

Shared: Single Sign-On Setup Guide

Last Revised: January 22, 2024

Applies to these SAP Concur solutions:

- Expense
 - Professional/Premium edition
 - Standard edition

- Travel
 - Professional/Premium edition
 - Standard edition

- Invoice
 - Professional/Premium edition
 - Standard edition

- Request
 - Professional/Premium edition
 - Standard edition

Table of Contents

Section 1: Permissions	1
Section 2: Overview	1
Feature Benefits	1
Requirement.....	2
Section 3: Obtaining Required Permissions	2
Professional Edition Customers with Concur Travel	2
Professional Edition Customers Without Concur Travel; All Standard Edition Customers	2
Section 4: Configuration – Two Methods for Web-Based Services	2
Important!.....	3
Identity Provider (IdP)-Specific Process.....	3
General Process	4
Section 5: Configuration for Web-Based Services – General Process	4
Access the Manage Single Sign-On Page	4
Configure an SSO App/Connector Without Encryption	6
Step 1: Obtain the EntityID and ACS Endpoint	6
Step 2: Provide the EntityID and ACS Endpoint	7
Step 3: Provide the Recipient URL and Destination URL	8
Step 4: Ensure the NameID (IdP) Matches the User Login_ID (SAP Concur Solutions).....	9
Step 5: Obtain the IdP Metadata.....	10
Step 6: Upload IdP Metadata to Concur	11
Step 7: Test IdP-Initiated SSO	15
Step 8: Test SP-Initiated SSO	17
Step 9: Enable SSO as Optional or Required	17
Editing SSO Configurations	18
View Previous Changes.....	19
Configure an SSO App/Connector with Encryption (Optional)	25
Step 1: Obtain and Save the Encryption Key	25
Step 2: Upload the encryption.crt to Your IdP.....	27
Section 6: FAQ	27
Section 7: Appendix - ADFS Setup	29
Getting Started	29
Configure Your ADFS Application	31
Configure Your SAP Concur Site	40
Test SSO Login	43
Testing IdP-Initiated SSO	43
Test SP-initiated SSO	43
Mobile Single Sign-On (SSO)	45
E-mail Notifications.....	45
Rollout	45
Section 8: Appendix - Microsoft Azure AD Setup	46
Getting Started	46
Configure Your Azure AD Application.....	48
Step 1: Create Gallery Application	48

Step 2: Provide Azure ID with Identifier and Reply URL	49
Step 3: Change Unique User Identifier	51
Step 5: Download the Azure AD Metadata File	51
Configure Your SAP Concur Site	52
Test SSO Login	56
Test IdP-initiated SSO	56
Test SP-initiated SSO	57
Mobile Single Sign-On (SSO)	59
E-mail Notifications.....	59
Rollout	59
Section 9: Appendix – Google Workspace Setup	60
Overview	60
SAP Concur Professional edition:	60
SAP Concur Standard edition:	61
Configure Your Google Workspace (IDP) APP	62
Step 1: Get the SAP Concur metadata	62
Step 2: Set up your own custom SAP Concur SAML app.....	62
Step 3: Turn on your SAML app.....	64
Step 4: Configure Your SAP Concur Site	64
Test SSO Login	66
Mobile Single Sign-On (SSO)	67
E-Mail Notifications	68
Rollout	69
View Previous Changes	70
Section 10: Appendix - Idaptive Setup	72
Getting Started	72
Configure Your Idaptive Application	74
Step 1: Create the Idaptive app	74
Configure Your SAP Concur Site	78
Test SSO Login	79
Test IdP-initiated SSO	79
Test SP-initiated SSO	79
Mobile Single Sign-On (SSO)	81
E-mail Notifications.....	81
Rollout	82
Section 11: Appendix - Okta Setup	82
Getting Started	82
Configure Your Okta Application	84
Step 1: Get the SAP Concur metadata	84
Step 2: Create an application on Okta	86
Step 3: Name ID configuration	88
Step 4: (Optional) Encrypting the application	89
Step 5: Finish the Configuration	93
Step 6: Download the Metadata File	93
Configure Your SAP Concur Site	94
Test SSO Login	97
Test IdP-initiated SSO	97
Test SP-initiated SSO	97

Mobile Single Sign-On (SSO)	98
E-mail Notifications.....	99
Rollout	100
View Previous Changes	101
Section 12: Appendix - PingOne Setup	101
Getting Started	101
Configure Your PingOne Application	103
Step 1: Create a non-gallery SAML application	103
Step 2: Application details	104
Step 3: Application configuration	105
Step 4: Attribute Mapping.....	106
Step 5: Provide access to user groups.....	107
Step 6: Review and finish	108
Configure Your SAP Concur Site	108
Test SSO Login	109
Testing IdP-initiated SSO	109
Testing SP-initiated SSO.....	110
Mobile Single Sign-On (SSO)	111
E-mail Notifications.....	111
Rollout	111
Section 13: Appendix - SAP Cloud Identity Services - Identity Authentication Service (SAP IAS) Setup.....	114
Getting Started	114
Configure Your SAP IAS Application	117
Step 1: Get the SAP Concur metadata.....	117
Step 2: Create an Application on SAP IAS	118
Step 3: Change Subject Name Identifier.....	121
Step 4: Change Default Name ID Format.....	123
Step 5: Download the metadata	124
Configure Your SAP Concur Site	126
Test SSO Login	128
Testing IdP-initiated SSO	128
Testing SP-initiated SSO.....	129
Mobile Single Sign-On (SSO)	129
E-mail Notifications.....	130
Rollout	132
View Previous Changes	133
Section 14: Appendix - SAP NetWeaver Setup.....	135
Overview.....	135
Configure Your SAP Netweaver Application	138
Step 1: Get the SAP Concur metadata.....	138
Step 2: Create an application on SAP Netweaver	139
Step 3: Name ID configuration	142
Step 4: Enabling the application	143
Step 5: Download the Metadata File	144
Configure Your SAP Concur Site	144
Test SSO Login	146
Test IdP-initiated SSO	146

Test SP-initiated SSO	147
Mobile Single Sign-On (SSO)	148
E-mail Notifications.....	149
Rollout	150
View Previous Changes	151
Section 15: Appendix – Google Workspace Setup.....	153
Overview.....	153
SAP Concur Professional edition:	154
SAP Concur Standard edition:	155
Configure Your Google Workspace (IDP) APP	155
Step 1: Get the SAP Concur metadata	155
Step 2: Set up your own custom SAP Concur SAML app.....	156
Step 3: Turn on your SAML app.....	157
Step 4: Configure Your SAP Concur Site	158
Test SSO Login	160
Mobile Single Sign-On (SSO)	160
E-Mail Notifications	161
Rollout	162
View Previous Changes	163

Revision History

Date	Notes/Comments/Changes
January 22, 2024	Updated bullet 2 in Getting Started in Section 13.
December 19, 2023	Updated Section 13 Appendix.
June 21, 2022	Updated <i>Configure Your SAP Concur Site</i> and <i>View Previous Changes</i> sections throughout
May 18, 2022	Updated <i>Appendix – ADFS Setup</i> .
March 21, 2022	Added a comma to the last revised date and fixed a formatting issue. No cover date change.
February 28, 2022	Added setup instructions for Google Workspace to the appendices
January 19, 2022	Updated instruction in the <i>Upload IdP Metadata to Concur</i> topic under the <i>Configuration for Web-Based Services – General Process</i> section
July 27, 2021	Added several appendices with setup instructions for SSO
April 15, 2021	Updated the copyright year; no other changes; cover date not updated
March 26, 2021	Added information about the new “View Previous Changes” feature
December 2, 2020	Fixed a typo. No cover date change
November 14, 2020	Initial publication

SSO Management

NOTE: Multiple SAP Concur product versions and UI themes are available, so this content might contain images or procedures that do not precisely match your implementation. For example, when SAP Fiori UI themes are implemented, home page navigation is consolidated under the SAP Concur Home menu.

Section 1: Permissions

This feature requires company administrator permissions.

The administrator should be aware that some of the tasks described in this guide can be completed only by SAP Concur support. In these cases, the customer must initiate a service request with SAP Concur support.

Section 2: Overview

Single Sign-On (SSO) allows users to access multiple applications using one set of sign-in credentials. The Manage Single Sign-On (SSO) feature provides SAP Concur customers with a self-service option for setting up SSO.

Currently, SAP Concur solutions has two methods for signing in to SAP Concur services: with a username and password **or** using SSO with identity provider (IdP) credentials, such as a user's sign-in credentials for their organization. SSO is currently supported for Concur Expense, Concur Invoice, Concur Request, and Concur Travel.

By configuring this feature, customers can set up single sign-on for users at their organization.

Feature Benefits

The Manage Single Sign-On feature provides the following:

- A self-service option that enables a company admin to set up both IdP-initiated and SP-initiated SSO at their organization on both web and mobile platforms
- The ability for a company that currently uses the existing SSO functionality to also use the new Manage Single Sign-On feature (both SSO options work concurrently)
- The ability to require SSO for all users
- Improvements to the user sign-in experience
- A higher sign-in success rate for users

This guide describes how to enable and configure the Manage Single Sign-On feature for SAP Concur services.

Requirement

To use this feature, customers must have an IdP (Identity Provider) that supports the SAML 2.0 standard and can generate IdP metadata.

Section 3: Obtaining Required Permissions

To access the **Manage Single Sign-On** page, a user must be assigned the Company Administration (Travel) permission.

After the required permission has been assigned to the user, they can access the **Manage Single Sign-On** page. The method for navigating to the page differs between SAP Concur Professional and Standard editions.



For instructions on how to access the page in SAP Concur Professional and Standard editions, see *Access the Manage Single Sign-On Page* in Section 5 of this document.

Professional Edition Customers with Concur Travel

For Professional Edition customers who have Concur Travel, the **Authentication Admin** menu automatically appears for all users who have the Company Administration (Travel) permission.

To provide access to additional users, the customer can assign the Company Administration (Travel) permission using **Administration > Company > Company Admin > User Permissions** (left menu) and then click the **Travel** tab.



For more information about assigning roles and permissions, refer to the *Shared: User Administration User Guide*.

Professional Edition Customers Without Concur Travel; All Standard Edition Customers

For Professional Edition customers who do not have Concur Travel and for Standard Edition customers, call SAP Concur support for assistance obtaining the required permissions. SAP Concur support will assign the permissions to the desired users.

Section 4: Configuration – Two Methods for Web-Based Services

There are two ways to configure SSO:

- Follow the Identity Provider (IdP)-specific process
- or –
- Follow the general process (described below)

Important!

Both methods are detailed below. However, **every admin should review the information in the general processes.** In some cases, a step from the general process might be required, even if you have used the information provided by the IdP.

Identity Provider (IdP)-Specific Process

SAP Concur worked with several IdPs to develop a reliable integration process. If your company is using one of the following IdPs. The best way to set up SSO is to click the appropriate link in the table below and follow the instructions.

NOTE: For specific appendix instructions and links in the following table, as content is sourced from the third-party provider, SAP Concur cannot guarantee its accuracy. If you encounter issues, it is recommended that you contact the third-party provider's support resources.

Identity Provider	Setup URL
ADFS	Refer to the appendix in this guide.
Azure AD	Refer to the appendix in this guide. For further reference: https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/concur-travel-and-expense-tutorial
Idaptive	Refer to the appendix in this guide.
JumpCloud	https://jumpcloud-support.force.com/support/s/article/Single-Sign-On-SSO-with-Concur-Travel-and-Expense
Okta	Refer to the appendix in this guide. For further reference: https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Concur-Travel-and-Expense.html
OneLogin	<p>Choose one of these:</p> <ul style="list-style-type: none"> For SAP Concur customers in the US (North America) data center: https://{subdomain}.onelogin.com/apps/new/124919 For SAP Concur customers in the EMEA data center: https://{subdomain}.onelogin.com/apps/new/125208 For SAP Concur customers in the China data center: https://{subdomain}.onelogin.com/apps/new/127148 <p>Note the following:</p> <ul style="list-style-type: none"> Customers must add their OneLogin domain to the URL above as indicated. After the customer uses the URL above to add the SAP Concur app to OneLogin, they will see the Setup tab. They must access that tab for instructions about uploading the OneLogin metadata to SAP Concur.

Identity Provider	Setup URL
Ping Identity	Refer to the appendix in this guide.
SAP Identity Authentication Service (IAS)	Refer to the appendix in this guide.
SAP NetWeaver	Refer to the appendix in this guide.

General Process

If your company is using an IdP that is not listed in the table above, follow the appropriate procedure in *Section 5*. *Section 5* provides procedures for configuring the following:

- SSO app/connector **without** encryption
- SSO app/connector **with** encryption

Section 5: Configuration for Web-Based Services – General Process

Once the proper permissions are assigned, you can configure SSO. The following pages describe how to:

- Access the **Manage Single Sign-On** page.
- Configure an SSO App/Connector Without Encryption.
- Configure an SSO App/Connector With Encryption (Optional).

Access the Manage Single Sign-On Page

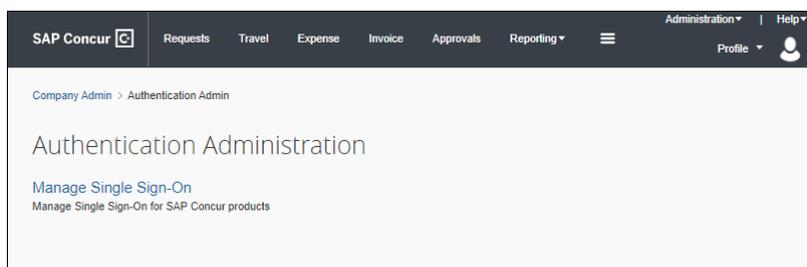
To access the **Manage Single Sign-On** page, a user must be assigned the Company Administration (Travel) permission.



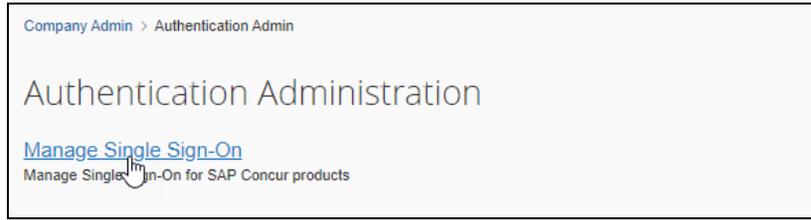
For information about obtaining the required permission, see *Section 3*.

▶ **To access the Manage Single Sign-On Page in Professional or Standard Edition:**

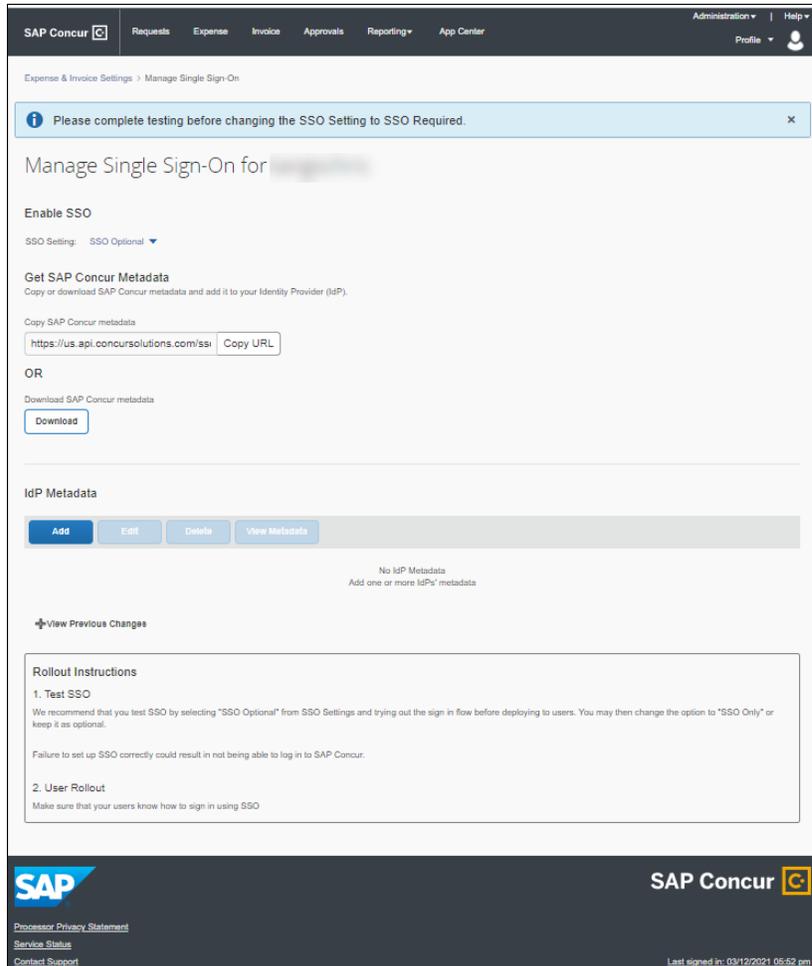
1. Click **Administration > Company > Authentication Admin**. The **Authentication Administration** page appears.



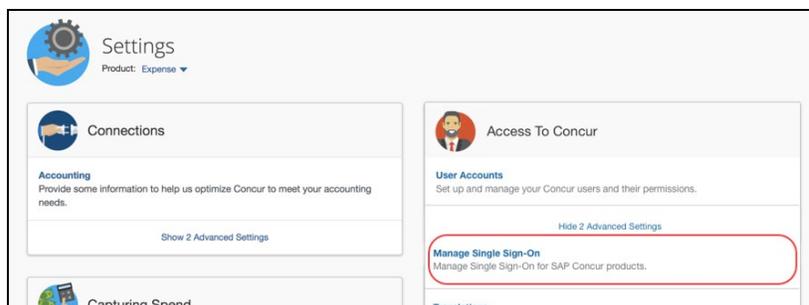
2. Click **Manage Single Sign-On**.



The **Manage Single Sign-On** page appears.



In SAP Concur Standard edition you can also access the **Manage Single Sign-On** page from Product Settings.



Configure an SSO App/Connector Without Encryption

Step 1 and Step 6 are completed in the SAP Concur service. Contact SAP Concur support for assistance.

Step 2 through Step 5 are completed in your IdP. If you have any questions, contact your Identity Provider for assistance.

Step 1: Obtain the EntityID and ACS Endpoint

The EntityID is a unique identifier of SAP Concur SSO; the ACS endpoint is the endpoint your IdP will use to POST SAML assertions to SAP Concur solutions. Both are required by the IdP.

You can obtain the EntityID and ACS endpoint by viewing the SAP Concur SP metadata. The metadata can be viewed by clicking the URL in this document for the appropriate region (data center) or through the **Manage Single Sign-On** page.

- ▶ **To Obtain the EntityID and ACS Endpoint by clicking the URL for the region in which your data center is located:**
 - Click the URL that follows for the region (data center) where your entity is hosted to view the SAP Concur SP metadata:

NOTE: Google Chrome is the recommended browser.

- ◆ **US (North America):** <https://www-us.api.concursolutions.com/sso/saml2/V1/sp/metadata/>
 - ◆ **EMEA:** <https://www-emea.api.concursolutions.com/sso/saml2/V1/sp/metadata/>
 - ◆ **China:** https://www-cn.api.concurcdc.cn/sso/saml2/V1/sp/metadata
- ▶ **To view the metadata from the Manage Single Sign-On page:**
 1. Click **Administration > Company > Authentication Admin**, and then click **Manage Single Sign-On**.

Different IdPs use different names for the EntityID and ACS Endpoint. The table below shows the field names for many popular IdPs.

IdP	Name for EntityID	Name for ACS Endpoint
Okta	Audience URI (SP EntityID)	Single sign on URL
Azure AD	Identifier (Entity ID)	Reply URL (Assertion Consumer Service URL)
OneLogin	Audience	ACS (Consumer) URL
Ping	SP entityID	ACS URL
JumpCloud	SP Entity ID / SP Issuer / Audience	Assertion Consumer Service (ACS) URL

If you are not sure where to add EntityID and ACS Endpoint, contact your Identity Provider for assistance.

Step 3: Provide the Recipient URL and Destination URL

Provide the Recipient URL and Destination URL to the custom app/connector in your IdP.

NOTE: This step is optional for some IdPs but required for others. If the IdP requires the Recipient URL and Destination URL, you can use the ACS Endpoint from the SAP Concur SP metadata to fill those fields.

Below are examples of how IdPs handle adding the Recipient URL and Destination URL.

For Okta, there is an option to use the ACS Endpoint as both Recipient URL and Destination URL.

The screenshot shows the 'GENERAL' configuration page for an application in Okta. It features two input fields and two checkboxes. The first input field is labeled 'Single sign on URL' and contains the URL 'https://us.api.concursolutions.com/sso/saml2/V1/acs/'. Below this field, the checkbox 'Use this for Recipient URL and Destination URL' is checked and highlighted with a red circle. The second checkbox, 'Allow this app to request other SSO URLs', is unchecked. The second input field is labeled 'Audience URI (SP Entity ID)' and contains the URL 'https://us.api.concursolutions.com'.

For OneLogin, there is a field to enter the Recipient URL (no destination URL option).

Application details	
RelayState	<input type="text"/>
Audience	<input type="text" value="https://us.api.concursolutions.com"/>
Recipient	<input type="text" value="https://us.api.concursolutions.com/sso/saml2/V1/acs/"/>
ACS (Consumer) URL Validator*	<input type="text" value="https://us.api.concursolutions.com/sso/saml2/V1/acs/"/>
	<small>*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest</small>
ACS (Consumer) URL*	<input type="text" value="https://us.api.concursolutions.com/sso/saml2/V1/acs/"/>
	<small>*Required</small>

Step 4: Ensure the NameID (IdP) Matches the User Login_ID (SAP Concur Solutions)

Make sure the value of the NameID field matches the SAP Concur user Login_ID. Your IdP will send a SAMLResponse XML file to SAP Concur solutions and within the SAMLResponse file there is a NameID field as shown in the following example:

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

SAP Concur matches username@domain.com from the NameID field to the Login_ID. If they do not match, the sign-in will fail because SAP Concur solutions will not be able to identify the correct user.

NOTE: If your email address at your IdP does not match the SAP Concur Login_ID, use a custom rule to construct an email address or username that matches Login_ID at Concur.

It is common for the email address from the IdP to be different from the Login_ID at SAP Concur. If this is the case for you, see the following examples of possible configurations on the IdP side:

For Okta:

- In the **Name ID format** field, select *EmailAddress*.
- In the **Application username** field, select *Email*.

Section 5: Configuration for Web-Based Services – General Process

GENERAL

Single sign on URL ?
 Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?
If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?
Update application username on

- Email
- Okta username
- Okta username prefix
- Email**
- Email prefix
- Custom
- (None)

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

For Azure AD, edit the **Unique User Identifier** field to *user.mail*.

2 User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.mail

If you are not sure how to configure the NameID field, contact your Identity Provider for assistance.

Step 5: Obtain the IdP Metadata

Your IdP generates an IdP metadata file or an IdP metadata link. Both are supported by SAP Concur solutions. Below are examples from Okta and Azure AD.

NOTE: For your IdP, if access to the metadata is not obvious, contact your IdP for assistance.

For Okta, use the **Identity Provider Metadata** link.

Settings
Edit

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Encryption Certificate concur.crt (CN=core-saml-prod.concur.com)

ⓘ

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

For Azure AD, use the **App Federation Metadata Url** link or the **Federation Metadata XML** download.

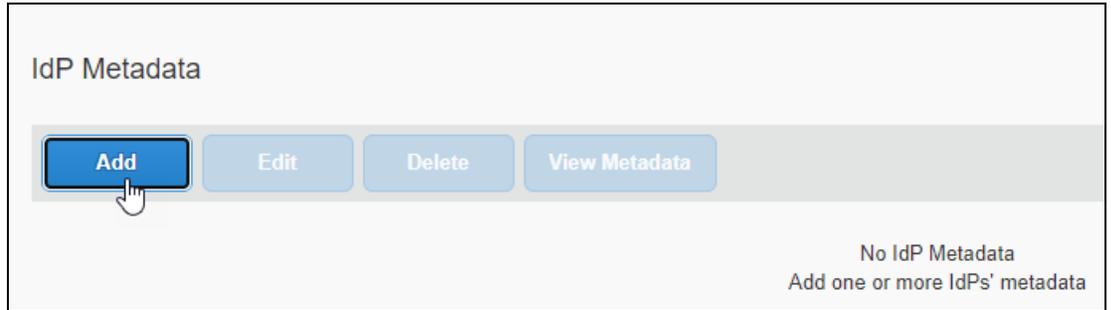
SAML Signing Certificate
✎

Status	Active
Thumbprint	668D07C8991F975A1BC07F403A617D8A48489A2E
Expiration	9/12/2022, 9:55:04 AM
Notification Email	concurcoretest@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/382a5a1c-567a-4... 📄
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

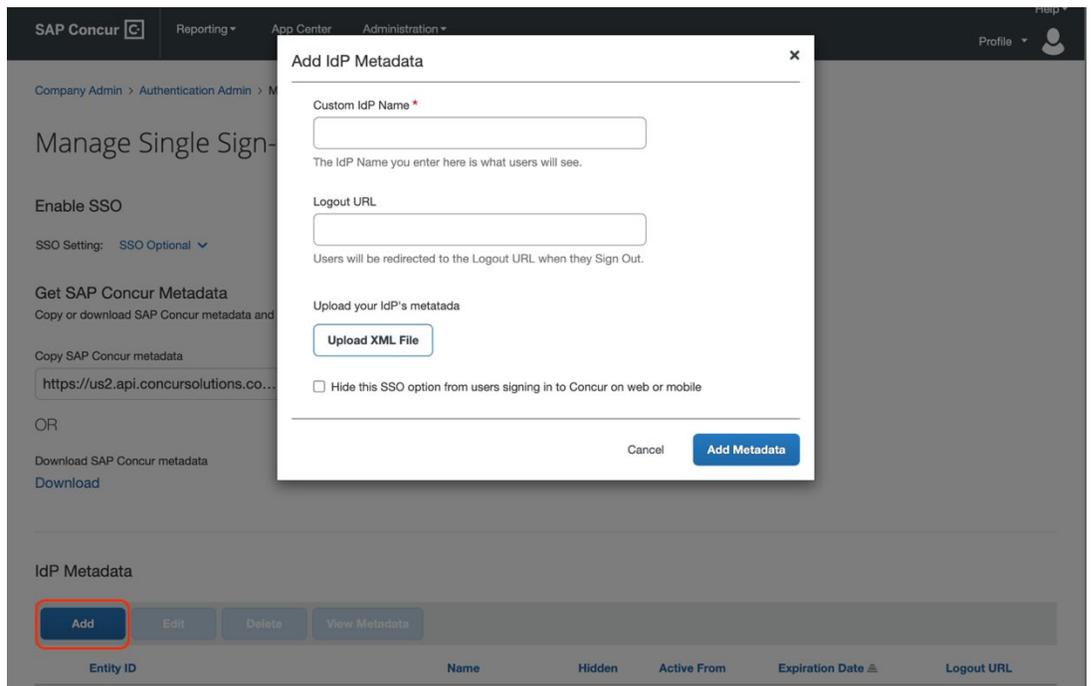
Step 6: Upload IdP Metadata to Concur

1. Click **Administration > Company > Authentication Admin**, and then click **Manage Single Sign-On**.

2. In the **IdP Metadata** section, click **Add**.

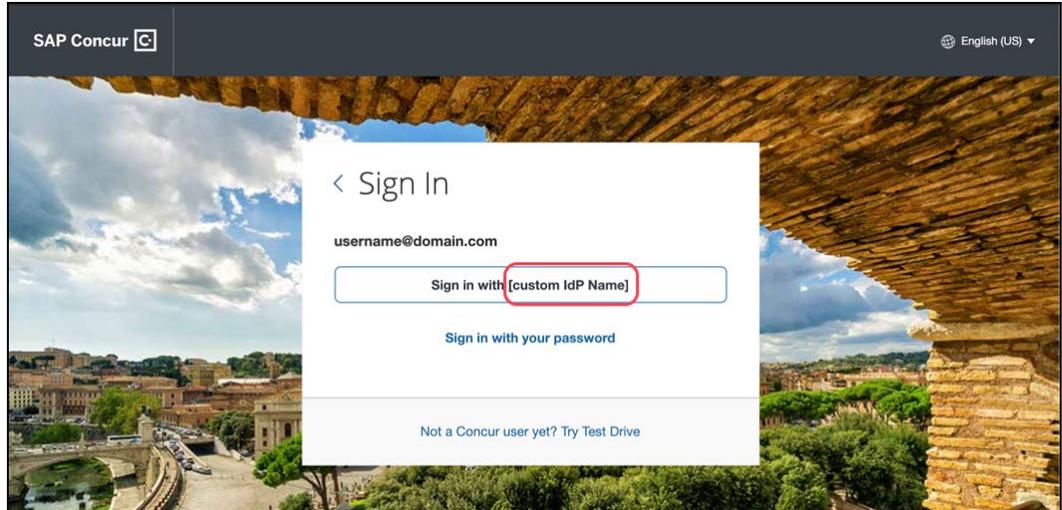


The **Add IdP Metadata** window appears.



3. In the **Custom IdP Name** field, enter a name.

The name you enter appears to users on the **Sign In** page. Best practice is to simply enter the IdP name. For example, if your IdP is Okta and if you enter *Okta* in this field, then the user will see *Sign in with Okta*.

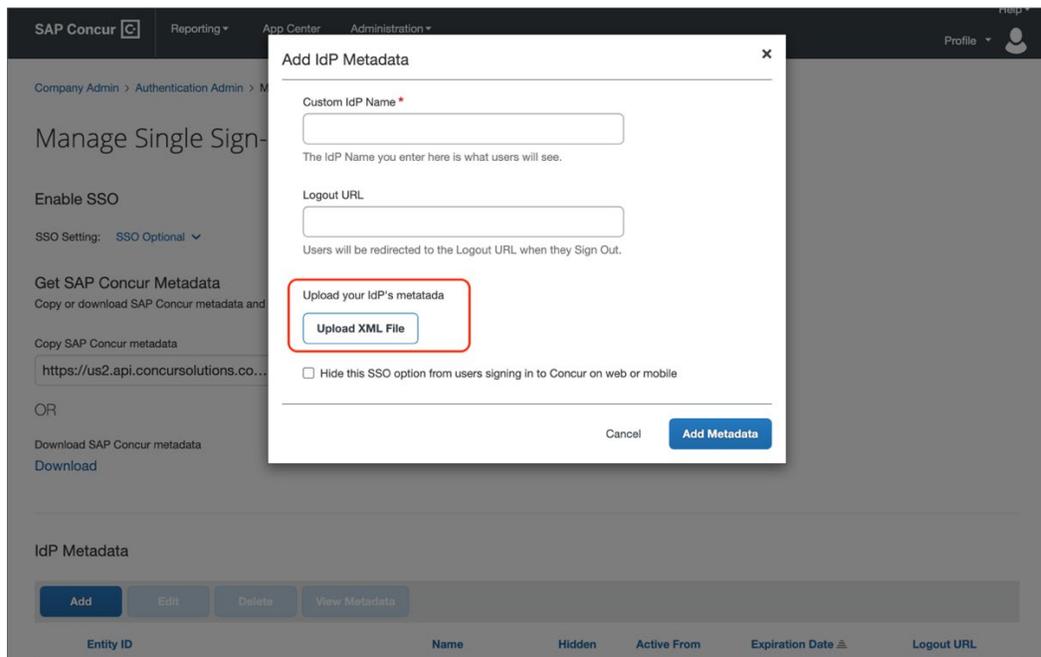


4. In the **Logout URL** field, enter a Logout URL.

By default, if no URL is entered, users will be redirected to where they started the authentication process upon sign out from SAP Concur.

If a custom Logout URL is specified, users are redirected to the specified URL when they sign out of SAP Concur solutions.

5. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP.



6. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox **Hide this SSO option from users signing in to Concur on web or mobile**.

Section 5: Configuration for Web-Based Services – General Process

By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.

The screenshot shows the 'Add IdP Metadata' dialog box. The 'Hide this SSO option from users signing in to Concur on web or mobile' checkbox is highlighted with a red box. The background shows the 'Manage Single Sign-On' configuration page with the following content:

Company Admin > Authentication Admin > Manage Single Sign-On

Manage Single Sign-On for Canonical Travel Test Company

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

Copy SAP Concur metadata

https://us2.api.concursolutions.com... Copy URL

OR

Download SAP Concur metadata

Download

IdP Metadata

Add Edit Delete View Metadata

Entity ID	Name	Hidden	Active From	Expiration Date	Logout URL
	SAML Monitor		09/30/2016	09/30/2026	
	muttals okta		02/27/2018	02/27/2028	
	Concur Okta	✓	02/27/2018	02/27/2028	

7. Click **Add Metadata**.

The screenshot shows the 'Manage Single Sign-On' configuration page. The 'Add Metadata' button is highlighted in the 'IdP Metadata' section. The background shows the 'Manage Single Sign-On' configuration page with the following content:

Company Admin > Authentication Admin > Manage Single Sign-On

Manage Single Sign-On for Canonical Travel Test Company

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

Copy SAP Concur metadata

Copy URL

OR

Download SAP Concur metadata

Download

IdP Metadata

Add Edit Delete View Metadata

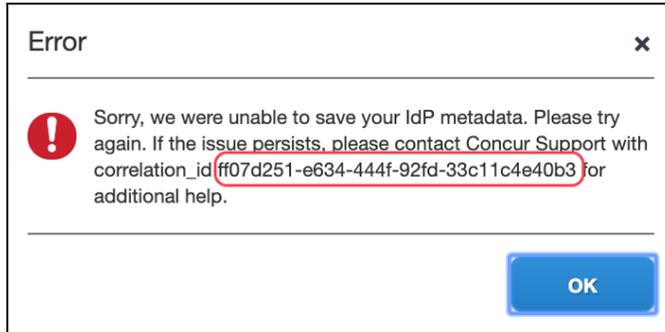
Entity ID	Name	Hidden	Active From	Expiration Date	Logout URL
	SAML Monitor		09/30/2016	09/30/2026	
	muttals okta		02/27/2018	02/27/2028	
	Concur Okta	✓	02/27/2018	02/27/2028	

View Previous Changes

The configuration will be added to the IdP Metadata table, which shows a summary of each configuration.

ERROR MESSAGE

If an error occurs, the following message appears.



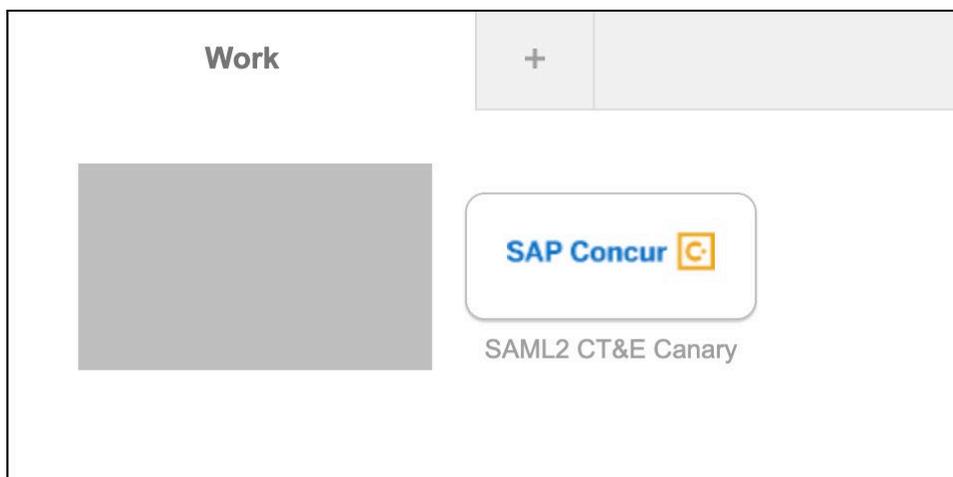
Save the correlation_id, contact SAP Concur support, and provide the correlation_id. SAP Concur support can look up the detailed error message and provide steps for troubleshooting the error.

Step 7: Test IdP-Initiated SSO

You must obtain the IdP-Initiated SSO URL from your Identity Provider. The location of the URL depends on your IdP. Below are examples of testing SSO on Okta and Azure AD. Your IdP will likely be similar.

After you obtain this IdP-Initiated SSO URL, you can paste the URL in the browser and try to sign in.

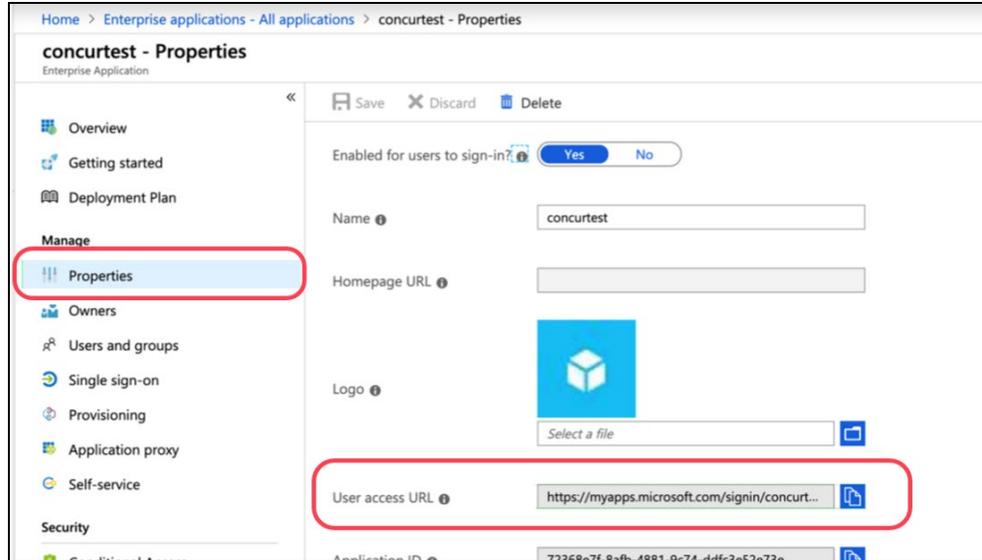
For Okta, click the app icon (embedded URL) in the Okta portal.



For Azure AD, use one of the following:

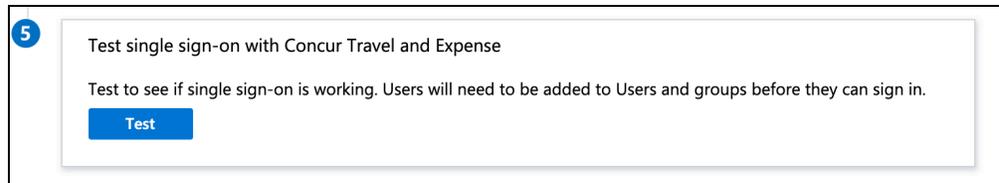
- **Properties > User access URL**

Section 5: Configuration for Web-Based Services – General Process



– OR –

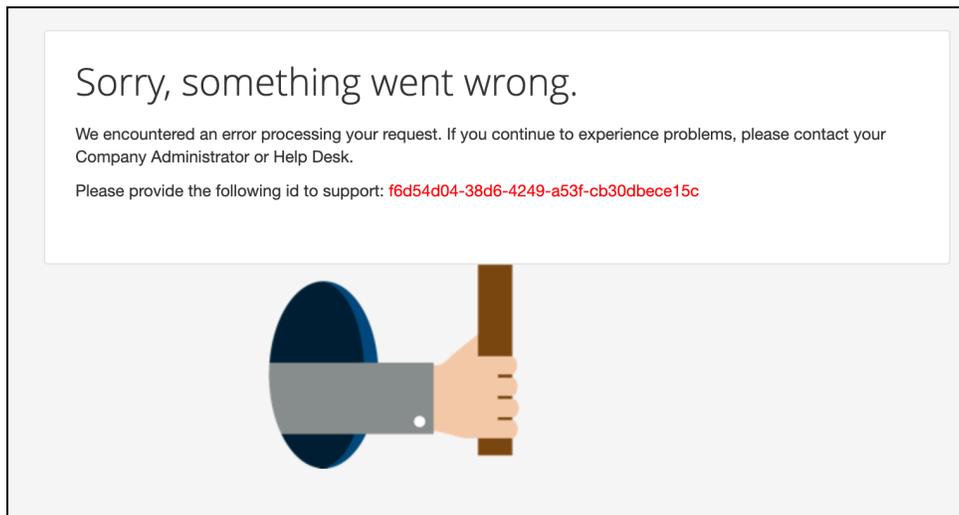
- **Test single sign-on with Concur Travel and Expense**



If you have questions about locating the IdP-Initiated SSO URL, contact your Identity Provider for assistance.

ERROR MESSAGE

If the SSO test sign-in fails, a message similar to the following appears.



The two most common causes are:

- The user does not exist in SAP Concur solutions.
- The Login_ID does not match between your IdP and SAP Concur user profile.

To determine the cause, do the following:

1. Use the SAMLtracer or the Inspect feature of the Chrome browser to locate the SAMLResponse. (Your IdP sends user information to SAP Concur solutions via SAMLResponse.)
2. Decode the SAMLResponse with base64decode tools. base64decode tools are readily available online.
3. Look for the value in the <saml2:NameID> field. For example:
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">username@domain.com</saml2:NameID>
4. Compare the value found in the <saml2:NameID> field (in the preceding example, username@domain.com) with the user's SAP Concur Login_ID.
 - ◆ If you cannot find a match, then you must first create a user with a matching SAP Concur Login_ID and then test again.
 - ◆ If you do find the user and the user's SAP Concur Login_ID matches the user's Login_ID at your IdP, contact SAP Concur support and provide the error ID that appears in the error message.

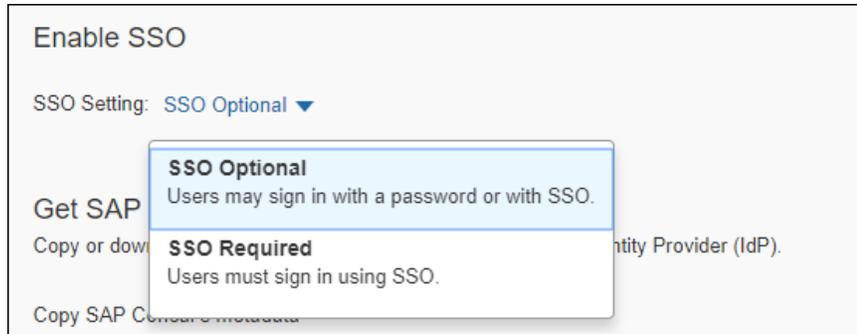
Step 8: Test SP-Initiated SSO

▶ **To test:**

1. Go to www.concursolutions.com.
2. Enter the SAP Concur username.
3. Click **Sign in with [Custom IdP Name]**. You will be redirected to your IdP. After you authenticate to the IdP, the SAP Concur home page appears.

Step 9: Enable SSO as Optional or Required

In the **Enable SSO** section, you have the option to change the SSO Setting from **SSO Optional** (Default value) to **SSO Required**.



! **IMPORTANT!** If this account is managed by a TMC, the TMC must be notified before the SSO setting is changed from **SSO Optional** to **SSO Required**.

If you change the SSO setting to **SSO Required**, all users will be required to sign in to concursolutions.com through an IdP using SSO. Users—including TMCs, admins, web services, and test user accounts—will be blocked from signing in to concursolutions.com with their username and password. This could cause a disruption in services for those users.

Best Practice is to use the **SSO Optional** setting until all users understand how to sign in with SSO. Before you change the setting to **SSO Required**, we recommend you provide your users with a 60-day notice or a notification timeframe that is standard for your organization.

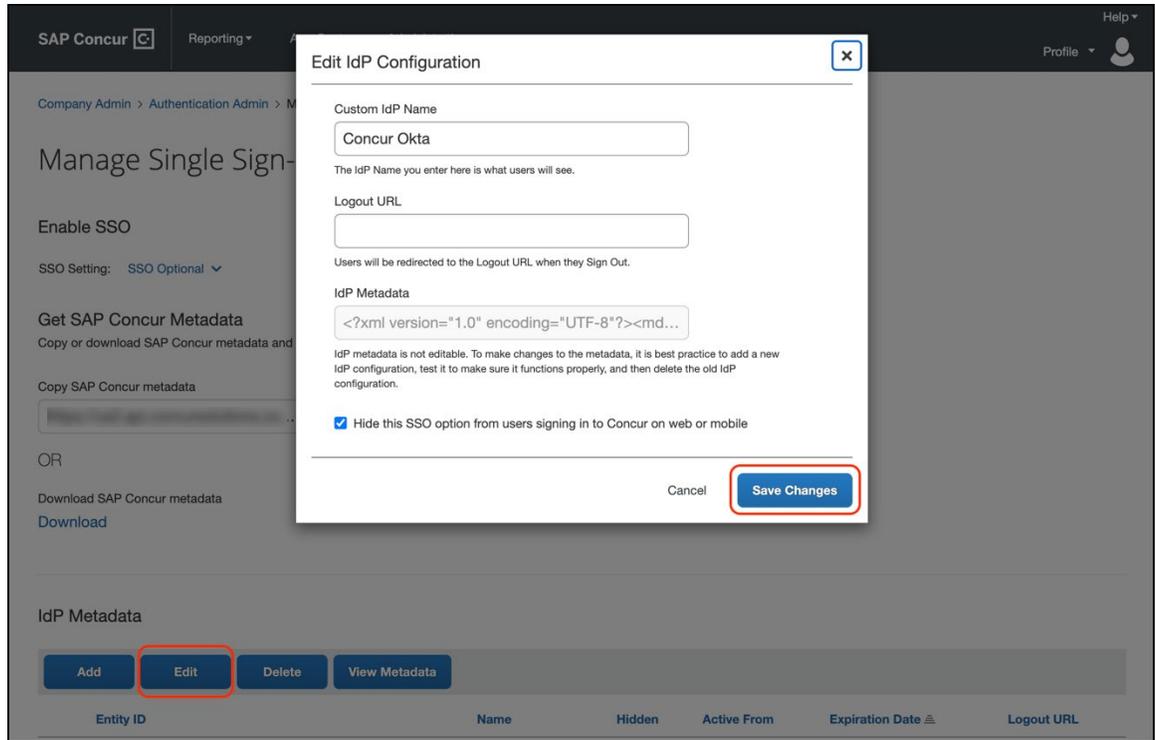
If you have any questions about making this change, contact SAP Concur Support for assistance.

