Shared: Single Sign-On

Setup Guide

Last Revised: January 22, 2024

Applies to these SAP Concur solutions:

- \boxtimes Expense
 - Professional/Premium editionStandard edition
- 🗵 Travel
 - ☑ Professional/Premium edition☑ Standard edition
- \boxtimes Invoice
 - ⊠ Professional/Premium edition
 - \boxtimes Standard edition
- ⊠ Request
 - ⊠ Professional/Premium edition
 - ⊠ Standard edition

Table of Contents

Section 1: Permissions1
Section 2: Overview1
Feature Benefits1
Requirement2
Section 3: Obtaining Required Permissions2
Professional Edition Customers with Concur Travel
Professional Edition Customers Without Concur Travel; All Standard Edition Customers2
Section 4: Configuration - Two Methods for Web-Based Services 2
Important!
Identity Provider (IdP)-Specific Process
General Process
Section F. Configuration for Web Paged Services Conexal Dresses
Access the Manage Single Sign-On Page
Configure on SSO App/Connector Without Encryption
Sten 1: Obtain the EntityID and ACS Endpoint
Step 2: Provide the EntityID and ACS Endpoint
Step 3: Provide the Recipient URL and Destination URL
Step 4: Ensure the NameID (IdP) Matches the User Login_ID (SAP Concur
Solutions)
Step 5: Uptain the IdP Metadata
Step 7: Test IdP-Initiated SSO
Step 8: Test SP-Initiated SSO
Step 9: Enable SSO as Optional or Required17
Editing SSO Configurations
View Previous Changes
Configure an SSO App/Connector with Encryption (Optional)
Step 1. Obtain and Save the Encryption Rey
Section 6: FAQ
Section 7: Appendix - ADFS Setup29
Getting Started
Configure Your ADFS Application
Configure Your SAP Concur Site
Test SSO Login
Test SP-initiated SSO
Mobile Single Sign-On (SSO) 45
F-mail Notifications
Rollout 45
Contine On Annually, Minescoft Annua AD Cotton
Section 8: Appendix - Microsoft Azure AD Setup
Gelling Stafted
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
	Nebile Circle Circle On (CCO)	. 57
	Mobile Single Sign-On (SSO)	. 59
	E-mail Notifications	. 59
	Rollout	. 59
Sec	tion 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	. 04 64
	Tost SSO Login	. 04 66
	Mehile Single Sign On (SSO)	.00
	Mobile Single Sign-On (SSO)	.0/
		. 00
		. 69
	View Previous Changes	. 70
Sec	tion 10: Appendix - Idaptive Setup	.72
Sec	tion 10: Appendix - Idaptive Setup Getting Started	72 72
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application	.72 .72 .74
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application Step 1: Create the Idaptive app	. 72 . 72 . 74 . 74
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application Step 1: Create the Idaptive app Configure Your SAP Concur Site	. 72 . 72 . 74 . 74 . 78
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application Step 1: Create the Idaptive app Configure Your SAP Concur Site Test SSO Login	. 72 . 72 . 74 . 74 . 78 . 79
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application Step 1: Create the Idaptive app Configure Your SAP Concur Site Test SSO Login Test IdP-initiated SSO	. 72 . 74 . 74 . 74 . 78 . 79 . 79
Sec	tion 10: Appendix - Idaptive Setup	. 72 . 74 . 74 . 74 . 78 . 79 . 79 . 79
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application Step 1: Create the Idaptive app Configure Your SAP Concur Site Test SSO Login Test IdP-initiated SSO Test SP-initiated SSO. Mobile Single Sign-On (SSO)	.72 .74 .74 .78 .79 .79 .79 .81
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .79 .81 .81
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .79 .81 .81 .82
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .74 .78 .79 .79 .79 .81 .81 .81 .82
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application Step 1: Create the Idaptive app Configure Your SAP Concur Site Test SSO Login Test IdP-initiated SSO Test SP-initiated SSO Mobile Single Sign-On (SSO) E-mail Notifications Rollout tion 11: Appendix - Okta Setup Getting Started	.72 .74 .74 .78 .79 .79 .79 .81 .81 .81 .82 .82
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .79 .81 .81 .82 .82 .82
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .81 .81 .82 .82 .82 .82 .84 .84
Sec	tion 10: Appendix - Idaptive Setup Getting Started Configure Your Idaptive Application Step 1: Create the Idaptive app Configure Your SAP Concur Site Test SSO Login Test IdP-initiated SSO Test SP-initiated SSO Mobile Single Sign-On (SSO) E-mail Notifications Rollout tion 11: Appendix - Okta Setup Getting Started Configure Your Okta Application Step 1: Get the SAP Concur metadata Step 2: Create an application on Okta	.72 .74 .74 .78 .79 .79 .81 .81 .81 .82 .82 .82 .84 .84 .84 .86
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .81 .81 .81 .82 .82 .82 .84 .84 .84 .88
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .79 .81 .81 .81 .82 .82 .82 .84 .84 .86 .88 .89
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .79 .81 .81 .82 .81 .82 .82 .84 .84 .84 .88 .88 .88 .89 .93
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .81 .81 .81 .82 .84 .84 .84 .84 .88 .88 .89 .93 .93
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .79 .81 .81 .81 .82 .82 .84 .84 .84 .88 .88 .89 .93 .93
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .79 .81 .81 .81 .81 .82 .82 .84 .84 .84 .88 .89 .93 .93 .94 .97
Sec	tion 10: Appendix - Idaptive Setup	.72 .74 .74 .78 .79 .79 .81 .81 .81 .82 .84 .84 .84 .88 .88 .93 .93 .93 .97 .97

Mobile Single Sign-On (SSO)	98
E-mail Notifications	
Rollout	100
View Previous Changes	101
Section 12: Appendix - PingOne Setup	101
Getting Started	101
Configure Your PingOne Application	102
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 Authenticat	ion
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
	129
	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 metadala file	144
Compute Your SAP Concur Site	144
Iest SSU Login	146
1651 107-111111dleu 350	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 Appendix – ADFS Setup.
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 IdPinitiated 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.

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 <u>Without</u> 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)

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.

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 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 <u>appendix</u> in this guide. For further reference: <u>https://docs.microsoft.com/en-us/azure/active-</u> <u>directory/saas-apps/concur-travel-and-expense-tutorial</u>
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 <u>appendix</u> 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	Choose one of these:
	 For SAP Concur customers in the US (North America) data center:
	htpps://{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
	Note the following:
	 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 <u>appendix</u> 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 <u>Without</u> Encryption.
- Configure an SSO App/Connector <u>With</u> 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 Autentication Administration page appears.



2. Click Manage Single Sign-On.



The Manage Single Sign-On page appears.

Administration • Help SAP Concur C	
Profile *	
Expense & Invoice Settings > Manage Single Sign-On	
Please complete testing before changing the SSO Setting to SSO Required. ×	
Manage Single Sign-On for	
Enable SSO	
SSO Setting: SSO Optional 🔻	
Get SAP Concur Metadata Copy or download SAP Concur metadata and add it to your Identity Provider (IdP).	
Copy SAP Concur metadata	
https://us.api.concursolutions.com/ssi Copy URL	
OR	
Download SAP Concur metadata	
Download	
IdP Metadata	
Add Edit Develo View Meladala	
No IdP Metadata	
Add one or more IdPs' metadata	
View Previous Changes	
Rollout Instructions	
1. Test SSO	
We recommend that you test SSO by selecting "SSO Optional" from SSO Settings and trying out the sign in flow before deploying to users. You may then change the option to "SSO Only" or keep it as optional.	
Failure to set up SSO correctly could result in not being able to log in to SAP Concur.	
2. User Rollout	
Make sure that your users know how to sign in using SSO	
SAP Concur G	•
Processor Privacy Statement	
Service Status Context Support Last signed in: 03/12/2021 06:52 p	<u>m</u>

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://wwwus.api.concursolutions.com/sso/saml2/V1/sp/metadata/
- EMEA: https://wwwemea.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.

2. Click Copy URL or Download.

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

Below are samples from SAP Concur US SP metadata at https://www-us.api.concursolutions.com/sso/saml2/V1/sp/metadata/.

The red boxes indicate the EntityID and ACS endpoint respectively.

