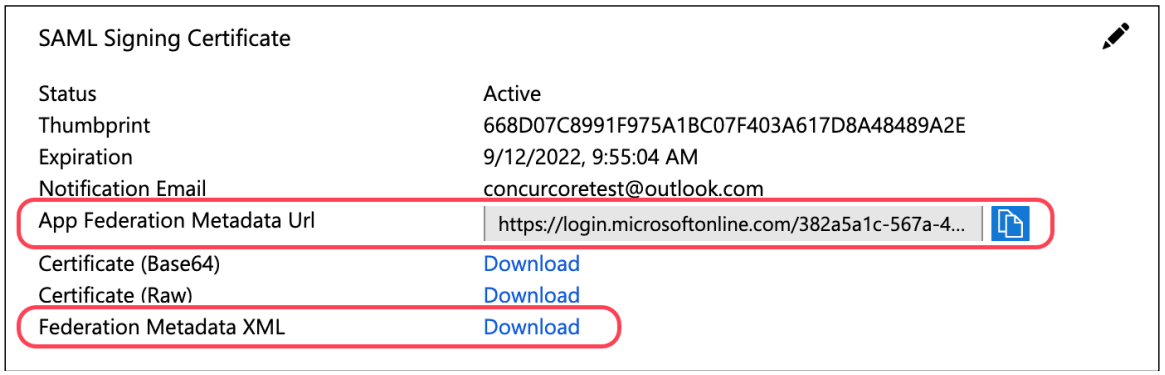
IdP は、IdP メタデータ ファイルまたは IdP メタデータ リンクを生成します。SAP Concur ソリューションでは、どちらともサポートしています。Okta と Azure AD の例を以下に示します。

NOTE: ご利用の IdP のメタデータへのアクセス方法が不明の場合は、IdP にお問い合わせください。

Okta の場合、**[Identity Provider Metadata]** リンクを使用します。



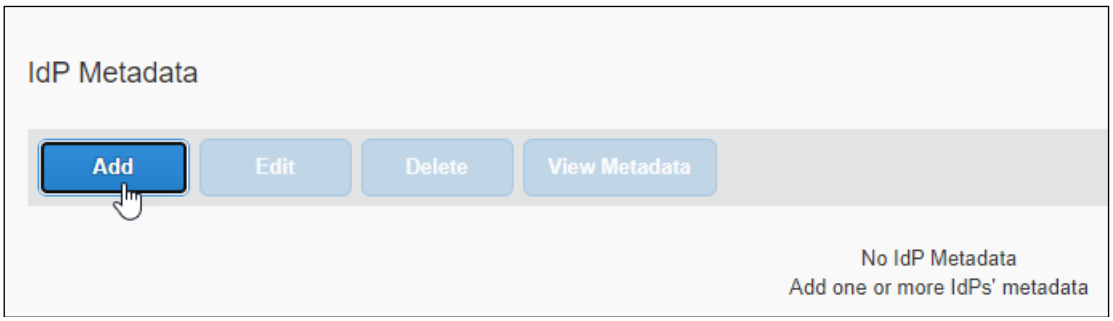
Azure AD の場合、**[アプリのフェデレーション メタデータ URL]** リンクまたは **[フェデレーション メタデータ XML]** ダウンロードを使用します。



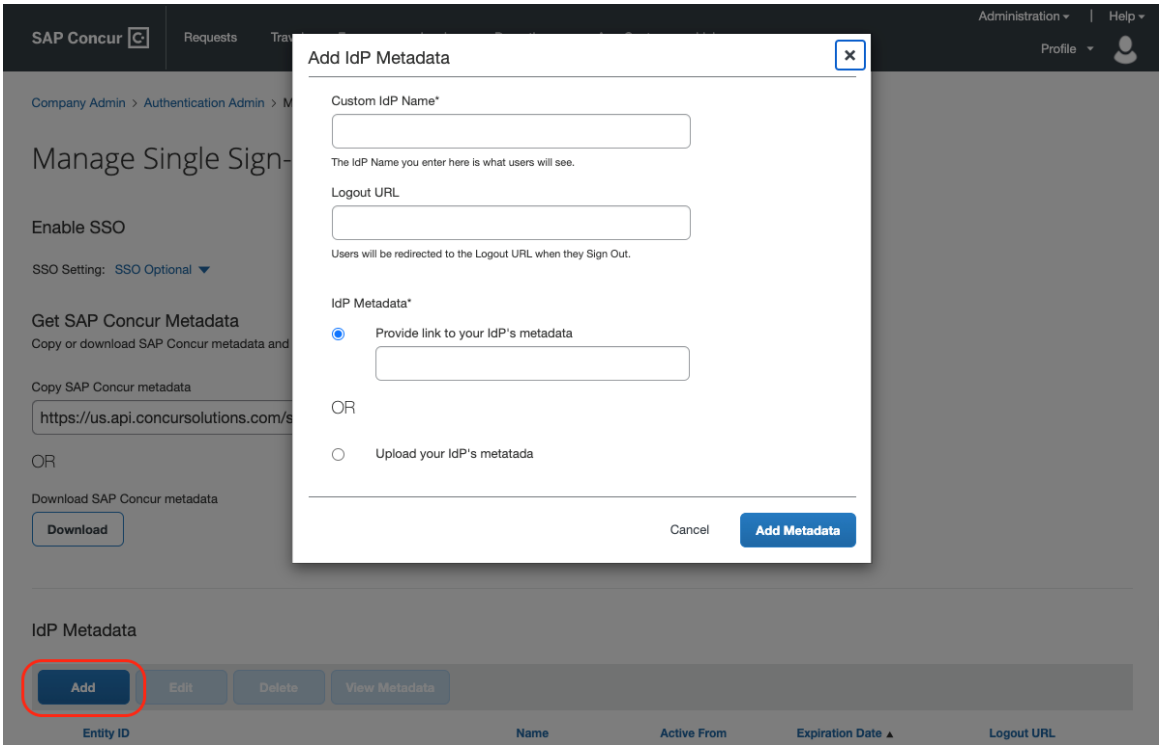
ステップ 6: IdP メタデータを Concur にアップロードする

1. **[管理]** > **[会社]** > **[認証管理]** をクリックしてから、**[シングル サインオンの管理]** をクリックします。

2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。

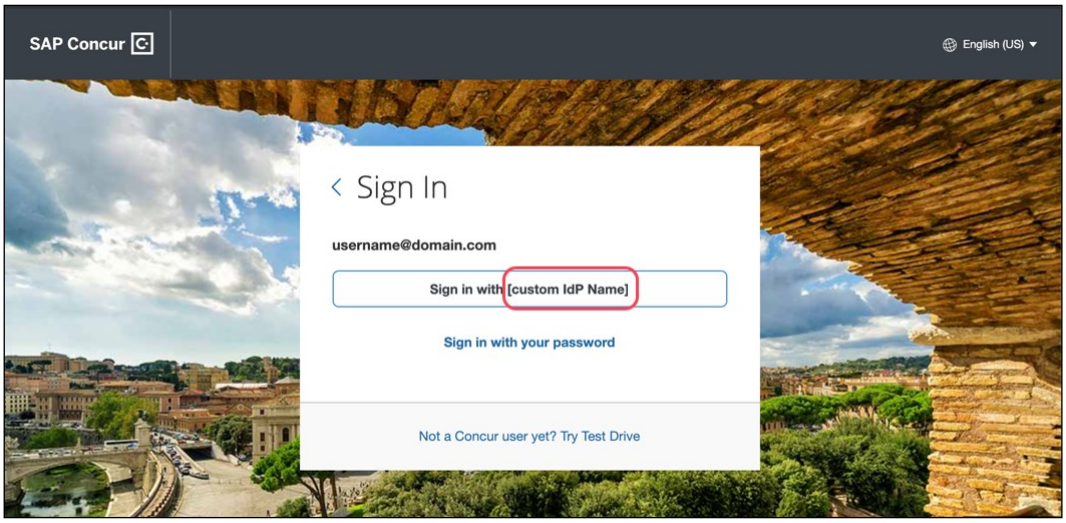


[IdP メタデータの追加] ウィンドウが表示されます。



3. **[カスタム IdP 名]** フィールドに名前を入力します。

入力する名前は、**[サインイン]** ページのユーザーに表示されます。ベスト プラクティスは単純に IdP 名を入力することです。たとえば、ご利用の IdP が Okta であり、このフィールドに「Okta」と入力する場合、ユーザーには [Okta を使用してサインイン] と表示されるようになります。



4. **[ログアウト URL]** フィールドにログアウト URL を入力します。

   既定では、もしこのフィールドが空欄のままの場合、ユーザーは SAP Concur からサインアウトした際に、認証プロセスを開始した場所にリダイレクトされます。

   カスタム ログアウト URL が指定されている場合、ユーザーは SAP Concur ソリューションからサインアウトすると、指定された URL にリダイレクトされます。

5. メタデータ リンクをコピーしたか、IdP からメタデータ ファイルをダウンロードしたかに応じて、次のいずれかを行います。

   - **[IdP のメタデータへのリンクの設定]** をクリックし、リンクを貼り付けます。

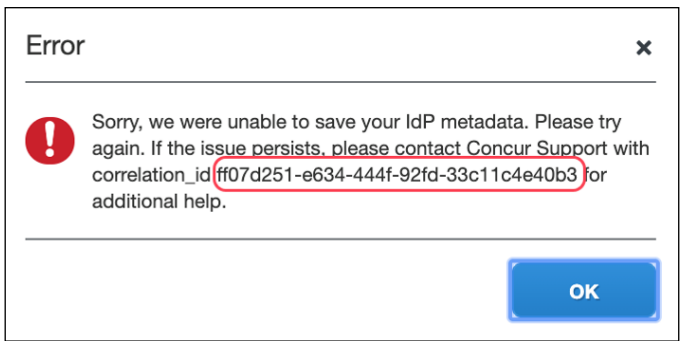
     - または -

   - **[IdP のメタデータのアップロード]** をクリックします。

6. **[メタデータの追加]** をクリックします。

エラー メッセージ

エラーが発生した場合、以下のメッセージが表示されます。



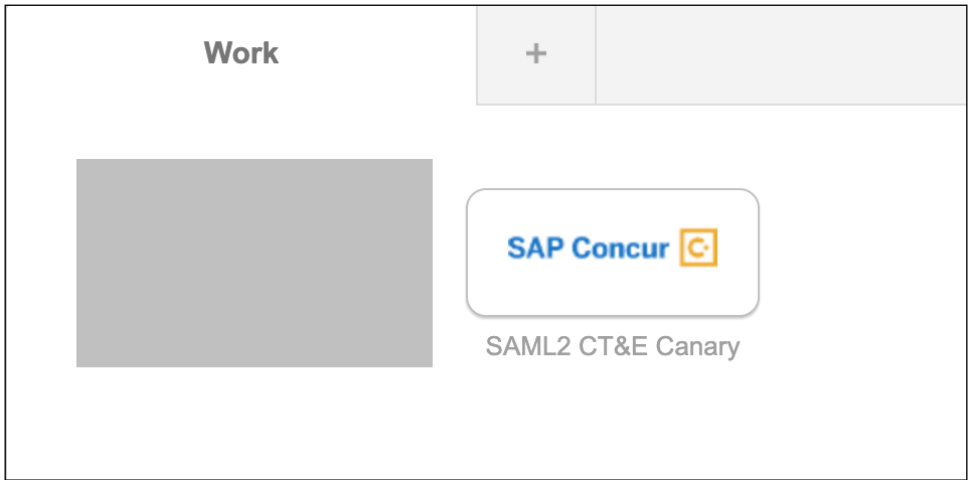
correlation_id を保存し、SAP Concur サポートに連絡して correlation_id を提供します。SAP Concur サポートは詳細エラー メッセージを調査して、エラー対応を行う手順を提供することができます。

ステップ 7: IdP-Initiated SSO をテストする

ご利用のアイデンティティ プロバイダから IdP-Initiated SSO URL を入手する必要があります。URL の場所は IdP によって異なります。以下に Okta と Azure AD で SSO のテストを実施する例を示します。ご利用の IdP も記載例と同様であると考えられます。

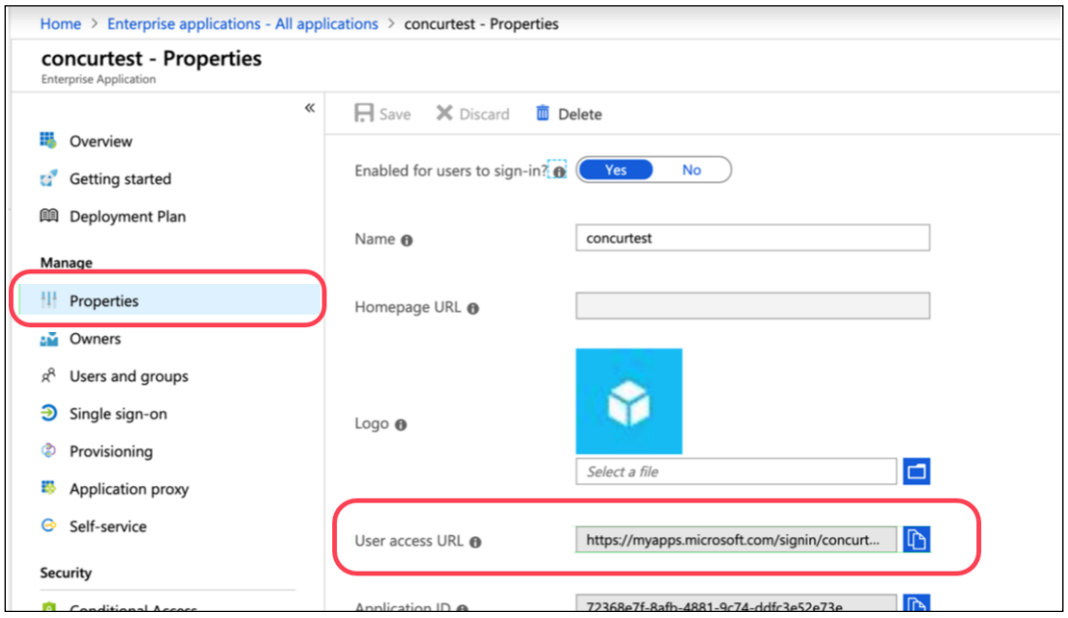
この IdP-Initiated SSO URL を入手すると、ブラウザに URL を貼り付けて、サインインを試すことができるようになります。

Okta の場合、Okta ポータルのアプリ アイコン（埋め込み URL）をクリックします。



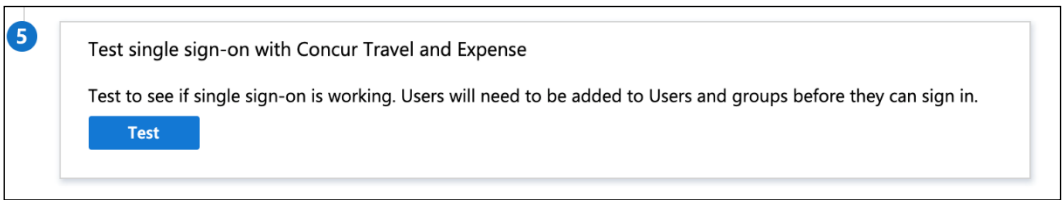
Azure AD の場合、次のいずれかを選択します。

- **[プロパティ] > [ユーザーのアクセス URL]**



- または -

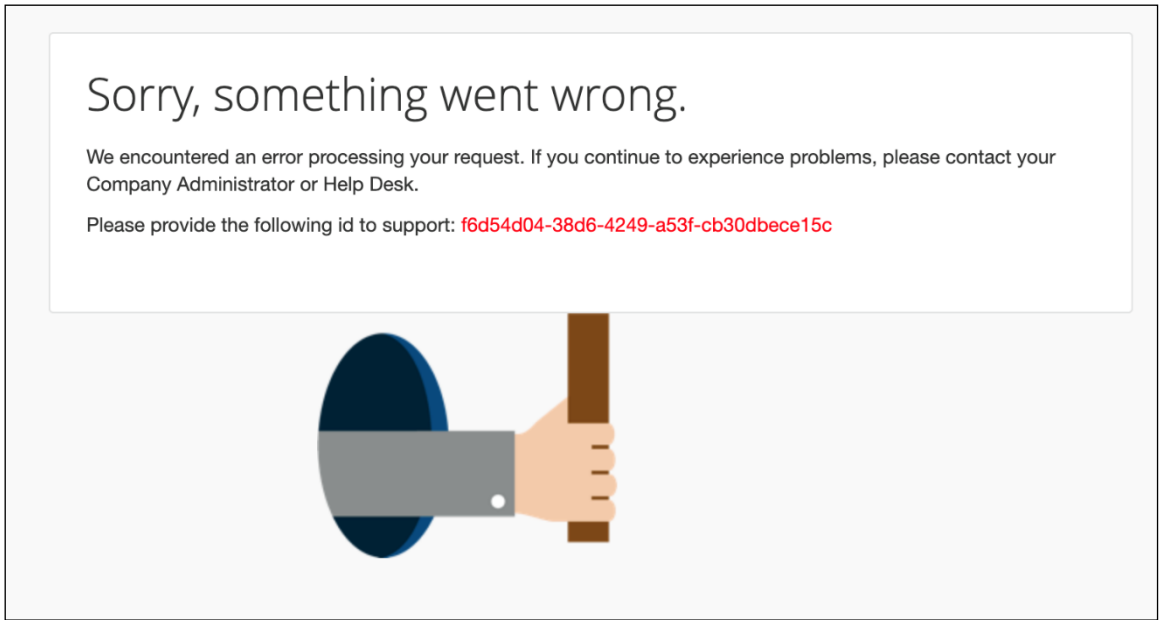
- **Concur Travel および Expense でシングル サインオンをテストする**



IdP-Initiated SSO URL の検索についてのご質問は、ご利用のアイデンティティ プロバイダにお問い合わせください。

エラー メッセージ

SSO テスト サインインが失敗する場合、次のようなメッセージが表示されます。



最も一般的な原因は以下の 2 つです。

- ユーザーが SAP Concur ソリューションに存在しない。
- ご利用の IdP と SAP Concur のユーザー プロファイルで Login_ID が一致しない。

原因を特定するには、以下の手順に従います。

1. SAMLtracer または Chrome ブラウザの検証機能を使用して、SAMLResponse を探します。（IdP は、SAMLResponse を介してユーザー情報を SAP Concur ソリューションに送信します。）

2. base64decode ツールで SAMLResponse をデコードします。base64decode ツールはインターネットですぐに入手できます。

3. <saml2:NameID> フィールドの値を探します。以下が例です。
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">username@domain.com</saml2:NameID>

4. <saml2:NameID> フィールドで見つけた値（前述の例では、username@domain.com）とユーザーの SAP Concur Login_ID を比較します。
   - 一致するものが見つからない場合、まず対応する SAP Concur Login_ID でユーザーを作成してから、再びテストを実施しなくてはなりません。
   - ユーザーが見つかり、当該ユーザーの SAP Concur Login_ID がご利用の IdP のユーザーの Login_ID と一致する場合、SAP Concur サポートに連絡し、エラーメッセージに表示されたエラー ID を提供します。

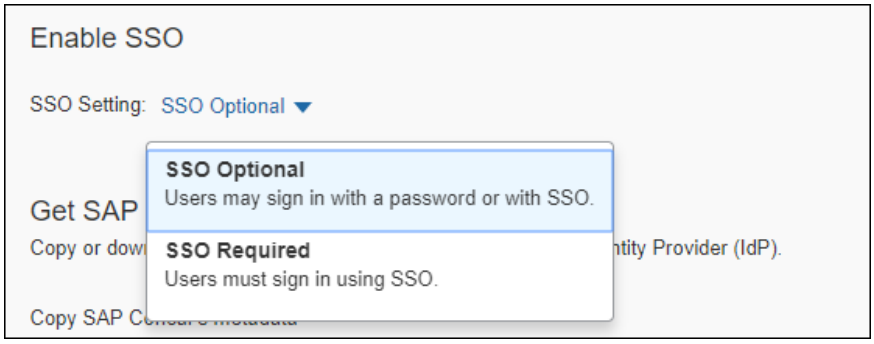
ステップ *8: SP-Initiated SSO* をテストする

テストを実施するには、次の手順に従います。

1. www.concursolutions.com に移動します。
2. SAP Concur ユーザー名を入力します。
3. **[[カスタム IdP 名] でサインイン]** をクリックします。ご利用の IdP にリダイレクトされます。IdP に対して認証を行うと、SAP Concur ホーム ページが表示されます。

ステップ *9:* 任意または必須として *SSO* を有効化する

[SSO の有効化] セクションには、SSO 設定を **[SSO 任意]**（既定値）から **[SSO 必須]** に変更するオプションがあります。



! **重要**このアカウントが TMC によって管理されている場合、SSO 設定を **[SSO 任意]** から **[SSO 必須]** に変更する前に TMC に通知する必要があります。

SSO 設定を **[SSO 必須]** に変更すると、すべてのユーザーが SSO を使用する IdP を介して concursolutions.com にサインインする必要があります。ユーザー（TMC、管理者、Web サービス、テスト ユーザ

– アカウントを含む）のユーザー名とパスワードによる concursolutions.com へのサインインはブロックされます。これは、ユーザーのサービスに混乱をもたらす可能性があります。

ベスト プラクティスは、すべてのユーザーが SSO を使用してサインインを行う方法を理解するまでは **[SSO 任意]** 設定を使用することです。設定を **[SSO 必須]** に変更する前に、60 日前、または組織で標準となっている通知期間でユーザーに通知することをお勧めします。

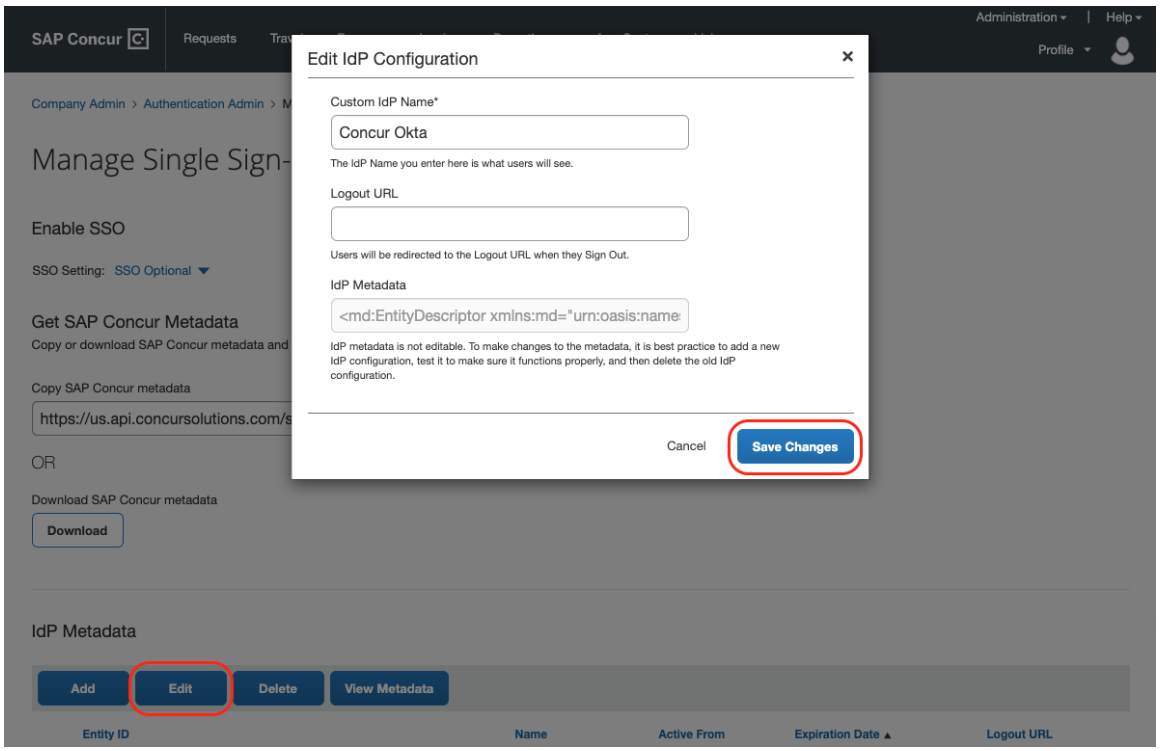
この変更に関するご質問は、SAP Concur サポートにお問い合わせください。

! **重要: SSO 設定を [SSO 必須] に変更すると、Web サインインとモバイル サインインの両方に影響します。** SAP Concur モバイル アプリのバージョン 9.86（11 月）から、SSO 設定を [SSO 必須] に変更する場合、Web とモバイル プラットフォームの両方で SSO を使用するサインインがユーザーに義務付けられるようになります。

SSO 設定の編集

上記のステップを使用して SSO 設定が作成されると、[カスタム IdP 名] および [ログアウト URL] の値を変更するために設定が編集される場合があります。 IdP メタデータは編集することができないため、その代わりのベスト プラクティスとしては、新しい設定を作成し、テストを行った上で元の設定を削除することです。

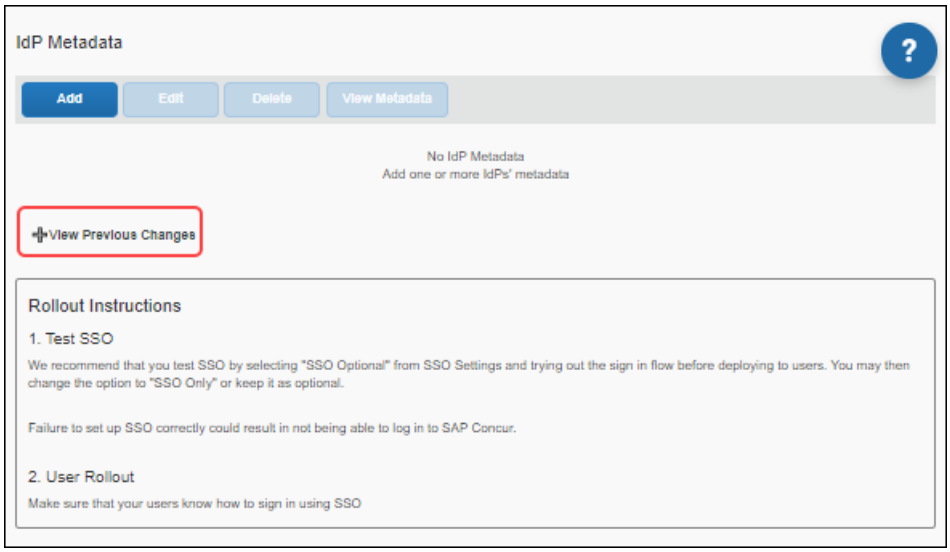
設定を編集するには、編集する設定を選択して [編集] をクリックします。



必要な変更を行ったら、**[保存]** をクリックします。

以前の変更を表示

現時点までに行われた SSO 構成への変更を表示するには、[以前の変更を表示] ボタンをクリックします。



テーブルに以前の変更が一覧表示されます。変更の一覧は、日付と時刻の降順で並べ替えられます。

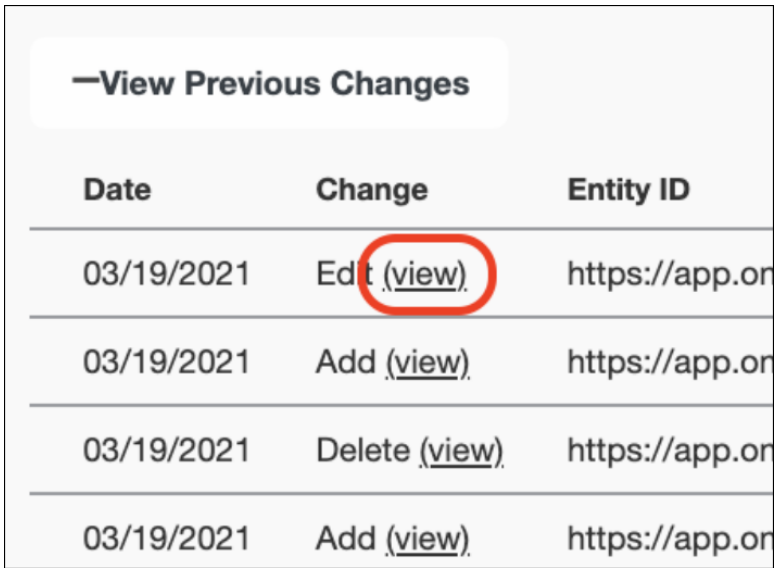
View Previous Changes

Date	Change	Entity ID	Name	Logout URL
03/19/2021	Edit (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concursolutions.com
03/19/2021	Add (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/19/2021	Delete (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/19/2021	Add (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/19/2021	Delete (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/18/2021	Add (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/18/2021	Delete (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/18/2021	Add (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/18/2021	Delete (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/17/2021	Edit (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test	https://concur.com
03/17/2021	Add (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test 123	https://concur.com
03/17/2021	Delete (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test 123	https://concur.com
03/17/2021	Add (view)	https://app.onelogin.com/saml/metadata/7dea77fe-7d24-4b2b-9fd1-958a56916380	concur test 123	https://concur.com

テーブルには、過去に行われた 100 件の変更が表示されます。テーブルにリストされる変更内容としては、以下のようなものが含まれます。

- 設定の追加
- 設定の削除
- **[カスタム IdP 名]** フィールドでの名前の編集
- **[ログアウト URL]** フィールドでの URL の編集

テーブルに一覧表示されている特定の変更に関する詳細情報を表示するには、目的のリスト項目の **[表示]** リンクをクリックします。



[表示] リンクをクリックすると、リスト項目の **[以前の変更を表示]** ページが表示されます。行った変更の種類により、ページに表示される詳細が異なります。

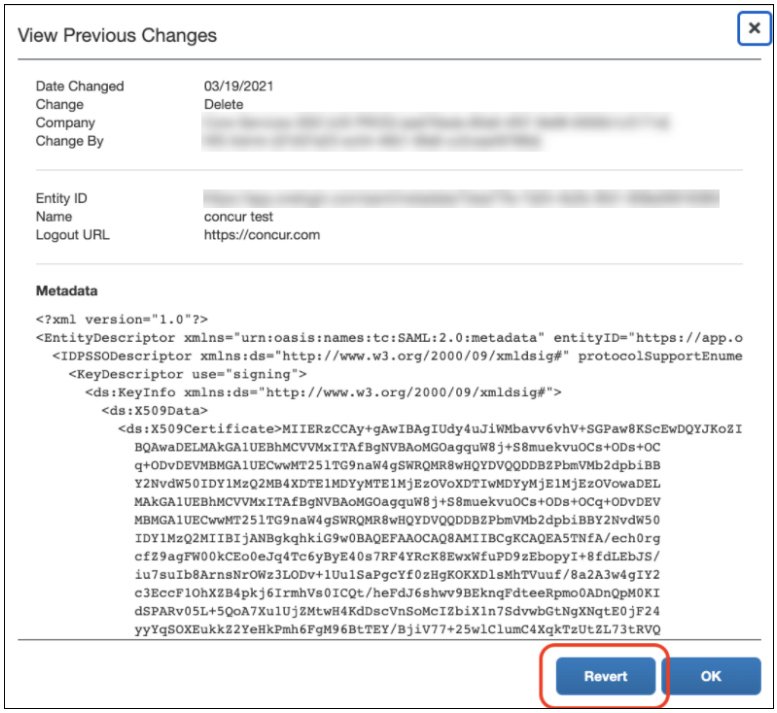
設定削除時の詳細

設定を削除した際に **[変更履歴の表示]** ページに表示される詳細としては以下のようなものが含まれます。

- 変更日
- 変更のタイプ（削除）
- 変更を行った会社
- 変更を行ったユーザーの名前および UUID
- エンティティ ID
- フレンドリ名
- ログアウト URL
- Metadata

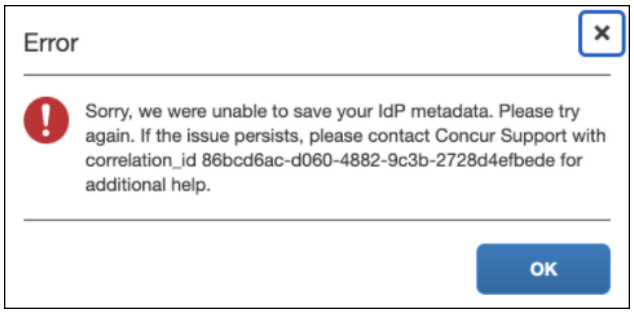
設定が削除されている場合、この設定を復元するための **[元に戻す]** ボタンが **[変更履歴の表示]**ページに表示されます。設定が復元されると、この設定をサインイン プロセス中にユーザーが使用できるようになります。

削除された設定の［変更履歴の表示］ページの表示例



［元に戻す］ボタンをクリックすると、設定を元に戻すためのアクションを確認するように求められます。設定の復元を確認するには **［メタデータを元に戻す］**をクリックします。設定の復元をキャンセルするには、**［元に戻すことを確認］**ページで **［元に戻さない］**をクリックします。

削除した設定を復元することを選択したが、設定を復元できない場合は、[メタデータを元に戻す]ボタンをクリックすると、次のようなメッセージが表示されます。

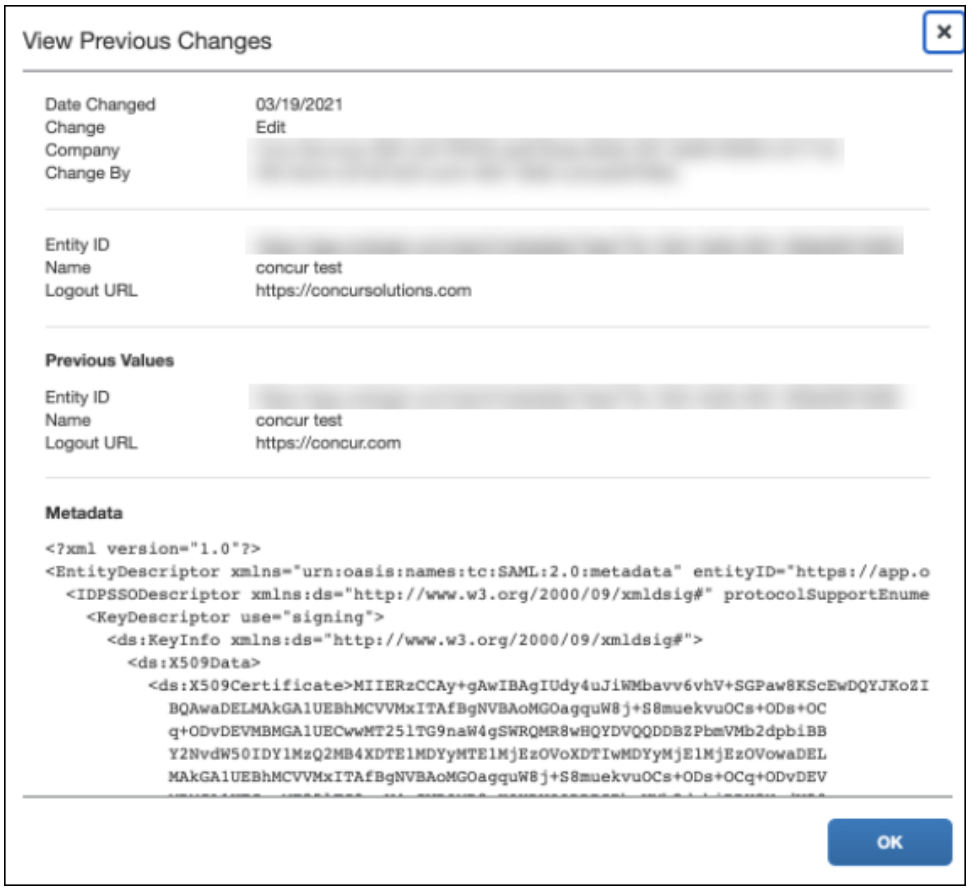


設定編集時の詳細

設定を編集した際に **[変更履歴の表示]** ページに表示される詳細としては以下のようなものが含まれます。

- 変更日
- 変更のタイプ（編集）
- 変更を行った会社
- 変更を行ったユーザーの名前および UUID
- 現在のエンティティ ID
- 現在のフレンドリ名
- 現在のログアウト URL
- 以前のエンティティ ID
- 以前のフレンドリ名
- 以前のログアウト URL
- Metadata

編集された設定の [変更履歴の表示] ページの表示例



設定追加時の詳細

設定を追加した際に [変更履歴の表示] ページに表示される詳細としては以下のようなものが含まれます。

- 変更日
- 変更のタイプ（追加）
- 変更を行った会社
- 変更を行ったユーザーの名前および UUID
- エンティティ ID
- フレンドリ名
- ログアウト URL
- Metadata

暗号化を使用する SSO アプリ/コネクタの設定（オプション）

テストを含め、「暗号化を使用しない SSO アプリ/コネクタの設定」セクションに記載されたステップをすべて行います。それから、ご利用の IdP が暗号化された SAMLResponse 機能に対応しているかどうかを確認します。対応している場合、以下のステップに従って暗号化を設定します。

ステップ *1:* 暗号化キーを入手して保存する

SAP Concur ソリューションから暗号化キーを入手して、encryption.crt ファイルに保存します。

暗号化キーを入手し、保存するには*:*

1. エンティティがホストされている地域（データ センター）に該当する URL をクリックして、SAP Concur SP メタデータを確認します（Chrome ブラウザ推奨）。
   - **アメリカ（北米）:** https://www-us.api.concursolutions.com/sso/saml2/V1/sp/metadata/
   - **EMEA:** https://www-emea.api.concursolutions.com/sso/saml2/V1/sp/metadata/
   - **中国:** https://www-cn.api.concurcdc.cn/sso/saml2/V1/sp/metadata
2. 以下の例に示されているように、暗号化キーを見つけます。

3. 暗号化証明書をプレーン テキスト ファイルにコピーします。

NOTE: Word などのリッチ テキスト エディタは使用しないでください。

---

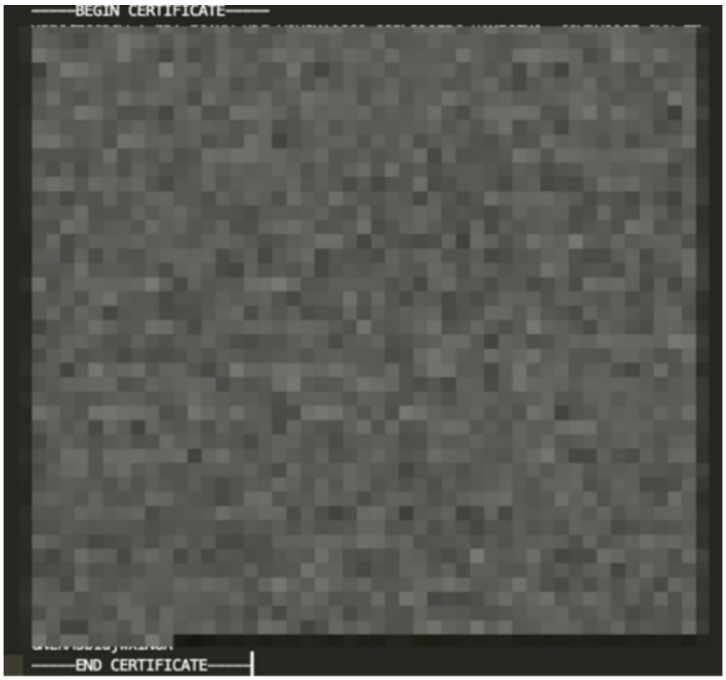
4. 次に示すように、BEGIN/END CERTIFICATE の 2 つの行の間に貼り付けます。

   -----BEGIN CERTIFICATE-----

   <コピーした証明書はここに貼り付ける>

   -----END CERTIFICATE-----

5. encryption.crt として保存します。

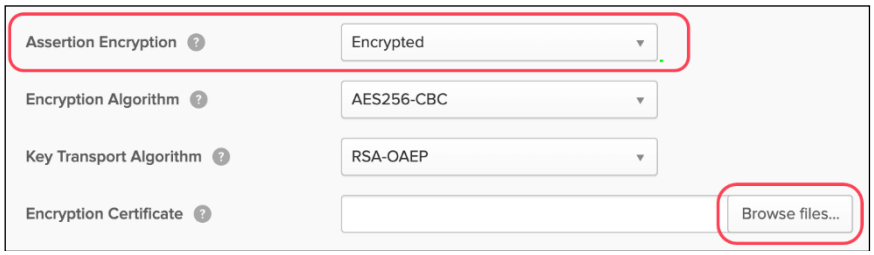


ステップ 2: IdP に encryption.crt をアップロードする

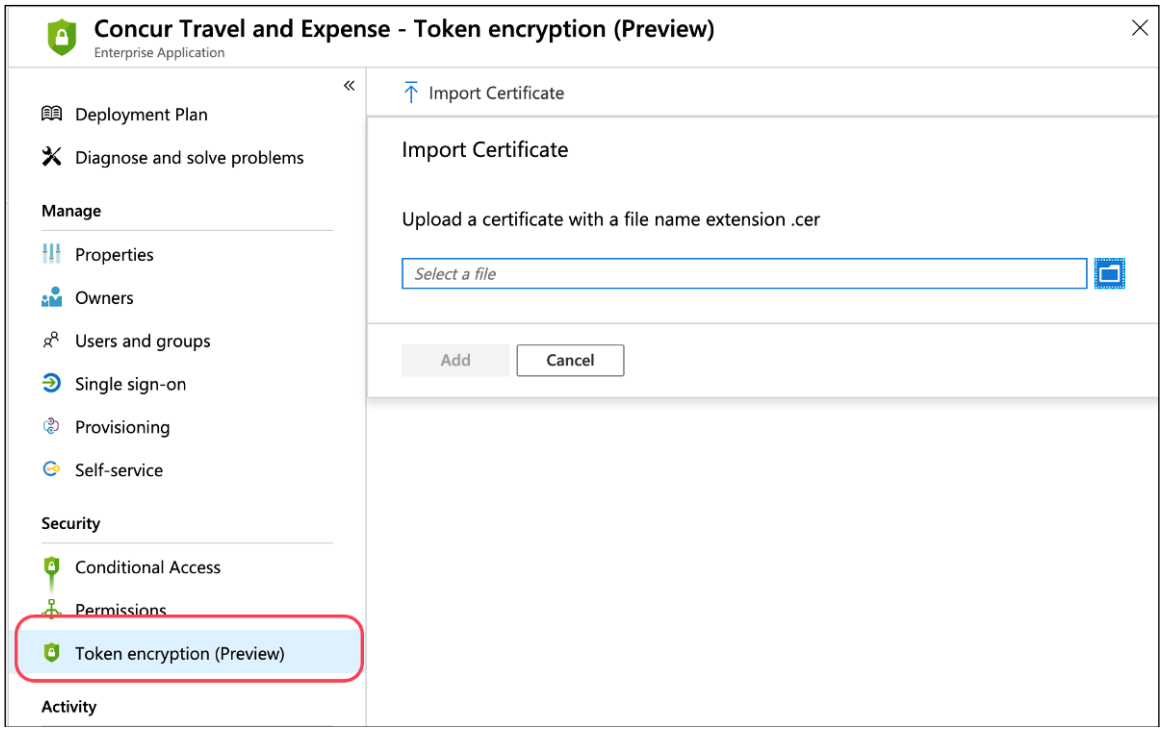
ご利用の IdP への encryption.crt のアップロードについてのご質問は、IdP にお問い合わせください。

例

Okta の場合、**[Assertion Encryption]** フィールドを **[Encrypted]** に設定してから、暗号化証明書をアップロードします。



Azure AD の場合、**[トークン暗号化（プレビュー）]** オプションを使用して、暗号化証明書をアップロードします。



セクション 6: よくある質問

Q. SAP Concur はどの IdP をサポートしていますか？

A. SAP Concur には、SAML 2.0 標準をサポートしているすべてのアイデンティティ プロバイダと互換性があります。

Q. SSO の強制はどのように機能しますか？

A. 現在、SAP Concur では、会社レベルでの SSO の強制にサポートしています。SAP Concur では、ユーザー ロールまたはユーザー グループに基づいた SSO の実施はサポートしていません。

SSO の設定する場合には、**[SSO 任意]** と **[SSO 必須]** という 2 つのオプションがあります。

[SSO 任意] は既定値です。このオプションを選択することは、会社の全員が標準のユーザー名とパスワード、**または** SSO 資格情報を使用して SAP Concur サービスにログインすることができるということを意味します。

SSO サインインのテストの終了後、SSO 設定を **[SSO 必須]** に変更できます。

! **重要** SSO 設定を [SSO 必須] に変更すると、サービスに混乱を引き起こす可能性があります。

SSO 設定を **[SSO 必須]** に変更した場合、すべてのユーザーが SSO を使用して IdP から concursolutions.com にサインインする必要があります。また、すべてのユーザー（TMC、管理者、Web サービス、およびテスト ユーザー アカウントを含む）は、ユーザー自身のユーザー名とパスワードを使用して concursolutions.com にサインインできなくなります。

! **重要**このアカウントが TMC によって管理されている場合、SSO 設定を **[SSO 必須]** に変更する前に TMC に通知する必要があります。

Q. SAP Concur では複数の IdP を設定できますか。

A. はい。SSO セルフサービス ツールにより、無制限に IdP を追加することができます。

Q. メタデータをアップロードしてから SSO サインインのテストをするまでどのくらい待つ必要がありますか。

A. ご利用の IdP の メタデータが SAP Concur に適切に保存されるとすぐに SSO サインインが機能します。

Q. 新しいセルフサービス プラットフォームに SSO を設定する場合、以前のプラットフォームの現行の SSO 設定に影響しますか。

新しいセルフサービス プラットフォームに SSO を設定しても、以前のプラットフォームの現行の SSO 設定に影響を与えることはありません。従来の Concur SSO スタックから独立しているため、既存の SSO 設定と並行して安全に使用することができます。既存の SSO をお使いのお客様は、SSO サービスの設定、テスト、および導入が完了したら、従来の SSO 設定の削除を依頼し、管理するツールを 1 つに絞ることができます。

Q. [シングル サインオンの管理] ページで現行の SSO 設定を表示できないのはなぜですか。

A: 現行の SSO 設定は以前の SSO サービスの一部であり、SAP Concur 従業員のみがその設定データにアクセスすることができるためです。

Q. [シングル サインオンの管理] ページからモバイル SSO を設定できますか。

A. はい。SAP Concur モバイル アプリのバージョン 9.86 から、本ドキュメントに記載されたプロセスを使用して SSO を設定すると、Web とモバイルの両方に対して SSO サインイン が有効化されるようになります。SSO 設定を **[SSO 任意]** から **[SSO 必須]** に変更する場合、ユーザーは Web とモバイル プラットフォームの両方で SSO を使用してサインインしなくてはなりません。

Q. SAP Concur は SAML SSO を介する「ジャストインタイム ユーザー プロビジョニング」をサポートしていますか。

A: 今後のアップデートの対象になっています。

Q. SAP Concur は「ホーム領域検出」をサポートしていますか。

A. はい。ホーム領域検出サービスは SP-Initiated SSO フローの背後にある API です。

セクション 7: 付録: ADFS の設定

NOTE: このセクションの説明はサード パーティー プロバイダにより提供されており、 SAP Concur はその正確性を保証することはできません。問題が発生した場合は、サード パーティー プロバイダのサポートにご連絡ください。

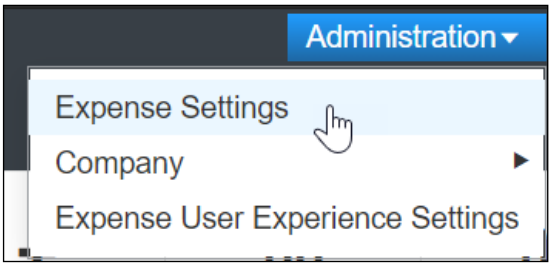
はじめに

設定を始める前に以下のことをご確認ください。

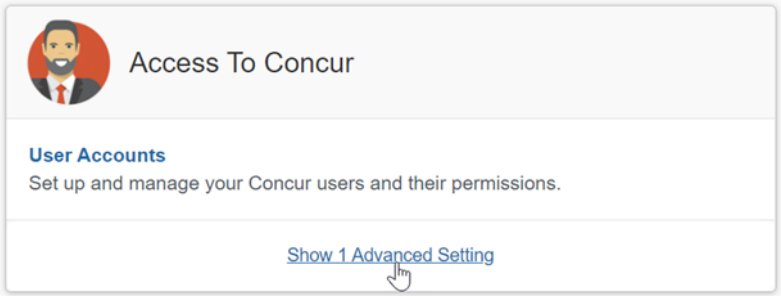
- ユーザーは ADFS および SAP Concur 両方に存在していること。現在 SAP Concur では自動ユーザー割当てがサポートされていないため、個別にユーザーを追加する必要があります。
- Azure AD から送信する属性が SAP Concur の各従業員の **[ログイン ID]**（**ユーザー名** / **CTE ログイン名**）フィールドと一致する。
- SAP Concur アカウントに割り当てられた組織管理者（Travel のアクセス許可）を取得している。アクセス許可を取得したら、お使いの SAP Concur のエディションに応じて、次のいずれかのパスを使用して **[SSO の管理]** ページにアクセスできるようになります。

SAP Concur **Standard** エディション：

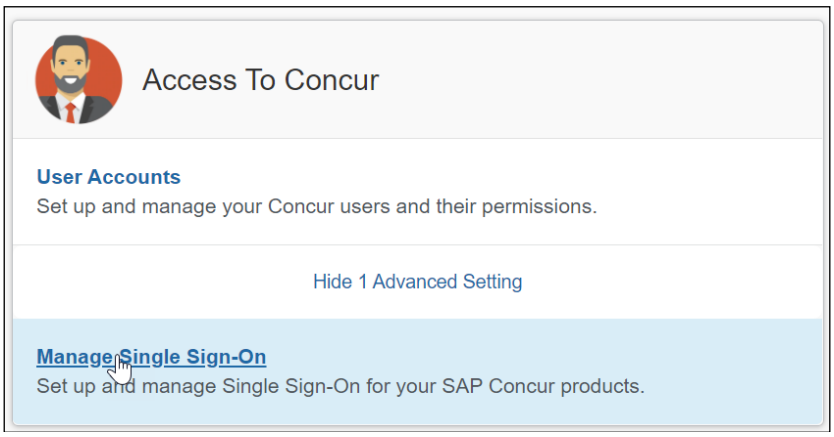
1. **[管理] > [経費の設定]** に移動します。



2. [Concur にアクセス] セクションで、**[1 つの詳細設定を表示]** をクリックします。

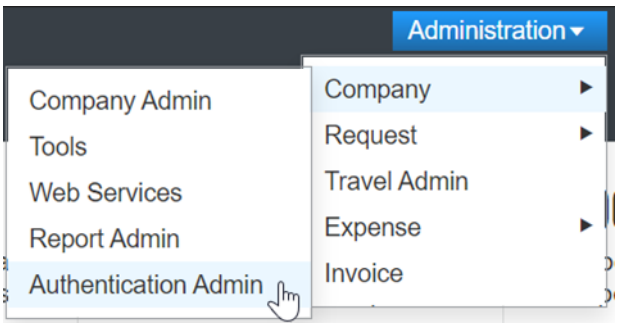


3. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。

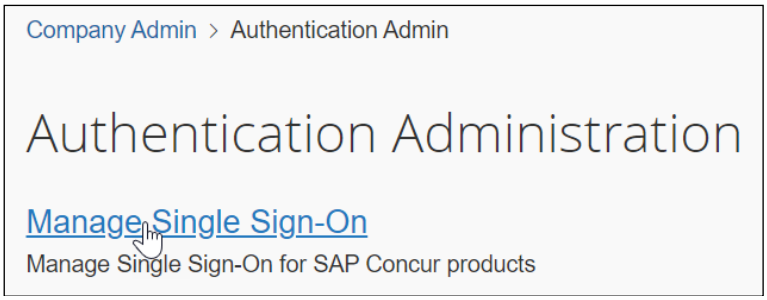


SAP Concur **Professional** エディション：

1. **[管理] > [会社] > [認証管理]** へ移動します。



2. **[シングル サインオンの管理]** をクリックして、[SSO の管理] ページにアクセスします。



または、以下のいずれかの URL を使用して、ページにアクセスすることができます。

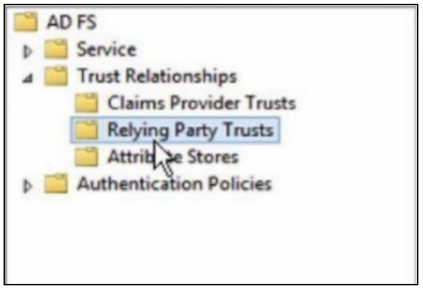
- US DC Prod: https://www.concursolutions.com/nui/authadmin/ssoadmin
- US DC Test: https://implementation.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Prod: https://eu1.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Test: https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin
- CN DC Prod: https://www.concurcdc.cn/nui/authadmin/ssoadmin