! **IMPORTANT: Changing the SSO Setting to SSO Required affects both web and mobile sign-in.** Beginning with the 9.86 (November) version of the SAP Concur mobile app, changing the SSO Setting to SSO Required mandates that users must sign in using SSO on both web and mobile platforms.

Editing SSO Configurations

Once an SSO configuration has been created using the previous steps, it may be edited to change the values of Custom IdP Name, Logout URL, and checkbox to **Hide this SSO option from users signing in to Concur on web or mobile**. The IdP Metadata is not editable; instead, the recommended best practice is to create a new configuration, test it, and then delete the original configuration.

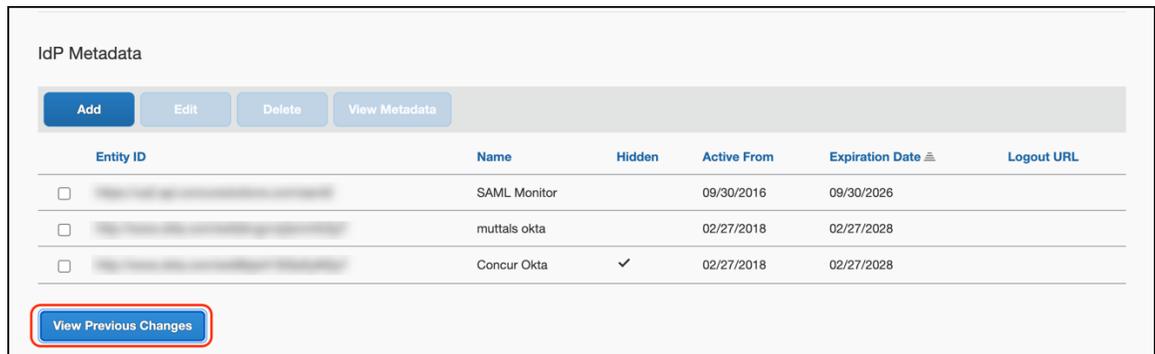
To edit a configuration, select the configuration to edit, and click **Edit**.



When the desired changes have been made, click **Save Changes**.

View Previous Changes

To view changes to the SSO configuration that have been made over time, click the **View Previous Changes** button.



A table listing previous changes appears. The list of changes is sorted in descending order by date and time.

View Previous Changes							
Date	Change	Entity ID	Name	Logout URL	Hidden	Details	
06/08/2022	Edit	[REDACTED]	Concur Okta		✓	View	
06/08/2022	Edit	[REDACTED]	ray test 2		✓	View	
06/08/2022	Edit	[REDACTED]	ray test 2			View	
06/08/2022	Edit	[REDACTED]	ray test 2		✓	View	
06/08/2022	Edit	[REDACTED]	ray test 2			View	
06/08/2022	Add	[REDACTED]	ray test 2		✓	View	
06/07/2022	Delete	[REDACTED]	ray test 2			View	
06/07/2022	Edit	[REDACTED]	ray test 2			View	
06/07/2022	Add	[REDACTED]	ray test 2		✓	View	
06/07/2022	Delete	[REDACTED]	ray test 2		✓	View	
06/07/2022	Edit	[REDACTED]	ray test 2		✓	View	
06/07/2022	Edit	[REDACTED]	ray test 2			View	

The table can display the last 100 changes. Changes that are listed in the table include:

- Adding a configuration
- Deleting a configuration
- Editing the name in the Custom IdP Name field
- Editing the URL in the Logout URL field
- Editing the Hide this SSO option from users signing in to Concur on web or mobile checkbox value.

To view more detailed information about a specific change listed in the table, click the **View** link for the desired list item.

View Previous Changes							
Date	Change	Entity ID	Name	Logout URL	Hidden	Details	
06/08/2022	Edit	[REDACTED]	Concur Okta		✓	View	
06/08/2022	Edit	[REDACTED]	ray test 2		✓	View	
06/08/2022	Edit	[REDACTED]	ray test 2			View	

After you click the **View** link, the **View Previous Changes** page for the list item appears. The details that appear on the page differ depending on the kind of change that was made.

DELETED CONFIGURATION DETAILS

The details that are displayed on the **View Previous Changes** page when a configuration is deleted include:

- Date Changed
- Type of change (Delete)
- Company that was changed
- Name and UUID for the user who made the change
- Entity ID
- Friendly name
- Logout URL
- Metadata
- Hidden

For configurations that are deleted, the **View Previous Changes** page includes a **Revert** button that enables you to reinstate the deleted configuration. After the configuration is reinstated, it will be available to users during the sign-in process.

Example View Previous Changes Page for Deleted Configuration

View Previous Changes
✕

Date Changed	05/24/2022
Change	Delete
Company	[Redacted]
Change By	[Redacted]

Entity ID	[Redacted]
Name	[Redacted]
Logout URL	https://logout.com
Hidden	

Metadata

```

<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn
<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn
<md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw
      A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YT:
      MBIGA1UECwwLU1NPUHJvdmlkZXIxEjA0BjNVBAMMB211dHRhbHMxHDAaBgkqhkiG9w0BCQEWdW
      Zm9Ab2t0YS5jb20wHhcNMjgwMjI3MTgzNDIyWWhcNMjgwMjI3MTgzNDIyWjCBjzELMAkGA1UEBh:
      VVMxEzARBgNVBAgMCkNhbG1mb3JuaWEeXjAUBgNVBACMDVNhbiBGcmFuY2lzY28xDALBgNVBA
      BE9rdGEeFDASBgNVBAcMINTT1Byb3ZpZGVyMRAwDgYDVQQDDAdXR0YXxzMRwwGgYJKoZIhvc:
      AQkBFglpbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgnM0Q
      yhB4v+OrwRqN8oSDs2bKa2wo2eQKInxi7xX7Yh4Q0E3Y630Pr4uXdl5boUynIsuyVZ4ahoXYy5:
      NL5kykz76FEVY6HR4fQzTgFnyYwRxp0rYbg9RmpggYvMcowYTVXphhkiKTW6W/k0Ff/isMme/VN
      
```

Revert
OK

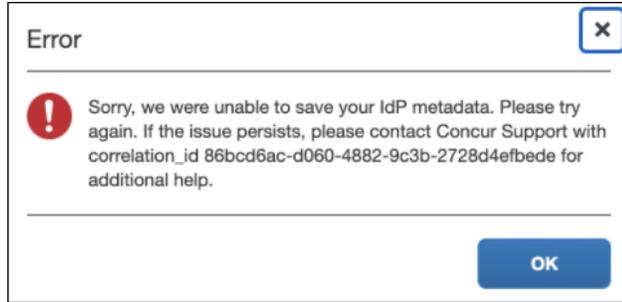
When you click the **Revert** button, you are prompted to confirm the action to reinstate the configuration. To confirm that you want to reinstate the configuration, click **Revert Metadata**. To cancel reinstatement of the configuration, on the **Confirm Revert** page, click **Do Not Revert**.

Confirm Revert
✕

Are you sure you want to revert this deletion, and make this configuration active?

Do Not Revert
Revert Metadata

If you choose to reinstate a deleted configuration but the configuration cannot be reinstated, after you click the **Revert Metadata** button, a message similar to the following appears:



EDITED CONFIGURATION DETAILS

The details displayed on the **View Previous Changes** page when a configuration is edited include:

- Date Changed
- Type of change (Edit)
- Company that was changed
- Name and UUID for the user who made the change
- Current Entity ID
- Current friendly name
- Current Logout URL
- Previous Entity ID
- Previous friendly name
- Previous Logout URL
- Metadata
- Hidden

View Previous Changes
X

Date Changed	06/07/2022
Change	Add
Company	[REDACTED]
Change By	[REDACTED]

Entity ID	[REDACTED]
Name	[REDACTED]
Logout URL	
Hidden	✓

Metadata

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="urn
<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn
<md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate>MIIDnJCcAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw
      A1UECAwKQ2FsaWZvcn5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YT
      MBIGAlUECwwLU1NPUHJvdmlkZkZlXDA0bG9uYVZvcn5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbz
      Zm9Ab2t0YS5jb2wHcNMTGwMjI3MTgzNDIyWhcNMjI3MTgzNDIyWhcNMjI3MTgzNDIyWhcNMjI3MT
      VVMxEzARBgNVBAgMCKNhG1mb3JuaW50eS5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1
      UECAwKQ2FsaWZvcn5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTMBIG
      AlUECwwLU1NPUHJvdmlkZkZlXDA0bG9uYVZvcn5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbzEN
      MAsGA1UECAwKQ2FsaWZvcn5pYTEwMmBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YT
      MAsGA1UECgwET2t0YTMBIGAlUECwwLU1NPUHJvdmlkZkZlXDA0bG9uYVZvcn5pYTEwMmBQGA1UEBww
      NLSykyz76FEVY6HR4fQzTqFnyYwRxp0rYbg9RmpggYvMmcwYTVXphhkiKTW6W/k0Ff/isMme/VN
```

OK

Configure an SSO App/Connector with Encryption (Optional)

Complete all steps described in the *Configure an SSO App/Connector Without Encryption* section, including testing. Then, check if your IdP supports encrypted SAMLResponse feature. If so, follow the steps below to configure the encryption.

Step 1: Obtain and Save the Encryption Key

Obtain the encryption key from SAP Concur solutions and save it in an encryption.crt file.

► **To obtain and save the encryption key:**

- Click the URL that corresponds to the region (data center) in which your entity is hosted to view the SAP Concur SP metadata (Chrome browser recommended):

- ◆ **US (North America):**

<https://www-us.api.concursolutions.com/sso/saml2/V1/sp/metadata/>

- ◆ **EMEA:**

<https://www-emea.api.concursolutions.com/sso/saml2/V1/sp/metadata/>

Step 2: Upload the encryption.crt to Your IdP

If you have questions about uploading the encryption certificate to your IdP, contact your IdP for assistance.

EXAMPLES

For Okta, set the **Assertion Encryption** field to **Encrypted** and then upload the encryption certificate.

The screenshot shows a configuration form with the following fields:

- Assertion Encryption**: Set to **Encrypted** (highlighted with a red box).
- Encryption Algorithm**: Set to **AES256-CBC**.
- Key Transport Algorithm**: Set to **RSA-OAEP**.
- Encryption Certificate**: An empty text field with a **Browse files...** button next to it (highlighted with a red box).

For Azure AD, use the **Token encryption (Preview)** option to upload the encryption certificate.

The screenshot shows the Azure AD configuration interface for 'Concur Travel and Expense - Token encryption (Preview)'. The left sidebar contains a navigation menu with the following items:

- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Users and groups
 - Single sign-on
 - Provisioning
 - Self-service
- Security
 - Conditional Access
 - Permissions
 - Token encryption (Preview)** (highlighted with a red box)
- Activity

The main content area shows the 'Import Certificate' dialog with the following text:

Import Certificate

Upload a certificate with a file name extension .cer

Select a file

Buttons: Add, Cancel

Section 6: FAQ

Q. Which IdPs are supported by SAP Concur?

A. SAP Concur is compatible with all identity providers that support the SAML 2.0 standard.

Q. How does SSO enforcement work?

A. Currently, SAP Concur supports enforcing SSO at the company level. SAP Concur does not support enforcing SSO based on user role or user group.

There are two options available when setting up SSO: **SSO Optional** and **SSO Required**.

SSO Optional is the default value and selecting it means that everyone from your company can sign in to SAP Concur services with a standard username and password **or** with SSO credentials.

After you have successfully tested SSO sign-in, you can change the SSO Setting to **SSO Required**.

! IMPORTANT! Changing the SSO setting to **SSO Required** could cause a disruption in service.

If you change the SSO setting to **SSO Required**, all users will be required to sign in to concursolutions.com through an IdP using SSO. All users—including TMCs, admins, web services, and test user accounts—will be blocked from signing in to concursolutions.com with their username and password.

! IMPORTANT! If this account is managed by a TMC, the TMC must be notified before the SSO setting is changed to **SSO Required**.

Q. Can I set up more than one IdP with SAP Concur?

A. Yes. The SSO self-service tool allows you to add unlimited IdPs.

Q. How long do I need to wait to test SSO sign-in after I have uploaded my metadata?

A. Once your IdP's metadata is saved properly at SAP Concur, SSO sign-in should work instantly.

Q. Will configuring SSO on the new self-service platform affect our current SSO configuration on your old platform?

A: No. Configuring SSO on the new self-service platform will not affect your current SSO configuration on the old platform. It is separate from the legacy Concur SSO stack and can safely be used in parallel to the existing SSO configurations. Once the SSO service has been configured, tested, and deployed, existing SSO customers can request the removal of their legacy SSO configurations so they have only a single tool to manage.

Q. Why can't I see my current SSO configuration on the **Manage Single Sign-On** page?

A: Your current SSO configuration is part of the old SSO service and that configuration data can be accessed only by SAP Concur employees

Q. Can I set up my mobile SSO via the **Manage Single Sign-On** page?

A. Yes. Beginning with the 9.86 version of the SAP Concur mobile app, configuring SSO using the processes described in this document enables SSO sign-in for both web and mobile. If you change the SSO Setting from **SSO Optional** to **SSO Required** users must sign in using SSO on both the web and mobile platforms.

Q. Does SAP Concur support "Just-In-Time User Provisioning" via SAML SSO?

A. No. It is targeted for a future update.

Q. Does SAP Concur support "Home Realm Discovery"?

A. Yes. Home Realm Discovery service is an API behind the SP-Initiated SSO flow.

Section 7: Appendix - ADFS Setup

NOTE: Per the appendix instructions in this section, as content is sourced from the third-party provider, SAP Concur cannot guarantee its accuracy. If you encounter issues, it is recommended that you contact the third-party provider's support resources.

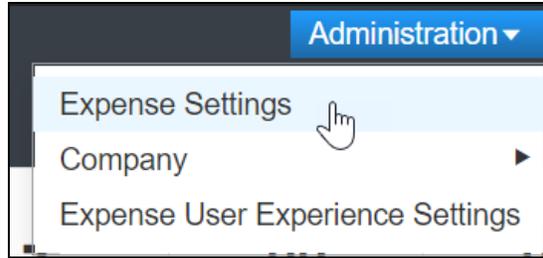
Getting Started

Before you start the configuration process, ensure that:

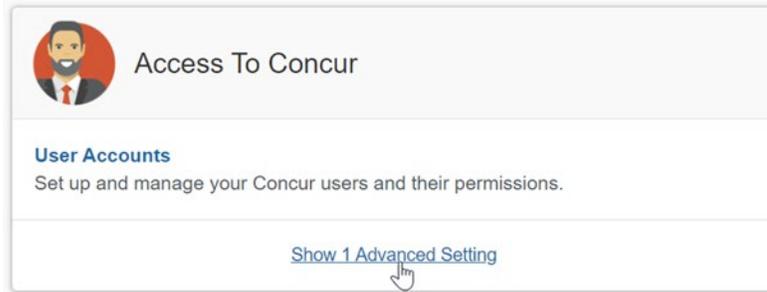
- Your users exist in both ADFS and SAP Concur. Auto user provisioning is not currently supported by SAP Concur, so you need to add users separately in there.
- The attribute you are sending from ADFS matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the **Manage SSO** page by using one of the following paths, depending on your SAP Concur edition.

For SAP Concur **Standard** edition:

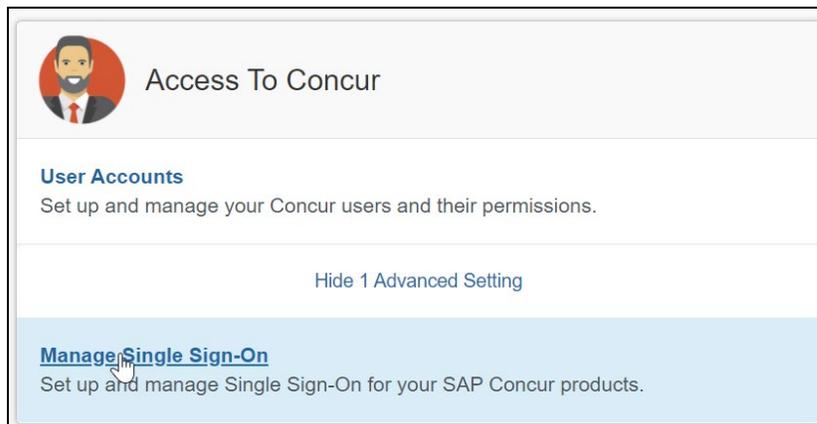
1. Go to **Administration > Expense Settings**.



2. Under Access to Concur section, click **Show 1 Advanced Setting**.

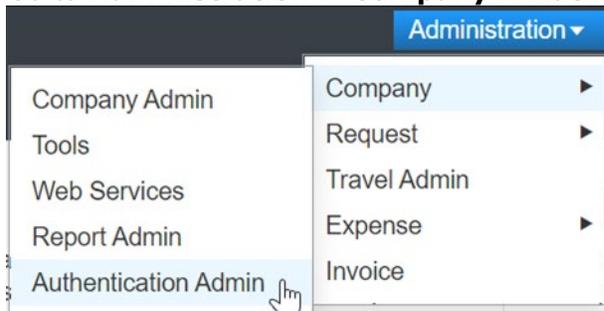


3. Click **Manage Single Sign-On** to access the **Manage SSO** page.

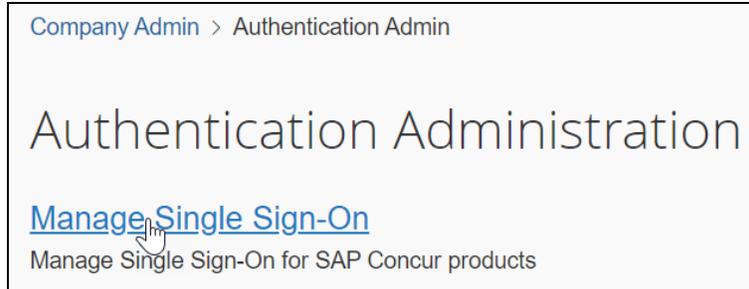


For the SAP Concur **Professional** edition:

1. Go to **Administration > Company > Authentication Admin**.



2. Click **Manage Single Sign-On** to access the Manage SSO page.



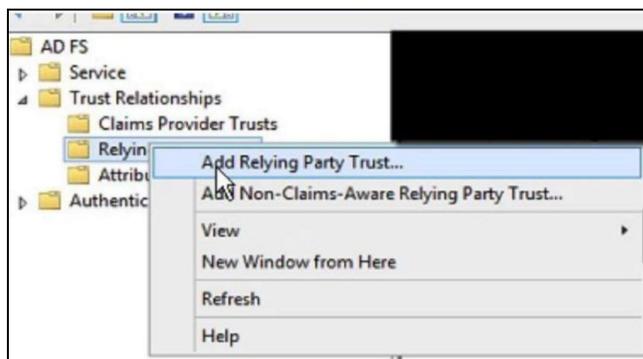
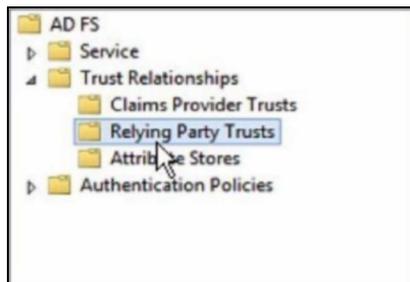
Alternatively, users can access the page using one of the following URLs:

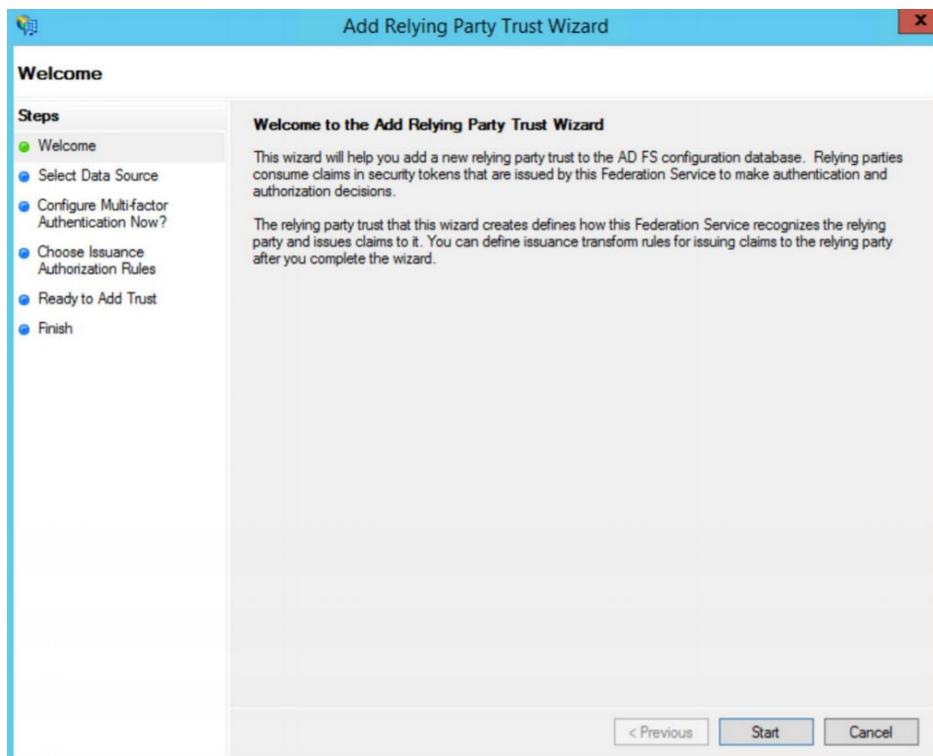
- US DC Prod: <https://www.concursolutions.com/nui/authadmin/ssoadmin>
- US DC Test: <https://implementation.concursolutions.com/nui/authadmin/ssoadmin>
- EMEA DC Prod: <https://eu1.concursolutions.com/nui/authadmin/ssoadmin>
- EMEA DC Test: <https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin>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

NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an authorized support contact at your company to open a case with SAP Concur support.

Configure Your ADFS Application

1. Run the **Relying Party Trust** wizard.

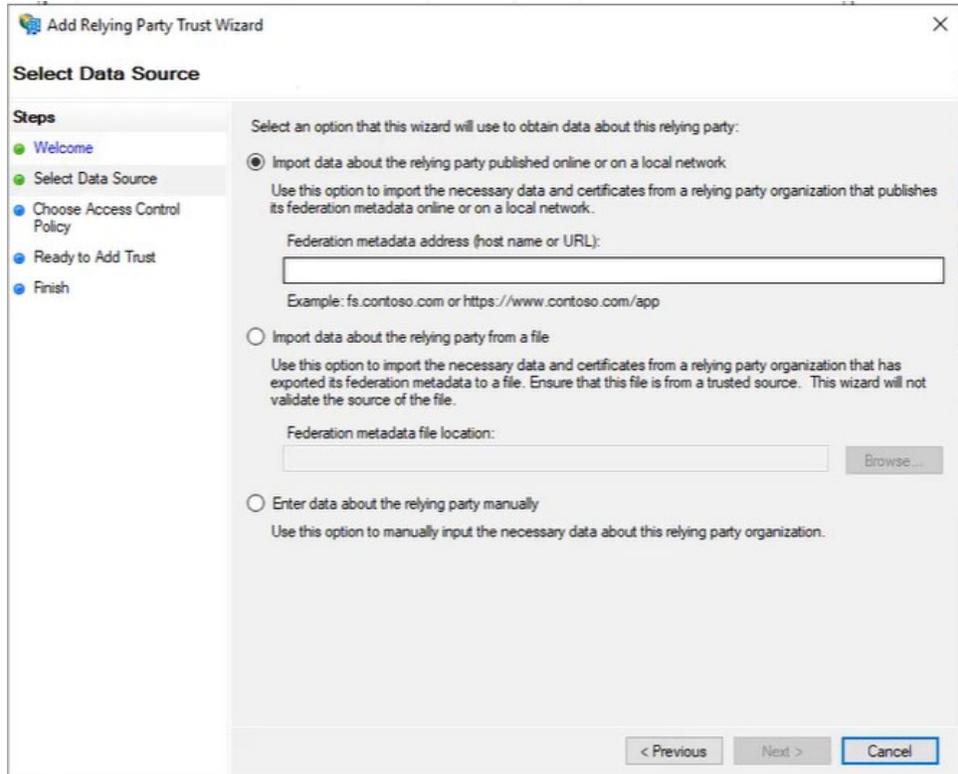




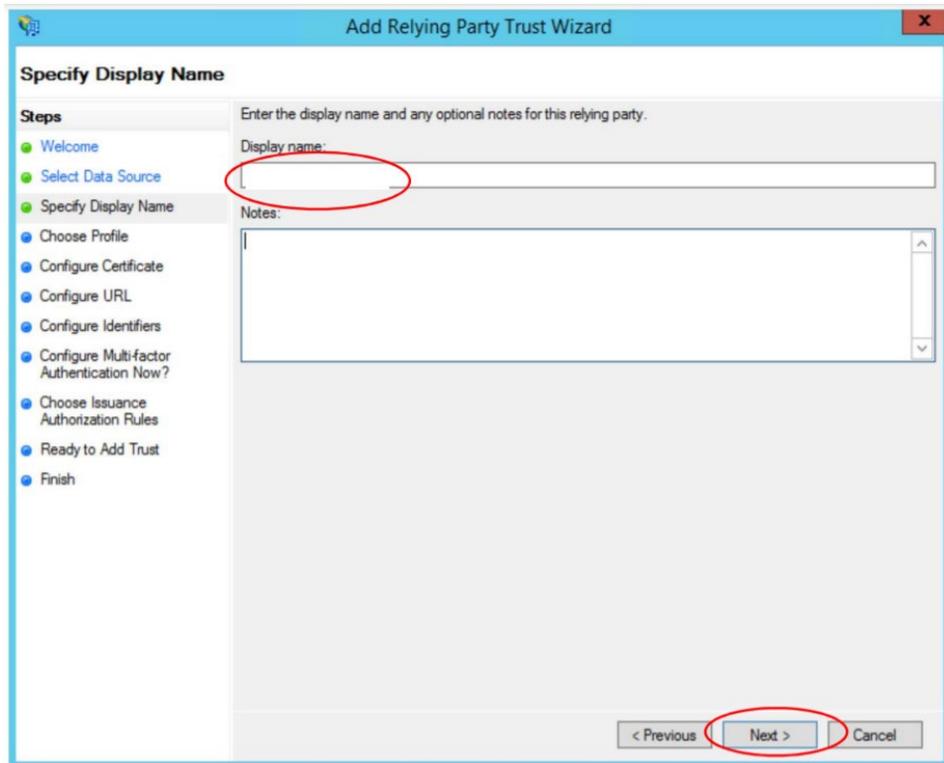
2. On the **Select Data Source** dialog, choose the option of your preference:
 - a. **Import data about the relying party published online or on a local network** (if you prefer to upload the metadata URL)
 - b. **Import data about the relying party from a file** (if you prefer to upload the metadata xml file)
 - c. **Enter data about the relying party manually** (if you prefer to manually fill the configuration fields)
3. After choosing your option, click **Next**.

The metadata file or the metadata URL can be obtained from the **Authentication Admin > Manage Single Sign-On** page on your SAP Concur account. Please refer to the previous *Getting Started* section for more information about how to access the page.

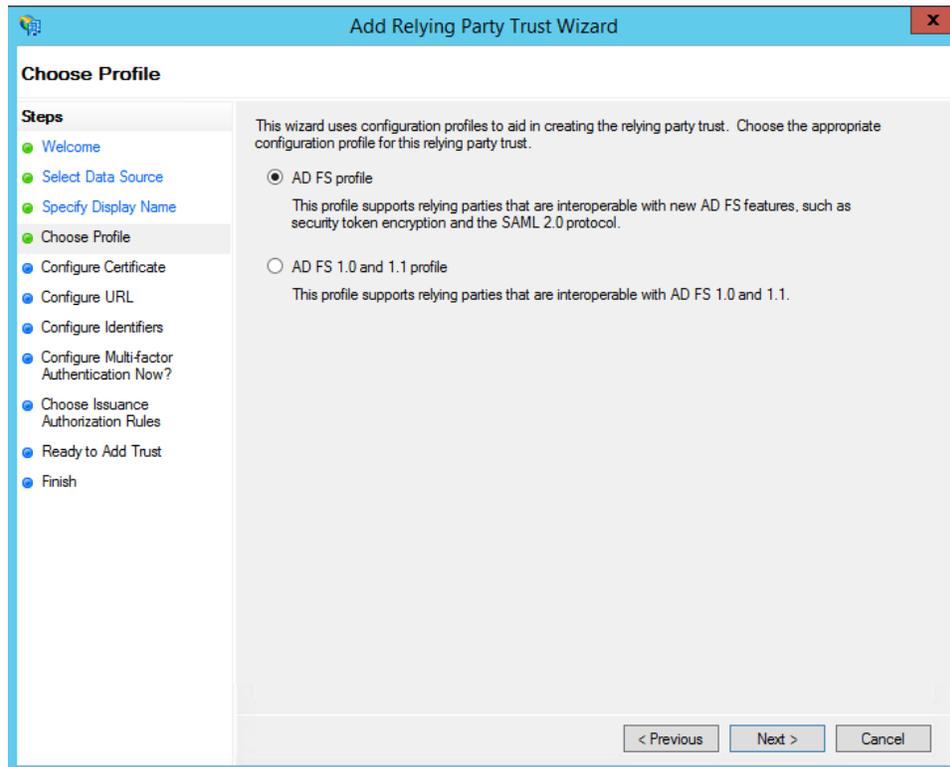
If you have chosen **Import data about the relying party published online or on a local network** or **Import data about the relying party from a file** this should automatically fill your **Configure Certificate, Configure URL** and **Configure Identifiers** sections on ADFS. In that case, please skip to step 8 on this guide. Steps 3-7 will be needed if you have chosen the manual setup.



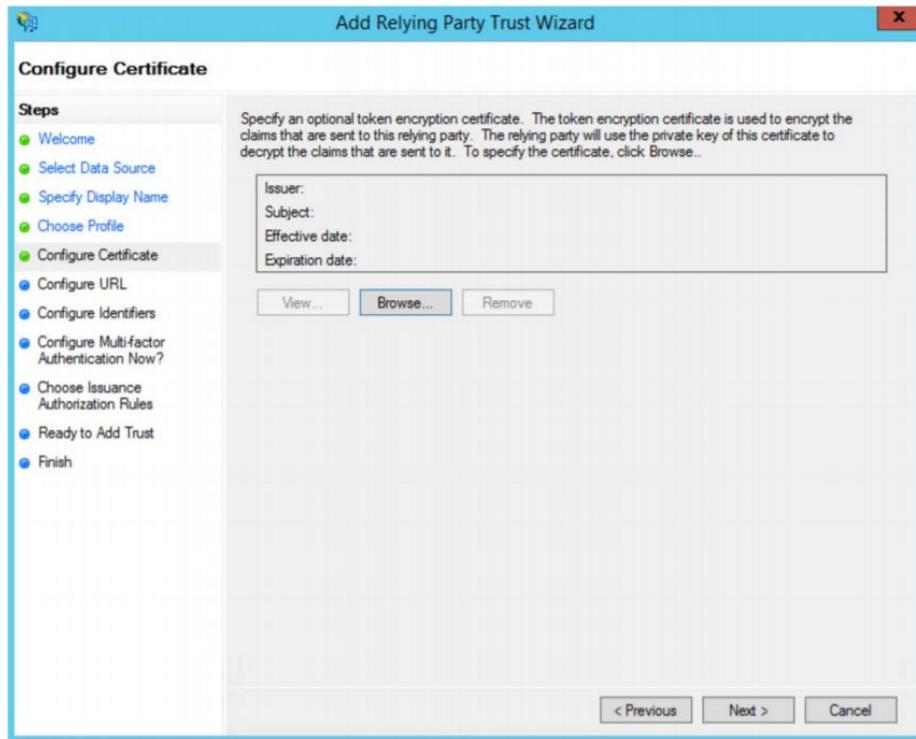
4. On the **Specify Display Name** dialog, in the **Display name** field, enter the label of your preference and click **Next**.



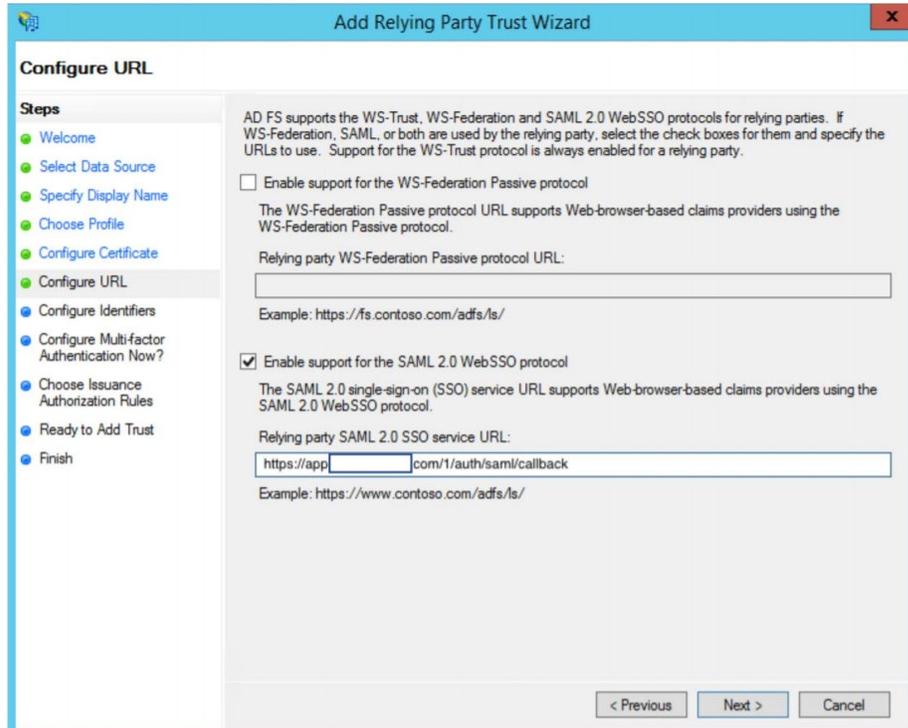
5. On the **Choose Profile** dialog, select **ADFS profile** option and click **Next**.



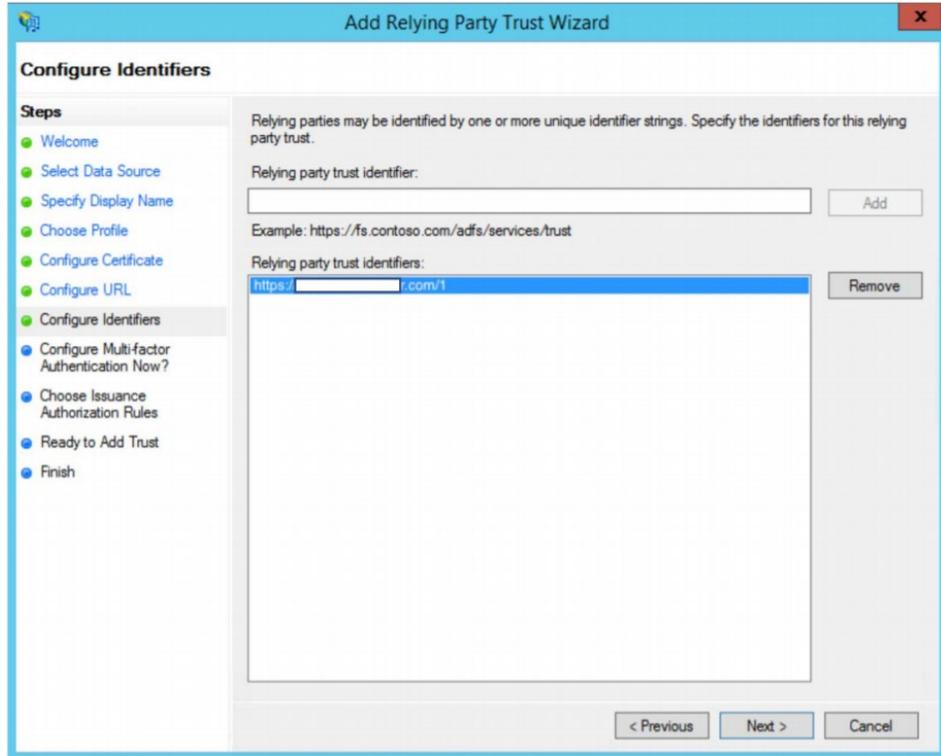
6. On the **Configure Certificate** dialog, manually upload the SAP Concur encryption certificate. It can be obtained from the **Manage SSO** page in SAP Concur as described in the *Getting Started* section. Then go to the SAP Concur metadata, extract the encryption certificate and save it to your PC. Browse and upload the encryption certificate and then click **Next**.



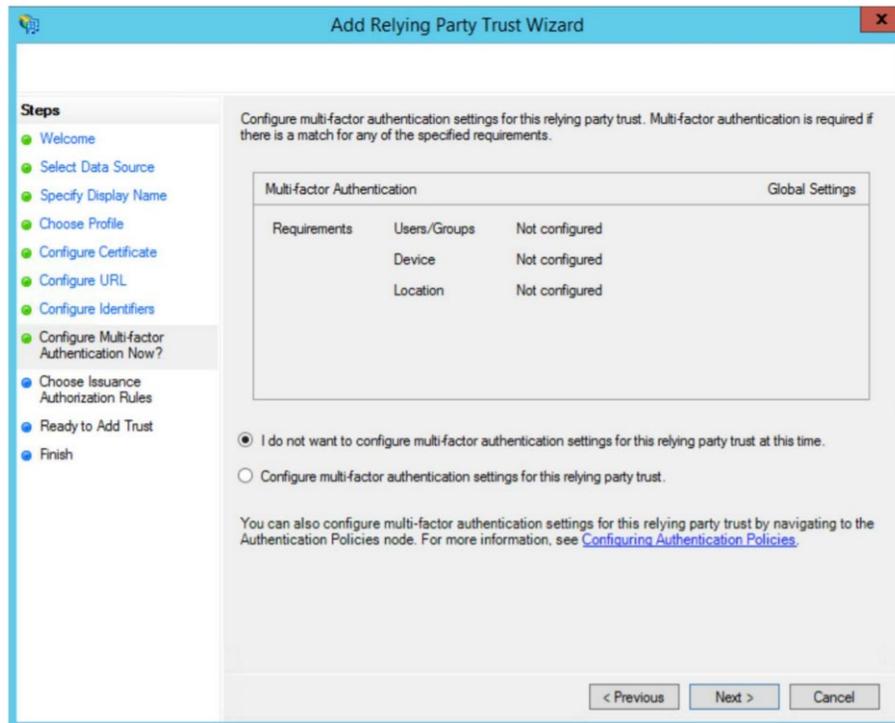
7. On the **Configure URL** dialog, select **Enable support for the SAML 2.0 Web SSO protocol** and enter the relying party SAML 2.0 SSO service URL:
 - ◆ US (North America): <https://www-us.api.concursolutions.com/sso/saml2/V1/acs/>
 - ◆ EMEA: <https://www-emea.api.concursolutions.com/sso/saml2/V1/acs/>
 - ◆ China: <https://www-cn.api.concursolutions.com/sso/saml2/V1/acs/>



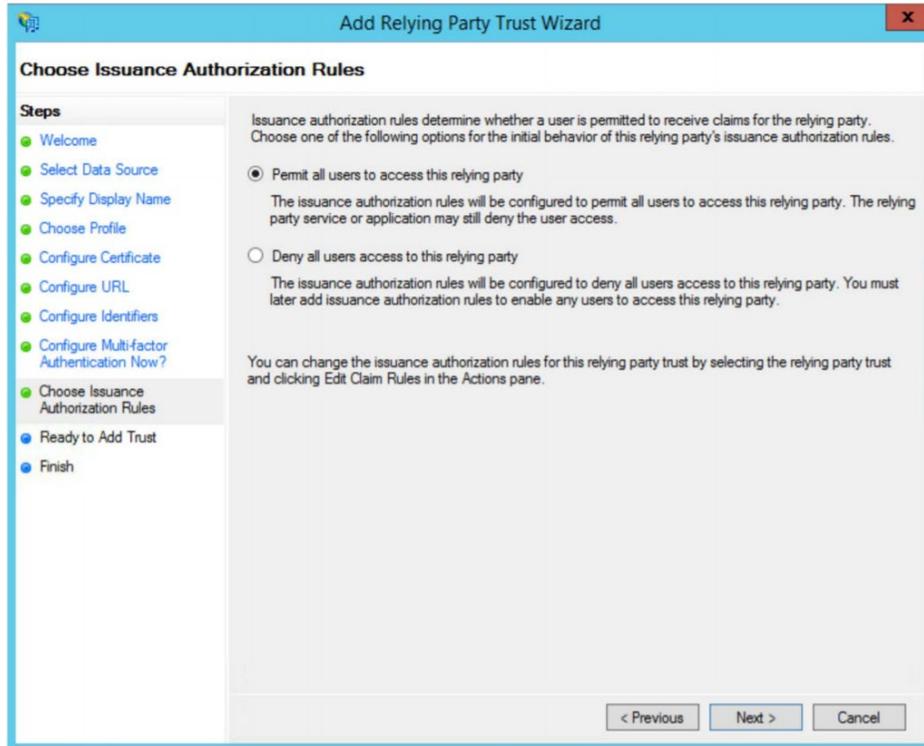
8. On the **Configure Identifiers** dialog, add the **Relying party trust identifier**:
 - ◆ US (North America): <https://us.api.concursolutions.com/saml2>
 - ◆ EMEA: <https://emea.api.concursolutions.com/saml2>
 - ◆ China: <https://cn.api.concursolutions.com/saml2>



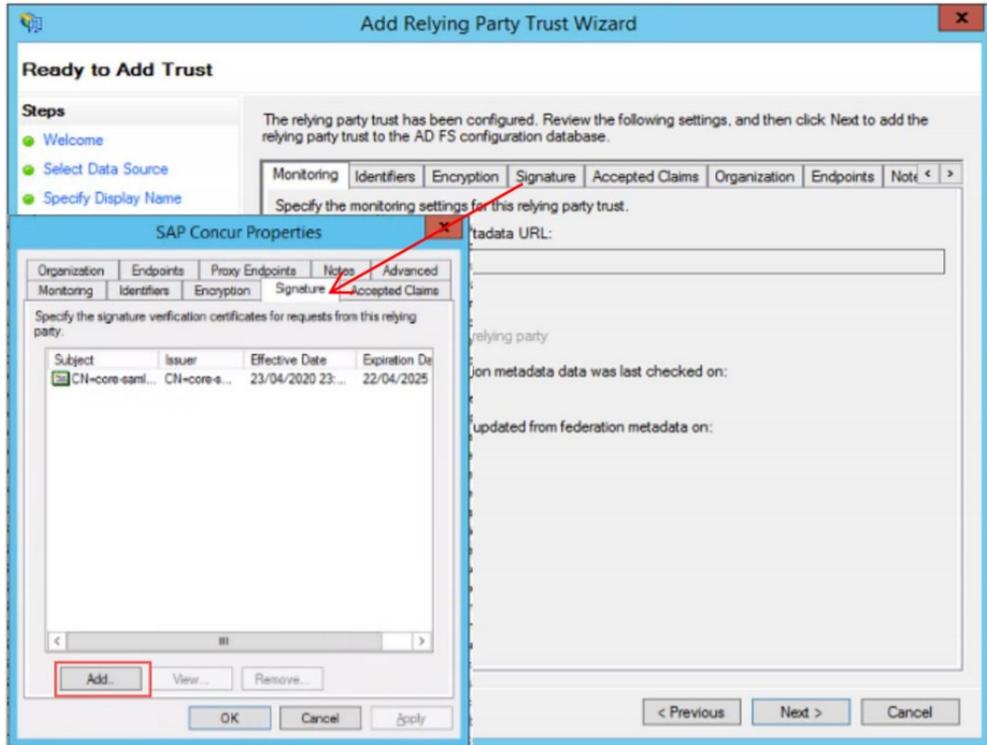
9. Select the **I do not want to configure multi-factor authentication settings for this relying party trust at this time** option and then click **Next**.



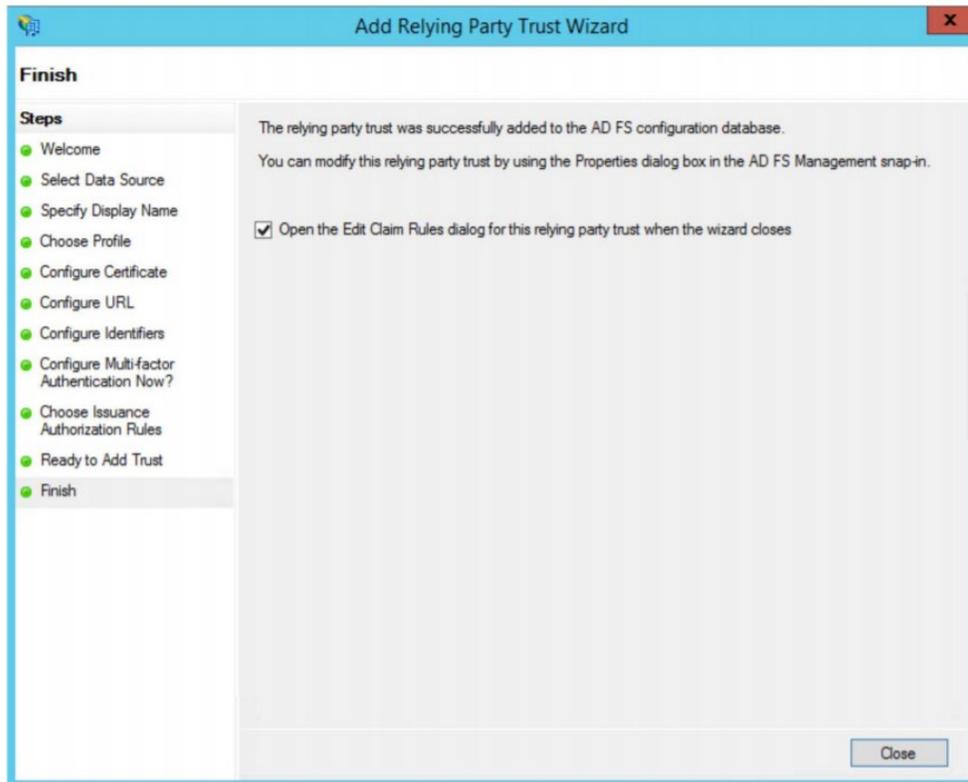
10. In the **Choose Issuance Authorization Rules** dialog, select the **Permit all users to access this relying party** option and then click **Next**.



11. Review the newly configured relying part trust if required. If you haven't updated the metadata already, on the **Ready to Add Trust** dialog click the **Signature** tab, add the SAP Concur metadata and then click **Next**.



- On the **Finish** dialog, select the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** option and then click **Close**.



The Add Transform Claim Rule Wizard appears automatically.

13. Create the following two rules:

Rule 1:

- 1) Set claim rule template as "Send LDAP Attributes in Claim".
- 2) Click **Next**.
- 3) Add Claim rule name and set your Attribute store. This will normally be "Active Directory".
- 4) LDAP Attribute = E-Mail Addresses
- 5) Outgoing Claim Type = E-Mail Address
- 6) Click **Finish**.

Rule 2:

- 1) Set claim rule template as "Transform an incoming claim".
- 2) Add Claim Rule Name.
- 3) Incoming Claim Type = Email Address
- 4) Outgoing Claim Type = NameID
- 5) Outgoing Name ID format = Email
- 6) Make sure "Pass through all claim values" is selected.
- 7) Click **Finish**.

For the Name ID value that is passed in the assertion when a user authenticates, this value *must* match the user's SAP Concur login ID. Most SAP Concur customers use email addresses as their login IDs therefore, by default, this is how the claim rule should be set up.

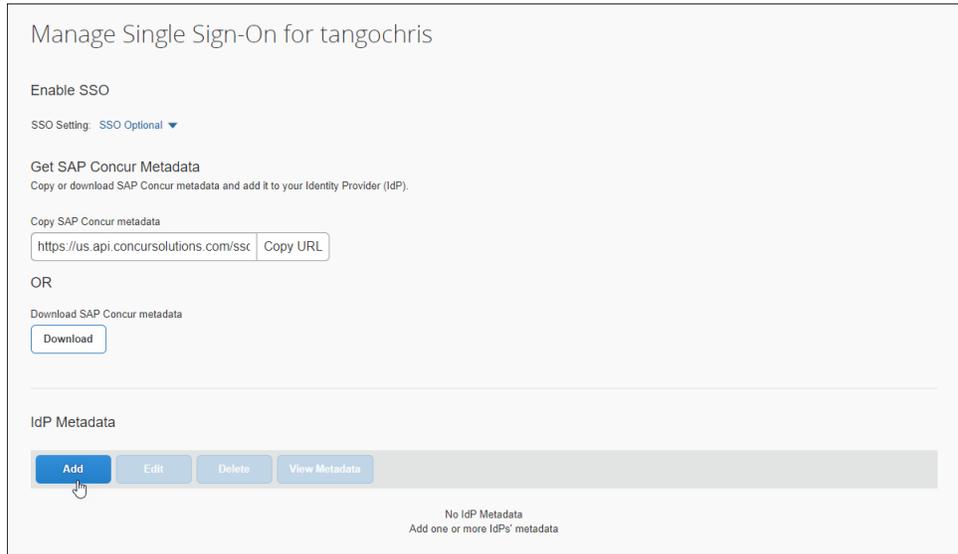
However, if your company uses a different format for your SAP Concur login IDs, for example, employeeID@companydomain.com, then you must customize this rule so that the LDAP Attribute sends the **employeeid** and **companydomain.com**. Any other custom roles created will need to make sure the Name ID format is sent as "email address", as this is a requirement for SP-Initiated logins.

Configure Your SAP Concur Site

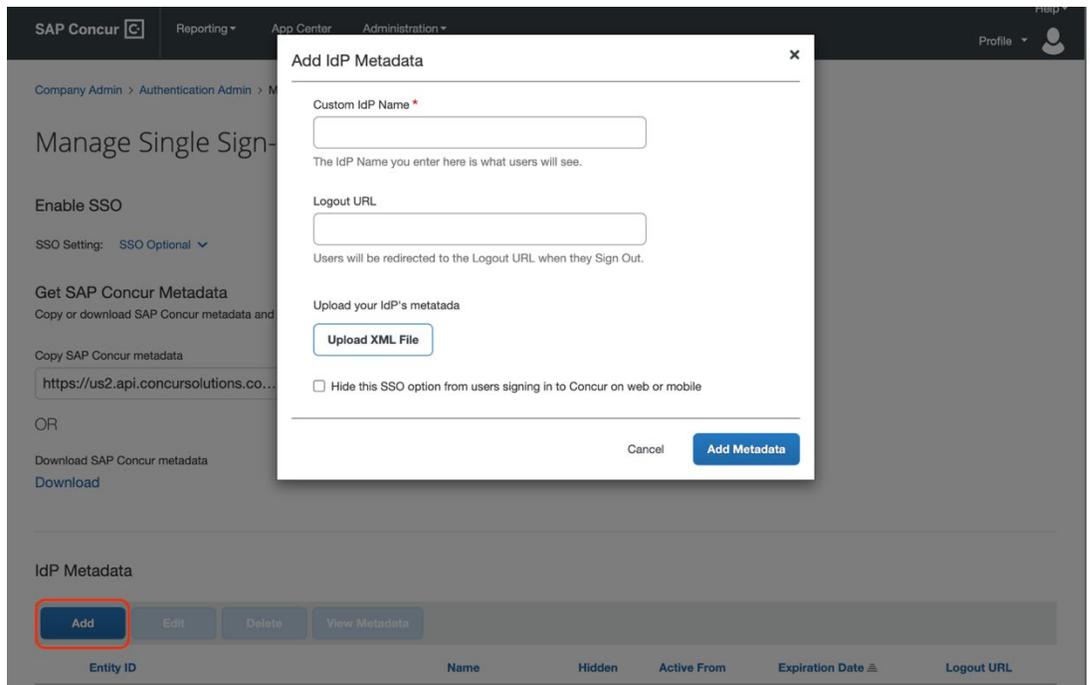
To complete the configuration, save a copy of the ADFS metadata file to your local machine.

► **To enter the ADFS metadata into SAP Concur:**

1. Sign into SAP Concur.
1. Access the **Manage Single Sign-On** page.
2. Click **Add** in the **IdP Metadata** section.

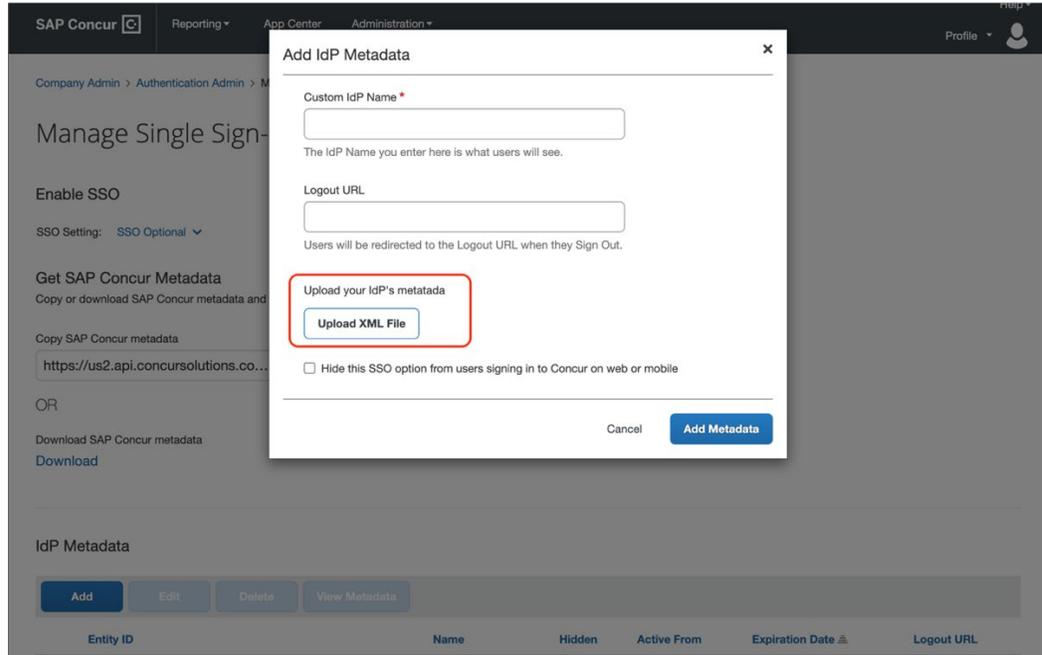


The **Add IdP Metadata** window appears.



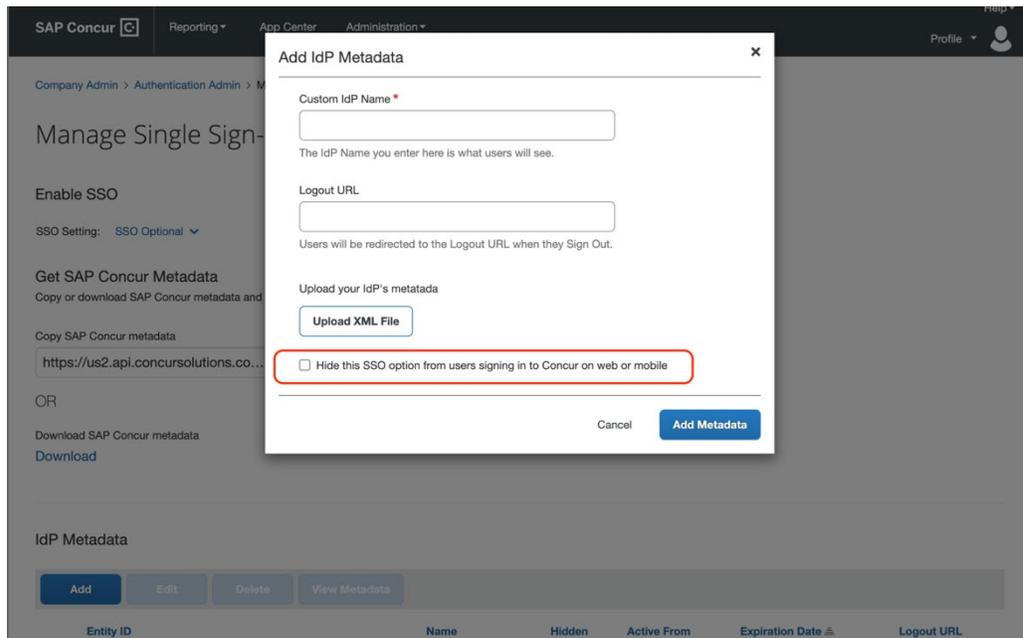
3. In the **Add IdP Metadata** window, **Upload your IdP's metadata** section, click **Upload XML File** and upload the ADFS metadata file.

Section 7: Appendix - ADFS Setup

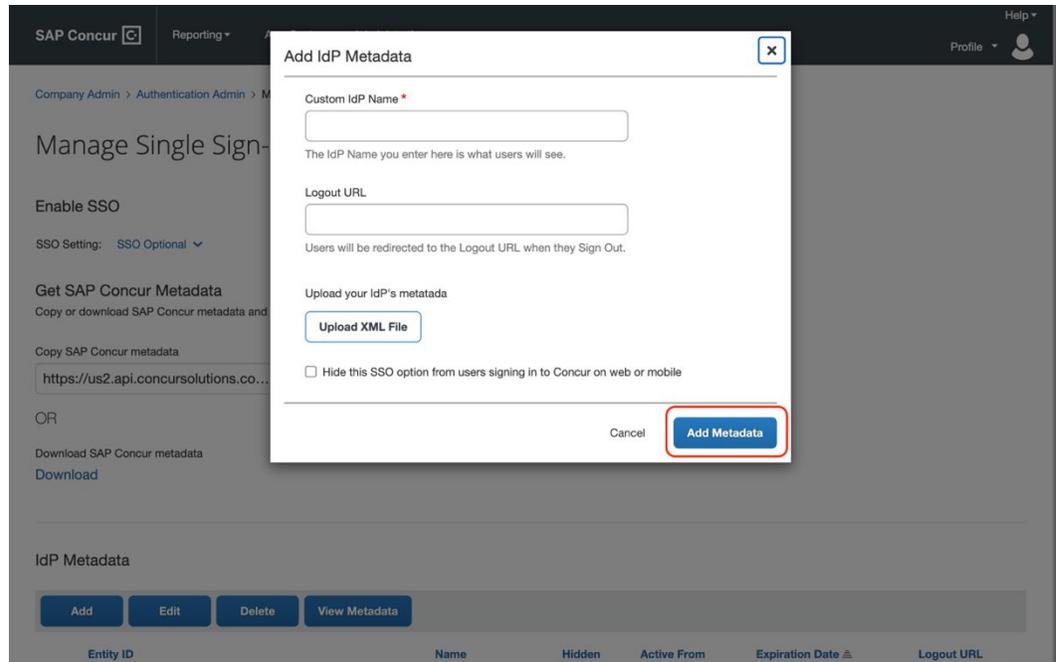


4. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox Hide this SSO option from users signing in to Concur on web or mobile.

By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.



5. Click **Add Metadata**.



Test SSO Login

Testing IdP-Initiated SSO

To test your IdP-Initiated SSO login, make sure you've assigned the new application in ADFS to the users and groups who will test this. Use the ADFS URL that looks like this:

```
https://[Federation Service Identifier
domain]/adfs/ls/idpinitiatedsignon.aspx?loginToRp= [Relying party trust
identifier]
```

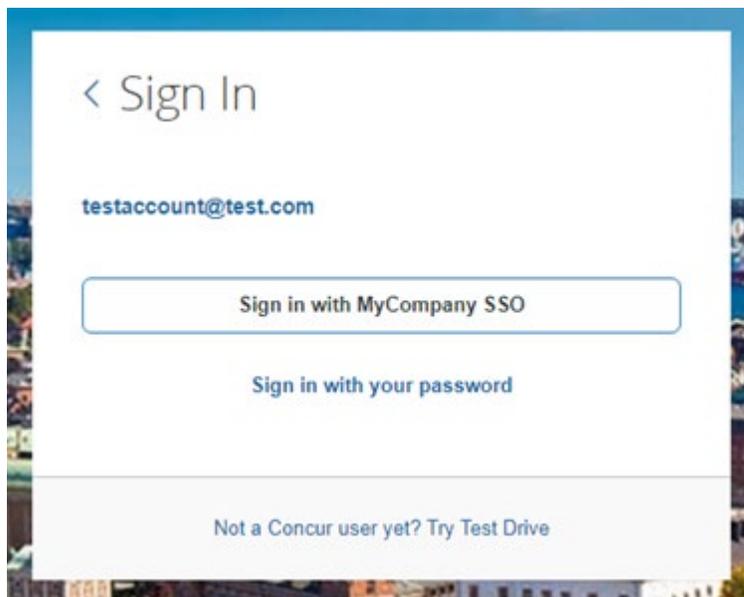
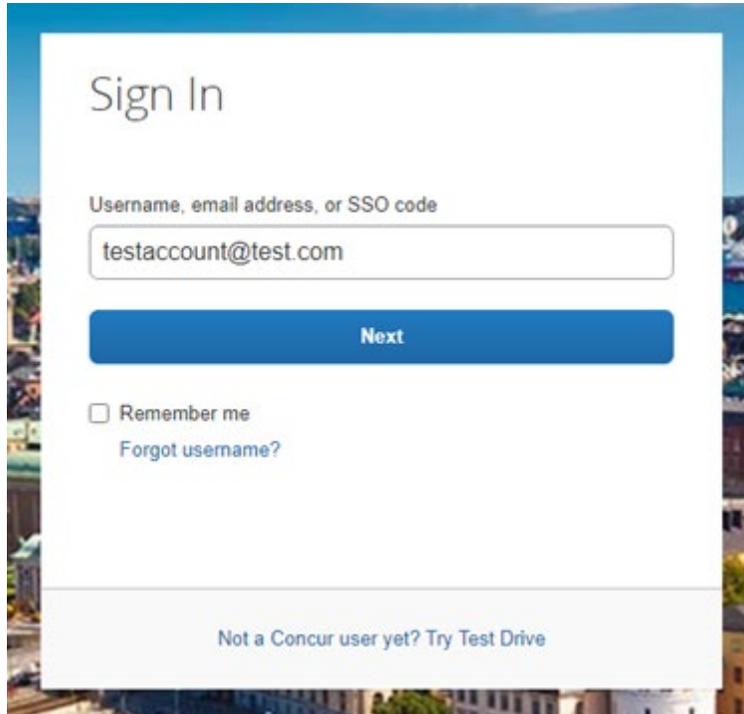
If correct, this URL should prompt you for your ADFS credentials and then redirect you to the already logged in SAP Concur home page.

Test SP-initiated SSO

To test the SP-initiated SSO:

1. Open the SAP Concur login page according to the environment you want to test.
 - ◆ 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. On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click **Next**, you should see an option for your recently created SSO configuration. Click to proceed with authenticating your identity provider account which should redirect you to SAP Concur.



After adding your ADFS credentials, if you receive an error message in ADFS, this could be a sign that the onfiguration is not completed. If the error message is on the SAP Concur side, this could be a matter of unmatching credentials, an invalid certificate or a missing setting. If the IdP-Initiated login is working but the SP-Initiated is not, this is probably happening because the

Name ID on the ADFS side is not being sent with the correct format. This is described in the *Configure Your ADFS Application* section.

If you're still having issues, please copy the error ID you received and contact SAP Concur support for assistance.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated using the previous *Test SSO Login* section.

NOTE: The automatic enabling of Mobile SSO is only visible on the app version 9.86 or higher and if the user is opting for the new sign in experience. Users on older versions or opting for the earlier sign in experience will not see this option automatically.

If you have any issues in authenticating with SSO on the mobile app, please open a ticket with the SAP Concur support team and provide any error IDs and/or messages received with screenshots.

E-mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket with the SAP Concur support team, providing the IDP URL from the application created on the IDP side so they can adjust the redirect URL for e-mail reminders. For more information on how to obtain the URL, see the *Test SSO login > Testing IdP-Initiated SSO* section of this appendix.

Rollout

After testing your new SSO configuration, you can then plan your rollout by assigning your new Azure AD application to all your users and groups who'll need this access.

The Manage SSO page also offers the option for you to enforce this new SSO connection by changing the SSO Setting from SSO Optional to **SSO Required**. If you change it, users will be redirected to SAP Concur by providing their Username via the SP-initiated flow.

If you need to enforce Mobile SSO only, please contact SAP Concur support.



Section 8: Appendix - Microsoft Azure AD Setup

NOTE: Per the appendix instructions in this section, as content is sourced from the third-party provider, SAP Concur cannot guarantee its accuracy. If you encounter issues, it is recommended that you contact the third-party provider's support resources.

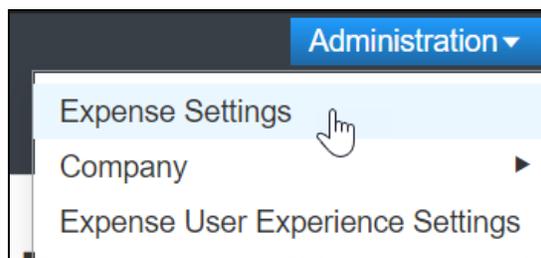
Getting Started

Before you start the configuration process, ensure that:

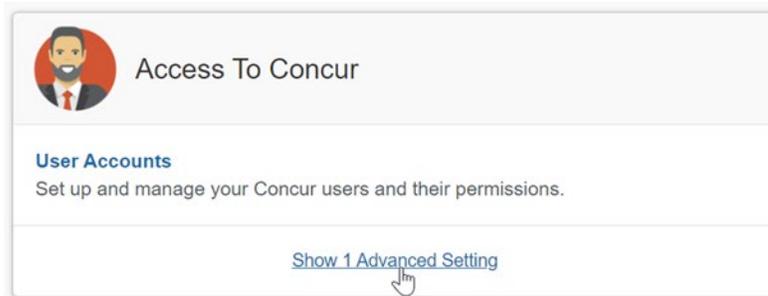
- Your users exist in both Azure AD and SAP Concur. Auto user provisioning is not currently supported by SAP Concur, so you need to add users separately in there.
- The attribute you are sending from Azure AD matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the **Manage SSO** page by using one of the following paths, depending on your SAP Concur edition.

For SAP Concur **Standard** edition:

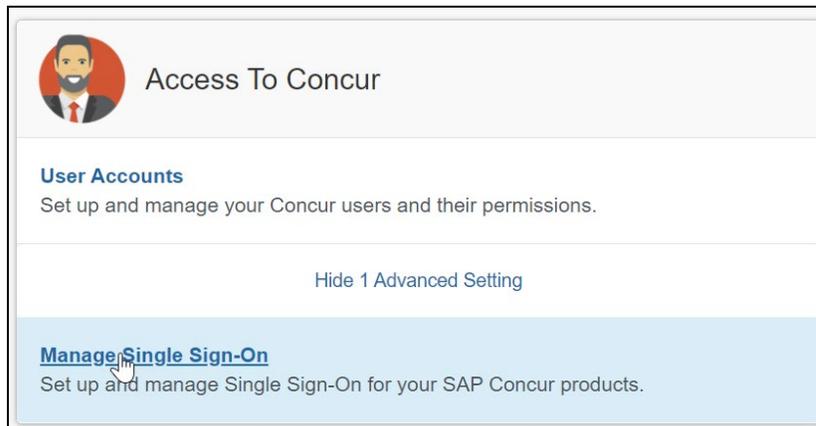
1. Go to **Administration > Expense Settings**.



2. Under Access to Concur section, click **Show 1 Advanced Setting**.

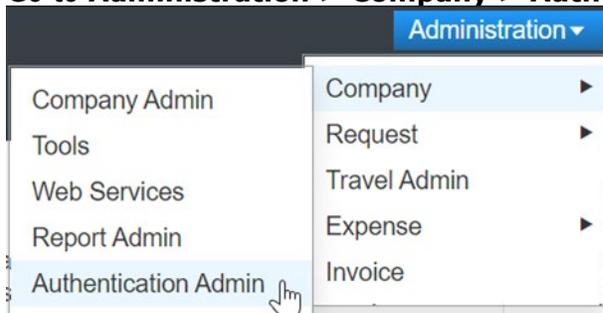


3. Click **Manage Single Sign-On** to access the **Manage SSO** page.

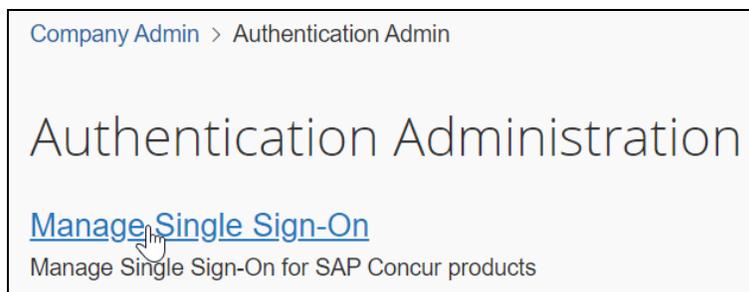


For the SAP Concur **Professional** edition:

4. Go to **Administration > Company > Authentication Admin.**



5. Click **Manage Single Sign-On** to access the Manage SSO page.



Alternatively, users can access the page using one of the following URLs:

- 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>

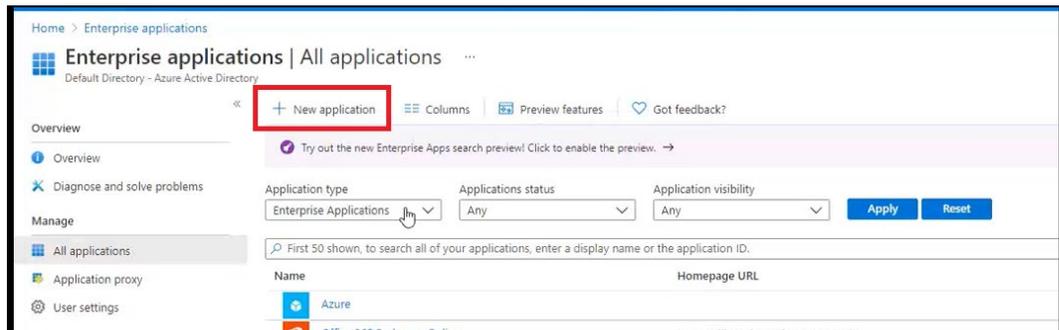
NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an authorized support contact at your company to open a case with SAP Concur support.

Configure Your Azure AD Application

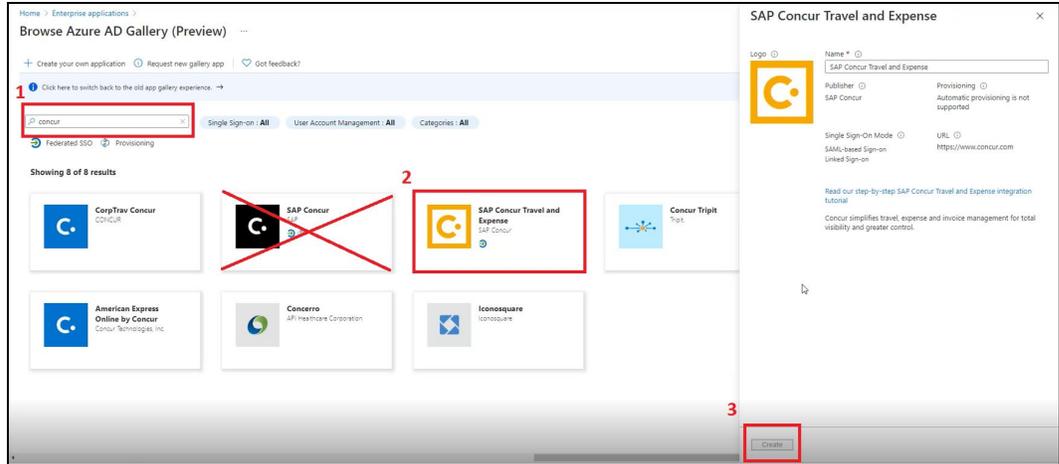
Please see the [Microsoft Azure AD Guide](#) as an additional reference for this section.

Step 1: Create Gallery Application

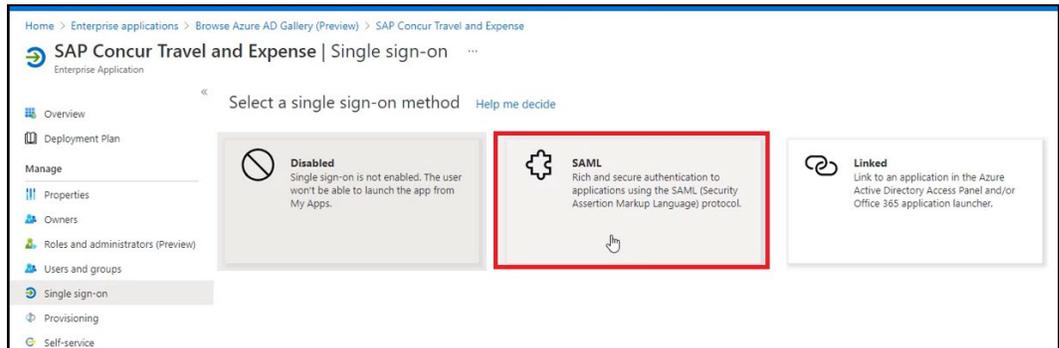
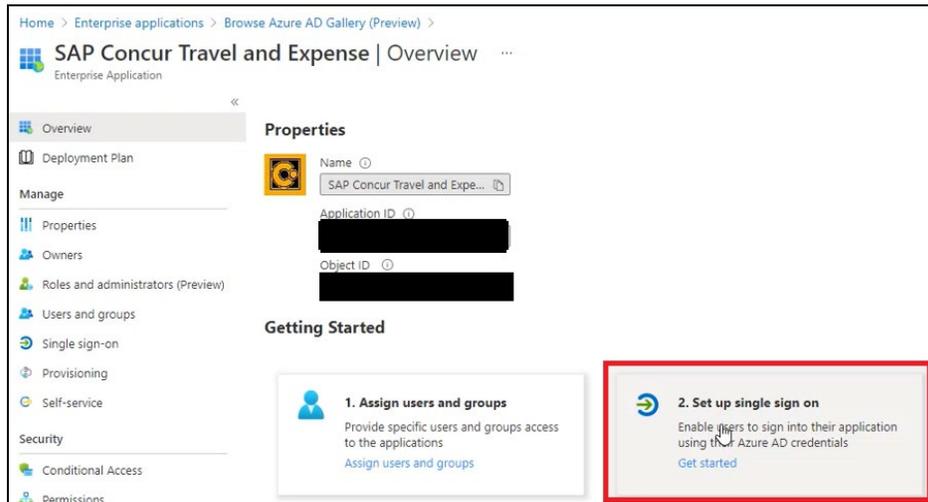
1. Go to **Home > Enterprise applications** and then click **New Application**.



2. Search for **Concur**.
3. Select the **SAP Concur Travel and Expense** option. Do not use the SAP Concur option with the black icon as this is used for the Legacy SSO platform and not the recommended SAML2 SSO platform.



4. Click **Create**.
5. Click **Set up Single sign on** and then click on **SAML**.



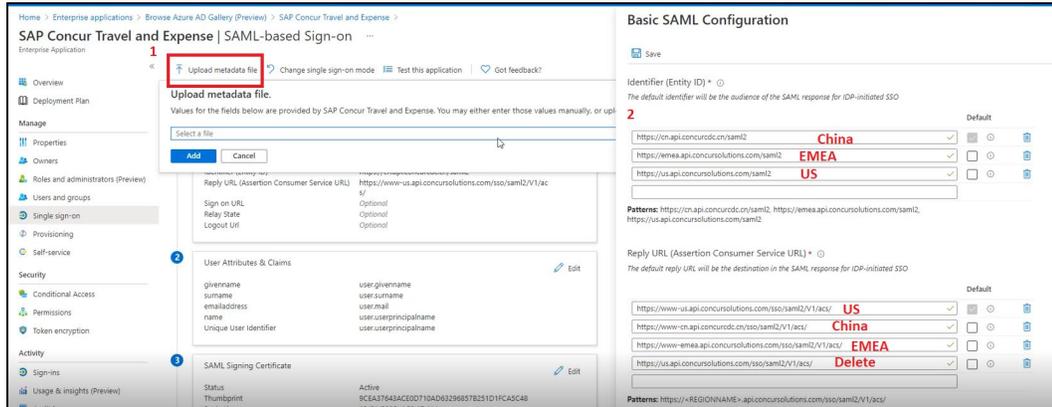
Step 2: Provide Azure ID with Identifier and Reply URL

1. Upload the SAP Concur Metadata by clicking the "upload metadata file".

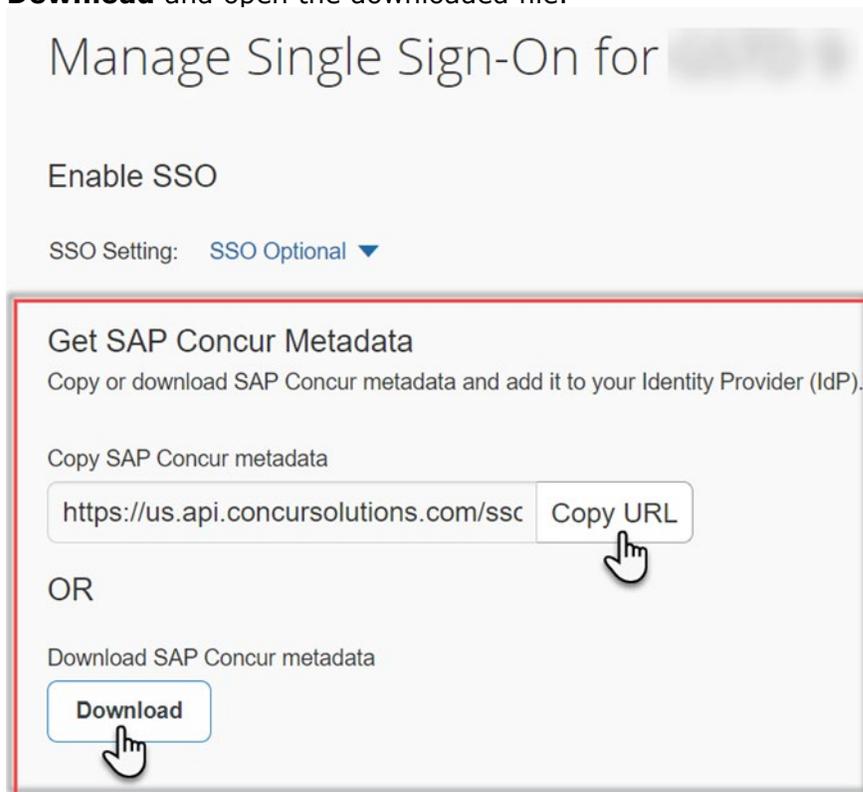
OR

2. Click **Edit** for the **Basic: SAML Configuration** option and remove the Identifiers (Entity IDs) and Reply URLs (Assertion Consumer Service URLs) that are not relevant for the datacenter your SAP Concur entity is on.

NOTE: For SAP Concur Test Entities you will always need to upload the SAP Concur Metadata to get the correct Identifiers (Entity IDs) and Reply URLs (Assertion Consumer Service URLs).



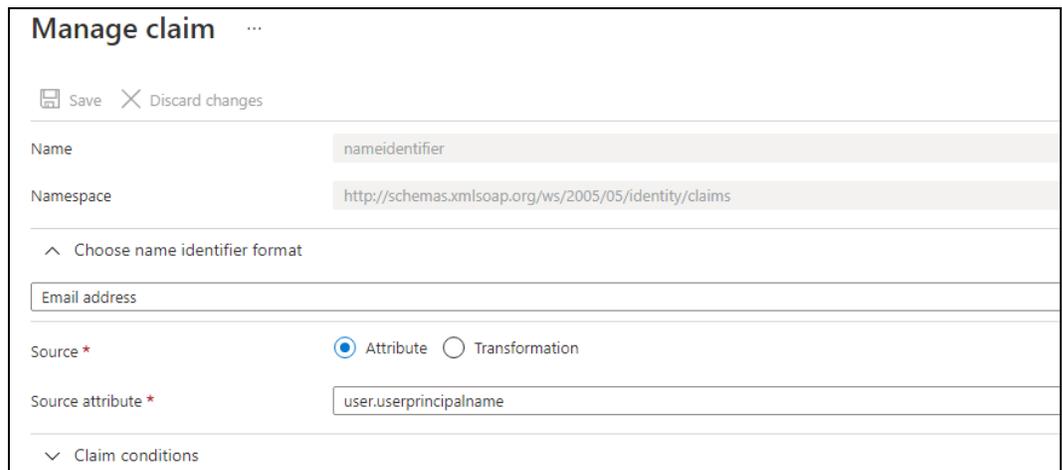
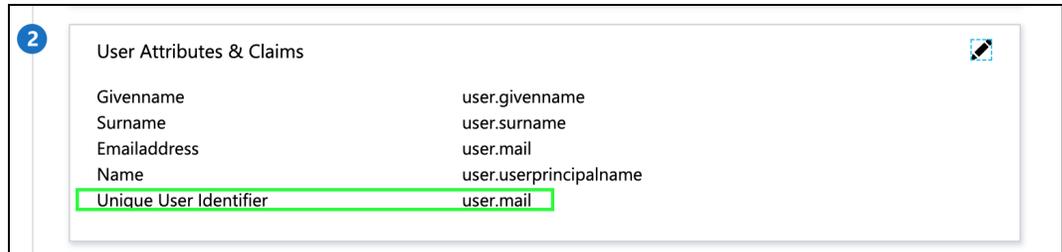
3. To obtain the SAP Concur metadata on the Manage SSO page, you can either click **Copy URL** and then paste the URL in a new browser tab or click **Download** and open the downloaded file.



Step 3: Change Unique User Identifier

The default Unique User Identifier is **user.userprincipalname**. In SAP Concur, the Unique User Identifier must use the email address format.

1. Click the pencil icon to edit this field under the **User Attributes & Claims** section.
2. Change the **user.userprincipalname** to "user.mail". After you make this change, it should look like the following screenshot.



If your login IDs in SAP Concur do not match email address, you can still build customizations on the unique user identifier, so it sends a different value to SAP Concur. However, for any transformation rule please ensure you still send it with the email address format. Different formats would affect the logins made on the mobile app and/or via concursolutions.com.

Step 5: Download the Azure AD Metadata File

Click **Download** to download the "Federation Metadata XML" and save the metadata to your local computer or click on the paper icon to copy the "App Federation Metadata Url".

3
SAML Signing Certificate ✎

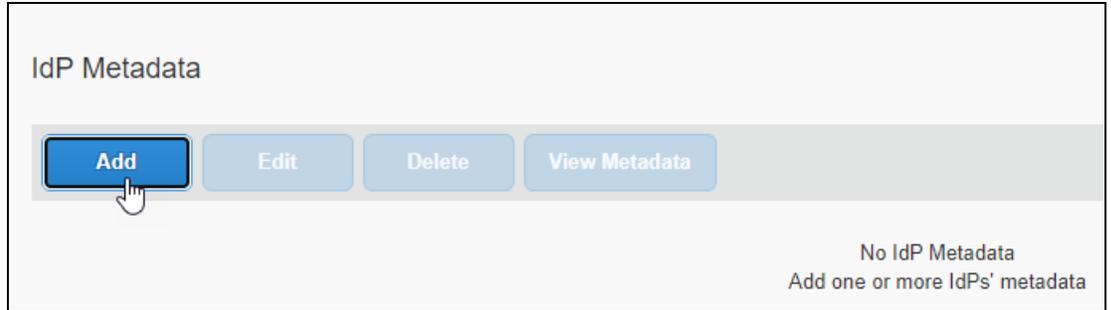
Status	Active
Thumbprint	D6D04C72318A683B457142A04C7DA67C4F9A8F4B
Expiration	6/10/2022, 4:44:49 PM
Notification Email	concurcoretest@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/382a5a1c-567a-4... 📄
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

NOTE: Before you upload your metadata file to SAP Concur, please make sure the **User assignment required?** setting via **Manage > Properties** is set accordingly. If set to the recommended setting of **Yes**, then you'll need to add users under **Users and groups**.

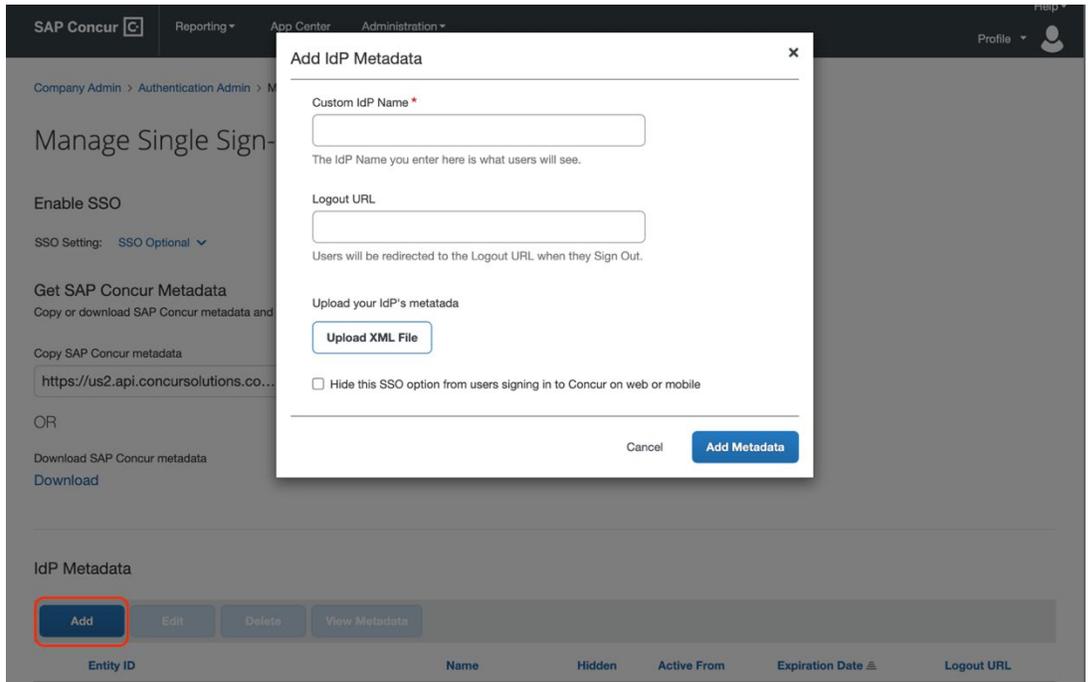
The screenshot shows the 'Concur - Properties' page in the Azure AD portal. The left sidebar contains navigation options like Overview, Deployment Plan, Manage, Security, Activity, and Troubleshooting + Support. The main content area shows various configuration fields for the application, including Name (Concur), Homepage URL, Logo, User access URL, Application ID, Object ID, Terms of Service URL, Privacy Statement URL, and Reply URL. The 'User assignment required?' toggle is highlighted with a red box and is currently set to 'Yes'. Other toggles include 'Enabled for users to sign-in?' (Yes) and 'Visible to users?' (Yes).

Configure Your SAP Concur Site

1. Go to the **Manage SSO** page by following the steps provided in the Overview section.
2. Click **Add** from the **IdP Metadata** section.

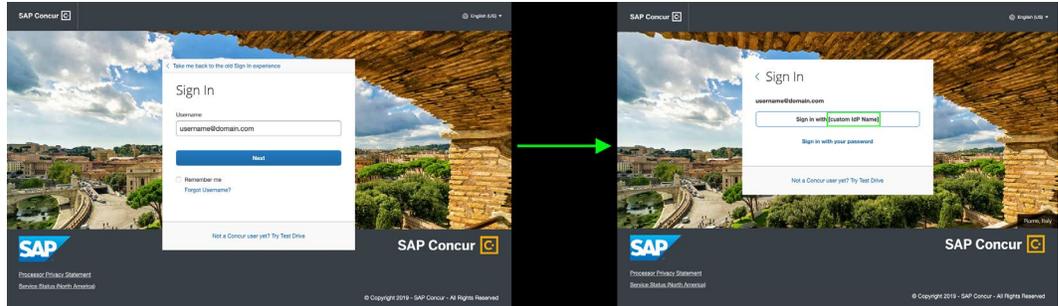


The **Add IdP Metadata** window appears.

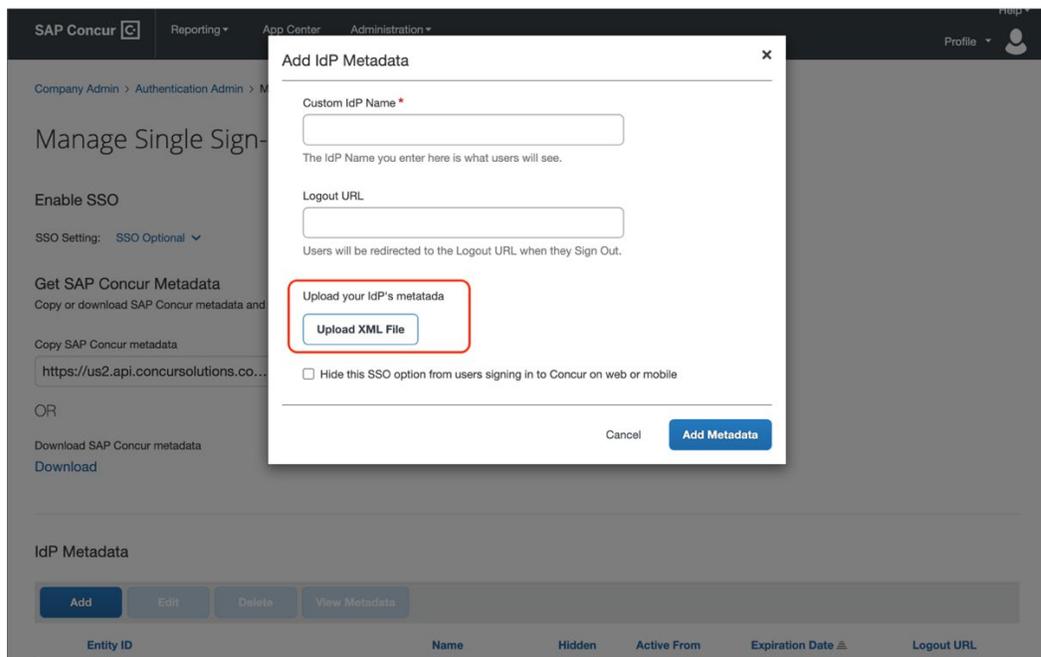


3. Enter an appropriate name in the **IdP connection** and enter it in the **Custom IdP Name** field.

NOTE: If you decide to use the SP-initiated flow (through SAP Concur’s public site: <https://www.concursolutions.com/nui/signin>), the **Custom IdP Name** will display on the **Sign In** page right after you provide the Username and click **Next**. For example, if your **Custom IdP Name** is "Azure", then you will see the **Sign in with Azure** option.

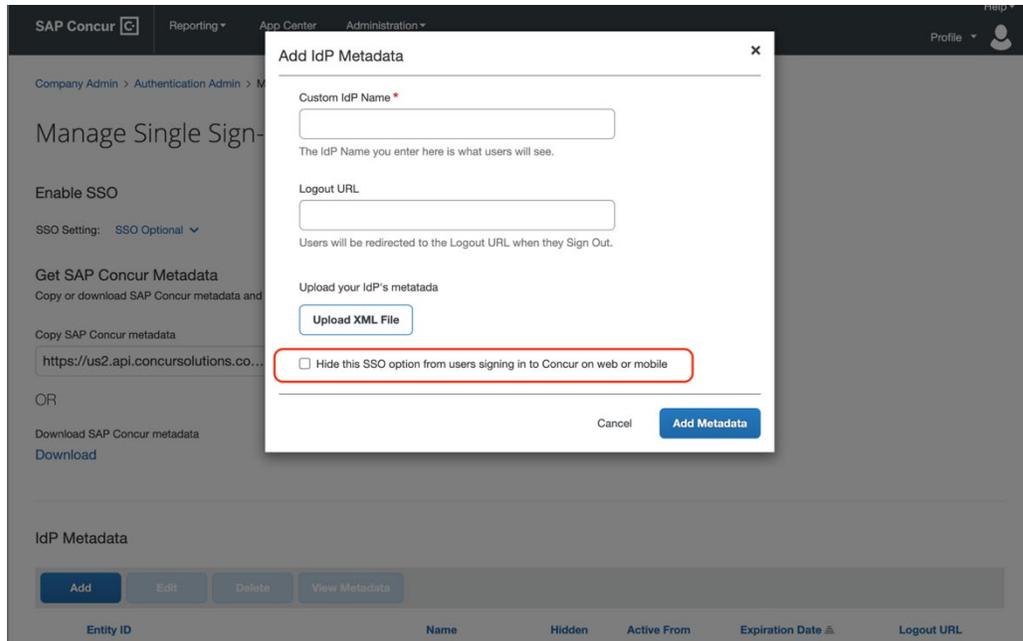


4. Provide a **Logout URL** (optional) for users to get redirected to a different place when they log out. By default, if no URL is entered, users will be redirected to where they started the authentication process.
5. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP which was previously saved locally.

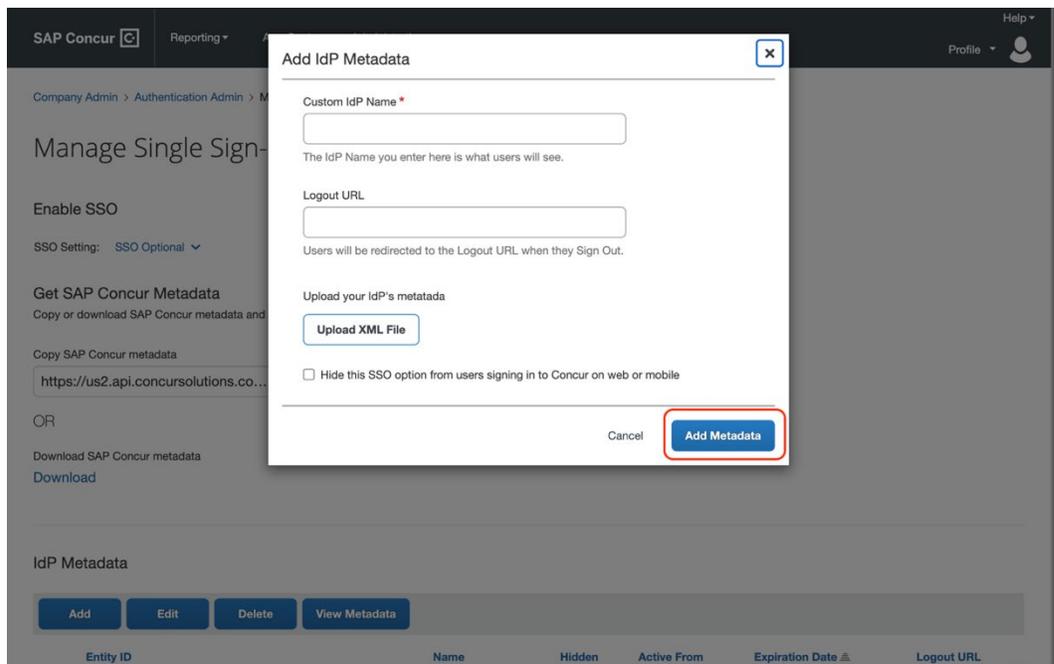


6. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox **Hide this SSO option from users signing in to Concur on web or mobile**.

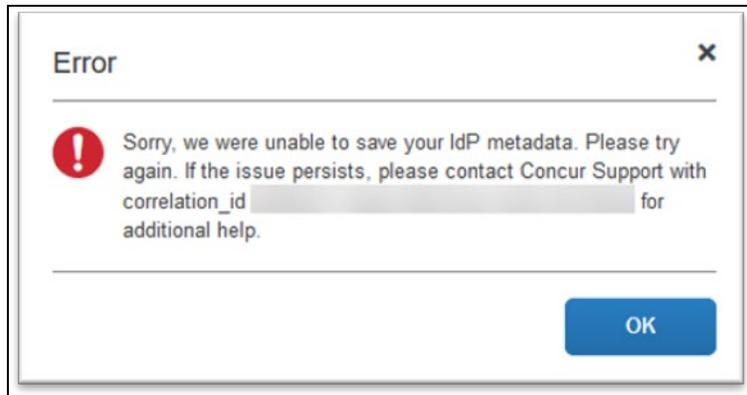
By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.



7. Click **Add Metadata**.



8. A successfully added confirmation or a something went wrong message displays. For the latter, please contact SAP Concur support and provide the Correlation ID.



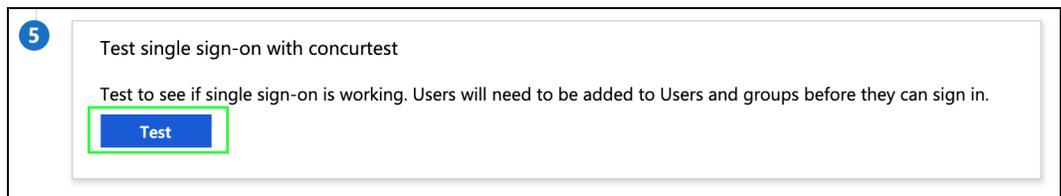
Test SSO Login

You can start testing SSO after you've successfully uploaded the IdP metadata to SAP Concur from the previous steps. In this section, you can test the IdP-Initiated (initiated on the identity provider side) and SP-Initiated (initiated on the service provider side) flows.

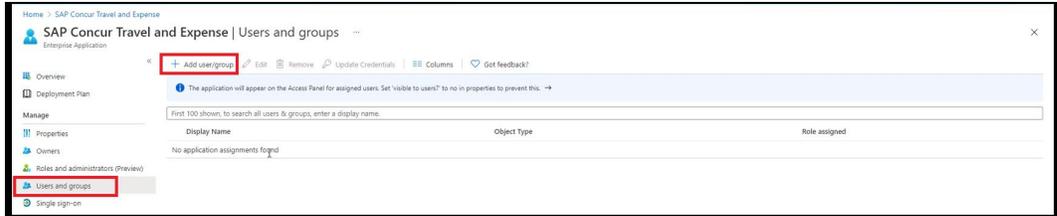
Test IdP-initiated SSO

(Option 1) To test IdP-initiated SSO with Test button:

1. If the same account with the same email address at Azure AD exists in SAP Concur, you can click **Test** in Azure to do a test login for the IDP-initiated flow. You will still need to test the SP-Initiated flow, as it will be important for Mobile SSO tests.

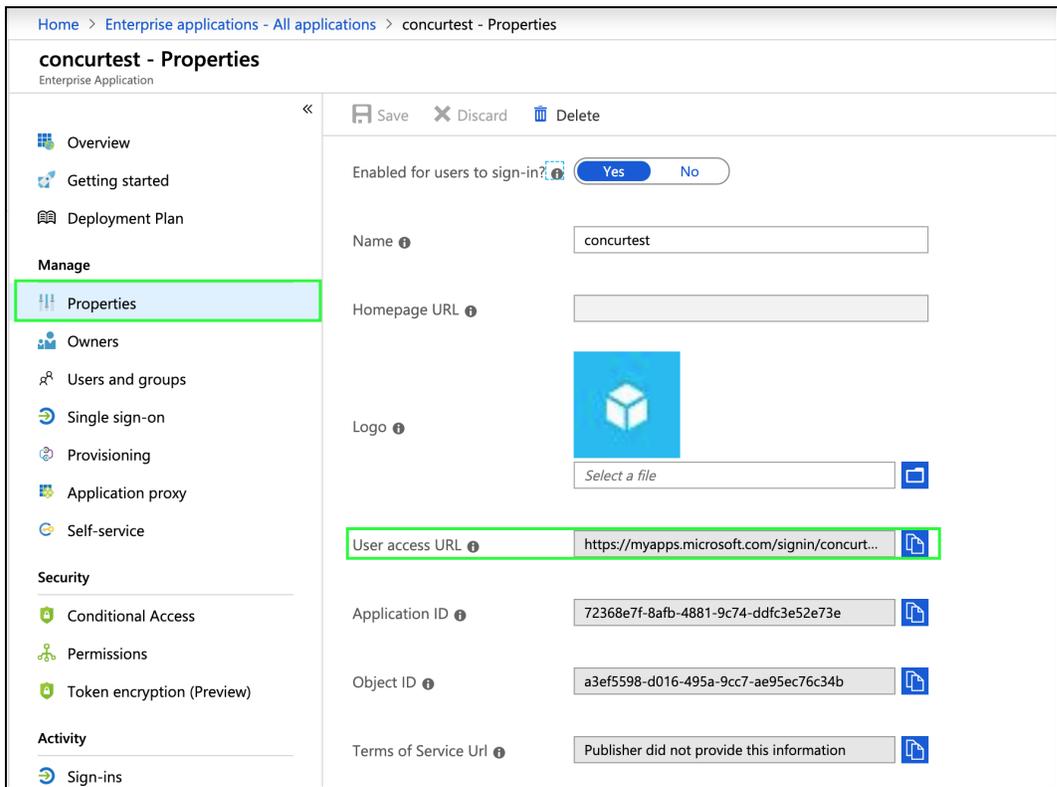


Before you test SSO, add additional users from Azure AD to this test application you just configured. To do so, click **Users and groups** and **+ Add user**.



(Option 2) To test IdP-initiated SSO with User Access URL:

1. Go to **Manage > Properties** and then copy the **User access URL**. Give this URL to your test users and ask them to copy paste this URL in the browser. They will see a Microsoft login page first. After that, they will be authenticated to SAP Concur directly without any other action.



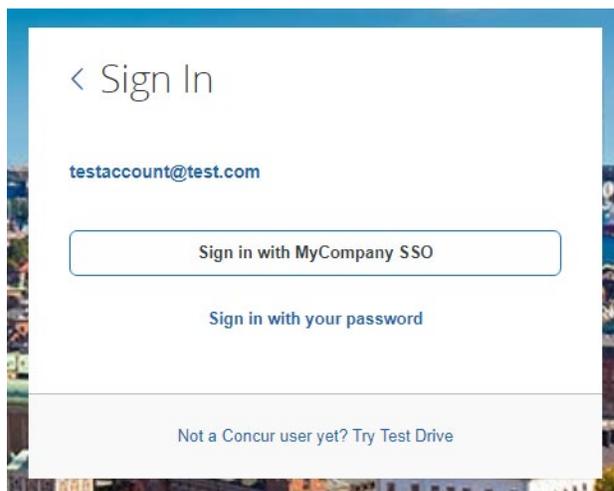
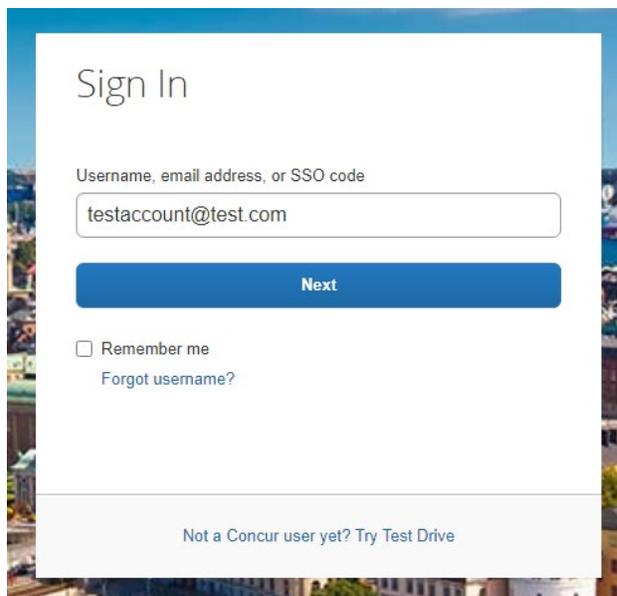
(Option 3) To test IdP-initiated SSO with Microsoft 365:

1. After you assign the application to a few test users, they will see a new application appear on their Microsoft 365 portal. The user can click on the new application and then they should be authenticated directly to SAP Concur. The URL behind the SAP Concur application icon is the same as User access URL from the first test option.

Test SP-initiated SSO

To test the SP-initiated SSO:

1. Open the SAP Concur login page according to the environment you want to test.
 - ◆ 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. On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click **Next**, you should see an option for your recently created SSO configuration. Click to proceed with authenticating your identity provider account which should redirect you to SAP Concur.



Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated using the previous *Test SSO login* section.

NOTE: The automatic enabling of Mobile SSO is only visible on the app version 9.86 or higher and if the user is opting for the new sign in experience. Users on older versions or opting for the earlier sign in experience will not see this option automatically. In that case, to guarantee that users are also able to log in with SSO on their mobile devices, please open a ticket with the SAP Concur support team providing the User Access URL from the application built on the Azure side so they can enable Mobile SSO for the legacy app versions. You can obtain this URL via **Manage > Properties** on your Azure admin account

If you have any issues in authenticating with SSO on the mobile app, please open a ticket with the SAP Concur support team and provide any error IDs and/or messages received with screenshots.

E-mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket with the SAP Concur support team, providing the IDP URL from the application created on the IDP side so they can adjust the redirect URL for e-mail reminders. For more information on how to obtain the URL, see the *Test SSO login > Testing IdP-Initiated SSO* section of this appendix.

Rollout

After testing your new SSO configuration, you can then plan your rollout by assigning your new Azure AD application to all your users and groups who'll need this access.

The Manage SSO page also offers the option for you to enforce this new SSO connection by changing the SSO Setting from SSO Optional to **SSO Required**. If you change it, users will be redirected to SAP Concur by providing their username via the SP-initiated flow.

If you need to enforce Mobile SSO only, please contact SAP Concur support.



Section 9: Appendix – Google Workspace Setup

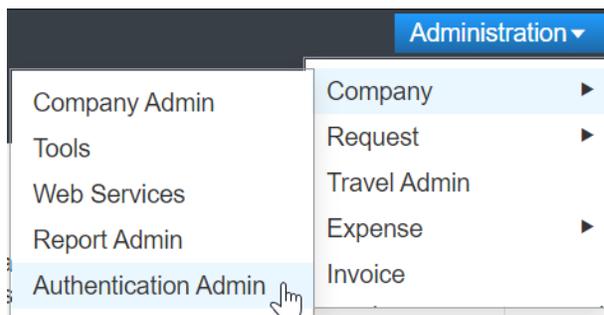
Overview

Before you start the configuration process, make sure that:

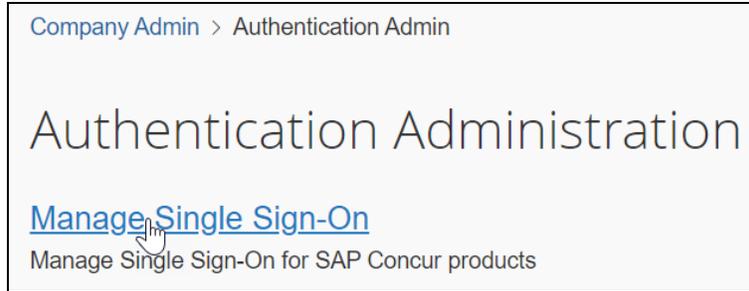
- You have admin access to the identity provider (Google Workspace). This will be needed so you can complete the application configuration on the Google Workspace side.
- Your users exist in both Google Workspace and SAP Concur. Auto user provisioning is not currently supported by Concur, so you need to add users separately in there.
- The attribute you are sending from Google Workspace matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the Manage SSO page by following one of the below paths, depending on your SAP Concur edition.

SAP Concur Professional edition:

3. Go to **Administration > Company > Authentication Admin.**



4. Hit **Manage Single Sign-On** to access the **Manage SSO** page.



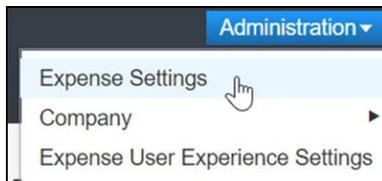
Alternatively, users can access the page using one of the following URLs:

- ◆ **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>

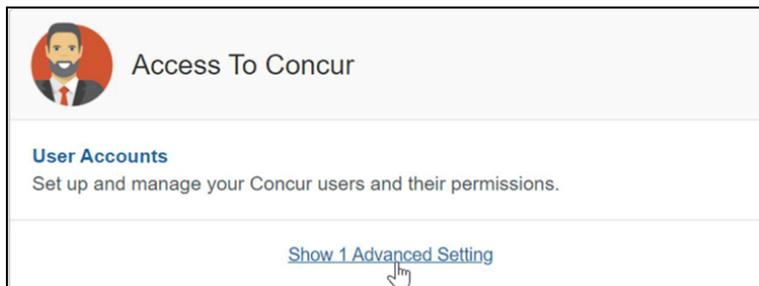
NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an Authorized Support Contact at your company to open a case with SAP Concur Support.

SAP Concur Standard edition:

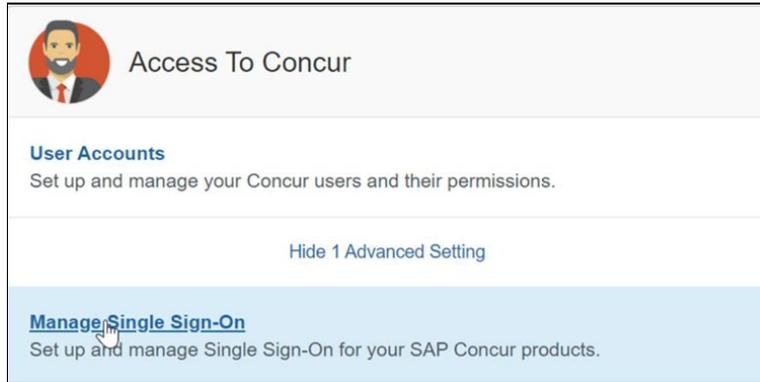
1. Go to **Administration > Expense Settings**.



2. Under **Access to Concur** click **Show 1 Advanced Setting**.



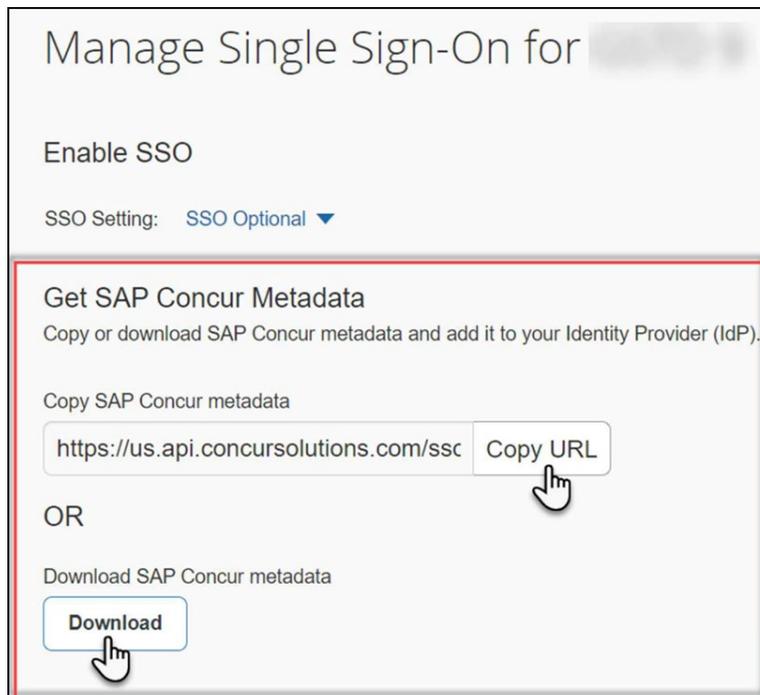
3. Click **Manage Single Sign-On** to access the **Manage SSO** page.



Configure Your Google Workspace (IDP) APP

Step 1: Get the SAP Concur metadata

To complete this you will need to follow the instructions on the **Preparation** section earlier in this guide login to your SAP Concur account and access the **Manage SSO** section. To obtain the **SAP Concur Metadata** on the **Manage SSO** page, you can either click on "Copy URL" and then paste the URL in a new browser tab or click **Download** and open the downloaded file.



Step 2: Set up your own custom SAP Concur SAML app

1. Sign into your **Google Admin** console.

NOTE: (Sign in using an account with super administrator privileges (does not end in @gmail.com or similar)).

2. From the Admin console Home page, go to **Apps Web** and mobile apps.
3. Click **Add App** to add **custom SAML** app.
4. On the **App Details** page:
 - ◆ **Custom app name**
Enter the name of the custom app, for example, '**SAP Concur**'
 - ◆ *(Optional)* **Upload an app icon**
The app icon appears on the Web and mobile apps list, on the app settings page, and in the app launcher. If you don't upload an icon, an icon is created using the first two letters of the app name
5. Click **Continue**.
6. On the **Google Identity Provider details** page, get the setup information needed by the service provider using the **Download the IDP metadata** option.
7. *(Optional)* In a separate browser tab or window, sign into your service provider and copy the information you entered in Step 4 into the appropriate SSO configuration page, then return to the Admin console.
8. Click **Continue**.
9. In the **Service Provider Details** window, enter the following ACS URL and Entity ID for your app.

ACS URL

 - **US (North America):** <https://www-us.api.concursolutions.com/sso/saml2/V1/acs/>
 - **EMEA:** <https://www-emea.api.concursolutions.com/sso/saml2/V1/acs/>
 - **China:** <https://www-cn.api.concurcdc.cn/sso/saml2/V1/acs/>

Entity ID

 - **US (North America):** <https://us.api.concursolutions.com/saml2>
 - **EMEA:** <https://emea.api.concursolutions.com/saml2>
 - **China:** <https://cn.api.concurcdc.cn/saml2>
10. The default **Name ID** is the primary email - multi-value input is not supported.
11. Click **Finish**.

Step 3: Turn on your SAML app

1. Sign into your **Google Admin** console.

NOTE: (Sign in using an account with super administrator privileges (does not end in @gmail.com or similar)).

2. From the Admin console Home page, go to **AppsWeb and mobile apps. +**.
3. Select your SAML app.
4. Click **User access**.
5. To toggle availability of a service for your organization, click **On** for everyone or **Off** for everyone, and then click **Save**.
6. (*Optional*) To turn a service on or off for an organizational unit:
 - ◆ At the left, select the **organizational unit**.
 - ◆ To change the Service status, select **On** or **Off**.
 - ◆ Choose one:
 - If the Service status is set to Inherited and you want to keep the updated setting, even if the parent setting changes click **Override**.
 - If the Service status is set to Overridden, either click **Inherit** to revert to the same setting as its parent, or click **Save** to keep the new setting, even if the parent setting changes.
7. To turn on a service for a set of users across or within organizational units, select an **access group**. For details, go to *Provide access to user groups* in this document.
8. Ensure that the **email addresses** your users use to sign in to the SAML app match the **email addresses** they use to sign into your Google domain. Changes typically take effect in minutes but can take up to 24 hours.

NOTE: Google Workspace doesn't support encryption of assertion currently. Please reach out to the IDP support if you need more information around this.

Step 4: Configure Your SAP Concur Site

1. Go to the **Manage SSO** page again by following the steps provided on the **Preparation** section.
2. Click on **Add** under **IdP Metadata** section. The **Add IdP Metadata** window appears.
3. Give your IdP connection a friendly name and enter it in the **Custom IdP Name** field.

4. Provide a **Logout URL** (optional), so the users get redirected to a different place when signing out.

By default, if no URL is entered, users will be redirected to where they started the authentication process. The logout endpoint for Google Workspace can be found on **Applications & Resources > Tenant Settings > Identity Provider Settings > Single Logout Endpoint**.

NOTE: Single Logout (SLO) is not officially supported by SAP Concur, so the logout process with the SLO endpoint may not work as expected regarding disconnecting the user from the IDP in addition to Concur. In that case, the user may be logged out from SAP Concur but not from Google Workspace entirely.

5. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP, which was previously saved locally.
6. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the **Hide this SSO option from users signing in to Concur on web or mobile** checkbox.

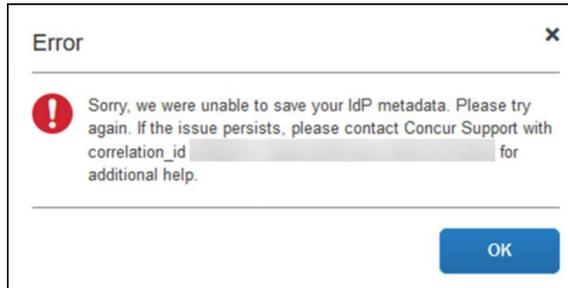
By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow

The screenshot shows a modal dialog titled "Add IdP Metadata" with the following fields and options:

- Custom IdP Name*:** Text input field containing "SAP IAS".
- Logout URL:** Text input field containing "https://help.sap.com".
- IdP Metadata*:** Two radio button options:
 - Provide link to your IdP's metadata
 - Upload your IdP's metadata
- Upload XML File:** A button next to the selected option, with a file named "SAP IAS Metadata.xml" listed next to it.

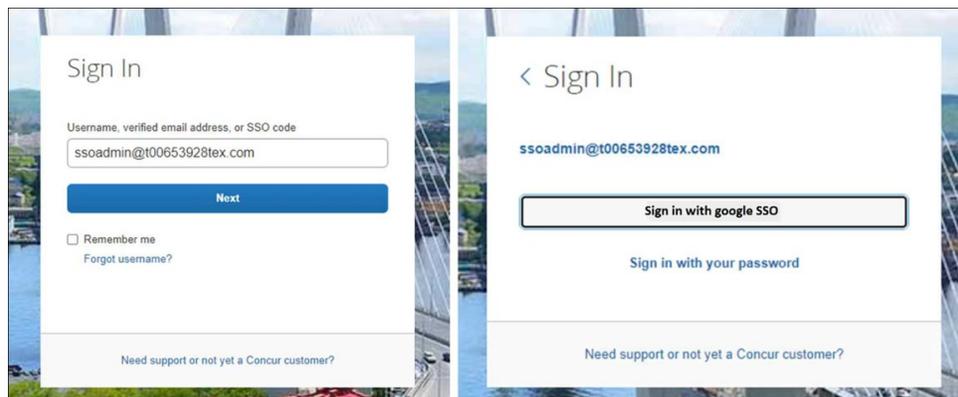
At the bottom of the dialog are "Cancel" and "Add Metadata" buttons. The background shows a blurred view of the SAP Concur interface, including a "Download SAP Concur metadata" button and "IdP Metadata" section.