<pre>w<md:entitydescriptor entitydescriptor.xmlns:md="urn:osc/saml2" xmlns:mm="urn:ossis:names:tc:SAML:2.0:metadata"> x<md:entitydescriptor xmlns:md="urn:osc/saml2"> x<md:entitydescriptor xmlns:md="urn:osc/saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"> x<md:saml2"< td=""></md:saml2"<></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:saml2"></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></md:entitydescriptor></pre>
Values as a second
wind responsible to the start start and the start sta
weakeysinto Amina, da- Help://www.wsioig/2000/03/Amidalig# >
MIGTICLEGNGAWIDAGIOARVONDEVVQASHAUGCSGGSIDSUDEDEWURHIGENGSWCGIDVQQGEWUVUZET INDGALUBCDHIVZEZAGLUZSKUD JERRAGALUBCHTQUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGUG
ALUCCERAVEZZGLUZZSKOJEKRAGGALUESZNUMYSDGVZGWZEJGLUGUGUGUGUCUNEUCEDDZICEEM MEGGALUCCZNAQZYZGSUZZAJZANALCZELMCAGALUGZZLACAGALUGZZLA HMCGALUCCERAVEZZGLUZZSKOJEKRAGGALUESZNUMYSDGVZGWZEJGLUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGUGU
w jb j r by ubsins in a eeb i poas 9// 5 zradosko ja de value i power a value valu
jpbirter kortasigaa nasikeoa in 5 gzwwarizhkiate/misuruscu 4 kubigen Dhittykizz jstrankoto in 5 jibirnet szczi w 2 skastraste ugruhyu/ osodagmi Larrni kriter
6Brob56Agmbngubev159+myxbwmuQM/eyskmpeS25/OccURhbu2sTIGousTXwvJNHPA6n.+81736 JwqT0gIBPYK61hLj2J5/8x8gTVK01qIFhU10W12BXjmzbwc1onjwg66Xan+UI/OpbzE0jtCkggGCF
2004/CG0VC-SCAKWEINGLVI2600/WKCHSAWKS/SCZEJINIZECT/IIIIINDIZEZ/UKCHSQIJOSOLIS901_GLDY9VKKDSGDC/UVSIISIH+0IKCU06601VL11/CSZKAC/U4FIX[T]C52HaWG5UDIINOUH/SDZZC Nalizihai Ivaanayawiki yi i / i / i / i / i / i / i / i / i /
ANO/FIDIBLEARAN JILIDUU AAAAN YY MADUU TUU TUU TUU TUU AAAN YY AAAN YY AAAN Y AAAN Y Y AUGU AAAN Y Y AUGU AAAN Y NUU TUU TI IN HAA Y AAAN Y Y AAAN Y Y AAAN Y Y AAAN Y Y Y Y
▼ <md:nameidformat></md:nameidformat>
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
<md:assertionconsumerservice binding="urn:oasis:names:tc:SAML:2.0;bindings:HTTP-POST" index="1" location='https://www-us.api.concursolutions.com/sso/saml2/V1/acs/"'></md:assertionconsumerservice>
<pre>\[md:Organization> </pre>
<pre>smd:OrganizationName xml:lang="en_US">www.concur.com</pre> /md:OrganizationName>

Step 2: Provide the EntityID and ACS Endpoint

Provide the EntityID and ACS Endpoint to the custom app/connector in your IdP.

IMPORTANT: If your IdP is *not* listed in the table in the *Identity Provider (IdP)-Specific Process* section in this guide, do not use your IdP's gallery/pre-configured SAP Concur app/connector; that is a legacy app/connector with legacy endpoints and will not work with the new SAP Concur SSO service. Instead, use a *custom* app or connector from your IdP. Return to the *Identity Provider (IdP)-Specific Process* section frequently to see if your IdP has been added to the table.

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.

GENERAL	
Single sign on URL 👔	https://us.api.concursolutions.com/sso/saml2/V1/acs/ Image: Concursolution URL and Destination URL Allow this app to request other SSO URLs
Audience URI (SP Entity ID) 🕜	https://uslapi.concursolutions.com

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

	Application details				
	RelayState				
	Audience				
	https://us.api.concursolutions.com				
(Recipient				
	https://us.api.concursolutions.com/sso/saml2/V1/acs/				
	ACS (Consumer) URL Validator*				
	https://us.api.concursolutions.com/sso/saml2/V1/acs/				
	(i) *Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest				
	ACS (Consumer) URL*				
	https://us.api.concursolutions.com/sso/saml2/V1/acs/				
	(j) *Required				

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:nameidformat: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*.

GENERAL		
Single sign on URL 👔	https://emea.api.concursolutions.com/sso/sa	aml2/V1/acs/
	Use this for Recipient URL and Destinatio	on URL
	Allow this app to request other SSO URLs	S
Audience URI (SP Entity ID) 👔	https://emea.api.concursolutions.com	
Default RelayState 🕐		
	If no value is set, a blank RelayState is sent	_
Name ID format 👔	EmailAddress v	
Application username 👔	Email 🔺	
Undate application username on	Okta username	
opute application aschlame on	Okta username prefix	
	Email	Show Advanced Setting
	Email prefix	
	Custom	
ATTRIBUTE STATEMENTS (OPTIONAL)	(None)	LEARN MORE

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

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.



Setting	S Edit
SIGN C	IN METHODS
The sig on meth	n-on method determines how a user signs into and manages their credentials for an application. Some sign- nods require additional configuration in the 3rd party application.
Applica	tion username is determined by the user profile mapping. Configure profile mapping
• SA	ML 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 s 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.

IdP Metadata	
Add Edit	
	No IdP Metadata Add one or more IdPs' metadata



SAP Concur C Reporting - Ap	p Center Administration -	Deefle v
	Add IdP Metadata ×	Pronie * 🛎
Company Admin > Authentication Admin > N	Custom IdP Name *	
Manage Single Sign-	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional V	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and	Upload your IdP's metatada Upload XML File	
https://us2.api.concursolutions.co	Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata Download	Cancel Add Metadata	
IdP Metadata		
Add Edit Delete		
Entity ID	Name Hidden Active From Expirat	ion Date 🚔 Logout URL

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*.

SAP Concur C		⊕ English (US) ▼
Ser. 1	< Sign In	
and the second	username@domain.com	
	Sign in with [custom IdP Name]	
	Sign in with your password	
	Not a Concur user yet? Try Test Drive	
	the second way when the standard and	

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.

SAP Concur	App Center Administration -	neip -
	Add IdP Metadata ×	Profile 👻
Company Admin > Authentication Admin >	Custom IdP Name *	
Manage Single Sigr	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional 🗸	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata a Copy SAP Concur metadata	Upload your IdP's metatada Upload XML File	
OR	Cancel Add Metadata	
Download		
IdP Metadata		
Add Edit De		
Entity ID	Name Hidden Active From Expiration Date 🛎	Logout URL

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.

SAP Concur C Reporting - Apr	p Center Administration -	Profile -
	Add IdP Metadata	
Company Admin > Authentication Admin > M	Custom IdP Name *	
Manage Single Sign-	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional ~	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and	Upload your IdP's metatada	
Copy SAP Concur metadata	Upload XML File	
https://us2.api.concursolutions.co	Hide this SSO option from users signing in to Concur on web or mobile	
OR		
Download SAP Concur metadata Download	Cancel Add Metadata	
IdP Metadata		
Add Edit Delete		
Entity ID	Name Hidden Active From Expiration Date 🛎	Logout URL

7. Click Add Metadata.

	oncur C	Reporting -	App Center	Administration •				Profile 🔹
ompan	y Admin > Authe	entication Admin	> Manage Single	Sign-On				
Mar	hage Sir	ngle Sig	n-On foi	⁻ Canonical Trav	el Test Co	ompany		
Enable	e SSO							
SSO Se	tting: SSO Opt	ional 🗸						
Get SA Copy or	AP Concur N download SAP C	letadata Concur metadata	and add it to your	Identity Provider (IdP).				
Copy SA	P Concur metad	ata						
-			Copy U	٦L				
DR								
ownloa Downlo	ad SAP Concur m Dad	letadata						
dP M	etadata							
A	.dd F							
	Entity ID			Name	Hidden	Active From	Expiration Date =	Logout URL
				SAML Monitor		09/30/2016	09/30/2026	
	1000							
				muttals okta		02/27/2018	02/27/2028	

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.

Erro	×
•	Sorry, we were unable to save your IdP metadata. Please try again. If the issue persists, please contact Concur Support with correlation_id (ff07d251-e634-444f-92fd-33c11c4e40b3) or additional help.
	ок

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.