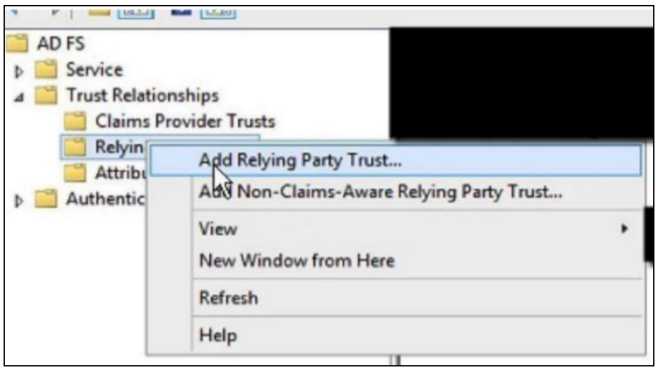
---

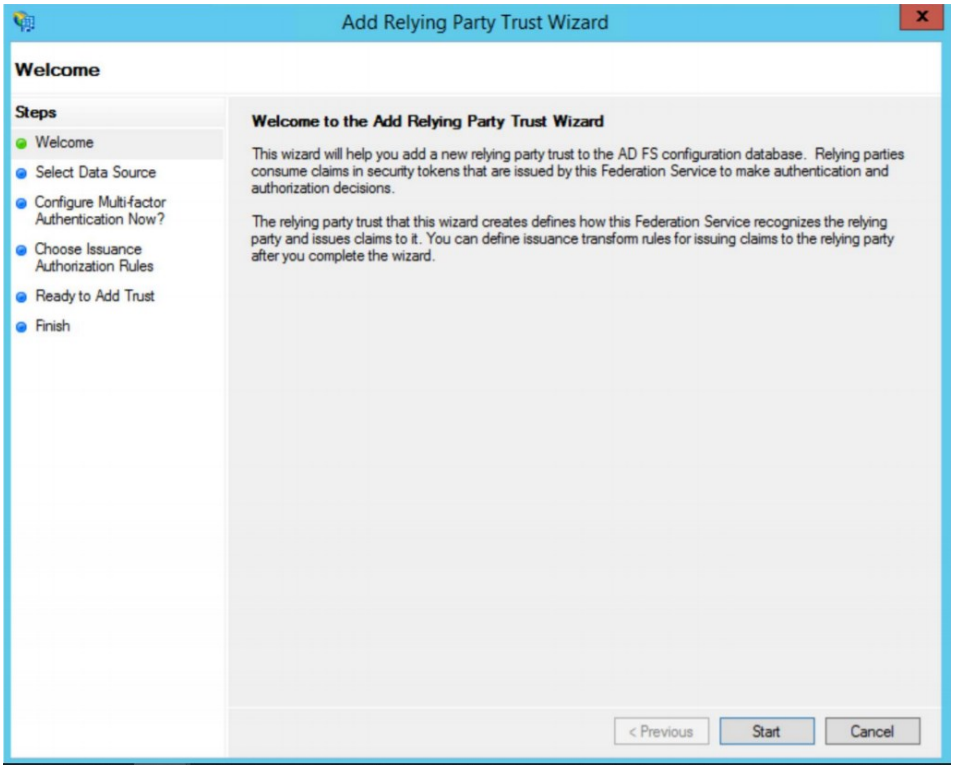
NOTE: アクセス許可を取得しておらず、自分のプロファイルに割り当てることもできない場合、会社のサポート問合せ権限の保持者に依頼し、SAP Concur サポートまでお問い合わせください。

ADFS の設定

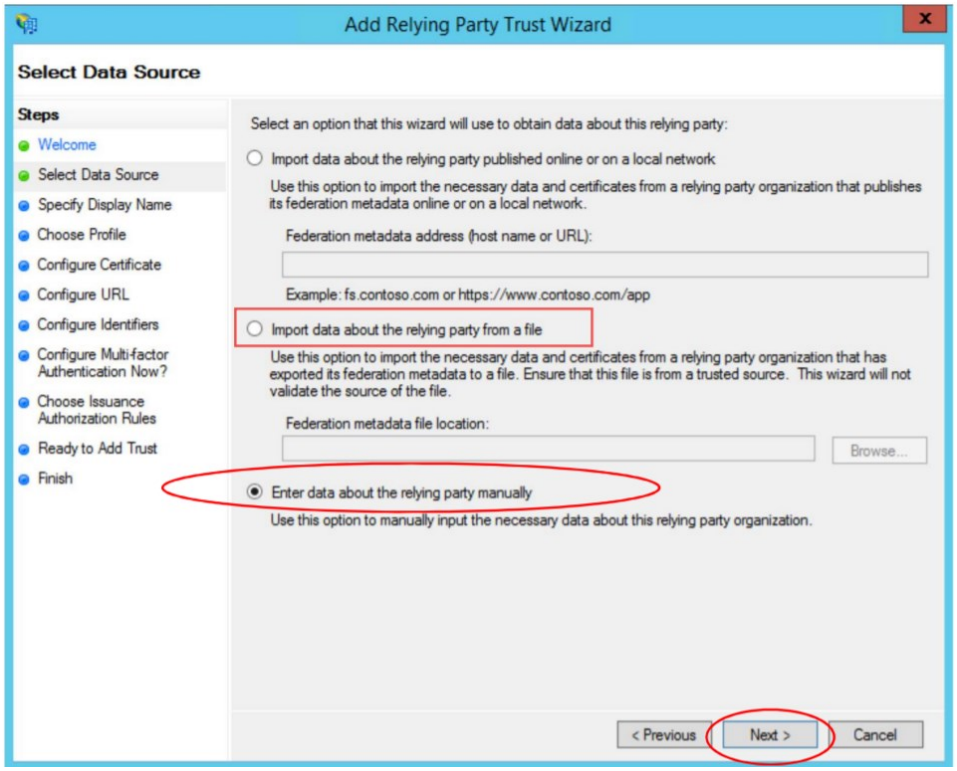
1. **[証明書利用者信頼]** ウィザードを起動します。



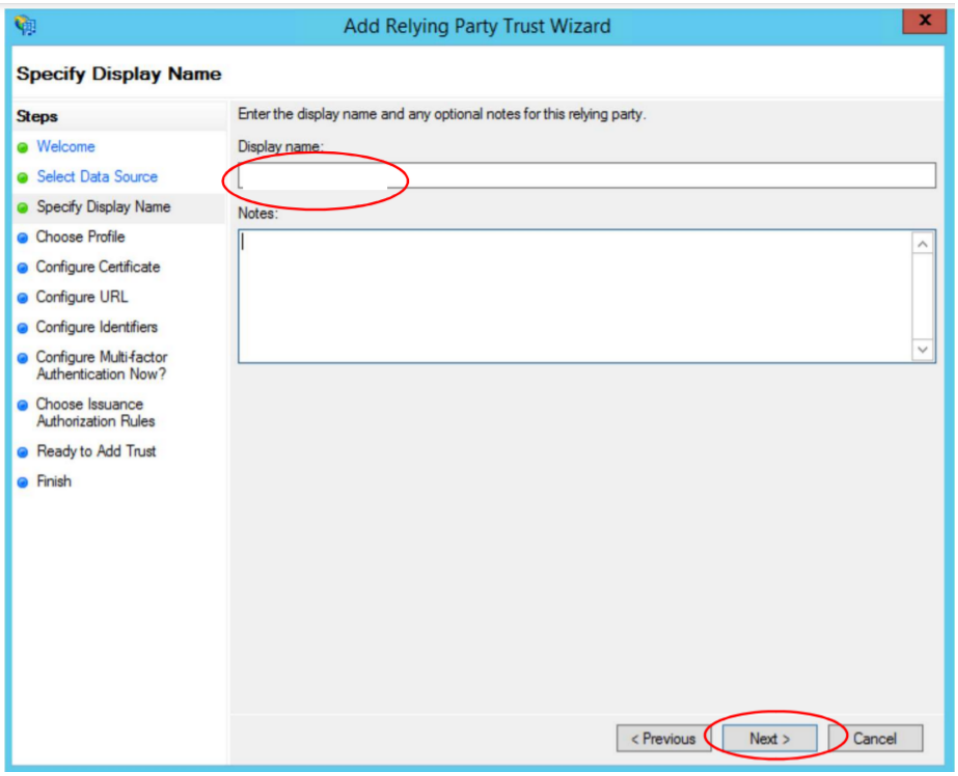




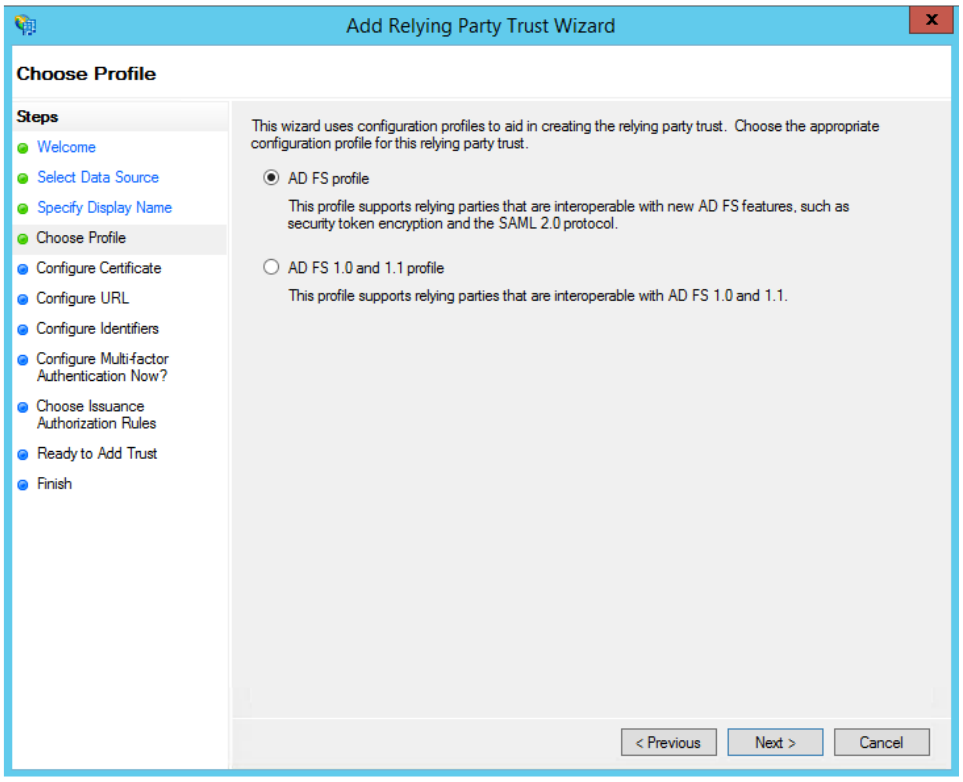
2. **[データ ソースの選択]** ステップでは、**[証明書利用者についてのデータを手動で入力する]** を選択してから、**[次へ]** をクリックします



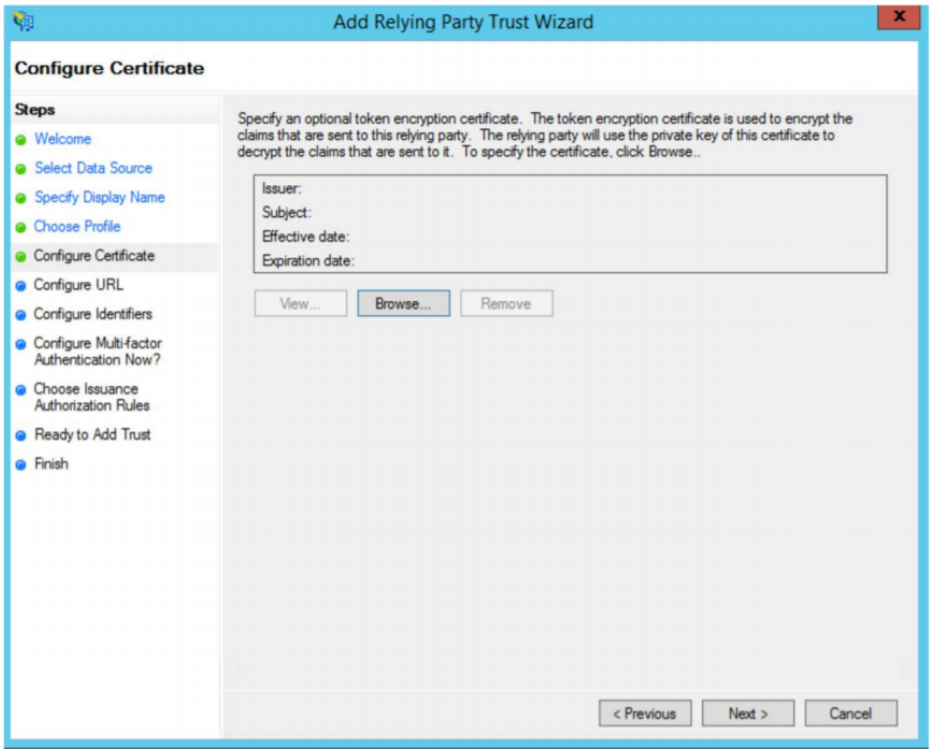
3. **[表示名の指定]** ステップでは、**[表示名]** フィールドに「SAP Concur」と入力してから、**[次へ]** をクリックします。



4. **[プロファイルの選択]** ステップでは、**[AD FS プロファイル]** を選択してから、**[次へ]**をクリックします。

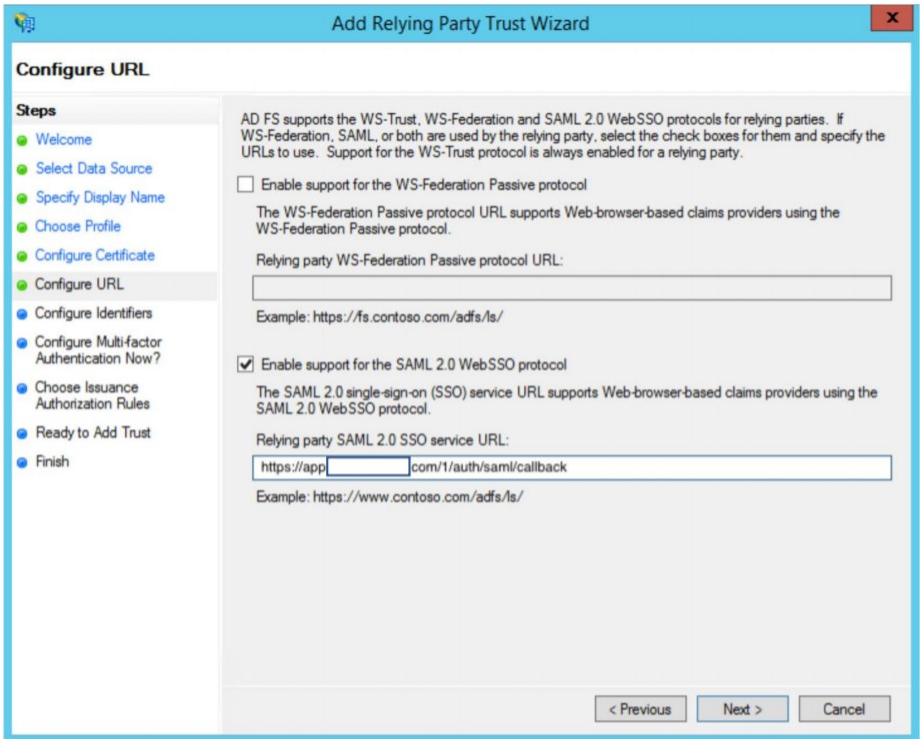


5. **[証明書の構成]** ダイアログでは、SAP Concur 暗号化証明書を手動でアップロードします。はじめに で説明されているように SAP Concur の **SSO の管理** より取得することができます。SAP Concur メタデータに移動し、暗号化証明書を抽出してお使いの PC に保存します。暗号化証明書をアップロードし、[次へ] をクリックします。



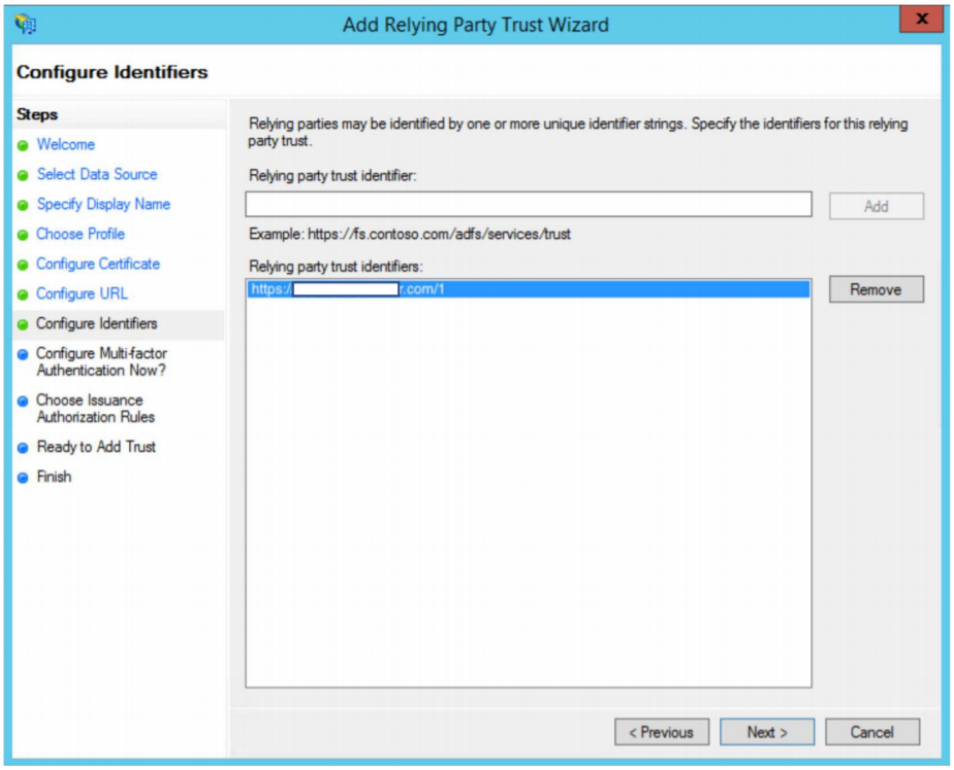
6. **[URL の構成]** ステップでは、**[SAML 2.0 WebSSO プロトコルのサポートを有効にする]** チェックボックスを選択し、 該当する SAML 2.0 SSO サービス URL を入力します。

   - アメリカ (北米): https://www-us.api.concursolutions.com/sso/saml2/V1/acs/
   - EMEA: https://www-emea.api.concursolutions.com/sso/saml2/V1/acs/
   - 中国: https://www-cn.api.concursolutions.com/sso/saml2/V1/acs/

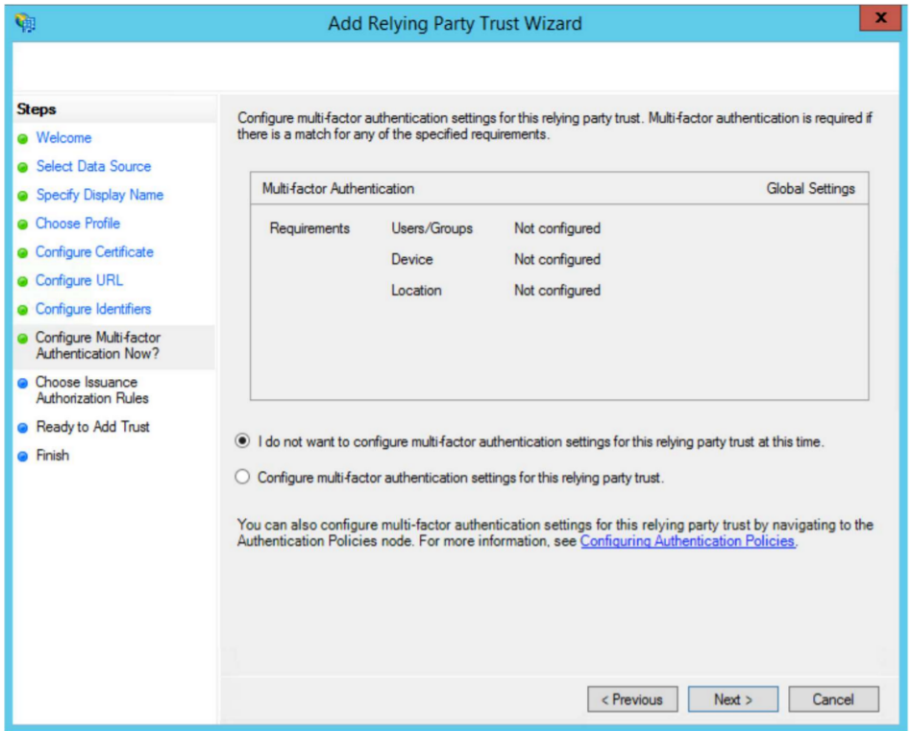


7. **[識別子の構成]** ダイアログで、**証明書利用者信頼の識別子**を追加します。

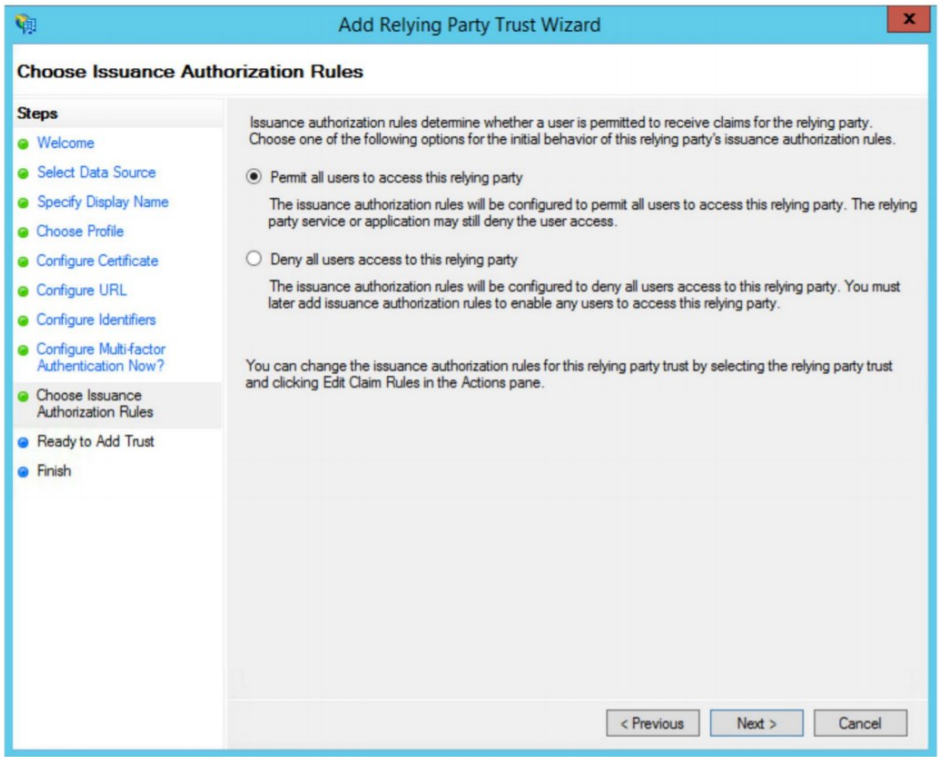
   - アメリカ (北米): https://us.api.concursolutions.com/saml2
   - EMEA: https://emea.api.concursolutions.com/saml2
   - 中国: https://cn.api.concursolutions.com/saml2



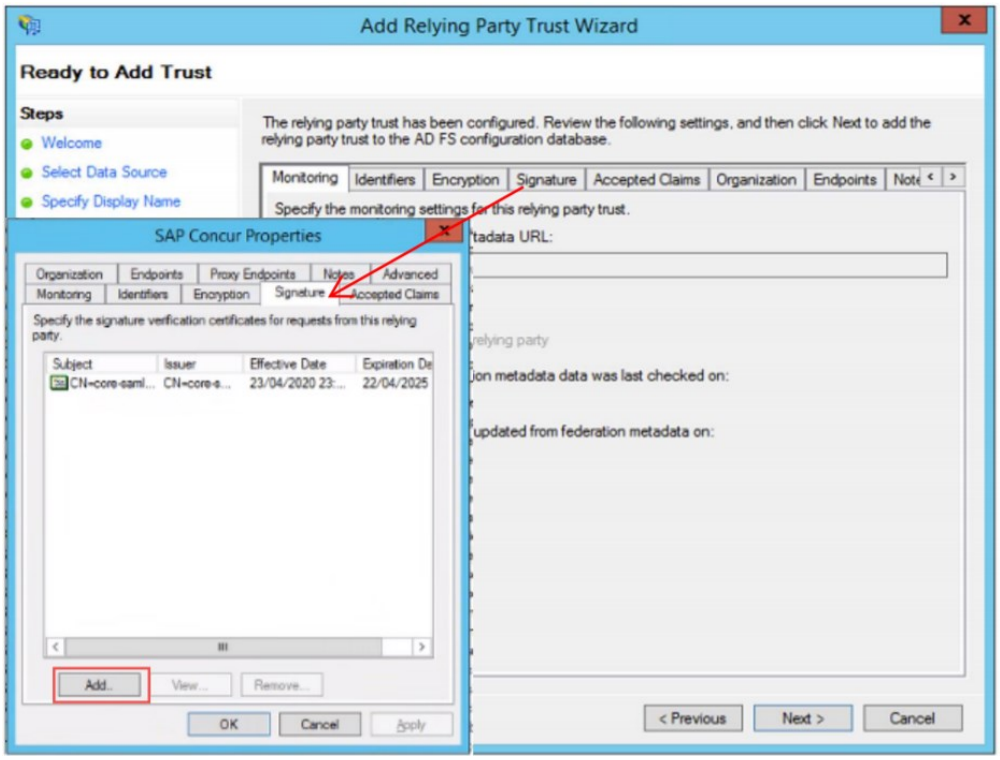
8. **[この証明書利用者信頼に対して多要素認証設定を構成しません]** を選択してから、**[次へ]** をクリックします。



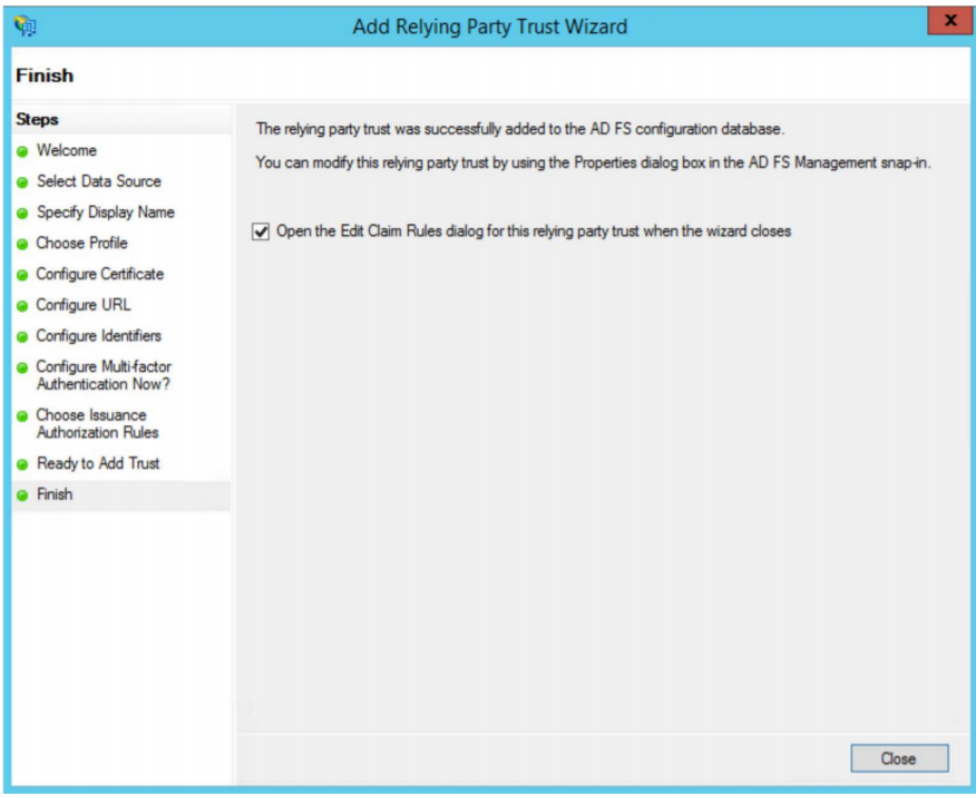
9. **[発行承認規則の選択]** ダイアログでは、**[この証明書利用者へのアクセスをすべてのユーザーに許可する]** を選択してから、**[次へ]** をクリックします。



10. 必要に応じて、新たに設定した証明書利用者信頼を見直します。まだメタデータを更新していない場合、**[信頼の追加の準備完了]** ダイアログで **[署名]** タブをクリックし、SAP Concur メタデータを追加してから **[次へ]** をクリックします。

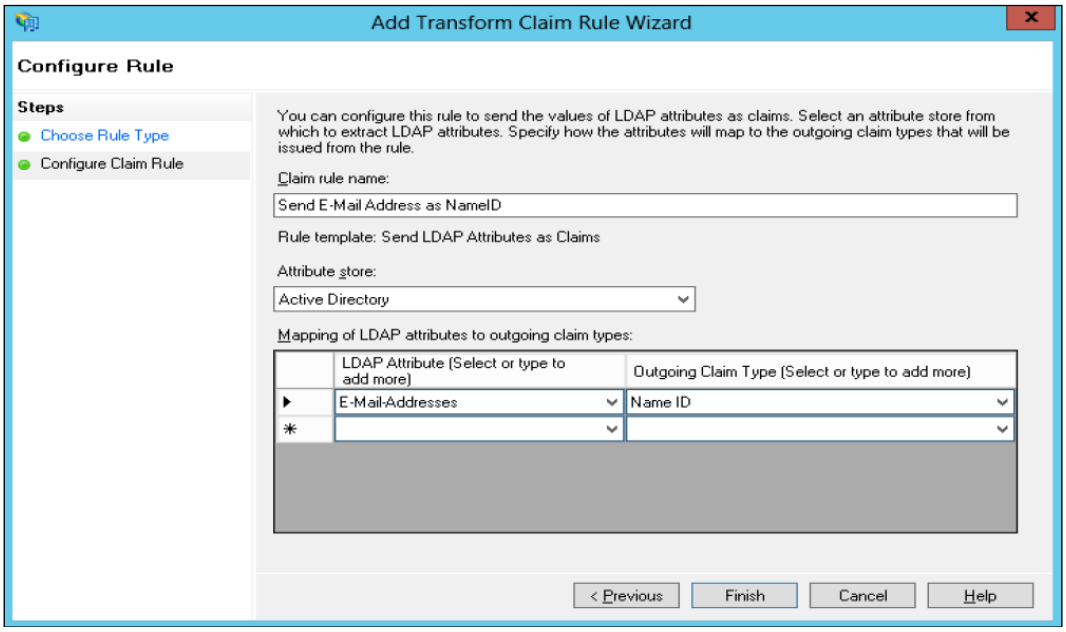


11. **[完了]** ダイアログで、**[ウィザードの終了時にこの証明書利用者信頼の要求規則の編集を開く]** オプションを選択し、**[閉じる]** をクリックします。



[変換要求規則追加] ウィザードが自動的に表示されます。

この **[構成ルール]** ダイアログのサンプルは、具体的な要求規則の設定内容を示しています。



12. 以下の 2 つの規則を作成します。

ルール 1:

1) 要求規則テンプレートを「LDAP 属性を要求として送信」として設定します。

2) **[次へ]** をクリックします。

3) 要求規則名を追加し、属性ストアを設定します。

4) LDAP 属性 = 電子メール アドレス

5) 出力方向の要求の種類 = 電子メール アドレス

6) **[終了]** をクリックします。

ルール 2:

1) 要求規則テンプレートを「入力方向の要求を変換」として設定します。

2) 要求規則名を追加します。

3) 入力方向の要求の種類 = 電子メール アドレス

4) 出力方向の要求の種類 = 名前 ID

5) 出力方向の名前 ID の形式 = 電子メール

6) 「すべての要求値をパス スルーする」が選択されていることを確認します。

7) **[終了]** をクリックします。

ユーザーが認証するときにアサーションで渡される名前 ID の値の場合、この値はユーザーの SAP Concur ログイン ID と一致する必要があります。SAP Concur をお使いのほとんどのお客様はログイン ID としてメール アドレスを使用していることから、既定では、これが要求規則を設定する方法になっています。

ただし、たとえば、employeeID@companydomain.com などの異なる形式を SAP Concur ログイン ID に使用している場合は、LDAP 属性が **employeeid** および **companydomain.com** を送信できるように、このルールをカスタマイズする必要があります。これは SP-Initiated ログインの要件であるため、作成されたその他のカスタム ロールは名前 ID の形式は必ず「メール アドレス」として送信されるようにする必要があります。

! **重要:** ベスト プラクティスは出力方向の要求の種類を名前 ID のままに保持することです。

SAP Concur サイトを設定する

設定を完了するには、次のいずれかを行います。

- ADFS メタデータ URL を入手する。
- ADFS メタデータ ファイルのコピーをローカル マシンに保存する。

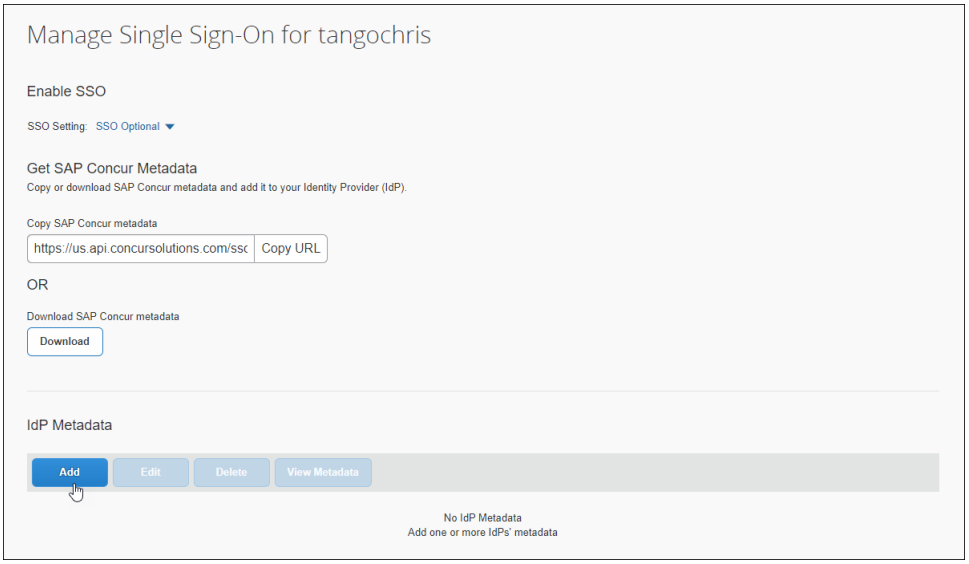
ADFS メタデータ URL または保存した ADFS メタデータ ファイルの入手後に、以下のステップを完了します。

SAP Concur に ADFS メタデータを入力するには:

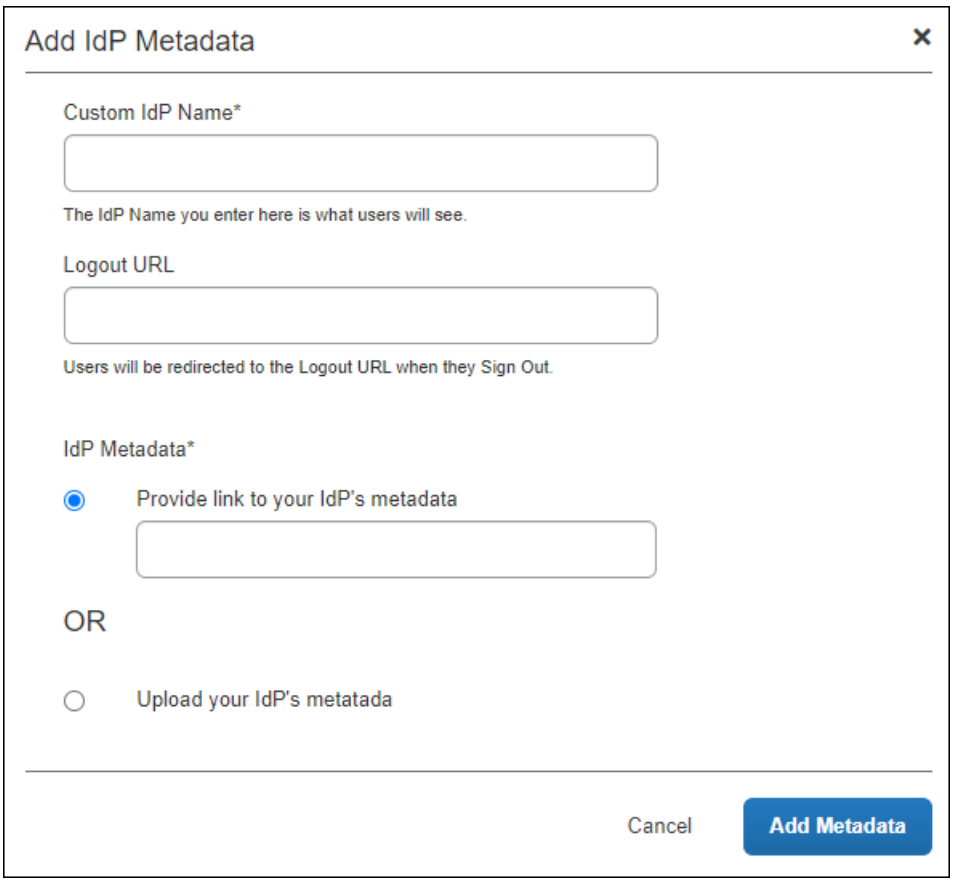
1. SAP Concur へのサインイン

1. **[シングル サインオンの管理]** ページにアクセスします。

2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。

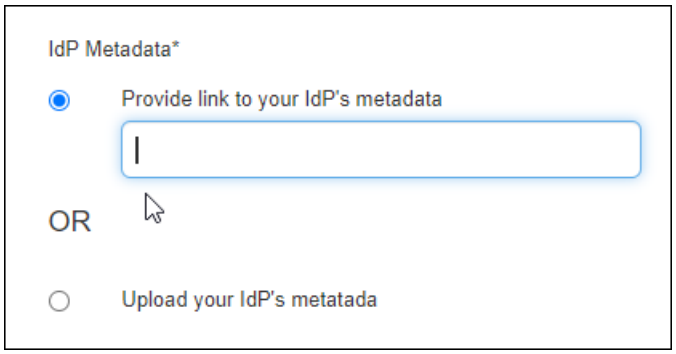


[IdP メタデータの追加] ページが表示されます。

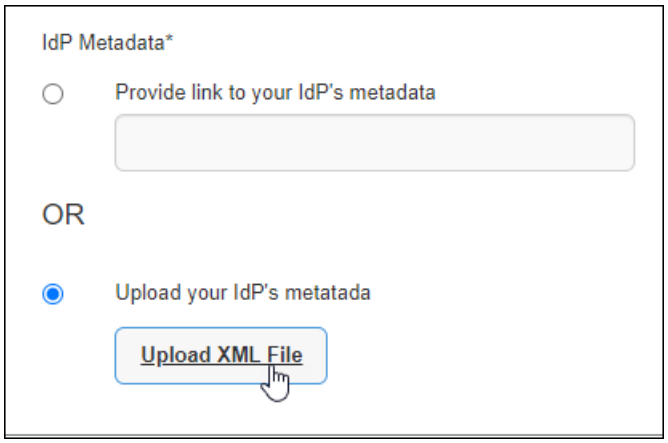


3. ADFS メタデータを入力するには、**[IdP メタデータ]** セクションで次のいずれかを行います。

   - ADFS メタデータ URL を **[IdP のメタデータへのリンクの設定]** フィールドに入力します。



- **または[IdP のメタデータのアップロード]** をクリックし、**[XML ファイルのアップロード]** をクリックし、ローカル マシンに保存した ADFS メタデータ ファイルを探して、**[開く]** をクリックします。



4. **[メタデータの追加]** をクリックします。

SSO ログインのテスト

IdP 主導型の SSO をテストする

IdP-Initiated SSO ログインをテストするために、このテストを行うユーザーやグループに ADFS の新しいアプリケーションを割り当てていることを確認します。次のような ADFS URL を使用します:

Https://[フェデレーション サービス識別子のドメイン]/adfs/ls/idpinitiatedsignon.aspx?loginToRp= [証明書利用者信頼の識別子]

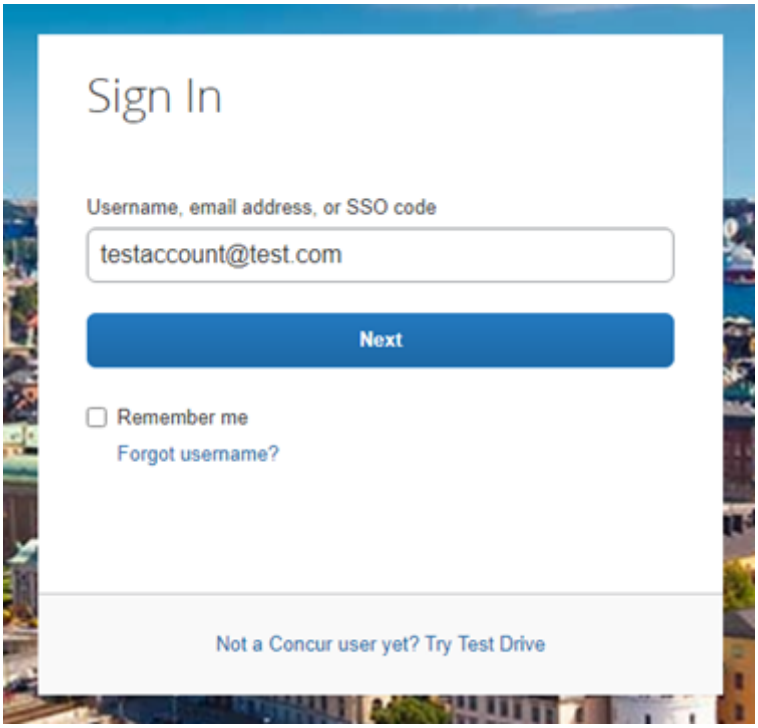
この URL が適切な場合、ADFS 資格情報の入力を促され、すでにログインしている SAP Concur ホーム ページにリダイレクトされます。

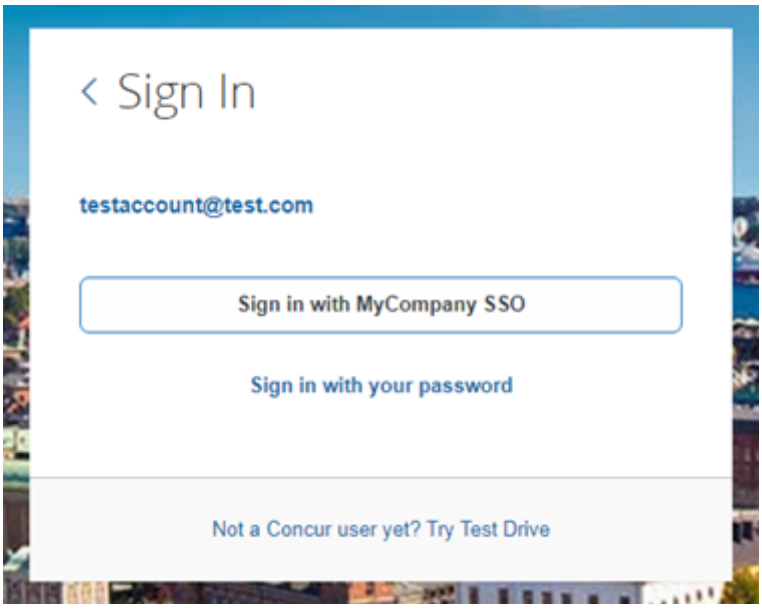
SP-Initiated SSO をテストする

SP-Initiated SSO をテストするには

1. テストを行いたい環境のログイン ページを開きます。
   - US DC Prod: https://www.concursolutions.com/
   - US DC Test: https://implementation.concursolutions.com/
   - EMEA DC Prod: https://eu1.concursolutions.com/
   - EMEA DC Test: https://eu1imp.concursolutions.com/
   - CN DC Prod: https://www.concurcdc.cn/

2. ログイン ページでユーザー名、照合済メール アドレス、または SSO コードを追加して続行できます。**[次へ]** をクリックすると、最近作成した SSO 設定のオプションが表示されます。クリックして、SAP Concur にリダイレクトするアイデンティティ プロバイダ アカウントの認証を続行します。





ADFS 資格情報を追加した後、ADFS でエラー メッセージが表示された場合、設定が完了していないことを示している可能性があります。エラー メッセージが SAP Concur 側のものである場合、資格情報が一致しない、証明書が無効である、または設定が指定されていない可能性があります。IdP-Initiated ログインが機能していても SP-Initiated ログインが機能していない場合、ADFS 側の名前 ID が適切なフォーマットで送信されていないことが原因で発生している可能性があります。これは「ADFS アプリケーションを設定する」セクションで説明しています。

問題が解決しない場合、表示されたエラー ID をコピーし、SAP Concur サポートにお問い合わせください。

Mobile シングル サインオン（SSO）

SAMLv2 プラットフォームで作成された SSO 設定の場合、モバイル SSO はメタデータが保存されるとすぐに自動的に有効にされます。ただし、このオプションが機能するには、SP-Initiated フローが機能している必要があります。これは、前述の「SSO ログインをテストする」セクションを使用して検証することができます。

NOTE: モバイル SSO の自動有効化は、アプリのバージョンが 9.86 以降であり、かつ、ユーザーが新しいサインイン操作を選択している場合のみ表示されます。このオプションは旧バージョンのユーザー、または以前のサインイン操作を選択しているユーザーには自動的に非表示になります。

モバイル アプリで SSO を使用する認証時に問題がある場合、SAP Concur サポート チームにチケットを作成し、表示されたエラー ID やメッセージをスクリーンショットと一緒に提供してください。

メール通知

備忘メールに SSO URL を反映する設定は、SAP Concur サポートで完了する必要のある変更です。設定を進めるには、SAP Concur サポート チームにチケットを作成し、サポート チームが備忘メールのリダイレクト URL を調整できるように、IDP 側で作成したアプリケーションの IDP URL を提供します。URL の入手方法に関する詳細については、この付録の 「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。

展開

新しい SSO 設定をテストしたら、このアクセスが必要なすべてのユーザーおよびグループに新しい Azure AD アプリケーションを割り当てることで、展開の計画を立てることができます。

[SSO の管理] ページでは、SSO 設定を [SSO 任意] から **[SSO 必須]** に変更するとこの新しい SSO 接続を強制するオプションも提供しています。この設定を変更する場合、ユーザーは SP-initiated フローからユーザー名を提供すると SAP Concur にリダイレクトされるようになります。

モバイル SSO のみを強制する必要がある場合は、SAP Concur サポートまでお問い合わせください。

セクション 8: 付録 - Microsoft Azure AD の設定

NOTE: このセクションの説明は、サード パーティー プロバイダから提供されているため、 SAP Concur はその正確性について保障することはできません。問題が発生した場合は、サード パーティー プロバイダのサポートにご連絡ください。

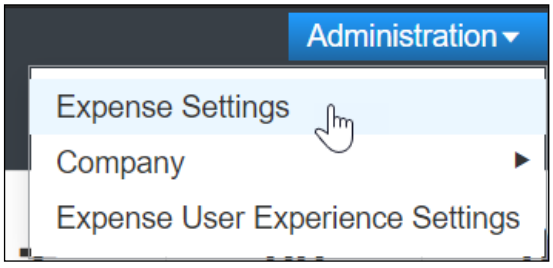
はじめに

設定プロセスを開始する前に、以下の点を確認します。

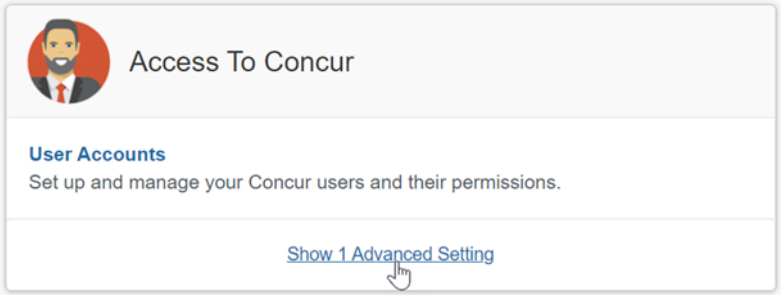
- Azure AD と SAP Concur の両方にユーザーが存在している。SAP Concur は現在、自動ユーザープロビジョニングをサポートしていないため、別途ユーザーを追加する必要があります。
- Azure AD から送信する属性が SAP Concur の各従業員の **[ログイン ID]**（**ユーザー名** / **CTE ログイン名**）フィールドと一致する。
- SAP Concur アカウントに割り当てられた組織管理者（Travel のアクセス許可）を取得している。アクセス許可を取得したら、お使いの SAP Concur のエディションに応じて、次のいずれかのパスを使用して **[SSO の管理]** ページにアクセスできるようになります。

SAP Concur **Standard** Edition の場合:

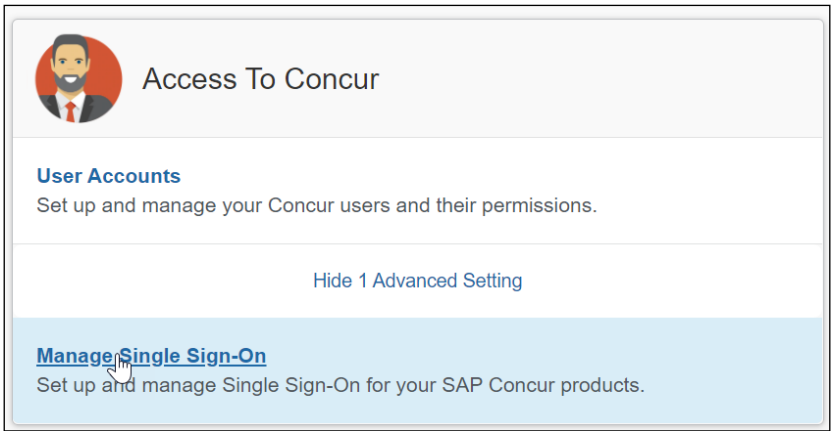
1. **[管理] > [経費の設定]** に移動します。



2. [Concur にアクセス] セクションの下にある **[1 つの詳細設定を表示]** をクリックします。

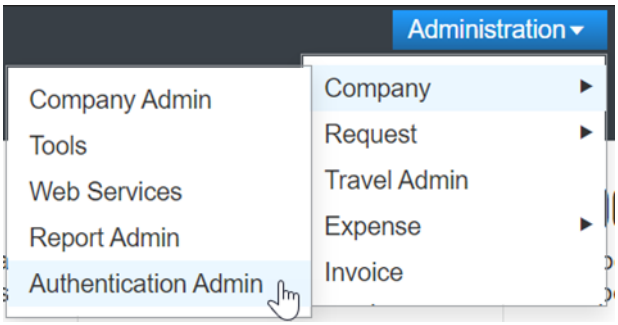


3. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。

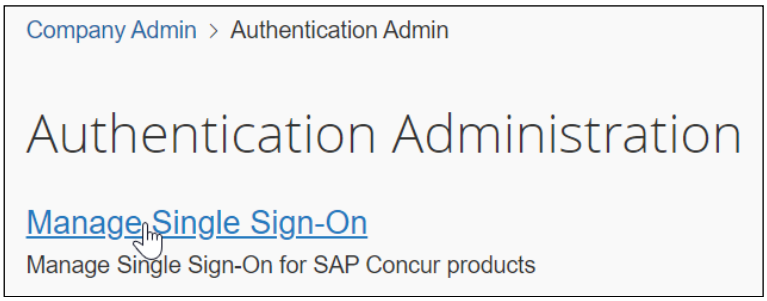


SAP Concur **Professional** Edition の場合:

4. **[管理]** > **[会社]** > **[認証管理]** に移動します。



5. **[シングル サインオンの管理]** をクリックして、[SSO の管理] ページにアクセスします。



または、以下のいずれかの URL を使用して、ページにアクセスすることができます。

- US DC Prod: https://www.concursolutions.com/nui/authadmin/ssoadmin
- US DC Test: https://implementation.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Prod: https://eu1.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Test: https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin
- CN DC Prod: https://www.concurcdc.cn/nui/authadmin/ssoadmin

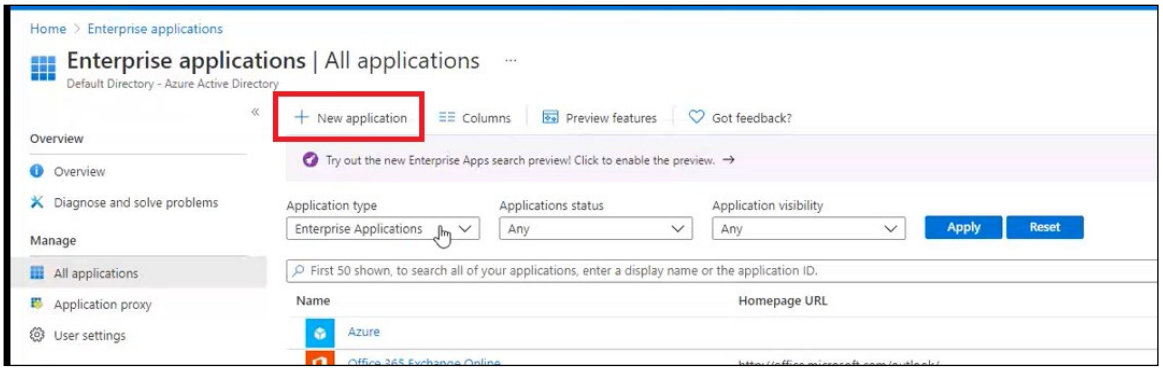
NOTE: アクセス許可を取得しておらず、自分のプロファイルに割り当てることもできない場合、会社のサポート問合せ権限の保持者に依頼し、SAP Concur サポートまでお問い合わせください。

Azure AD アプリケーションを設定する

詳細はこちら Microsoft Azure AD Guide（英語）をご参照ください。

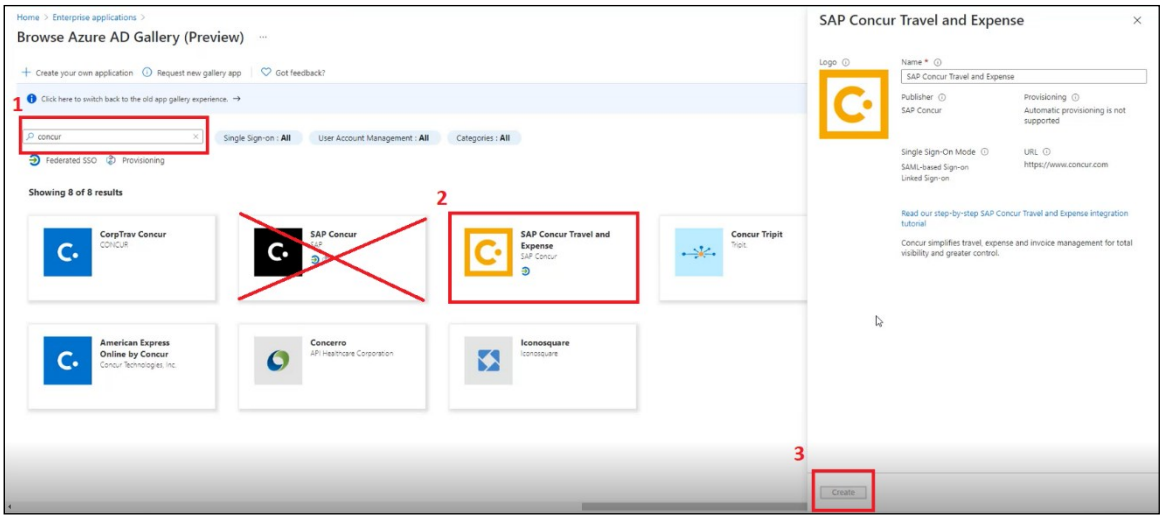
ステップ *1:* ギャラリー アプリケーションを作成する

1. **[ホーム] > [エンタープライズ アプリケーション]** に移動して、**[新しいアプリケーション]** をクリックします。



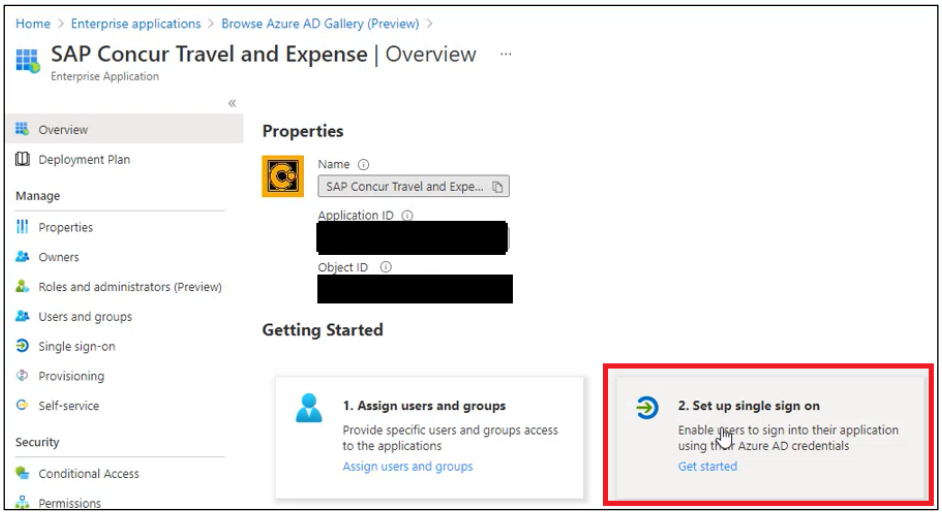
2. 「**Concur**」を検索します。

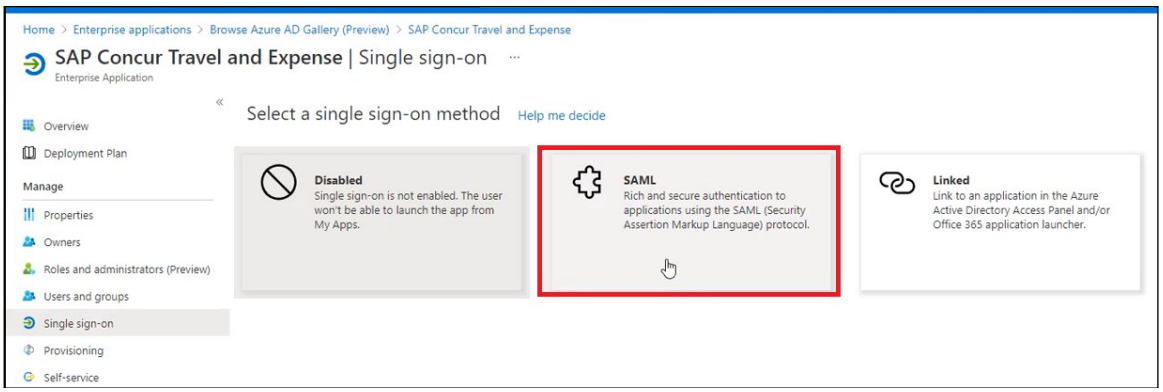
3. **[SAP Concur Travel and Expense]** オプションを選択します。黒いアイコンはレガシー SSO プラットフォームで使用されていますが、SAML2 SSO プラットフォームでは推奨されていないため、SAP Concur オプションにこのアイコンを使用しないでください。



4. **[作成]** をクリックします。

5. [**Set up Single sign on**]（シングル サインオンのセットアップ）をクリックしてから、[**SAML**] をクリックします。





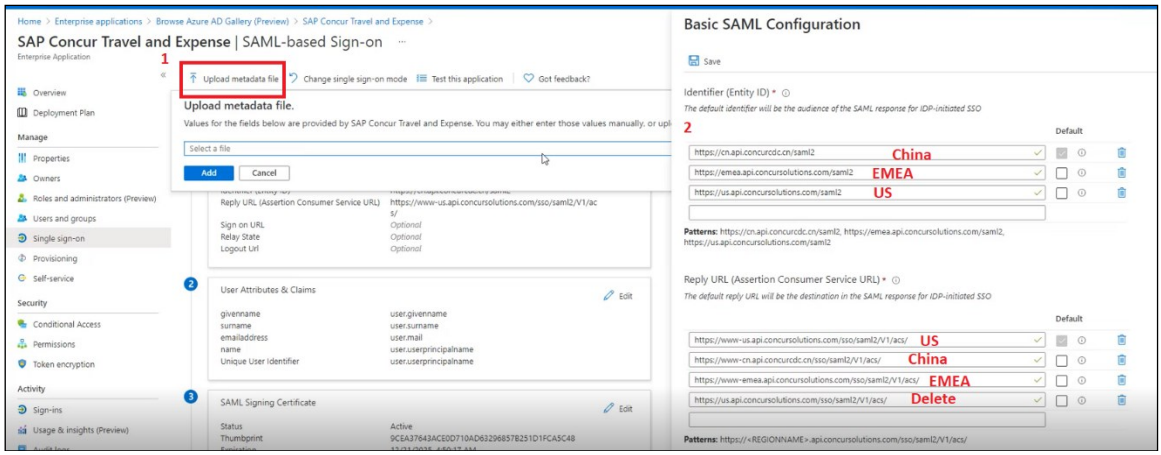
ステップ *2:* *ID* および 応答 *URL* と *Azure iD* を提供する

1. [upload metadata file]（メタデータ ファイルのアップロード）をクリックして SAP Concur メタデータをアップロードします。

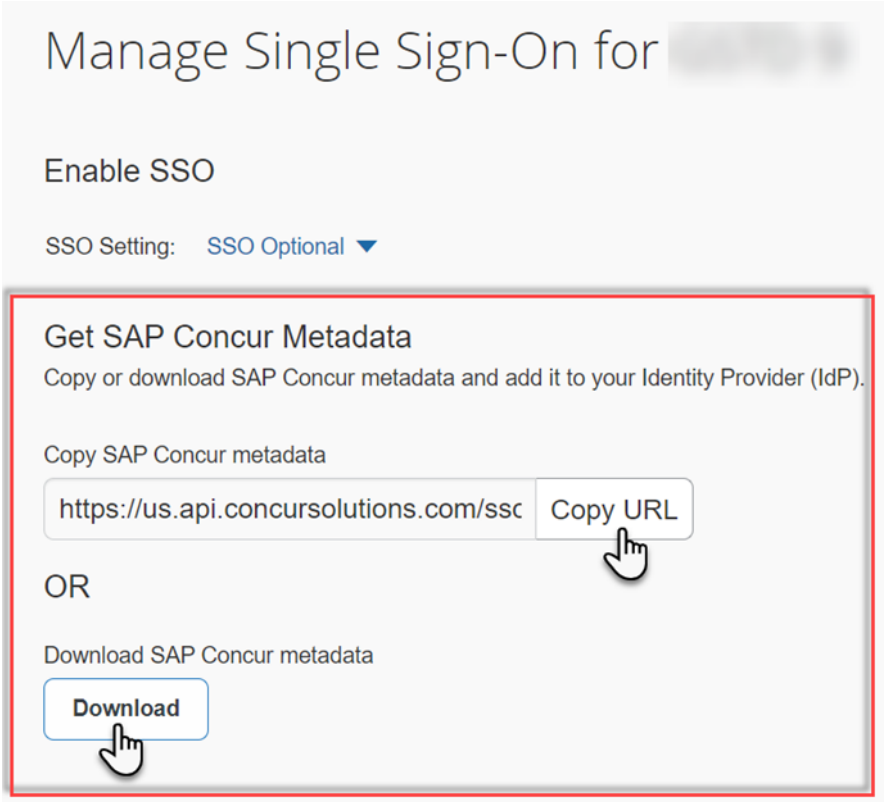
   または

2. [**基本的な SAML 構成**] オプションの [**編集**] をクリックして、SAP Concur エンティティのデータセンターとは関係のない識別子（エンティティ ID）および応答 URL (Assertion Consumer Service URL) を削除します。

NOTE: SAP Concur テスト エンティティの場合、必ず SAP Concur メタデータをアップロードして、適切な識別子（エンティティ Id）と応答 URL (Assertion Consumer Service URL) を取得する必要があります。



3. [SSO の管理] ページで SAP Concur メタデータを取得するには、**[URL をコピー]** をクリックしてから新しいブラウザ タブにその URL をクリックするか、**[ダウンロード]** をクリックしてダウンロードしたファイルを開きます。

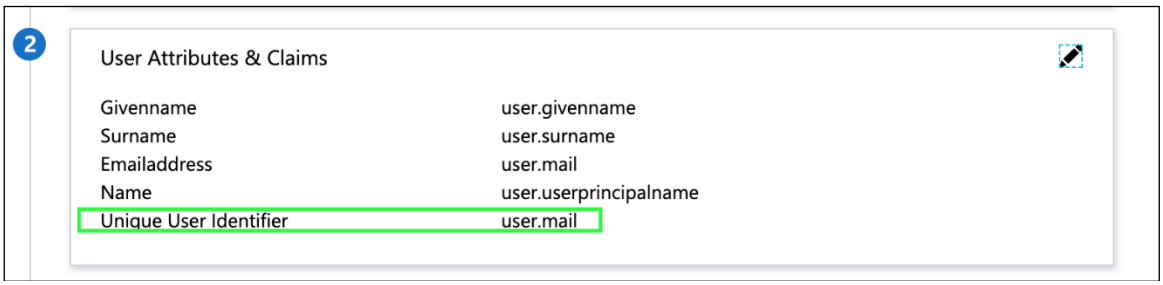


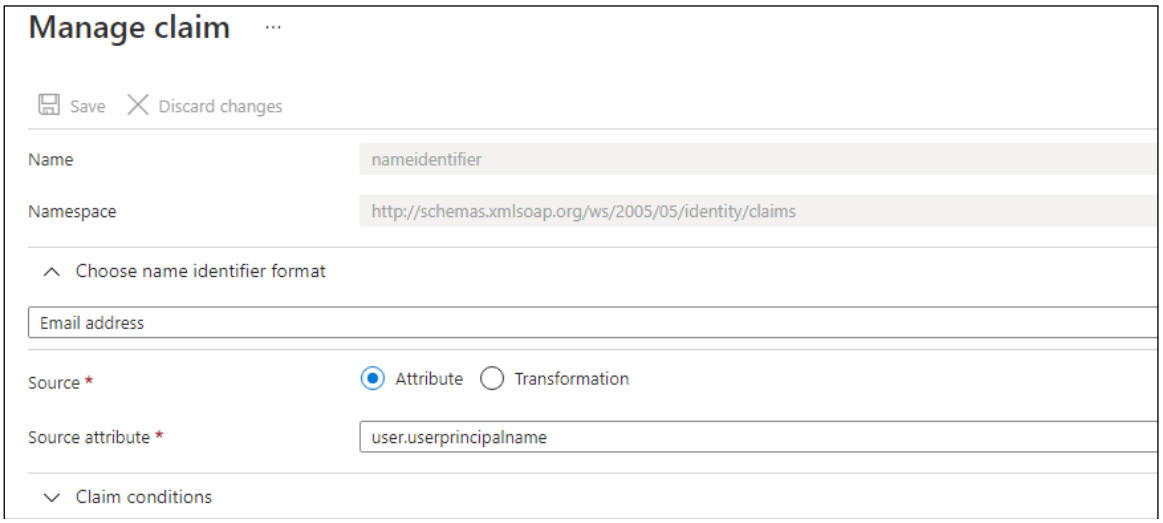
ステップ *3:* 一意のユーザー *ID* の変更

既定の一意のユーザー ID は **user.userprincipalname** です。SAP Concur では、一意のユーザー ID にメール アドレス形式を使用する必要があります。

1. 鉛筆アイコンをクリックして、**[ユーザー属性とクレーム]** セクション下のこのフィールドを編集します。

2. **user.userprincipalname** を「user.mail」に変更します。この変更を行うと、次のスクリーンショットのように表示されます。

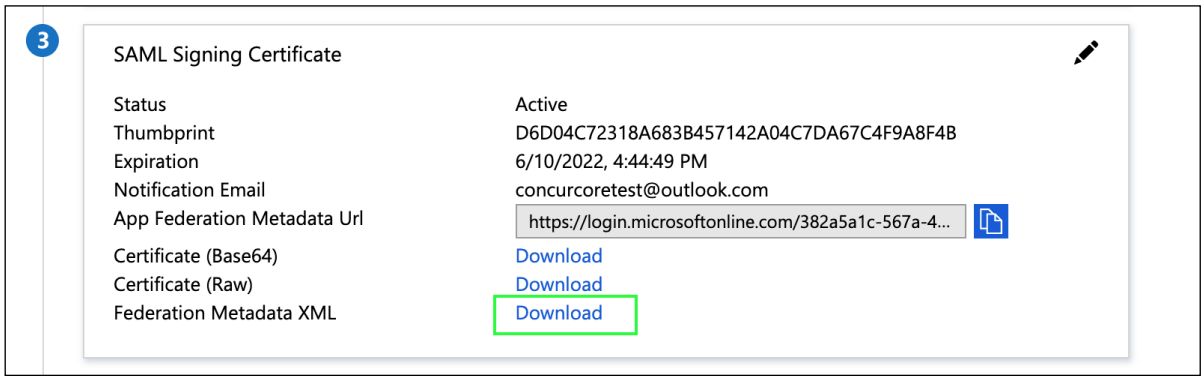




SAP Concur のログイン ID がメール アドレスと一致しない場合、[一意のユーザー ID] でカスタマイズできるため、SAP Concur に異なる値が送信されます。ただし、移行規則については、必ずメール アドレス形式で送信するようにしてください。異なる形式はモバイル アプリや concursolutions.com から行ったログインに影響を与える可能性があります。

ステップ 5: Azure AD メタデータ ファイルをダウンロードする

[ダウンロード] をクリックして「フェデレーション メタデータ XML」をダウンロードし、メタデータをローカル コンピュータに保存するか、紙のアイコンをクリックして「アプリのフェデレーション メタデータ URL」をクリックします。

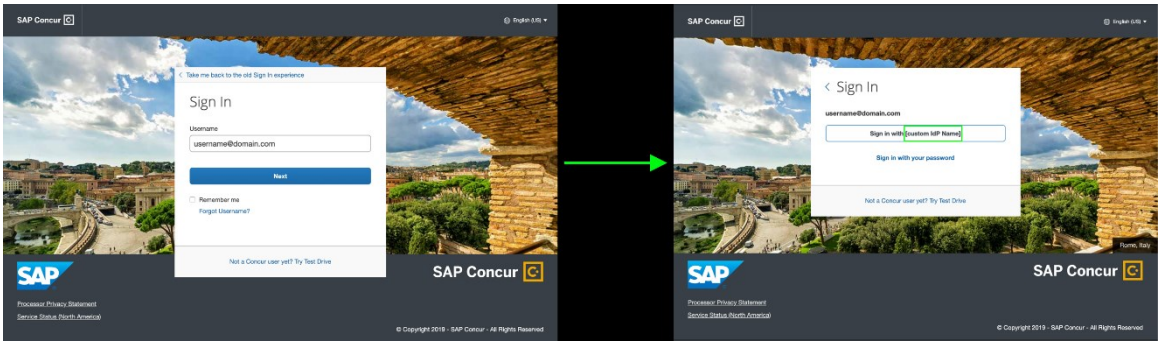


NOTE: メタデータ ファイルを SAP Concur にアップロードする前に、**[管理] > [プロパティ]** から **[ユーザーの割り当てが必要ですか?]** 設定が適切に設定されていることを確認してください。推奨設定の「はい」に設定すると、**[ユーザーとグループ]** にユーザーを追加する必要があります。

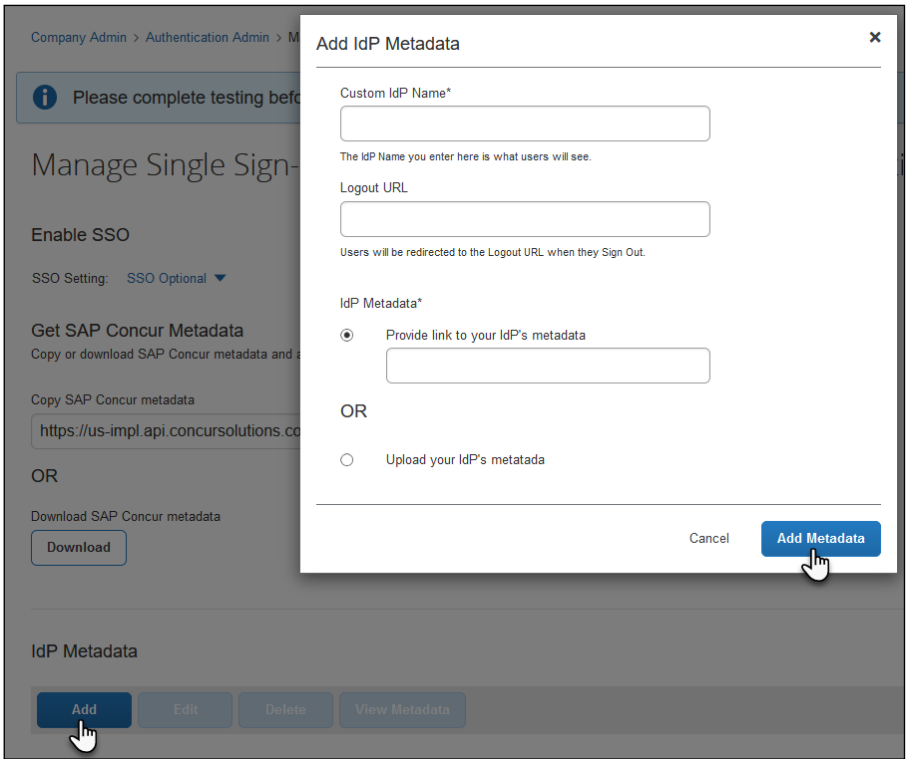
SAP Concur サイトを設定する

1. 「概要」セクションに記載されたステップに従って **[SSO の管理]** ページに移動します。
2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。
3. **[IdP 接続]** に適切な名前を入力し、その名前を **[カスタム IdP 名]** フィールドに入力します。

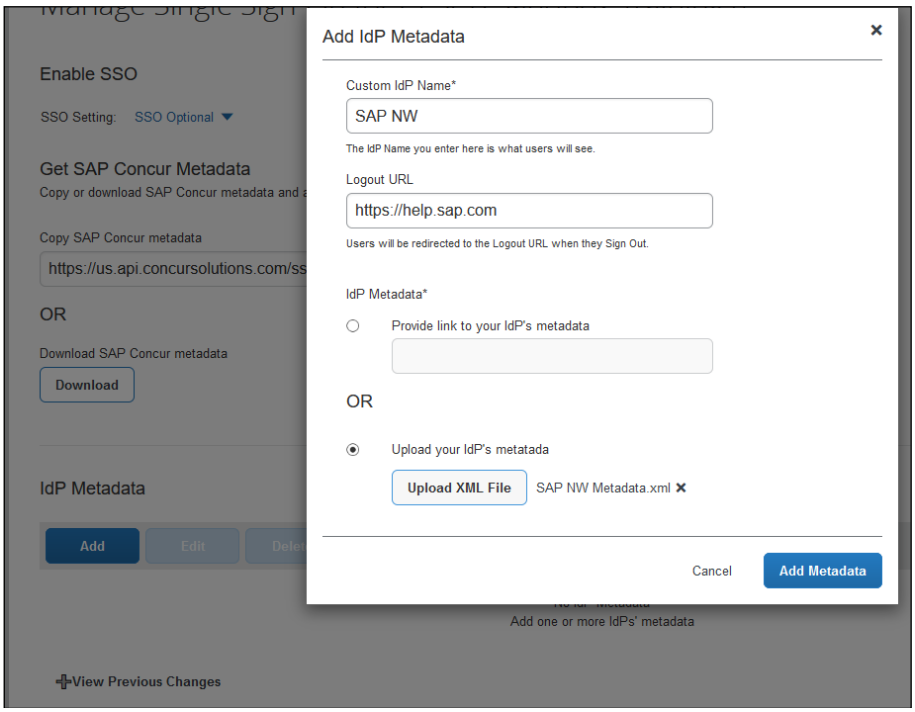
NOTE: SP-initiated フローを使用することにした場合（SAP Concur 公式サイト: https://www.concursolutions.com/nui/signin を利用）、ユーザー名を入力し **[次へ]** をクリックすると、 **[サインイン]** ページに **[カスタム IdP 名]** が表示されます。たとえば、**カスタム IdP 名** が「Azure」の場合、**[Azure でサインイン]** オプションが表示されます。



4. ユーザーがログアウトした際にほかの場所にリダイレクトされるようにログアウト URL（オプション）を入力します。既定では、URL が入力されない場合、ユーザーは認証プロセスを開始した場所にリダイレクトされます。
5. **[IdP メタデータ]** で IdP メタデータ（**アプリのフェデレーション メタデータ Url**）のリンクを入力するか、事前にローカルに保存した、IdP メタデータを含む XML ファイルをアップロードします。

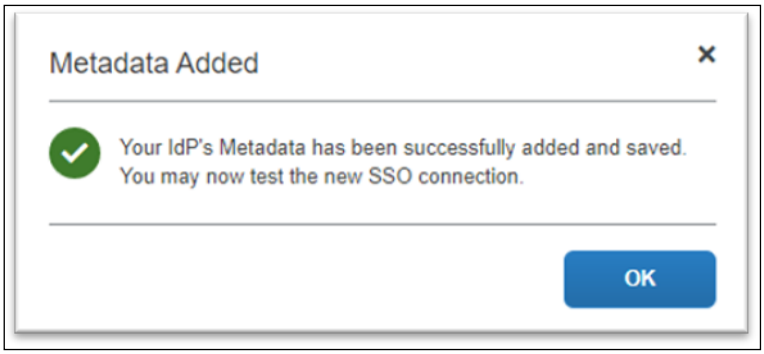


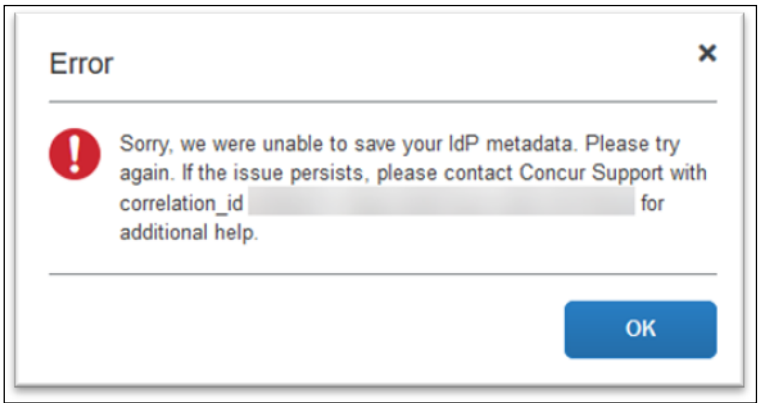
すべての詳細を入力すると、次のように表示されます。



6. **[メタデータの追加]** をクリックします。

7. 追加の成功を示す確認メッセージまたは問題の発生を示すメッセージが表示されます。後者の場合、SAP Concur サポートに問い合わせて、相関 ID をご提供ください。





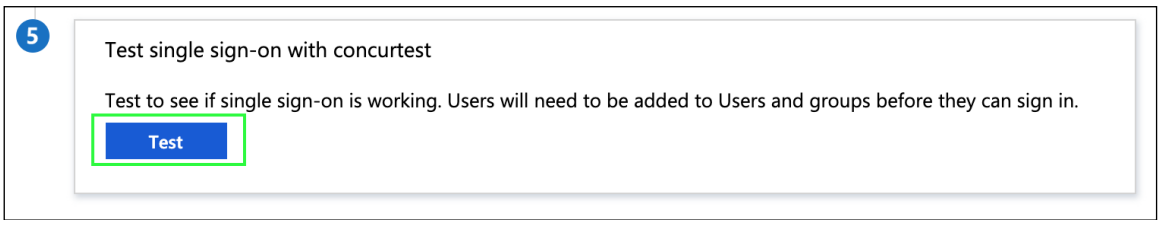
SSO ログインをテストする

前述のステップで IdP メタデータが SAP Concur に正常にアップロードされると、SSO のテストを開始できます。このセクションでは、IdP-Initiated（アイデンティティ プロバイダ側で開始される）フローおよび SP-Initiated（サービス プロバイダ側で開始される）フローをテストすることができます。

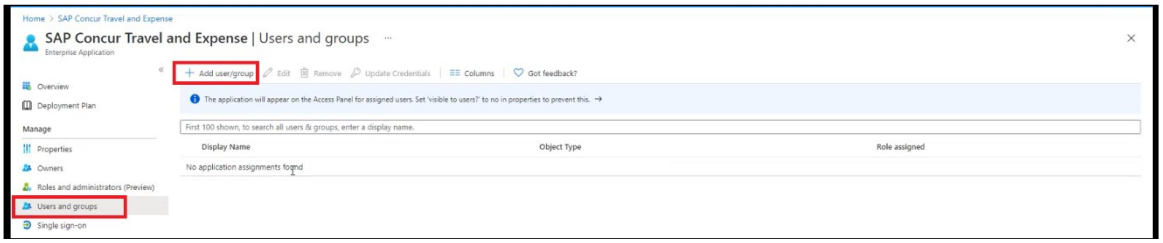
IdP-initiated SSO をテストする

（オプション 1）[テスト] ボタンを使用して IdP-initiated SSO をテストするには:

1. Azure AD で同じメール アドレスを持つ同一のアカウントが SAP Concur に存在する場合、Azure で **[テスト]** をクリックして IDP-initiated フローのログインをテストできます。Mobile SSO テストで重要になることから、SP-Initiated フローをテストする必要があることには変わりありません。

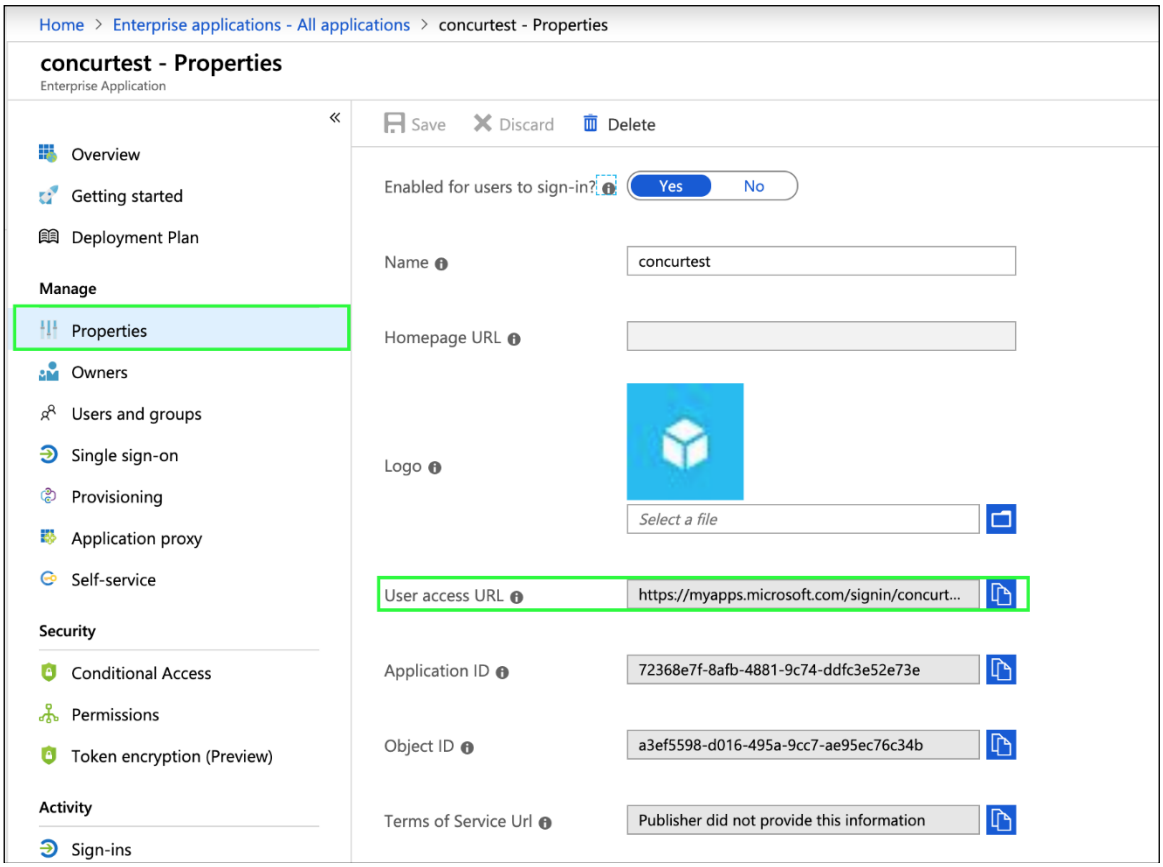


SSO をテストする前に、先ほど設定したこのテスト アプリケーションに Azure AD から新たに追加するユーザーを追加します。これを行うには、**[ユーザーとグループ]** および **[+ ユーザーの追加]** をクリックします。



（オプション 2）ユーザーのアクセス URL で IdP-initiated SSO をテストするには:

1. **[管理] > [プロパティ]** に移動し、**[ユーザーのアクセス URL]** をコピーします。テスト ユーザーにこの URL を提供し、ブラウザにコピー ペーストするように依頼します。まず、Microsoft のログイン ページが表示されます。その後、ほかの操作を行うことなく、直接 SAP Concur に対して認証が行われます。



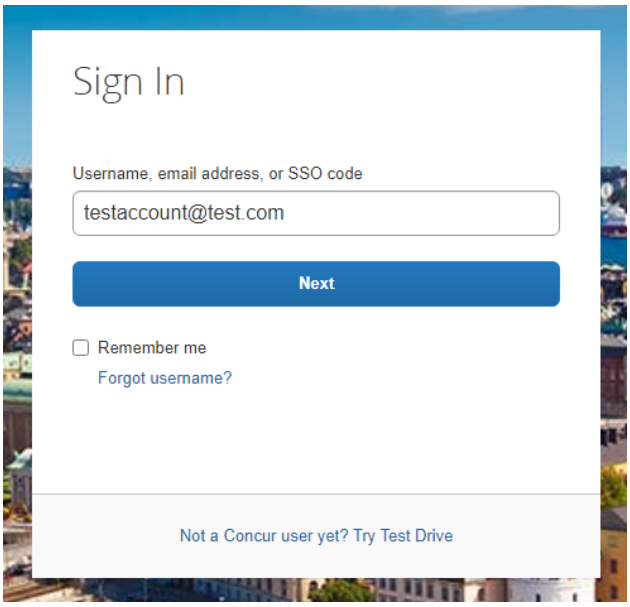
（オプション 3）Microsoft 365 で IdP-initiated SSO をテストするには:

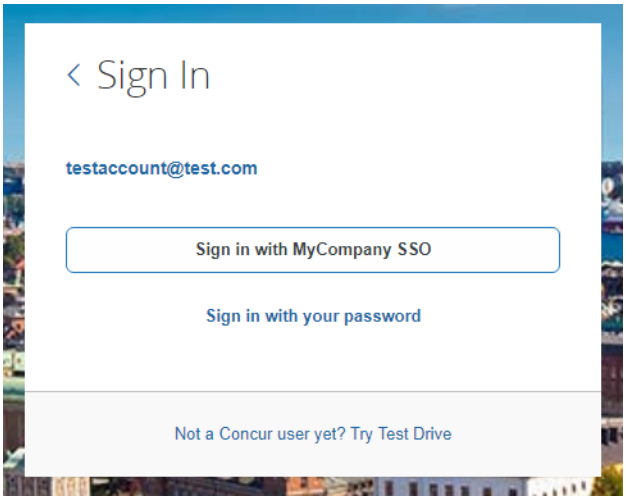
1. アプリケーションを数人のテスト ユーザーに割り当てると、Microsoft 365 ポータルに新しいアプリケーションが表示されるようになります。ユーザーは新しいアプリケーションをクリックできるようになり、それから SAP Concur に対して直接認証されることになります。SAP Concur アプリケーション アイコンの背後の URL は 1 つ目のテスト オプションのユーザーのアクセス URL と同じです。

SP-initiated SSO をテストする

SP-initiated SSO をテストするには:

1. テストを行う環境に応じた SAP Concur ログイン ページを開きます。
   - US DC Prod: https://www.concursolutions.com/
   - US DC Test: https://implementation.concursolutions.com/
   - EMEA DC Prod: https://eu1.concursolutions.com/
   - EMEA DC Test: https://eu1imp.concursolutions.com/
   - CN DC Prod: https://www.concurcdc.cn/
2. ログイン ページでユーザー名、照合済メール アドレス、または SSO コードを追加して続行できます。**[次へ]** をクリックすると、最近作成した SSO 設定のオプションが表示されます。クリックして、SAP Concur にリダイレクトするアイデンティティ プロバイダ アカウントの認証を続行します。





モバイル シングル サインオン（SSO）

SAMLv2 プラットフォームで作成された SSO 設定の場合、モバイル SSO はメタデータが保存されるとすぐに自動的に有効にされます。ただし、このオプションが機能するには、SP-Initiated フローが機能している必要があります。これは、前述の「SSO ログインをテストする」セクションを使用して検証することができます。

NOTE: モバイル SSO の自動有効化は、アプリのバージョンが 9.86 以降であり、かつ、ユーザーが新しいサインイン操作を選択している場合のみ表示されます。このオプションは旧バージョンのユーザー、または以前のサインイン操作を選択しているユーザーには自動的に非表示になります。そのような場合、ユーザーがモバイル端末でも SSO を使用して必ずログインできるようにするには、SAP Concur サポート チームにチケットを作成し、サポート チームが従来のアプリ バージョンにモバイル SSO を有効化できるように、Azure 側で構築したアプリケーションの「ユーザーのアクセス URL」を提供してください。この URL は Azure 管理者アカウントの **[管理] > [プロパティ]** から入手できます。

モバイル アプリで SSO を使用する認証時に問題がある場合、SAP Concur サポート チームにチケットを作成し、表示されたエラー ID やメッセージをスクリーンショットと一緒に提供してください。

メール通知

備忘メールに SSO URL を反映する設定は、SAP Concur サポートで完了される必要のある変更です。設定を進めるには、SAP Concur サポート チームにチケットを作成し、サポート チームが備忘メールのリダイレクト URL を調整できるように、IDP 側で作成したアプリケーションの IDP URL を提供します。URL の入手方法に関する詳細については、この付録の 「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。

展開

新しい SSO 設定をテストしたら、このアクセスが必要なすべてのユーザーおよびグループに新しい Azure AD アプリケーションを割り当てることで、展開の計画を立てることができます。

[SSO の管理] ページで、SSO 設定を [SSO 任意] から **[SSO 必須]** に変更すると、この新しい SSO 接続を強制するオプションも提供されます。この設定を変更する場合、ユーザーは SP-initiated フローからユーザー名を提供すると SAP Concur にリダイレクトされるようになります。

モバイル SSO のみを強制する必要がある場合は、SAP Concur サポートまでお問い合わせください。

セクション 9: 付録- Idaptive の設定

NOTE: このセクションの説明はサード パーティー プロバイダから提供されているため、 SAP Concur はその正確性について保障することはできません。問題が発生した場合は、サード パーティー プロバイダのサポートにご連絡ください。

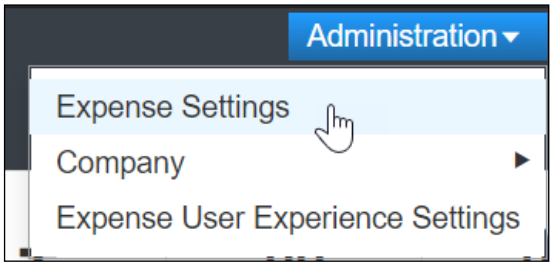
はじめに

設定プロセスを開始する前に、以下の点を確認します。

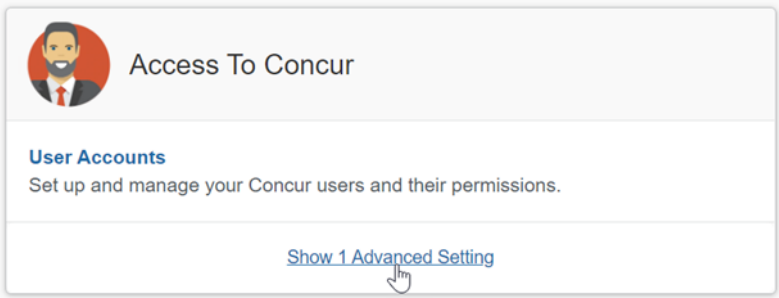
- Idaptive と SAP Concur の両方にユーザーが存在している。SAP Concur は現在、自動ユーザー プロビジョニングをサポートしていないため、別途ユーザーを追加する必要があります。
- Idaptive から送信する属性が SAP Concur の各従業員の **[ログイン ID]**（**ユーザー名 / CTE ログイン名**）フィールドと一致する。
- SAP Concur アカウントに割り当てられた組織管理者（Travel のアクセス許可）を取得している。アクセス許可を取得したら、お使いの SAP Concur のエディションに応じて、次のいずれかのパスを使用して **[SSO の管理]** ページにアクセスできるようになります。

SAP Concur **Standard** Edition の場合:

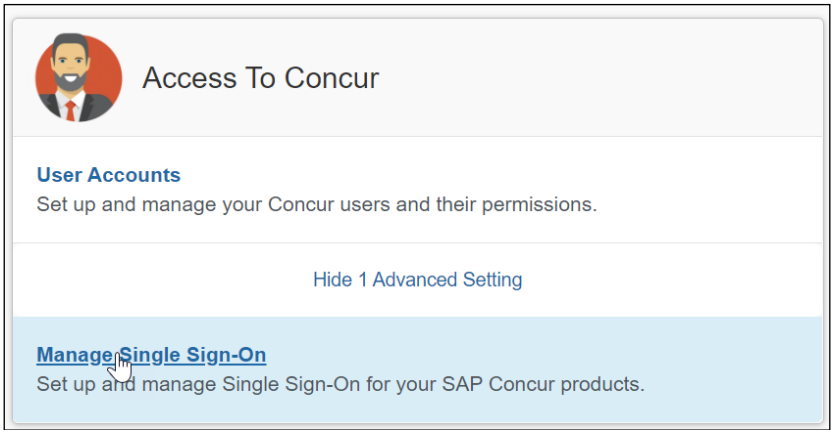
1. **[管理] > [経費の設定]** に移動します。



2. [Concur にアクセス] セクションの下にある **[1 つの詳細設定を表示]** をクリックします。

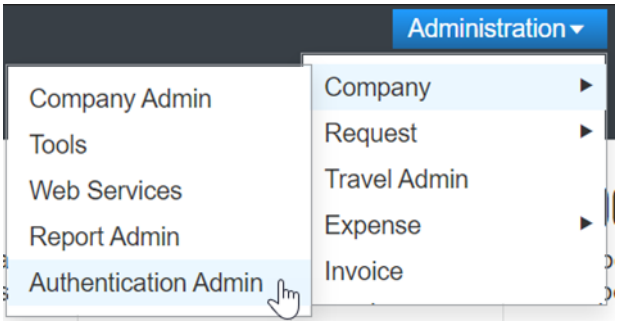


3. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。

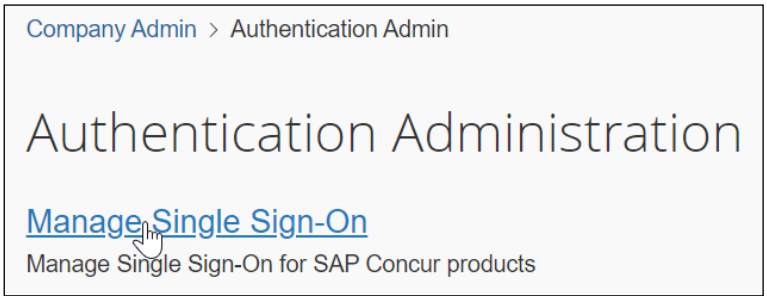


SAP Concur **Professional** Edition の場合:

1. **[管理]** > **[会社]** > **[認証管理]** に移動します。



2. **[シングル サインオンの管理]** をクリックして、[SSO の管理] ページにアクセスします。



または、以下のいずれかの URL を使用して、ページにアクセスすることができます。

- US DC Prod: https://www.concursolutions.com/nui/authadmin/ssoadmin
- US DC Test: https://implementation.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Prod: https://eu1.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Test: https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin
- CN DC Prod: https://www.concurcdc.cn/nui/authadmin/ssoadmin

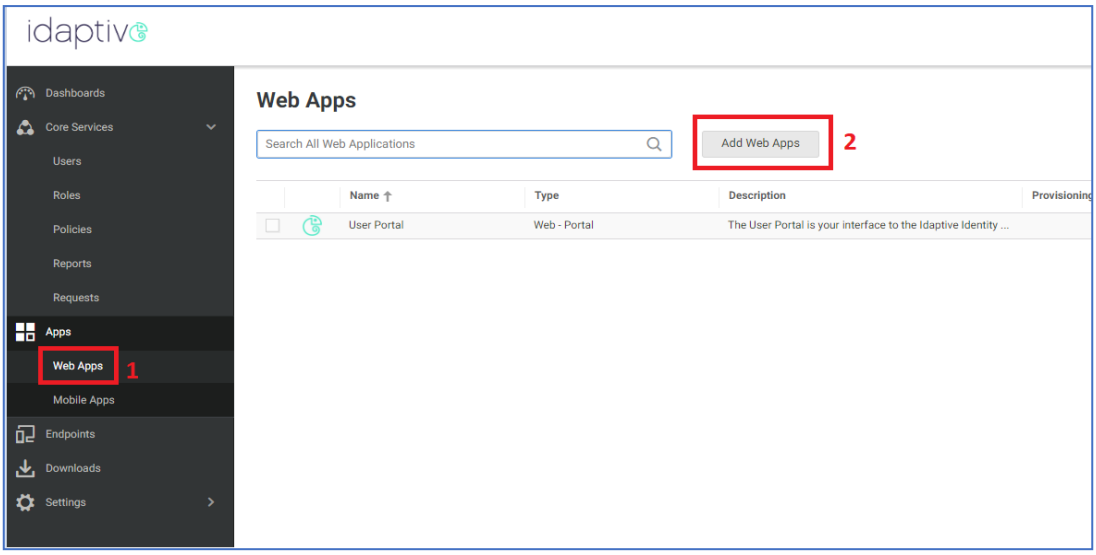
---

NOTE: アクセス許可を取得しておらず、自分のプロファイルに割り当てることもできない場合、会社のサポート問合せ権限の保持者に依頼し、SAP Concur サポートまでお問い合わせください。

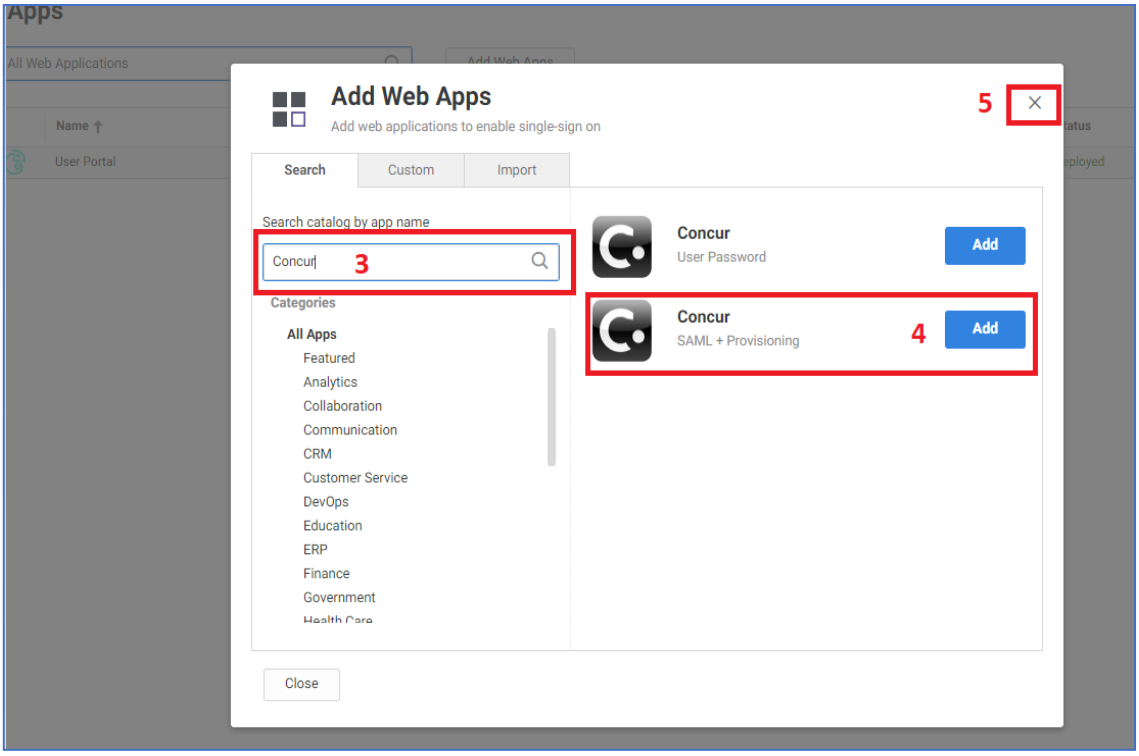
Idaptive アプリケーションを設定する

ステップ 1: Idaptive アプリを作成する

1. Idaptive の管理者用ホーム ページで **[Web Apps]** をクリックします。
2. **[Add Web Apps]** をクリックします。



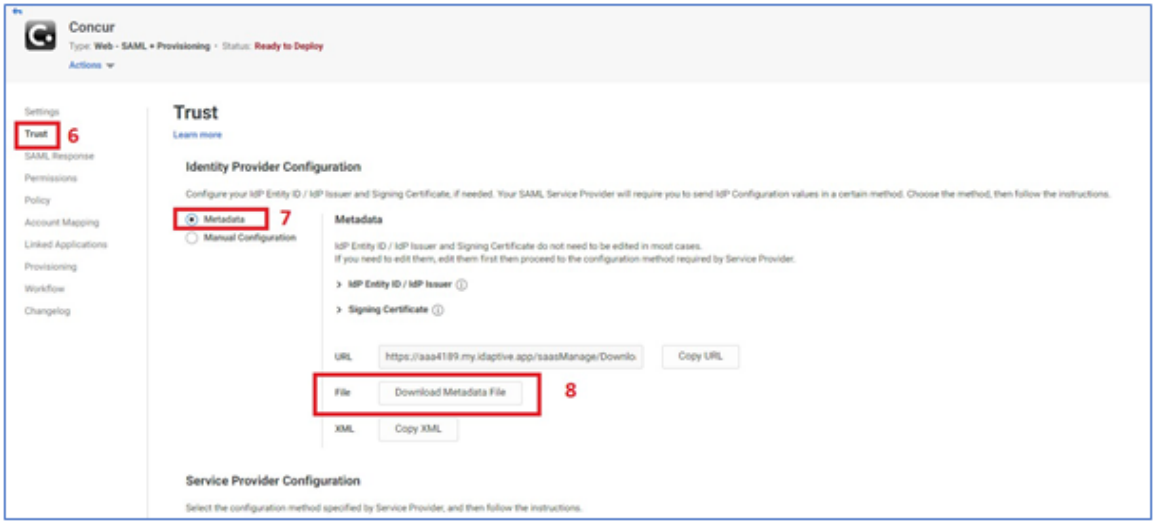
3. 「**Concur**」を検索します。
4. **[SAML + Provisioning]** オプションの隣の **[Add]** をクリックします。ポップアップが表示されたら、そのポップアップを閉じます。