7. Click **Add Metadata**.
8. A successfully added or something went wrong message displays.



For help with the second one (above) please reach out to *SAP Concur Support* and provide the correlation id.

For step 3 above, if you decide to use the *SP-initiated flow* (through SAP Concur's public site: <https://www.concursolutions.com/nui/signin>), the **Custom IdP Name** will be displayed on the **Sign In** page right after a user provides their **Username** and hits **Next** (see below image). For example, if your "Custom IdP Name" is "google SSO", then all users will see the option "Sign in with google SSO" as shown in the following:



Test SSO Login

You can start testing SSO after you've successfully uploaded the IdP metadata to *SAP Concur* from the previous step. We'll test the **IdP-Initiated** (initiated on the identity provider side) and **SP-Initiated** (initiated on the service provider side) flows.

1. TESTING IDP-INITIATED SSO

In the IdP-Initiated flow we start the login process on the identity provider. To test it, we can append parameters from the application we built to the SSO endpoint from Google Workspace.

An example of IdP-Initiated URL is:

Format: `https://accounts.google.com/o/saml2/initssso?idpid=CLIENT_IDP_ID&spid=SERVICE_PROVIDER_ID&forceauthn=false`

Example: `https://accounts.google.com/o/saml2/initssso?idpid=C03fj4v82&spid=710982774547&forceauthn=false`

NOTE: You must fill CLIENT_IDP_ID and SERVICE_PROVIDER_ID with values from Google Workspace and it's something you can get by copying the URL from the **Test SAML login** button on the application

2. TESTING SP-INITIATED SSO

In order to test the SP-initiated flow, you will need to open the SAP Concur login page.

- **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/>

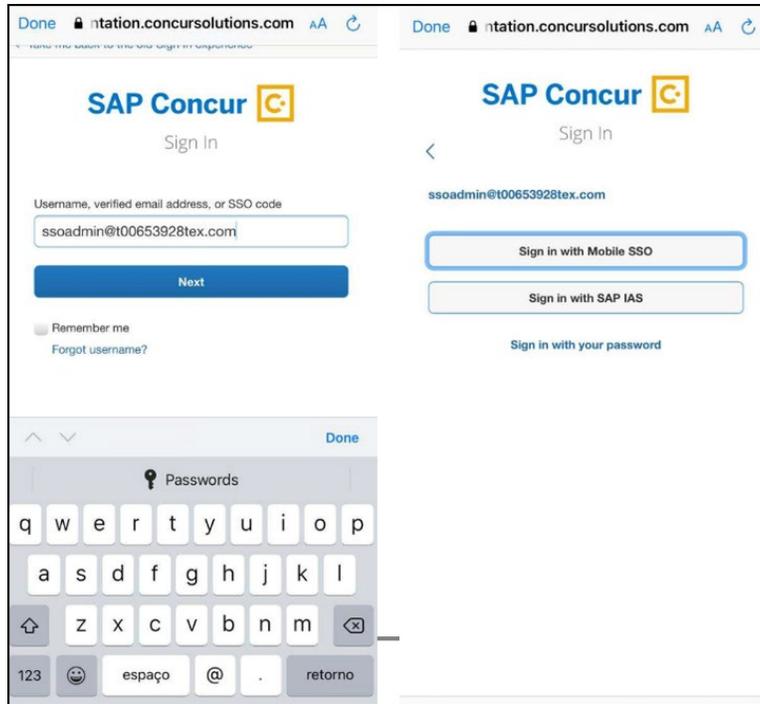
On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click on **Next**, you should see an option for your recently created SSO configuration. You can click on that and proceed with authenticating to your Google account which should redirect you back to SAP Concur after that.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated on the 'Test SSO login' section on this guide.

If you have issues to authenticate with SSO on the mobile app, please open a ticket to the SAP Concur support team providing any error IDs and/or messages received.

It's important to note that if you were using another IdP and you were already using Mobile SSO, you'll probably see 2 options when trying to sign-in as follows:



The **Sign in with Mobile SSO** option will have your old IdP link embedded, so it will redirect users to your old SSO connection.

For both cases, please open a ticket to the SAP Concur support team providing them the following information.

- If the users plan to use an older (legacy) version, provide the IdP-Initiated URL from the application built on the Google Workspace side so Support can enable Mobile SSO for the legacy app versions. More information about how to get the URL can be found on the 'Test SSO login > Testing IdP-Initiated SSO' section on this guide.
- If you want to remove the 'Sign in with Mobile SSO' option so it doesn't confuse your users, please inform that to the support team.

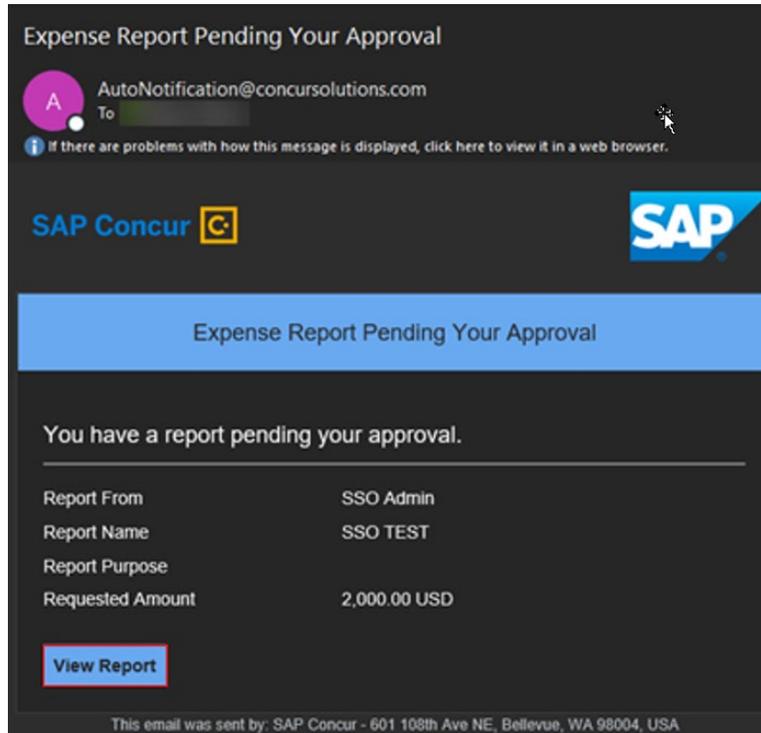
If you have any issues to authenticate with SSO on the mobile app, please open a ticket to the SAP Concur Support team providing any error IDs and/or messages received with screenshots.

E-Mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket to the *SAP Concur* support team providing the IDP URL from the application built on the IDP side so they can adjust the redirect URL for E-Mail reminders. More information about how to get the URL can be found on the *Test SSO login > Testing IdP-Initiated SSO* section on this guide.

- The URL will appear embedded on the **View Report** button

- This change will only be reflected in emails generated after the change - all emails prior to that will keep using the previous URL.
- This change will take effect up to 4 hours after the update.



If you hover the cursor over the **View Report** button you will see what's the URL currently embedded. The URL should appear between "ctedeepurl=" and "&hpo=" terms.

Rollout

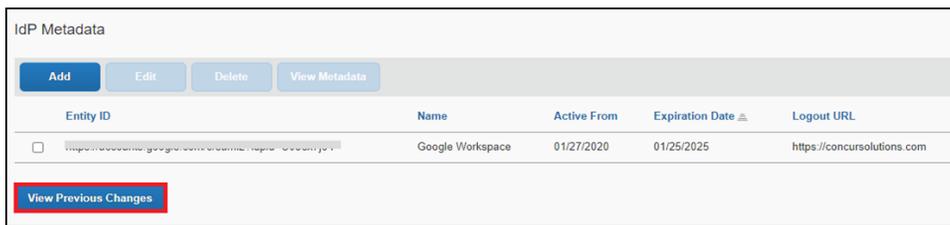
After testing your new SSO configuration, you can then plan your rollout by assigning your Google Workspace application to all your users and groups who'll need this access.

The **Manage SSO** page also offers the option for you to enforce this new SSO connection by changing *SSO Setting* from *SSO Optional* to *SSO Required*. If you change it, users will be redirected to Concur by just providing their Username via SP-initiated flow.



View Previous Changes

This feature was developed to help admins to keep track of all changes completed under the **Manage SSO** page. To view changes to the SSO configuration that have been made over time, click on the **View Previous Changes** button.



A table listing previous changes appears and is sorted in descending order by date and time.

View Previous Changes							
Date	Change	Entity ID	Name	Logout URL	Hidden	Details	
06/08/2022	Edit	[Redacted]	Concur Okta		✓	View	
06/08/2022	Edit	[Redacted]	ray test 2		✓	View	
06/08/2022	Edit	[Redacted]	ray test 2			View	
06/08/2022	Edit	[Redacted]	ray test 2		✓	View	
06/08/2022	Edit	[Redacted]	ray test 2			View	
06/08/2022	Add	[Redacted]	ray test 2		✓	View	
06/07/2022	Delete	[Redacted]	ray test 2			View	
06/07/2022	Edit	[Redacted]	ray test 2			View	
06/07/2022	Add	[Redacted]	ray test 2		✓	View	
06/07/2022	Delete	[Redacted]	ray test 2		✓	View	
06/07/2022	Edit	[Redacted]	ray test 2		✓	View	
06/07/2022	Edit	[Redacted]	ray test 2			View	

The table can display the last 100 changes. Changes that are listed in the table include:

- Add a configuration
- Delete a configuration
- Edit Custom IdP Name, Logout URL, or Hidden fields

To view more detailed information about a specific change listed in the table, click the **View** link for the desired list item.

View Previous Changes						
Date	Change	Entity ID	Name	Logout URL	Hidden	Details
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	Concur Okta		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2			View

Inside each log, you'll see the field **Company** and **Change by** in the format **[first name last name] [(UUID code)]**, which will mean who has performed such action. In case you don't recognize that user, you can always reach out to support requesting further details about it.

For deleted configurations, **View Previous Changes** includes a **Revert** button so you can reinstate the deleted configuration. After the configuration is reinstated, it will be available to users during the sign-in process.

View Previous Changes ✕

Date Changed	05/24/2022
Change	Delete
Company	
Change By	

Entity ID	
Name	
Logout URL	https://logout.com
Hidden	

Metadata

[Blurred metadata text]

Revert OK

-  For more info, please refer to the following documentation resources:
- ◆ SAP Concur - [SSO Overview Guide](#)
 - ◆ SAP Help Portal - [SAP Single Sign-On](#)

Section 10: Appendix - Idaptive Setup

NOTE: Per the appendix instructions in this section, as content is sourced from the third-party provider, SAP Concur cannot guarantee its accuracy. If you encounter issues, it is recommended that you contact the third-party provider's support resources.

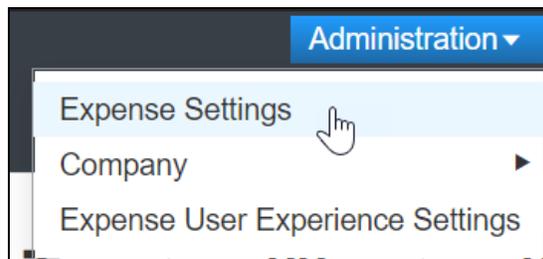
Getting Started

Before you start the configuration process, ensure that:

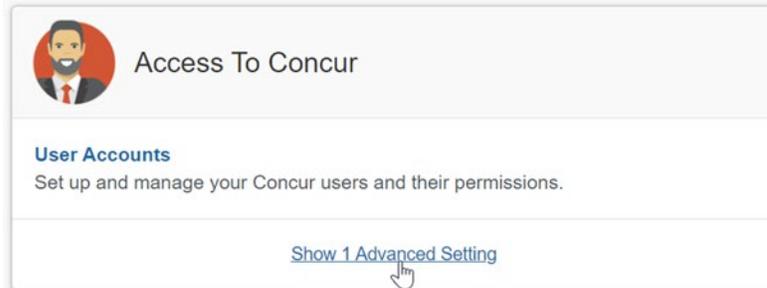
- Your users exist in both Idaptive and SAP Concur. Auto user provisioning is not currently supported by SAP Concur, so you need to add users separately in there.
- The attribute you are sending from Idaptive matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the **Manage SSO** page by using one of the following paths, depending on your SAP Concur edition.

For SAP Concur **Standard** edition:

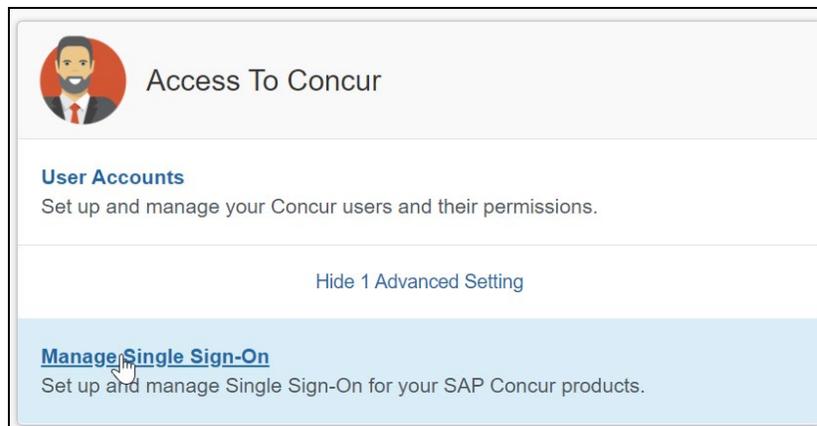
1. Go to **Administration > Expense Settings**.



2. Under Access to Concur section, click **Show 1 Advanced Setting**.

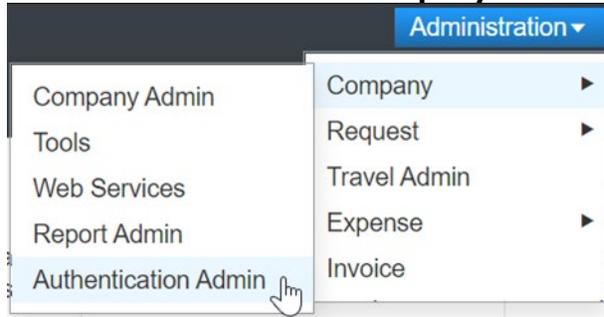


3. Click **Manage Single Sign-On** to access the **Manage SSO** page.

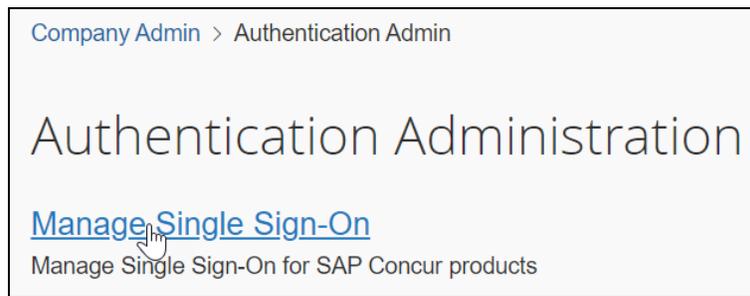


For the SAP Concur **Professional** edition:

1. Go to **Administration > Company > Authentication Admin**.



2. Click **Manage Single Sign-On** to access the Manage SSO page.



Alternatively, users can access the page using one of the following URLs:

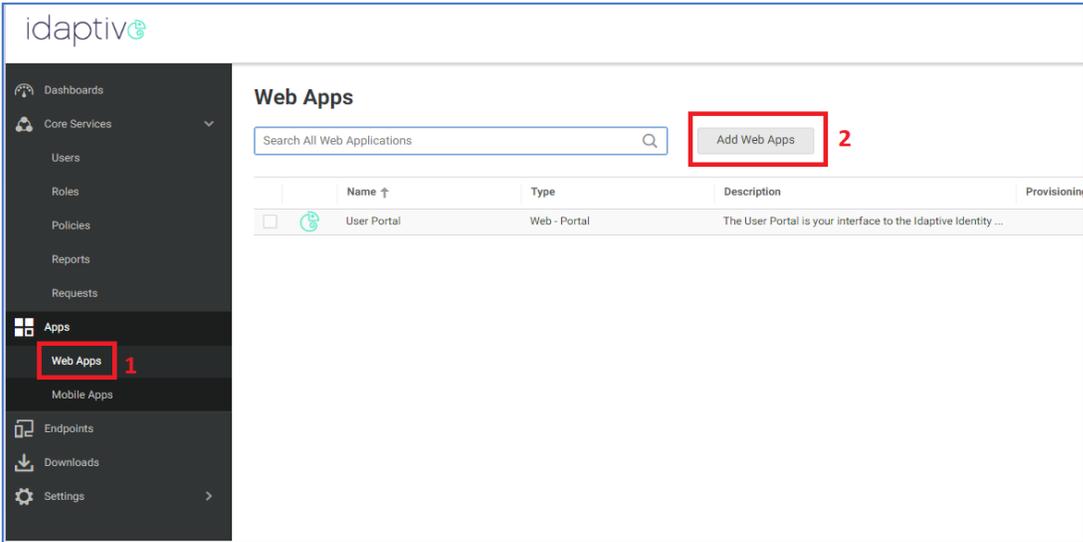
- US DC Prod: <https://www.concursolutions.com/nui/authadmin/ssoadmin>
- US DC Test: <https://implementation.concursolutions.com/nui/authadmin/ssoadmin>
- EMEA DC Prod: <https://eu1.concursolutions.com/nui/authadmin/ssoadmin>
- EMEA DC Test: <https://eu1imp.concursolutions.com/nui/authadmin/ssoadmin>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

NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an authorized support contact at your company to open a case with SAP Concur support.

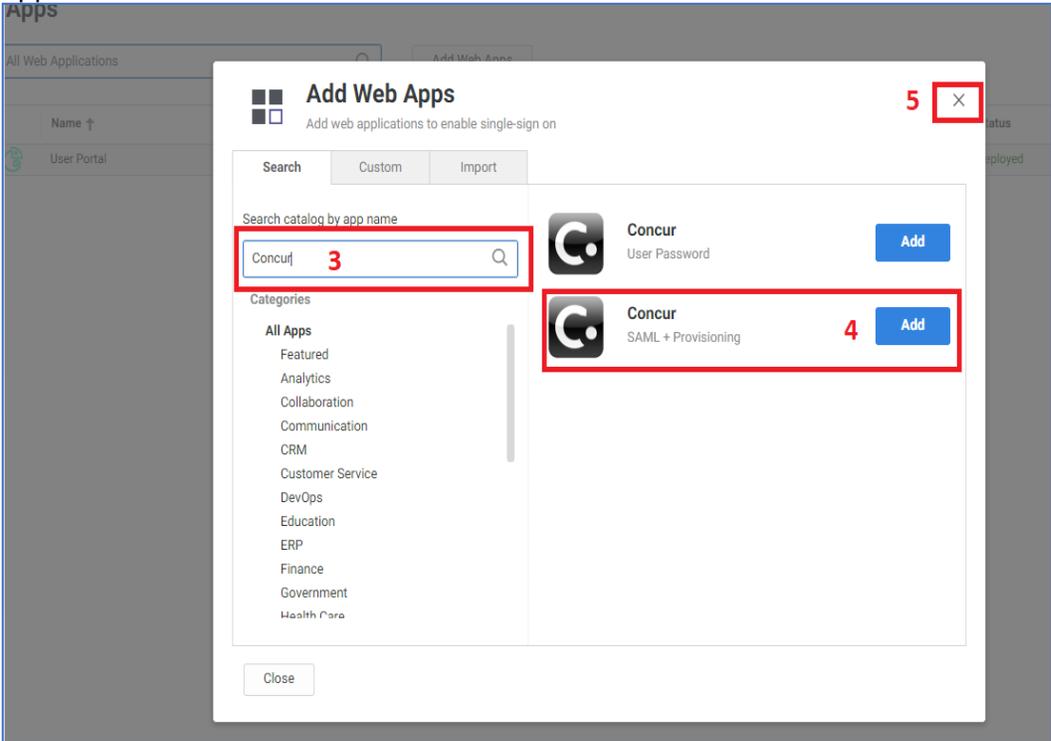
Configure Your Idaptive Application

Step 1: Create the Idaptive app

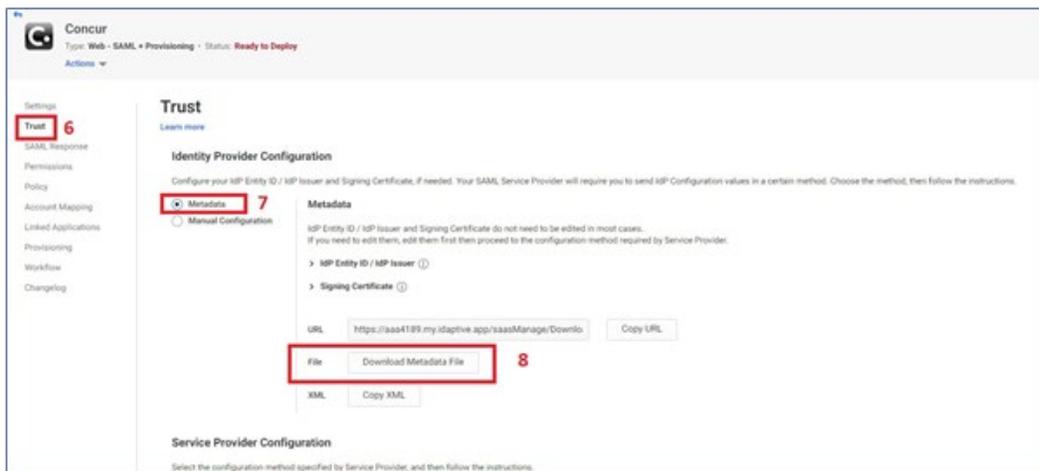
1. From the Idaptive Admin Home page, click **Web Apps**.
2. Click **Add Web Apps**.



- 3. Search for **Concur**.
- 4. By the **SAML + Provisioning** option, click **Add**. Close the popup when it appears.



- 5. In the Concur app configuration, click **Trust**.
- 6. Select the **Metadata** option.
- 7. Click **Download Metadata File** (for later use when uploading your metadata to SAP Concur).



8. Scroll down to the **Service Provider Configuration** section.
9. Open the SAP Concur metadata, copy the **Entity ID** value and paste it to the **SP Entity ID / SP Issuer / Audience** field.
10. Copy the Location value from the metadata and paste it to the **Assertion Consumer Service (ACS) URL**.
11. Ensure that the **Same as ACS URL** option is selected for the Recipient.
12. For the **NameID Format** field, this must match your SAP Concur Login IDs. Select **emailAddress** if your SAP Concur login IDs are in the same format as your email addresses or choose a different option according to the format of your SAP Concur login IDs (e.g., employeeid@companydomain.com). Even though the format of your login IDs may be different than email address, the Name ID format on the SAML Response must be in an email address format.

The screenshot shows the 'Trust' configuration page. At the top, there is a 'Trust' header with a 'Learn more' link. Below this is the 'Service Provider Configuration' section, which is highlighted with a red box and the number 9. It contains two radio buttons: 'Metadata' and 'Manual Configuration', with 'Manual Configuration' selected. Below the radio buttons is the instruction: 'Select the configuration method specified by Service Provider, and then follow the instructions.' The 'Manual Configuration' section is titled 'Manual Configuration' and includes the instruction: 'Fill out the form below with information given by your Service Provider. Be sure to save your work when done.' The form contains several fields: 'SP Entity ID / SP Issuer / Audience' (text input, highlighted with a red box and number 10, containing 'https://emea.api.concursolutions.com/saml2'), 'Assertion Consumer Service (ACS) URL' (text input, highlighted with a red box and number 11, containing 'https://emea.api.concursolutions.com/sso/saml2/V1/acs/'), 'Recipient' (text input, highlighted with a red box and number 12, with a checked checkbox 'Same as ACS URL' and a placeholder 'Enter Recipient here'), 'Sign Response or Assertion?' (radio buttons for 'Response' and 'Assertion', with 'Response' selected), 'NameID Format' (dropdown menu, highlighted with a red box and number 13, showing 'emailAddress'), 'Single Logout URL' (text input, placeholder 'Enter URL here'), 'Encrypt SAML Response Assertion' (checkbox, unchecked), 'Choose File' (button), 'Encryption Certificate (Required)' (text input), and 'Relay State' (text input). At the bottom left, there is a 'Save' button (highlighted with a red box and number 14) and a 'Cancel' button.

- 13. Click **Save**.
- 14. Click **Permissions**.
- 15. Add the groups/users that need to access the SAP Concur app and click **Save**.

The screenshot shows the 'Concur' interface. At the top, there is a 'Concur' header with a logo, 'Type: Web - SAML + Provisioning', and 'Status: Ready to Deploy'. Below this is a 'Permissions' section with a 'Learn more' link. The 'Permissions' section is highlighted with a red box and the number 15. It contains an 'Add' button (highlighted with a red box and number 16) and a table with columns for 'Name', 'Grant', 'View', and 'Run'. The table has one row with the name 'sysadmin', a checked 'Grant' box, a checked 'View' box, and an unchecked 'Run' box.

Configure Your SAP Concur Site

1. Go to the **Manage SSO** page by following the steps provided in the Overview section.
2. Click **Add** from the **IdP Metadata** section. The **Add IdP Metadata** window appears.
3. Enter an appropriate name in the **IdP connection** and enter it in the **Custom IdP Name** field.

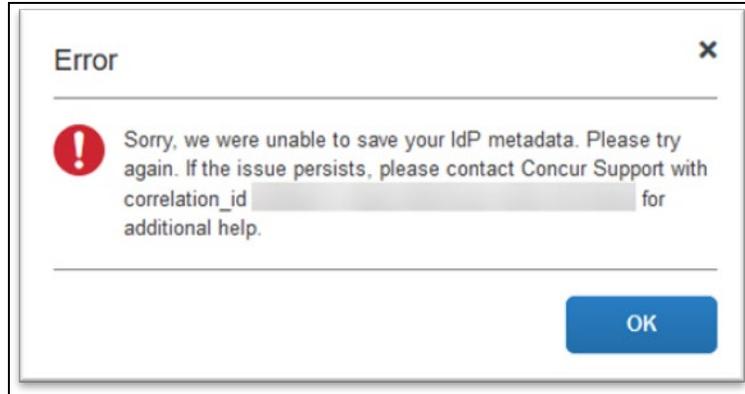
NOTE: If you decide to use the SP-initiated flow (through SAP Concur's public site: <https://www.concursolutions.com/nui/signin>), the **Custom IdP Name** will display on the **Sign In** page right after a user provides their Username and clicks **Next**.

4. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP.
5. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox Hide this SSO option from users signing in to Concur on web or mobile.

By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.

6. Click **Add Metadata**.
7. You should see either a successfully added confirmation or a something went wrong message. For the latter, please contact SAP Concur support and provide the Correlation ID.





Test SSO Login

Test IdP-initiated SSO

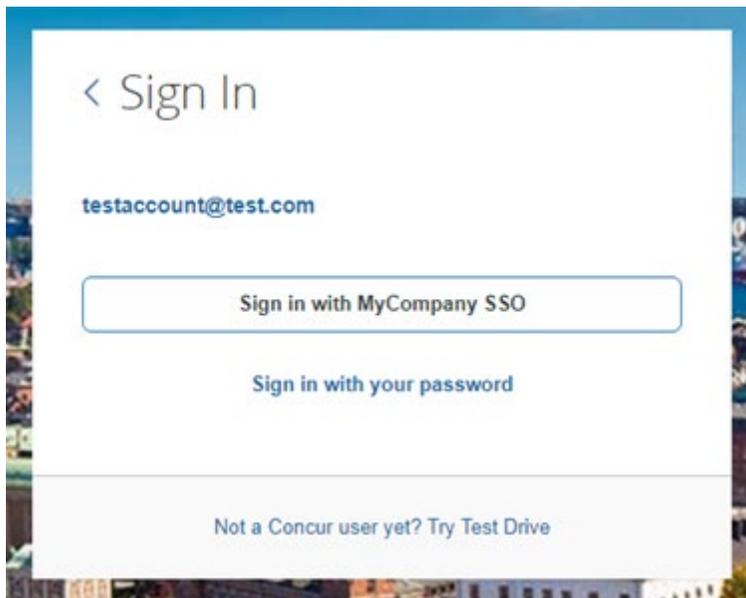
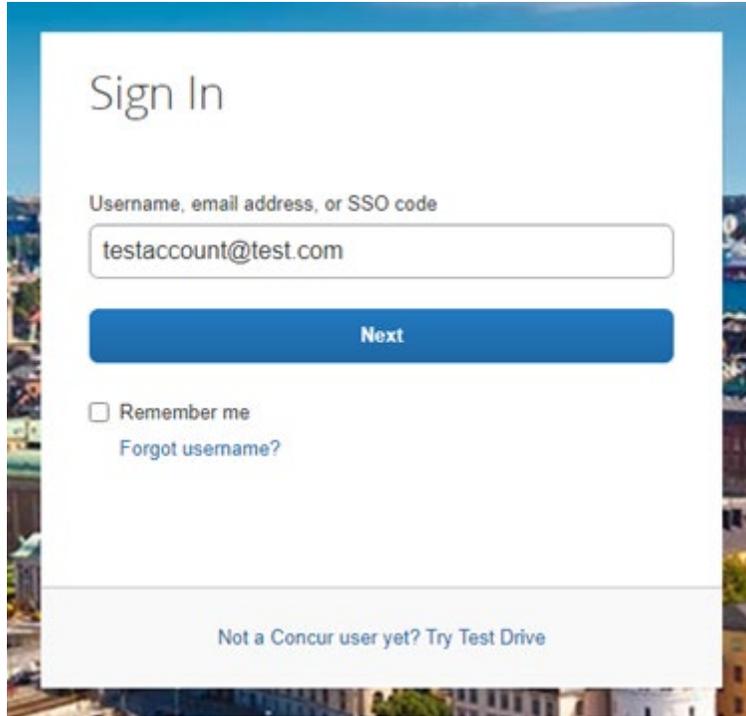
To test your SSO login from Idaptive, you'll need to make sure you've assigned the new application configured in Idaptive to the users and groups who will test this.

Once this is completed, you can login to your account in Idaptive and look for the SAP Concur application. This application should redirect you to your account on SAP Concur, already logged in.

Test SP-initiated SSO

To test the SP-initiated SSO:

1. Open the SAP Concur login page according to the environment you want to test.
 - ◆ 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. On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click **Next**, you should see an option for your recently created SSO configuration according to the note in *Configure Your SAP Concur Site*. Click to proceed with authenticating your identity provider account which should redirect you to SAP Concur.



If after adding your SSO credentials you receive an error message, this is a sign that your configuration is possibly not completed. If the error message is on the SAP Concur side. It may be an issue of unmatching credentials, an invalid certificate, or a missing setting. If the IdP-Initiated login is working but the SP-Initiated is not, this could be sure to the Name ID on the Idaptive side not sent with the correct format (email address).

If you're still having issues, please contact SAP Concur Support for assistance providing any error IDs you receive.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated using the previous *Test SSO login* section.

NOTE: The automatic enabling of Mobile SSO is only visible on the app version 9.86 or higher and if the user is opting for the new sign in experience. Users on older versions or opting for the earlier sign in experience will not see this option automatically.

The **Sign in with Mobile SSO** option will have your earlier IdP link embedded, so it will redirect users to your old SSO connection.

For both cases, please open a ticket with the SAP Concur support team, providing them the following information.

- If the users plan to use an older version, please provide SAP Concur support with the IdP-Initiated URL from the application created on the Idaptive side so they can enable Mobile SSO for the legacy app versions. For more information on how to obtain the URL see *Test SSO login > Testing IdP-Initiated SSO* section on this guide.
- If you want to remove the **Sign in with Mobile SSO** option to eliminate potential confusion, please inform the support team.

If you have any issues in authenticating with SSO on the mobile app, please open a ticket with the SAP Concur support team and provide any error IDs and/or messages received with screenshots.

E-mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket with the SAP Concur support team, providing the IDP URL from the application created on the IDP side so they can adjust the redirect URL for e-mail reminders. For more information on how to obtain the URL, see the *Test SSO login > Testing IdP-Initiated SSO* section of this appendix.

Rollout

After testing your new SSO configuration, you can then plan your rollout by assigning your new Idaptive application to all your users and groups who'll need this access.

The Manage SSO page also offers the option for you to enforce this new SSO connection by changing the SSO Setting from SSO Optional to **SSO Required**. If you change it, users will be redirected to SAP Concur by providing their Username via the SP-initiated flow.



If you need to enforce Mobile SSO only, please contact SAP Concur support.

Section 11: Appendix - Okta Setup

NOTE: Per the appendix instructions in this section, as content is sourced from the third-party provider, SAP Concur cannot guarantee its accuracy. If you encounter issues, it is recommended that you contact the third-party provider's support resources.

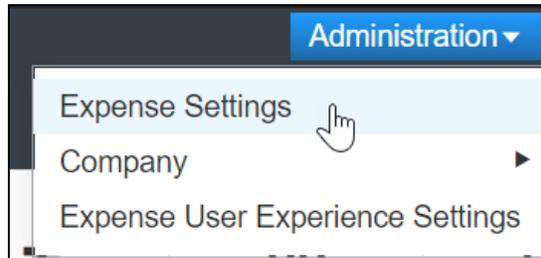
Getting Started

Before you start the configuration process, ensure that:

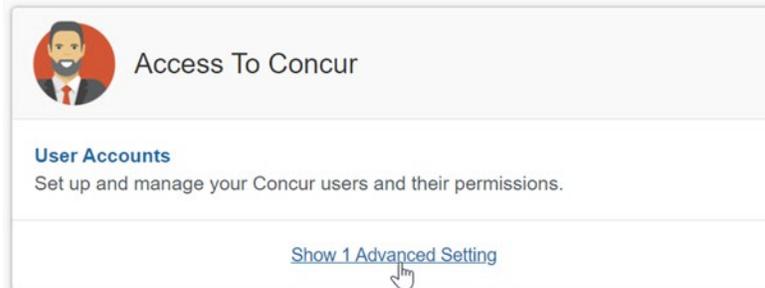
- You have admin access to the identity provider (Okta). This will be needed so you can complete the application configuration on the Okta side.
- Your users exist in both Okta and SAP Concur. Auto user provisioning is not currently supported by SAP Concur, so you need to add users separately in there.
- The attribute you are sending from Okta matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the **Manage SSO** page by using one of the following paths, depending on your SAP Concur edition.

For SAP Concur **Standard** edition:

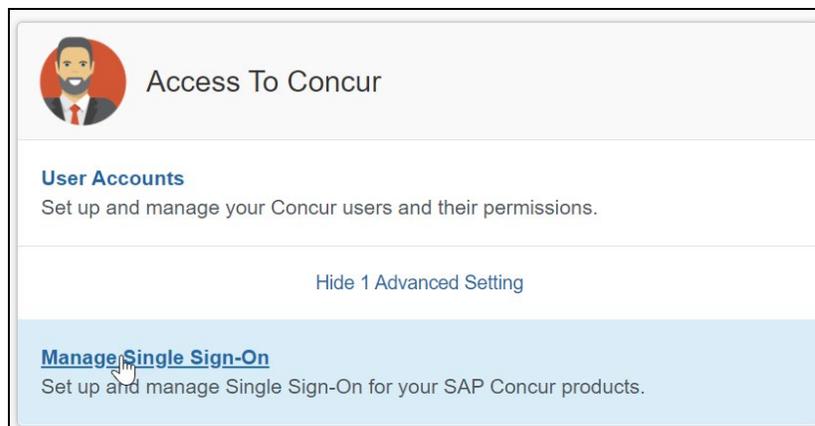
1. Go to **Administration > Expense Settings**.



2. Under Access to Concur section, click **Show 1 Advanced Setting**.

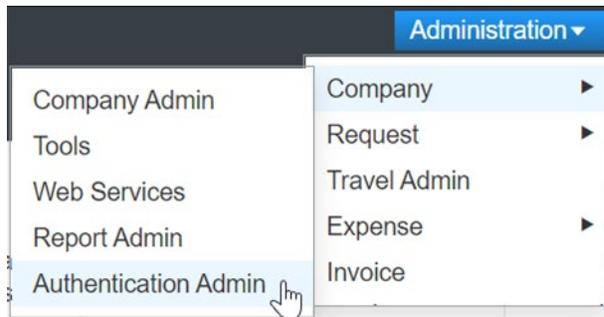


3. Click **Manage Single Sign-On** to access the **Manage SSO** page.

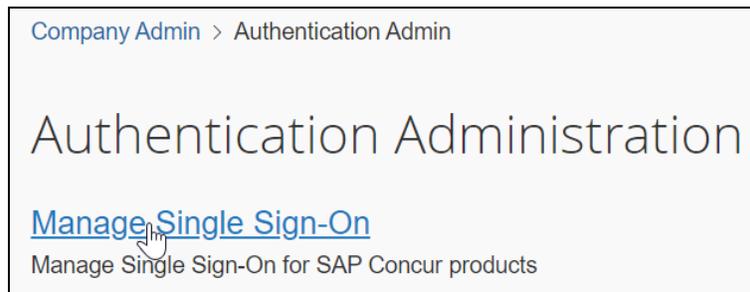


For the SAP Concur **Professional** edition:

1. Go to **Administration > Company > Authentication Admin**.



2. Click **Manage Single Sign-On** to access the Manage SSO page.



Alternatively, users can access the page using one of the following URLs:

- 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: If you don't have that permission and cannot have this assigned to your profile, please ask an authorized support contact at your company to open a case with SAP Concur support.

Configure Your Okta Application

Step 1: Get the SAP Concur metadata

To configure:

1. Get the SAP Concur metadata. To complete this, follow the instructions in the Overview section to log in to your SAP Concur account and access the **Manage SSO** section. To obtain the SAP Concur metadata on the **Manage SSO** page, you can either click **Copy URL** and then paste it in a new browser tab or click **Download** and open the downloaded file.

Manage Single Sign-On for [REDACTED]

Enable SSO

SSO Setting: SSO Optional ▼

Get SAP Concur Metadata

Copy or download SAP Concur metadata and add it to your Identity Provider (IdP).

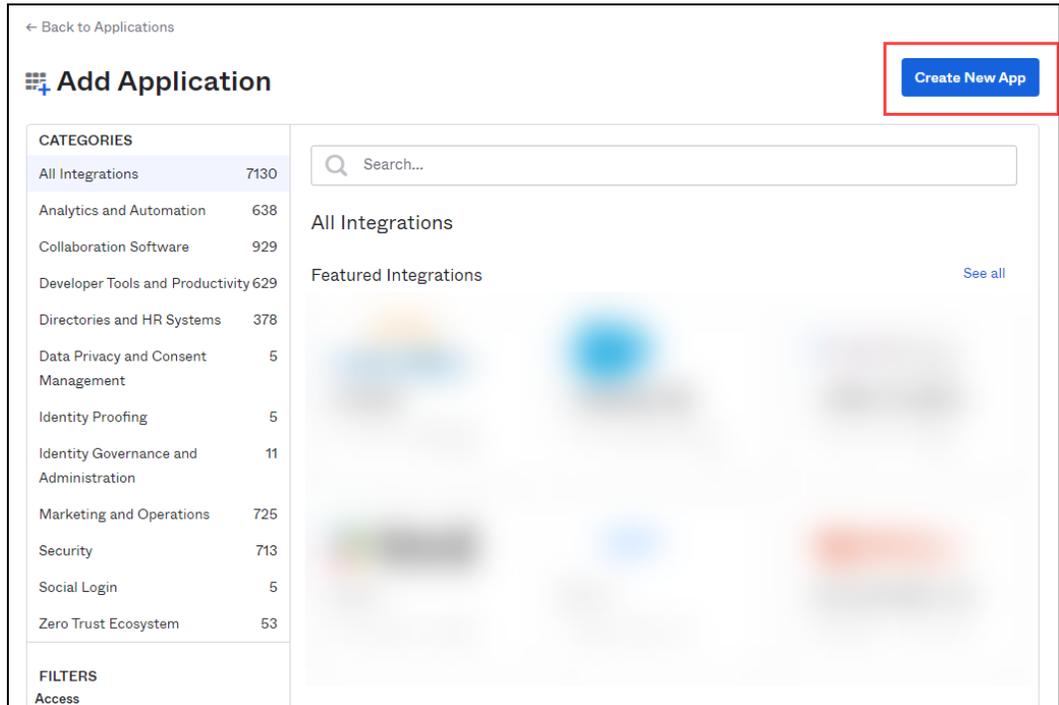
Copy SAP Concur metadata

OR

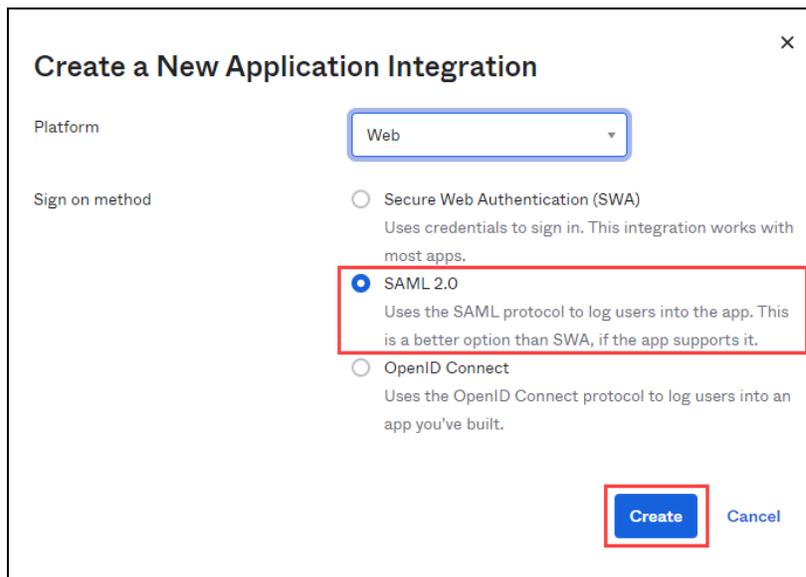
Download SAP Concur metadata

Step 2: Create an application on Okta

1. First, log in with an administrator account in Okta to complete the following.
2. Click **Applications** at the top to start creating your new application. Do not use the default SAP Concur application in Okta, as the default SAP Concur applications in the gallery may point you to the incorrect endpoint.



3. Select **SAML 2.0**.
4. Enter a name for the configuration and then click **Create**.



5. Enter an App Name, select a logo (optional), and then click **Next**.

Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

1 General Settings

App name: [Encryption] Concur - SSO Support Test

App logo (optional) [gear icon]

[Browse] [Upload Logo]

Requirements

- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

App visibility

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

[Cancel] [Next]

6. Open the SAP Concur metadata, scroll down and locate **Location=**. Copy the URL value and paste it into the **Single sign on URL** field in the Okta application.