Work	+
	SAP Concur C
	SAML2 CT&E Canary

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

For Azure AD, use one of the following:

• Properties > User access URL

concurtest - P Enterprise Application	roperties		
B Overview	*	🕞 Save 🗶 Discard 볩 D	elete
Getting started	an	Enabled for users to sign-in?	Yes No
Manage		Name	concurtest
Properties		Homepage URL	
ج ^ع Users and grou	ps		
 Single sign-on Provisioning 		Logo	<u> </u>
Application pro	ху		Select a file
Security		User access URL 🜒	https://myapps.microsoft.com/signin/concurt
,		Application ID a	77350-76 0-8- 4001 0-74 4462-52-73-

– or –

• Test single sign-on with Concur Travel and Expense

	est single si	gn-on with Concur Haver and Expense
Te	est to see if s	ingle sign-on is working. Users will need to be added to Users and groups before they can sign in.
	Test	

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.
- Look for the value in the <saml2:NameID> field. For example: <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameidformat: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**.

Enable S	SO	
SSO Setting:	SSO Optional 🔻	
Get SAP	SSO Optional Users may sign in with a password or with SSO.	
Copy or down	SSO Required Users must sign in using SSO.	ntity Provider (IdP).
Copy SAP C	birour o motavata	J

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**.

			Help •
SAP Concur ⓒ	Reporting + A	Edit IdP Configuration	Profile 🔻 💄
Company Admin > Auth	entication Admin > M	Custom IdP Name	
		Concur Okta	
Manage Si	ngle Sign-	The IdP Name you enter here is what users will see.	
		Logout URL	
Enable SSO			
SSO Setting: SSO Opt	tional 🗸	Users will be redirected to the Logout URL when they Sign Out.	
		IdP Metadata	
Get SAP Concur M	Metadata	xml version="1.0" encoding="UTF-8"? <md< td=""><td></td></md<>	
Copy or download SAP C	Concur metadata and	IdP metadata is not editable. To make changes to the metadata, it is best practice to add a new IdP configuration, test it to make sure it functions properly, and then delete the old IdP configuration.	
Man link as on		Hide this SSO option from users signing in to Concur on web or mobile	
OR			
Download SAP Concur n	netadata	Cancel Save Changes	
Download			
IdP Metadata			
Add	Edit Deleta	View Metadata	
Entity ID		Name Hidden Active From Expiration Date 🛎	Logout URL

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.

,	Add Edit						
	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	

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 D	etails
06/08/2022	Edit		Concur Okta		~ (View
06/08/2022	Edit	14 - 14 - 14 - 17 - 18 May - 18 - 18 - 18 - 18 - 18 - 18 - 18 - 1	ray test 2		~ [View
06/08/2022	Edit		ray test 2		(View
06/08/2022	Edit		ray test 2		~ (View
06/08/2022	Edit		ray test 2		(View
06/08/2022	Add		ray test 2		~ (View
06/07/2022	Delete	-	ray test 2		(View
06/07/2022	Edit		ray test 2		(View
06/07/2022	Add		ray test 2		~ (View
06/07/2022	Delete		ray test 2		~ (View
06/07/2022	Edit		ray test 2		~ (View
06/07/2022	Edit	-	ray test 2		ſ	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 Cl	hanges				
	Date	Change	Entity ID	Name	.ogout URL Hide	den Details
_	06/08/2022	Edit		Concur Okta	~	View
	06/08/2022	Edit		ray test 2	~	View
	06/08/2022	Edit		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.

Date Changed	05/24/2022
Change	Delete
Company Change By	
Entity ID	
Name	
Logout URL Hidden	https://logout.com
Metadata xml version='<br <md:entitydesc: <md:idpssodes <md:keydesc< th=""><th>'1.0" encoding="UTF-8"?> riptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn scriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn sriptor use="signing"></th></md:keydesc<></md:idpssodes </md:entitydesc: 	'1.0" encoding="UTF-8"?> riptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn scriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn sriptor use="signing">
Metadata xml version='<br <md:entitydesc: <md:idpssodesc <md:keydesc <ds:keyin <ds:keyin <ds:x50< td=""><td>'1.0" encoding="UTF-8"?> Tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn scriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn scriptor use="signing"> nfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 19Data></td></ds:x50<></ds:keyin </ds:keyin </md:keydesc </md:idpssodesc </md:entitydesc: 	'1.0" encoding="UTF-8"?> Tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn scriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn scriptor use="signing"> nfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 19Data>
Metadata xml version='<br <md:entitydesc: <md:idpssodes <md:keydesc <ds:keyir <ds:keyir <ds:x50 <ds:x50< td=""><td>1.0" encoding="UTF-8"?> Tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn Scriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> 16 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 19Data> 19Data> 1509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw</td></ds:x50<></ds:x50 </ds:keyir </ds:keyir </md:keydesc </md:idpssodes </md:entitydesc: 	1.0" encoding="UTF-8"?> Tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn Scriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> 16 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 19Data> 19Data> 1509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw
Metadata xml version='<br <md:entitydesc <md:idpssodes <md:keydesc <ds:keyin <ds:keyin <ds:x5(<ds:1) All</ds:1) </ds:x5(</ds:keyin </ds:keyin </md:keydesc </md:idpssodes </md:entitydesc 	<pre>'1.0" encoding="UTF-8"?> tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn scriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> ifo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ifo xmlns:ds="http://wwwwwwa.org/2000/09/xmldsig#"> ifo xmlns:ds="http://wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww</pre>
Metadata xml version='<br <md:entitydesc <md:idpssodes <md:keydesc <ds:keyir <ds:x5(<ds:x Alt MB1 Zmm</ds:x </ds:x5(</ds:keyir </md:keydesc </md:idpssodes </md:entitydesc 	<pre>'1.0" encoding="UTF-8"?> tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn triptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> ifo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ifo xmlns:ds="http://wwwww#"/wwwww#"/wwww#"/wwww#"/wwww#"/www#"</pre>
Metadata xml version='<br <md:entitydesc: <md:idpssodesc <md:keydesc <ds:keyinc <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:keyinc </md:keydesc </md:idpssodesc </md:entitydesc: 	<pre>'1.0" encoding="UTF-8"?> tiptor entityID="http://www.okta.com/exk5537fynNWEDL222p7" xmlns:md="urn triptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> ifo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ifo xmlns:ds=wifito xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ifo xmlns:ds=wifito xmlns:ds=wif</pre>
Metadata xml version='<br <md:entitydesc: <md:idpssodesc <md:keydesc <ds:keyinc <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:keyinc </md:keydesc </md:idpssodesc </md:entitydesc: 	<pre>'1.0" encoding="UTF-8"?> tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn triptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> ifo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ifo xmlns:ds="http://wwwwwwwwwwawwwwwwwwwwwwwwwwwwwwwwwww</pre>
Metadata xml version='<br <md:entitydesc: <md:idpssodes <md:keydesc <ds:keyin <ds:keyin <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:keyin </ds:keyin </md:keydesc </md:idpssodes </md:entitydesc: 	<pre>'1.0" encoding="UTF-8"?> tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn triptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> ifo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> i9Data> t509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw JECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YT iGA1UECwwLU1NPUHJvdmlkZXIxEDAOBgNVBAMMB211dHRhbHMxHDAaBgkqhkiG9w0BCQEWDW Ab2t0YS5jb20wHhcNMTgwMjI3MTgzNDIyWhcNMjgwMjI3MTgzNTIyWjCBjzELMAkGA1UEBh txEzARBgNVBAgMCKNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY21zY28xDTALBgNVBA DrdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRAwDgYDVQQDDAtdXR0YwxzMRwwGgYJKcZIhv tBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgfnM0Q</pre>
Metadata xml version='<br <md:entitydesc: <md:idpssodes <ds:keydesc <ds:keyin <ds:keyin <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:x50 <ds:y0 Alt MB1 Zm2 VVN BE2 AQ1 yhI</ds:y0 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:x50 </ds:keyin </ds:keyin </ds:keydesc </md:idpssodes </md:entitydesc: 	<pre>'1.0" encoding="UTF-8"?> tiptor entityID="http://www.okta.com/exk5537fynNWEDLz22p7" xmlns:md="urn triptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn triptor use="signing"> ifo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> iPoData> t509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw JECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YT iGA1UECwwLU1NPUHJvdmlkZXIxEDAOBgNVBAMMB211dHRhbHMxHDAaBgkqhkiG9w0BCQEWDW iAb2t0YS5jb20wHhcNMTgwMjI3MTgzNDIyWhcNMjgwMjI3MTgzNTIyWjCBjzELMAkGA1UEBw txEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY21zY28xDTALEgNVBA DrdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRAwDgYDVQQDDAtdXR0YwxzMRwwGgYJKoZIhv tBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgfnM0Q 44v+0rwRqN8oSDs2bKa2wo2eQKInxi7xX7Yh4Q0E3Y630Pr4uXdL5boUynIsuyVZ4ahoXYy5</pre>

Example View Previous Changes Page for Deleted Configuration

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**.