5. Concur のアプリケーション設定で、**[Trust]** をクリックします。

6. **[Metadata]** オプションを選択します。

7. **[Download Metadata File]** をクリックします（後で SAP Concur にメタデータをアップロードする際に使用するため）。



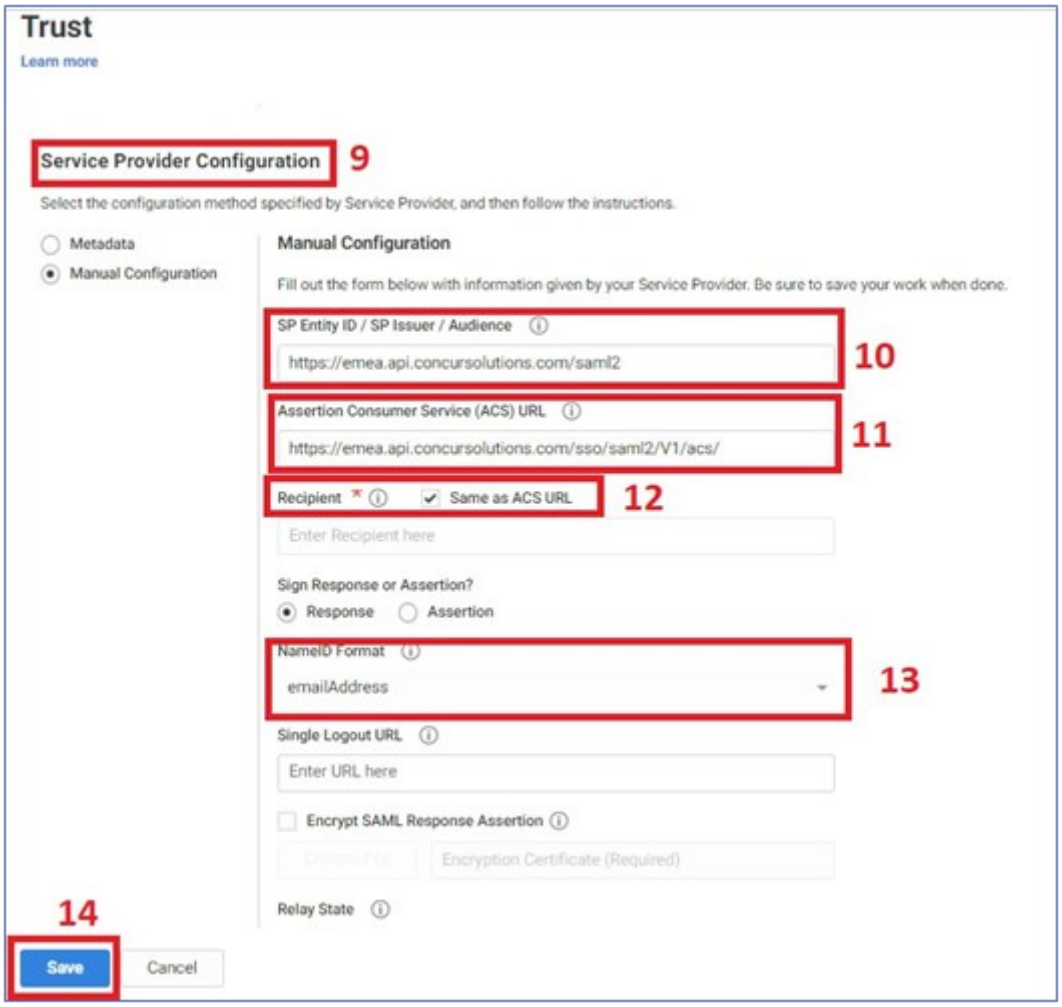
8. **[Service Provider Configuration]** セクションにスクロール ダウンします。

9. SAP Concur メタデータを開き、**エンティティ ID** の値をコピーして **[SP Entity ID / SP Issuer / Audience]** フィールドに貼り付けます。

10. メタデータから所在地の値をコピーして **[Assertion Consumer Service (ACS) URL]** に貼り付けます。

11. [Recipient] で **[Same as ACS URL]** オプションが選択されていることを確認します。

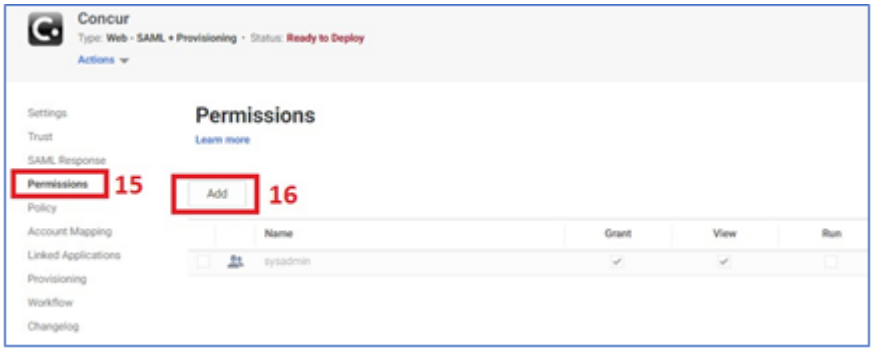
12. **[NameID Format]** フィールドについては、この形式が SAP Concur ログイン ID と一致している必要があります。SAP Concur ログイン ID がメール アドレスと同じ形式である場合は **[emailAddress]** を選択しますが、SAP Concur ログイン ID の形式（例: employeeid@companydomain.com）に応じで別のオプションを選択します。ログイン ID の形式がメール アドレスとは異なる場合でも、SAML 応答の [Name ID format] はメール アドレス形式である必要があります。



13. **[保存]** をクリックします。

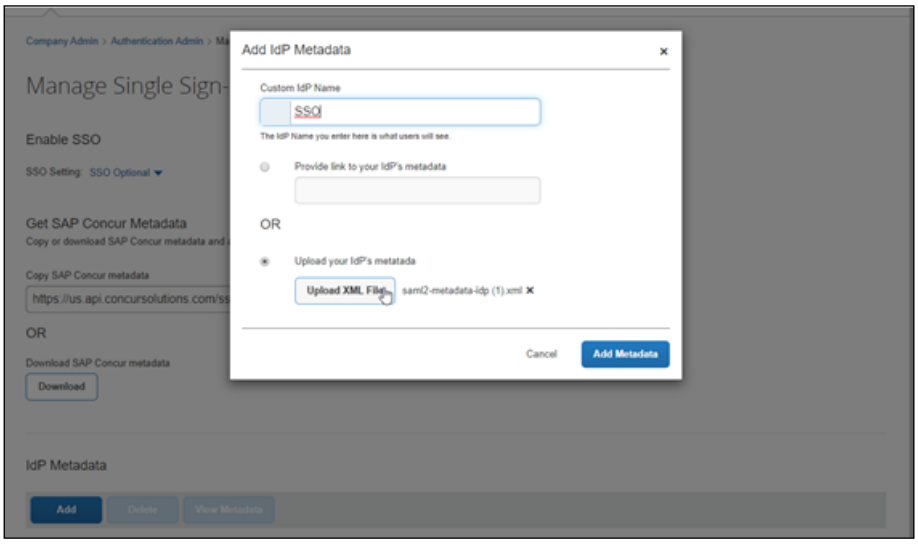
14. **[Permissions]** をクリックします。

15. SAP Concur アプリにアクセスする必要のあるグループやユーザーを追加し、**[Save]** をクリックします。



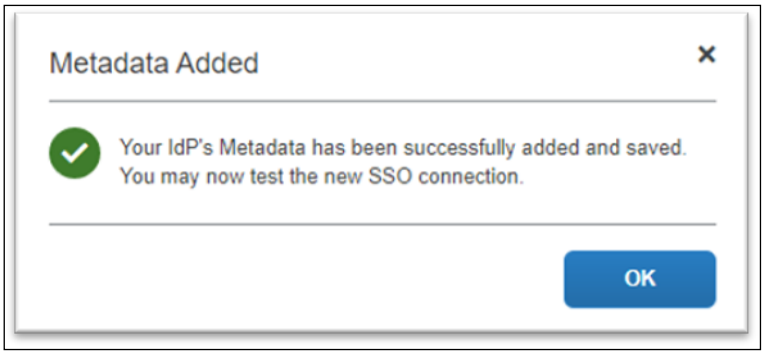
SAP Concur サイトを設定する

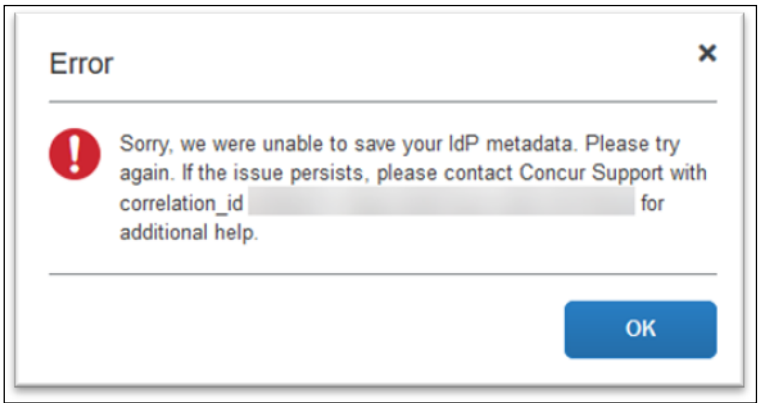
1. 「概要」セクションに記載されたステップに従って **[SSO の管理]** ページに移動します。
2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。
3. **[IdP 接続]** に適切な名前を入力し、その名前を **[カスタム IdP 名]** フィールドに入力します。



NOTE: SP-initiated フローを使用することにした場合（SAP Concur 公式サイト: https://www.concursolutions.com/nui/signin を利用）、ユーザー名を入力し **[次へ]** をクリックすると、 **[サインイン]** ページに **[カスタム IdP 名]** が表示されます。

4. **[メタデータの追加]** をクリックします。
5. 追加の成功を示す確認メッセージまたは問題の発生を示すメッセージが表示されます。後者の場合、SAP Concur サポートに連絡し、相関 ID を提供してください。





SSO ログインをテストする

IdP-initiated SSO をテストする

Idaptive から SSO ログインをテストするには、テストを行うユーザーやグループに Idaptive で設定した新しいアプリケーションを必ず割り当てている必要があります。

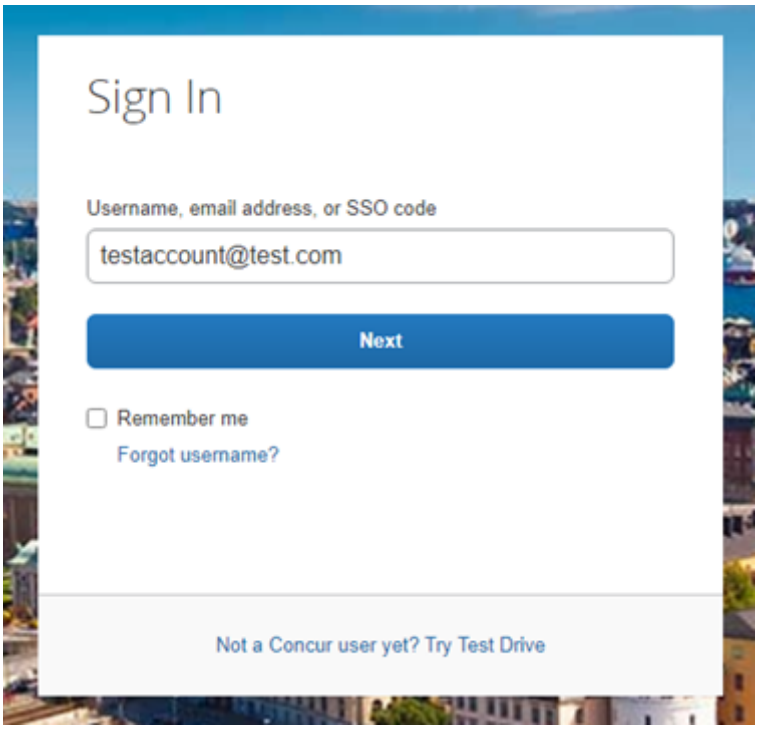
これが完了すると、Idaptive にログインして SAP Concur アプリケーションを検索できるようになります。このアプリケーションはすでにログインしている SAP Concur のアカウントにリダイレクトします。

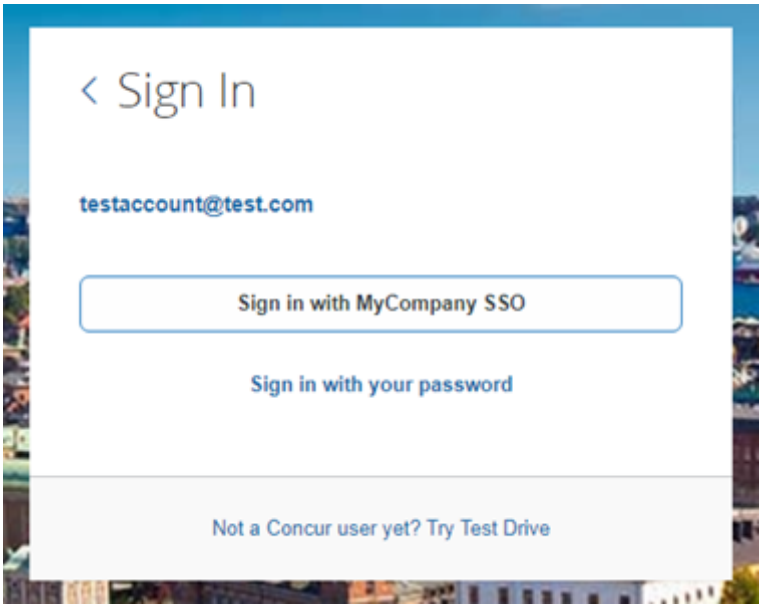
SP-initiated SSO をテストする

SP-initiated SSO をテストするには:

1. テストを行う環境に応じた SAP Concur ログイン ページを開きます。
   - US DC Prod: https://www.concursolutions.com/
   - US DC Test: https://implementation.concursolutions.com/
   - EMEA DC Prod: https://eu1.concursolutions.com/
   - EMEA DC Test: https://eu1imp.concursolutions.com/
   - CN DC Prod: https://www.concurcdc.cn/

2. ログイン ページでユーザー名、照合済メール アドレス、または SSO コードを追加して続行できます。**[次へ]** をクリックすると、「SAP Concur サイトを設定する」の注記のとおり、最近作成した SSO 設定のオプションが表示されます。クリックして、SAP Concur にリダイレクトするアイデンティティ プロバイダ アカウントの認証を続行します。





SSO 資格情報を追加した後にエラー メッセージが表示された場合、設定が完了していない可能性があることを示しています。SAP Concur 側のエラー メッセージの場合、資格情報が一致しない、証明書が無効である、または設定が指定されていないという問題である可能性があります。IdP-Initiated ログインは機能していて、SP-Initiated が機能していない場合、Idaptive 側の名前 ID が適切な形式で（メール アドレス）で送信されていない可能性があります。

問題が解決しない場合、SAP Concur サポートに問い合わせ、表示されたエラー ID を提供してください。

モバイル シングル サインオン（SSO）

SAMLv2 プラットフォームで作成された SSO 設定の場合、モバイル SSO はメタデータが保存されるとすぐに自動的に有効にされます。ただし、このオプションが機能するには、SP-Initiated フローが機能している必要があります。これは、前述の「SSO ログインをテストする」セクションを使用して検証することができます。

NOTE: モバイル SSO の自動有効化は、アプリのバージョンが 9.86 以降であり、かつ、ユーザーが新しいサインイン操作を選択している場合のみ表示されます。このオプションは旧バージョンのユーザー、または以前のサインイン操作を選択しているユーザーには自動的に非表示になります。

[モバイル SSO でサインイン] オプションにより以前の IdP リンクが埋め込まれるため、ユーザーは以前の SSO 接続にリダイレクトされます。

いずれの場合も、SAP Concur サポート チームにチケットを作成し、次の情報を提供してください。

- ユーザーが以前のバージョンを使用する予定の場合、当該アプリ バージョンにモバイル SSO を有効化できるように、Idaptive 側で作成したアプリケーションの IdP-Initiated URL を SAP Concur サポートに提供してください。URL の入手方法に関する詳細については、このガイドの「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。
- 混乱する可能性を排除するために **[モバイル SSO でサインイン]** オプションを削除する場合、サポート チームにご連絡ください。

モバイル アプリで SSO を使用する認証時に問題がある場合、SAP Concur サポート チームにチケットを作成し、表示されたエラー ID やメッセージをスクリーンショットと一緒に提供してください。

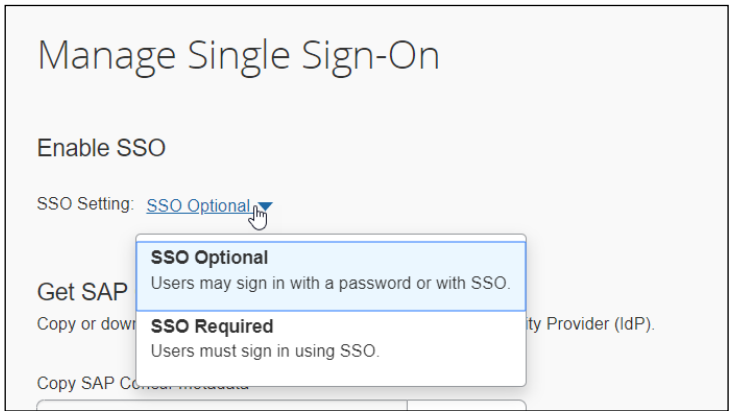
メール通知

備忘メールに SSO URL を反映する設定は、SAP Concur サポートで完了される必要のある変更です。設定を進めるには、SAP Concur サポート チームにチケットを作成し、サポート チームが備忘メールのリダイレクト URL を調整できるように、IDP 側で作成したアプリケーションの IDP URL を提供します。URL の入手方法に関する詳細については、この付録の「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。

展開

新しい SSO 設定をテストしたら、このアクセスが必要なすべてのユーザーおよびグループに新しい Idaptive アプリケーションを割り当てることで、展開の計画を立てることができます。

[SSO の管理] ページでは、SSO 設定を [SSO 任意] から **[SSO 必須]** に変更するとこの新しい SSO 接続を強制するオプションも提供しています。この設定を変更する場合、ユーザーは SP-initiated フローからユーザー名を提供すると SAP Concur にリダイレクトされるようになります。



モバイル SSO のみを強制する必要がある場合は、SAP Concur サポートまでお問い合わせください。

セクション 10: 付録- Okta の設定

NOTE: このセクションの説明はサード パーティー プロバイダから提供されているため、 SAP Concur はその正確性について保障することはできません。問題が発生した場合は、サード パーティー プロバイダのサポートにご連絡ください。

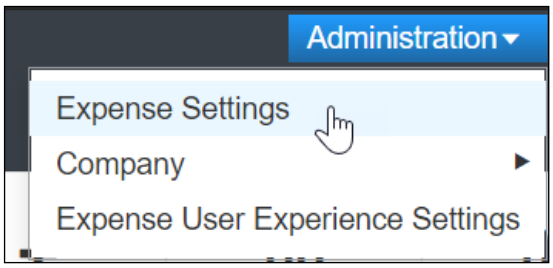
はじめに

設定を始める前に以下のことをご確認ください。

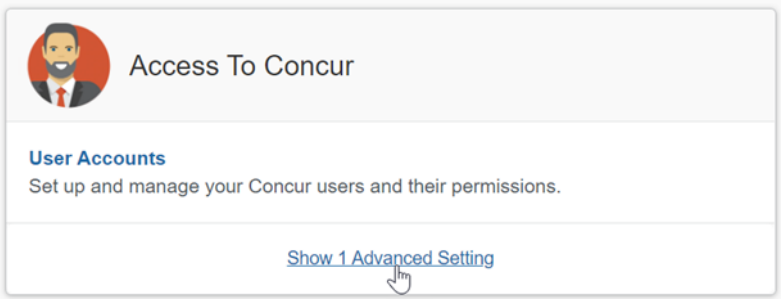
- アイデンティティ プロバイダ（Okta）の管理者アクセス権を取得している。これは Okta 側でアプリケーションの設定を完了するために必要になります。
- Okta と SAP Concur の両方にユーザーが存在している。SAP Concur は現在、自動ユーザー プロビジョニングをサポートしていないため、別途ユーザーを追加する必要があります。
- Okta から送信する属性が SAP Concur の各従業員の **[ログイン ID]**（**ユーザー名 / CTE ログイン名**）フィールドと一致する。
- SAP Concur アカウントに割り当てられた組織管理者（Travel のアクセス許可）を取得している。アクセス許可を取得したら、お使いの SAP Concur のエディションに応じて、次のいずれかのパスを使用して **[SSO の管理]** ページにアクセスできるようになります。

SAP Concur **Standard** Edition の場合:

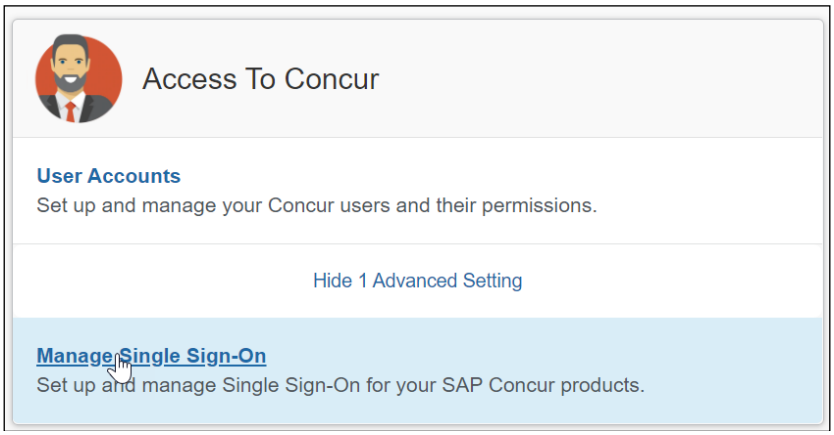
1. **[管理] > [経費の設定]** に移動します。



2. [Concur にアクセス] セクションの下にある **[1 つの詳細設定を表示]** をクリックします。

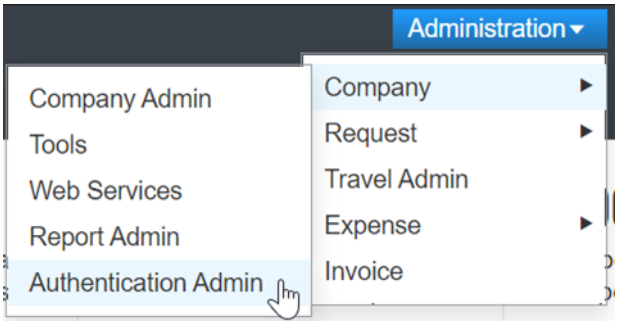


3. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。

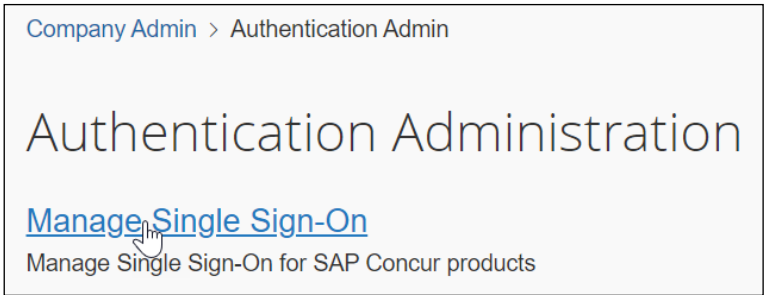


SAP Concur **Professional** Edition の場合:

1. **[管理]** > **[会社]** > **[認証管理]** に移動します。



2. **[シングル サインオンの管理]** をクリックして、[SSO の管理] ページにアクセスします。



または、以下のいずれかの URL を使用して、ページにアクセスすることができます。

- US DC Prod: https://www.concursolutions.com/nui/authadmin/ssoadmin
- US DC Test: https://implementation.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Prod: https://eu1.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Test: https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin
- CN DC Prod: https://www.concurcdc.cn/nui/authadmin/ssoadmin

---

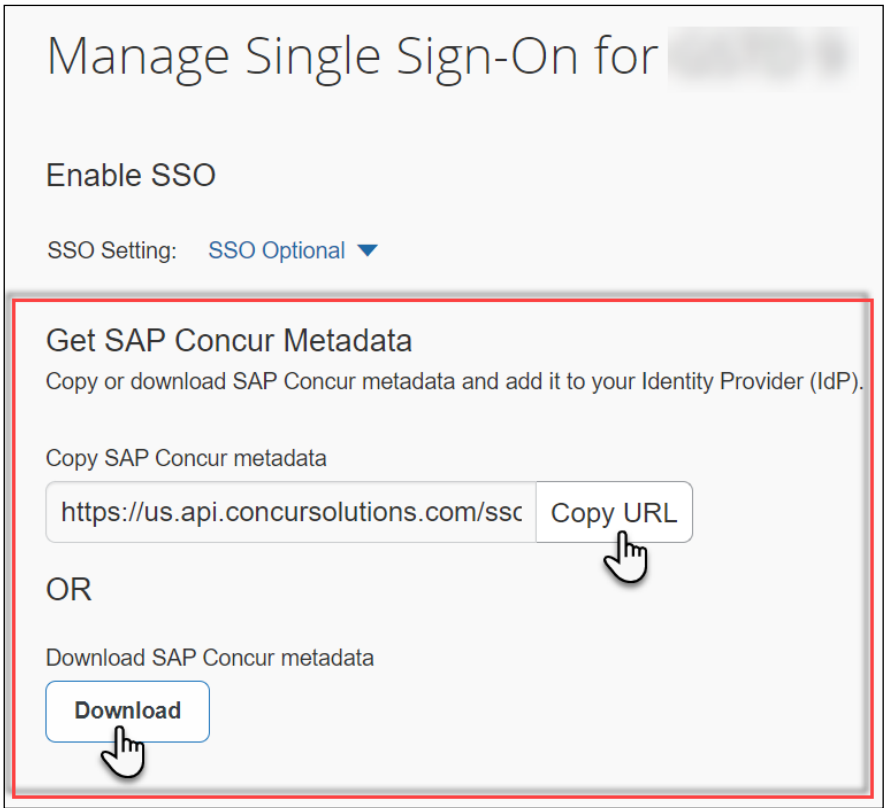
NOTE: アクセス許可を取得しておらず、自分のプロファイルに割り当てることもできない場合、会社のサポート問合せ権限の保持者に依頼し、SAP Concur サポートまでお問い合わせください。

Okta アプリケーションを設定する

ステップ 1:SAP Concur メタデータを入手する

設定方法:

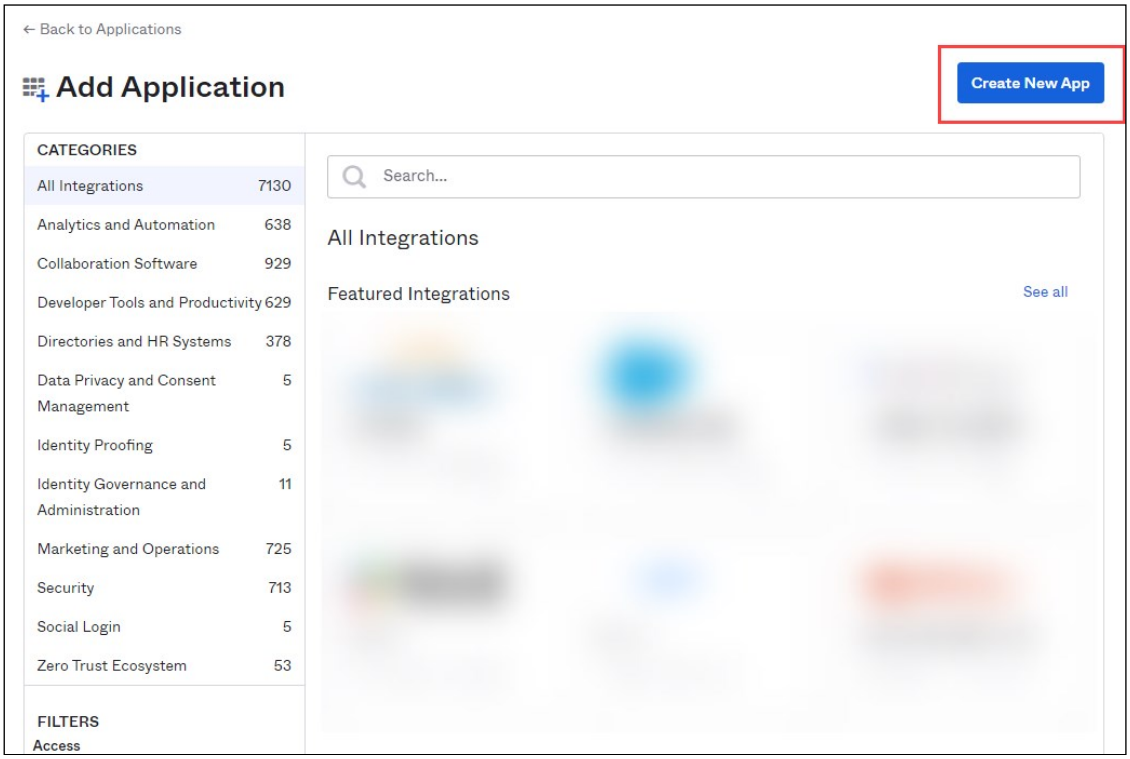
1. SAP Concur メタデータを入手します。これを完了するには、「概要」セクションの説明に従って SAP Concur アカウントにログインし、**[SSO の管理]** セクションにアクセスします。[SSO の管理] ページで SAP Concur メタデータを取得するには、**[URL をコピー]** をクリックしてから新しいブラウザ タブにその URL をクリックするか、**[ダウンロード]** をクリックしてダウンロードしたファイルを開きます。


Manage Single Sign-On for
Enable SSO
SSO Setting:
SSO Optional
Get SAP Concur Metadata
Copy or download SAP Concur metadata and add it to your Identity Provider (IdP).
Copy SAP Concur metadata
https://us.api.concursolutions.com/ssc
Copy URL
OR
Download SAP Concur metadata
Download

ステップ *2: Okta* でアプリケーションを作成する

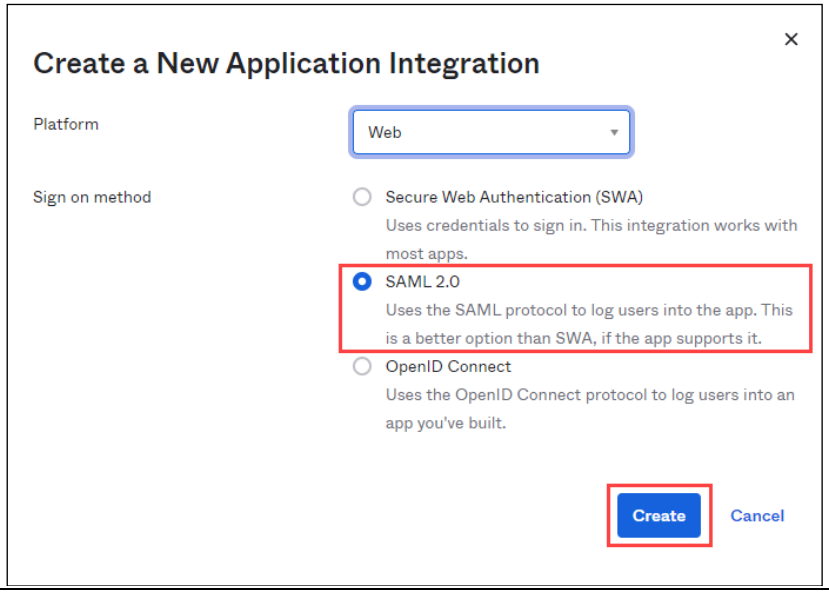
1. まず、Okta に管理者アカウントでログインして、以下の操作を行います。

2. 上部の **[Applications]** をクリックして、新しいアプリケーションの作成を開始します。ギャラリーにある既定の SAP Concur アプリケーションは誤ったエンドポイントをポイントする可能性があることから、既定の SAP Concur アプリケーションは Okta で使用しないでください。

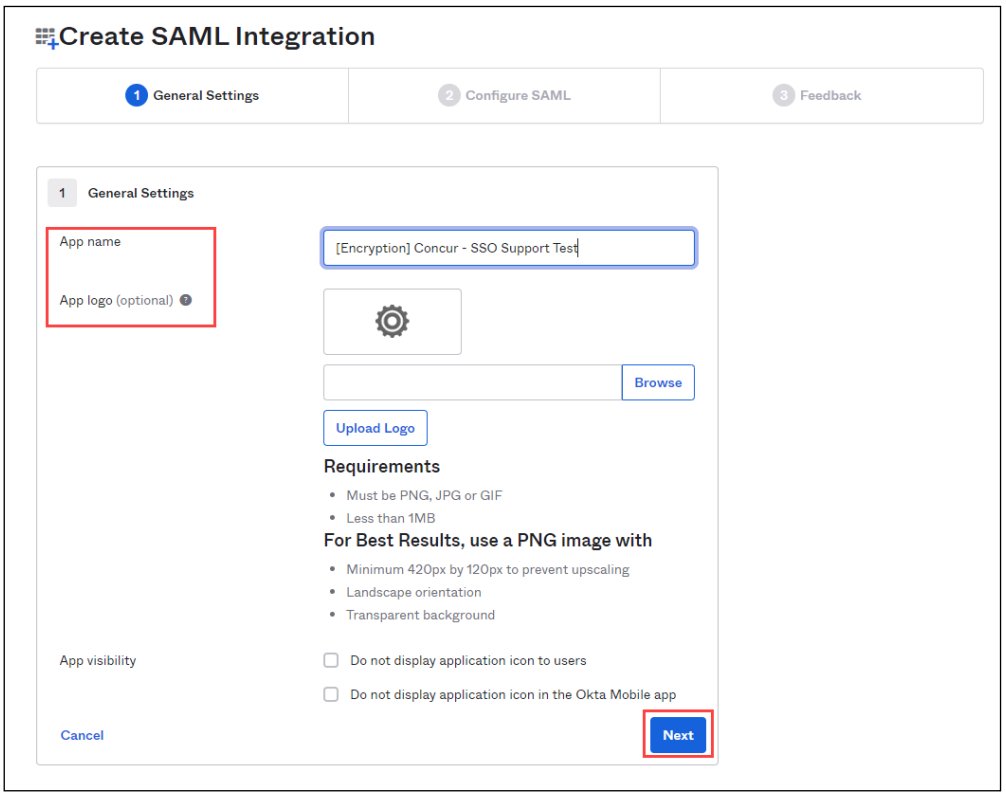


3. **[SAML 2.0]** を選択します。

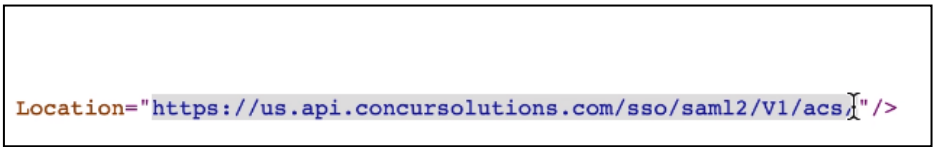
4. お気に入りの配賦の名前を入力して **[作成]** をクリックします。

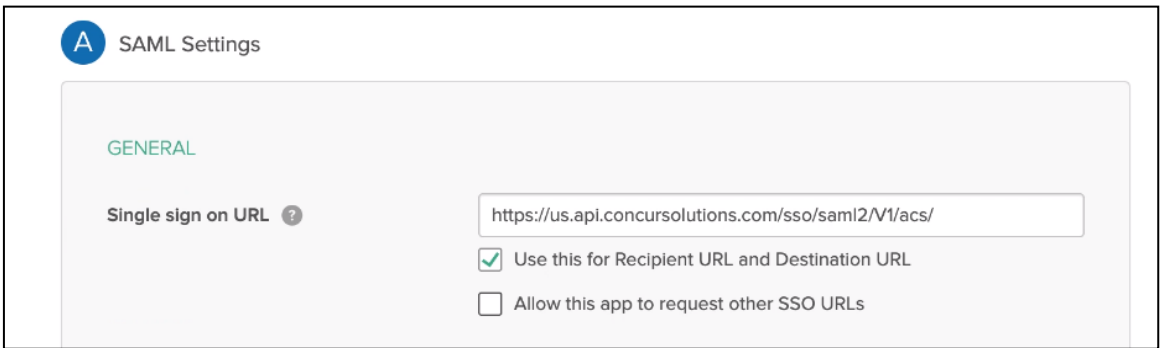


5. アプリ名を入力し、ロゴ（任意）を選択してから、**[Next]** をクリックします。

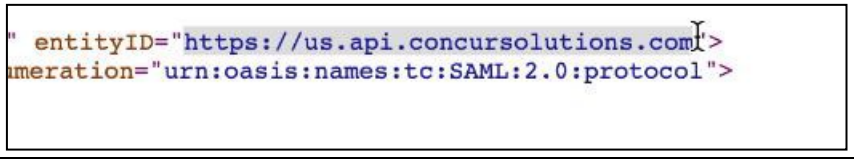


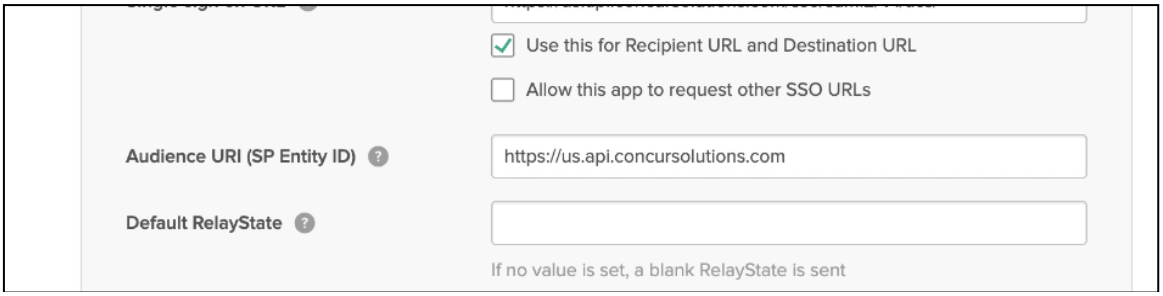
6. SAP Concur メタデータを開き、スクロール ダウンして「**Location=**」を探します。その URL 値をコピーして Okta アプリケーションの **[Single sign on URL]** フィールドに貼り付けます。





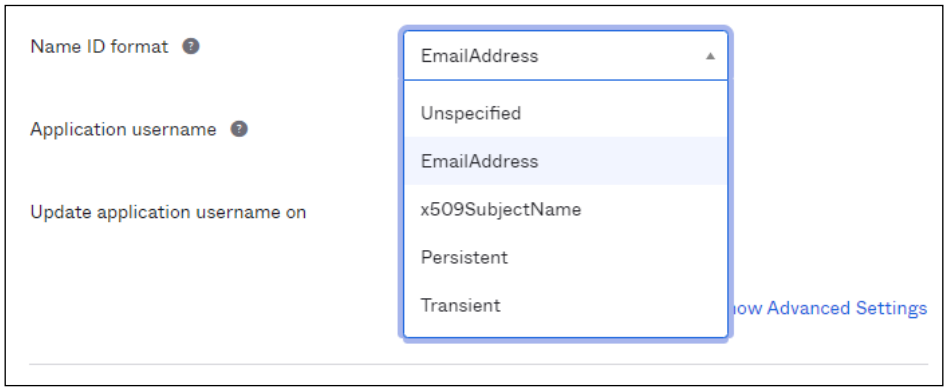
7. SAP Concur メタデータに戻り、上部で「**entityID=**」を探します。その URL をコピーして、Okta アプリケーションの **[Audience URI]**（**SP Entity ID**）フィールドに貼り付けます。





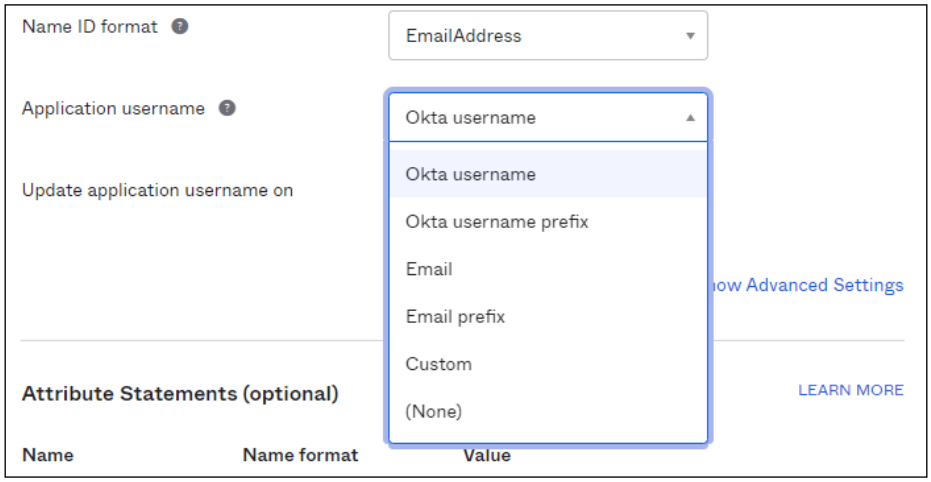
ステップ *3:* 名前 *ID* の構成

アプリケーションの設定時に、**名前 ID** を設定する必要があります。**名前 ID** は、SAP Concur で従業員に登録した**ログイン ID**（**CTE ログイン名**）と一致する必要があります。**[Name ID format]** を **[EmailAddress]** に設定することを強くお勧めします。



これは concursolutions.com またはモバイル アプリから開始する SP-Initiated ログインを行うために SAP Concur で必要になります。

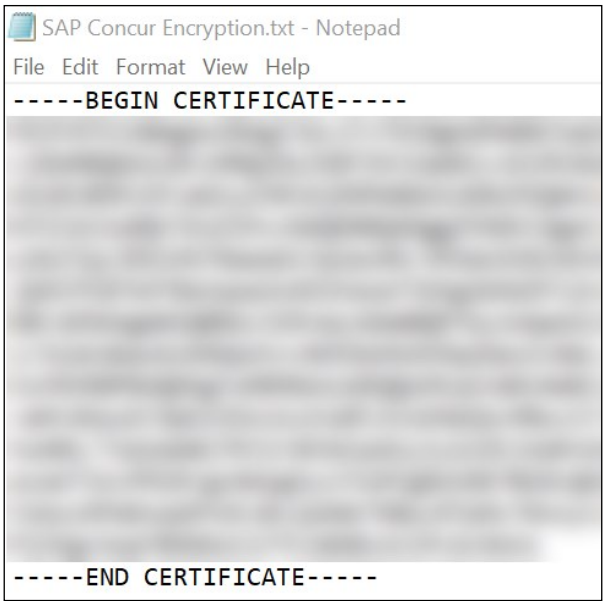
場合によっては、指定可能なアプリケーションのユーザー名は SAP Concur のユーザー名と一致しないことがあります。このような場合、SAP Concur で従業員インポートを実行し、ユーザー名が送信する属性と一致しているかどうかを確かめることができます。または、Okta の製品サポートに連絡し、名前 ID 設定のサポートを要請することができます。



SAML アサーションを暗号化する場合、ステップ 4 の説明に従ってください。不要な場合は、ステップ 5 に進みます。

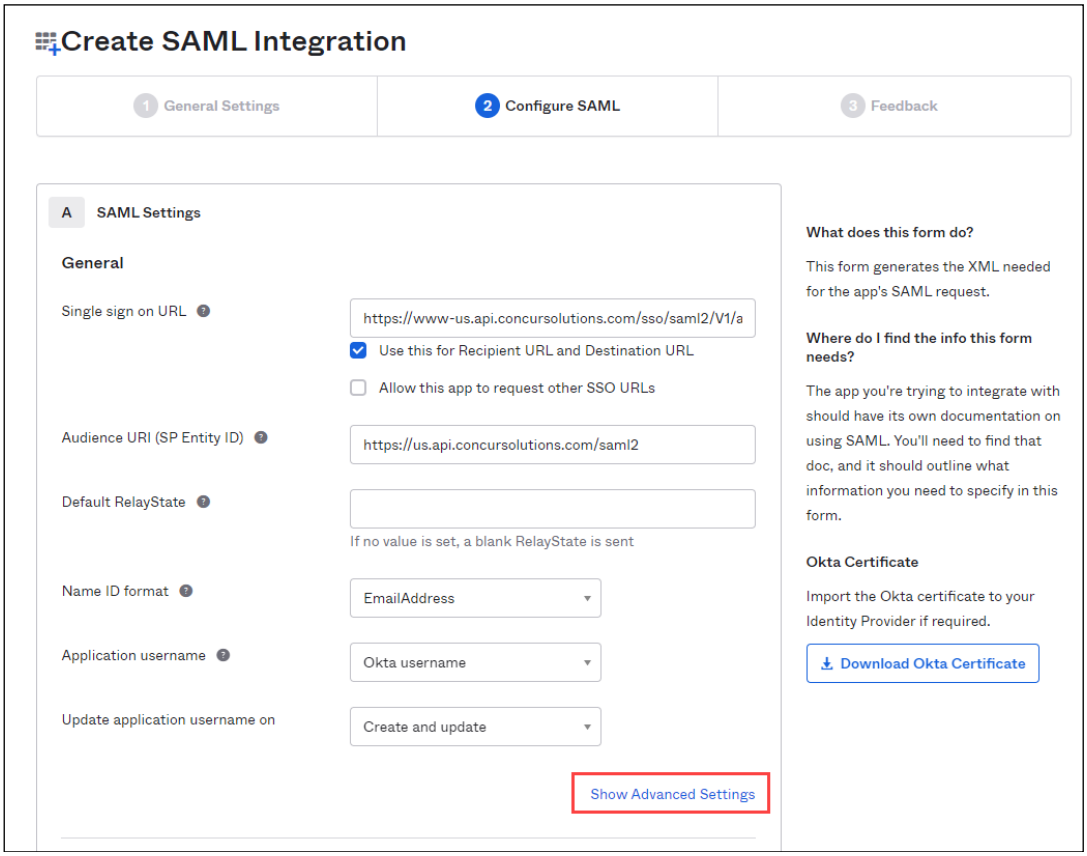
ステップ *4:*（オプション）アプリケーションを暗号化する

1. SAP Concur メタデータに戻り、スクロール ダウンして「**use="Encryption"**」タグを探します。X509 証明書をコピーして、テキスト ファイル（例: メモ帳）に貼り付けます。貼り付ける位置は、以下に示すように BEGIN CERTIFICATE 行と END CERTIFICATE 行の間です。

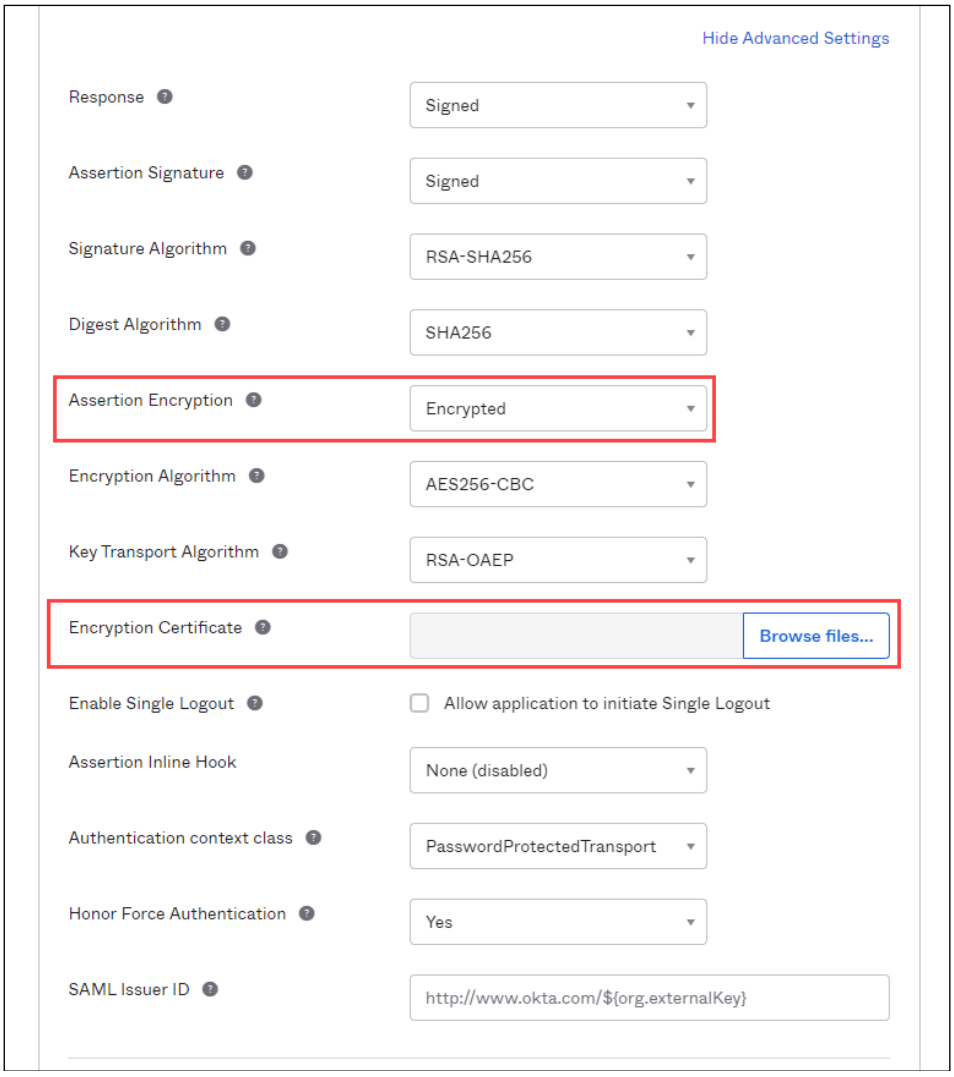


2. このファイルを .crt 形式で保存します。

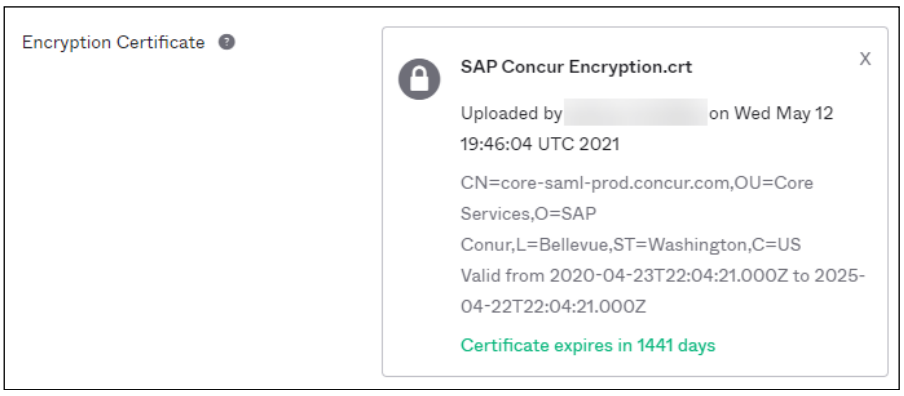
3. Okta アプリケーションで、ハイパーリンクの **[Show Advanced Settings]** をクリックします。



4. **[Assertion Encryption]** を **[Encrypted]** に変更し、保存した暗号化証明書を探します。



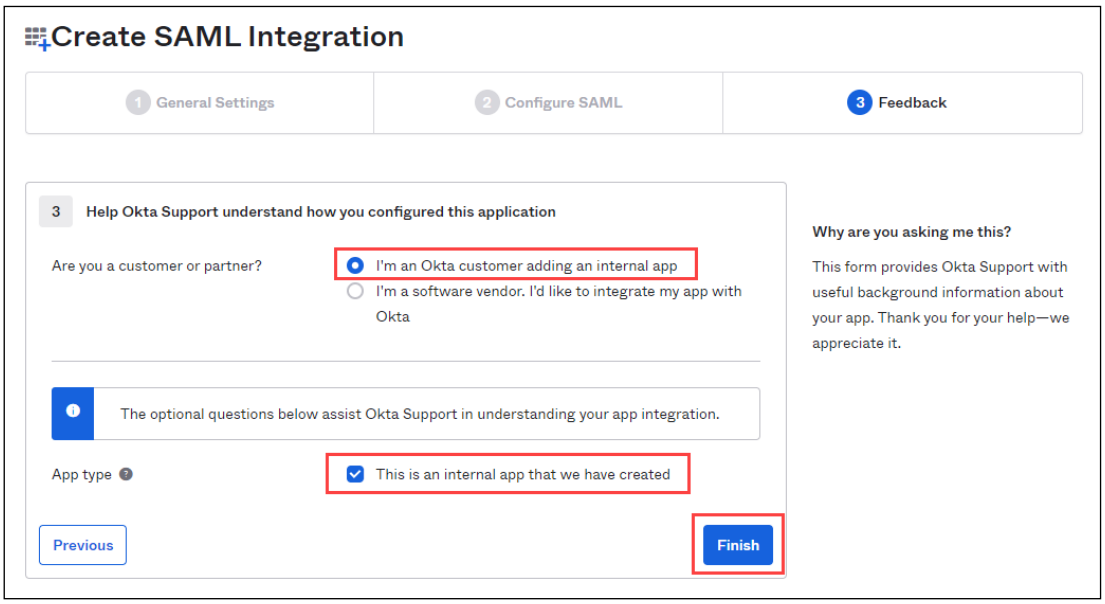
5. このファイルがアップロードされると、**[Encryption Certificate]** に次の情報が表示されます。