```
Location="https://us.api.concursolutions.com/sso/saml2/v1/acs/" />
```

SAML Settings

GENERAL

Single sign on URL [https://us.api.concursolutions.com/sso/saml2/v1/acs/]

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

7. Return to SAP Concur metadata and, at the top, locate **entityID=**. Copy the URL and paste it into the **Audience URI (SP Entity ID)** field on your Okta application.

```
" entityID="https://us.api.concursolutions.com">  
meration="urn:oasis:names:tc:SAML:2.0:protocol">
```

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Step 3: Name ID configuration

During the application configuration, you will need to configure the **Name ID**. The **Name ID** must match the **Login ID (CTE Login Name)** registered for your employees in SAP Concur. We strongly recommend you set the **Name ID format** to **EmailAddress**.

Name ID format

Application username

Update application username on

Show Advanced Settings

This is required by SAP Concur for the SP-Initiated logins, starting from concursolutions.com or from the mobile app.

In some cases, the available Application username may not match the usernames in SAP Concur. If this is the case, you can run employee imports in SAP Concur to make sure they match the attribute you send. Alternatively, you can reach out to product support for Okta for further help with Name ID configurations.

The screenshot shows the 'Name ID format' dropdown menu set to 'EmailAddress'. Below it, the 'Application username' dropdown menu is open, showing options: 'Okta username', 'Okta username prefix', 'Email', 'Email prefix', 'Custom', and '(None)'. The 'Okta username' option is highlighted. To the right of the dropdown menu, there are links for 'Show Advanced Settings' and 'LEARN MORE'. Below the dropdown menu, there is a table with columns 'Name', 'Name format', and 'Value'.

If you want to encrypt your SAML assertion, please follow Step 4 instructions. If this is not needed, please proceed to Step 5.

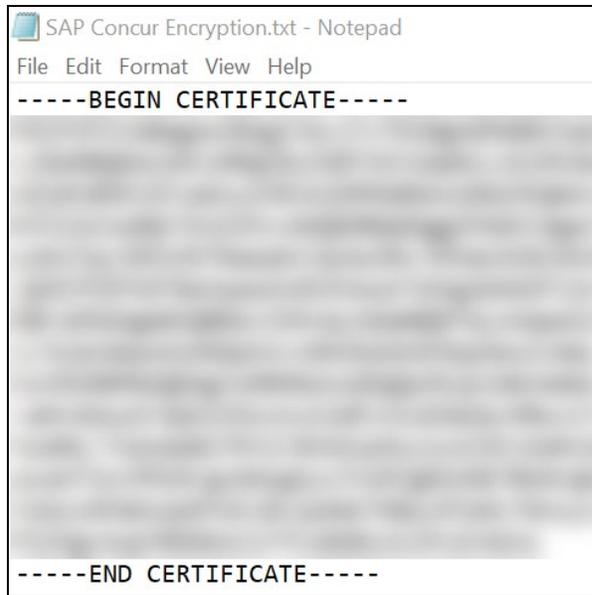
Step 4: (Optional) Encrypting the application

1. Return to SAP Concur metadata, scroll down and locate the tag **use="Encryption"**. Copy the X509 certificate and paste it into a text file (e.g., Notepad), between two BEGIN/END CERTIFICATE rows as shown here:

```

<-md:KeyDescriptor use="encryption">
  <-ds:KeyInfo>
    <-ds:X509Data>
      <-ds:X509Certificate>
        [Redacted Certificate Content]
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>

```



2. Save this file in .crt format.



3. In the Okta application, click the hyperlink **Show Advanced Settings**.

Create SAML Integration

1 General Settings
2 Configure SAML
3 Feedback

A SAML Settings

General

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

What does this form do?
This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate
Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

4. Change the **Assertion Encryption** to **Encrypted** and browse to the encryption certificate file you saved.

Hide Advanced Settings

Response [?] Signed

Assertion Signature [?] Signed

Signature Algorithm [?] RSA-SHA256

Digest Algorithm [?] SHA256

Assertion Encryption [?] Encrypted

Encryption Algorithm [?] AES256-CBC

Key Transport Algorithm [?] RSA-OAEP

Encryption Certificate [?] [Browse files...](#)

Enable Single Logout [?] Allow application to initiate Single Logout

Assertion Inline Hook None (disabled)

Authentication context class [?] PasswordProtectedTransport

Honor Force Authentication [?] Yes

SAML Issuer ID [?] http://www.okta.com/\${org.externalKey}

5. Once this file has been uploaded, you will see the following information under **Encryption Certificate**:

Encryption Certificate [?]

SAP Concur Encryption.crt X

Uploaded by ██████████ on Wed May 12 19:46:04 UTC 2021

CN=core-saml-prod.concur.com,OU=Core Services,O=SAP
Conur,L=Bellevue,ST=Washington,C=US
Valid from 2020-04-23T22:04:21.000Z to 2025-04-22T22:04:21.000Z

Certificate expires in 1441 days

Step 5: Finish the Configuration

1. In the Help Okta Support feedback section, choose **I'm an Okta customer adding an internal app**.
2. Scroll to the bottom and click **Finish**.

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type

This is an internal app that we have created

This is an external app that we have created

Previous Finish

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

Step 6: Download the Metadata File

To finish the configuration on the SAP Concur side, upload the metadata file extracted from your application in Okta.

1. On the **Sign On** settings page, click the Identity Provider metadata close to **View Setup Instructions**.

The screenshot shows the configuration page for the SAP Concur application. The 'Sign On' tab is active. Under 'Settings', the 'Sign on methods' section is expanded to show 'SAML 2.0' configuration. The 'Default Relay State' field is empty, and the 'Encryption Certificate' field contains the text 'SAP Concur Encryption.crt (CN=core-saml-prod.concur.cor)'. A yellow warning box indicates that SAML 2.0 is not configured until setup instructions are completed. A red box highlights the text 'Identity Provider metadata' in the footer of the settings section.

2. If your browser does not download the metadata xml automatically, please right click the tab with the metadata and save it as .xml.



Configure Your SAP Concur Site

1. Go to the **Manage SSO** page by following the steps provided in the Overview section.
2. Click **Add** from the **IdP Metadata** section.
3. Enter an appropriate name in the **IdP connection** and enter it in the **Custom IdP Name** field.

NOTE: If you decide to use the SP-initiated flow (through SAP Concur's public site: <https://www.concursolutions.com/nui/signin>), the **Custom IdP Name** will display on the **Sign In** page right after a user provides their Username and clicks **Next**. For example, if your **Custom IdP Name** is "Okta SSO [Encrypted]", then all users will see the option "Sign in with Okta SSO [Encrypted]".

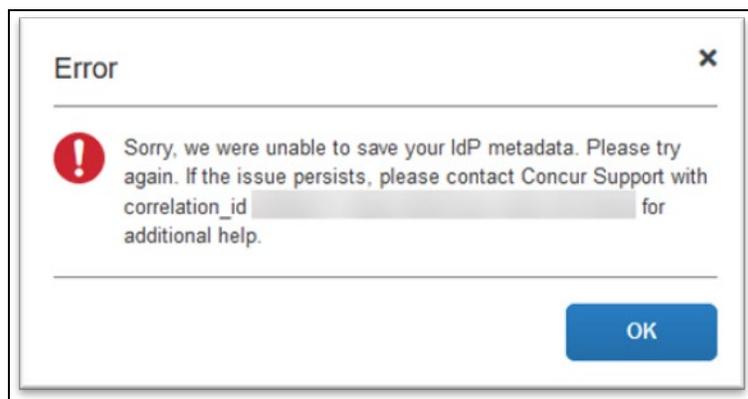
4. Provide a Logout URL (optional) for users to get redirected to a different place when they log out. By default, if no URL is entered, users will be redirected to where they started the authentication process. The logout endpoint for Okta can be found on **Local Provider > Identity Provider Settings > Single Log-Out Service (SLO) > Endpoint URL**.

NOTE: Single Logout (SLO) is not officially supported by SAP Concur, so the logout process with the SLO endpoint may not work as expected regarding disconnecting the user from the IDP in addition to SAP Concur. In that case, the user may be logged out from SAP Concur but not from Okta entirely.

5. In the Upload your IdP's metadata section, click **Upload XML File** and upload the metadata file from the IdP, which was previously saved locally.
6. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox Hide this SSO option from users signing in to Concur on web or mobile.

By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.

7. Click **Add Metadata**.
8. You should see either a successfully added confirmation or a something went wrong message. For the latter, please contact SAP Concur support and provide the Correlation ID.



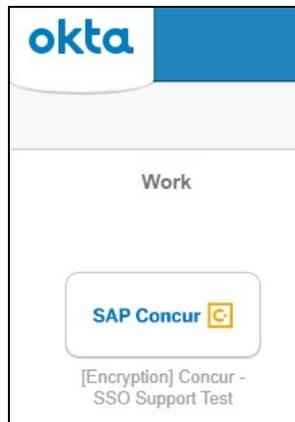
Test SSO Login

You can start testing SSO after you've successfully uploaded the IdP metadata to SAP Concur from the previous steps. In this section, you can test the IdP-Initiated (initiated on the identity provider side) and SP-Initiated (initiated on the service provider side) flows.

Test IdP-initiated SSO

To test IdP-initiated SSO:

1. In the IdP-Initiated flow, start the login process on the identity provider side. To test it, log in to your Okta account, go to your applications and search for the tile referencing the new SAP Concur app you just configured. Click the tile and check whether you're redirected to your SAP Concur profile directly.



You can also go to the **SSO** tab on your application and test with the **Embedded URL** field. It should look like this:

`https://companydomain.okta.com/home/concur/xxxxxxxxxxx/xxx.`

Test SP-initiated SSO

To test the SP-initiated SSO:

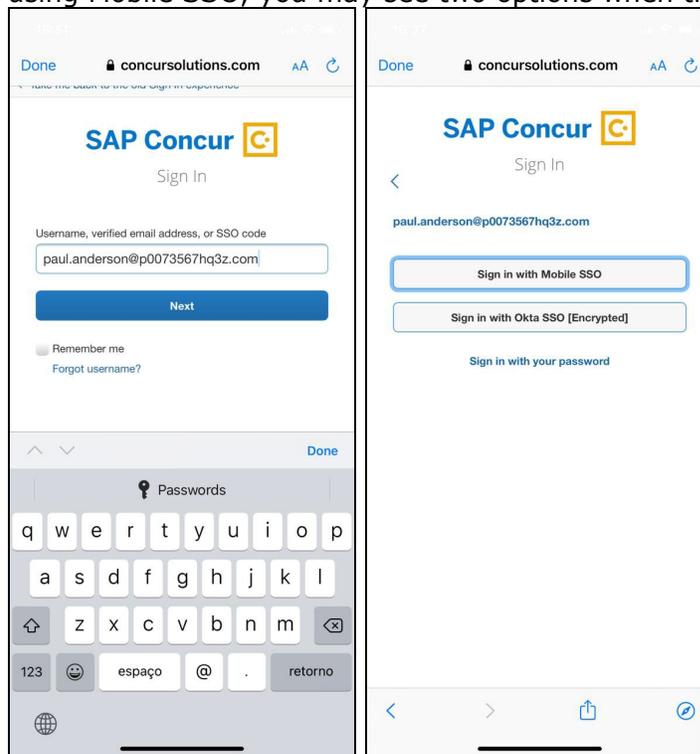
1. Open the SAP Concur login page according to the environment you want to test.
 - ◆ US DC Prod: <https://www.concursolutions.com/>
 - ◆ US DC Test: <https://implementation.concursolutions.com/>
 - ◆ EMEA DC Prod: <https://eu1.concursolutions.com/>
 - ◆ EMEA DC Test: <https://eu1imp.concursolutions.com/>
 - ◆ CN DC Prod: <https://www.concurcdc.cn/>
2. On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click **Next**, you should see an option for your recently created SSO configuration according to the note in *Configure Your*

SAP Concur Site. Click to proceed with authenticating your identity provider account which should redirect you to SAP Concur.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated using the previous *Test SSO login* section.

NOTE: The automatic enabling of Mobile SSO is only visible on the app version 9.86 or higher and if the user is opting for the new sign in experience. Users on older versions or opting for the earlier sign in experience will not see this option automatically. However, if you were using another IdP and already using Mobile SSO, you may see two options when trying to sign-in as follows:



The **Sign in with Mobile SSO** option will have your earlier IdP link embedded, so it will redirect users to your old SSO connection.

For both cases, please open a ticket with the SAP Concur support team, providing them the following information.

- If the users plan to use an older version, please provide SAP Concur support with the IdP-Initiated URL from the application created on the Okta side so they can enable Mobile SSO for the legacy app versions. For more information on how to obtain the URL see *Test SSO login > Testing IdP-Initiated SSO* section on this guide.
- If you want to remove the **Sign in with Mobile SSO** option to eliminate potential confusion, please inform the support team.

If you have any issues in authenticating with SSO on the mobile app, please open a ticket with the SAP Concur support team and provide any error IDs and/or messages received with screenshots.

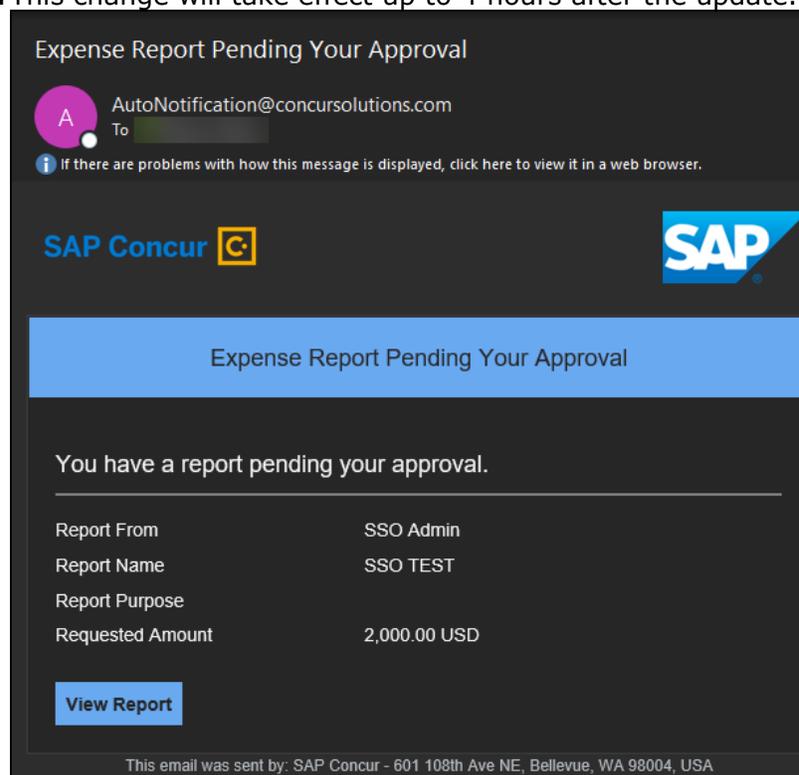
E-mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket with the SAP Concur support team, providing the IDP URL from the application created on the IDP side so they can adjust the redirect URL for e-mail reminders. For more information on how to obtain the URL, see the *Test SSO login > Testing IdP-Initiated SSO* section of this appendix.

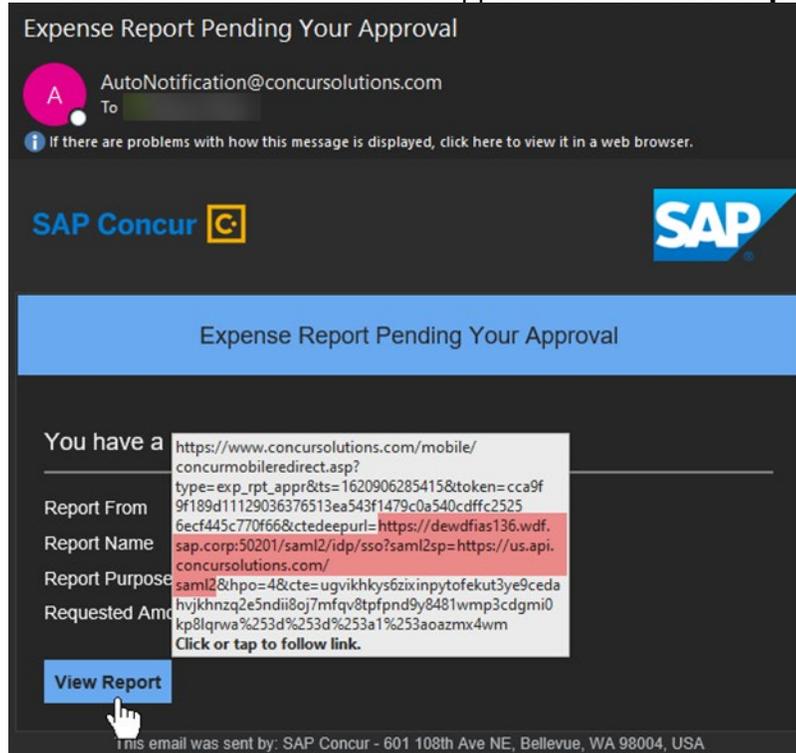
NOTE: The URL will appear embedded on the **View Report** button.

NOTE: This change will only be reflected in emails generated after the change. All emails prior to that will keep using the previous URL.

NOTE: This change will take effect up to 4 hours after the update.



If you hover the cursor over the **View Report** button, you will see the currently embedded URL. The URL should appear between **ctedeepurl=** and **&hpo=** terms.



Rollout

After testing your new SSO configuration, you can then plan your rollout by assigning your new Okta application to all your users and groups who'll need this access.

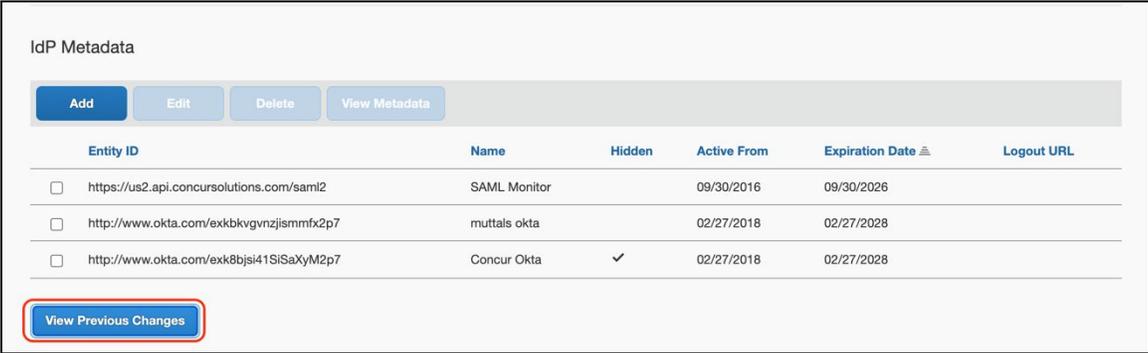
The Manage SSO page also offers the option for you to enforce this new SSO connection by changing the SSO Setting from SSO Optional to **SSO Required**. If you change it, users will be redirected to SAP Concur by providing their Username via the SP-initiated flow.



View Previous Changes

This featured was developed to help admins keep track of all changes completed under the **Manage SSO** page.

To view changes to the SSO configuration that have been made over time, click **View Previous Changes**.



A table listing previous changes appears and it is sorted in descending order by date and time.

The table can display the last 100 changes. Changes that are listed in the table include:

- Add a configuration
- Delete a configuration
- Edit Custom IdP Name, Logout URL, or Hidden fields

To view more detailed information about a specific change listed in the table, click the **View** link for the desired list item.

Inside each log, you'll see the **Company** and **ChangeBy** fields in the format [first_name last_name] [(UUID code)]; this refers to the user who performed the action. In case you don't recognize that user, you can contact support to request further details about it.

Section 12: Appendix - PingOne Setup

NOTE: Per the appendix instructions in this section, as content is sourced from the third-party provider, SAP Concur cannot guarantee its accuracy. If you encounter issues, it is recommended that you contact the third-party provider's support resources.

Getting Started

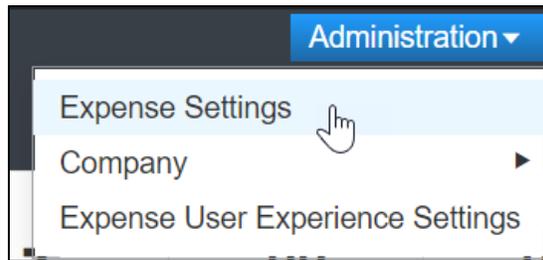
This appendix shows how to create a new application in PingOne and then upload this new configuration to your SAP Concur site on the new SAMLv2 platform.

Before you start the configuration process, ensure that:

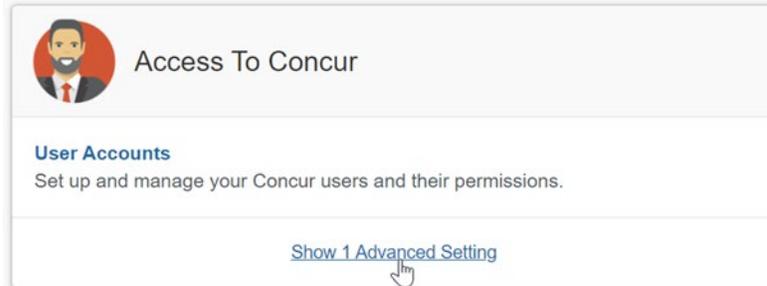
- Your users exist in both PingOne and SAP Concur.
- The attribute you are sending from PingOne matches the **Login ID (CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (**companyadmin**; a Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the **Manage SSO** page by using one of the following paths, depending on your SAP Concur edition.

For SAP Concur **Standard** edition:

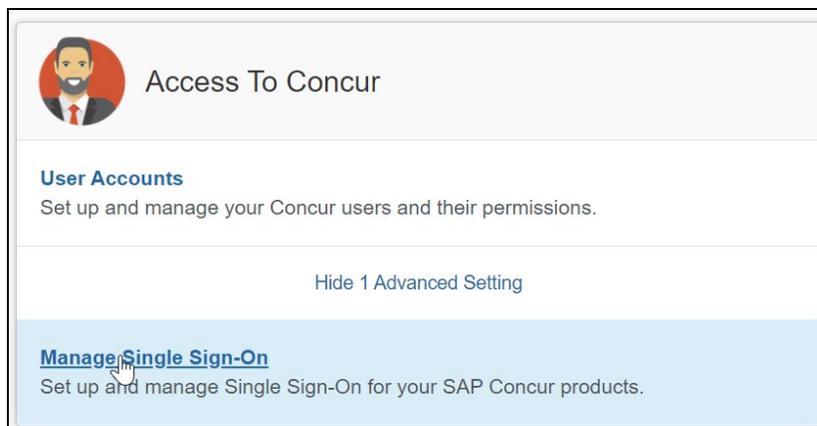
1. Go to **Administration > Expense Settings**.



2. Under Access to Concur section, click **Show 1 Advanced Setting**.

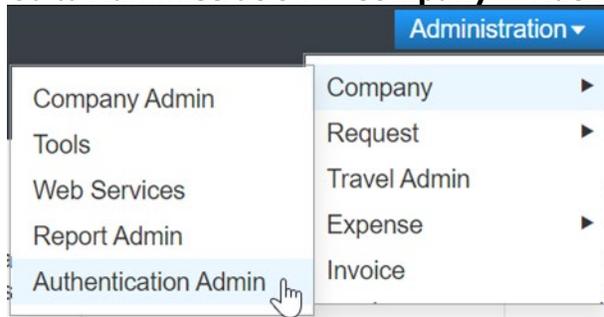


3. Click **Manage Single Sign-On** to access the **Manage SSO** page.

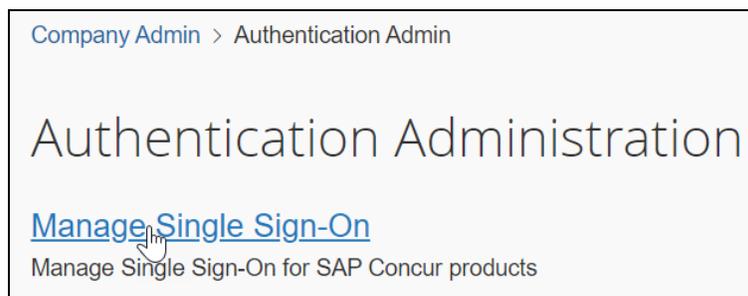


For the SAP Concur **Professional** edition:

1. Go to **Administration > Company > Authentication Admin**.



2. Click **Manage Single Sign-On** to access the **Manage SSO** page.



Alternatively, users can access the page using one of the following URLs:

- 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>

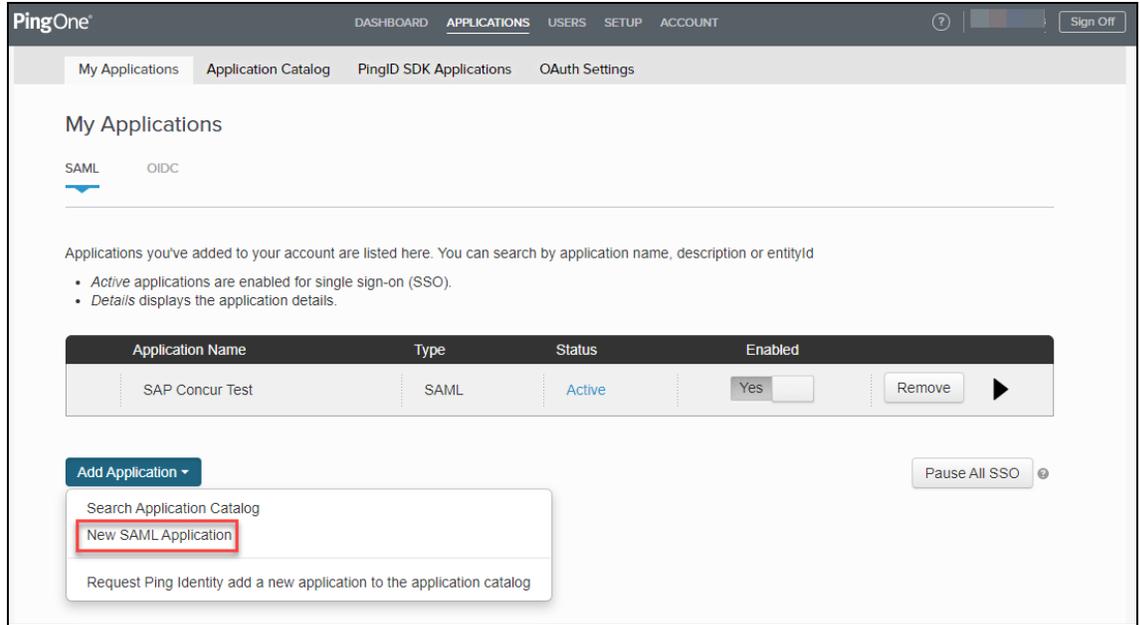
NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an authorized support contact at your company to open a case with SAP Concur support.

Configure Your PingOne Application

Step 1: Create a non-gallery SAML application

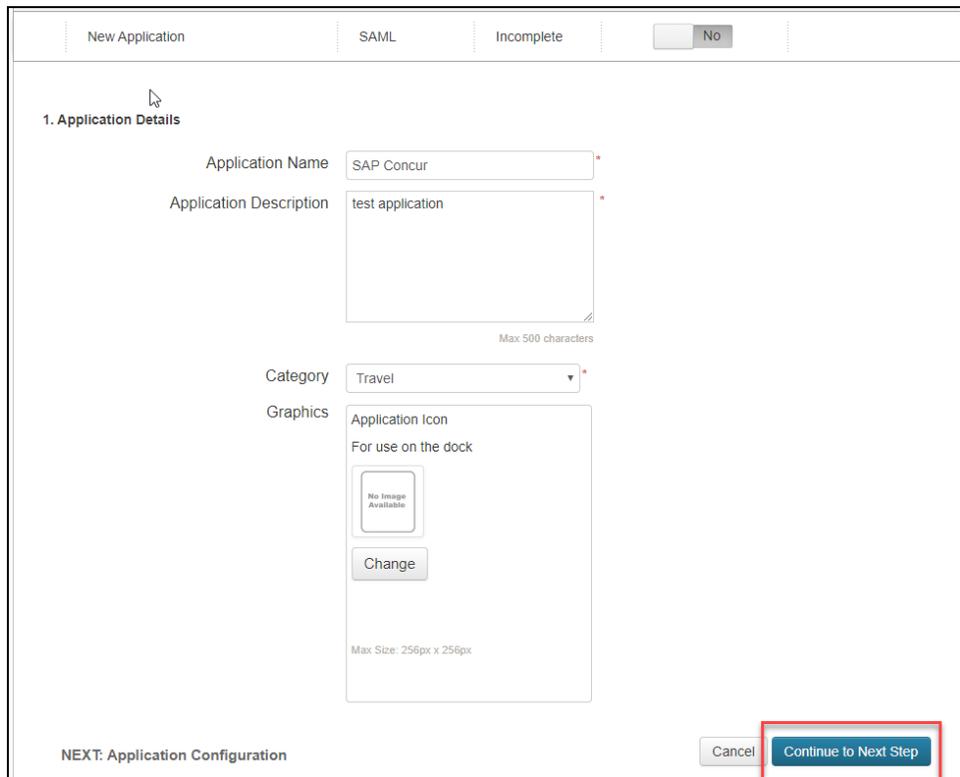
To configure:

1. Log in to your PingOne admin account and go to the **Applications** tab.
2. Click **Add Application > New SAML Application**.



Step 2: Application details

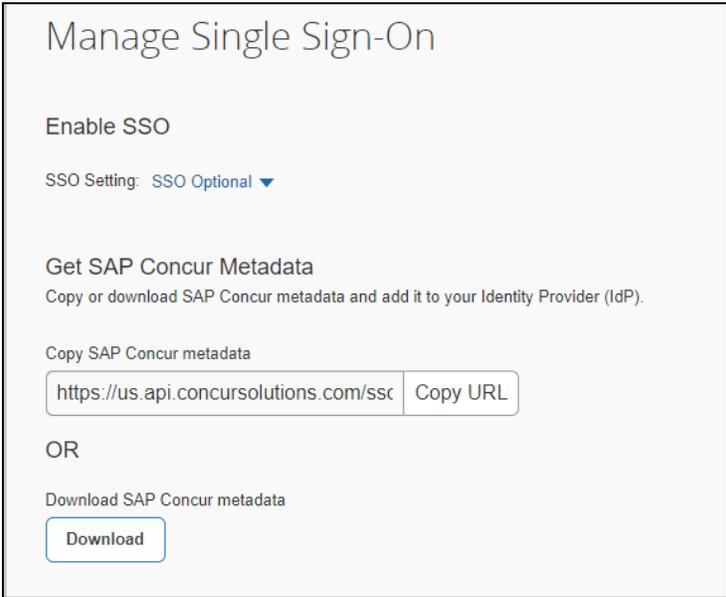
1. Fill in the application details as needed and then click **Continue to Next Step**.



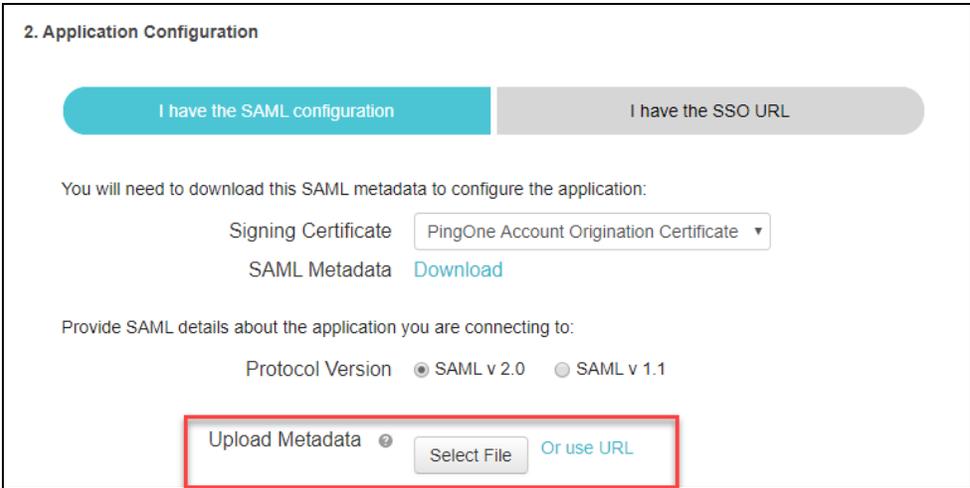
Step 3: Application configuration

To complete this step, log in to your SAP Concur account and access the **Manage SSO** section using the links in the Overview.

- 1. Once you've accessed **Manage SSO**, you can obtain SAP Concur metadata by clicking **Copy URL** (to get the metadata URL) or **Download** (to download the metadata XML file).



- 2. Use your browser to open the metadata URL or XML file. PingOne supports metadata files upload, so you can go to **Upload Metadata** and load the xml file. You can also click **Or use URL** and add the metadata URL.



Once the metadata is loaded through the XML file or the URL, these fields should be automatically filled in:

- ◆ Assertion Customer Service (ACS)

- ◆ Entity ID
- ◆ Primary Verification Certificate
- ◆ Encrypt Assertion checkbox
- ◆ Encryption Algorithm
- ◆ Encryption Certificate
- ◆ Transport Algorithm
- ◆ Signing (from Sign Assertion to Sign Response)

The screenshot displays the SAML configuration interface for an application. The settings are as follows:

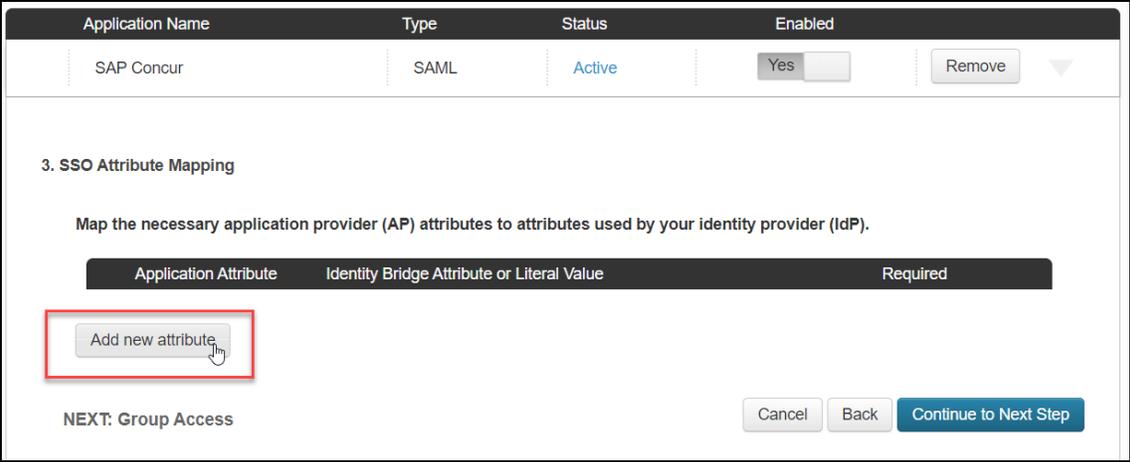
- Upload Metadata:** Uploaded file: metadata(1).xml. Buttons: Select File, Or use URL.
- Assertion Consumer Service (ACS):** https://www-us.api.concursolutions.com *
- Entity ID:** https://us.api.concursolutions.com/sam *
- Application URL:** (Empty text box)
- Single Logout Endpoint:** example.com/slo.endpoint
- Single Logout Response Endpoint:** example.com/sloresponse.endpoint
- Single Logout Binding Type:** Redirect Post
- Primary Verification Certificate:** Escolher arquivo. Nenhum arquivo selecionado. saml20metadata.cer
- Secondary Verification Certificate:** Escolher arquivo. Nenhum arquivo selecionado
- Encrypt Assertion:**
- Encryption Certificate:** Escolher arquivo. Nenhum arquivo selecionado. saml20metadata-encryption.cer
- Encryption Algorithm:** AES_256
- Transport Algorithm:** RSA_OAEP
- Signing:** Sign Assertion Sign Response
- Signing Algorithm:** RSA_SHA256
- Force Re-authentication:**

3. **Encrypt Assertion** is an optional setting. If you prefer to track your SAML assertions for troubleshooting purposes, you may deselect this checkbox and then click **Continue to the Next Step**.

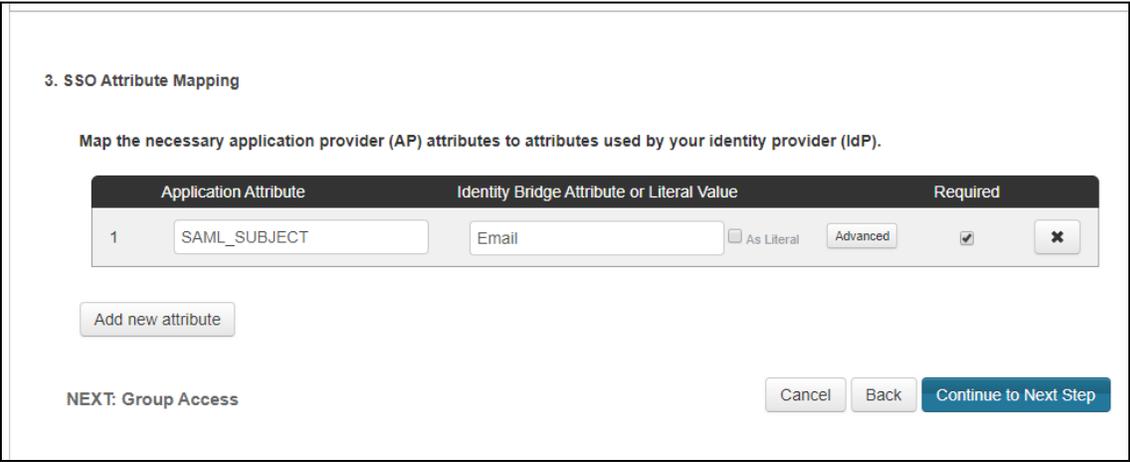
Step 4: Attribute Mapping

Once you get to the attribute mapping section, you need to build the attribute that will be sent to SAP Concur for validation. This attribute must match the employee's **Login ID** field in SAP Concur.

1. To add a new attribute, click **Add new attribute**.



If your Ping e-mail address matches the **Login ID** field in SAP Concur, you can build an attribute like the following:



If your Login IDs in SAP Concur have a different structure, you'll need to open the **Advanced settings** in **SSO Attribute Mapping** and configure a custom attribute. Ping has written [an article](#) in their community that can help you with this customization.

Step 5: Provide access to user groups

You'll be prompted with a screen for Group Access. Add your user groups to this application. Please ensure all of your SAP Concur employees are included and click **Continue to Next Step**.

4. Group Access

Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will see this application on their personal dock.

Group Name

Users@directory	Remove
Domain Administrators@directory	Add
Test Users	Add

NEXT: Review Setup Continue to Next Step

Step 6: Review and finish

Review your application configuration. Then download the SAML metadata from your configuration so you can upload it to SAP Concur later.

Finish your configuration by clicking **Finish**.

Single Sign-On (SSO) Relay State <https://pingone.com/1.0/9c9fc5fd-81c8-4696-b57e-7079fea1a0ae>

Signing Certificate [Download](#)

SAML Metadata [Download](#) 1

SAML Metadata URL <https://admin-api.pingone.com/latest/metadata/8e57b587-c81f-4eac-b52f-0a810ce1507d>

Single Logout Endpoint

Single Logout Response Endpoint

Signing [Assertion](#)

Signing Algorithm [RSA_SHA256](#)

Encrypt Assertion [false](#)

Force Re-authentication [false](#)

Click the link below to open the Single Sign-On page:
[Single Sign-On](#)

2

Edit **Finish**

Configure Your SAP Concur Site

1. Go to the **Manage SSO** page by following the steps provided in the Overview section.
2. Click **Add** from the **IdP Metadata** section. The **Add IdP Metadata** window appears.
3. Enter an appropriate name in the **IdP connection** and enter it in the **Custom IdP Name** field.

NOTE: For SP-initiated SSO, the **Custom IdP Name** will display on the **Sign In** page right after a user provides their Username and clicks **Next**.

4. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP.
5. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox Hide this SSO option from users signing in to Concur on web or mobile.

By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.

6. Click **Add Metadata**.

Once the metadata is successfully added, you can start testing your new configuration.

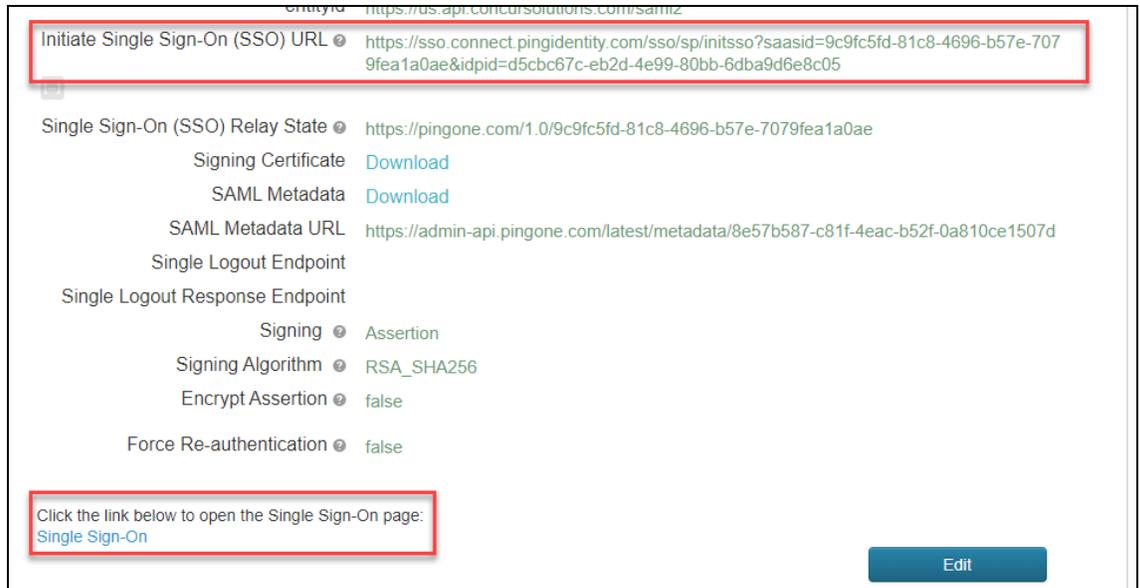
Test SSO Login

You can start testing SSO after you've successfully uploaded the IdP metadata to SAP Concur from the previous steps. In this section, you can test the IdP-Initiated (initiated on the identity provider side) and SP-Initiated (initiated on the service provider side) flows.

Testing IdP-initiated SSO

To test IdP-initiated SSO:

1. Open your recently created application. The Initiate Single Sign-On (SSO) URL and **Single Sign-On** link open the Single Sign-On page.



Testing SP-initiated SSO

To test the SP-initiated SSO:

1. Open the SAP Concur login page according to the environment you want to test.
 - ◆ 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. On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click **Next**, you should see an option for your recently created SSO configuration. Click the SSO authentication option to proceed with authenticating your PingOne credentials which should redirect to your profile on SAP Concur.

If after adding your PingOne credentials you receive a PingOne error message, your configuration may be incomplete or is missing something. If the IdP-Initiated SSO login is working but the SP-Initiated is not, this is most likely an issue with the name ID format. To make sure the Name ID format is correct, please confirm if SAML_SUBJECT is set to **Email** as described in the attribute mapping step of *Create Your PingOne Application*.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated using the previous *Test SSO login* section.

NOTE: The automatic enabling of Mobile SSO is only visible on the app version 9.86 or higher and if the user is opting for the new sign in experience. Users on older versions or opting for the earlier sign in experience will not see this option automatically.

If you have any issues in authenticating with SSO on the mobile app, please open a ticket with the SAP Concur support team and provide any error IDs and/or messages received with screenshots.

E-mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket with the SAP Concur support team, providing the IDP URL from the application created on the IDP side so they can adjust the redirect URL for e-mail reminders. For more information on how to obtain the URL, see the *Test SSO login > Testing IdP-Initiated SSO* section of this appendix.

Rollout

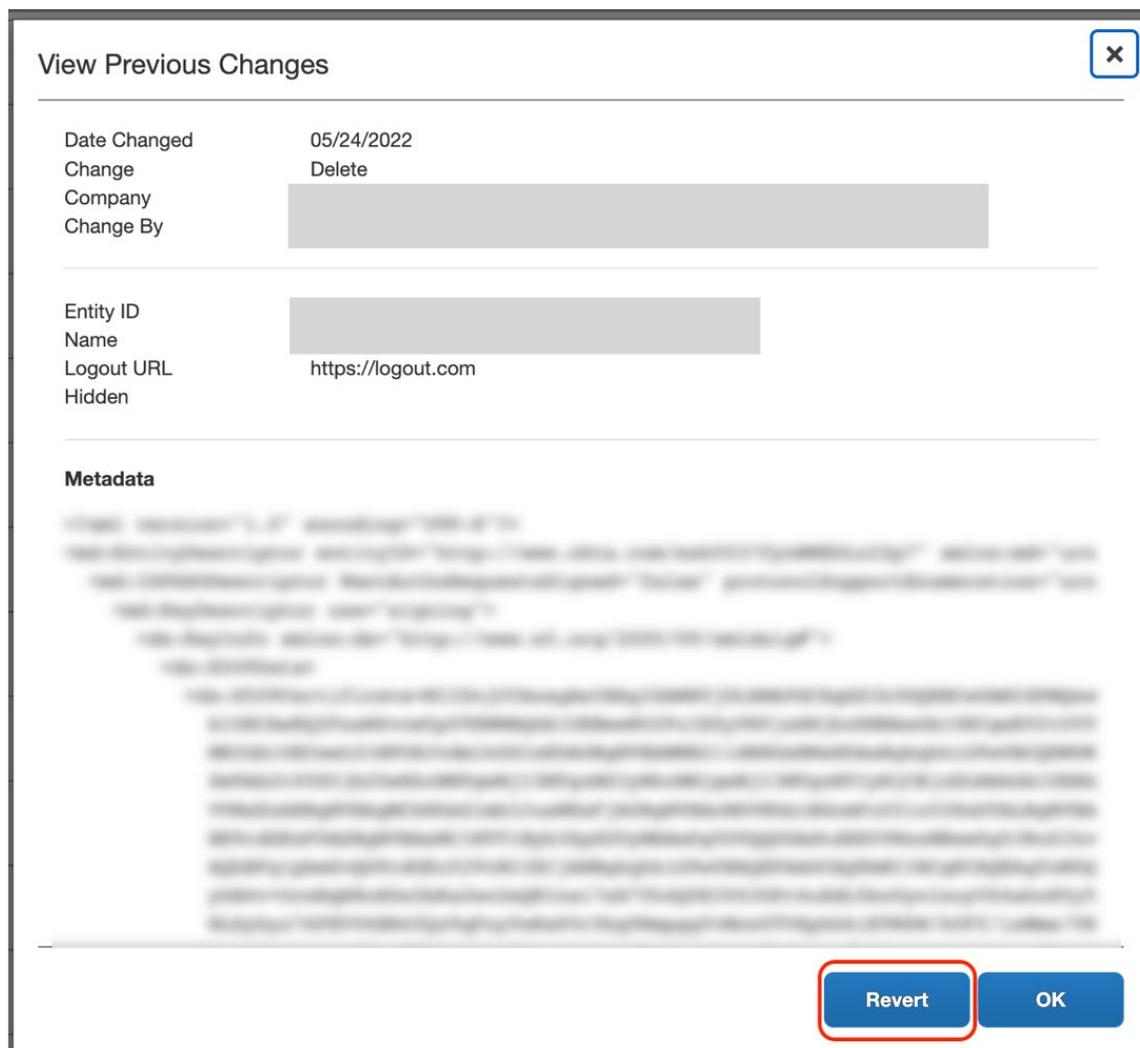
After testing your new SSO configuration, you can then plan your rollout by assigning your new application to all your users and groups who'll need this access.

The Manage SSO page also offers the option for you to enforce this new SSO connection by changing the SSO Setting from SSO Optional to **SSO Required**. If you change it, users will be redirected to SAP Concur by providing their Username via the SP-initiated flow.

If you need to enforce Mobile SSO only, please contact SAP Concur support.



For deleted configurations, the **View Previous Changes** page includes a **Revert** button that enables you to reinstate the deleted configuration. After the configuration is reinstated, it will be available to users during the sign-in process.



Section 13: Appendix - SAP Cloud Identity Services - Identity Authentication Service (SAP IAS) Setup

Getting Started

Before you start the configuration process, ensure that:

- You have admin access to the identity provider (SAP IAS) so that you can complete the application configuration on the SAP IAS side. In the [Viewing Assigned Tenants and Administrators](#) documentation you can see how to find the tenants that your company owns and who the administrators are.
- Your users exist in both SAP IAS and SAP Concur. For user integration, SAP Concur supports flat file imports and APIs. For integration with SAP products,

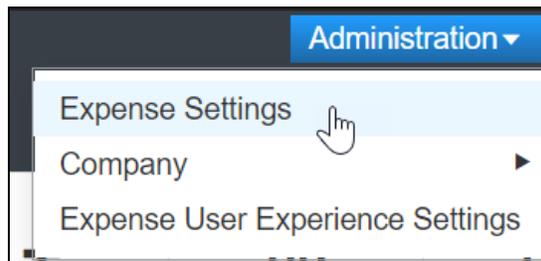
SAP offers automated user provisioning based on SAP Cloud Identity Service Identity Provisioning.

 For more information, refer to [SAP Concur Integration Scenario](#) on the SAP Help portal.

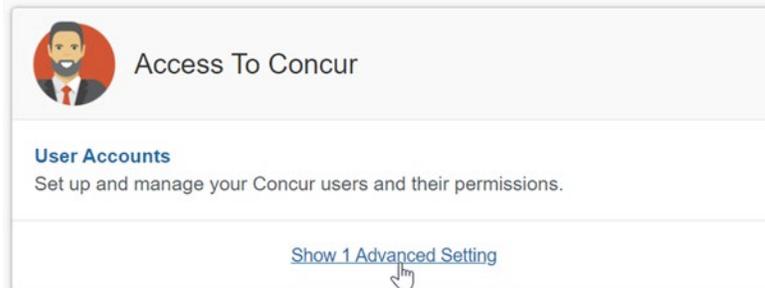
- The attribute you are sending as Subject Name Identifier from SAP IAS matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the **Manage SSO** page by using one of the following paths, depending on your SAP Concur edition.

For SAP Concur **Standard** edition:

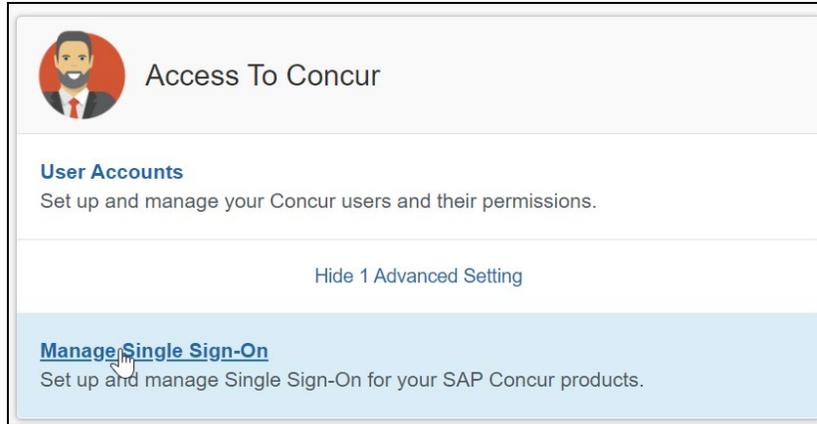
1. Go to **Administration > Expense Settings**.



2. Under Access to Concur section, click **Show 1 Advanced Setting**.

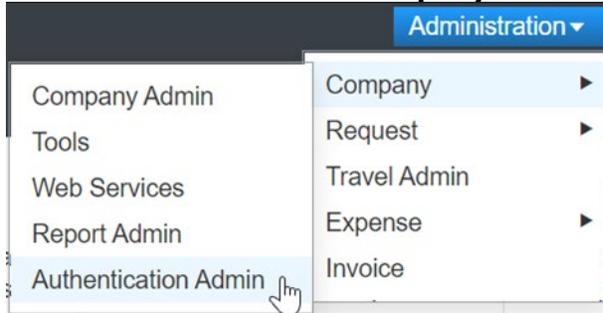


3. Click **Manage Single Sign-On** to access the **Manage SSO** page.

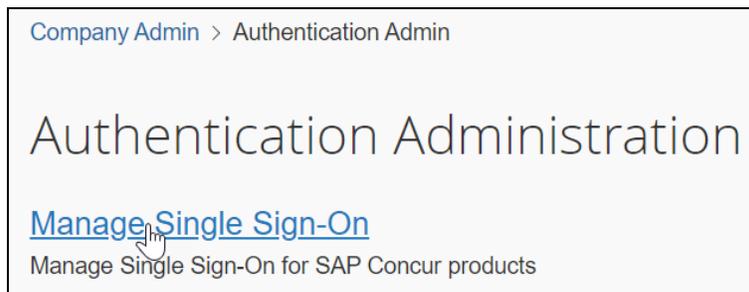


For the SAP Concur **Professional** edition:

1. Go to **Administration > Company > Authentication Admin.**



2. Click **Manage Single Sign-On** to access the **Manage SSO** page.



Alternatively, users can access the page using one of the following URLs:

- 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>