Conf	ïrm Revert	×
Â	Are you sure you want to revert this dele configuration active?	ation, and make this
	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

Date Changed	06/08/2022	
Change	Edit	
Company		
Change By		
Entity ID		
Name	Concur Okta	
Logout URL		
Hidden	✓	
Previous Values		
Entity ID		
Name	Concur Okta	
Logout URL		
Hidden		
Metadata		
xml version='</td <td>'1.0" encoding="UTF-8"?></td> <td></td>	'1.0" encoding="UTF-8"?>	
<md:entitydesci< td=""><td>riptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="u:</td><td>rn</td></md:entitydesci<>	riptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="u:	rn
<md:idpssodes< td=""><td>criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="u</td><td>rn</td></md:idpssodes<>	criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="u	rn
<md:keydesc< td=""><td>riptor use="signing"></td><td></td></md:keydesc<>	riptor use="signing">	
<ds:keyir< td=""><td>1fo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></td><td></td></ds:keyir<>	1fo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">	
<ds:x50< td=""><td>)9Data></td><td></td></ds:x50<>)9Data>	
<ds:></ds:>	<pre>(509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQ</pre>	SW
A11	JECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECqwET2t0	YT:

Example View Previous Changes Page for Edited Configuration

ADDED CONFIGURATION DETAILS

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

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

Example View Previous Changes Page for Added Configuration

Date Changed	06/07/2022
Change	Add
Company	
Change By	
Entity ID	
Name	
Logout URL	
Hidden Metadata xml version="<br <md:entitydescr <md:idpssodes <md:keydesc< th=""><th><pre> 1.0" encoding="UTF-8"?> iptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="urn criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn riptor use="signing"> </pre></th></md:keydesc<></md:idpssodes </md:entitydescr 	<pre> 1.0" encoding="UTF-8"?> iptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="urn criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn riptor use="signing"> </pre>
Hidden Metadata xml version="<br <md:entitydescr <md:idpssodes <md:keydesc <ds:keyin <ds:x50< td=""><td><pre> .0" encoding="UTF-8"?> iptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="urn criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn riptor use="signing"> fo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 9Data></pre></td></ds:x50<></ds:keyin </md:keydesc </md:idpssodes </md:entitydescr 	<pre> .0" encoding="UTF-8"?> iptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="urn criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn riptor use="signing"> fo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 9Data></pre>
Hidden Metadata xml version="<br <md:entitydescr <md:idpssodes <md:keydesc <ds:keyin <ds:x50 <ds:x< td=""><td><pre> .0" encoding="UTF-8"?> iptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="urn criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn riptor use="signing"> fo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 9Data> 509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw </pre></td></ds:x<></ds:x50 </ds:keyin </md:keydesc </md:idpssodes </md:entitydescr 	<pre> .0" encoding="UTF-8"?> iptor entityID="http://www.okta.com/exk8bjsi41SiSaXyM2p7" xmlns:md="urn criptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn riptor use="signing"> fo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> 9Data> 509Certificate>MIIDnjCCAoagAwIBAgIGAWHYjDLXMA0GCSqGSIb3DQEBCwUAMIGPMQsw </pre>
Hidden Metadata <rxml <br="" version="
<md:EntityDescr
<md:IDPSSODes
<md:KeyDesc
<ds:KeyIn
<ds:X50
<ds:X
Alture
NDT</td><td><pre></td></tr><tr><td>Hidden
Metadata
<?xml version="><md:entitydescr <md:idpssodes <md:keydesc <ds:keyin <ds:x50 <ds:x alu<br="">MBI zm9</ds:x></ds:x50 </ds:keyin </md:keydesc </md:idpssodes </md:entitydescr </rxml>	<pre></pre>
Hidden Metadata xml version="<br <md:entitydescr <md:idpssodes <md:keydesc <ds:keyin <ds:keyin <ds:x50 <ds:x50 <ds:x AlU MBI Zm9 VVM</ds:x </ds:x50 </ds:x50 </ds:keyin </ds:keyin </md:keydesc </md:idpssodes </md:entitydescr 	<pre></pre>
Hidden Metadata xml version="<br <md:entitydescr <md:idpssodes <md:keydesc <ds:keyin <ds:x50 <ds:x50 <ds:x50 <ds:x40 MBI Zm9 VVM BE9</ds:x40 </ds:x50 </ds:x50 </ds:x50 </ds:keyin </md:keydesc </md:idpssodes </md:entitydescr 	<pre></pre>
Hidden Metadata xml version="<br <md:entitydescr <md:idpssodes <md:keydesc <ds:keyin <ds:keyin <ds:x50 <ds:x AlU MBI Zm9 VVM BE9 AQk</ds:x </ds:x50 </ds:keyin </ds:keyin </md:keydesc </md:idpssodes </md:entitydescr 	<pre></pre>
Hidden Metadata xml version="<br <md:entitydescr <md:idpssodes <md:keydesc <ds:keyin <ds:keyin <ds:x50 <ds:x AlU MBI Zm9 VVM BE9 AQk yhB</ds:x </ds:x50 </ds:keyin </ds:keyin </md:keydesc </md:idpssodes </md:entitydescr 	<pre></pre>

Configure an SSO App/Connector with Encryption (Optional)

Complete all steps described in the *Configure an SSO App/Connector* <u>Without</u> *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 a encryption.crt file.

- To obtain and save the encryption key:
 - 1. 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/

- China: https://www-cn.api.concurcdc.cn/sso/saml2/V1/sp/metadata
- 2. Find the encryption key as shown in the following example:

* <md:keydescriptor tencryption="" use=""></md:keydescriptor>
<pre>w<ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></ds:keyinfo></pre>
▼ <ds:x509data></ds:x509data>
▼ <ds:x509certificate></ds:x509certificate>
MIIGÉTCCBGWgAwIBAgIJAMVoHDFvVQXSMA0GCSqGSIb3DQEBCwUAMIGFMQswCQYDVQQGEwJVU2ET MBEGA1UECBMKV2F2aGluZ3RvbjERMA8GA1UEBxMIQmVsbGV2dWUxEjAQBgNVBAoTCVNBUCBDb251
cjEWHBQGA1UECXMNQ29yZSBTZXJZaWN1czEiMCAGA1UEAXMZY29yZS1zYW1sLXByb2QuY29uY3Vy LmNvbTAeFw0xODA2MjYyHDIxMjNaFw0yHDA2MjUyHDIxMjNaMIGFMQswCQYDVQQGEwJVUzETMBEG
A1UECBMKV2FzaG1uZ3RvbjERMA8GA1UEBxMIQmVsbGV2dWUxEjAQBgNVBAoTCVNBUCBDb251cjEW MBQGA1UECxMNQ29yZSBTZXJZaWN1czEiMCAGA1UEAxMZY29yZS1zYW1sLXByb2QuY29uY3VyLmNv
bTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALvWJvcbuskNPDLQOk8Df0pGmKAWT2sI 0Ug9HxyWmSoXR5ltHvHZ8nZ0eQvMzgXJ02dT70+7SuIg6or3IZG2jCi30tjlolIPB6pdbQtHe+em
wjbjTpyJDS1H57NaeebiYpUas9H/3PAdo3K8Jdt4zbwjzbg7vvL0SIDpW428sUsnJgTc75asjreA hZikW0tohnKfRRp606CXJgissx3KdNpGD7bu1NKtfmb2NGve7Igt/qZt63ZEEjLn01TgQAM1cZaL
jp61fC87k6T8a3gaa2ndSIKeoa7lb5g2WVWZF12nkLd+e/m5Lr0SCeJ4X0bGeNDnH+MyAT8xKZL2 jSGraNko46ibL36100AP8/LfDprmP+0SczIw42sxHSGf8E0grOHyu/oSodWgMuiLdrFhN1xYRT8W
6BroD56AgmbhQ0Dev159+myxbWm0QM7eyskmpeS25/OccURhbu2sTIGousTXwvjNHPA6hJ+8iTJ6 JWqTOg1BPYk6iHLjYj5/8x8gTVRo1giFnUl0Wl2BXjmzbWclonjwQ66XaN+017OpbZEUjtGRgQCr
i/51ekdWaxbib90pVnvv9Ht9oHk6tMgUHasZv6WLeZJKAB9LngPdfUjwBB5p4eLsbqP27oi6gpp1 2YyW3F0tkf/F0nTjZ4UZFWj2vt4JnDdTQ1nyR1D0xJJdAgMBAAGjge0wgeowHQYDVR00BBYEFNB9
GvAfl2g8B7bW2piKwaCL2+80MIG6BgNVHSMEgbIwga+AFNB9GvAfl2g8B7bW2piKwaCL2+80oYGL pIGIMIGFMQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2F2aG1uZ3RvbjERMA8GA1UEBXMIQmVsbGV2
dWUxEjAQBgNVBAoTCVNBUCBDb251cjEWMBQGA1UECxMNQ29yZSBTZXJ2aWN1czEiMCAGA1UEAxMZ Y29yZS1zYW1sLXByb2QuY29uY3VyLmNvbYIJAMVoHDFvVQXSMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggIBAEf+NDdxUs18FUbvZ6+3cGXR10rhnQAAe64tkhY80WM0JtLf4E1S14EI45M1 nz6a8RgsE08FzDjHjFmhFGIkAXYyg401pQnE8pE3ICzikI3pos9JU6Vw9o6206m7Zqb32FnnFTy8
z6oqVcgoyC3CZk0wYmTGiviz8d0VvRtH3XvR57o22bhX2ztyhm4bHMb2ezF0RH9kpi03PoLu39U1 G1D+9Vkkb3gEQcuVshSn48nR20066cYQ1T+czN2N2C+u4FIRj+t3PLwe5tUDYm8u4mC7bPTZDP2C
AwU7P41JYsrpzxzvNjlKli/iICJa3kASKQ93wKBBi64D7CUITpjzQ+k3eVUw4T4QZJajp8DdaHGI of+jPQDedqrrWb3DrtX/7zYyuy+kJHog60AtetT3718pXocITn0NcH4fWOhivfcyeMPtXqXCbJVW
puVzrBpzLp1bkb538hKeMg3ytXkg0gTMg8SDsqkf67dmRoQM9yF8tKmWHZs7fRrCKZxv9KY7AwuV MzqBsJhYVVg0cDspmbZkUoCNrA/V5Fg06osEf1X8IyWN9/7uLI7zKAB2VQMaqIKA8avSUfx0ItOb
bpDc71fXQz305bvWH/Om4utDLJNbyR1ffLNSjOA4luvJNmMd/Bg5ughX7DHGbOuF5hOarcRz1hRa_GNLnMSbldjwxIN8X