ステップ *5:* 設定の完了

1. Help Okta Support の [Feedback] セクションで、**[I'm an Okta customer adding an internal app]** を選択します。

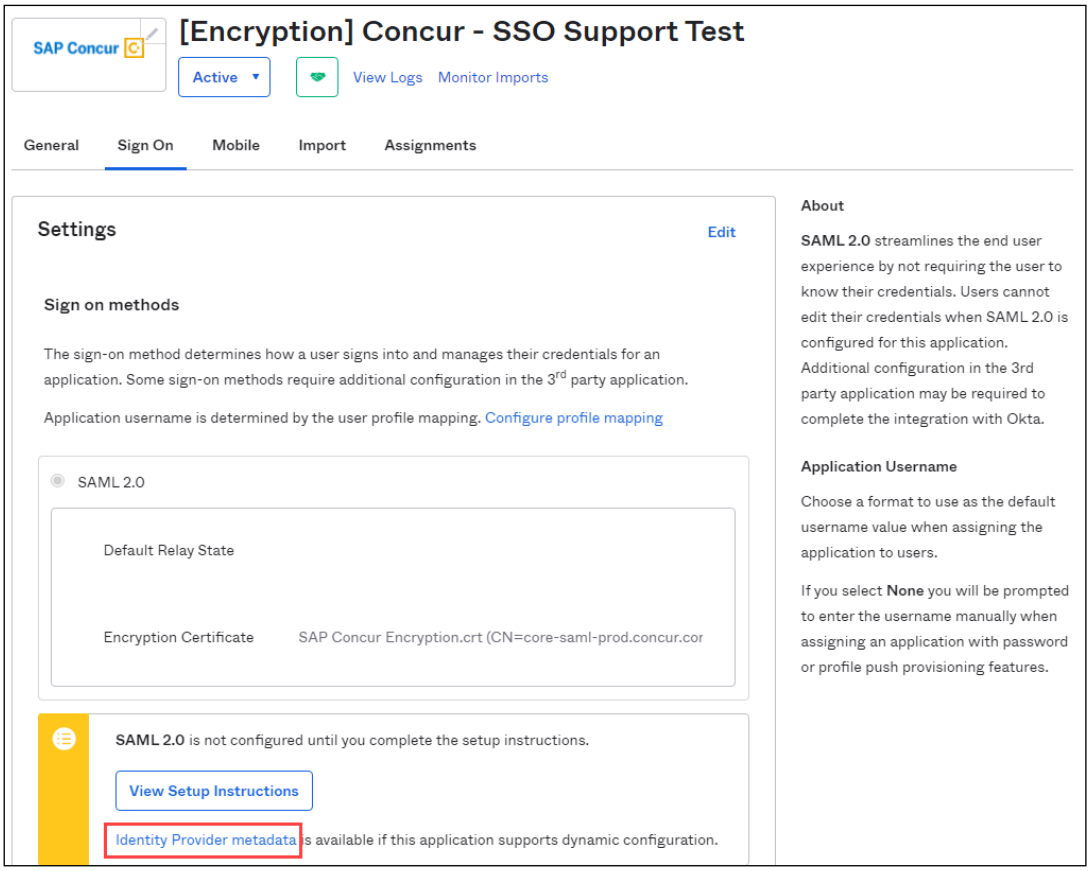
2. ページの一番下までスクロールして、**[完了]** をクリックします。



ステップ *6:* メタデータ ファイルをダウンロードする

SAP Concur 側で設定を完了するには、Okta のアプリケーションから抽出したメタデータ ファイルをアップロードします。

1. **[Sign On]** 設定ページで、**[View Setup Instructions]** のそばにある「Identity Provider metadata」をクリックします。

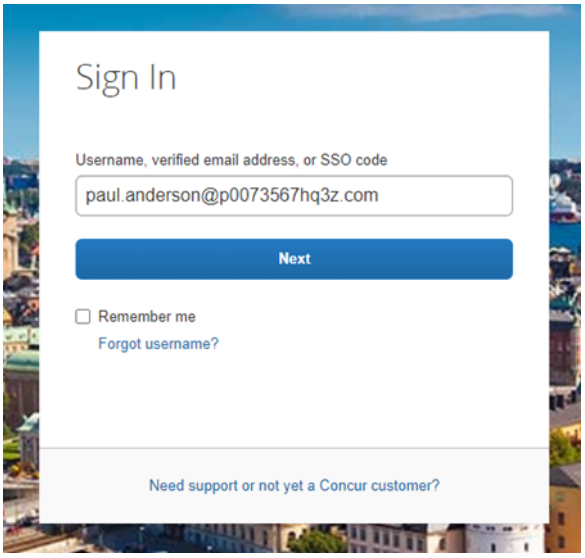


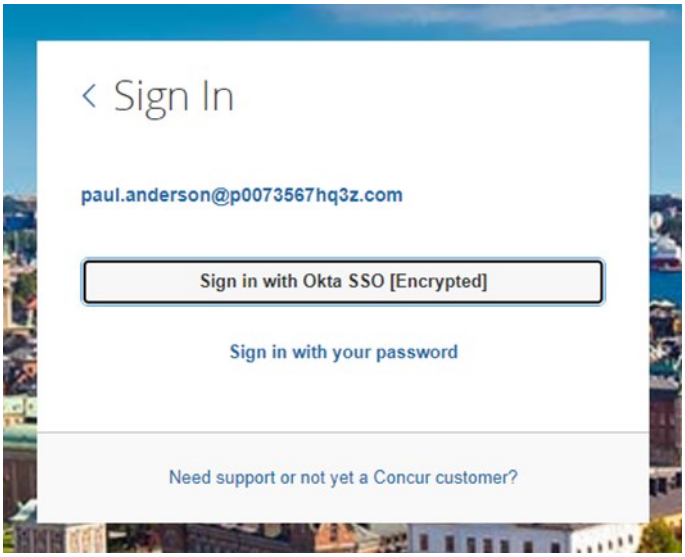
2. もしブラウザが メタデータ xml を自動的にダウンロードしない場合は、メタデータを含むタブを右クリックし .xml ファイルとして保存してください。

SAP Concur サイトを設定する

1. 「概要」セクションに記載されたステップに従って **[SSO の管理]** ページに移動します。
2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。
3. **[IdP 接続]** に適切な名前を入力し、その名前を **[カスタム IdP 名]** フィールドに入力します。

NOTE: SP-initiated フローを使用することにした場合（SAP Concur 公式サイト: https://www.concursolutions.com/nui/signin を利用）、ユーザー名を入力し **[次へ]** をクリックすると、 **[サインイン]** ページに **[カスタム IdP 名]** が表示されます。たとえば、**カスタム IdP 名**が「Okta SSO [Encrypted]」の場合、すべてのユーザーに [Okta SSO [Encrypted] でサインイン] オプションが表示されます。



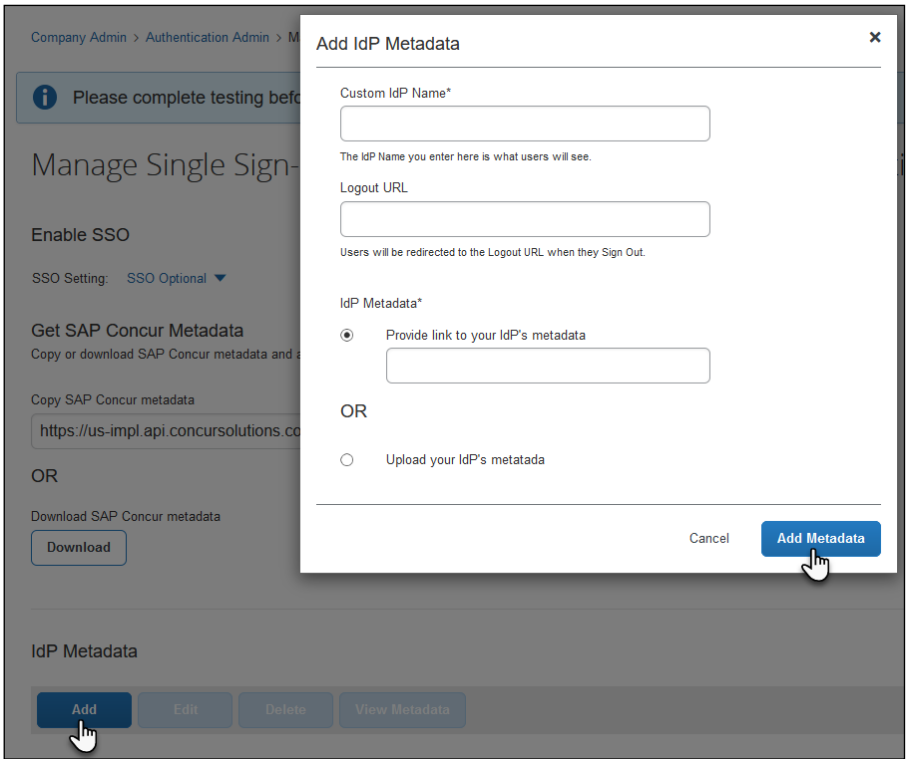


4. ユーザーがログアウトした際にほかの場所にリダイレクトされるようにログアウト URL（オプション）を入力します。既定では、URL が入力されない場合、ユーザーは認証プロセスを開始した場所にリダイレクトされます。Okta のログアウト エンドポイントは **[Local Provider] > [Identity Provider Settings] > [Single Log-Out Service (SLO)] > [Endpoint URL]** で確認できます。

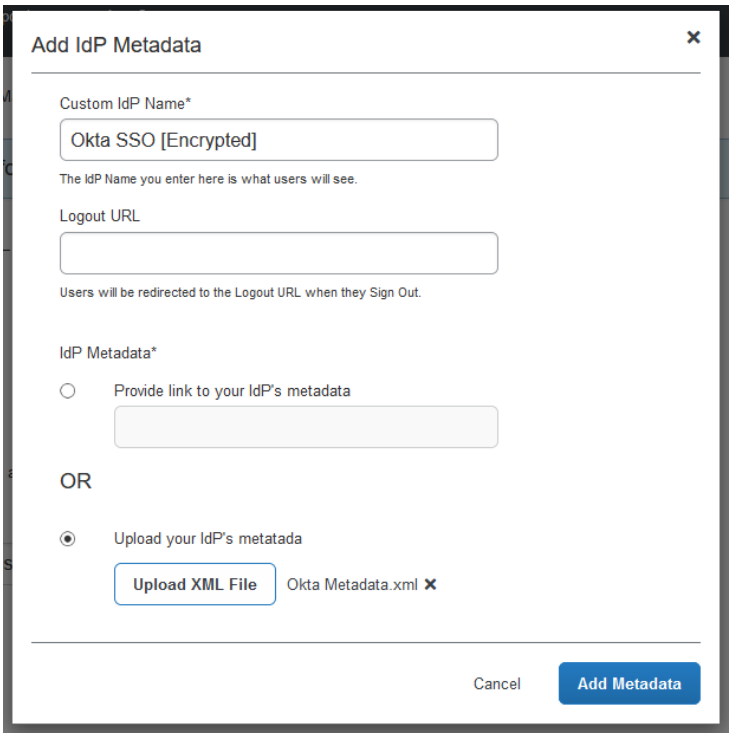
NOTE: Single Logout (SLO) は SAP Concur で正式にサポートされていないため、SAP Concur に加えて IDP からユーザーを切断することに関しては、SLO エンドポイントを使用するログアウト プロセスは期待どおりに動作しない可能性があります。そのような場合、ユーザーは SAP Concur からログアウトされますが、Okta からは完全にログアウトされないことがあります。

---

5. **[IdP Metadata]** で、IdP メタデータのリンクを入力するか、事前にローカルに保存した、IdP メタデータを含む XML ファイルをアップロードできます。

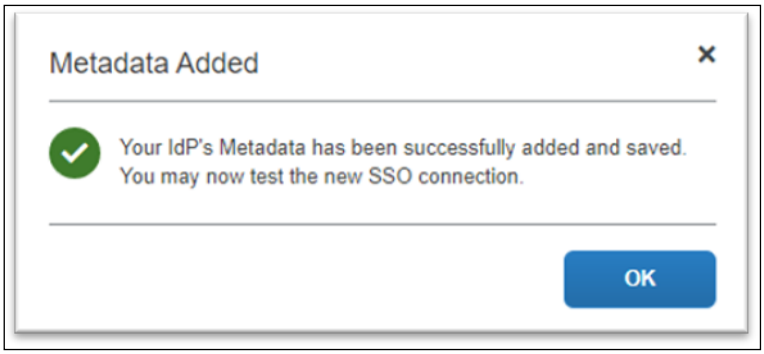


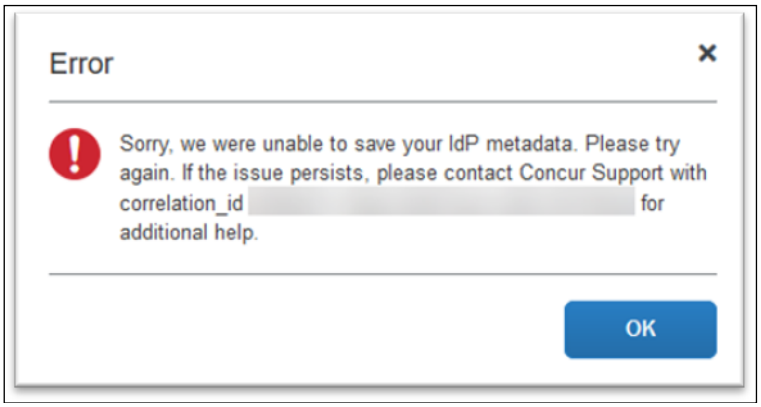
すべての詳細を入力すると、次のように表示されます。



6. **[メタデータの追加]** をクリックします。

7. 追加の成功を示す確認メッセージまたは問題の発生を示すメッセージが表示されます。後者の場合、SAP Concur サポートに連絡し、相関 ID を提供してください。





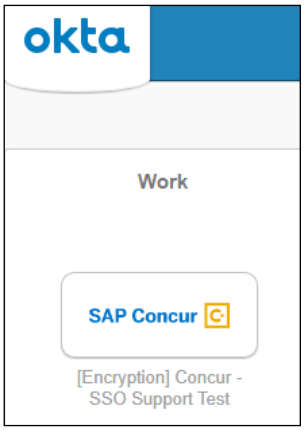
SSO ログインをテストする

前述のステップで IdP メタデータが SAP Concur に正常にアップロードされると、SSO のテストを開始できます。このセクションでは、IdP-Initiated（アイデンティティ プロバイダ側で開始される）フローおよび SP-Initiated（サービス プロバイダ側で開始される）フローをテストすることができます。

IdP-initiated SSO をテストする

IdP-initiated SSO をテストするには:

1. IdP-Initiated フローで、アイデンティティ プロバイダ側でログイン プロセスを開始します。テストを行うには、Okta アカウントにログインしてアプリケーションに移動し、先ほど設定した新しい SAP Concur アプリを参照するタイルを検索します。そのタイルをクリックし、SAP Concur プロファイルに直接リダイレクトされるかどうかを確認します。



また、アプリケーションの **[SSO]** タブに移動して、**[Embedded URL]** フィールドでテストすることもできます。この URL は次のように表示されます。

https://companydomain.okta.com/home/concur/xxxxxxxxxx/xxx.

SP-Initiated SSO をテストする

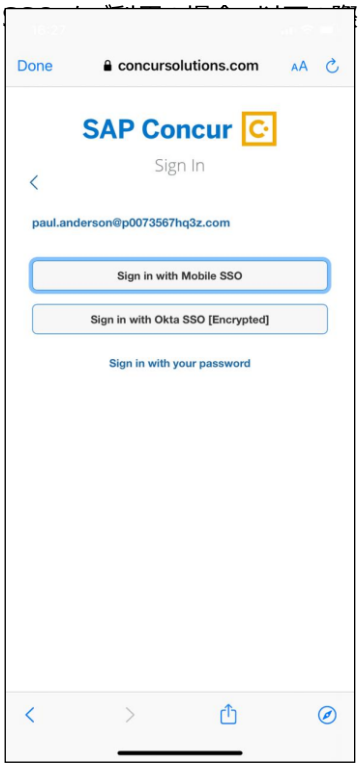
SP-Initiated SSO をテストするには

1. テストを行いたい環境のログイン ページを開きます。
   - US DC Prod: https://www.concursolutions.com/
   - US DC Test: https://implementation.concursolutions.com/
   - EMEA DC Prod: https://eu1.concursolutions.com/
   - EMEA DC Test: https://eu1imp.concursolutions.com/
   - CN DC Prod: https://www.concurcdc.cn/
2. ログイン ページでユーザー名、照合済メール アドレス、または SSO コードを追加して続行できます。**[次へ]** をクリックすると、「SAP Concur サイトを設定する」の注記のとおり、最近作成した SSO 設定のオプションが表示されます。クリックして、SAP Concur にリダイレクトするアイデンティティ プロバイダ アカウントの認証を続行します。

モバイル シングル サインオン（SSO）

SAMLv2 プラットフォームで作成された SSO 設定の場合、モバイル SSO はメタデータが保存されるとすぐに自動的に有効にされます。ただし、このオプションが機能するには、SP-Initiated フローが機能している必要があります。これは、前述の「SSO ログインをテストする」セクションを使用して検証することができます。

NOTE: モバイル SSO の自動有効化は、アプリのバージョンが 9.86 以降であり、かつ、ユーザーが新しいサインイン操作を選択している場合のみ表示されます。このオプションは旧バージョンのユーザー、または以前のサインイン操作を選択しているユーザーには自動的に非表示になります。もし以前に他の IdP をお使いで既にモバイル [illegible] 2 つのオプションが表示される可能性があります。



[モバイル SSO でサインイン] オプションにより以前の IdP リンクが埋め込まれるため、ユーザーは以前の SSO 接続にリダイレクトされます。

いずれの場合も、SAP Concur サポート チームにチケットを作成し、次の情報を提供してください。

- ユーザーが以前のバージョンを使用する予定の場合、当該アプリ バージョンにモバイル SSO を有効化できるように、Okta 側で作成したアプリケーションの IdP-Initiated URL を SAP Concur サポートに提供してください。URL の入手方法に関する詳細については、このガイドの「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。
- 混乱する可能性を排除するために **[モバイル SSO でサインイン]** オプションを削除する場合、サポート チームにご連絡ください。

モバイル アプリで SSO を使用する認証時に問題がある場合、SAP Concur サポート チームにチケットを作成し、表示されたエラー ID やメッセージをスクリーンショットと一緒に提供してください。

メール通知

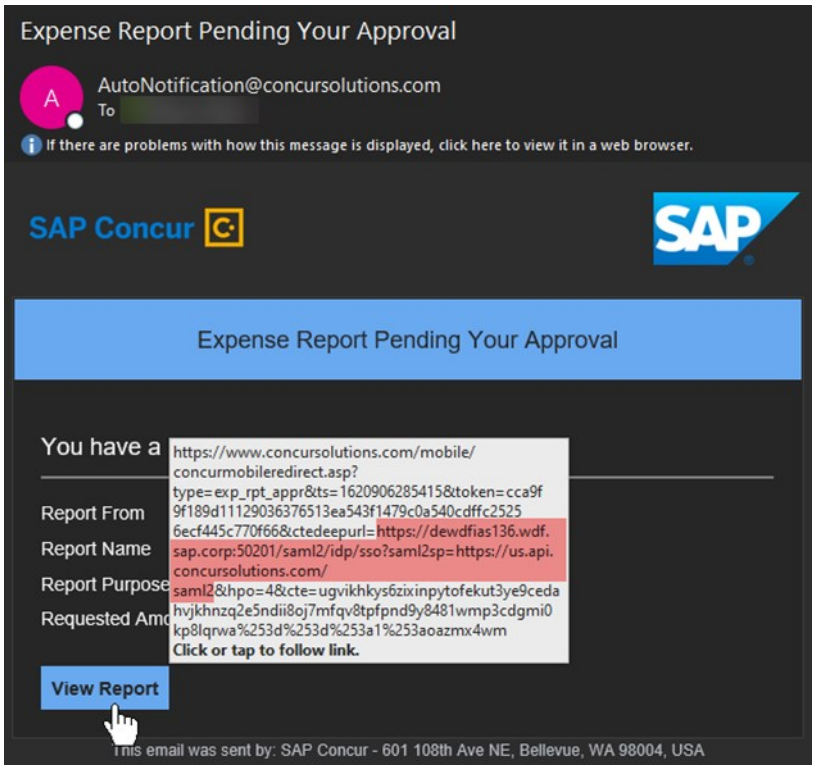
備忘メールに SSO URL を反映する設定は、SAP Concur サポートで完了される必要のある変更です。設定を進めるには、SAP Concur サポート チームのチケットを発行し、サポート チームが備忘メールのリダイレクト URL を調整できるように、IDP 側で作成したアプリケーションの IDP URL を提供します。URL の入手方法に関する詳細については、この付録の「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。

NOTE: URL は **[レポートの表示]** ボタンに埋め込まれて表示されます。

NOTE: この変更は変更後に生成されたメールにのみ反映されます。変更前に生成されたすべてのメールは以前の URL を引き続き使用します。

NOTE: この変更は反映されるまで最大 4 時間程度かかります。

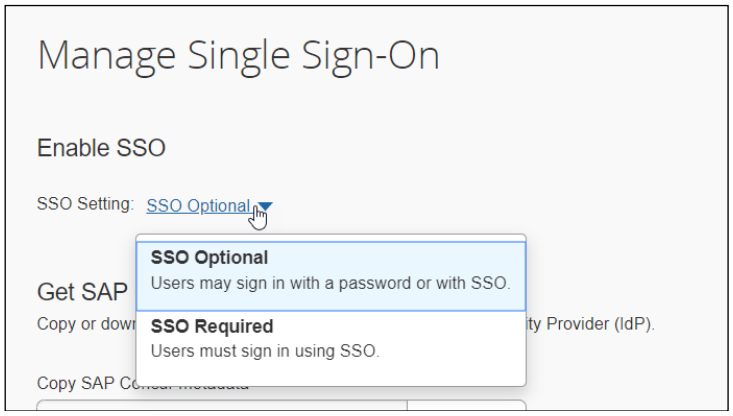
[レポートの表示] ボタンにカーソルを乗せると、現在挿入されている URL が表示されます。URL は **ctedeepurl=** と **&hpo=** の間に表示されます。



展開

新しい SSO 設定をテストしたら、このアクセスが必要なすべてのユーザーおよびグループに新しい Okta アプリケーションを割り当てることで、展開の計画を立てることができます。

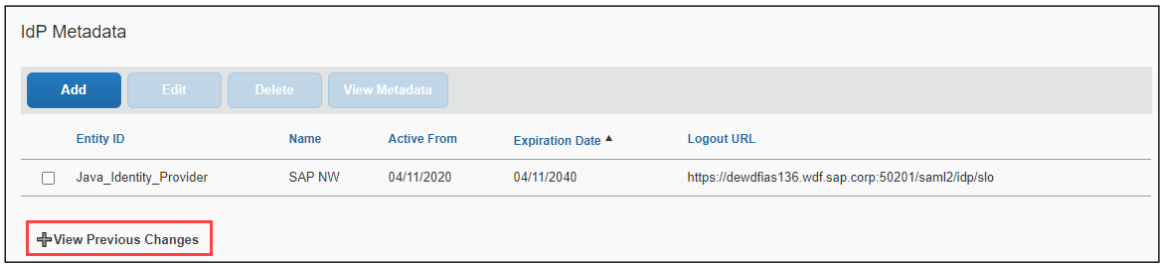
[SSO の管理] ページでは、SSO 設定を [SSO 任意] から **[SSO 必須]** に変更するとこの新しい SSO 接続を強制するオプションも提供しています。この設定を変更する場合、ユーザーは SP-initiated フローからユーザー名を提供すると SAP Concur にリダイレクトされるようになります。



以前の変更を表示

この機能は、**[SSO の管理]** ページで完了したすべての変更を管理者が追跡できるようにするために開発されました。

現時点までに行われた SSO 構成への変更を表示するには、**[以前の変更を表示]** をクリックします。

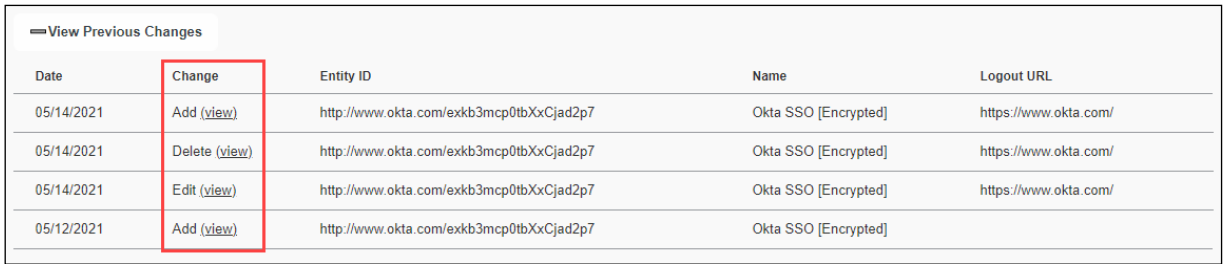


以前の変更が記載された表が表示され、日付と時刻の降順で並べ替えられています。

テーブルには、過去に行われた 100 件の変更が表示されます。テーブルにリストされる変更内容としては、以下のようなものが含まれます。

- 設定の追加
- 設定の削除
- [カスタム IdP 名] または [ログアウト URL] フィールドの編集

テーブルに一覧表示されている特定の変更に関する詳細情報を表示するには、目的のリスト項目の **[表示]** リンクをクリックします。



各ログの内部では、**[会社]** および **[変更者]** フィールドが [first_name last_name] [(UUID code)] 形式で表示されます。これは、そのアクションを行ったユーザーを参照しています。そのユーザーに見覚えがない場合、サポートに問い合わせて、詳細をリクエストすることができます。

セクション 11: 付録- PingOne の設定

NOTE: このセクションの説明はサード パーティー プロバイダから提供されているため、 SAP Concur はその正確性について保障することはできません。問題が発生した場合は、サード パーティー プロバイダのサポートにご連絡ください。

はじめに

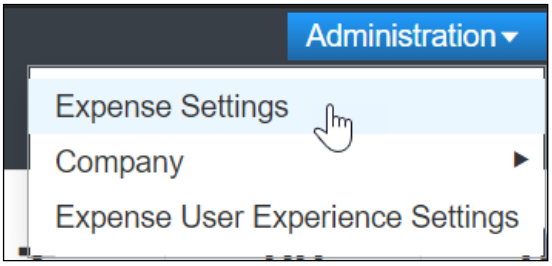
この付録では、PingOne で新しいアプリケーションを作成し、新しい SAMLv2 プラットフォームで SAP Concur サイトにこの新しい設定をアップロードする方法を示します。

設定プロセスを開始する前に、以下の点を確認します。

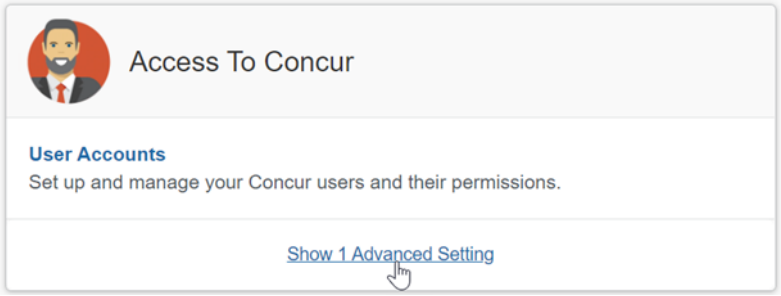
- PingOne と SAP Concur の両方にユーザーが存在している。
- PingOne から送信する属性が SAP Concur の各従業員の **[ログイン ID]**（**ユーザー名** / CTE ログイン名）フィールドと一致する。
- SAP Concur アカウントに割り当てられた組織管理者（**組織管理**、Travel のアクセス許可）を取得している。アクセス許可を取得したら、お使いの SAP Concur のエディションに応じて、次のいずれかのパスを使用して **[SSO の管理]** ページにアクセスできるようになります。

SAP Concur **Standard** Edition の場合:

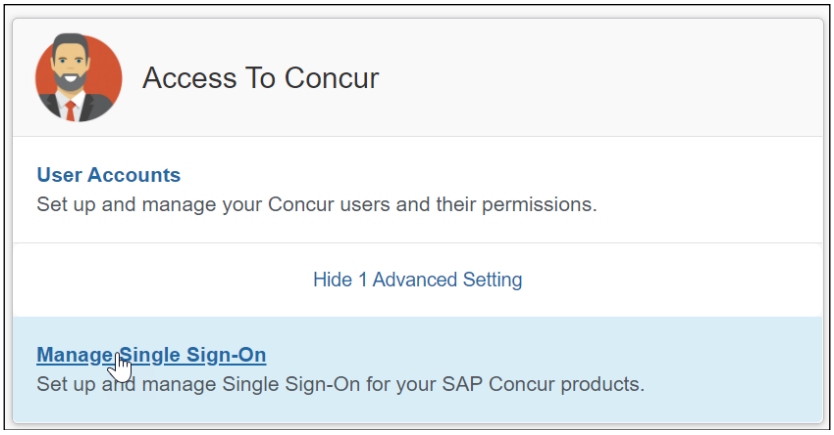
1. **[管理] > [経費の設定]** に移動します。



2. [Concur にアクセス] セクションの下にある **[1 つの詳細設定を表示]** をクリックします。

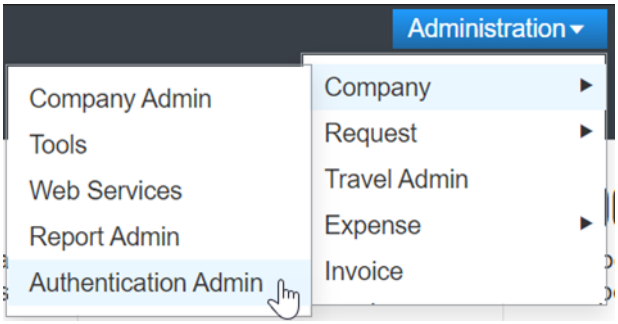


3. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。

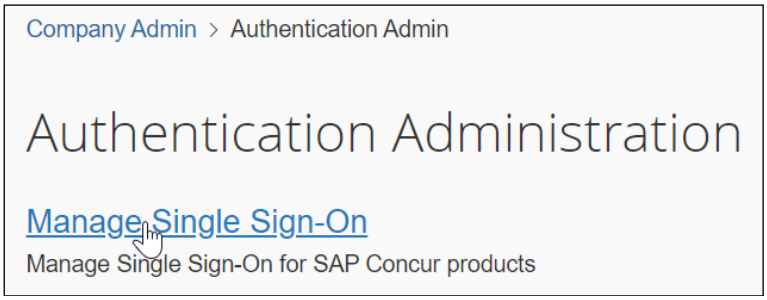


SAP Concur **Professional** Edition の場合:

1. **[管理]** > **[会社]** > **[認証管理]** に移動します。



2. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。



または、以下のいずれかの URL を使用して、ページにアクセスすることができます。

- US DC Prod: https://www.concursolutions.com/nui/authadmin/ssoadmin
- US DC Test: https://implementation.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Prod: https://eu1.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Test: https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin
- CN DC Prod: https://www.concurcdc.cn/nui/authadmin/ssoadmin

---

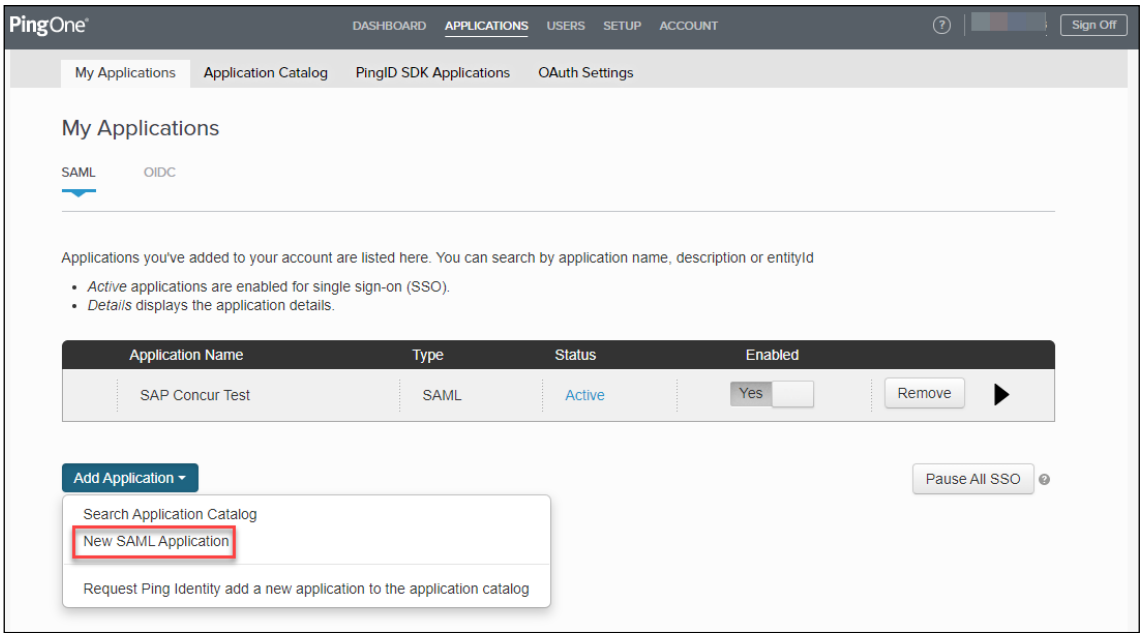
NOTE: アクセス許可を取得しておらず、自分のプロファイルに割り当てることもできない場合、会社のサポート問合せ権限の保持者に依頼し、SAP Concur サポートまでお問い合わせください。

PingOne アプリケーションを設定する

ステップ *1:* 非ギャラリー *SAML* アプリケーションを作成する

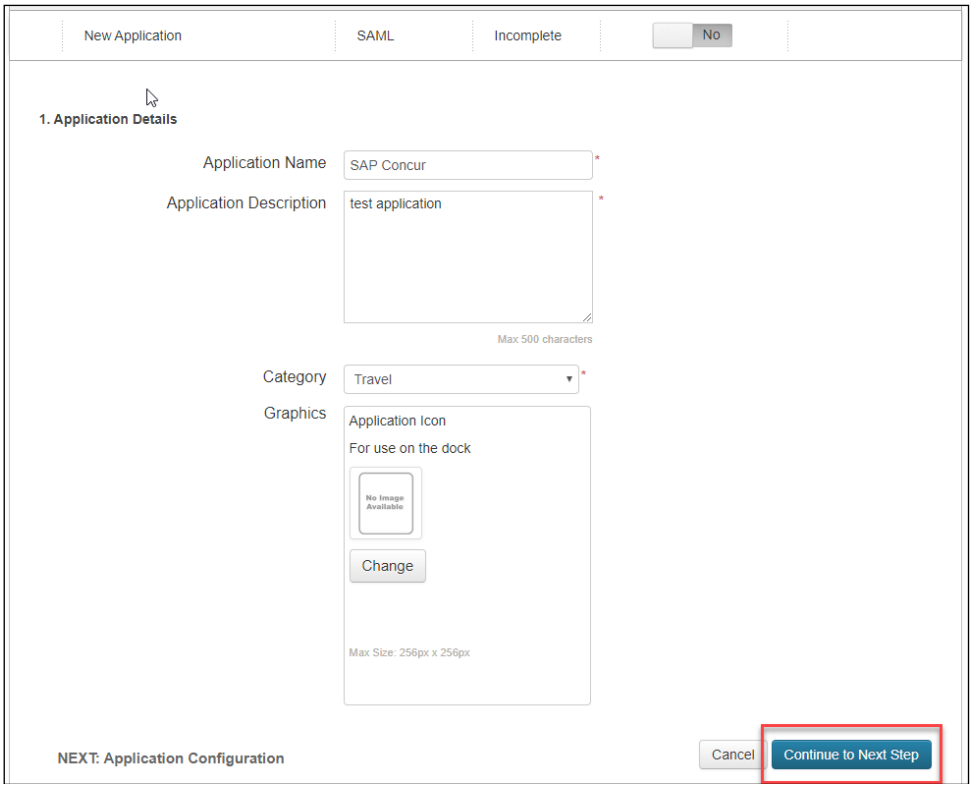
設定方法:

1. PingOne 管理者アカウントにログインし、**[Applications]** タブに移動します。
2. **[Add Application] > [New SAML Application]** をクリックします。



ステップ *2:* アプリケーションの詳細

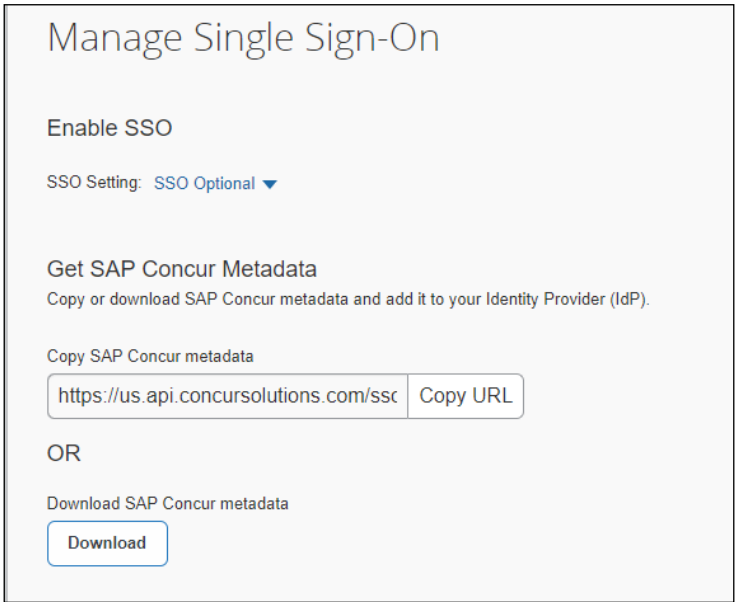
1. 必要に応じてアプリケーションの詳細を入力してから、**[Continue to Next Step]** をクリックします。



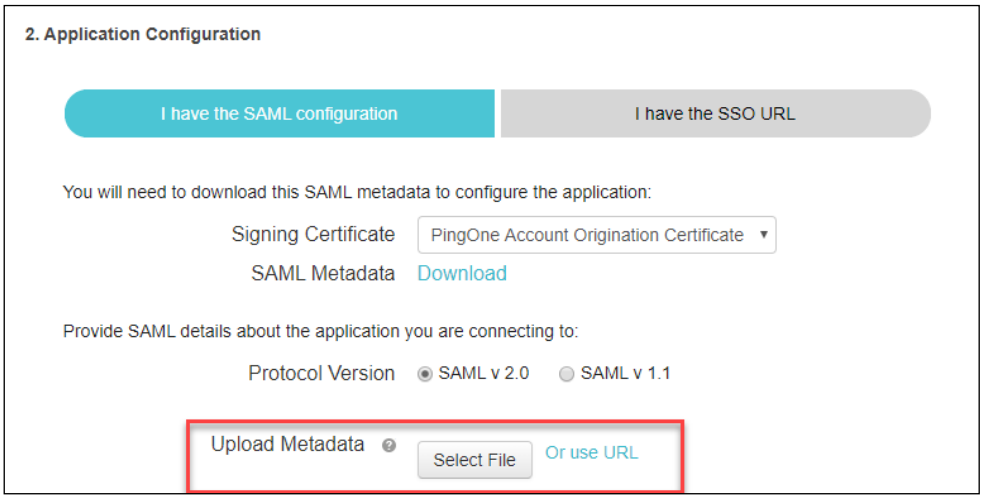
ステップ 3: アプリケーションの設定

このステップを完了するには、SAP Concur アカウントにログインし、「概要」のリンクを使用して **[SSO の管理]** セクションにアクセスします。

1. **[SSO の管理]** にアクセスした後は、メタデータの URL を入手するために **[URL コピー]** をクリックするか、メタデータの XML ファイルをダウンロードするために **[ダウンロード]** をクリックして、SAP Concur メタデータを入手することができます。

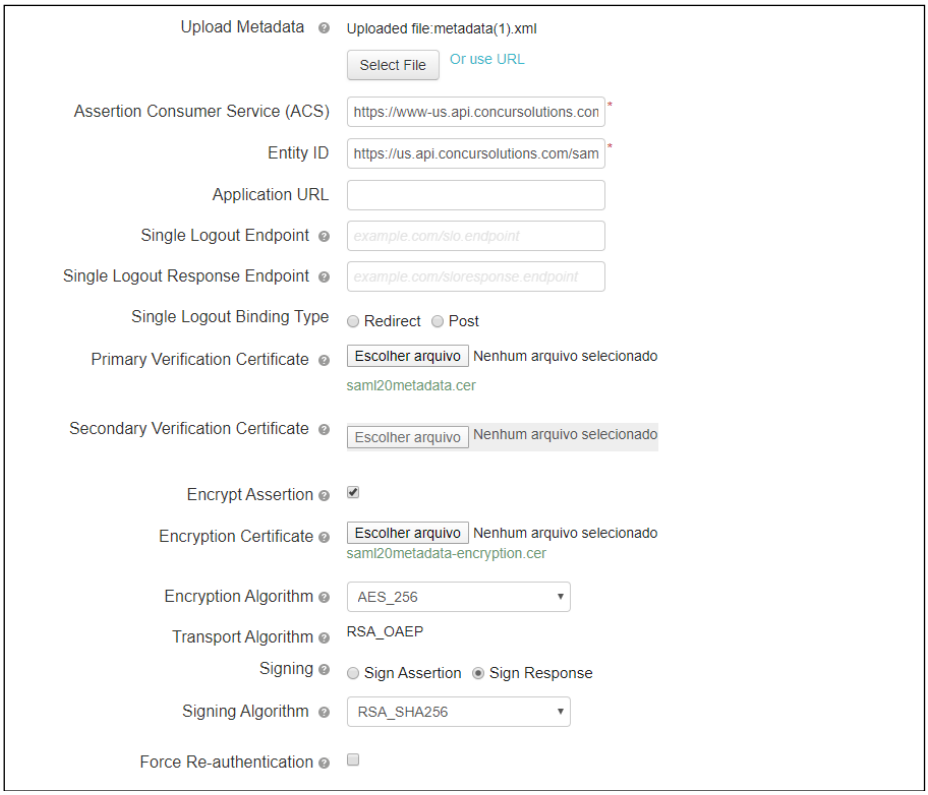


2. ブラウザを使用して、メタデータの URL または XML ファイルを開きます。PingOne はメタデータ ファイルのアップロードをサポートしているため、**[Upload Metadata]** に移動して xml ファイルを読み込むことができます。また、**[Or use URL]** をクリックして、メタデータ URL を追加することも可能です。



XML ファイルまたは URL からメタデータが読み込まれると、以下のフィールドは自動的に入力されます。

- Assertion Customer Service (ACS)
- エンティティ ID
- Primary Verification Certificate
- Encrypt Assertion checkbox
- Encryption Algorithm
- Encryption Certificate
- Transport Algorithm
- Signing（[Sign Assertion] から [Sign Response]）

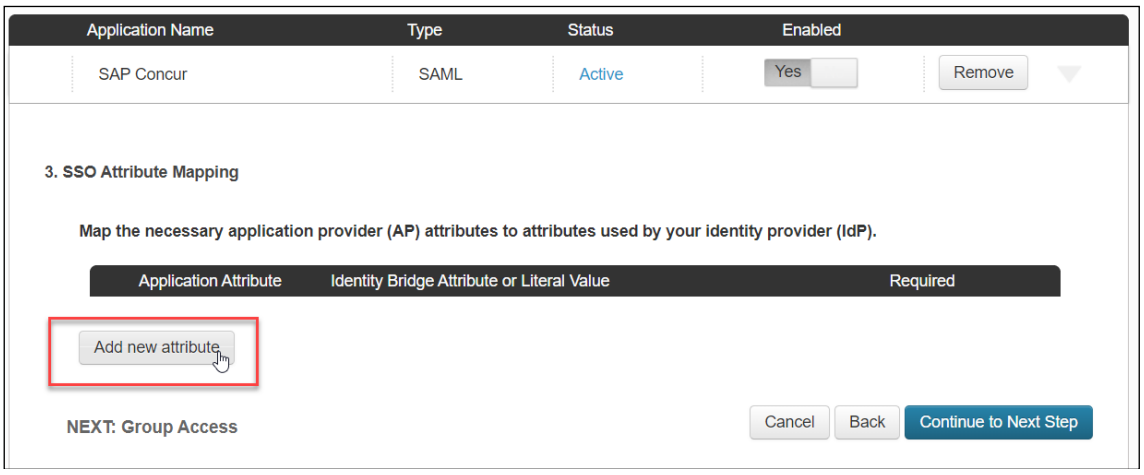


3. **[Encrypt Assertion]** の設定は任意です。トラブルシューティングの目的で SAML アサーションを追跡する場合、このチェックボックスの選択を解除してから、**[Continue to the Next Step]** をクリックします。

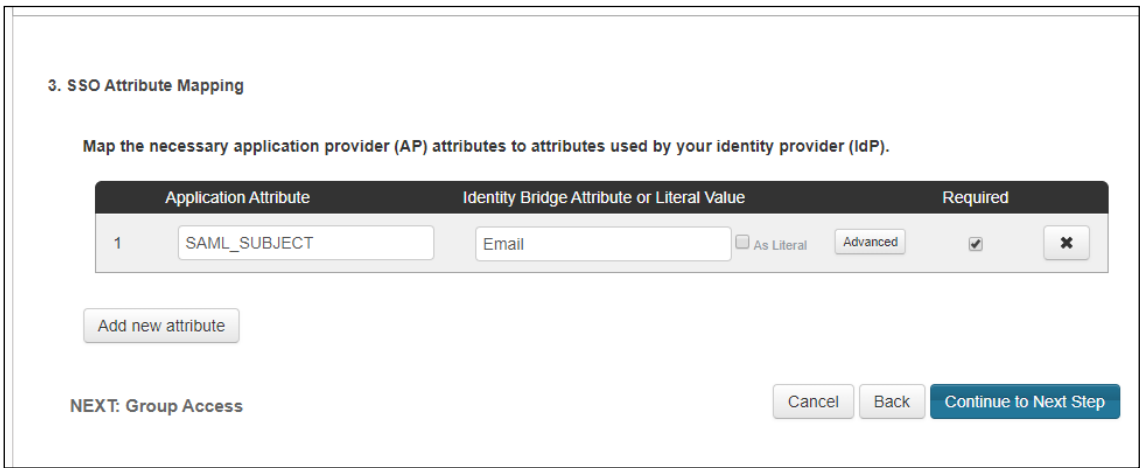
ステップ *4:* 属性マッピング

属性マッピングのセクションに移動したら、検証のために SAP Concur に送信される属性を構築する必要があります。この属性は SAP Concur の従業員の **[Login ID]** フィールドに一致しなくてはなりません。

1. 新しい属性を追加するには、**[Add new attribute]** をクリックします。



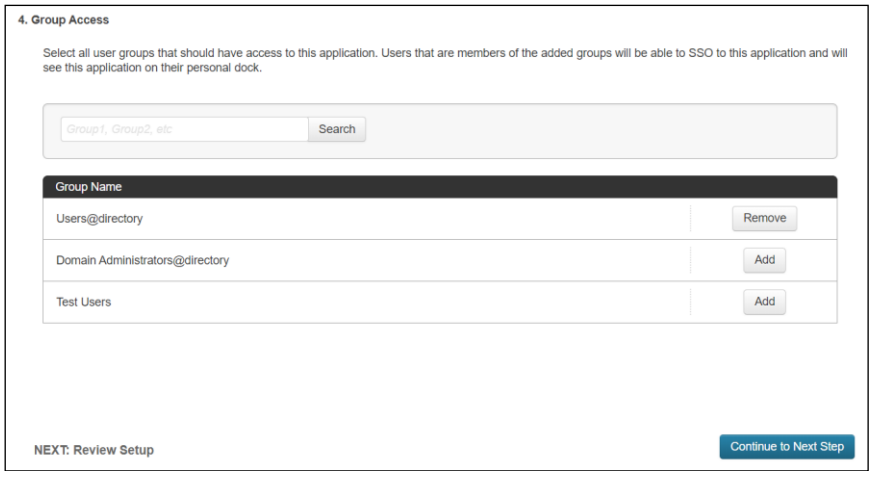
Ping のメール アドレスが SAP Concur の **[ログイン ID]** フィールドに一致すると、次のような属性を構築できます。



SAP Concur のログイン ID が異なる構造を備えている場合、**[SSO Attribute Mapping]** の **[Advanced settings]** を開き、カスタム属性を設定する必要があります。Ping コミュニティでこのカスタマイズに役立つ記事 （英語）を公開しています。

ステップ *5:* ユーザー グループにアクセスを付与する

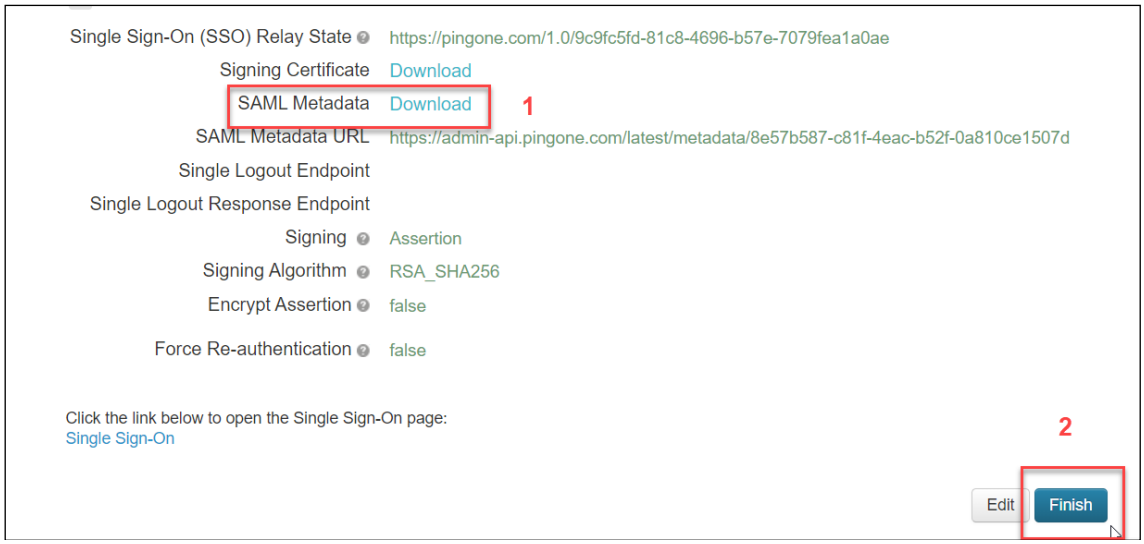
[Group Access] の画面が表示されます。このアプリケーションにユーザー グループを追加します。SAP Concur 従業員全員が含まれていることを確認し、**[Continue to Next Step]** をクリックします。