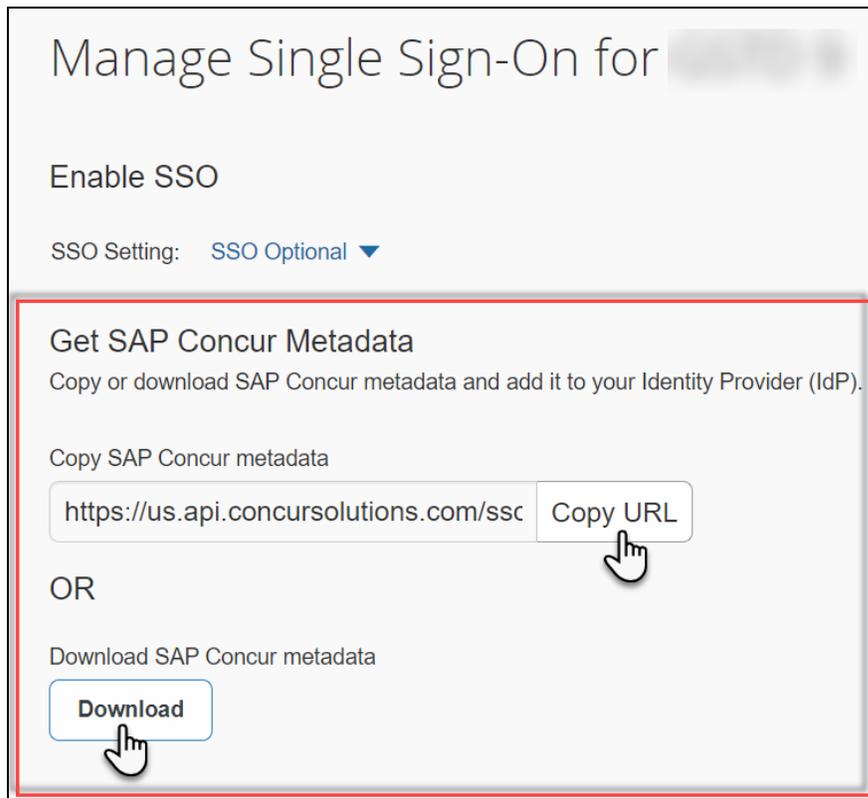
NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an authorized support contact at your company to open a case with SAP Concur support.

Configure Your SAP IAS Application

Step 1: Get the SAP Concur metadata

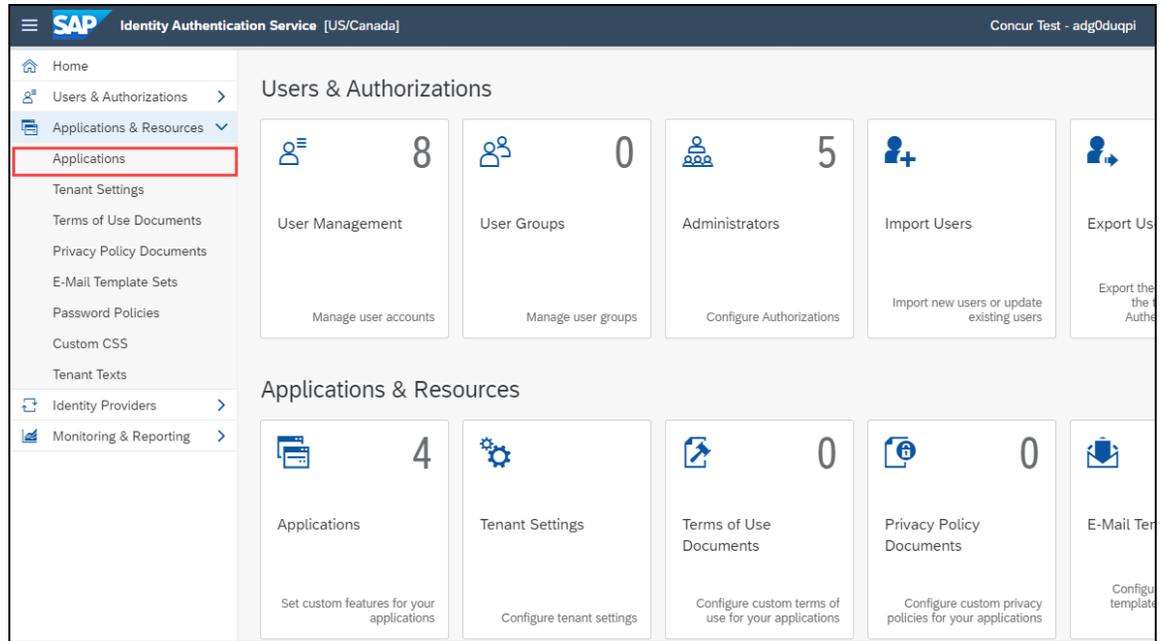
To configure:

1. Get the SAP Concur metadata. To complete this, follow the instructions in the previous *Overview* section to log in to your SAP Concur account and access the **Manage SSO** section. To obtain the SAP Concur metadata on the **Manage SSO** page, you can either click **Copy URL** and then paste it in a new browser tab or click **Download** and open the downloaded file.

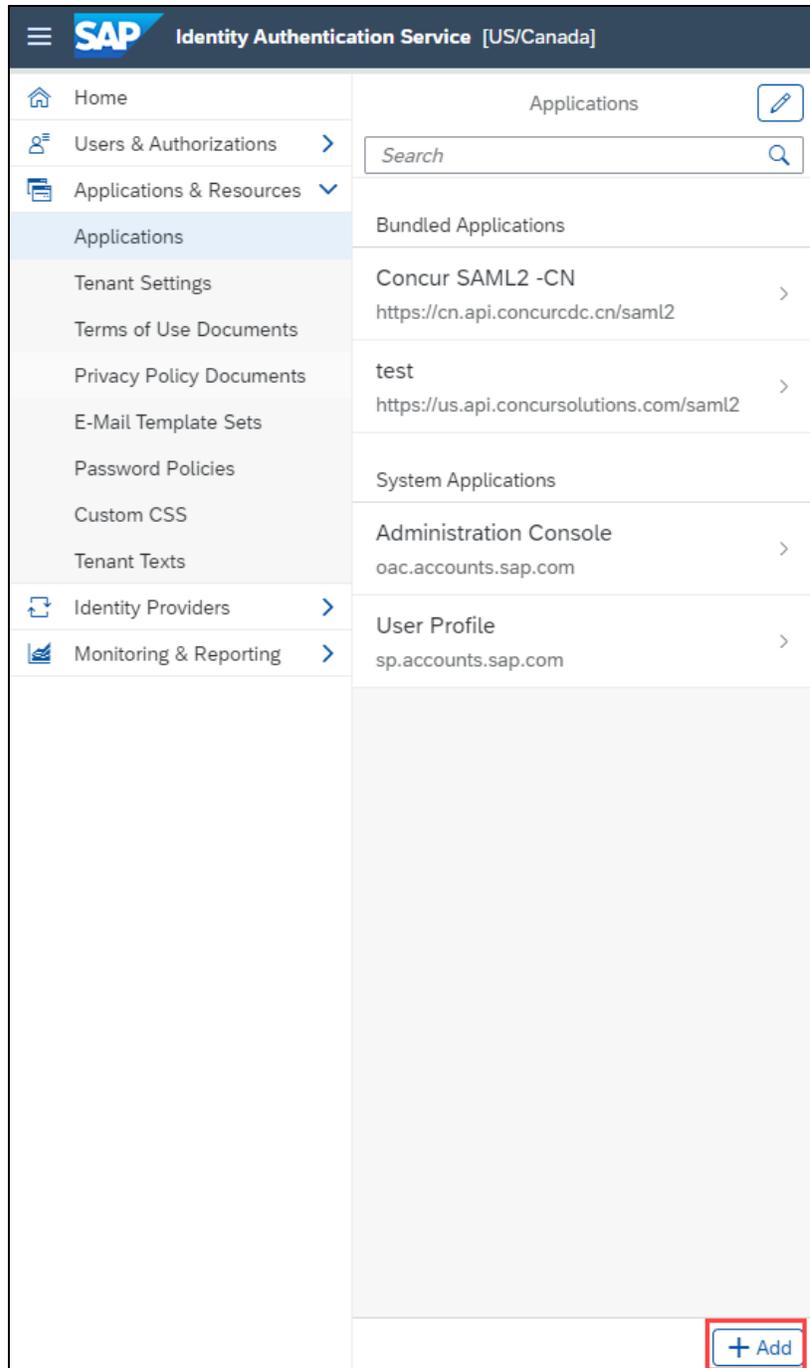


Step 2: Create an Application on SAP IAS

1. Create an application in SAP IAS. After logging in to SAP IAS, you will need to access **Applications & Resources > Applications**.

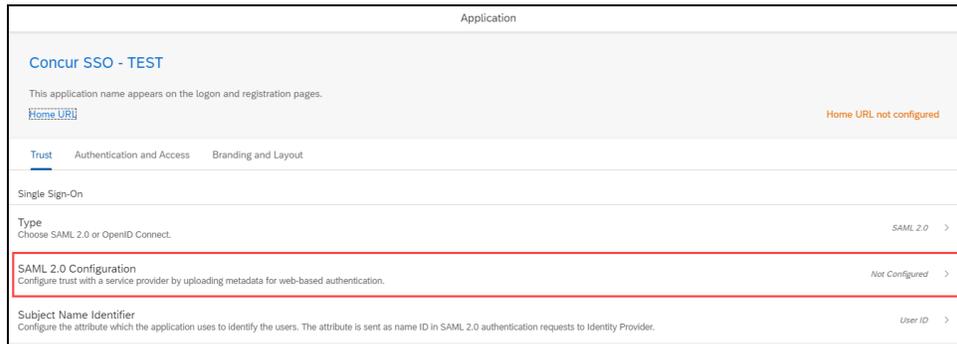


2. This will list all applications created. Click **+Add** to add a new application.

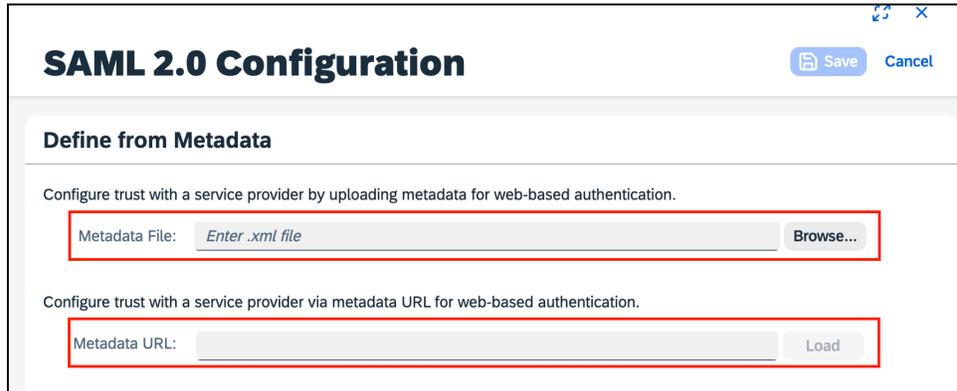


3. Enter a name and click **Save**.

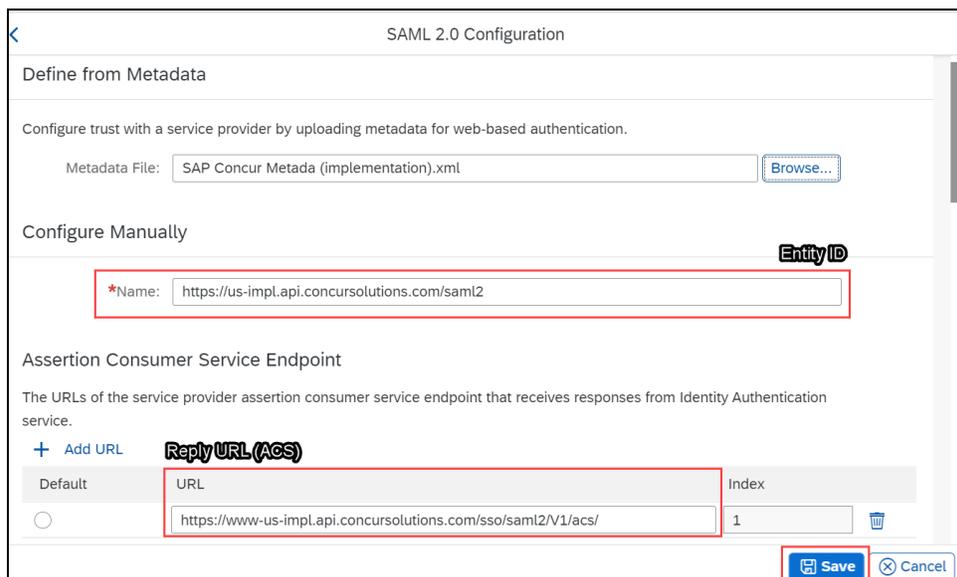
- This will be a SAML (Security Assertion Markup Language) configuration, so you will need to access SAML 2.0 Configuration.



- As you already downloaded the SAP Concur metadata file, or copied the URL from a previous step, you can click **Browse** to upload the file via **Metadata File** input, or enter the URL in **Metadata URL**.

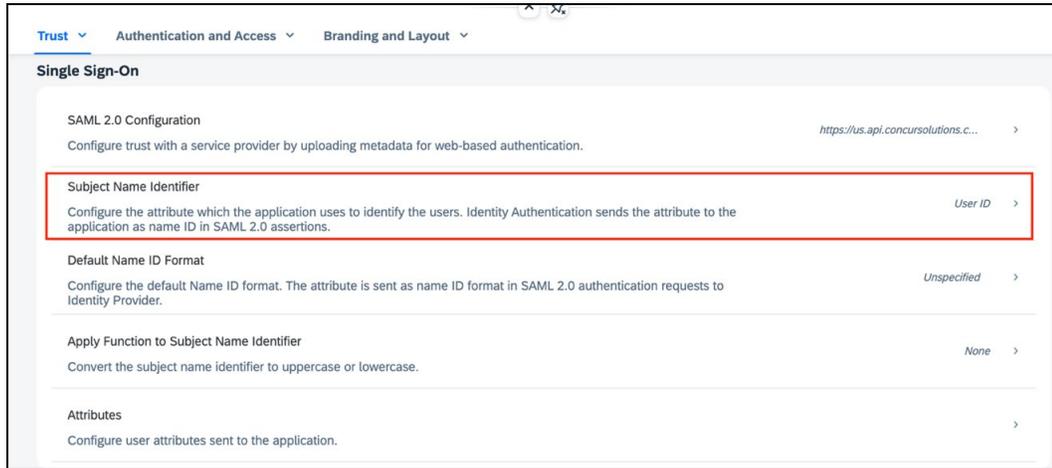


- After uploading the file, the SAP IAS should fill in fields accordingly by taking all values from the metadata. Then, click **Save**.



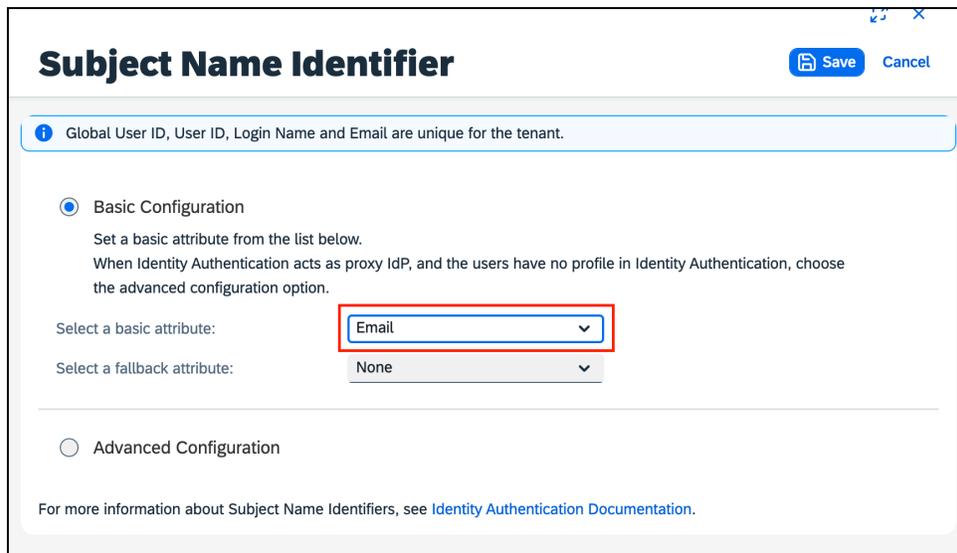
Step 3: Change Subject Name Identifier

The default Subject Name Identifier is **User ID**.



This should be updated based on the **Login IDs (Usernames / CTE Login Names)** of your users in SAP Concur:

- If the email addresses of your users are used as Logon IDs in SAP Concur, then in the **Basic Configuration** section you should configure **Email** in the **Select a basic attribute** drop-down.



- if the login names (usernames) of your users are with email format and are used as Logon IDs in Concur, then in the **Basic Configuration** section you should configure **Login Name** in the **Select a basic attribute** drop-down.

Subject Name Identifier Save Cancel

i Global User ID, User ID, Login Name and Email are unique for the tenant.

Basic Configuration
 Set a basic attribute from the list below.
 When Identity Authentication acts as proxy IdP, and the users have no profile in Identity Authentication, choose the advanced configuration option.

Select a basic attribute: Login Name ▼

Select a fallback attribute: None ▼

Advanced Configuration

For more information about Subject Name Identifiers, see [Identity Authentication Documentation](#).

- If your login IDs in SAP Concur do not match any user attribute but are constructed based on some user attribute with a static domain as suffix, then you can use **Advanced Configuration** to construct a value from that user attribute following the procedures [Configure the Subject Name Identifier Sent to the Application](#) procedure.

Subject Name Identifier Save Cancel

i Global User ID, User ID, Login Name and Email are unique for the tenant.

Basic Configuration

Advanced Configuration
 Set an attribute with dynamic value in the following pattern: <prefix> \${attribute_technical_name} <suffix>.
 When Identity Authentication acts as proxy IdP, and the users have no profile in Identity Authentication, set an attribute with the following dynamic value: <prefix> \${corporateIdP.<corporateIdP attribute>} <suffix>.

Dynamic subject name identifier value: \${loginName}@sap.com

Select a fallback attribute: None ▼

For more information about Subject Name Identifiers, see [Identity Authentication Documentation](#).

Step 4: Change Default Name ID Format

After finishing the application configuration, you will need to configure the **Name ID**. The **Name ID** must match the **Login ID (CTE Login Name)** registered for your employees in Concur. We also strongly recommend you set the Name ID format to **Email address**. This is required by SAP Concur for the SP-Initiated logins, starting from concursolutions.com or from the mobile app. The default Name ID Format is "Unspecified", so click **Default Name ID Format** to change it.

The screenshot shows the 'Application' configuration page in SAP IAS. The 'Trust' tab is selected. Under 'Single Sign-On', the 'Default Name ID Format' field is highlighted with a red box. The field description reads: 'Configure the default Name ID format. The attribute is sent as name ID format in SAML 2.0 authentication requests to Identity Provider.' The current value is 'Unspecified'. Other fields include 'Home URL' (not configured), 'Type' (SAML 2.0), 'SAML 2.0 Configuration' (https://us-impl.api.concursolutions...), 'Subject Name Identifier' (Login Name), and 'Apply Function to Subject Name Identifier' (None). A 'Delete' button is visible at the bottom right.

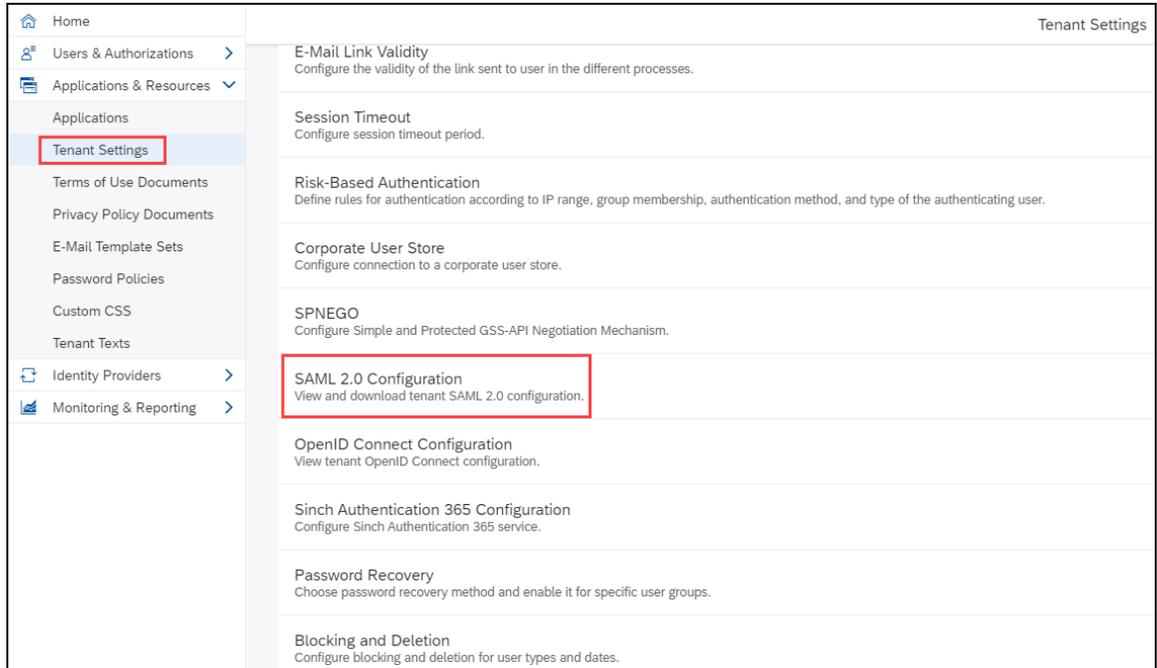
After you select the email, click **Save**.

The screenshot shows the 'Default Name ID Format' selection screen. There are two radio button options: 'Unspecified' (urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified) and 'E-Mail' (urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress). The 'E-Mail' option is selected and highlighted with a red box. Below the options, there is a link to 'Identity Authentication Documentation'. At the bottom right, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a red box.

In some cases, this may not match the usernames in SAP Concur. If this is the case, you can run employee imports in SAP Concur to make sure they match the attribute you send. Alternatively, you can reach out to product support for SAP IAS for further help with Name ID configurations.

Step 5: Download the metadata

To complete the configuration on the SAP Concur side, upload the metadata file extracted from your application in SAP IAS. To do so, go to **Applications & Resources > Tenant Settings > SAML 2.0 Configuration**.



This displays the Identity Provider Settings screen where you can review your configuration and choose to **Download Metadata File**.

<
SAML 2.

Identity Provider Settings

Name:

Single Sign-On Endpoint

The URLs of the identity provider single sign-on endpoint that receive authentication requests

Binding	URL
HTTP-Redirect	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com
HTTP-POST	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com

Assertion Consumer Service Endpoint

The URLs of the identity provider assertion consumer service endpoint that receive authentication responses

Binding	URL
HTTP-POST	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com

Single Logout Endpoint

The URLs of the identity provider single logout endpoint that receive logout messages

Binding	URL
HTTP-Redirect	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com
HTTP-POST	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com

Signing Certificate

A certificate used by the identity provider to digitally sign the messages for the applications

Certificate File:

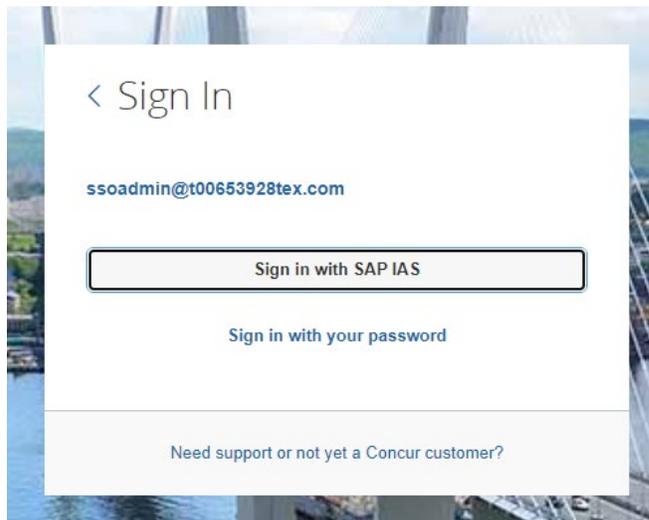
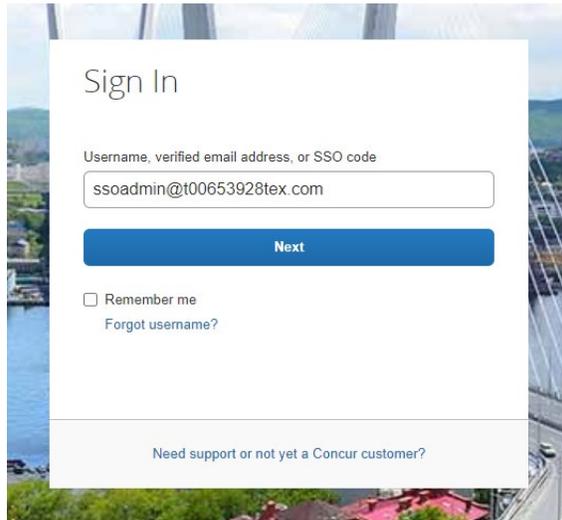
↓ Download Metadata File

You are now ready to upload your metadata file to SAP Concur.

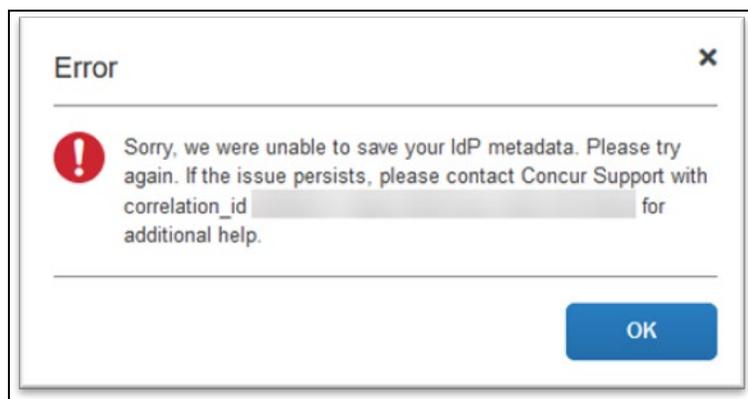
Configure Your SAP Concur Site

1. Go to the **Manage SSO** page by following the steps provided in the Overview section.
2. Click **Add** from the **IdP Metadata** section. The **Add IdP Metadata** window appears.
3. Enter an appropriate name in the **IdP connection** and enter it in the **Custom IdP Name** field.

NOTE: If you decide to use the SP-initiated flow (through SAP Concur's public site: <https://www.concursolutions.com/nui/signin>), the **Custom IdP Name** will display on the **Sign In** page right after a user provides their Username and clicks **Next**. For example, if your **Custom IdP Name** is "SAP IAS", then all users will see the option "Sign in with SAP IAS".



4. Provide a Logout URL (optional) for users to get redirected to a different place when they log out. By default, if no URL is entered, users will be redirected to where they started the authentication process. The logout endpoint for SAP IAS can be found in **Applications & Resources > Tenant Settings > Identity Provider Settings > Single Logout Endpoint**. Please note that **Single Logout (SLO)** is not officially supported by SAP Concur, so the logout process with the SLO endpoint may not work as expected regarding disconnecting the user from the IDP in addition to SAP Concur. In that case, the user may be logged out from SAP Concur but not from SAP IAS entirely.
5. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP.
6. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox Hide this SSO option from users signing in to Concur on web or mobile.
7. By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.
8. Click **Add Metadata**.
9. You should see either a successfully added confirmation or a something went wrong message. For the latter, please contact SAP Concur support and provide the Correlation ID.



Test SSO Login

You can start testing SSO after you've successfully uploaded the IdP metadata to SAP Concur from the previous steps. In this section, you can test the IdP-Initiated (initiated on the identity provider side) and SP-Initiated (initiated on the service provider side) flows.

Testing IdP-initiated SSO

To test IdP-initiated SSO:

1. In the IdP-Initiated flow, start the login process on the identity provider side. To test, append the parameters from the application you just created to the SSO endpoint from SAP IAS. A format example of IdP-Initiated URL would be:

Format: [**tenantName***]?saml2sp=[**SP Identifier****]

Example:

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

***TenantName:** Go to **Applications & Resources > Tenant Settings**.

****SP Identifier:** You can obtain it from the SAP Concur metadata. It will be the same as **Entity ID** or **Audience**.

NOTE: SAP IAS has 5 different landscapes, but only one – the PROD environment (*.accounts.ondemand.com) – is relevant for customers.

The screenshot shows the 'Identity Provider Settings' page in SAP IAS. The 'Name' field is highlighted with a red box and contains the URL 'https://adg0duqpi.accounts400.ondemand.com'. Below it, the 'Single Sign-On Endpoint' section shows a table with two rows: HTTP-Redirect and HTTP-POST, both pointing to the same SAML2 endpoint URL.

Binding	URL
HTTP-Redirect	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com
HTTP-POST	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com

This URL should redirect you to a login page on the SAP IAS side. Once you login with your credentials, you should be redirected to the SAP Concur homepage.

Testing SP-initiated SSO

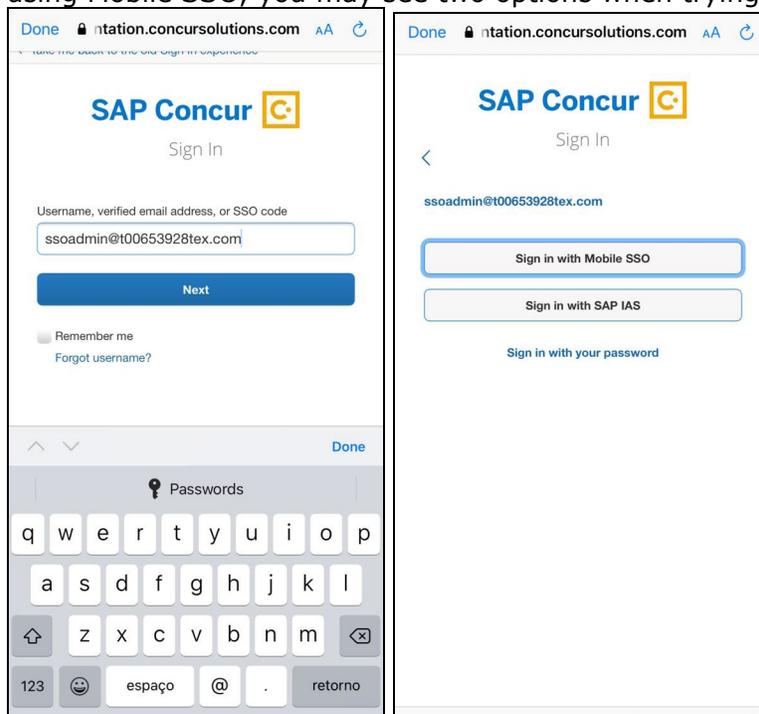
To test the SP-initiated SSO:

1. Open the SAP Concur login page according to the environment you want to test.
 - ◆ 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. On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click **Next**, you should see an option for your recently created SSO configuration according to the note in *Configure Your SAP Concur Site*. Click to proceed with authenticating your identity provider account which should redirect you to SAP Concur.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated using the previous *Test SSO login* section.

NOTE: The automatic enabling of Mobile SSO is only visible on the app version 9.86 or higher and if the user is opting for the new sign in experience. Users on older versions or opting for the earlier sign in experience will not see this option automatically. However, if you were using another IdP and already using Mobile SSO, you may see two options when trying to sign-in as follows:



The **Sign in with Mobile SSO** option will have your earlier IdP link embedded, so it will redirect users to your old SSO connection.

For both cases, please open a ticket with the SAP Concur support team, providing them the following information.

- If the users plan to use an older version, please provide SAP Concur support with the IdP-Initiated URL from the application created on the SAP NetWeaver side so they can enable Mobile SSO for the legacy app versions. For more information on how to obtain the URL see *Test SSO login > Testing IdP-Initiated SSO* section on this guide.
- If you want to remove the **Sign in with Mobile SSO** option to eliminate potential confusion, please inform the support team.

If you have any issues in authenticating with SSO on the mobile app, please open a ticket with the SAP Concur Support team and provide any error IDs and/or messages received with screenshots.

E-mail Notifications

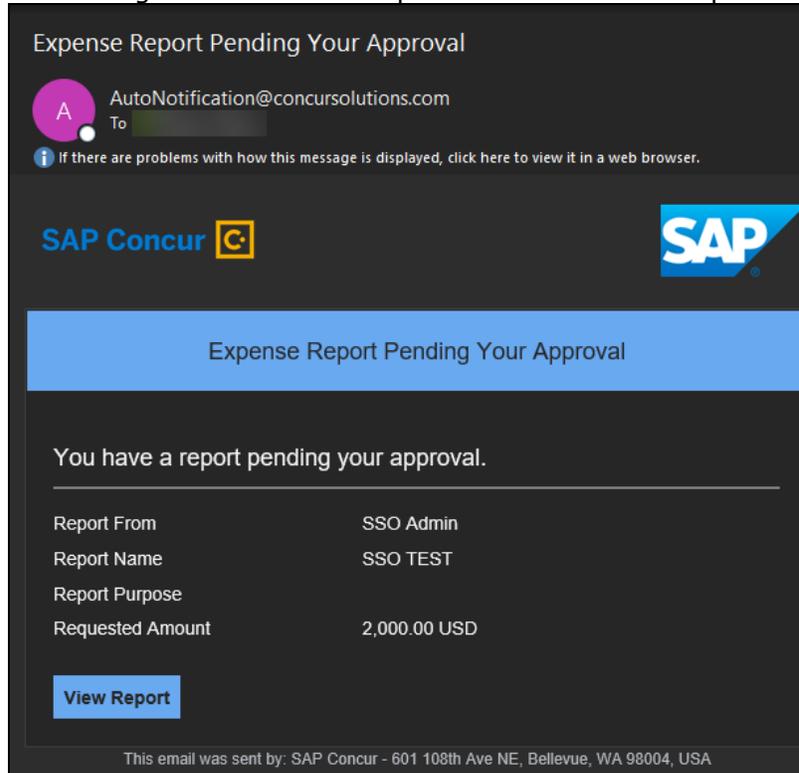
The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket with the SAP Concur support team, providing the IDP URL from the application created on the

IDP side so they can adjust the redirect URL for e-mail reminders. For more information on how to obtain the URL, see the *Test SSO login > Testing IdP-Initiated SSO* section of this appendix.

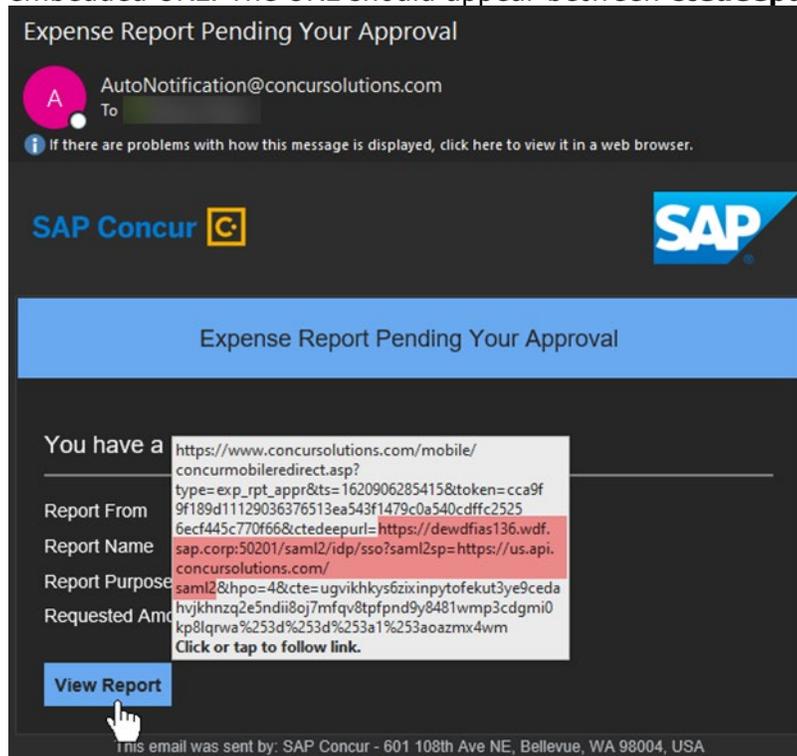
NOTE: The URL will appear embedded on the **View Report** button.

NOTE: This change will only be reflected in emails generated after the change. All emails prior to that will keep using the previous URL.

NOTE: This change will take effect up to 4 hours after the update.



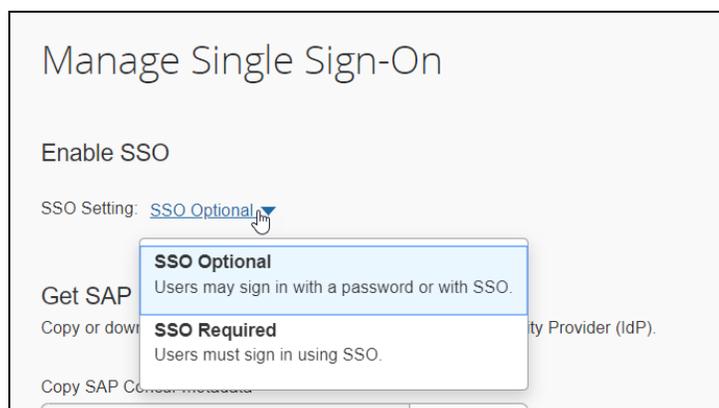
If you hover the cursor over the **View Report** button, you will see the currently embedded URL. The URL should appear between **ctedeepurl=** and **&hpo=** terms.



Rollout

After testing your new SSO configuration, you can then plan your rollout by assigning your new SAP IAS application to all your users and groups who'll need this access.

The Manage SSO page also offers the option for you to enforce this new SSO connection by changing the SSO Setting from SSO Optional to **SSO Required**. If you change it, users will be redirected to SAP Concur by providing their Username via the SP-initiated flow.



View Previous Changes

This featured was developed to help admins keep track of all changes completed under the **Manage SSO** page.

To view changes to the SSO configuration that have been made over time, click **View Previous Changes**.

A table listing previous changes appears and it is sorted in descending order by date and time.

The table can display the last 100 changes. Changes that are listed in the table include:

- Add a configuration
- Delete a configuration
- Edit Custom IdP Name, Logout URL, or Hidden fields

To view more detailed information about a specific change listed in the table, click the **View** link for the desired list item.

View Previous Changes						
Date	Change	Entity ID	Name	Logout URL	Hidden	Details
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	Concur Okta		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2			View

Inside each log, you'll see the **Company** and **ChangeBy** fields in the format [first_name last_name] [(UUID code)]; this refers to the user who performed the action. In case you don't recognize that user, you can contact support to request further details about it.

View Previous Changes
X

Date Changed	06/08/2022
Change	Edit
Company	[REDACTED]
Change By	[REDACTED]

Entity ID	[REDACTED]
Name	Concur Okta
Logout URL	
Hidden	✓

Previous Values

Entity ID	[REDACTED]
Name	Concur Okta
Logout URL	
Hidden	

Metadata

[REDACTED]

OK

For configurations that are deleted, the **View Previous Changes** page includes a **Revert** button that enables you to reinstate the deleted configuration. After the configuration is reinstated, it will be available to users during the sign-in process.



For more info, please refer to the following documentation resources:

- ◆ SAP Concur - [SSO Overview Guide](#)
- ◆ SAP Help Portal - [SAP Cloud Identity Services - Identity Authentication](#)
- ◆ SAP KBA - [2701851 - SAP Cloud Platform Identity Authentication Service \(IAS\) - Guided Answers](#)

Section 14: Appendix - SAP NetWeaver Setup

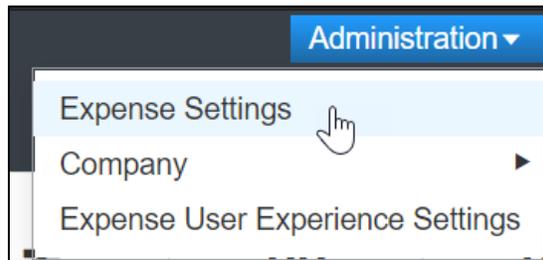
Overview

Before you start the configuration process, ensure that:

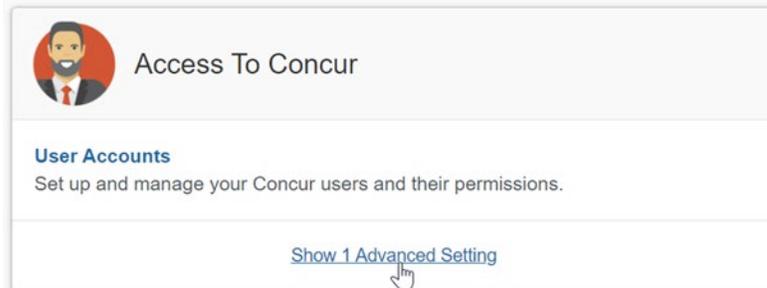
- You have admin access to the identity provider (SAP NetWeaver). This will be needed so you can complete the application configuration on the SAP NetWeaver side.
- Your users exist in both SAP NetWeaver and SAP Concur. Auto user provisioning is not currently supported by SAP Concur, so you need to add users separately in there.
- The attribute you are sending from SAP NetWeaver matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the **Manage SSO** page by using one of the following paths, depending on your SAP Concur edition.

For SAP Concur **Standard** edition:

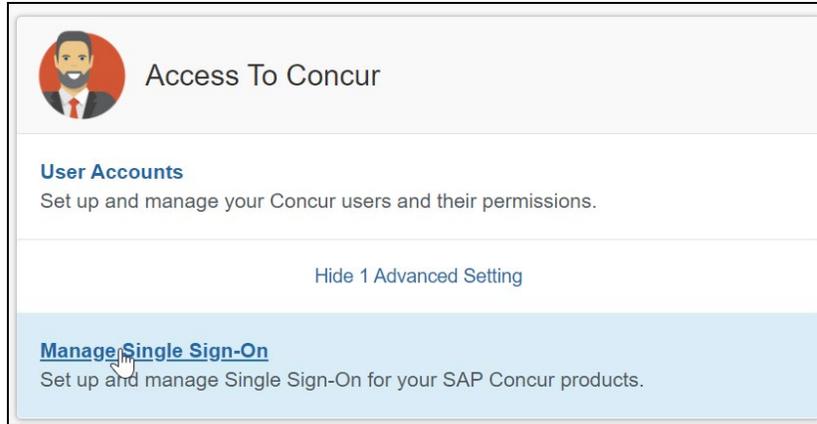
1. Go to **Administration > Expense Settings**.



2. Under Access to Concur section, click **Show 1 Advanced Setting**.

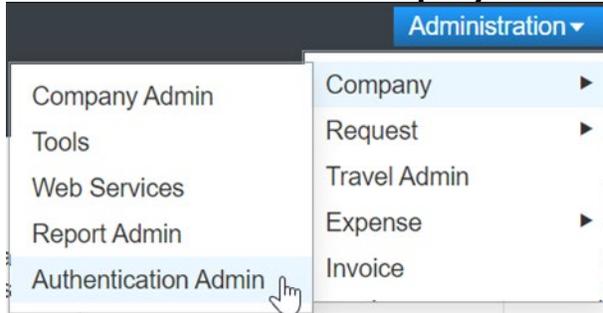


3. Click **Manage Single Sign-On** to access the **Manage SSO** page.

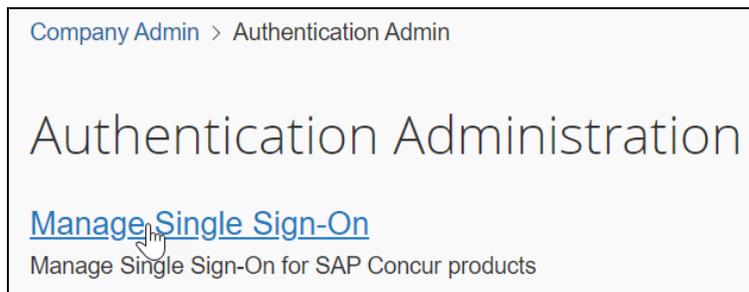


For the SAP Concur **Professional** edition:

1. Go to **Administration > Company > Authentication Admin.**



2. Click **Manage Single Sign-On** to access the Manage SSO page.



Alternatively, users can access the page using one of the following URLs:

- 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>

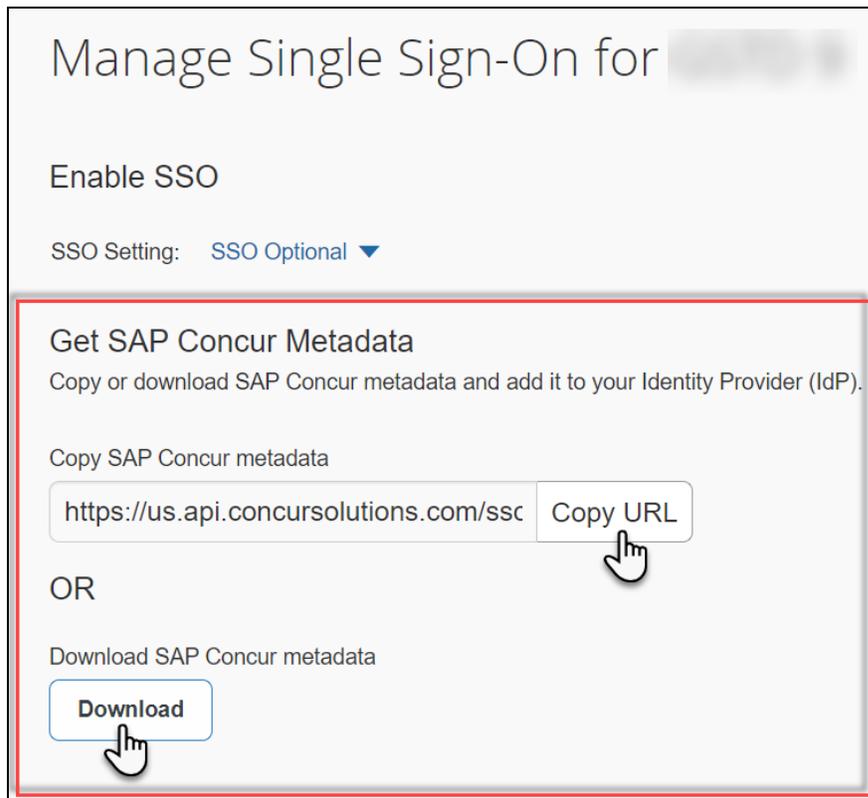
NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an authorized support contact at your company to open a case with SAP Concur support.

Configure Your SAP Netweaver Application

Step 1: Get the SAP Concur metadata

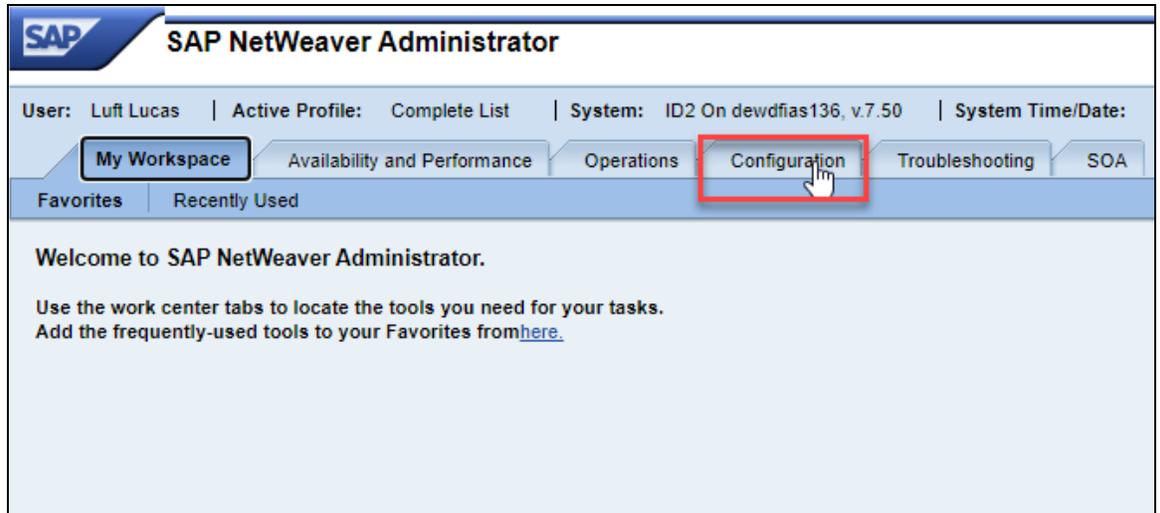
To configure:

1. Get the SAP Concur metadata. To complete this, follow the instructions in the Overview section to log in to your SAP Concur account and access the **Manage SSO** section. To obtain the SAP Concur metadata on the **Manage SSO** page, you can either click **Copy URL** and then paste it in a new browser tab or click **Download** and open the downloaded file.

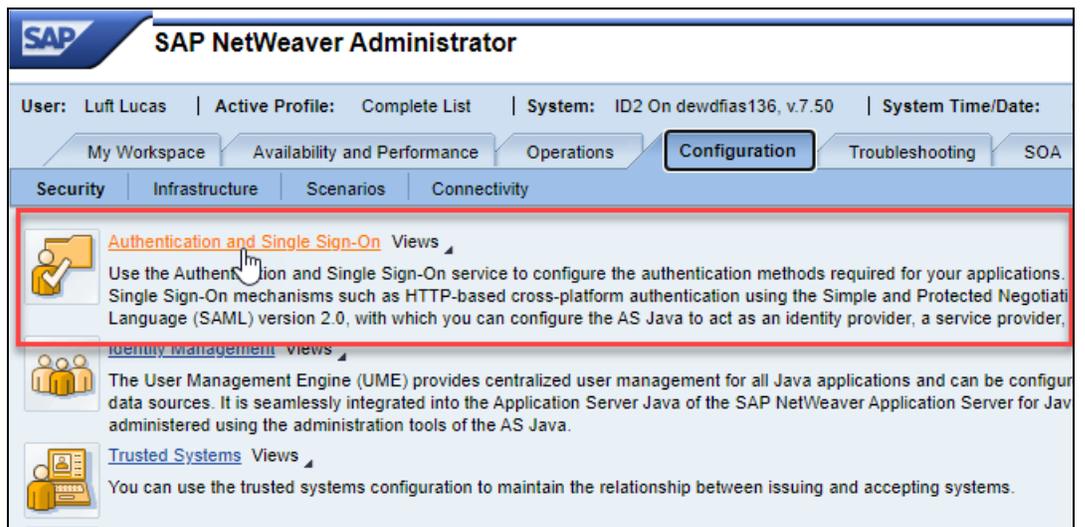


Step 2: Create an application on SAP Netweaver

1. Create an application in SAP Netweaver. After logging in to SAP NetWeaver, you will need to access the Configuration tab.



2. On the Configuration tab, click **Authentication and Single Sign-On**.



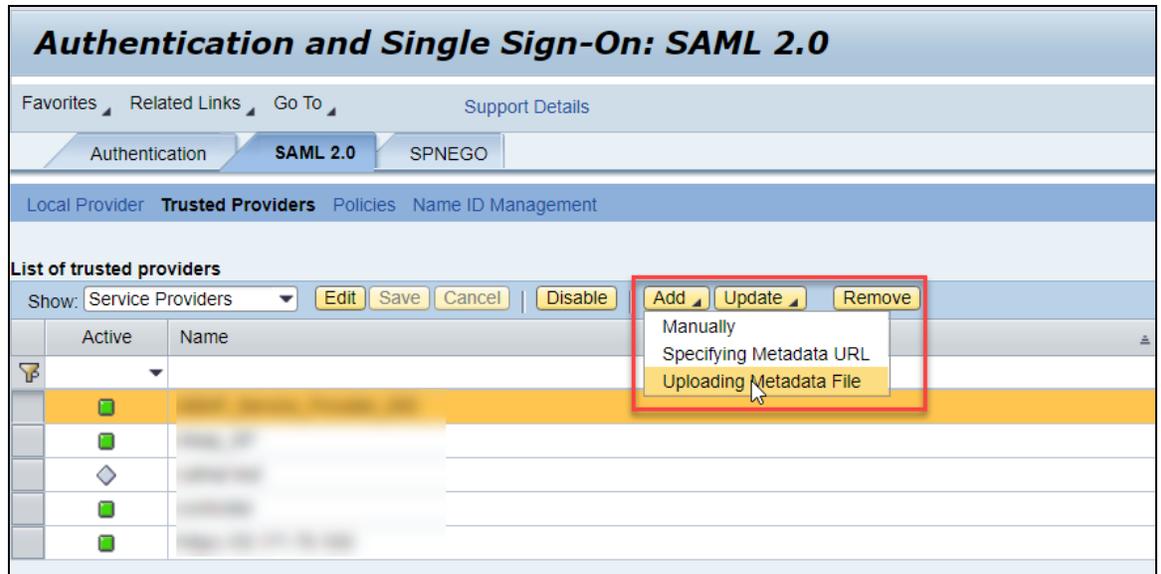
3. This will be a SAML (Security Assertion Markup Language) configuration. Click the **SAML 2.0** tab.



4. To start creating the SAP Concur application, click **Trusted Providers**.



5. The Trusted Providers section should show all existing service providers connected to your SAP NetWeaver tenant. To add a new application, click **Add**. Since you have already downloaded the SAP Concur metadata file in the first step, choose the **Uploading Metadata File** option.

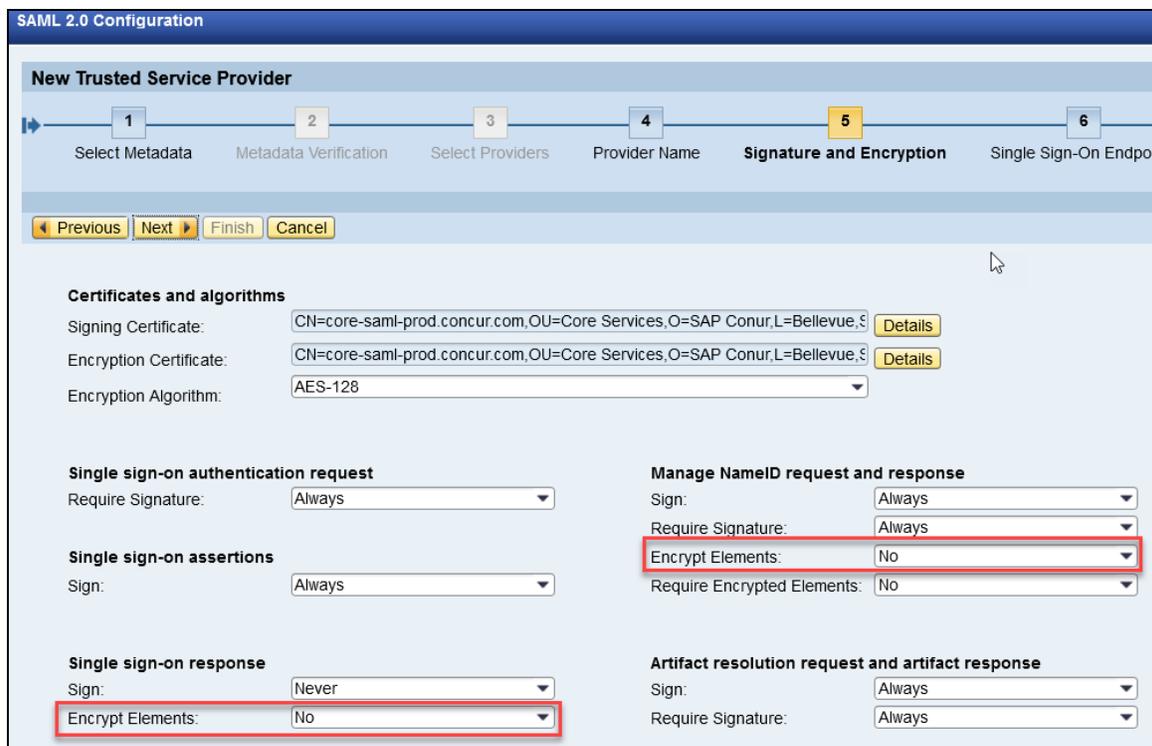


6. Click **Browse** to look for the metadata file on your computer and then click **Next**.



7. After that you should see steps 2 (**Metadata Verification**) and 3 (**Select Providers**) greyed out and skipped automatically. You can also click **Next** to skip step 4 (**Provider Name**) since it will be automatically filled with the proper identifier (also called **Entity ID**) from the metadata.

For step 5 (**Signature and Encryption**) you can also click **Next** without making any changes. However, if you want to encrypt the assertion and/or the **NameID** request and response, you will need to adjust the **Encrypt Elements** field so this is enabled. Then, click **Next** again.



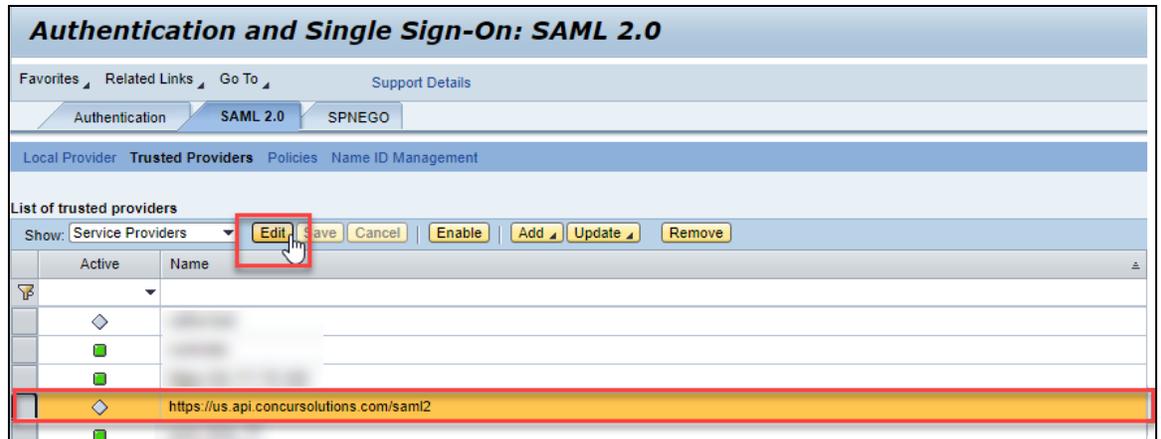
Step 6 (**Single Sign-On Endpoints**) will be filled automatically with the proper ACS URL taken from the metadata xml, so you can skip it. You can do the same for steps 7 (**Single Log-Out Endpoints**), 8 (**Artifact Endpoints**) and 9 (**Manage Name ID Endpoints**) until you are able to click **Finish**.



Step 3: Name ID configuration

After finishing the application configuration, you need to configure the **Name ID**. The **Name ID** must match the Login ID (**CTE Login Name**) registered for your employees in SAP Concur. We also strongly recommend that you set the **Name ID** format to **Email address**. This is required by SAP Concur for the SP-Initiated logins, starting from concursolutions.com or from the mobile app.

1. To set the **Name ID** format, search for your new application, click it and then click **Edit**.



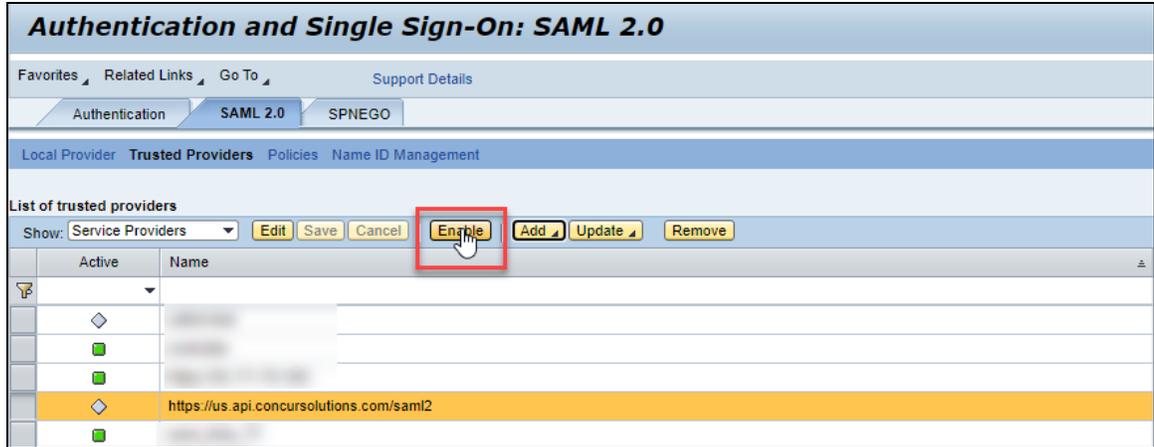
2. On the Name ID Format popup, make sure you select **E-mail**. Fill in **Source Name** with the attribute matching your employees' Login ID in SAP Concur.



3. In some cases, the available Source Name may not match the usernames in SAP Concur. If this is the case, you can run employee imports in SAP Concur to make sure they match the attribute you send. Alternatively, you can reach out to product support for SAP NetWeaver for further help with Name ID configurations.

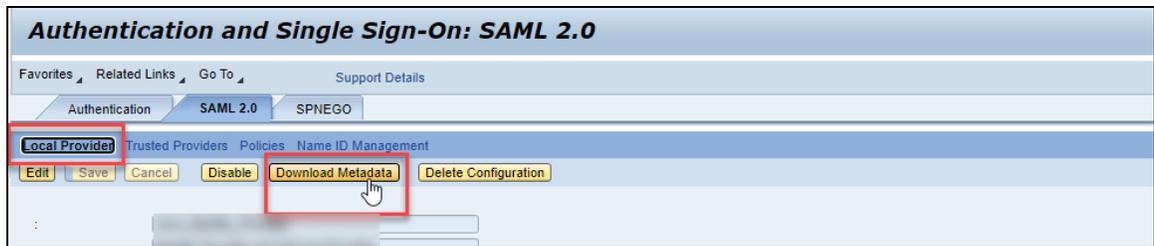
Step 4: Enabling the application

With the **Name ID** configured you should be able to go back to the SAML 2.0 tab, select the new application and click **Enable**. This should change the **Active** column icon to a green square, confirming the application is active.



Step 5: Download the Metadata File

To finish the configuration on the SAP Concur side, upload the Metadata file extracted from your application in SAP Netweaver. On the **SAML 2.0** tab, go to **Local Provider** and click **Download Metadata** to download the metadata xml.



Configure Your SAP Concur Site

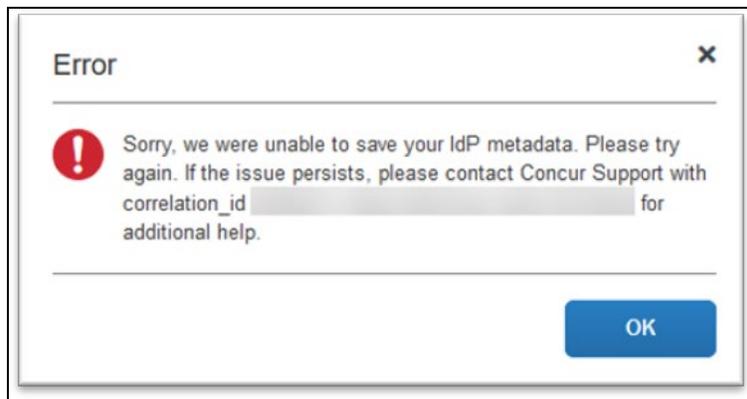
1. Go to the **Manage SSO** page by following the steps provided in the Overview section.
2. Click **Add** from the **IdP Metadata** section. The Add IdP Metadata window appears.
3. Enter an appropriate name in the **IdP connection** and enter it in the **Custom IdP Name** field.

NOTE: If you decide to use the SP-initiated flow (through SAP Concur's public site: <https://www.concursolutions.com/nui/signin>), the **Custom IdP Name** will display on the **Sign In** page right after a user provides their Username and clicks **Next**. For example, if your **Custom IdP Name** is "SAP NW", then all users will see the option "Sign in with SAP NW".