3. Copy the encryption certificate into a plain text file.

NOTE: Do not use a rich text editor like Word.

4. Paste between two BEGIN/END CERTIFICATE rows as shown below:

```
-----BEGIN CERTIFICATE-----
< your copied cert here >
-----END CERTIFICATE-----
```

5. Save as encryption.crt.



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.

Assertion Encryption	Encrypted	•	
Encryption Algorithm	AES256-CBC	v	
Key Transport Algorithm 👔	RSA-OAEP	•	
Encryption Certificate 👔			Browse files

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

Concur Travel and Expens	e - Token encryption (Preview) $ imes$
《	↑ Import Certificate
	Import Certificate
Manage	Upload a certificate with a file name extension .cer
Properties	Salact a file
🔐 Owners	
۶ ^۹ Users and groups	Add Cancel
Single sign-on	
Provisioning	
Self-service	
Security	
Conditional Access	
Permissions	
Token encryption (Preview)	
Activity	

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**.

Access To Concur	
User Accounts Set up and manage your Concur users and their permissions.	
Show 1 Advanced Setting	

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



For the SAP Concur **Professional** edition:

1. <u>Go to Administration > Company > Authentication Admin</u>.

	Administra	ition -
Company Admin	Company	►
Tools	Request	•
Web Services	Travel Admin	
Report Admin	Expense	•
Authentication Admin	Invoice	
C)		

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

Company Admin > Authentication Admin

Authentication Administration

Manage Single Sign-On Manage Single Sign-On for SAP Concur products

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

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.

Select Data Source	
Steps • Welcome • Select Data Source • Choose Access Control Policy • Ready to Add Trust • Finish	Select an option that this wizard will use to obtain data about this relying party:

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

\$	Add Relying Party Trust Wizard
Specify Display Nan	ne
Steps	Enter the display name and any optional notes for this relying party.
Welcome	Display name:
Select Data Source	
Specify Display Name	Notes:
Choose Profile	
Configure Certificate	
Configure URL	
Configure Identifiers	
Configure Multi-factor Authentication Now?	
Choose Issuance Authorization Rules	
Ready to Add Trust	
Finish	
	\frown
	< Previous (Next >) Cancel

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

\$	Add Relying Party Trust Wizard	x		
Choose Profile				
Steps	This wizard uses configuration profiles to aid in creating the relving party trust. Choose the appropriate			
Welcome	configuration profile for this relying party trust.			
Select Data Source	 AD FS profile 			
Specify Display Name	This profile supports relying parties that are interoperable with new AD FS features, such as			
Choose Profile	security token encryption and the SAML 2.0 protocol.			
Configure Certificate	○ AD FS 1.0 and 1.1 profile			
Configure URL	This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.			
 Configure Identifiers 				
Configure Multi-factor Authentication Now?				
 Choose Issuance Authorization Rules 				
Ready to Add Trust				
Finish				
	< Previous Next > Cancel			

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**.

Ŵ	Add Relying Party Trust Wizard
Configure Certificate	
Configure Certificate Steps Velcome Select Data Source Specify Display Name Choose Profile Configure URL Configure URL Configure Identifiers Configure Multi-Actor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to it. To specify the certificate, click Browse Issuer: Subject: Effective date: Expiration date: View Browse Remove
	< Previous Next > Cancel

- 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): <u>https://www-us.api.concursolutions.com/sso/saml2/V1/acs/</u>
 - EMEA: <u>https://www-emea.api.concursolutions.com/sso/saml2/V1/acs/</u>
 - China: <u>https://www-cn.api.concursolutions.com/sso/saml2/V1/acs/</u>



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

\$ 1	Add Relying Party Trust Wizard
Configure Identifiers	
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying
Welcome	party trust.
Select Data Source	Relying party trust identifier:
Specify Display Name	Add
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust
Configure Certificate	Relying party trust identifiers:
Configure URL	https:/Remove
Configure Identifiers	
Configure Multi-factor Authentication Now?	
Choose Issuance Authorization Rules	
Ready to Add Trust	
Finish	
	< Previous Next > Cancel

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.

\$	Add Relying Party Trust Wizard				
Steps Welcome Select Data Source	Configure multifactor authentication settings for this relying p there is a match for any of the specified requirements.	party trust. Multi-factor authentication is required if			
Specify Display Name	Multi-factor Authentication	Global Settings			
Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules	Requirements Users/Groups Not configure Device Not configure Location Not configure	ed ed			
 Ready to Add Trust Finish 	 I do not want to configure multifactor authentication setti Configure multifactor authentication settings for this relyin You can also configure multi-factor authentication settings Authentication Policies node. For more information, see Q 	ings for this relying party trust at this time. ng party trust. s for this relying party trust by navigating to the configuring Authentication Policies.			
		< Previous Next > Cancel			

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

\$ 1	Add Relying Party Trust Wizard
Choose Issuance A	uthorization Rules
Choose Issuance At Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi Flactor Authonization Rules	uthorization Rules Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules. Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
 Ready to Add Trust Finish 	< Previous Next > Cancel

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**.

\$	ŀ	Add Relyin	g Party T	rust V	Vizard			×
Ready to Add Trust								
Steps Welcome Select Data Source Specify Display Name	The relying party relying party trust Monitoring Id Specify the mo	trust has been to the AD FS entifiers Encontoring setting	n configured. configuration ryption Sign gs for this rely	Review datab	w the following setti ase. Accepted Claims ty trust.	ngs, and then o	click Next to	add the
Organization Endpoints Prov Monitoring Identifiers Encopy Specify the signature verification cert party. Subject Issuer CN-core-sami CN-core-s	y Endpoints Notes ion Signature Lock Ricates for requests from th Effective Date E 23/04/2020 23:	Advanced cepted Claims his relying Expiration De 122/04/2025	relying part	ta data	a was last checked eration metadata or	on:		
< Hi Add View O	Remove) Čsply			< Previo	ous Nei	d >	Cancel

12. 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**.

\$	Add Relying Party Trust Wizard
Finish	
Steps Velcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in. ✓ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
	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.

Manage Single Sign-On for tangochris
Enable SSO
SSO Setting: SSO Optional
Get SAP Concur Metadata Copy or download SAP Concur metadata and add it to your Identity Provider (IdP).
Copy SAP Concur metadata
https://us.api.concursolutions.com/ssc Copy URL
OR
Download SAP Concur metadata Download
IdP Metadata
Add Edit Delete View Metadata
No IdP Metadata Add one or more IdPs' metadata

The Add IdP Metadata window appears.