ステップ *6:* 見直しと完了

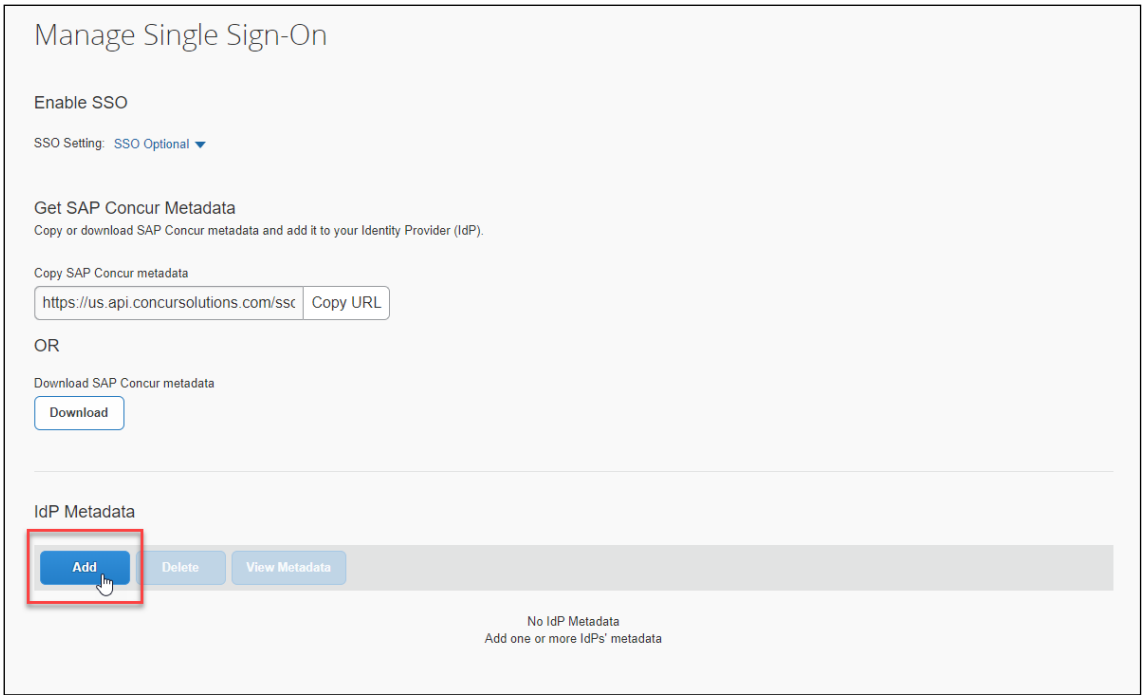
アプリケーションの設定を見直します。それから、後で SAP Concur にアップロードできるように、設定から SAML メタデータをダウンロードします。

[Finish] をクリックして、設定を完了します。

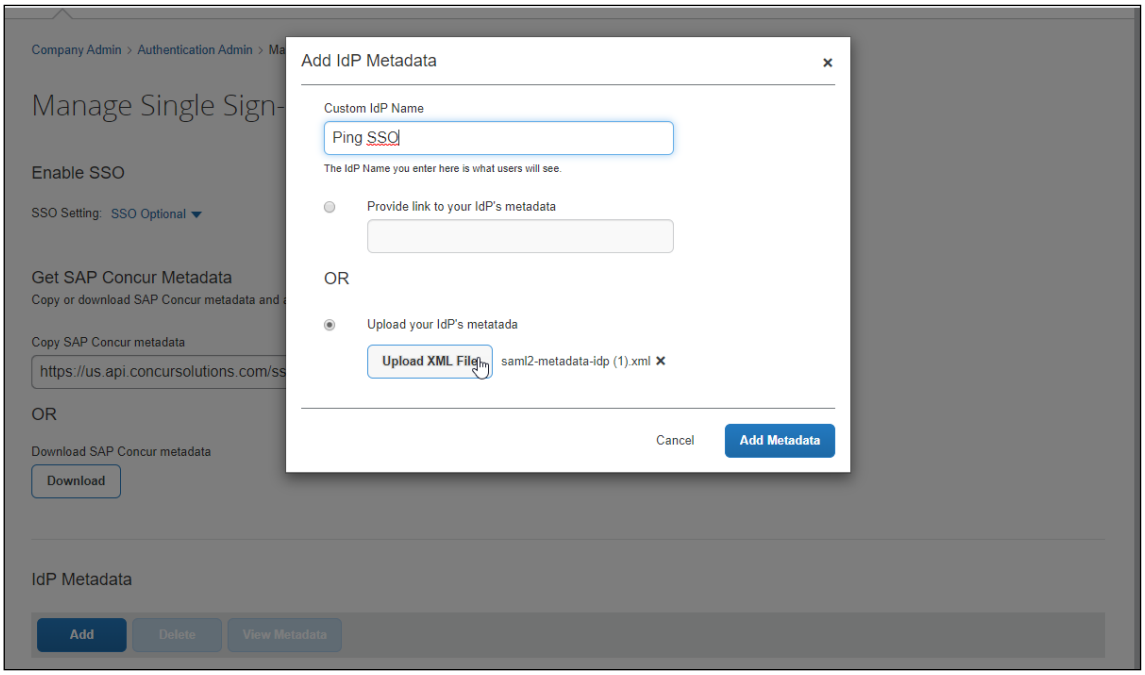


SAP Concur サイトを設定する

1. 「概要」セクションに記載されたステップに従って **[SSO の管理]** ページに移動します。
2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。



3. **[IdP 接続]** に適切な名前を入力し、その名前を **[カスタム IdP 名]** フィールドに入力します。



NOTE: SP-initiated SSO の場合、ユーザーがユーザー名を入力して **[次へ]** をクリックすると直ぐに **[カスタム IdP 名]** が **[サインイン]** ページに表示されます。

メタデータが正常に追加されると、新しい設定のテストを開始できます。

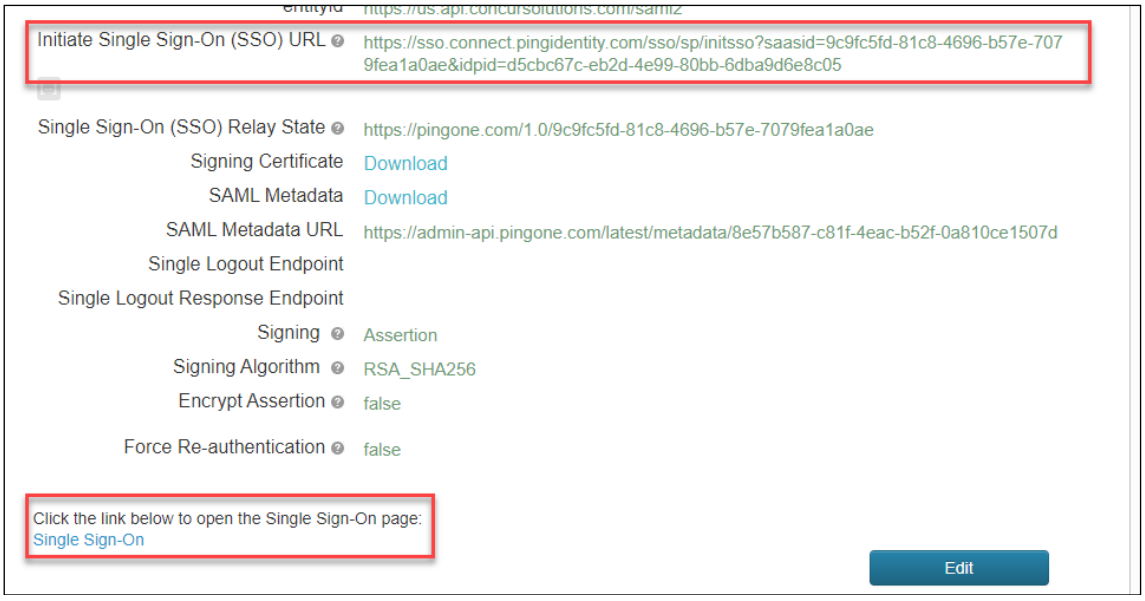
SSO ログインをテストする

前述のステップで IdP メタデータが SAP Concur に正常にアップロードされると、SSO のテストを開始できます。このセクションでは、IdP-Initiated（アイデンティティ プロバイダ側で開始される）フローおよび SP-Initiated（サービス プロバイダ側で開始される）フローをテストすることができます。

IdP-Initiated SSO のテスト

IdP-initiated SSO をテストするには:

1. 先ほど作成したアプリケーションを開きます。[Initiate Single Sign-On (SSO) URL] および **[Single Sign-On]** リンクは [Single Sign-On] ページを開きます。



SP-Initiated SSO のテスト

SP-Initiated SSO をテストするには

1. テストを行いたい環境のログイン ページを開きます。
   - US DC Prod: https://www.concursolutions.com/
   - US DC Test: https://implementation.concursolutions.com/
   - EMEA DC Prod: https://eu1.concursolutions.com/
   - EMEA DC Test: https://eu1imp.concursolutions.com/
   - CN DC Prod: https://www.concurcdc.cn/
2. ログイン ページでユーザー名、照合済メール アドレス、または SSO コードを追加して続行できます。**[次へ]** をクリックすると、最近作成した SSO 設定のオプションが表示されます。SSO 認証のオプションをクリックして、SAP Concur のプロファイルにリダイレクトする PingOne 資格情報の認証を続行します。

   PingOne 資格情報の追加後に PingOne エラー メッセージが表示された場合、設定が未完了になっているか、不足しているものがある可能性があります。IdP-Initiated ログインは機能していても、SP-Initiated が機能していない場合は、名前 ID の形式が問題となっている可能性が高くなります。名前 ID の形式が適切であることを確認するには、「PingOne アプリケーションを作成する」の属性マッピングの手順に記載されているように SAML_SUBJECT が **[Email]** に設定されているかどうかを確認してください。

モバイル シングル サインオン（SSO）

SAMLv2 プラットフォームで作成された SSO 設定の場合、モバイル SSO はメタデータが保存されるとすぐに自動的に有効にされます。ただし、このオプションが機能するには、SP-Initiated フローが機能している必要があります。これは、前述の「SSO ログインをテストする」セクションを使用して検証することができます。

NOTE: モバイル SSO の自動有効化は、アプリのバージョンが 9.86 以降であり、かつ、ユーザーが新しいサインイン操作を選択している場合のみ表示されます。このオプションは旧バージョンのユーザー、または以前のサインイン操作を選択しているユーザーには自動的に非表示になります。

モバイル アプリで SSO を使用する認証時に問題がある場合、SAP Concur サポート チームにチケットを作成し、表示されたエラー ID やメッセージをスクリーンショットと一緒に提供してください。

メール通知

備忘メールに SSO URL を反映する設定は、SAP Concur サポートで完了される必要のある変更です。設定を進めるには、SAP Concur サポート チームにチケットを作成し、サポート チームが備忘メールのリダイレクト URL を調整できるように、IDP 側で作成したアプリケーションの IDP URL を提供します。URL の入手方法に関する詳細については、この付録の「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。

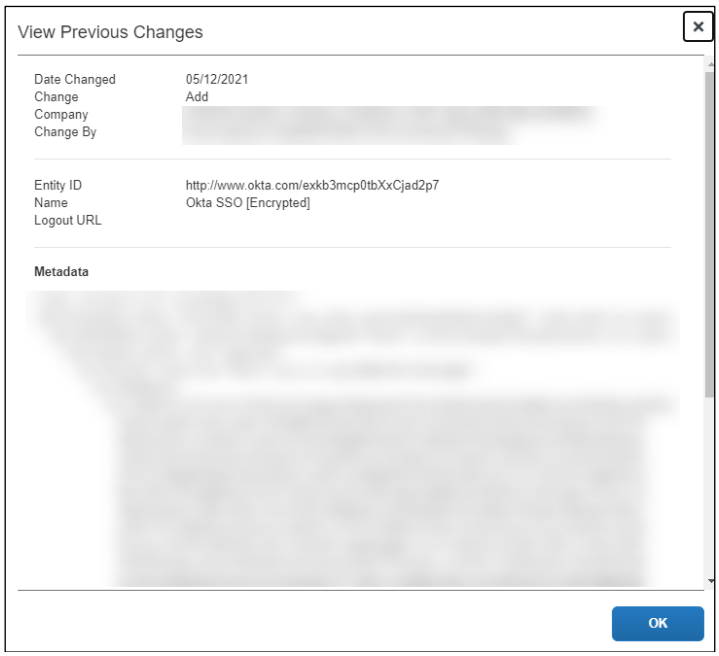
展開

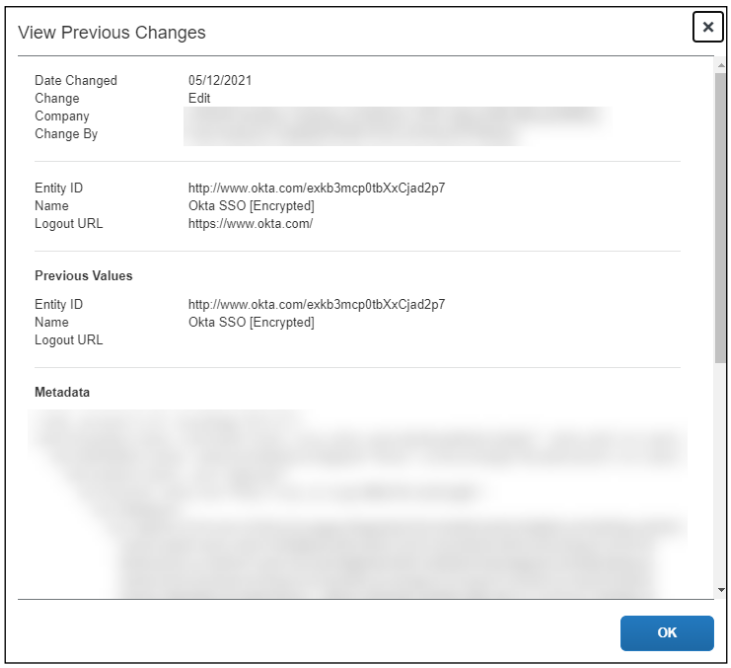
新しい SSO 設定をテストしたら、このアクセスが必要なすべてのユーザーおよびグループに新しいアプリケーションを割り当てることで、展開の計画を立てることができます。

[SSO の管理] ページでは、SSO 設定を [SSO 任意] から **[SSO 必須]** に変更するとこの新しい SSO 接続を強制するオプションも提供しています。この設定を変更する場合、ユーザーは SP-initiated フローからユーザー名を提供すると SAP Concur にリダイレクトされるようになります。

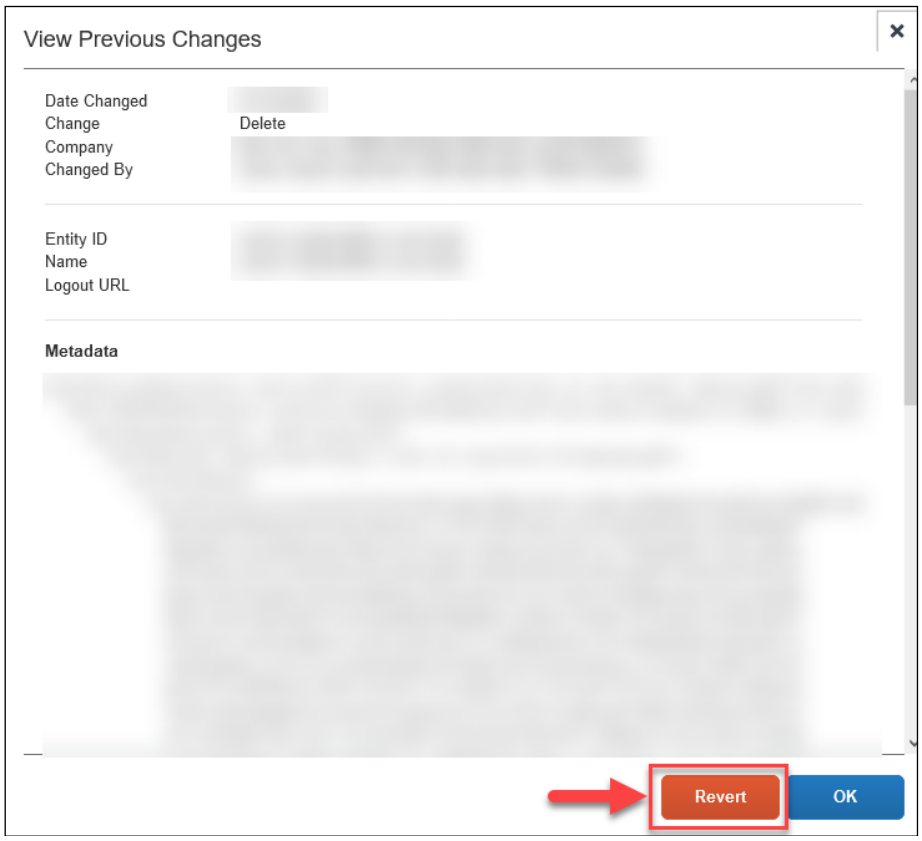
モバイル SSO のみを強制する必要がある場合は、SAP Concur サポートまでお問い合わせください。

ログの例:


View Previous Changes
Date Changed
05/12/2021
Change
Add
Company
Change By
Entity ID
http://www.okta.com/exkb3mcp0tbXxCjad2p7
Name
Okta SSO [Encrypted]
Logout URL
Metadata
OK


View Previous Changes
Date Changed
05/12/2021
Change
Edit
Company
Change By
Entity ID
http://www.okta.com/exkb3mcp0tbXxCjad2p7
Name
Okta SSO [Encrypted]
Logout URL
https://www.okta.com/
Previous Values
Entity ID
http://www.okta.com/exkb3mcp0tbXxCjad2p7
Name
Okta SSO [Encrypted]
Logout URL
Metadata
OK

設定が削除されている場合、この設定を復元するための **[元に戻す]** ボタンが **[変更履歴の表示]** ページに表示されます。設定が復元されると、この設定をサインイン プロセス中にユーザーが使用できるようになります。



📖 さらに詳しい情報は、次の文書をご参照ください。

- Okta - How to Configure SAML 2.0 for Concur Travel and Expense

セクション 12: 付録 - SAP Identity Authentication Service (IAS) 設定

はじめに

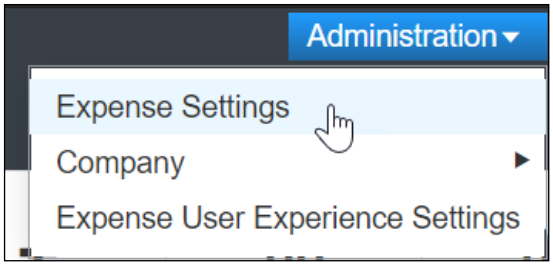
設定プロセスを開始する前に、以下の点を確認します。

- アイデンティティ プロバイダ (SAP IAS) の管理者アクセス権を取得している。これは SAP IAS 側でアプリケーションの設定を完了するために必要になります。
- SAP IAS と SAP Concur の両方にユーザーが存在している。SAP Concur は現在、自動ユーザー プロビジョニングをサポートしていないため、別途ユーザーを追加する必要があります。
- SAP IAS から送信する属性が SAP Concur の各従業員の **[ログイン ID]**（**ユーザー名 / CTE ログイン名**）フィールドと一致する。

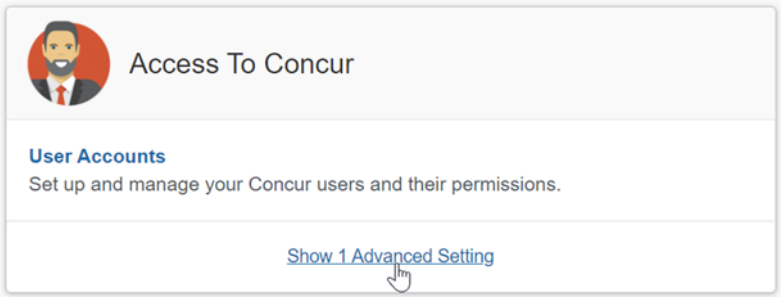
- SAP Concur アカウントに割り当てられた組織管理者（Travel のアクセス許可）を取得している。アクセス許可を取得したら、お使いの SAP Concur のエディションに応じて、次のいずれかのパスを使用して **[SSO の管理]** ページにアクセスできるようになります。

SAP Concur **Standard** Edition の場合:

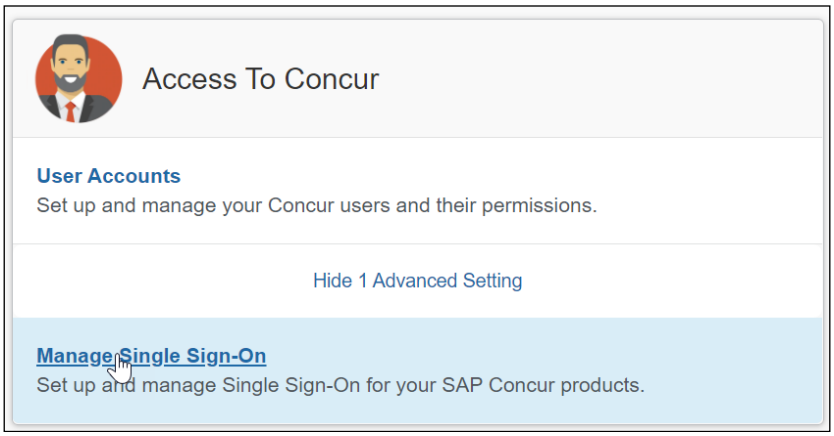
1. **[管理] > [経費の設定]** に移動します。



2. [Concur にアクセス] セクションの下にある **[1 つの詳細設定を表示]** をクリックします。

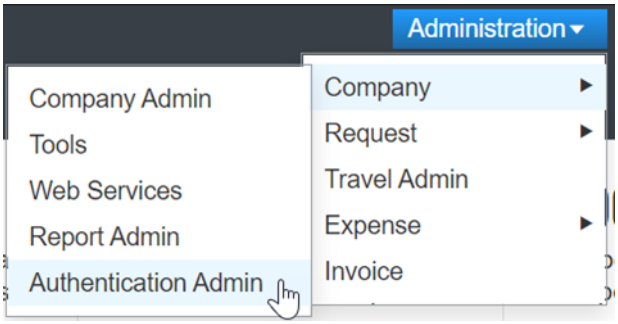


3. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。

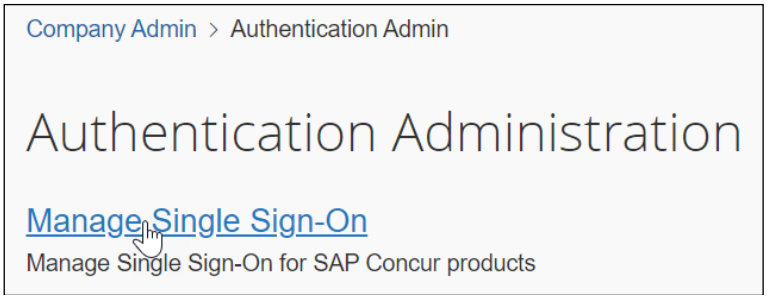


SAP Concur **Professional** Edition の場合:

1. **[管理]** > **[会社]** > **[認証管理]** に移動します。



2. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。



または、以下のいずれかの URL を使用して、ページにアクセスすることができます。

- US DC Prod: https://www.concursolutions.com/nui/authadmin/ssoadmin
- US DC Test: https://implementation.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Prod: https://eu1.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Test: https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin
- CN DC Prod: https://www.concurcdc.cn/nui/authadmin/ssoadmin

---

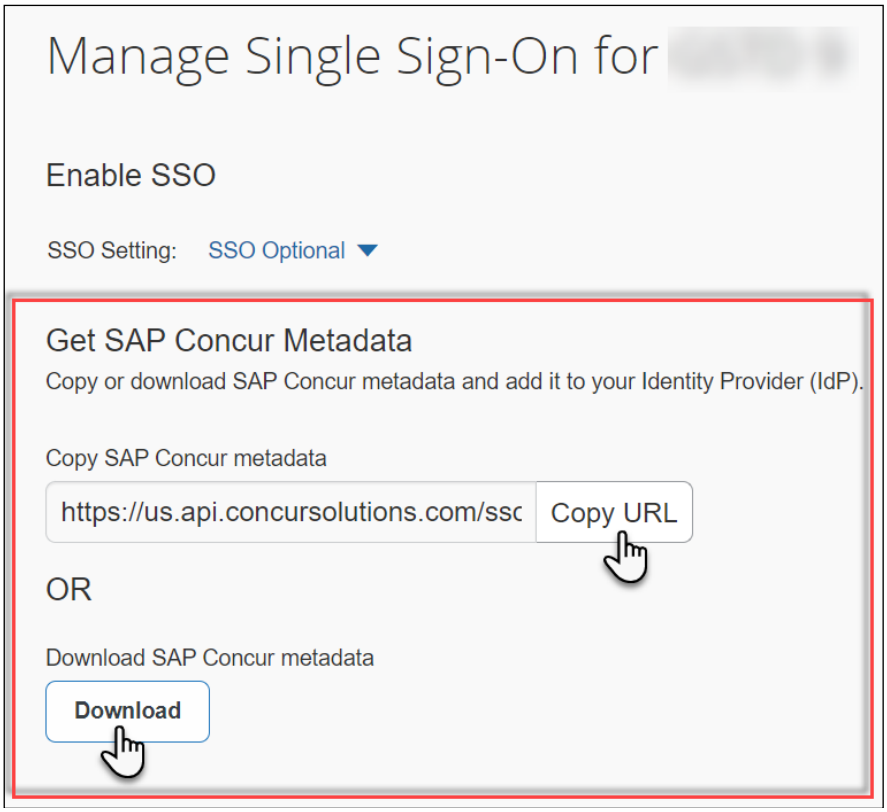
NOTE: アクセス許可を取得しておらず、自分のプロファイルに割り当てることもできない場合、会社のサポート問合せ権限の保持者に依頼し、SAP Concur サポートまでお問い合わせください。

SAP IAS アプリケーションを設定する

ステップ 1:SAP Concur メタデータを入手する

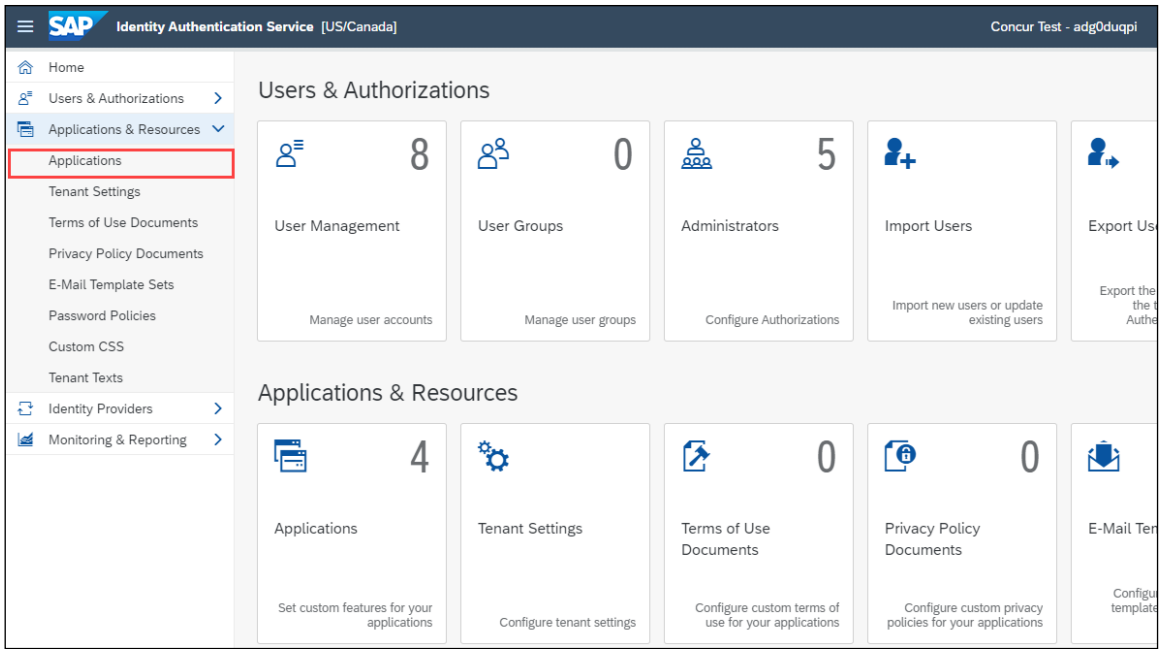
設定方法:

1. SAP Concur メタデータを入手します。これを完了するには、前述の「概要」セクションの説明に従って SAP Concur アカウントにログインし、**[SSO の管理]** セクションにアクセスします。[SSO の管理] ページで SAP Concur メタデータを取得するには、**[URL をコピー]** をクリックしてから新しいブラウザ タブにその URL をクリックするか、**[ダウンロード]** をクリックしてダウンロードしたファイルを開きます。

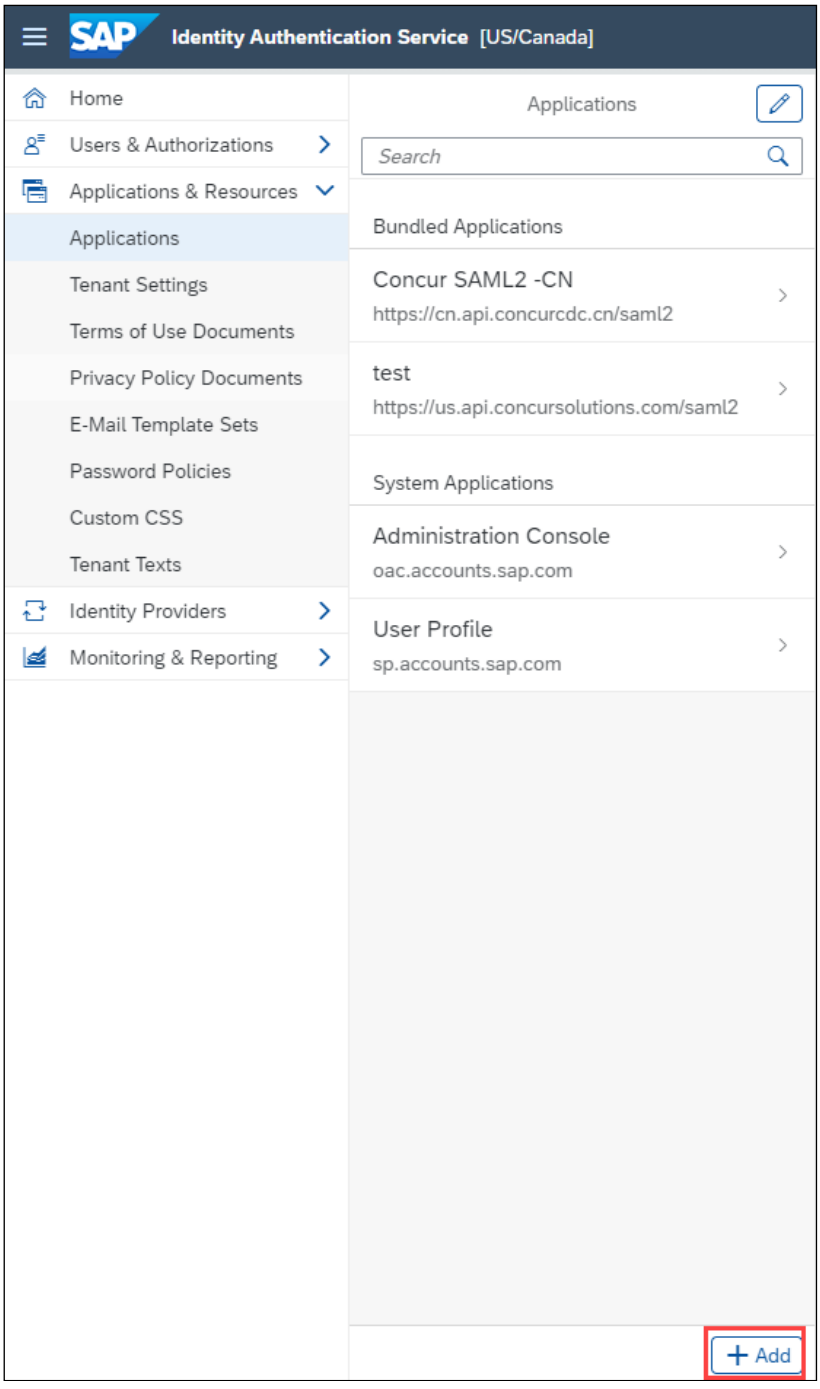


ステップ *2: SAP IAS* でアプリケーションを作成する

1. SAP IAS でアプリケーションを作成します。SAP IAS にログイン後、**[Applications & Resources]** > **[Applications]** にアクセスする必要があります。

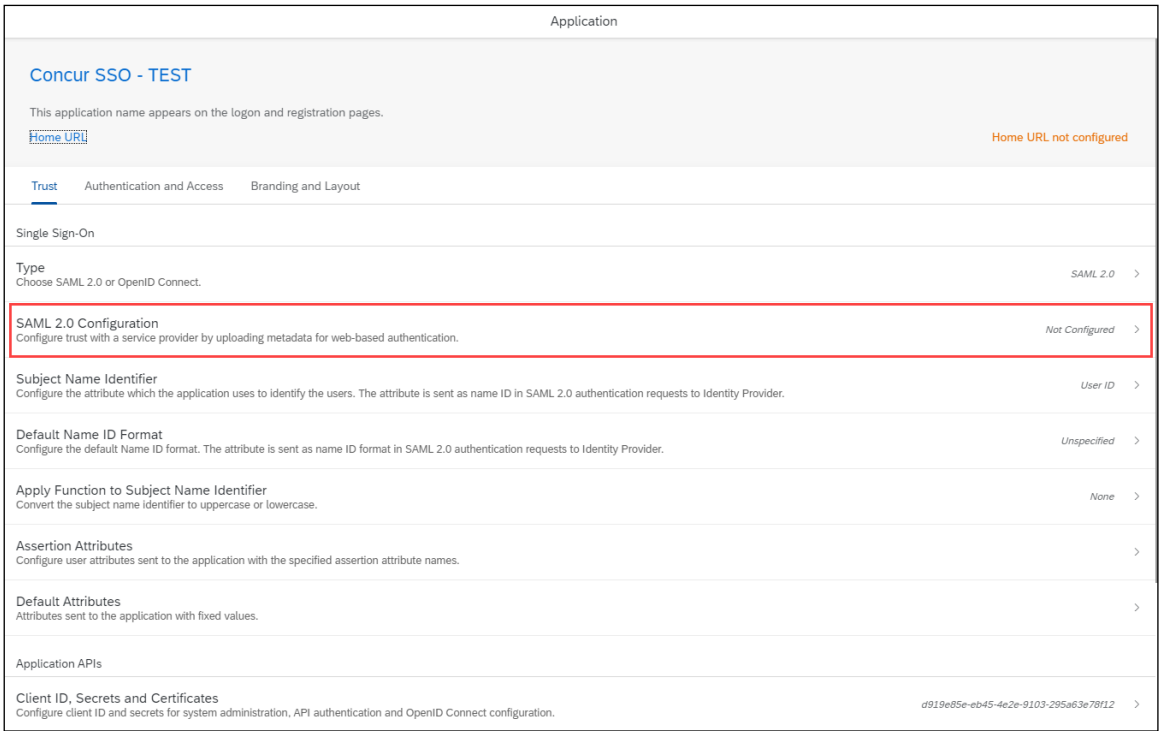


2. これにより、作成されたすべてのアプリケーションがリスト表示されます。**[+Add]** をクリックして新規アプリケーションを追加します。

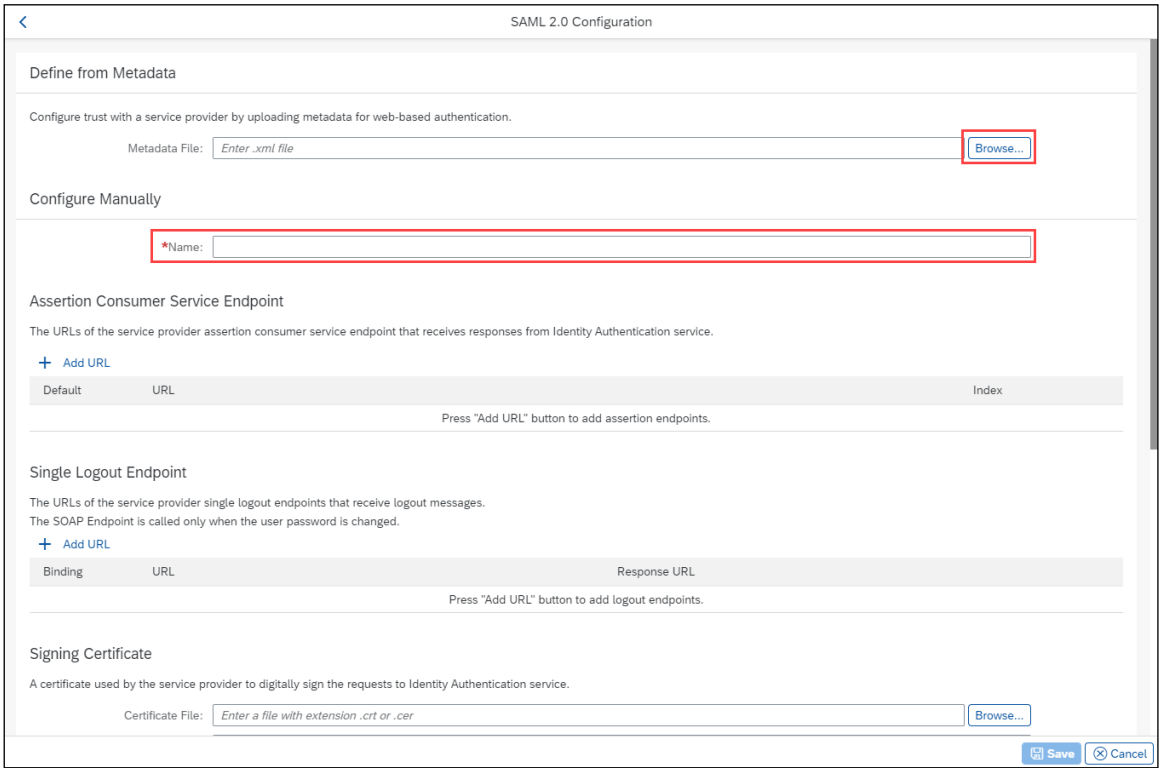


3. 名前を入力し、**[保存]** をクリックします。

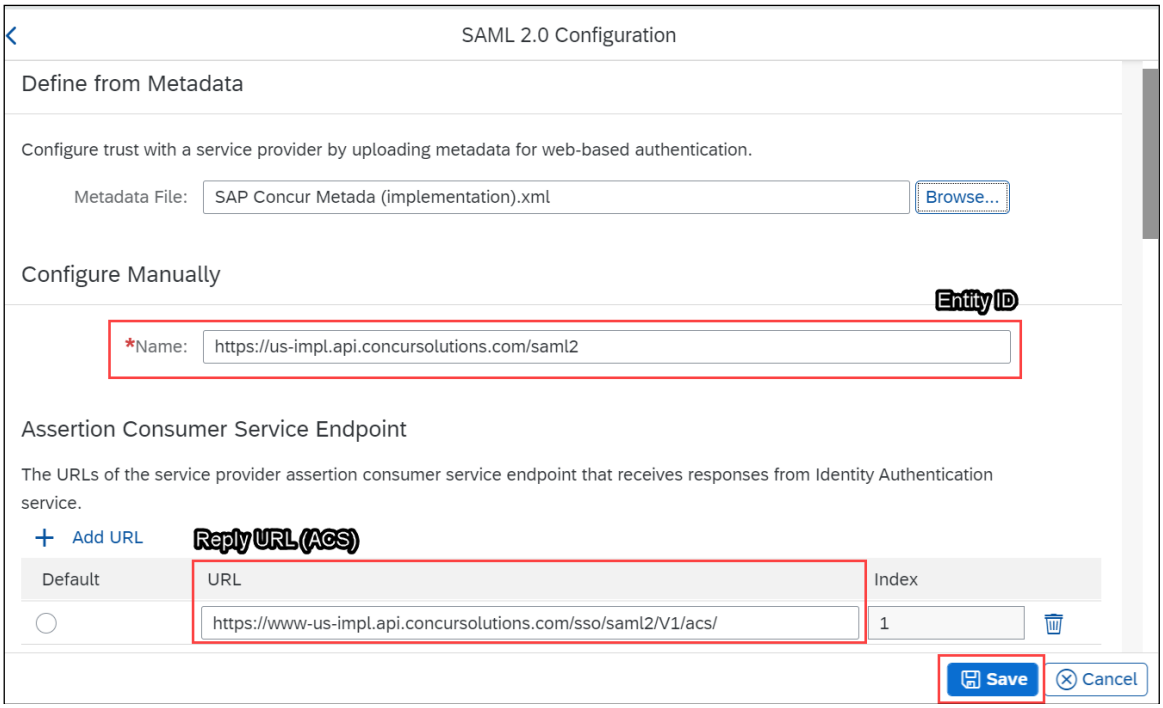
4. これが SAML (Security Assertion Markup Language) 設定になるため、[SAML 2.0 Configuration] にアクセスする必要があります。



5. 前述のステップで SAP Concur のメタデータ ファイルをダウンロードしているため、**[Browse]** をクリックしてファイルをアップロードし、その接続の **[Name]** を入力できます。

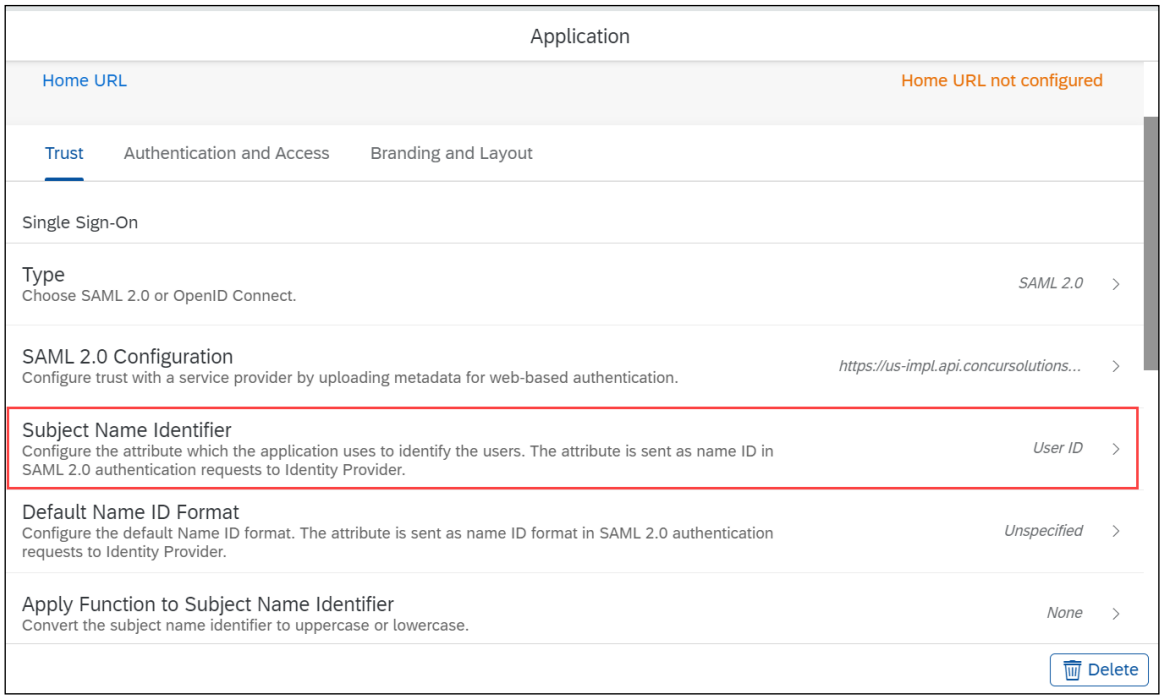


6. ファイルのアプロード後、SAP IAS はメタデータからすべての値を取り出し、それに応じてフィールドに入力する必要があります。次に、**[Save]** をクリックします。

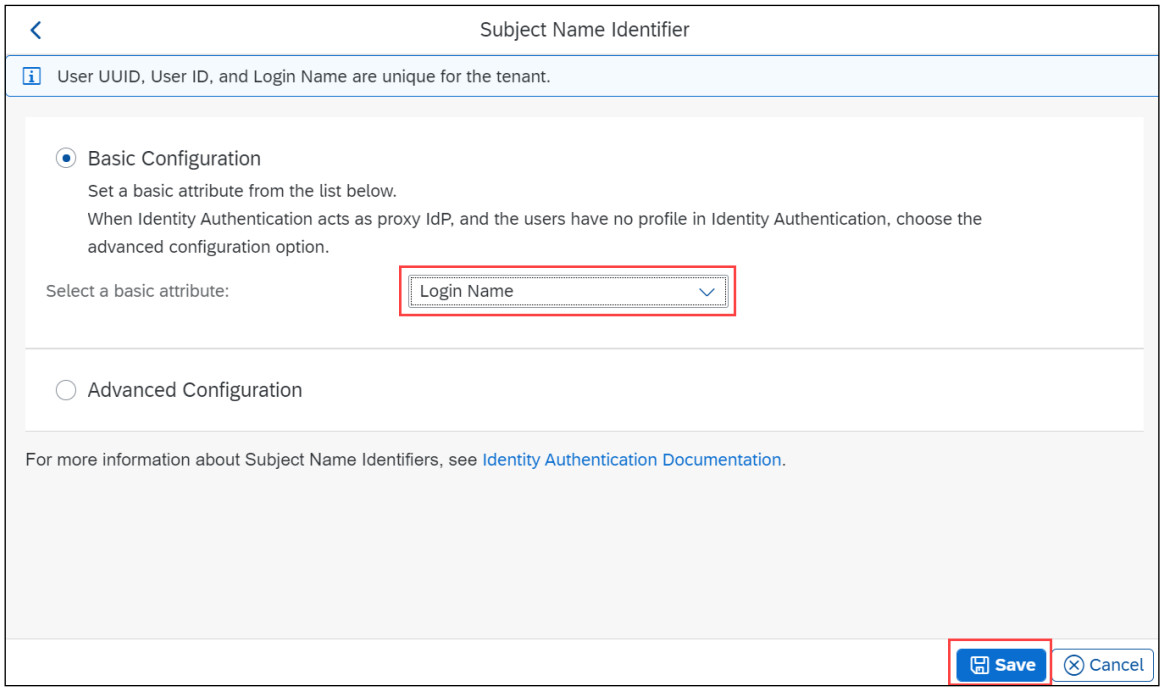


ステップ 3: [Subject Name Identifier] を変更する

既定の Subject Name Identifier は **User ID** です。SAP Concur と連携するには、[Unique User Identifier] を「ログイン名」形式にする必要があります。

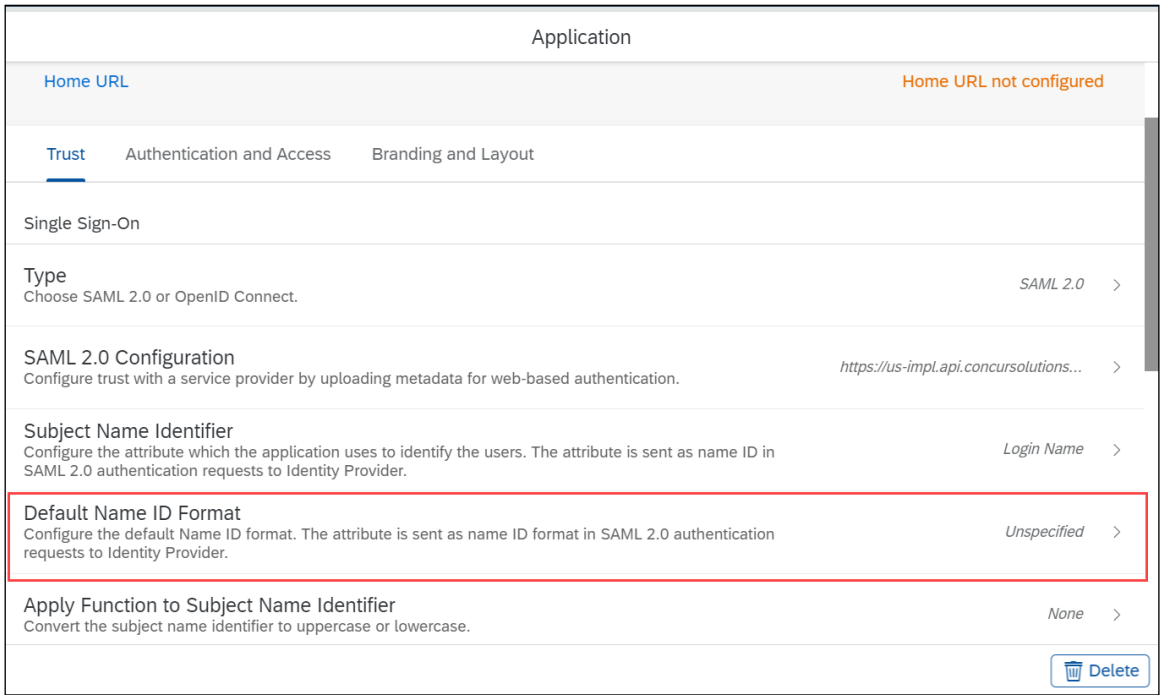


NOTE: ユーザー UUID、**ユーザー ID**、および**ログイン名**はテナントに固有のものです。[Basic Configuration] は選択したままにして、基本属性を変更します。次に、**[Save]** をクリックします。

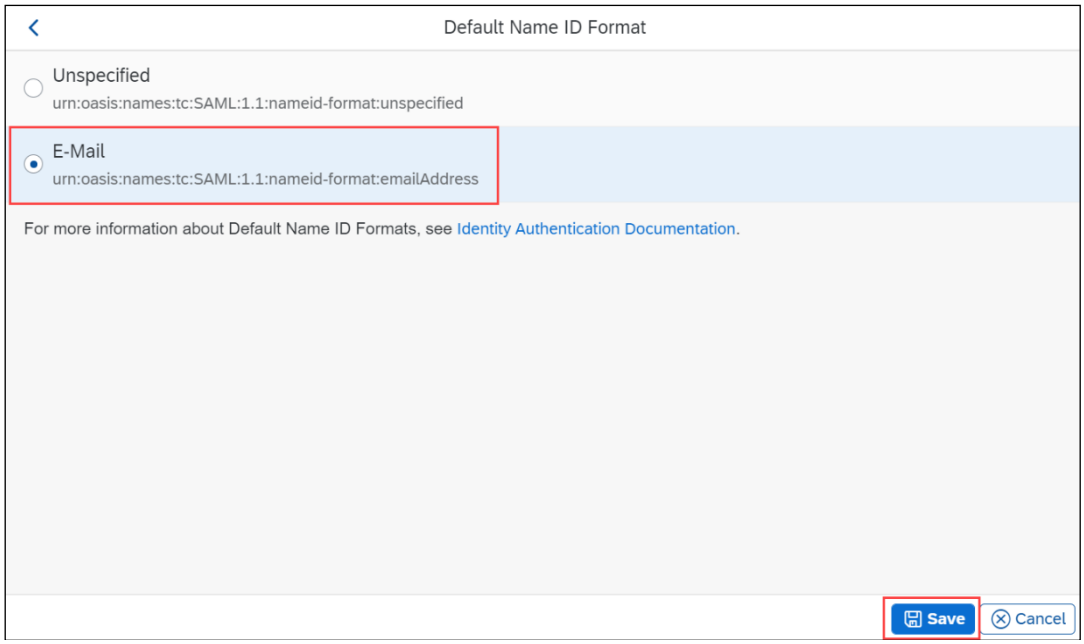


ステップ 4: [Default Name ID Format] を変更する

アプリケーションの設定完了後、**名前 ID** を設定する必要があります。**名前 ID** は、Concur で従業員に登録した**ログイン ID（CTE ログイン名）**と一致する必要があります。また、名前 ID の形式を「**メール アドレス**」に設定することを強くお勧めします。これは concursolutions.com またはモバイル アプリから開始する SP-Initiated ログインを行うために SAP Concur で必要になります。既定の [Name ID Format] は「Unspecified」であるため、**[Default Name ID Format]** をクリックして変更します。