4. Provide a Logout URL (optional) for users to get redirected to a different place when they log out. By default, if no URL is entered, users will be redirected to where they started the authentication process. The logout endpoint for SAP NetWeaver can be found on **Local Provider > Identity Provider Settings > Single Log-Out Service (SLO) > Endpoint URL**. Please note that **Single Logout (SLO)** is not officially supported by SAP Concur, so the logout process with the SLO endpoint may not work as expected regarding disconnecting the user from the IDP in addition to SAP Concur. In that case, the user may be logged out from SAP Concur but not from SAP NetWeaver entirely.
5. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP, which was previously saved locally.
6. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox **Hide this SSO option from users signing in to Concur on web or mobile**.

By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.

7. Click **Add Metadata**.
8. You should see either a successfully added confirmation or a something went wrong message. For the latter, please contact SAP Concur support and provide the Correlation ID.



Test SSO Login

You can start testing SSO after you've successfully uploaded the IdP metadata to SAP Concur from the previous steps. In this section, you can test the IdP-Initiated (initiated on the identity provider side) and SP-Initiated (initiated on the service provider side) flows.

Test IdP-initiated SSO

To test IdP-initiated SSO:

1. In the IdP-Initiated flow, start the login process on the identity provider side. To test that, append the parameters from the application you just created to the SSO endpoint from SAP NetWeaver. A format example of IdP-Initiated URL would be:

Format: [**SSO Endpoint URL***]?saml2sp=[**SP Identifier****]

Example:

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

****SP Identifier:** You can obtain this value from the SAP Concur metadata. It will be the same as **Entity ID** or **Audience**.

***SSO Endpoint URL:** You can obtain this value by following this path: **SAML 2.0 > Local Provider > Identity Provider Settings > Single Sign-On Service (SSO) > Endpoint URL**.

The screenshot shows the 'Authentication and Single Sign-On: SAML 2.0' configuration page. The 'Identity Provider Settings' tab is active. Under the 'Single Sign-On Service (SSO)' section, the 'Endpoint URL' is set to 'https://dewdfias136.wdf.sap.corp:50201/saml2/idp/sso', which is highlighted with a red box. Other settings include 'Supported SSO Types' (IdP-Initiated and SP-Initiated checked), 'Supported Bindings' (HTTP Redirect, HTTP POST, HTTP Artifact, and SOAP checked), 'Session Timeout' (3.600 Seconds), and 'Cleanup Interval for Expired Sessions' (360 Minutes).

This URL should redirect to a login page on the SAP NetWeaver side. Once you login with your credentials, you should be redirected to the SAP Concur homepage.

Test SP-initiated SSO

To test the SP-initiated SSO:

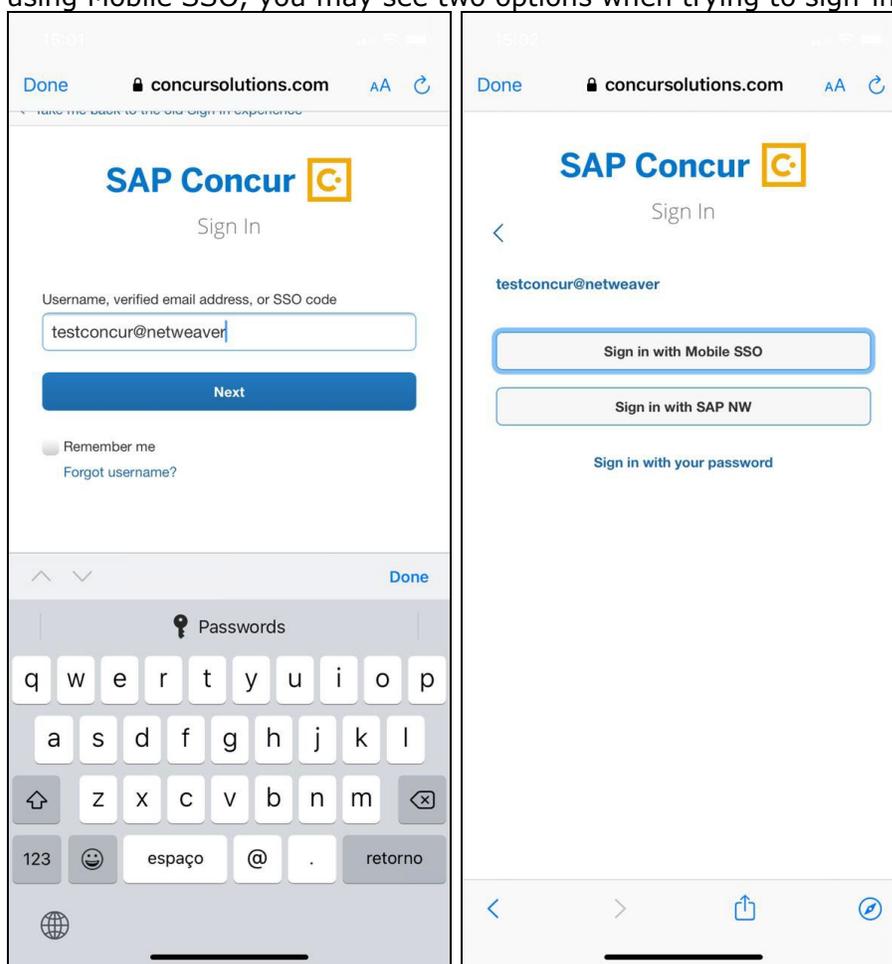
- Open the SAP Concur login page according to the environment you want to test.
 - US DC Prod: <https://www.concursolutions.com/>
 - US DC Test: <https://implementation.concursolutions.com/>
 - EMEA DC Prod: <https://eu1.concursolutions.com/>
 - EMEA DC Test: <https://eu1imp.concursolutions.com/>
 - CN DC Prod: <https://www.concurcdc.cn/>
- On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click **Next**, you should see an option for your recently created SSO configuration according to the note in *Configure Your*

SAP Concur Site. Click to proceed with authenticating your identity provider account which should redirect you to SAP Concur.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated using the previous *Test SSO login* section.

NOTE: The automatic enabling of Mobile SSO is only visible on the app version 9.86 or higher and if the user is opting for the new sign in experience. Users on older versions or opting for the earlier sign in experience will not see this option automatically. However, if you were using another IdP and already using Mobile SSO, you may see two options when trying to sign-in as follows:



The **Sign in with Mobile SSO** option will have your earlier IdP link embedded, so it will redirect users to your old SSO connection.

For both cases, please open a ticket with the SAP Concur support team, providing them the following information.

- If the users plan to use an older version, please provide SAP Concur support with the IdP-Initiated URL from the application created on the SAP NetWeaver side so they can enable Mobile SSO for the legacy app versions. For more information on how to obtain the URL see *Test SSO login > Testing IdP-Initiated SSO* section on this guide.
- If you want to remove the **Sign in with Mobile SSO** option to eliminate potential confusion, please inform the support team.

If you have any issues in authenticating with SSO on the mobile app, please open a ticket with the SAP Concur support team and provide any error IDs and/or messages received with screenshots.

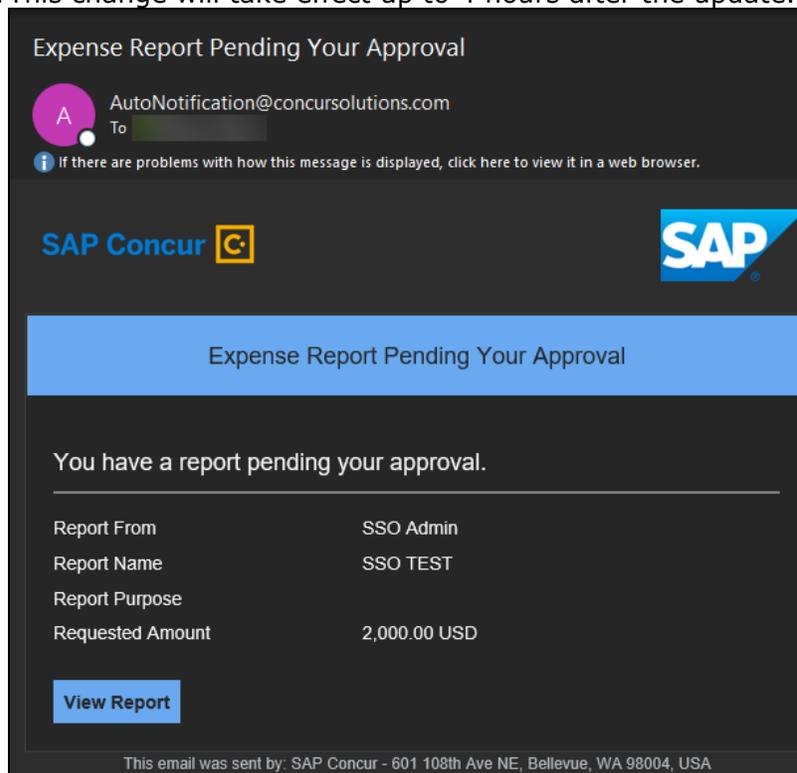
E-mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket with the SAP Concur support team, providing the IDP URL from the application created on the IDP side so they can adjust the redirect URL for e-mail reminders. For more information on how to obtain the URL, see the *Test SSO login > Testing IdP-Initiated SSO* section of this appendix.

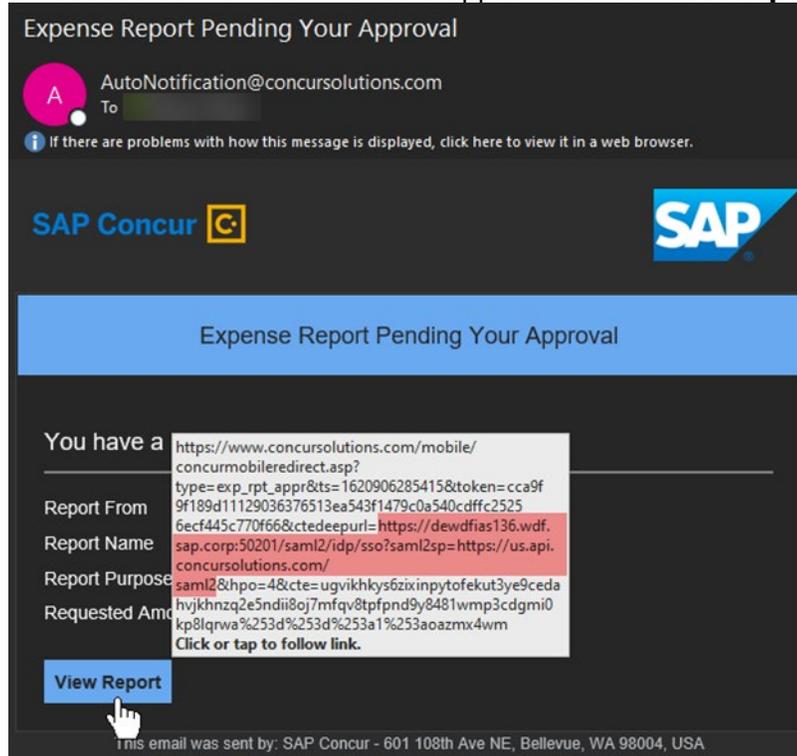
NOTE: The URL will appear embedded on the **View Report** button.

NOTE: This change will only be reflected in emails generated after the change. All emails prior to that will keep using the previous URL.

NOTE: This change will take effect up to 4 hours after the update.



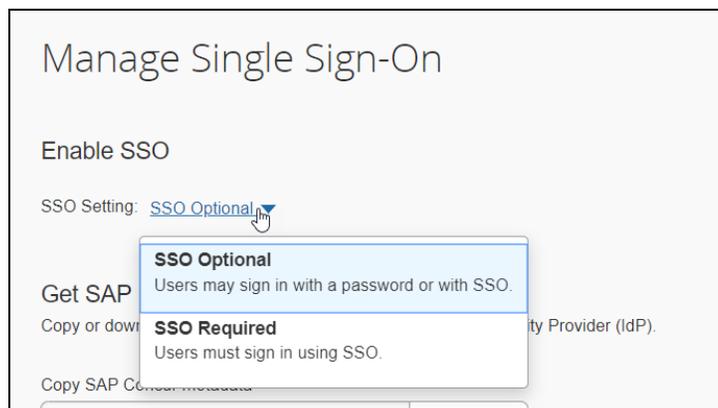
If you hover the cursor over the **View Report** button, you will see the currently embedded URL. The URL should appear between **ctedeepurl=** and **&hpo=** terms.



Rollout

After testing your new SSO configuration, you can then plan your rollout by assigning your new SAP NetWeaver application to all your users and groups who'll need this access.

The Manage SSO page also offers the option for you to enforce this new SSO connection by changing the SSO Setting from SSO Optional to **SSO Required**. If you change it, users will be redirected to SAP Concur by providing their Username via the SP-initiated flow.



View Previous Changes

This featured was developed to help admins keep track of all changes completed under the **Manage SSO** page.

To view changes to the SSO configuration that have been made over time, click **View Previous Changes**.

A table listing previous changes appears and it is sorted in descending order by date and time.

The table can display the last 100 changes. Changes that are listed in the table include:

- Add a configuration
- Delete a configuration
- Edit Custom IdP Name, Logout URL, or Hidden fields

To view more detailed information about a specific change listed in the table, click the **View** link for the desired list item.

View Previous Changes						
Date	Change	Entity ID	Name	Logout URL	Hidden	Details
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	Concur Okta		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2			View

Inside each log, you'll see the **Company** and **ChangeBy** fields in the format [first_name last_name] [(UUID code)]; this refers to the user who performed the action. In case you don't recognize that user, you can contact support to request further details about it.

View Previous Changes
X

Date Changed	06/08/2022
Change	Edit
Company	[REDACTED]
Change By	[REDACTED]

Entity ID	[REDACTED]
Name	Concur Okta
Logout URL	
Hidden	✓

Previous Values

Entity ID	[REDACTED]
Name	Concur Okta
Logout URL	
Hidden	

Metadata

[REDACTED]

OK

For deleted configurations, the **View Previous Changes** page includes a **Revert** button that enables you to reinstate the deleted configuration. After the configuration is reinstated, it will be available to users during the sign-in process.



For more info, please refer to the following documentation resources:

- ◆ SAP Concur - [SSO Overview Guide](#)
- ◆ SAP Help Portal - [SAP Single Sign-On](#)
- ◆ SAP Help Portal - [Configuring AS Java as a Service Provider](#)
- ◆ SAP Help Portal - [Identity Provider Implementation Guide \(HTML\)](#)

Section 15: Appendix – Google Workspace Setup

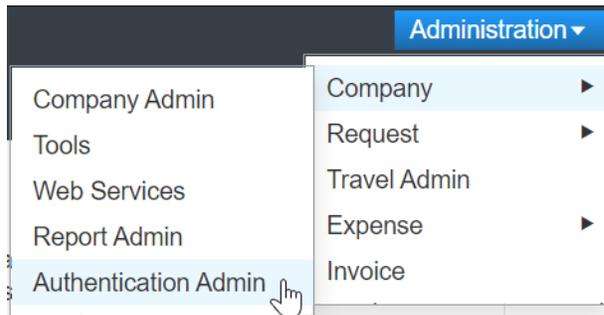
Overview

Before you start the configuration process, make sure that:

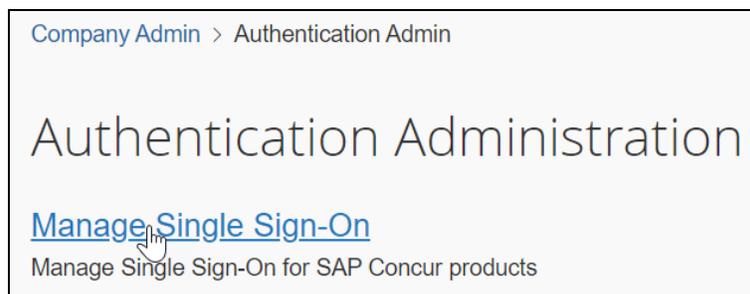
- You have admin access to the identity provider (Google Workspace). This will be needed so you can complete the application configuration on the Google Workspace side.
- Your users exist in both Google Workspace and SAP Concur. Auto user provisioning is not currently supported by Concur, so you need to add users separately in there.
- The attribute you are sending from Google Workspace matches the **Login ID (Username / CTE Login Name)** field for each employee in SAP Concur.
- You have the Company Administrator (Travel permission) assigned to your SAP Concur account. Once you have the permission, you can access the Manage SSO page by following one of the below paths, depending on your SAP Concur edition.

SAP Concur Professional edition:

1. Go to Administration > Company > Authentication Admin.



2. Hit **Manage Single Sign-On** to access the **Manage SSO** page.



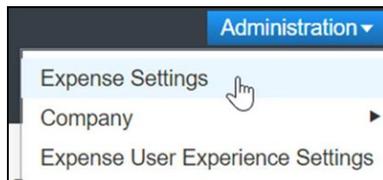
Alternatively, users can access the page using one of the following URLs:

- ◆ **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>

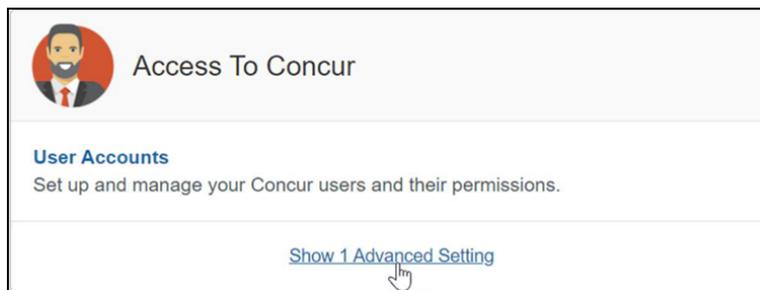
NOTE: If you don't have that permission and cannot have this assigned to your profile, please ask an Authorized Support Contact at your company to open a case with SAP Concur Support.

SAP Concur Standard edition:

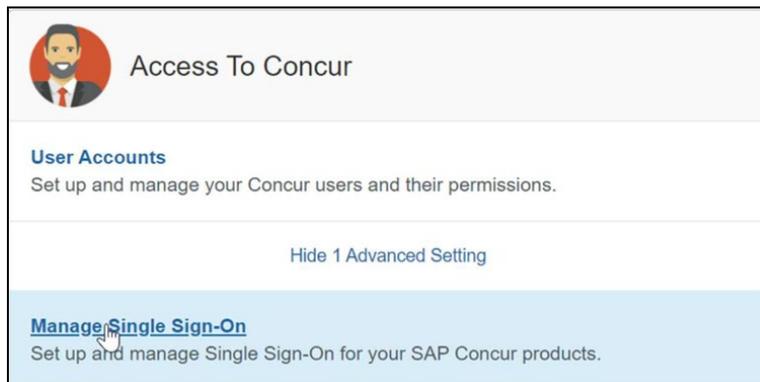
1. Go to **Administration > Expense Settings**.



2. Under **Access to Concur** click **Show 1 Advanced Setting**.



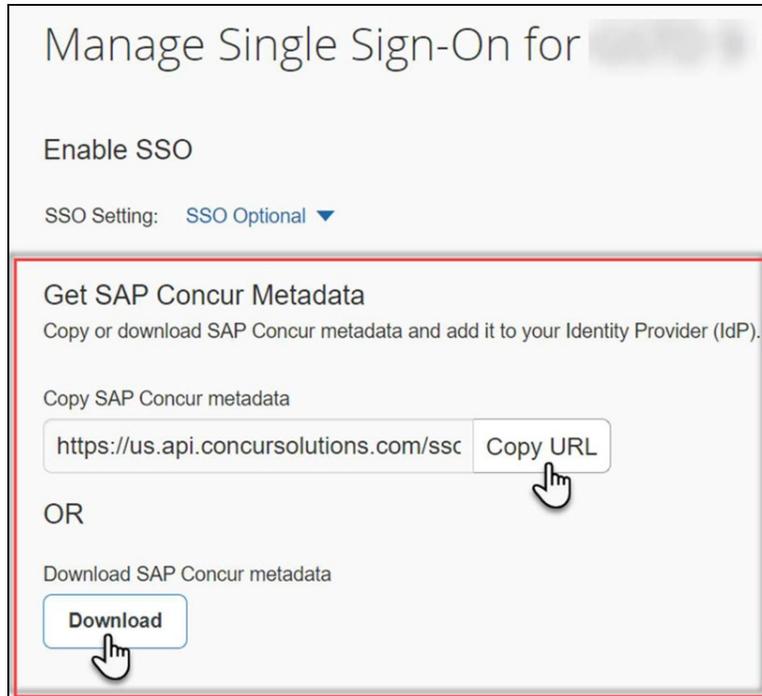
3. Click **Manage Single Sign-On** to access the **Manage SSO** page.



Configure Your Google Workspace (IDP) APP

Step 1: Get the SAP Concur metadata

To complete this you will need to follow the instructions on the **Preparation** section earlier in this guide login to your SAP Concur account and access the **Manage SSO** section. To obtain the **SAP Concur Metadata** on the **Manage SSO** page, you can either click on "Copy URL" and then paste the URL in a new browser tab or click **Download** and open the downloaded file.



Step 2: Set up your own custom SAP Concur SAML app

1. Sign into your **Google Admin** console.

NOTE: (Sign in using an account with super administrator privileges (does not end in @gmail.com or similar)).

2. From the Admin console Home page, go to **Apps Web** and mobile apps.
3. Click **Add App** to add **custom SAML** app.
4. On the **App Details** page:
 - ◆ **Custom app name**
Enter the name of the custom app, for example, '**SAP Concur**'
 - ◆ *(Optional)* **Upload an app icon**
The app icon appears on the Web and mobile apps list, on the app settings page, and in the app launcher. If you don't upload an icon, an icon is created using the first two letters of the app name
5. Click **Continue**.
6. On the **Google Identity Provider details** page, get the setup information needed by the service provider using the **Download the IDP metadata** option.
7. *(Optional)* In a separate browser tab or window, sign into your service provider and copy the information you entered in Step 4 into the appropriate SSO configuration page, then return to the Admin console.

8. Click **Continue**.
9. In the **Service Provider Details** window, enter the following ACS URL and Entity ID for your app.

ACS URL

- **US (North America):** <https://www-us.api.concursolutions.com/sso/saml2/V1/acs/>
- **EMEA:** <https://www-emea.api.concursolutions.com/sso/saml2/V1/acs/>
- **China:** <https://www-cn.api.concurcdc.cn/sso/saml2/V1/acs/>

Entity ID

- **US (North America):** <https://us.api.concursolutions.com/saml2>
- **EMEA:** <https://emea.api.concursolutions.com/saml2>
- **China:** <https://cn.api.concurcdc.cn/saml2>

10. The default **Name ID** is the primary email - multi-value input is not supported.
11. Click **Finish**.

Step 3: Turn on your SAML app

1. Sign into your **Google Admin** console.

NOTE: (Sign in using an account with super administrator privileges (does not end in @gmail.com or similar)).

2. From the Admin console Home page, go to **AppsWeb and mobile apps. +**
3. Select your SAML app.
4. Click **User access**.
5. To toggle availability of a service for your organization, click **On** for everyone or **Off** for everyone, and then click **Save**.
6. (*Optional*) To turn a service on or off for an organizational unit:
 - ◆ At the left, select the **organizational unit**.
 - ◆ To change the Service status, select **On** or **Off**.
 - ◆ Choose one:
 - If the Service status is set to Inherited and you want to keep the updated setting, even if the parent setting changes click **Override**.

- If the Service status is set to Overridden, either click **Inherit** to revert to the same setting as its parent, or click **Save** to keep the new setting, even if the parent setting changes.
7. To turn on a service for a set of users across or within organizational units, select an **access group**. For details, go to *Provide access to user groups* in this document.
 8. Ensure that the **email addresses** your users use to sign in to the SAML app match the **email addresses** they use to sign into your Google domain. Changes typically take effect in minutes but can take up to 24 hours.

NOTE: Google Workspace doesn't support encryption of assertion currently. Please reach out to the IDP support if you need more information around this.

Step 4: Configure Your SAP Concur Site

1. Go to the **Manage SSO** page again by following the steps provided on the **Preparation** section.

Click on **Add** under **IdP Metadata** section. The **Add IdP Metadata** window appears.

2. Give your IdP connection a friendly name and enter it in the **Custom IdP Name** field.
3. Provide a **Logout URL** (optional), so the users get redirected to a different place when signing out.

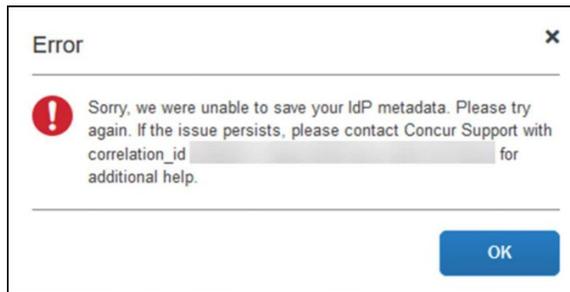
By default, if no URL is entered, users will be redirected to where they started the authentication process. The logout endpoint for Google Workspace can be found on **Applications & Resources > Tenant Settings > Identity Provider Settings > Single Logout Endpoint**.

NOTE: Single Logout (SLO) is not officially supported by SAP Concur, so the logout process with the SLO endpoint may not work as expected regarding disconnecting the user from the IDP in addition to Concur. In that case, the user may be logged out from SAP Concur but not from Google Workspace entirely.

4. In the **Upload your IdP's metadata** section, click **Upload XML File** and upload the metadata file from the IdP, which was previously saved locally.
5. To hide the sign-in option from users on mobile and signing in through concursolutions.com, select the checkbox **Hide this SSO option from users signing in to Concur on web or mobile**.

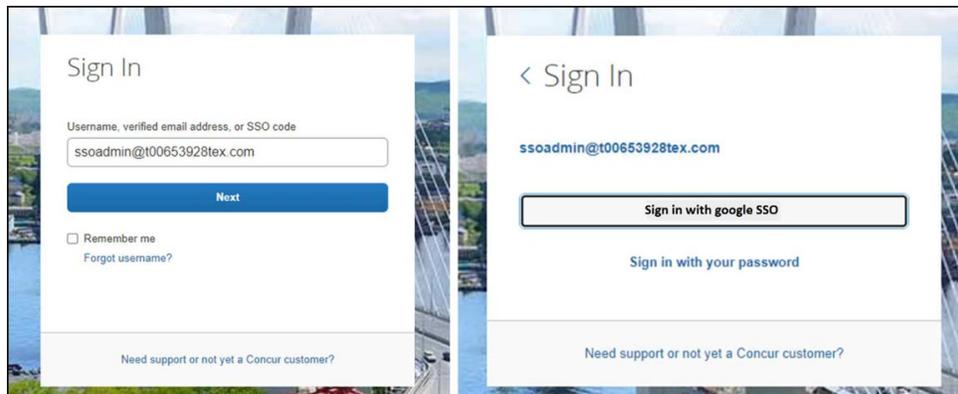
By default, the option is available to users when they begin an SP-initiated sign-in through concursolutions.com or the mobile app. The option can be hidden in those cases that require users to sign-in through an IdP-initiated flow.

6. Click **Add Metadata**.
7. You should see one of following prompts on your screen saying it was successfully added or saying something went wrong while adding it.



For help with the latter, please contact *SAP Concur Support* and provide the correlation ID.

For step 3 above, if you decide to use the *SP-initiated flow* (through SAP Concur's public site: <https://www.concursolutions.com/nui/signin>), the **Custom IdP Name** will be displayed on the **Sign In** page right after a user provides their **Username** and hits **Next** (see below image). For example, if your "Custom IdP Name" is "google SSO", then all users will see the option "Sign in with google SSO " as shown in the following:



Test SSO Login

You can start testing SSO after you've successfully uploaded the IdP metadata to *SAP Concur* from the previous step. We'll test the **IdP-Initiated** (initiated on the identity provider side) and **SP-Initiated** (initiated on the service provider side) flows.

1. TESTING IDP-INITIATED SSO

In the IdP-Initiated flow we start the login process on the identity provider. To test it, we can append parameters from the application we built to the SSO endpoint from Google Workspace.

An example of IdP-Initiated URL is:

Format: `https://accounts.google.com/o/saml2/initssoidpid=CLIENT_IDP_ID&spid=SERVICE_PROVIDER_ID&forceauthn=false`

Example: `https://accounts.google.com/o/saml2/initssoidpid=C03fj4v82&spid=710982774547&forceauthn=false`

NOTE: You must fill CLIENT_IDP_ID and SERVICE_PROVIDER_ID with values from Google Workspace and it's something you can get by copying the URL from the **Test SAML login** button on the application

2. TESTING SP-INITIATED SSO

In order to test the SP-initiated flow, you will need to open the SAP Concur login page.

- **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/>

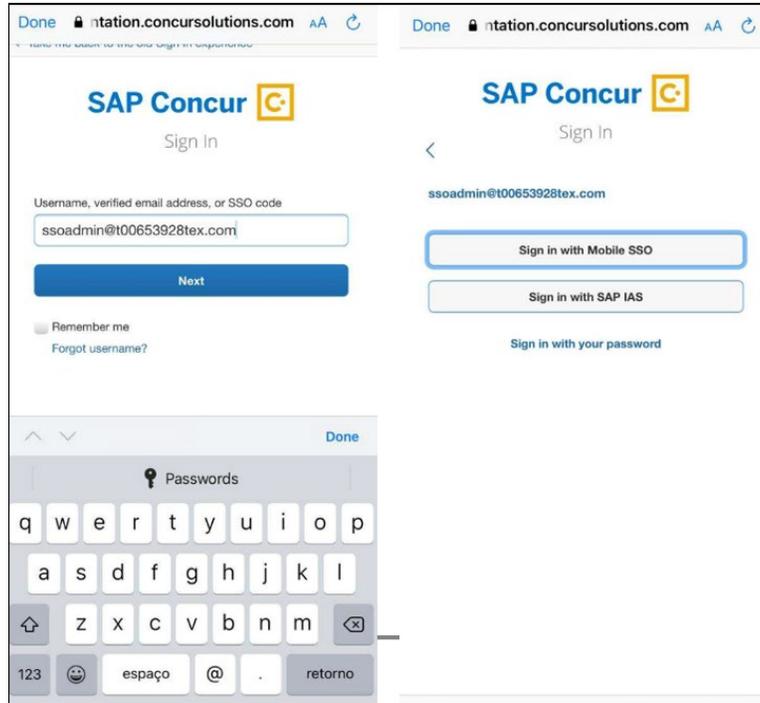
On the login page, you can add your username, verified e-mail address or SSO code to proceed. Once you click on **Next**, you should see an option for your recently created SSO configuration. You can click on that and proceed with authenticating to your Google account which should redirect you back to SAP Concur after that.

Mobile Single Sign-On (SSO)

For SSO configurations created on our SAMLv2 platform, the Mobile SSO should be enabled automatically as soon as the metadata is saved. However, for this option to work, the SP-Initiated flow needs to be functioning. This can be validated on the 'Test SSO login' section on this guide.

If you have issues to authenticate with SSO on the mobile app, please open a ticket to the SAP Concur support team providing any error IDs and/or messages received.

It's important to note that if you were using another IdP and you were already using Mobile SSO, you'll probably see 2 options when trying to sign-in as follows:



The **Sign in with Mobile SSO** option will have your old IdP link embedded, so it will redirect users to your old SSO connection.

For both cases, please open a ticket to the SAP Concur support team providing them the following information.

- If the users plan to use an older (legacy) version, provide the IdP-Initiated URL from the application built on the Google Workspace side so Support can enable Mobile SSO for the legacy app versions. More information about how to get the URL can be found on the 'Test SSO login > Testing IdP-Initiated SSO' section on this guide.
- If you want to remove the 'Sign in with Mobile SSO' option so it doesn't confuse your users, please inform that to the support team.

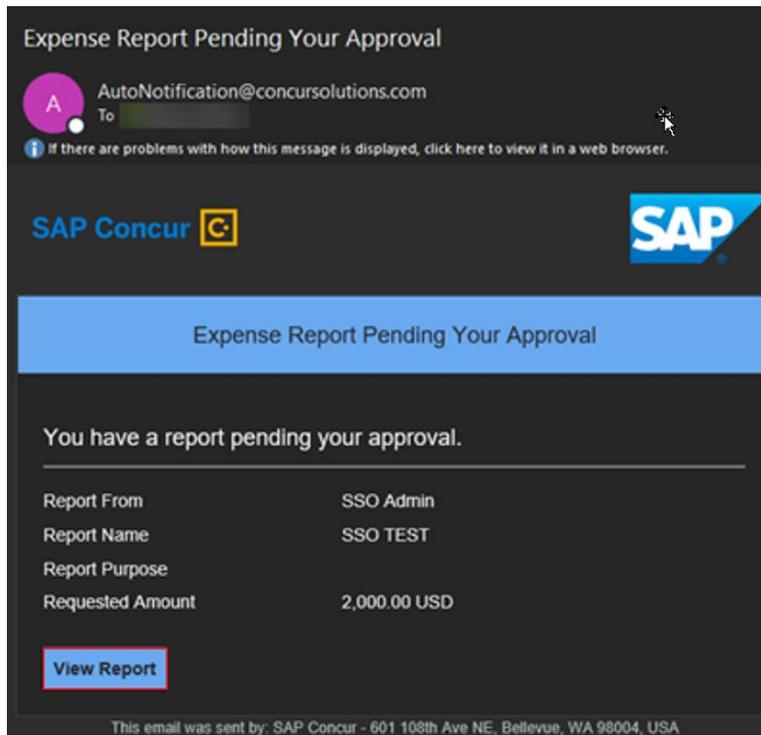
If you have any issues to authenticate with SSO on the mobile app, please open a ticket to the SAP Concur Support team providing any error IDs and/or messages received with screenshots.

E-Mail Notifications

The configuration of e-mail reminders to reflect your SSO URL are changes that need to be completed by SAP Concur support. To proceed, please open a ticket to the *SAP Concur* support team providing the IDP URL from the application built on the IDP side

so they can adjust the redirect URL for E-Mail reminders. More information about how to get the URL can be found on the *Test SSO login > Testing IdP-Initiated SSO* section on this guide.

- The URL will appear embedded on the **View Report** button
- This change will only be reflected in emails generated after the change - all emails prior to that will keep using the previous URL.
- This change will take effect up to 4 hours after the update.



If you hover the cursor over the **View Report** button you will see what's the URL currently embedded. The URL should appear between "ctedeepurl=" and "&hpo=" terms.

Rollout

After testing your new SSO configuration, you can then plan your rollout by assigning your Google Workspace application to all your users and groups who'll need this access.

The **Manage SSO** page also offers the option for you to enforce this new SSO connection by changing *SSO Setting* from *SSO Optional* to *SSO Required*. If you change it, users will be redirected to Concur by just providing their Username via SP-initiated flow.



View Previous Changes

This feature was developed to help admins to keep track of all changes completed under the **Manage SSO** page. To view changes to the SSO configuration that have been made over time, click on the **View Previous Changes** button.

A table listing previous changes appears and is sorted in descending order by date and time. The table can display the last 100 changes. Changes that are listed in the table include:

- Add a configuration
- Delete a configuration
- Edit Custom IdP Name, Logout URL, or Hidden fields

To view more detailed information about a specific change listed in the table, click the **View** link for the desired list item.

View Previous Changes						
Date	Change	Entity ID	Name	Logout URL	Hidden	Details
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	Concur Okta		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2		✓	View
06/08/2022	Edit	http://www.okta.com/exk8bjsi41SiSaXyM2p7	ray test 2			View

Inside each log, you'll see the field **Company** and **Change by** in the format **[first name last name] [(UUID code)]**, which will mean who has performed such action. In case you don't recognize that user, you can always reach out to support requesting further details about it.

For deleted configurations, **View Previous Changes** includes a **Revert** button so you can reinstate the deleted configuration. After the configuration is reinstated, it will be available to users during the sign-in process.



For more info, please refer to the following documentation resources:

- ◆ SAP Concur - [SSO Overview Guide](#)
- ◆ SAP Help Portal - [SAP Single Sign-On](#)