SAP Concur C Reporting *	Add IdP Metadata ×	Profile 👻 💄
Company Admin > Authentication Admin > N	Custom IdP Name *	
Manage Single Sign-	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional V	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and	Upload your IdP's metatada	
Copy SAP Concur metadata	Upload XML File	
https://us2.api.concursolutions.co	Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata	Cancel Add Metadata	
Download		
IdP Metadata		
Add Edit Delot		
Entity ID	Name Hidden Active From Expiration Date 🛎	Logout URL

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

SAP Concur C. Reporting -	App Center Administration -	Help •
	Add IdP Metadata	Profile 👻
Company Admin > Authentication Admin > 1	Custom IdP Name *	
Manage Single Sign	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional ~	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and	Upload your IdP's metatada	
Copy SAP Concur metadata	Opload XML File	
https://us2.api.concursolutions.co	Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata	Cancel Add Metadata	
Download		
IdP Metadata		
Add Edit Dele		
Entity ID	Name Hidden Active From Expiration Date 🏯	Logout URL

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.

SAP Concur C Reporting App	Add IdP Metadata ×	Profile 👻 💄
Company Admin > Authentication Admin > M	Custom IdP Name *	
Manage Single Sign-	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional V	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and	Upload your IdP's metatada	
Copy SAP Concur metadata		
https://us2.api.concursolutions.co	Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata	Cancel Add Metadata	
IdP Metadata		
Add Edit Delete		
Entity ID	Name Hidden Active From Expiration Date	🚊 Logout URL

5. Click Add Metadata.

SAP Concur C Reporting +	Add IdP Metadata	Profile 🝷 💄
Company Admin > Authentication Admin > M	Custom IdP Name *	
Manage Single Sign-	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional ~	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and Copy SAP Concur metadata	Upload your IdP's metatada Upload XML File	
https://us2.api.concursolutions.co	Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata	Cancel Add Metadata	
Download		
IdP Metadata		
Add Edit Delete	View Metadata	
Entity ID	Name Hidden Active From Expiration Date 🏯	Logout URL

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

 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.

0		
Username	e, email address, or SSO code	
testacc	count@test.com	
	Next	
Remer	mber me	
Forgot	usemame?	
	Not a Concur user vet? Trv Test Drive	
< Sig	n In	
< Sig	n In	
< Sig	n In unt@test.com	
< Sig	Sign in with MyCompany SSO	
< Sig	Sign in with MyCompany SSO	

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.

Manag	Manage Single Sign-On					
Enable SS	60					
SSO Setting:	SSO Optional					
Get SAP	SSO Optional Users may sign in with a password or with SSO.					
Copy or dowr	SSO Required Users must sign in using SSO.	ty Provider (IdP).				
Copy SAP Co						

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.

	Administration -
Expense Settings	_Ռո
Company	
Expense User Exp	perience 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. <u>Go to Administration > Company > Authentication Admin</u>.

	Administra	ation -
Company Admin	Company	•
Tools	Request	•
Web Services	Travel Admin	
Report Admin	Expense	•
Authentication Admin	Invoice	
6		.1

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

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 <u>Microsoft Azure AD Guide</u> as an additional reference for this section.

Step 1: Create Gallery Application

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

Enterprise applica Default Directory - Azure Active Dire	tions All applicatio	ns …			
	≪ + New application ≣≣	Columns 🛛 🔂 Preview feature	es 🛛 💙 Got feedback?		
Overview	🕜 Try out the new Enterpris	e Apps search preview! Click to enable	a the preview. \rightarrow		
Uverview					
X Diagnose and solve problems	Application type	Applications status	Application visibili	ity	
Manage	Enterprise Applications	Any	Any	~	Apply Reset
All applications	P First 50 shown, to search a	Il of your applications, enter a disp	lay name or the application ID	D.	
Application proxy	Name		Homepage U	JRL	
🛞 User settings	Azure				
	Office 265 Euchana	Online	1		1.7

- 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.

wse Azure AD Gallery (Preview)				
	Logo 🛈	Logo 🕕 Name * 🛈		
reate your own application 🕜 Request new gailety app 🗸 Got reconstruct		SAP Concur Travel and Expe	inse	
Click here to suitch back to the old app galley experience>	C	Publisher ③ SAP Concur	Provisioning ① Automatic provisioning is not supported	
Decorreg		Single Sign-On Mode ① SAML-based Sign-on Linked Sign-on	URL () https://www.concur.com	
Concer Triple		Read our step-by-step SAP C tutorial Concur simplifies travel, expe visibility and greater control.	oncur Travel and Expense integration	
C• Centrolan Darres Online by Concer Colors Servergine Inc. Centroland Constraints Centroland Cen	Þ			
	3			

- 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".

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).

nome > enterprise applications > B	owse Azur	e AD Gallery (Preview) > SAP Concur Travel an	a cipense 🤌		Basic SAML Configuration				
SAP Concur Travel an	d Expe	ense SAML-based Sign-on							
interprise Application	1 —				🚼 Save				
	[™]	Upload metadata file 🏷 Change single sign-on	mode 📕 Test this application 🛛 🛇 Got feedback?						
Overview				Identifier (Entity ID) * 💿					
Deployment Plan	Upi	oad metadata file.			The default identifier will be the audience of the SAML response for IDP-initiated SSO				
anage	Value	es for the fields below are provided by SAP Con-	cur Travel and Expense. You may either enter those va	lues manually, or up	2		Default		
Properties	Sele	ect a file	N		https://cn.api.concurede.en/saml2 China		0		
Owpers		Add Cancel	Le ²		https://emea.api.concursolutions.com/saml2 EMEA		0		
Roles and administrators (Dreview)		terentioner (entry set)	mgay/magneereereere		https://us.api.concursolutions.com/saml2 US		0		
notes and doministrators (renew)		Reply URL (Assertion Consumer Service URL)	https://www-us.api.concursolutions.com/sso/saml2/V1/i s/	IC .					
Users and groups		Sign on URL	Optional		Patterns: https://cn.ani.concurrdc.co/saml2_https://emea.ani.concursolutions.com/saml2				
Single sign-on		Relay State	Optional		https://us.api.concursolutions.com/saml2				
Provisioning									
Self-service	0				Reply URL (Assertion Consumer Service URL) * ①				
outh	-	User Attributes & Claims		6 Edit	The default reply URL will be the destination in the SAML response for IDP-initiated SSO				
curry		givenname	user.givenname				Default		
Conditional Access		sumame	user.sumame		Contraction of the second s		-	~	
Permissions		name	user.userprincipalname		https://www-us.api.concursolutions.com/sso/sami2/v1/acs/		0		
Token encryption		Unique User Identifier	user.userprincipalname		https://www-cn.api.concuredc.cn/sso/saml2/V1/acs/ China	~	0		
tivity					https://www-emea.api.concursolutions.com/sso/saml2/V1/acs/ EMEA	~	0	۵	
	3	SAML Signing Certificate		1.000	https://us.api.concursolutions.com/sso/sam12/V1/acs/ Delete		0		
Sign-ins				e sort					
Usage & insights (Preview)		Status	Active 9CE0376430CE0D7100D632968578251D1EC05C48		Dattarar http:///REGION/MAMEs and constantial store com/reg/ram/2/0/1/set/				
Audit land		Eurication	12/02/0035 45047 414		Participant in the second control of the second of solution (1550/341112/21/4C3/				

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.

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

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.

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

Manage claim				
☐ Save X Discard changes				
Name	nameidentifier			
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims			
∧ Choose name identifie	er format			
Email address				
Source *	Attribute Transformation			
Source attribute *	user.userprincipalname			
✓ Claim conditions				

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".

Status	Active
Гhumbprint	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

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**.

Home > Enterprise applications - All applications > Concur - Properties				
Concur - Properties Enterprise Application				
"	🔚 Save 🗙 Discard 📋 Delete			
Overview				
Deployment Plan	Enabled for users to sign-in? ((); Yes No			
X Diagnose and solve problems	Namo 🔿	Concur		
Manage	Name	concur		
Properties	Homepage URL 🕡			
A Owners				
Users and groups		C.		
Single sign-on	Logo 🗊			
Provisioning				
Application proxy				
 Self-service 	User access URL ①			
Security	- (
Conditional Access	Application ID 🕞	Contraction of the second s		
🔏 Permissions	·			
Token encryption (Preview)	Object ID 🕕			
Activity	Terms of Service Url (i)	Publisher did not provide this information		
Sign-ins	0			
🕍 Usage & insights (Preview)	Privacy Statement Url 🕡	Publisher did not provide this information		
Audit logs				
Provisioning logs (Preview)	Reply URL	https://www-us.api.concursolutions.com/s		
E Access reviews				
Troubleshooting + Support	User assignment required? 🕕	(Yes No		
😤 Virtual assistant (Preview)	Visible to users? ①	Yes No		
New support request	Ŭ			

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.