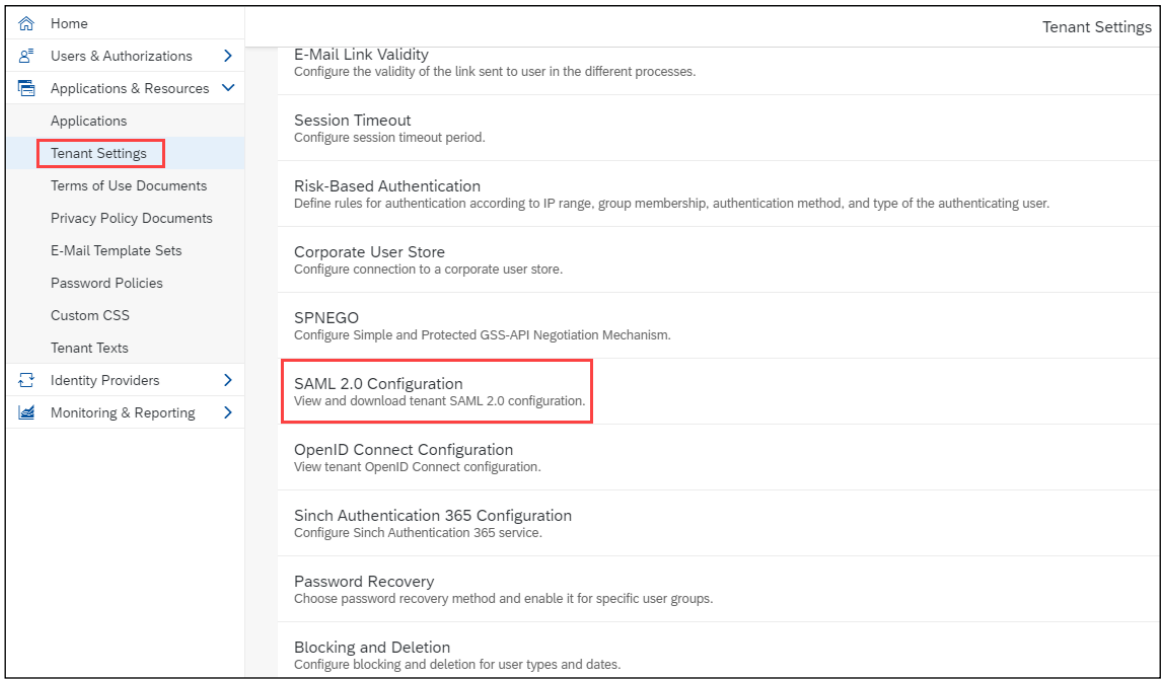
[Email] を選択したら、**[Save]** をクリックします。



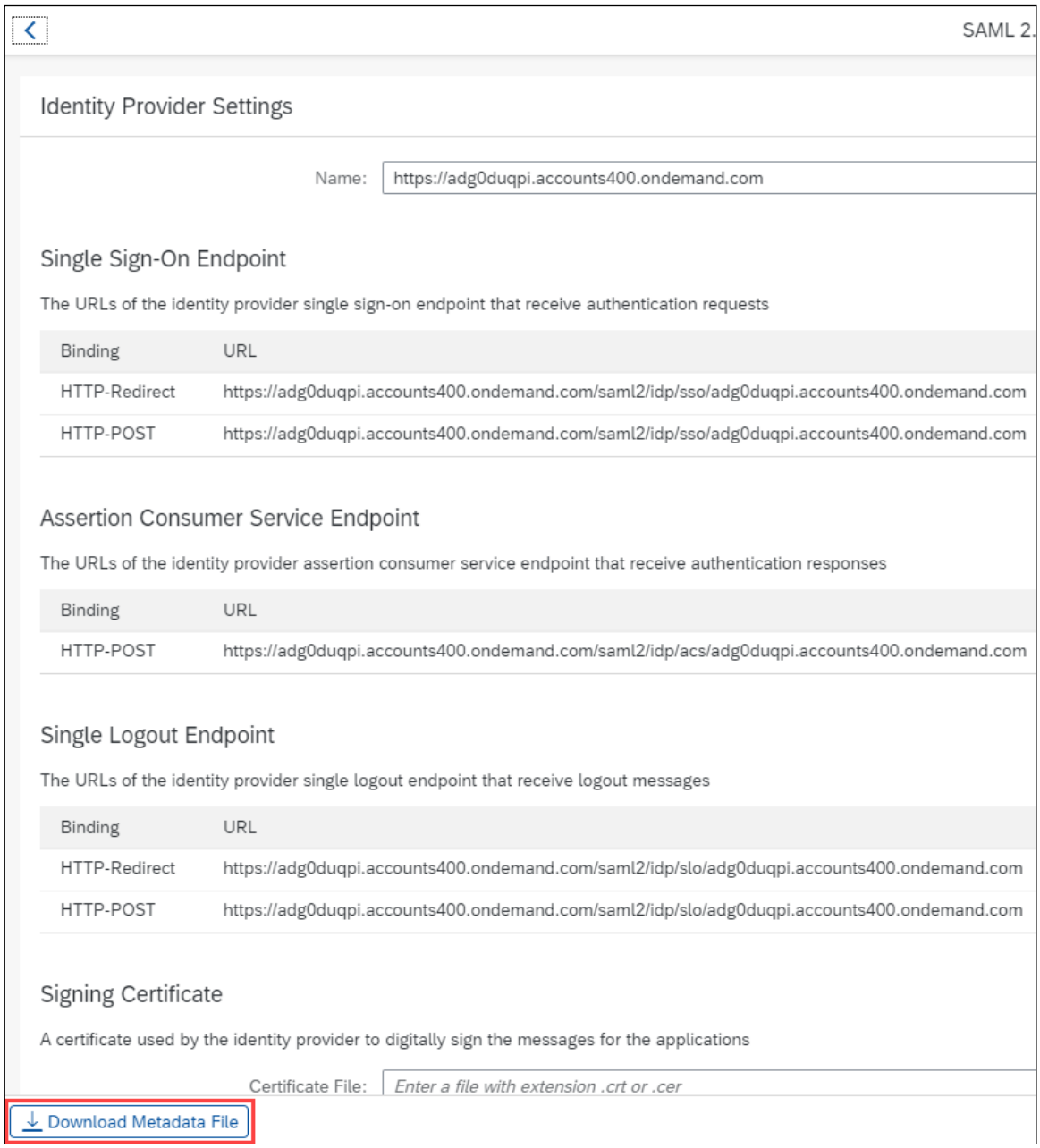
場合によっては、これは SAP Concur のユーザー名と一致しないことがあります。このような場合、SAP Concur で従業員インポートを実行し、ユーザー名が送信する属性と一致しているかどうかを確かめることができます。または、SAP IAS の製品サポートに連絡し、名前 ID 設定のサポートを要請することができます。

ステップ *5:* メタデータをダウンロードする

SAP Concur 側で設定を完了するには、SAP IAS のアプリケーションから抽出したメタデータ ファイルをアップロードします。これを行うには、**[Applications & Resources] > [Tenant Settings] > [SAML 2.0 Configuration]** に移動します。



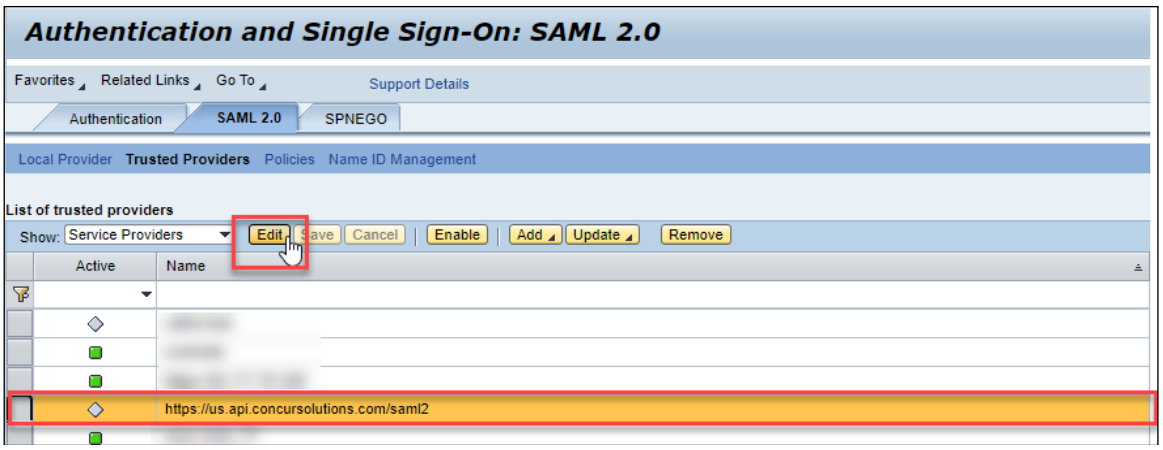
これで［Identity Provider Settings］画面が表示されます。この画面では設定を見直し、**[Download Metadata File]** を選択することができます。



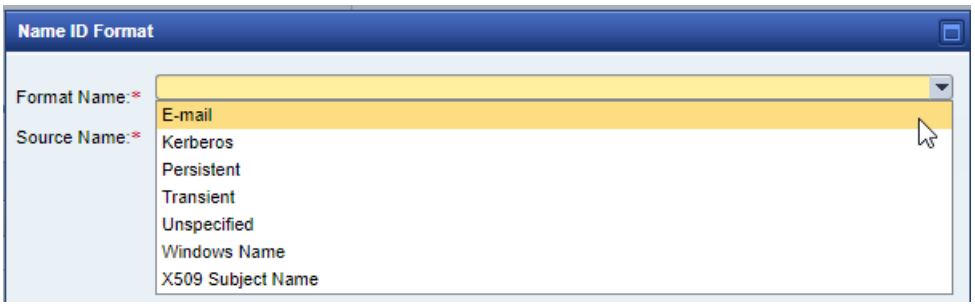
これでメタデータ ファイルを SAP Concur にアップロードする用意が整いました。

アプリケーションの設定完了後、**名前 ID** を設定する必要があります。**名前 ID** は、SAP Concur で従業員に登録したログイン ID（**CTE ログイン名**）と一致する必要があります。また、**名前 ID** の形式を「**メール アドレス**」に設定することを強くお勧めします。これは concursolutions.com またはモバイル アプリから開始する SP-Initiated ログインを行うために SAP Concur で必要になります。

1. **名前 ID** 形式を設定するには、新しいアプリケーションを検索してクリックし、次に **[Edit]** をクリックします



2. [Name ID Format] ポップアップで、必ず **[E-mail]** を選択します。**[Source Name]** に SAP Concur の従業員ログイン ID と一致する属性を入力します。

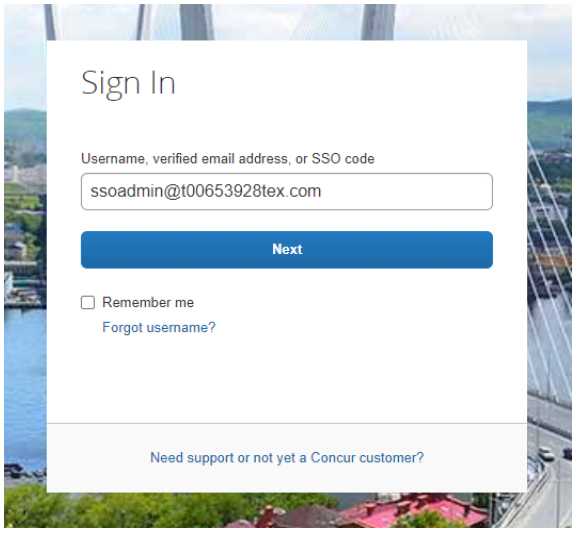


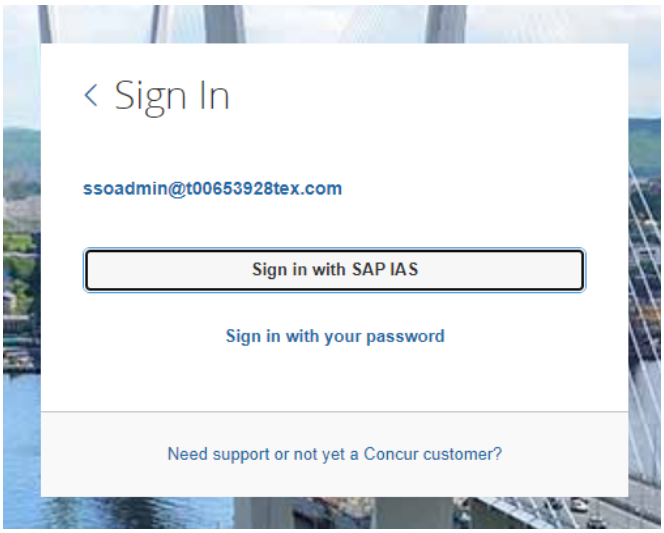
3. 場合によっては、指定可能な Source Name は SAP Concur のユーザー名と一致しないことがあります。このような場合、SAP Concur で従業員インポートを実行し、ユーザー名が送信する属性と一致しているかどうかを確かめることができます。または、SAP NetWeaver の製品サポートに連絡し、名前 ID 設定のサポートを要請することができます。

SAP Concur サイトを設定する

1. 「概要」セクションに記載されたステップに従って **[SSO の管理]** ページに移動します。
2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。
3. **[IdP 接続]** に適切な名前を入力し、その名前を **[カスタム IdP 名]** フィールドに入力します。

NOTE: SP-initiated フローを使用することにした場合（SAP Concur 公式サイト: https://www.concursolutions.com/nui/signin を利用）、ユーザー名を入力し **[次へ]** をクリックすると、 **[サインイン]** ページに **[カスタム IdP 名]** が表示されます。たとえば、**カスタム IdP 名**が「SAP IAS」の場合、すべてのユーザーに [SAP IAS でサインイン] オプションが表示さ

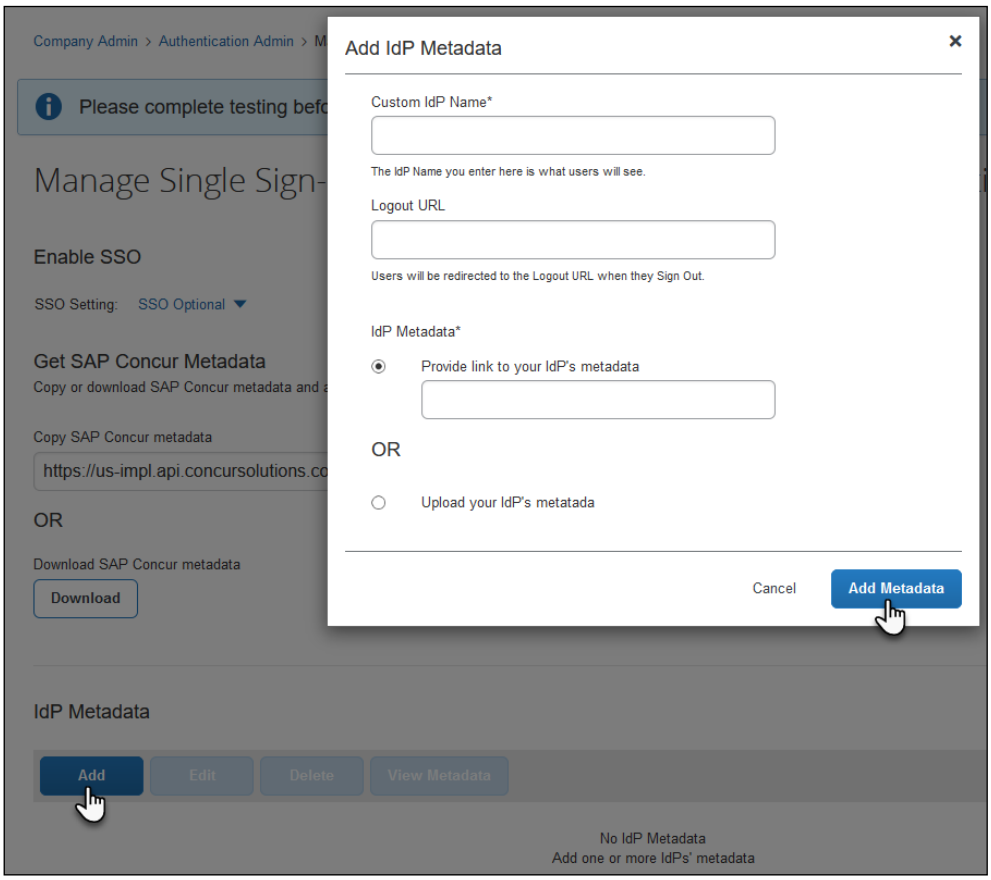




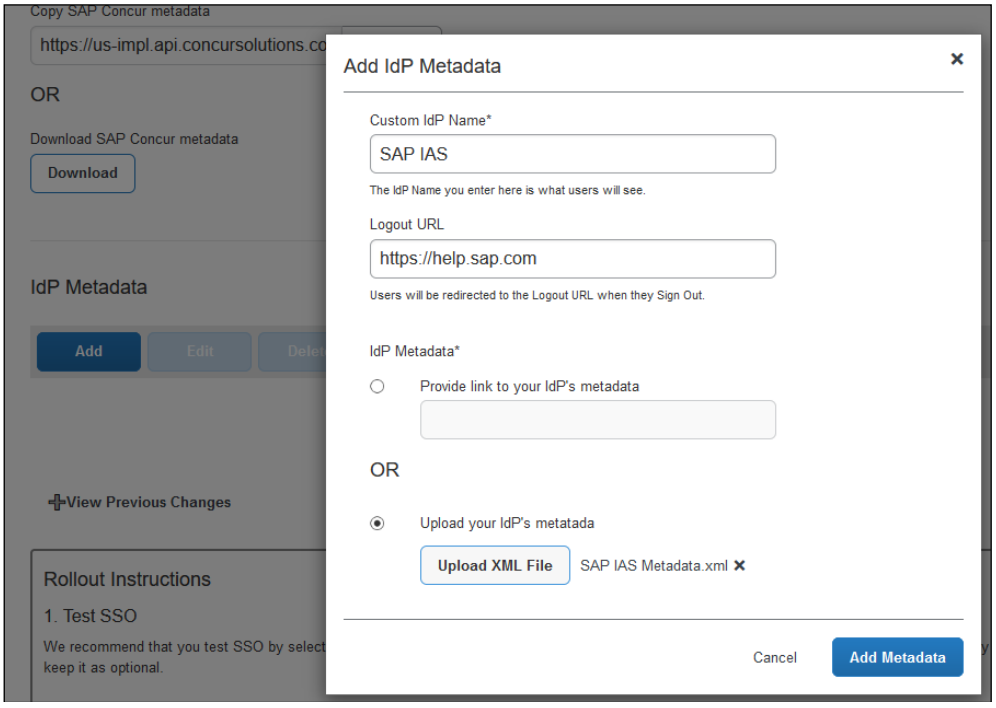
4. ユーザーがログアウトした際にほかの場所にリダイレクトされるようにログアウト URL（オプション）を入力します。既定では、URL が入力されない場合、ユーザーは認証プロセスを開始した場所にリダイレクトされます。SAP IAS のログアウト エンドポイントからは、**[Applications & Resources] > [Tenant Settings] > [Identity Provider Settings] > [Single Logout Endpoint]** で確認できます。**Single Logout (SLO)** は SAP Concur で正式にサポートされていないため、SAP Concur に加えて IDP からユーザーを切断することに関しては、SLO エンドポイントを使用するログアウト プロセスは期待どおりに動作しない可能性があります。そのような場合、ユーザーは SAP Concur からログアウトされますが、SAP IAS からは完全にログアウトされないことがあります。

5. **IdP Metadata** で、https://[**TenantID**].[**Environment**].ondemand.com/saml2/metadata の形式に従った

IdP メタデータのリンクを入力するか、事前にローカルに保存された、IdP メタデータを含む XML ファイルをアップロードします。

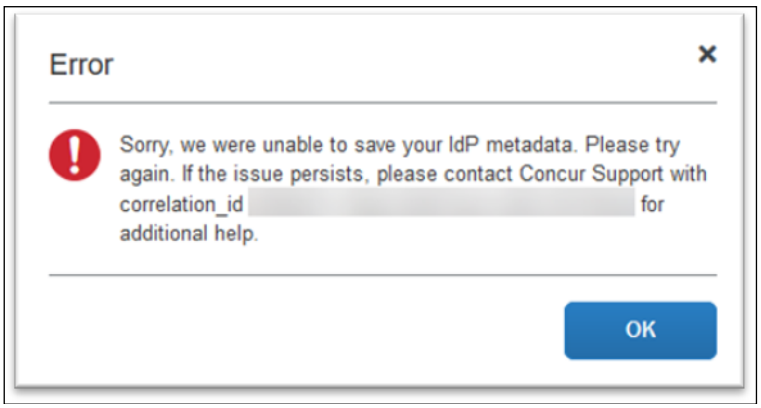


6. すべての詳細を入力すると、次のように表示されます。



7. **[メタデータの追加]** をクリックします。

8. 追加の成功を示す確認メッセージまたは問題の発生を示すメッセージが表示されます。後者の場合、SAP Concur サポートに連絡し、相関 ID を提供してください。



SSO ログインのテスト

前述のステップで IdP メタデータが SAP Concur に正常にアップロードされると、SSO のテストを開始できます。このセクションでは、IdP-Initiated（アイデンティティ プロバイダ側で開始される）フローおよび SP-Initiated（サービス プロバイダ側で開始される）フローをテストすることができます。

IdP-initiated SSO のテスト

IdP-initiated SSO をテストするには:

1. IdP-Initiated フローで、アイデンティティ プロバイダ側でログイン プロセスを開始します。テストを行うには、先ほど作成したアプリケーションのパラメーターを SAP IAS の SSO エンドポイントに付加します。IdP-Initiated URL の形式の例は次のようになります。

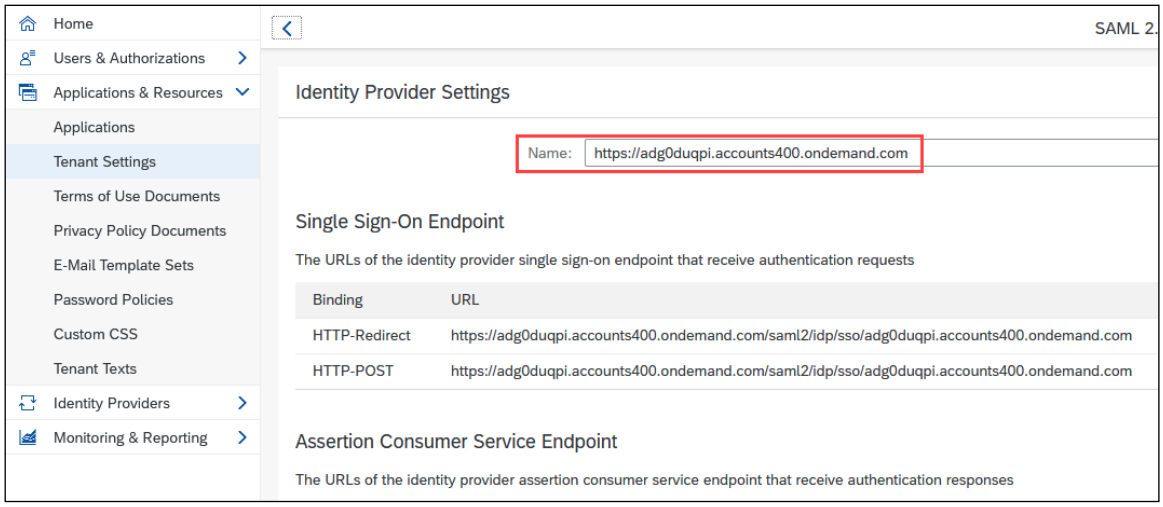
   形式: [**テナント名***]?saml2sp=[**SP 識別子****]

   例: https://adg0duqpi.accounts400.ondemand.com/saml2/idp/sso?sp=https://us-impl.api.concursolutions.com/saml2

***テナント名: [Applications & Resources] > [Tenant Settings]** に移動します。

****SP 識別子**: SAP Concur メタデータから入手できます。**エンティティ ID** または **Audience** と同じです。

NOTE: SAP IAS には異なる 5 つの環境がありますが、お客様に関連があるのは PROD 環境 (*.accounts.ondemand.com) のみです。



この URL は SAP IAS 側のログイン ページにリダイレクトします。資格情報を使用してログインすると、SAP Concur ホームページにリダイレクトされます。

SP-Initiated SSO のテスト

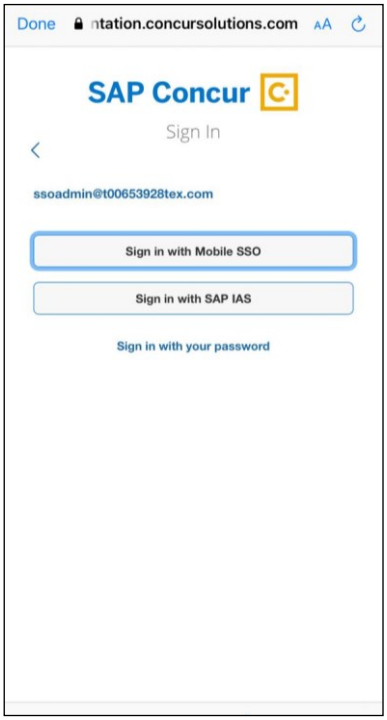
SP-initiated SSO をテストするには:

1. テストを行いたい環境のログイン ページを開きます。
   - US DC Prod: https://www.concursolutions.com/
   - US DC Test: https://implementation.concursolutions.com/
   - EMEA DC Prod: https://eu1.concursolutions.com/
   - EMEA DC Test: https://eu1imp.concursolutions.com/
   - CN DC Prod: https://www.concurcdc.cn/
2. ログイン ページでユーザー名、照合済メール アドレス、または SSO コードを追加して続行できます。**[次へ]** をクリックすると、「SAP Concur サイトを設定する」の注記のとおり、最近作成した SSO 設定のオプションが表示されます。クリックして、SAP Concur にリダイレクトするアイデンティティ プロバイダ アカウントの認証を続行します。

モバイル シングル サインオン（SSO）

SAMLv2 プラットフォームで作成された SSO 設定の場合、モバイル SSO はメタデータが保存されるとすぐに自動的に有効にされます。ただし、このオプションが機能するには、SP-Initiated フローが機能している必要があります。これは、前述の「SSO ログインをテストする」セクションを使用して検証することができます。

NOTE: モバイル SSO の自動有効化は、アプリのバージョンが 9.86 以降であり、かつ、ユーザーが新しいサインイン操作を選択している場合のみ表示されます。このオプションは旧バージョンのユーザー、または以前のサインイン操作を選択しているユーザーには自動的に非表示になります。もし以前に他の IdP をお使いで既にモバイル SSO をご利用の場合、以下の際 2 つのオプションが表示される可能性があります。



[モバイル SSO でサインイン] オプションにより以前の IdP リンクが埋め込まれるため、ユーザーは以前の SSO 接続にリダイレクトされます。

いずれの場合も、SAP Concur サポート チームにチケットを作成し、次の情報を提供してください。

- ユーザーが以前のバージョンを使用する予定の場合、当該アプリ バージョンにモバイル SSO を有効化できるように、SAP NetWeaver 側で作成したアプリケーションの IdP-Initiated URL を SAP Concur サポートに提供してください。URL の入手方法に関する詳細については、このガイドの「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。
- 混乱する可能性を排除するために **[モバイル SSO でサインイン]** オプションを削除する場合、サポート チームにご連絡ください。

モバイル アプリで SSO を使用する認証時に問題がある場合、SAP Concur サポート チームにチケットを作成し、表示されたエラー ID やメッセージをスクリーンショットと一緒に提供してください。

メール通知

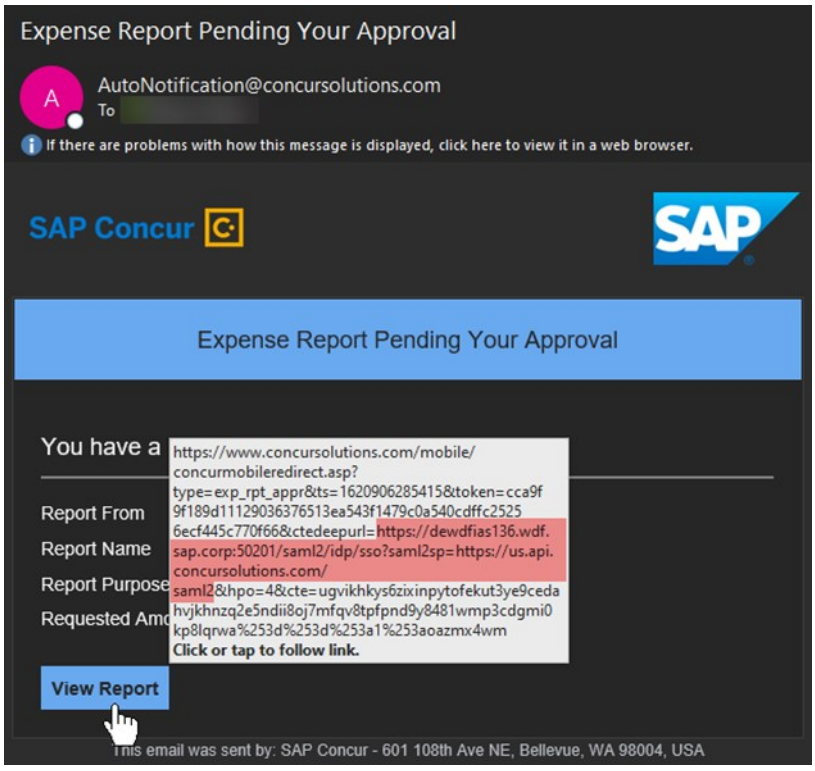
備忘メールに SSO URL を反映する設定は、SAP Concur サポートで完了する必要のある変更です。設定を進めるには、SAP Concur サポート チームにチケットを作成し、サポート チームが備忘メールのリダイレクト URL を調整できるように、IDP 側で作成したアプリケーションの IDP URL を提供します。URL の入手方法に関する詳細については、この付録の「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。

NOTE: URL は **[レポートの表示]** ボタンに埋め込まれて表示されます。

NOTE: この変更は変更後に生成されたメールにのみ反映されます。変更前に生成されたすべてのメールは以前の URL を引き続き使用します。

NOTE: この変更は反映されるまで最大 4 時間程度かかります。

[レポートの表示] ボタンにカーソルを乗せると、現在挿入されている URL が表示されます。URL は **ctedeepurl=** と **&hpo=** の間に表示されます。



展開

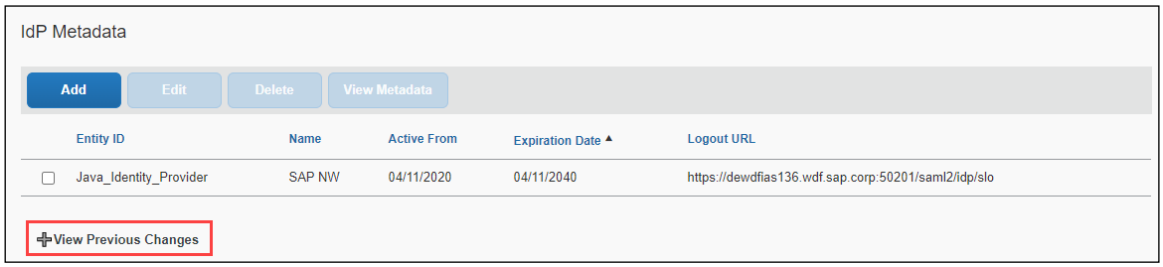
新しい SSO 設定をテストしたら、このアクセスが必要なすべてのユーザーおよびグループに新しい SAP IAS アプリケーションを割り当てることで、展開の計画を立てることができます。

[SSO の管理] ページでは、SSO 設定を [SSO 任意] から **[SSO 必須]** に変更するとこの新しい SSO 接続を強制するオプションも提供しています。この設定を変更する場合、ユーザーは SP-initiated フローからユーザー名を提供すると SAP Concur にリダイレクトされるようになります。

以前の変更を表示

この機能は、**[SSO の管理]** ページで完了したすべての変更を管理者が追跡できるようにするために開発されました。

現時点までに行われた SSO 設定への変更を表示するには、**[以前の変更を表示]** をクリックします。

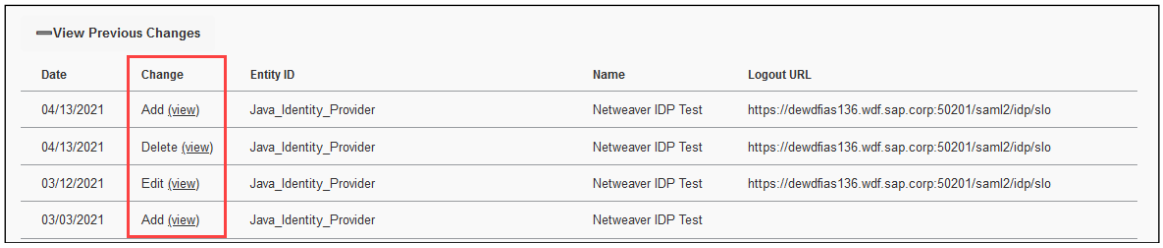


以前の変更が記載された表が表示され、日付と時刻の降順で並べ替えられています。

テーブルには、過去に行われた 100 件の変更が表示されます。テーブルにリストされる変更内容としては、以下のようなものが含まれます。

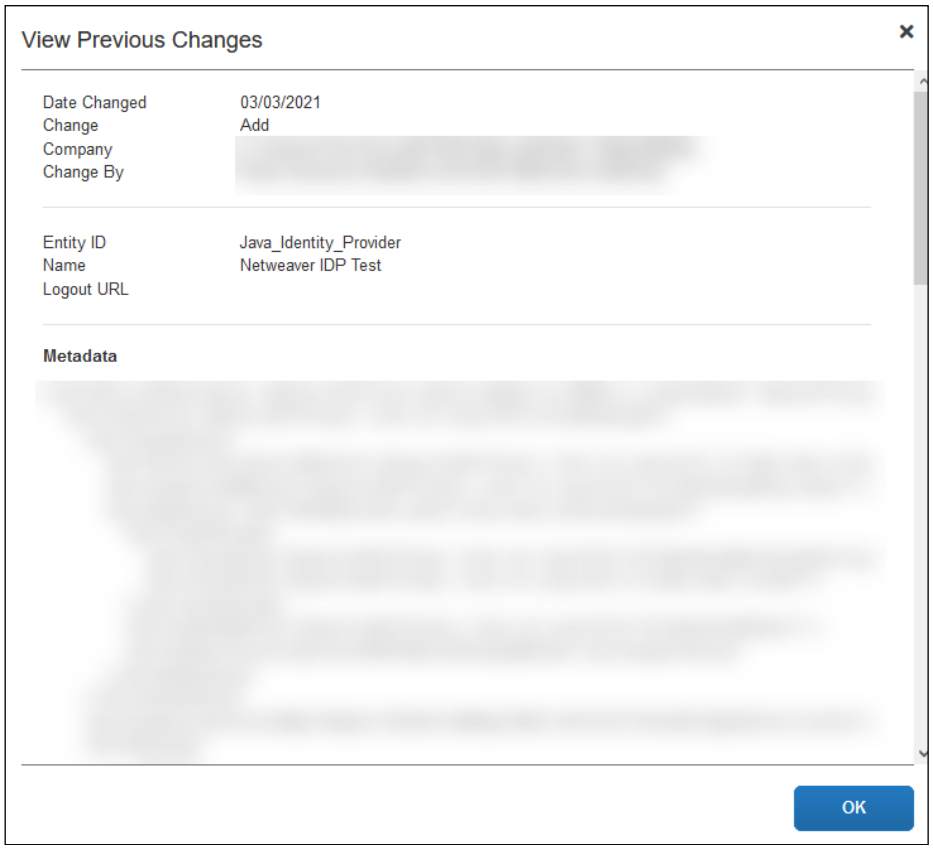
- 設定の追加
- 設定の削除
- [カスタム IdP 名] または [ログアウト URL] フィールドの編集

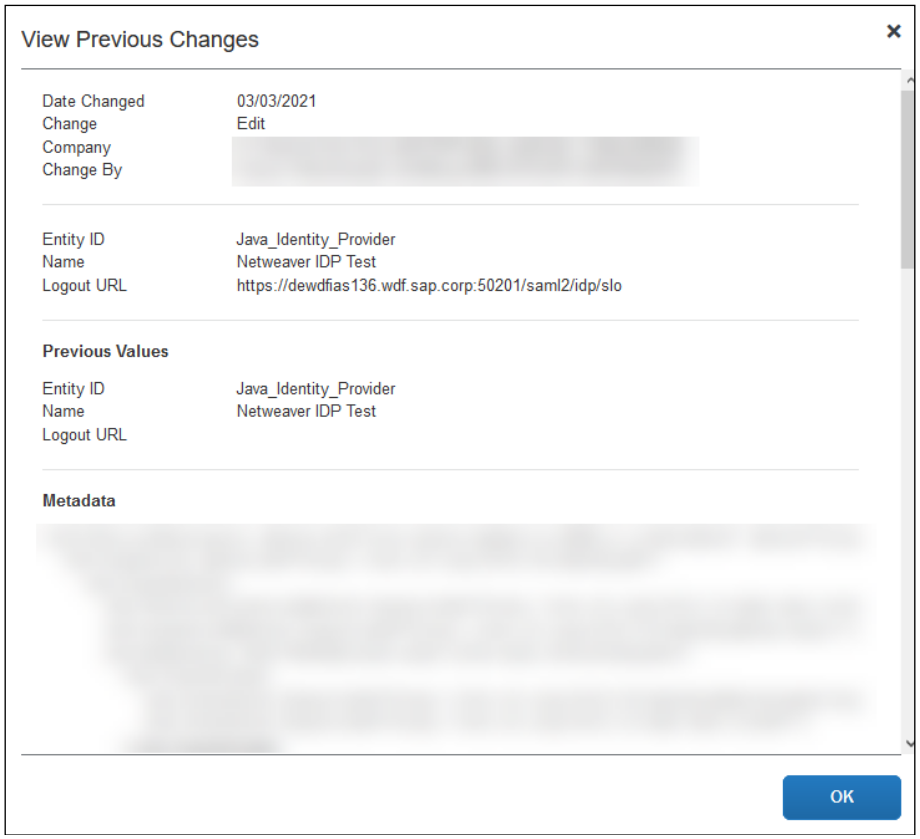
テーブルに一覧表示されている特定の変更に関する詳細情報を表示するには、目的のリスト項目の **[表示]** リンクをクリックします。



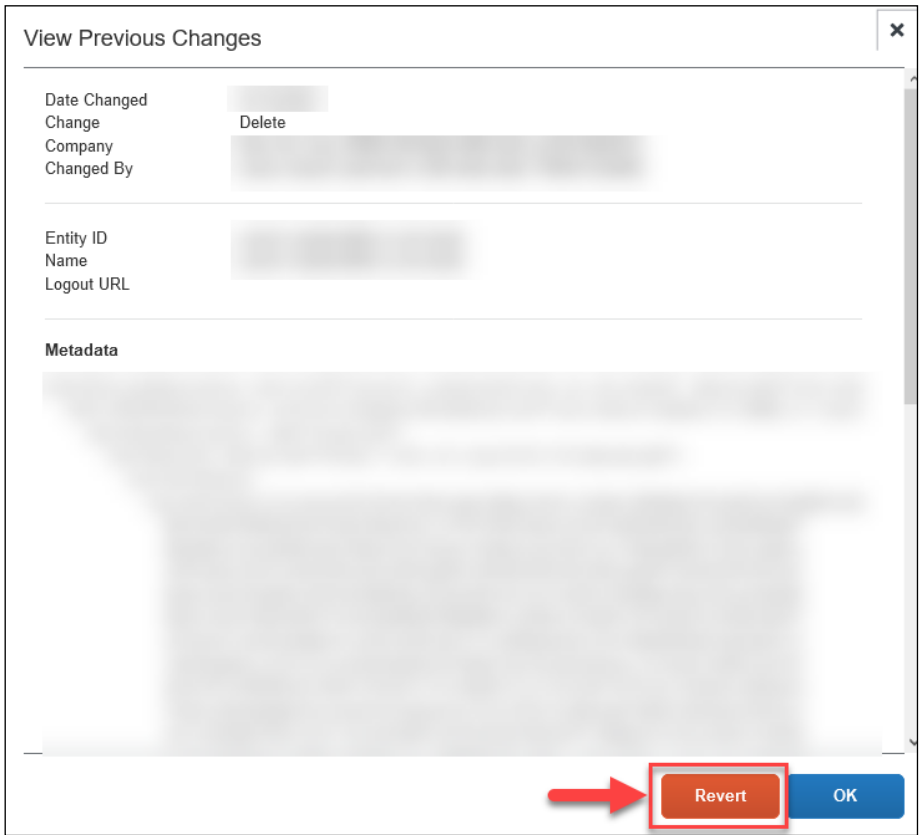
各ログの内部では、**[会社]** および **[変更者]** フィールドが [first_name last_name] [(UUID code)] 形式で表示されます。これは、そのアクションを行ったユーザーを参照しています。そのユーザーに見覚えがない場合、サポートに問い合わせて、詳細をリクエストすることができます。

ログの例:





設定が削除されている場合、この設定を復元するための **[元に戻す]** ボタンが **[変更履歴の表示]** ページに表示されます。設定が復元されると、この設定をサインイン プロセス中にユーザーが使用できるようになります。



📖 さらに詳しい情報は、次の文書をご参照ください。

- SAP Concur - SSO 概要
- SAP Help Portal - SAP Cloud Identity Services - Identity Authentication
- SAP KBA - 2701851 - SAP Cloud Platform Identity Authentication Service (IAS) - Guided Answers

セクション 13: 付録: SAP NetWeaver の設定

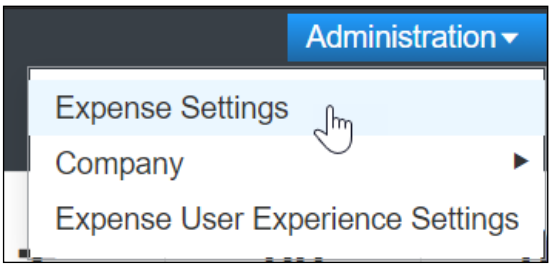
概要

設定プロセスを開始する前に、以下の点を確認します。

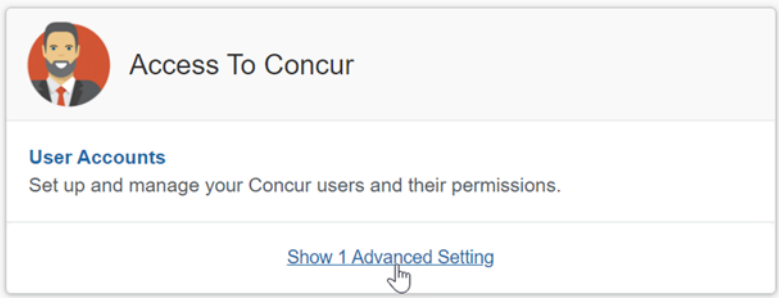
- アイデンティティ プロバイダ（SAP NetWeaver）の管理者アクセス権を取得している。これは SAP NetWeaver 側でアプリケーションの設定を完了するために必要になります。
- SAP NetWeaver の と SAP Concur の両方にユーザーが存在している。SAP Concur は現在、自動ユーザー プロビジョニングをサポートしていないため、別途ユーザーを追加する必要があります。
- SAP NetWeaver から送信する属性が SAP Concur の各従業員の **[ログイン ID]**（**ユーザー名** / **CTE ログイン名**）フィールドと一致する。
- SAP Concur アカウントに割り当てられた組織管理者（Travel のアクセス許可）を取得している。アクセス許可を取得したら、お使いの SAP Concur のエディションに応じて、次のいずれかのパスを使用して **[SSO の管理]** ページにアクセスできるようになります。

SAP Concur **Standard** Edition の場合:

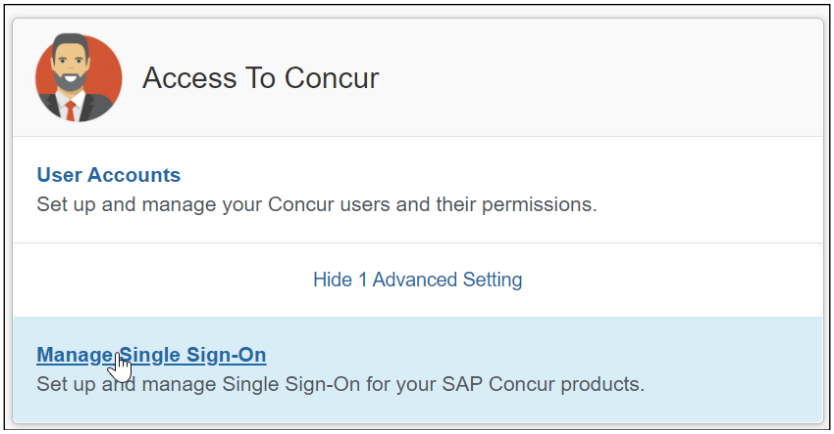
1. **[管理] > [経費の設定]** に移動します。



2. [Concur にアクセス] セクションの下にある **[1 つの詳細設定を表示]** をクリックします。

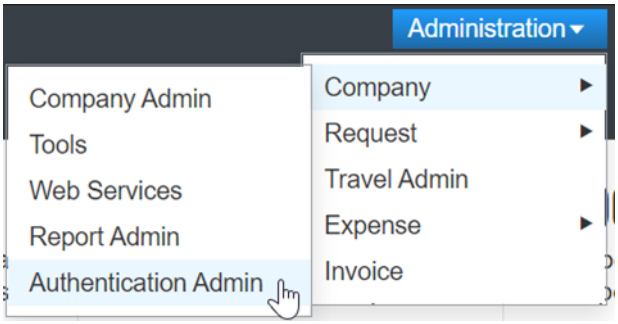


3. **[シングル サインオンの管理]** をクリックして、**[SSO の管理]** ページにアクセスします。

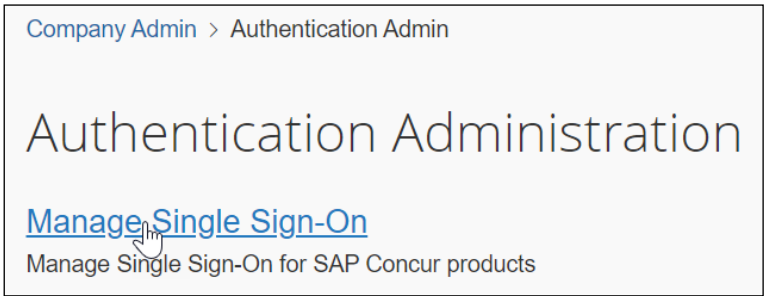


SAP Concur **Professional** エディション：

1. **[管理] > [会社] > [認証管理]** へ移動します。



2. **[シングル サインオンの管理]** をクリックして、[SSO の管理] ページにアクセスします。



または、以下のいずれかの URL を使用して、ページにアクセスすることができます。

- US DC Prod: https://www.concursolutions.com/nui/authadmin/ssoadmin
- US DC Test: https://implementation.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Prod: https://eu1.concursolutions.com/nui/authadmin/ssoadmin
- EMEA DC Test: https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin
- CN DC Prod: https://www.concurcdc.cn/nui/authadmin/ssoadmin

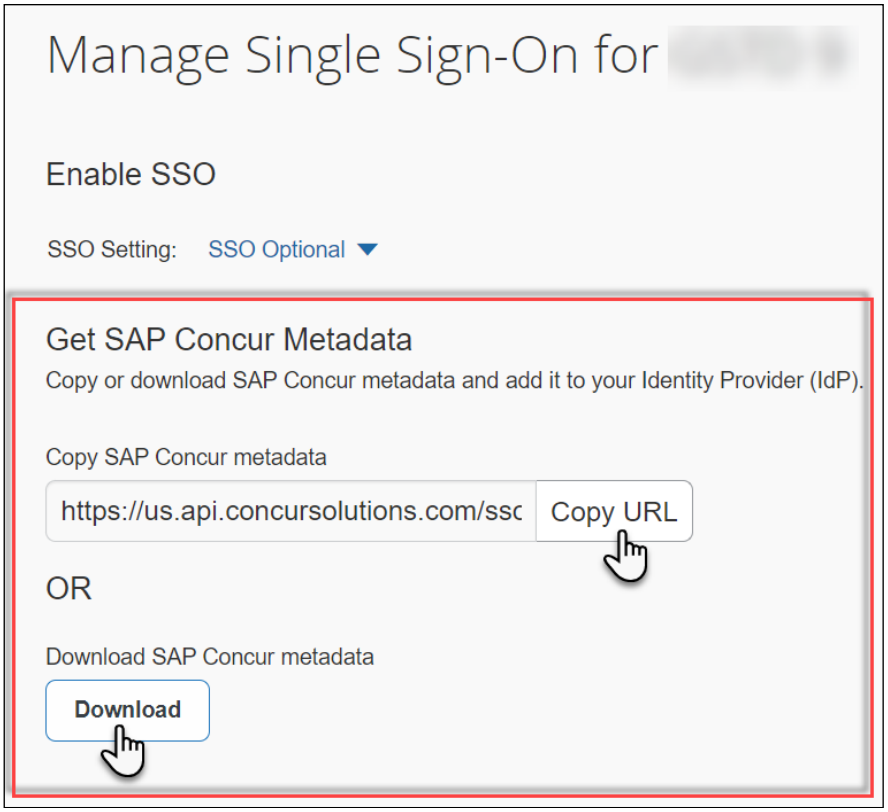
NOTE: アクセス許可を取得しておらず、自分のプロファイルに割り当てることもできない場合、会社のサポート問合せ権限の保持者に依頼し、SAP Concur サポートまでお問い合わせください。

SAP NetWeaver アプリケーションを設定する

ステップ *1:SAP Concur* メタデータを入手する

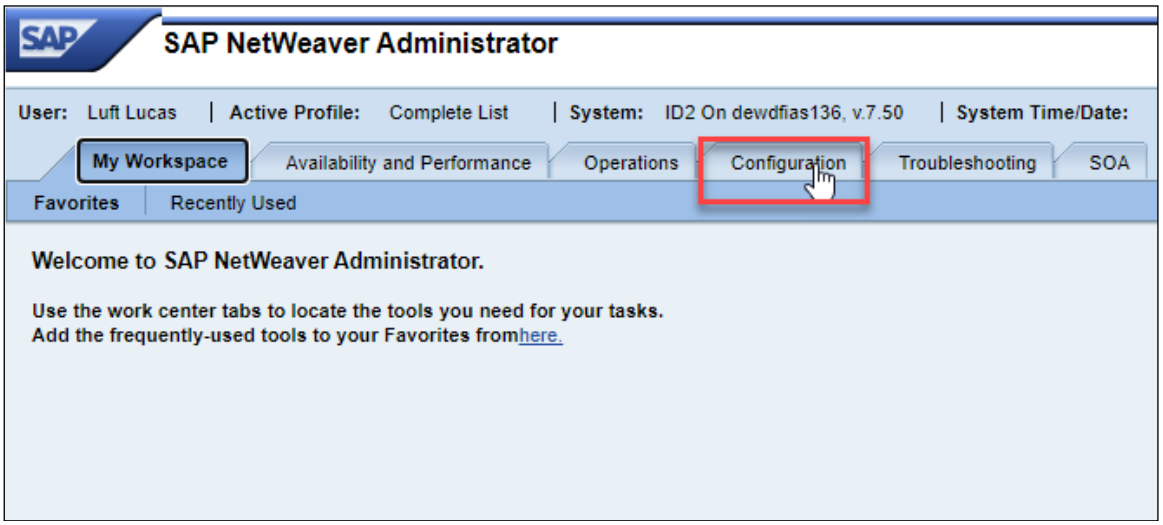
設定方法:

1. SAP Concur メタデータを入手します。これを完了するには、「概要」セクションの説明に従って SAP Concur アカウントにログインし、**[SSO の管理]** セクションにアクセスします。[SSO の管理] ページで SAP Concur メタデータを取得するには、**[URL をコピー]** をクリックしてから新しいブラウザ タブにその URL をクリックするか、**[ダウンロード]** をクリックしてダウンロードしたファイルを開きます。