IdP Metadata	
Add Edit I	
	No IdP Metadata Add one or more IdPs' metadata



SAP Concur C	Reporting - Ar	p Center Administration *	Heip
	Toporning 7	Add IdP Metadata ×	Profile 👻 🖕
Company Admin > Auth	nentication Admin > M	Custom IdP Name *	
Manage Si	ngle Sign-	The IdP Name you enter here is what users will see.	
Enable SSO		Logout URL	
SSO Setting: SSO Op	itional 🗸	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Copy or download SAP	Metadata Concur metadata and	Upload your IdP's metatada Upload XML File	
Copy SAP Concur meta https://us2.api.cor	data	Hide this SSQ option from users signing in to Concur on web or mobile	
OR Download SAP Concur Download	metadata	Cancel Add Metadata	
IdP Metadata			
Add			
Entity ID		Name Hidden Active From Expiration Date #	Logout URL

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: <u>https://www.concursolutions.com/nui/signin</u>), 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.

SAP Concur C Reporting *	App Center Administration +	
	Add IdP Metadata ×	Profile * 🛎
Company Admin > Authentication Admin >	Custom IdP Name *	
Manage Single Sign	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional V	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and	Upload your IdP's metatada Upload XML File	
https://us2.api.concursolutions.co	Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata Download	Cancel Add Metadata	
IdP Metadata		
Add Edit Dele		
Entity ID	Name Hidden Active From Expiration Date 🏝	Logout URL

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.

SAP Concur C Reporting *	App Center Administration +	Profile 👻 👤
	Add IdP Metadata ×	
Company Admin > Authentication Admin	S M Custom IdP Name *	
Manage Single Sig	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional ~	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata	and Upload your IdP's metatada	
Copy SAP Concur metadata	Upload XML File	
https://us2.api.concursolutions.co	D Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata	Cancel Add Metadata	
Download		
IdP Metadata		
Add Edit D		
Entity ID	Name Hidden Active From Expiration Date 🏯	Logout URL

7. Click Add Metadata.

SAP Concur C Reporting - A	Add IdP Metadata	Profile 🝷 💄
Company Admin > Authentication Admin > M	Custom IdP Name *	
Manage Single Sign-	The IdP Name you enter here is what users will see.	
Enable SSO	Logout URL	
SSO Setting: SSO Optional V	Users will be redirected to the Logout URL when they Sign Out.	
Get SAP Concur Metadata Copy or download SAP Concur metadata and Copy SAP Concur metadata	Upload your IdP's metatada Upload XML File I Hide this SSO option from users signing in to Concur on web or mobile	
OR Download SAP Concur metadata Download	Cancel Add Metadata	
IdP Metadata		
Add Edit Delete	View Metadata	
Entity ID	Name Hidden Active From Expiration Date 🛋	Logout URL

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:

 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.

5	Test single sign-on with concurtest
	Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

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**.

Hone > SAP Concur Travel and Expense					
SAP Concur Travel and Expense Users and groups ··· ×					
×	Ad usergroup 2/ Edit Remove 2/ Update Cvidential EE Columns ♥ Got feedback? Columns ♥ Got feedback?				
16 Overview					
Deployment Plan	IT he application will appear on the Access Panel for assigned users. Set \visible to users? to no in properties to prevent this. →				
Manage	First 100 shown, to search all users & groups, enter a display name.				
Properties	Display Name	Object Type	Role assigned		
24 Owners	No application assignments found				
8. Roles and administrators (Preview)					
28 Uses and groups					
Single sign-on					

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

 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.

Home > Enterprise applications - All applications > concurtest - Properties				
concurtest - Properties				
*	🔚 Save 🗙 Discard 🛅 De	elete		
Overview Getting started	Enabled for users to sign-in?	Yes No		
飼 Deployment Plan	Name 🚯	concurtest		
Manage				
11 Properties	Homepage URL 🚯			
🍰 Owners				
^ജ Users and groups				
Single sign-on	Logo 🚯			
Provisioning				
Application proxy				
😔 Self-service	User access URL	https://myapps.microsoft.com/signin/concurt		
Security		· • • •		
Conditional Access	Application ID 🚯	72368e7f-8afb-4881-9c74-ddfc3e52e73e		
🖧 Permissions				
Token encryption (Preview)	Object ID 🚯	a3ef5598-d016-495a-9cc7-ae95ec76c34b		
Activity	Torms of Sonviso Ltd.	Publisher did not provide this information		
Sign-ins				

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

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

Usernan	e, email address	s, or SSO co	ode		
testad	count@test.c	om			
		Next			
Rem	ember me				
Forg	ot username?				
	Not a Con	cur user yet	? Try Test Dri	ve	
			S.J.III		
< Sig	n In				
< Sig	gn In				
< Si	gn In unt@test.com	1			
< Sig	ʒn In unt@test.com				
< Sig	gn In unt@test.com Sign in	with MyCon	mpany SSO		
< Si	on In unt@test.com Sign in	with MyCo	mpany SSO		
< Sig	gn In unt@test.com Sign in Sign in	with MyCon	mpany SSO password		

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.

Mana	ge Single Sign-On	
Enable SS	60	
SSO Setting:	SSO Optional	
Get SAP	SSO Optional Users may sign in with a password or with SSO.	
Copy or dowr	SSO Required Users must sign in using SSO.	ty Provider (IdP).
Copy SAP Co		

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.

Company 🕨
Request •
Travel Admin
Expense •
Invoice

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

Company Admin > Authentication Admin Authentication Administration <u>Manage</u> Single Sign-On Manage Single Sign-On for SAP Concur products

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.







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.

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

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://wwwus.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

oup) are contain minimum		
https://us-impl.api.concursolutions.co	Add IdP Metadata	×
OR		
	Custom IdP Name*	
Download SAP Concur metadata	SAP IAS	
Download	The IdP Name you enter here is what users will see.	
	Logout URL	
	https://help.sap.com	
IdP Metadata	Users will be redirected to the Logout URL when they Sign Out.	
Add Edit Delet	IdP Metadata*	
	O Provide link to your IdP's metadata	
	OP	
-Wiour Provious Changes	0R	
-g-view Flevious citaliges	 Upload your IdP's metatada 	
	Ilpload XMI File SAP IAS Metadata xml X	
Rollout Instructions		
1. Test SSO		
We recommend that you test SSO by select keep it as optional.	Cancel Add Metao	data

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: <u>https://www.concursolutions.com/nui/signin</u>), 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:

Sign In	< Sign In
Username, verified email address, or SSO code ssoadmin@t00653928tex.com	ssoadmin@t00653928tex.com
Next	Sign in with google SSD
Remember me Forgot usemame?	Sign in with your password
Need support or not yet a Concur customer?	Need support or not yet a Concur customer?

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/ initsso?idpid=CLIENT_IDP_ID&spid=SERVICE_PROVIDER_ID&forceauthn=fals e

Example: *https://accounts.google.com/o/saml2/ initsso?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:

Done Antation.concursolutions.com AA C	Done antation.concursolutions.com AA 🖒
SAP Concur C Sign In	SAP Concur C Sign In
Username, verified email address, or SSO code	ssoadmin@t00653928tex.com
ssoadmin@t00653928tex.com	Sign in with Mobile SSO
Next	Sign in with SAP IAS
Forgot username?	Sign in with your password
Passwords	
qwertyuiop asdfghjkl	
	-
123 😄 espaço @ . retorno	

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.

Expense Report Pending	g Your Approval	
AutoNotification@cc To I) If there are problems with how thi	oncursolutions.com is message is displayed, click here to view it in a web brow	ster.
SAP Concur 🖸		SAP
Expense	e Report Pending Your Approval	
You have a report pen	ding your approval.	
Report From	SSO Admin	
Report Name	SSO TEST	
Report Purpose		
Requested Amount	2,000.00 USD	
View Report		
This amail was and here	CAD Consure COL 40005 Aug NE Dellause MIL 00004	1104

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.

Manag	ge Single Sign-On	
Enable SS	80	
SSO Setting:	SSO Optional	
Get SAP	SSO Optional Users may sign in with a password or with SSO.	
Copy or down	SSO Required Users must sign in using SSO.	ty Provider (IdP).
Copy SAP Co	nour monutur.	

View Previous Changes

This featured 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.