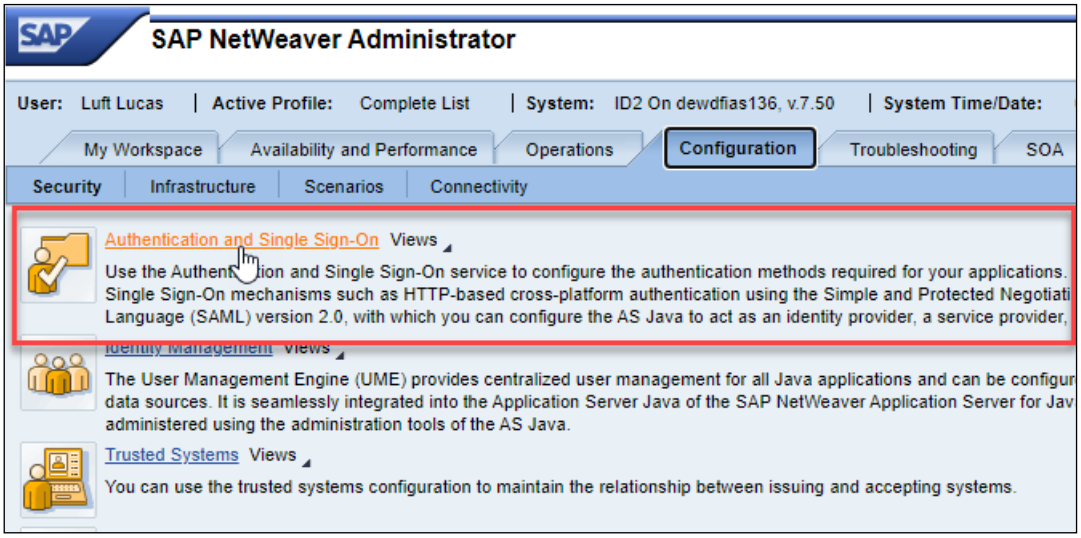


ステップ 2: SAP NetWeaver でアプリケーションを作成する

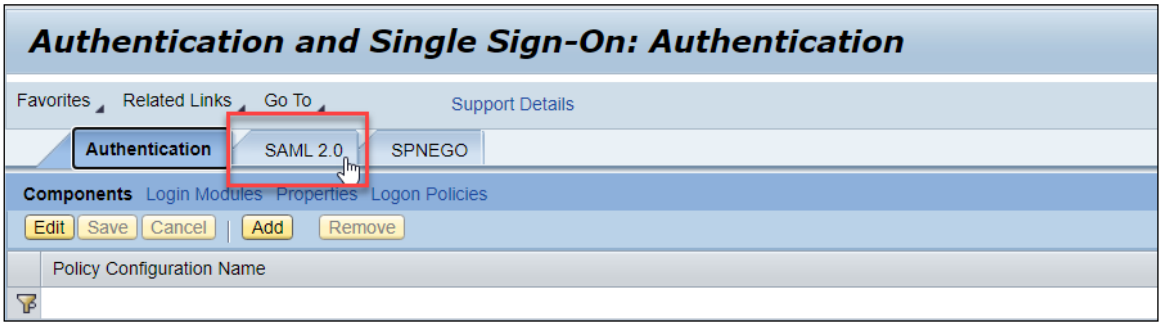
1. SAP NetWeaver でアプリケーションを作成します。SAP NetWeaver にアクセスしたら、[Configuration] タブにアクセスする必要があります。



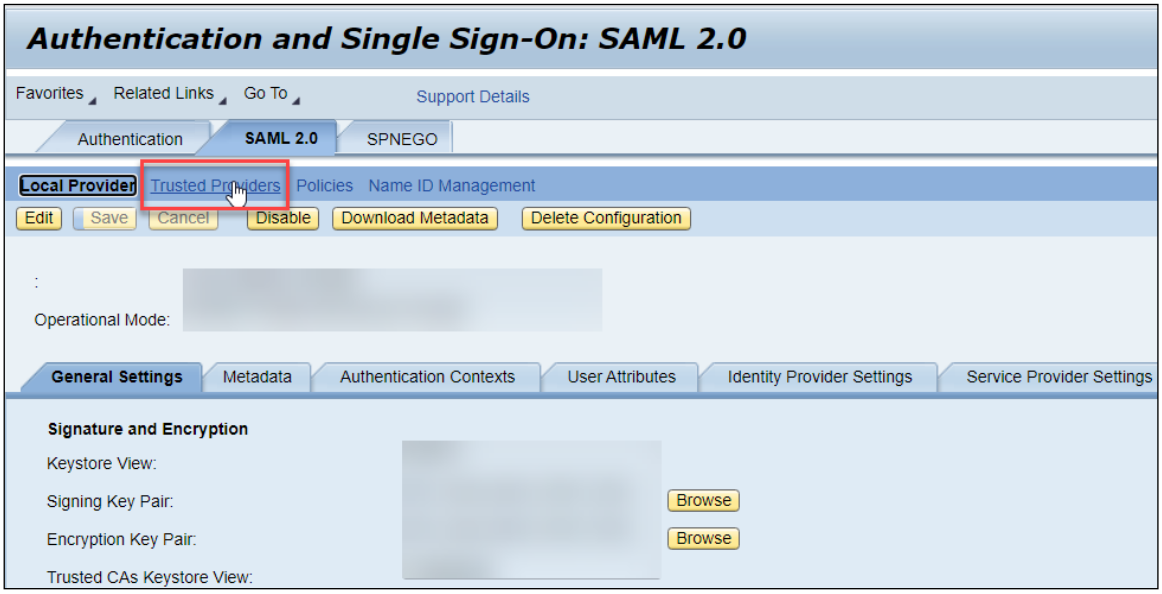
2. [Configuration] タブで、**[Authentication and Single Sign-On]** をクリックします。



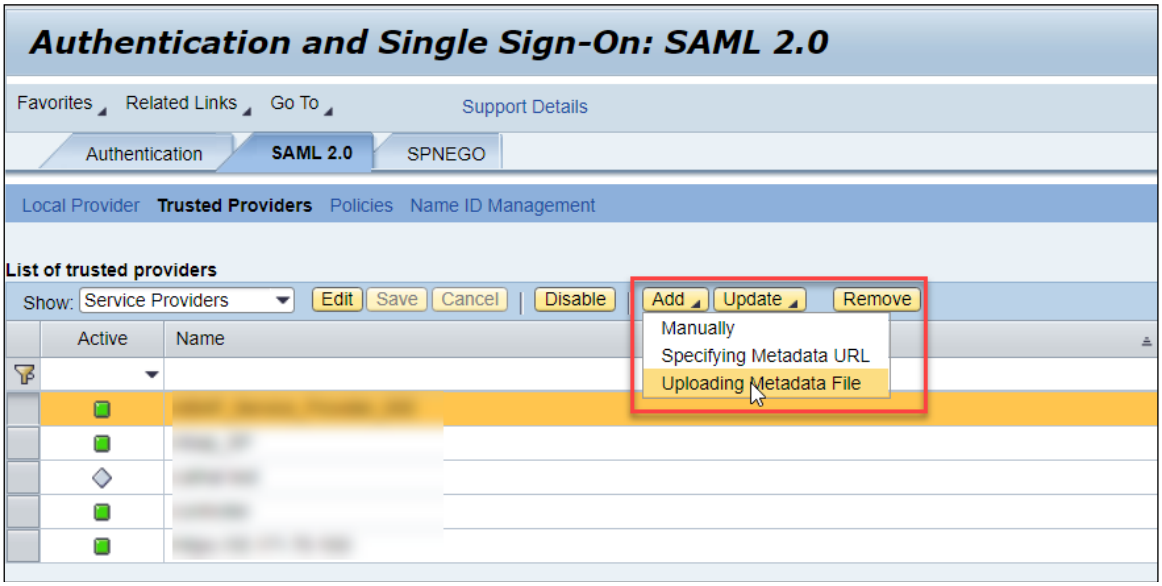
3. これは SAML (Security Assertion Markup Language) 設定になります。**[SAML 2.0]** タブをクリックします。



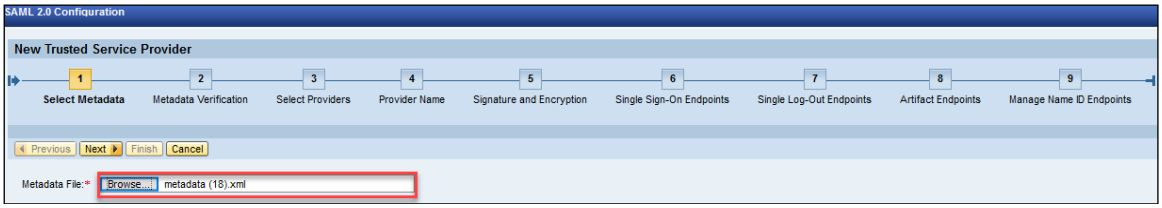
4. SAP Concur アプリケーションの作成を開始するには、**[Trusted Providers]** をクリックします。



5. [Trusted Providers] セクションには、SAP NetWeaver テナントに接続された既存のすべてのサービス プロバイダが表示されます。新しいアプリケーションを追加するには、**[Add]** をクリックします。1 つ目のステップで SAP Concur メタデータ ファイルをすでにダウンロードしているため、**[Uploading Metadata File]** オプションをクリックします。

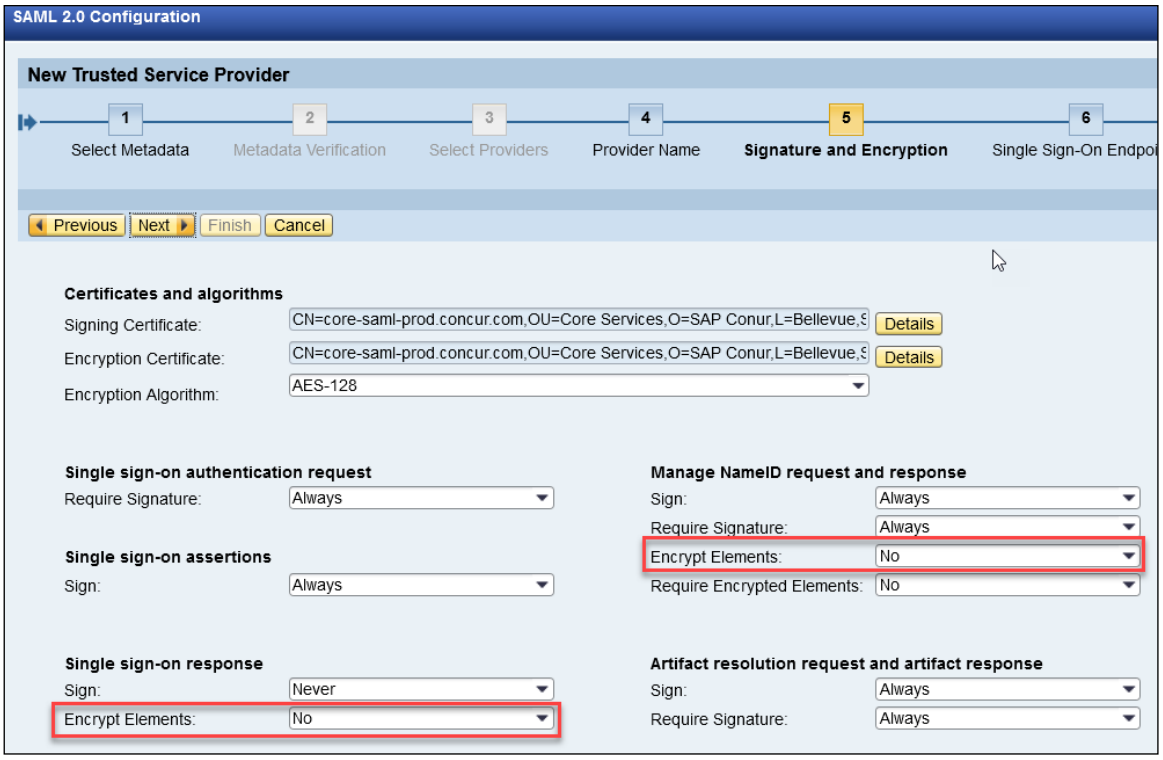


6. **[Browse]** をクリックして、お使いのコンピュータでメタデータ ファイルを探し、**[Next]** をクリックします。

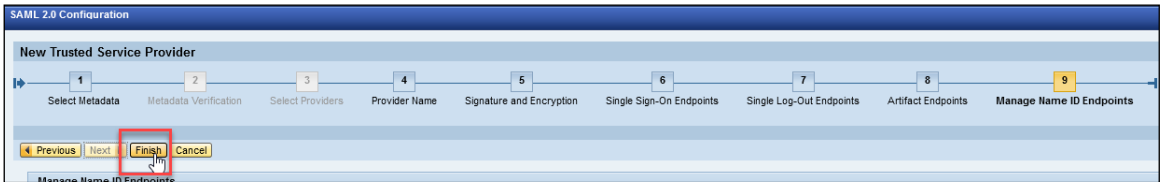


7. その後、ステップ 2 (**[Metadata Verification]**) およびステップ 3 (**[Select Providers]**) がグレー表示され、自動的にスキップされます。メタデータから適切な識別子 (**エンティティ ID**) が自動的に入力されるため、**[Next]** をクリックしてステップ 4 (**[Provider Name]**) をスキップすることもできます。

   ステップ 5 (**[Signature and Encryption]**) では、変更せずに **[Next]** をクリックできます。ただし、アサーションや **名前 ID** リクエストと応答を暗号化する場合、暗号化が有効化されるように **[Encrypt Elements]** フィールドを調整する必要があります。次に、再び **[Next]** をクリックします。



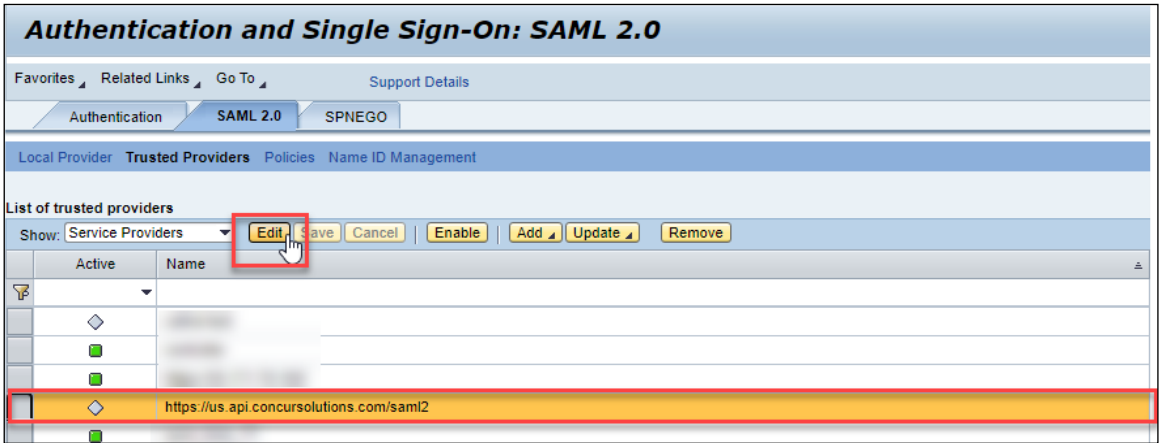
   ステップ 6 (**[Single Sign-On Endpoints]**) は、メタデータ xml から取得した適切な ACS URL が自動的に入力されるため、スキップすることができます。**[Finish]** をクリックできるようになるまで、ステップ 7 (**[Single Log-Out Endpoints]**)、ステップ 8 (**[Artifact Endpoints]**) およびステップ 9 (**[Manage Name ID Endpoints]**) も同様にスキップできます。



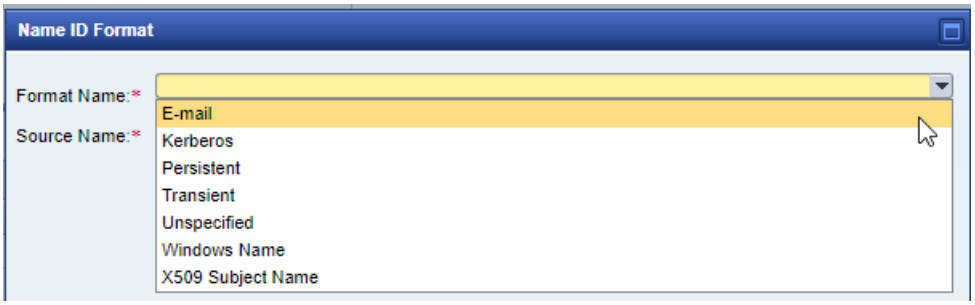
ステップ *3:* 名前 *ID* 設定

アプリケーションの設定完了後、**名前 ID** を設定する必要があります。**名前 ID** は、SAP Concur で従業員に登録したログイン ID (**CTE ログイン名**) と一致する必要があります。また、**名前 ID** の形式を「**メール アドレス**」に設定することを強くお勧めします。これは concursolutions.com またはモバイル アプリから開始する SP-Initiated ログインを行うために SAP Concur で必要になります。

1. **名前 ID** 形式を設定するには、新しいアプリケーションを検索してクリックし、次に **[Edit]** をクリックします



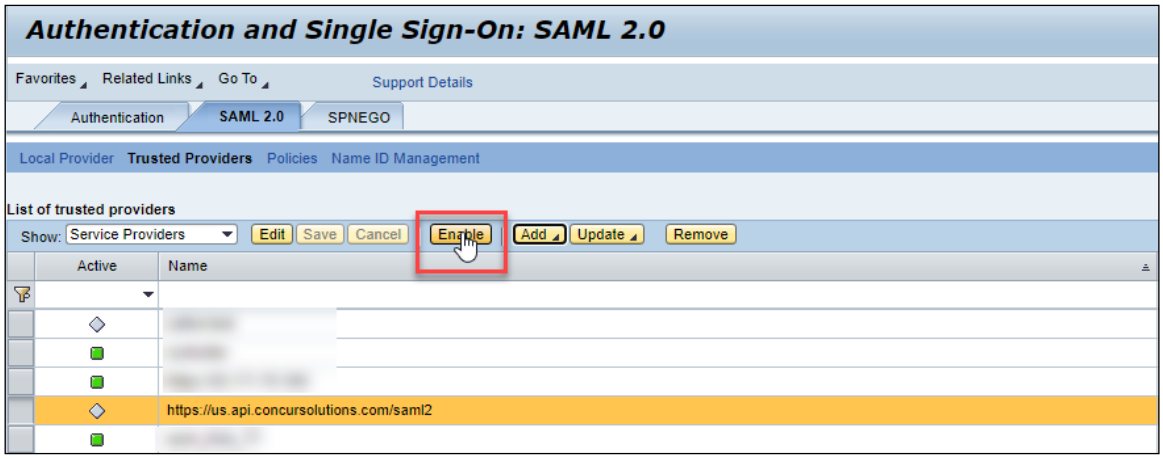
2. [Name ID Format] ポップアップで、必ず **[E-mail]** を選択します。**[Source Name]** に SAP Concur の従業員ログイン ID と一致する属性を入力します。



3. 場合によっては、指定可能な Source Name は SAP Concur のユーザー名と一致しないことがあります。このような場合、SAP Concur で従業員インポートを実行し、ユーザー名が送信する属性と一致しているかどうかを確かめることができます。または、SAP NetWeaver の製品サポートに連絡し、名前 ID 設定のサポートを要請することができます。

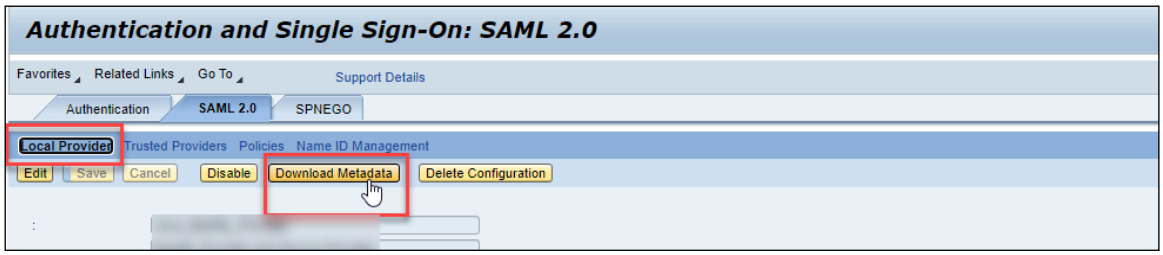
ステップ *4:* アプリケーションを有効化する

名前 ID を設定したら、[SAML 2.0] タブに戻ることができます。新しいアプリケーションを選択して、**[Enable]** をクリックします。これにより **[Active]** 列のアイコンが緑の四角に変わり、アプリケーションが有効であることを示します。



ステップ *5:* メタデータ ファイルをダウンロードする

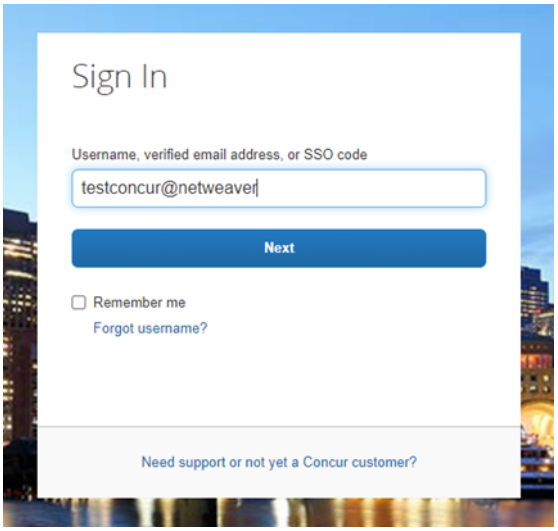
SAP Concur 側で設定を完了するには、SAP Netweaver のアプリケーションから抽出したメタデータ ファイルをアップロードします。**[SAML 2.0]** タブで **[Local Provider]** に移動し、**[Download Metadata]** をクリックしてメタデータ xml をダウンロードします。

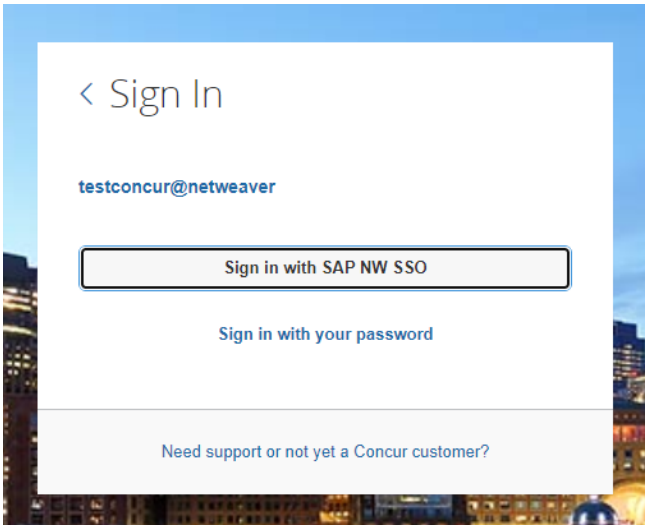


SAP Concur サイトを設定する

1. 「概要」セクションに記載されたステップに従って **[SSO の管理]** ページに移動します。
2. **[IdP メタデータ]** セクションで **[追加]** をクリックします。
3. **[IdP 接続]** に適切な名前を入力し、その名前を **[カスタム IdP 名]** フィールドに入力します。

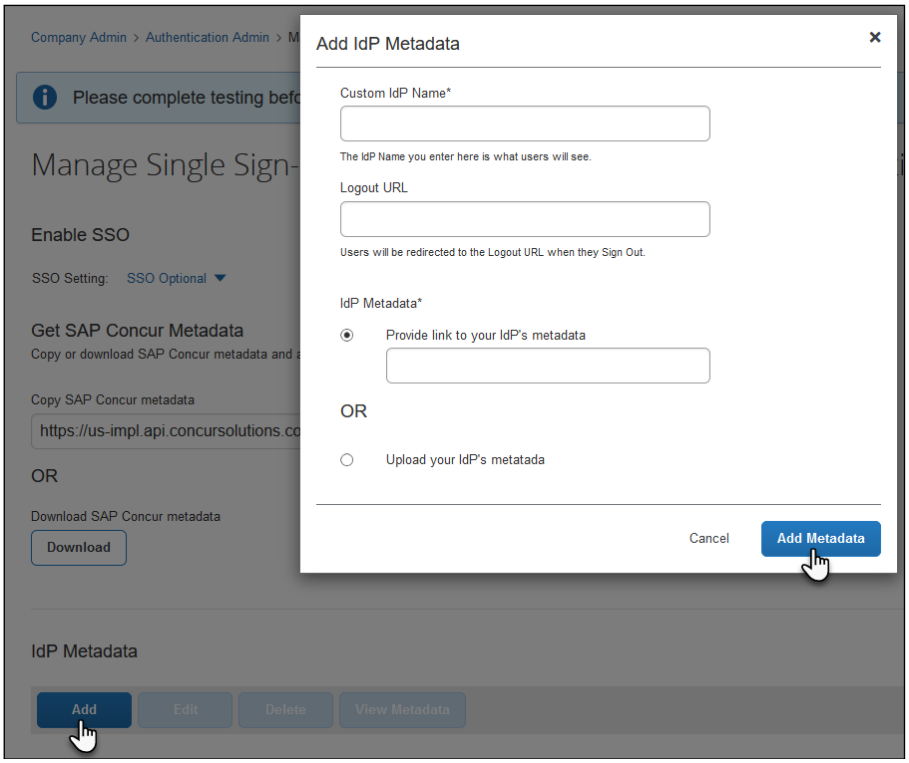
NOTE: SP-initiated フローを使用することにした場合（SAP Concur 公式サイト: https://www.concursolutions.com/nui/signin を利用）、ユーザー名を入力し **[次へ]** をクリックすると、 **[サインイン]** ページに **[カスタム IdP 名]** が表示されます。たとえば、**カスタム IdP 名**が「SAP NW」の場合、すべてのユーザーに [SAP NW でサインイン] オプションが表示されます。



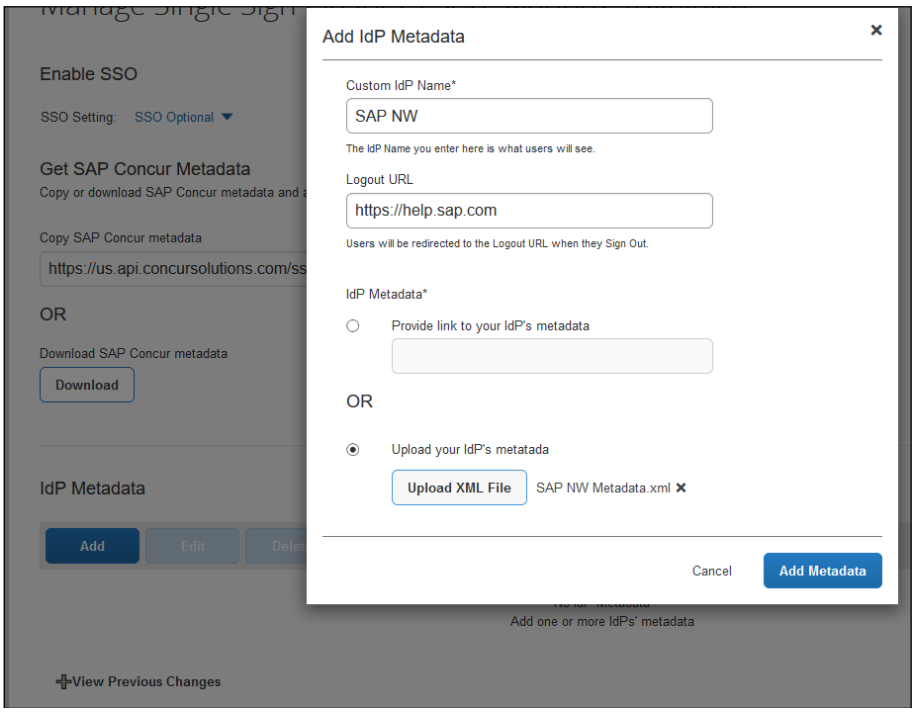


4. ユーザーがログアウトした際にほかの場所にリダイレクトされるようにログアウト URL（オプション）を入力します。既定では、URL が入力されない場合、ユーザーは認証プロセスを開始した場所にリダイレクトされます。SAP NetWeaver のログアウト エンドポイントは **[Local Provider] > [Identity Provider Settings] > [Single Log-Out Service (SLO)] > [Endpoint URL]** で確認できます。**Single Logout (SLO)** は SAP Concur で正式にサポートされていないため、SAP Concur に加えて IDP からユーザーを切断することに関しては、SLO エンドポイントを使用するログアウト プロセスは期待どおりに動作しない可能性があります。そのような場合、ユーザーは SAP Concur からログアウトされますが、SAP NetWeaver からは完全にログアウトされない場合があります。

5. **[IdP Metadata]** で、IdP メタデータのリンクを入力するか、事前にローカルに保存した、IdP メタデータを含む XML ファイルをアップロードできます。

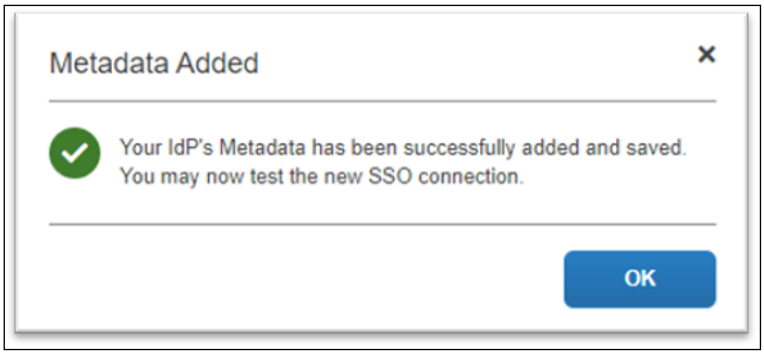


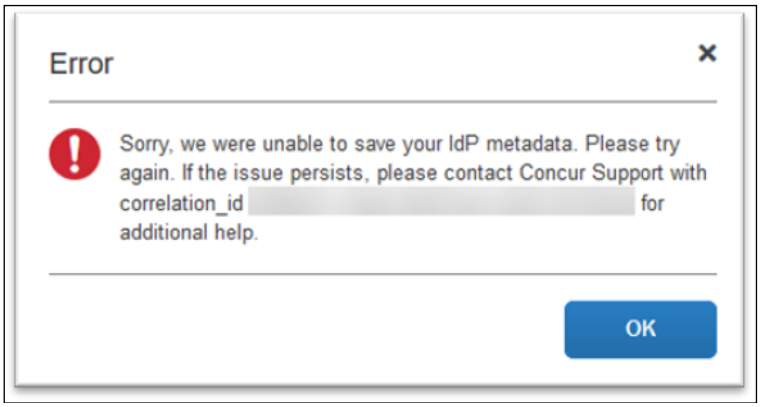
すべての詳細を入力すると、次のように表示されます。



6. **[メタデータの追加]** をクリックします。

7. 追加の成功を示す確認メッセージまたは問題の発生を示すメッセージが表示されます。後者の場合、SAP Concur サポートに連絡し、相関 ID を提供してください。





SSO ログインをテストする

前述のステップで IdP メタデータが SAP Concur に正常にアップロードされると、SSO のテストを開始できます。このセクションでは、IdP-Initiated（アイデンティティ プロバイダ側で開始される）フローおよび SP-Initiated（サービス プロバイダ側で開始される）フローをテストすることができます。

IdP-initiated SSO のテスト

IdP-initiated SSO をテストするには:

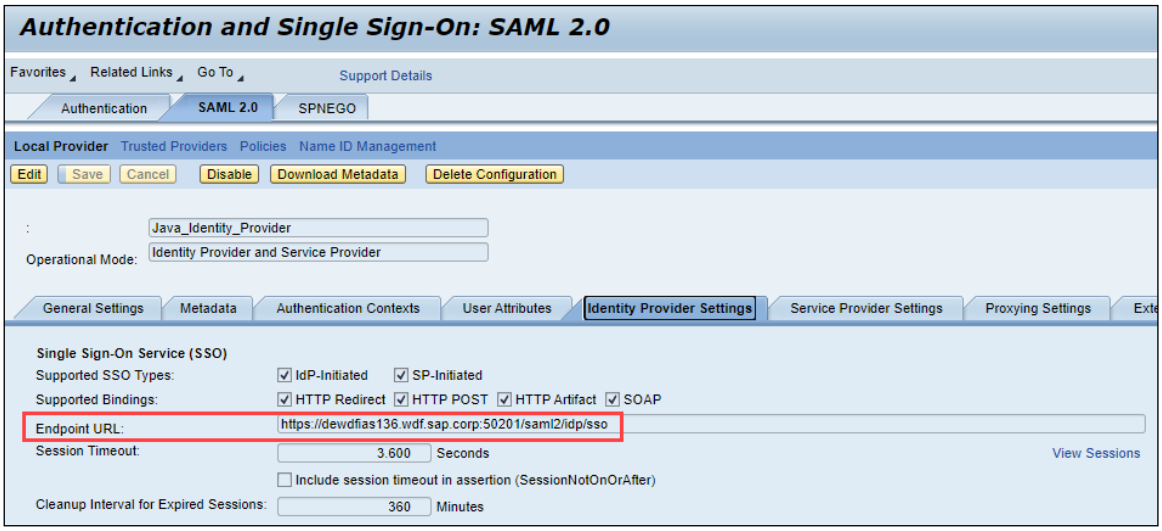
1. IdP-Initiated フローで、アイデンティティ プロバイダ側でログイン プロセスを開始します。テストを行うには、先ほど作成したアプリケーションのパラメーターを SAP NetWeaver の SSO エンドポイントに付加します。IdP-Initiated URL の形式の例は次のようになります。

   形式: [**SSO エンドポイント URL***]?saml2sp=[**SP 識別子****]

   例:
   https://idp.example.com:50001/saml2/idp/sso?saml2sp=**https://us.api.concursolutions.com/saml2**

   ****SP 識別子**: この値は SAP Concur メタデータから取得できます。**エンティティ ID** または **Audience** と同じです。

*__SSO Endpoint URL__: __[SAML 2.0] > [Local Provider] > [Identity Provider Settings] > [Single Sign-On Service (SSO)] > [Endpoint URL]__ のパスからこの値を入力できます。



この URL は SAP NetWeaver 側のログイン ページにダイレクトします。資格情報を使用してログインすると、SAP Concur ホームページにリダイレクトされます。

SP-Initiated SSO をテストする

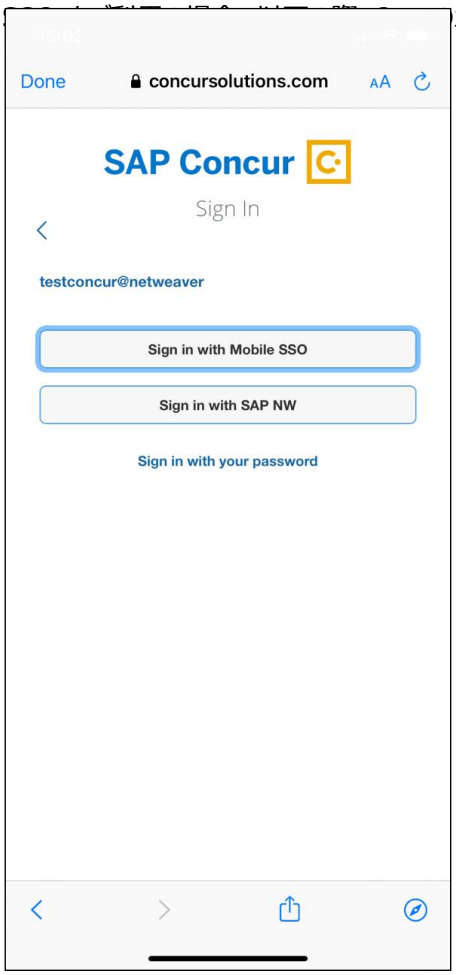
SP-Initiated SSO をテストするには

1. テストを行いたい環境のログイン ページを開きます。
   - US DC Prod: https://www.concursolutions.com/
   - US DC Test: https://implementation.concursolutions.com/
   - EMEA DC Prod: https://eu1.concursolutions.com/
   - EMEA DC Test: https://eu1imp.concursolutions.com/
   - CN DC Prod: https://www.concurcdc.cn/
2. ログイン ページでユーザー名、照合済メール アドレス、または SSO コードを追加して続行できます。**[次へ]** をクリックすると、「SAP Concur サイトを設定する」の注記のとおり、最近作成した SSO 設定のオプションが表示されます。クリックして、SAP Concur にリダイレクトするアイデンティティ プロバイダ アカウントの認証を続行します。

モバイル シングル サインオン（SSO）

SAMLv2 プラットフォームで作成された SSO 設定の場合、モバイル SSO はメタデータが保存されるとすぐに自動的に有効にされます。ただし、このオプションが機能するには、SP-Initiated フローが機能している必要があります。これは、前述の「SSO ログインをテストする」セクションを使用して検証することができます。

NOTE: モバイル SSO の自動有効化は、アプリのバージョンが 9.86 以降であり、かつ、ユーザーが新しいサインイン操作を選択している場合のみ表示されます。このオプションは旧バージョンのユーザー、または以前のサインイン操作を選択しているユーザーには自動的に非表示になります。もし以前に他の IdP をお使いで既にモバイル [illegible] オプションが表示される可能性があります。



[モバイル SSO でサインイン] オプションにより以前の IdP リンクが埋め込まれるため、ユーザーは以前の SSO 接続にリダイレクトされます。

いずれの場合も、SAP Concur サポート チームにチケットを作成し、次の情報を提供してください。

- ユーザーが以前のバージョンを使用する予定の場合、当該アプリ バージョンにモバイル SSO を有効化できるように、SAP NetWeaver 側で作成したアプリケーションの IdP-Initiated URL を SAP Concur サポートに提供してください。URL の入手方法に関する詳細については、このガイドの「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。
- 混乱する可能性を排除するために **[モバイル SSO でサインイン]** オプションを削除する場合、サポート チームにご連絡ください。

モバイル アプリで SSO を使用する認証時に問題がある場合、SAP Concur サポート チームにチケットを作成し、表示されたエラー ID やメッセージをスクリーンショットと一緒に提供してください。

メール通知

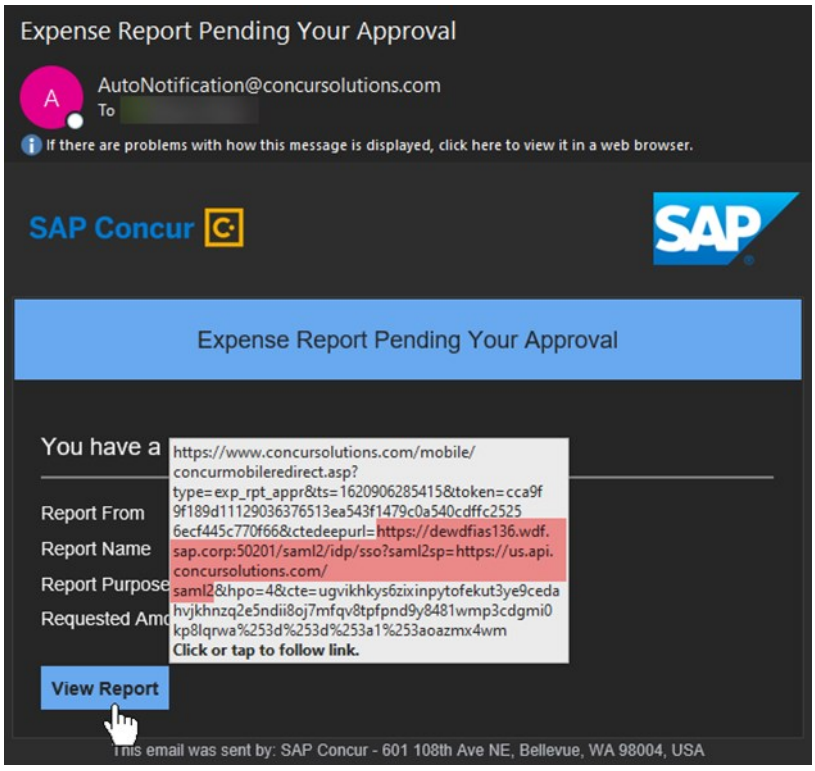
備忘メールに SSO URL を反映する設定は、SAP Concur サポートで完了する必要のある変更です。設定を進めるには、SAP Concur サポート チームにチケットを作成し、サポート チームが備忘メールのリダイレクト URL を調整できるように、IDP 側で作成したアプリケーションの IDP URL を提供します。URL の入手方法に関する詳細については、この付録の「SSO ログインをテストする」セクションの「IdP-Initiated SSO のテスト」を参照してください。

NOTE: URL は **[レポートの表示]** ボタンに埋め込まれて表示されます。

NOTE: この変更は変更後に生成されたメールにのみ反映されます。変更前に生成されたすべてのメールは以前の URL を引き続き使用します。

NOTE: この変更は反映されるまで最大 4 時間程度かかります。

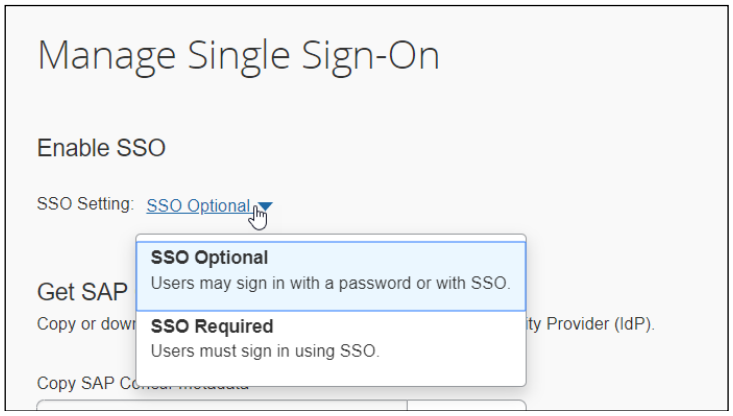
[レポートの表示] ボタンにカーソルを乗せると、現在挿入されている URL が表示されます。URL は **ctedeepurl=** と **&hpo=** の間に表示されます。



展開

新しい SSO 設定をテストしたら、このアクセスが必要なすべてのユーザーおよびグループに新しい SAP NetWeaver アプリケーションを割り当てることで、展開の計画を立てることができます。

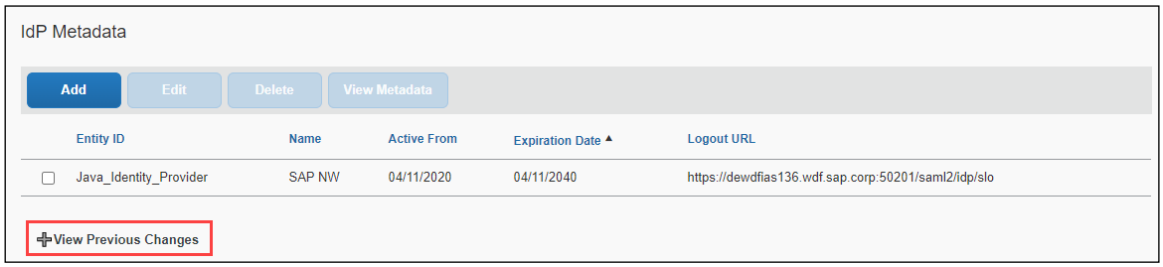
[SSO の管理] ページでは、SSO 設定を [SSO 任意] から **[SSO 必須]** に変更するとこの新しい SSO 接続を強制するオプションも提供しています。この設定を変更する場合、ユーザーは SP-initiated フローからユーザー名を提供すると SAP Concur にリダイレクトされるようになります。



以前の変更を表示

この機能は、**[SSO の管理]** ページで完了したすべての変更を管理者が追跡できるようにするために開発されました。

現時点までに行われた SSO 構成への変更を表示するには、**[以前の変更を表示]** をクリックします。

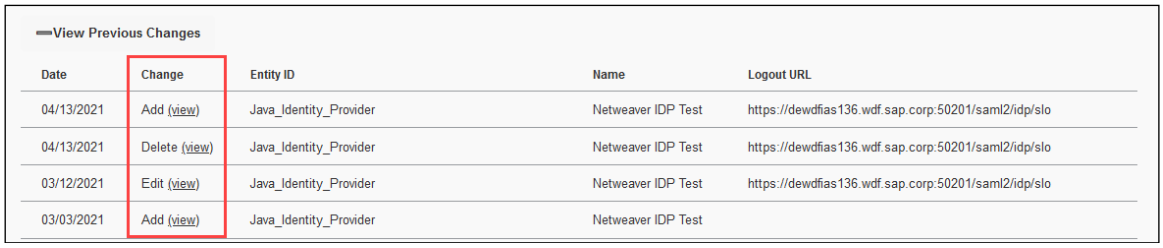


以前の変更が記載された表が表示され、日付と時刻の降順で並べ替えられています。

テーブルには、過去に行われた 100 件の変更が表示されます。テーブルにリストされる変更内容としては、以下のようなものが含まれます。

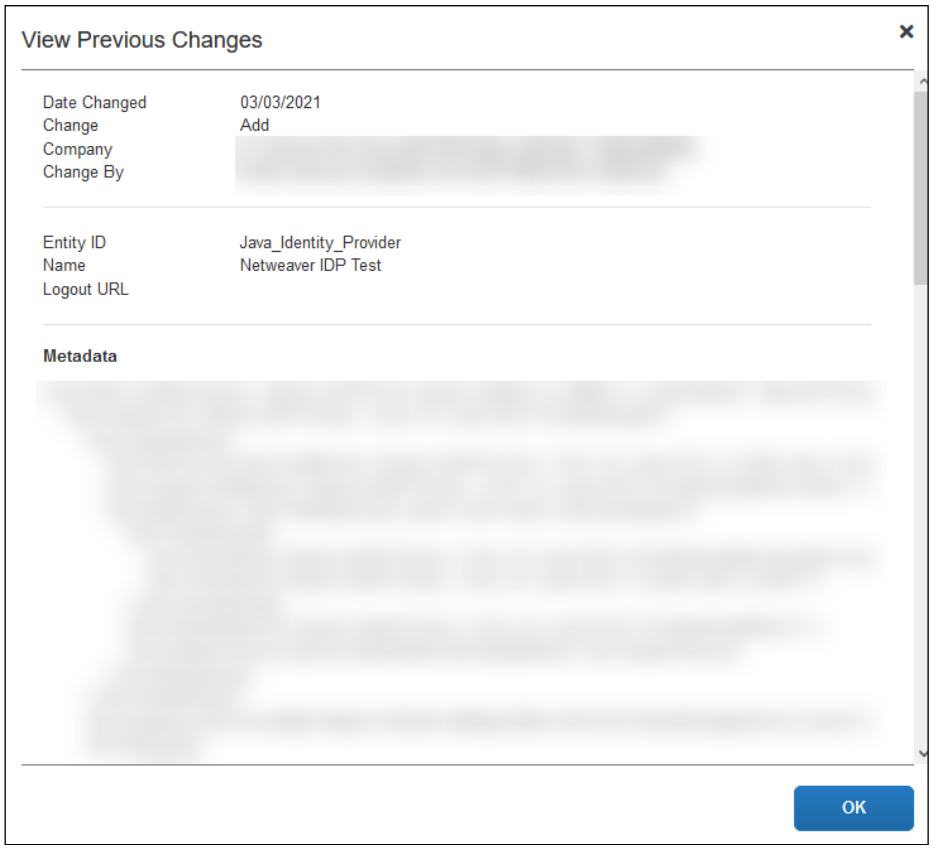
- 設定の追加
- 設定の削除
- [カスタム IdP 名] または [ログアウト URL] フィールドの編集

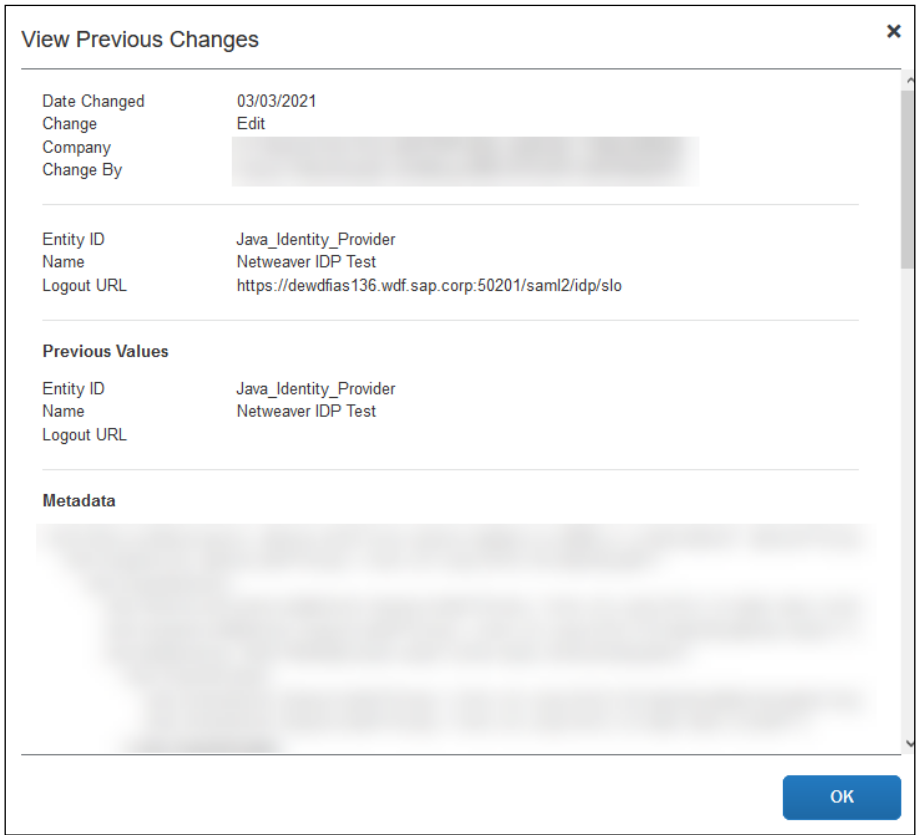
テーブルに一覧表示されている特定の変更に関する詳細情報を表示するには、目的のリスト項目の **[表示]** リンクをクリックします。



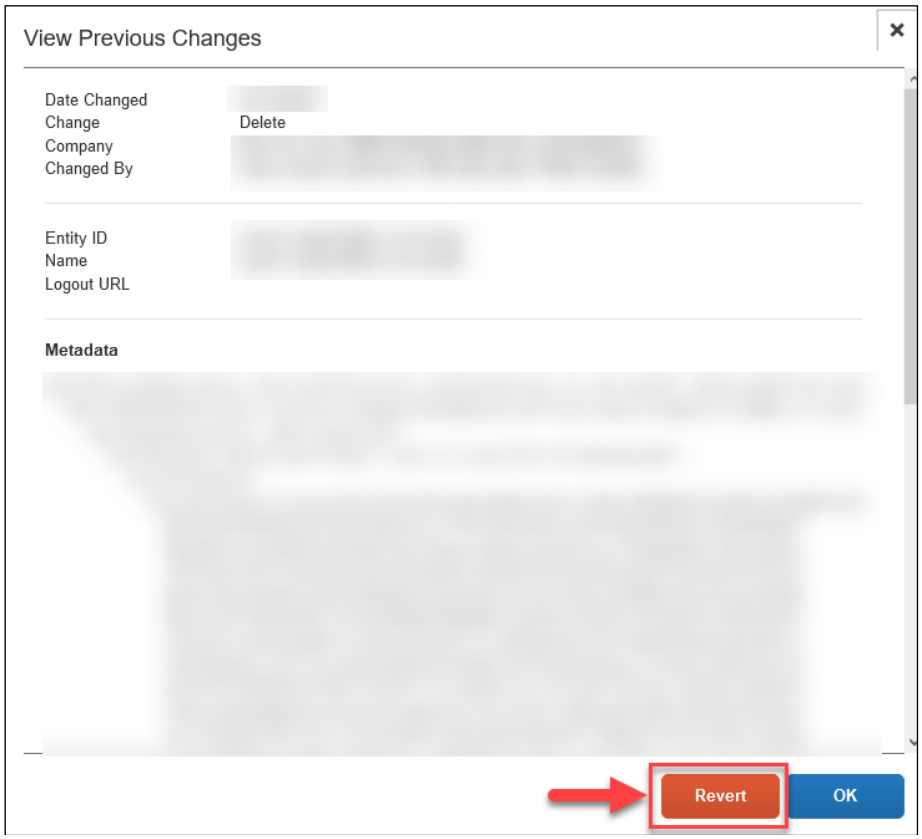
各ログの内部では、**[会社]** および **[変更者]** フィールドが [first_name last_name] [(UUID code)] 形式で表示されます。これは、そのアクションを行ったユーザーを参照しています。そのユーザーに見覚えがない場合、サポートに問い合わせて、詳細をリクエストすることができます。

ログの例:





設定が削除されている場合、この設定を復元するための **[元に戻す]** ボタンが **[変更履歴の表示]** ページに表示されます。設定が復元されると、この設定をサインイン プロセス中にユーザーが使用できるようになります。



📖 さらに詳しい情報は、次の文書をご参照ください。

- SAP Concur - SSO 概要
- SAP Help Portal - SAP シングル サインオン
- SAP Help Portal - Configuring AS Java as a Service Provider
- SAP Help Portal - Identity Provider Implementation Guide (HTML)