IdP Me	tadata				
Ad	d Edit Delete View Metadata				
	Entity ID	Name	Active From	Expiration Date 🚊	Logout URL
	mporraceounte.google.comeercanne.repre-eventrje-	Google Workspace	01/27/2020	01/25/2025	https://concursolutions.com
View P	revious Changes				

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

Date	Change	Entity ID	Name Logout URL	Hidden	Details
)6/08/2022	Edit		Concur Okta	~	View
06/08/2022	Edit		ray test 2	~	View
06/08/2022	Edit		ray test 2		View
06/08/2022	Edit		ray test 2	~	View
06/08/2022	Edit		ray test 2		View
06/08/2022	Add		ray test 2	~	View
06/07/2022	Delete		ray test 2		View
06/07/2022	Edit		ray test 2		View
06/07/2022	Add		ray test 2	~	View
06/07/2022	Delete		ray test 2	~	View
06/07/2022	Edit		ray test 2	~	View
06/07/2022	Edit	the rate of a second second second second	rav 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.

Date Changed	05/24/2022 Delate	
Company Change By		
Entity ID Name		
Logout URL Hidden	https://logout.com	
Metadata		
and the second s		
-	1.1" monthing "100-4" to spece monthly "requirements on a contraction of a second to the	
And Anna Capitality And Cambridge Mark Reports And Angles	1.1" monthings' 100-0'15 (prior moning)?" "Engl: "max.dets.com/initial/path/ministig/" minister's signed monthly and the path "form" protocollogger (formation) " organs.max" togothy " to minister's comparison of any "toto to ministig".	
	1.17 mendings''''''''''''''''''''''''''''''''''''	

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. <u>Go to Administration > Company > Authentication Admin</u>.



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

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.

idaptiv®								
P Dashboards	~	Web Ap Search All W	ps eb Applications		Q	Add Web Apps	2	
Roles			Name 🕇	Туре		Description		Provisioning
Policies			User Portal	Web - Portal		The User Portal is you	r interface to the Idaptive Identity	
Reports								
Requests								
Apps								
Web Apps 1								
Mobile Apps								
➡ Downloads								
Settings	>							

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

Add Web Ap	IPS to enable single-sign on		5 × at
Add web applications t	to enable single-sign on		tal
Search Custom	Import		ep
Search catalog by ann name	_		
Gearch catalog by app hame		Concur	Add
Concur 3	۹ 🖸	User Password	
Categories			
All Anns		Concur	Add
Featured		SAML + Provisioning	
Analytics			
Collaboration			
Communication			
CRM			
Customer Service			
DevOps			
Education			
ERP			
Finance			
Government			
Health Care			
	Search catalog by app name Concurt 3 Categories All Apps Featured Analytics Collaboration Communication CRM Customer Service DevOps Education ERP Finance Government Health Care	Search catalog by app name Concurt Concurt Categories All Apps Featured Analytics Collaboration Communication CRM Customer Service DevOps Education ERP Finance Government Health Care	Search catalog by app name Concurt Concurt Categories All Apps Featured Analytics Collaboration Communication CRM Customer Service DevOps Education ERP Finance Government Health Care

- 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).

6	Trust	
ML Response	Martin Devider Conf.	
missions	Identity Provider Contri	
ky	Meterine 7	or insur an signing unmodel, in order, mor sow, procerveries will report put is serie or consignation values in a order memory, device the memory, then took the memory and the series of the series o
count Mapping ked Applications	Manual Configuration	International
wisioning		If you need to edit them, edit them first then proceed to the configuration method required by Service Provider.
ridios		> MP Entity ID / MP Issuer ()
polagna		> Signing Certificate (j)
		The American State of the American American Provide Constant
		una, respertitazion any response appresazionariagei bolomico. Costy una
		File Download Metadata File 8

- 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.

ervice Provider Confi	guration 9	
elect the configuration metho	od specified by Service Provider, and then follow the instructions.	
Manual Configuration	Fill out the form below with information given by your Service Provider. Be s	ure to save your work when do
	SP Entity ID / SP Issuer / Audience ()	
	https://emea.api.concursolutions.com/saml2	10
	Assertion Consumer Service (ACS) URL (1)	-
	https://emea.api.concursolutions.com/sso/saml2/V1/acs/	11
	Recipient * () Same as ACS URL 12	
	Enter Recipient here	
	Sign Response or Assertion?	
	Response Assertion	_
	emailAddress	- 13
	Single Logout URL (j)	
	Enter URL here	
	Encrypt SAML Response Assertion (i)	
	Encounting Cartificate (Deculard)	

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

Concur Type: Web - SAU Actions -	AL + Provisioning - Status: Ready to Deploy			
Settings Trust SAML Response Permissions 15	Permissions Learn more Add 16			
Account Mapping	Name	Grant	View	Rat
Linked Applications Provisioning Workflow Changelog	L 25 sysadmin	2	2	

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.

- 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.



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



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

Manage Single Sign-On					
Enable S	Enable SSO				
SSO Setting: SSO Optional					
Get SAP	SSO Optional Users may sign in with a password or with SSO.				
Copy or down	SSO Required Users must sign in using SSO.	ty Provider (IdP).			
Copy SAP Co					

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.

	Administra	ation 🗸
Company Admin	Company	►
Tools	Request	•
Web Services	Travel Admin	
Report Admin	Expense	•
Authentication Admin	Invoice	

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

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:

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

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.

← Back to Applications			
🖏 Add Applicat	ion		Create New App
CATEGORIES			
All Integrations	7130	Q Search	
Analytics and Automation	638	All Integrations	
Collaboration Software	929	Anniegrations	
Developer Tools and Productiv	ity 629	Featured Integrations	See all
Directories and HR Systems	378		
Data Privacy and Consent Management	5		
Identity Proofing	5		
Identity Governance and Administration	11		
Marketing and Operations	725		
Security	713		
Social Login	5		
Zero Trust Ecosystem	53		
FILTERS			

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

× Create a New Application Integration		
Platform	Web *	
Sign on method	 Secure Web Authentication (SWA) Uses credentials to sign in. This integration works with most apps. SAML 2.0 Uses the SAML protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. This is a better protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users into the app. if the protocol to log users if the prot	
	OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.	

1 General Settings	2 Configure SAML	3 Feedback
General Settings		
App name	[Encryption] Concur - SSO Support Test	
App logo (optional) 🕥	Ø	
		Browse
	Upload Logo Requirements	
	Must be PNG, JPG or GIF	
	• Less than 1MB	
	For Best Results, use a PNG image wi	ith
	Minimum 420px by 120px to prevent upscaling	
	Transparent background	
App visibility	Do not display application icon to users	
	Do not display application icon in the Okta Mob	bile app

5. Enter an App Name, select a logo (optional), and then click **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.c	concursolutions.com/sso/saml2/V1/acs ["/>
A SAML Settings GENERAL Single sign on URL (2)	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

 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.

<pre>" entityID="https://us.api meration="urn:oasis:names:t</pre>	concursolutions.com ^I > tc:SAML:2.0:protocol">	
	Use this for Recipient URL and Destination URL Allow this app to request other SSO URLs	J
Audience URI (SP Entity ID) 🔞	https://us.api.concursolutions.com]
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 🛛 🕖	EmailAddress	
Application username 👔	Unspecified	
	EmailAddress	
Update application username on	x509SubjectName	
	Persistent	
	Transient	iow 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.

Name ID format 🛛	EmailAddress •	
Application username 💿	Okta username 🔺	
Update application username on	Okta username	
	Okta username prefix	
	Email	ow Advanced Settings
	Email prefix	
	Custom	
Attribute Statements (optional)	(None)	LEARN MORE
Name Name format	Value	r

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

 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:





2. Save this file in .crt format.



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

General Settings	2 Configure SA	ML	3 Feedback
A SAML Settings General			What does this form do? This form generates the XML needed
Single sign on URL	https://www-us.api.concursolution Use this for Recipient URL and Du Allow this app to request other St	s.com/sso/saml2/V1/a estination URL SO URLs	for the app's SAML request. Where do I find the info this form needs? The app you're trying to integrate wi
Audience URI (SP Entity ID)	https://us.api.concursolutions.com/	saml2	should have its own documentation using SAML. You'll need to find that doc, and it should outline what information you need to specify in th
Name ID format	If no value is set, a blank RelayState is	s sent	orm. Okta Certificate
Application username	EmailAddress •		Import the Okta certificate to your Identity Provider if required.
Update application username on	Create and update •		

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

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.externalKev}

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



Step 5: Finish the Configuration

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

1 General Settings	2 Configure SAML	3 Feedback
3 Help Okta Support understand Are you a customer or partner?	 I how you configured this application I'm an Okta customer adding an internal app I'm a software vendor. I'd like to integrate my app with Okta 	Why are you asking me this? This form provides Okta Support wi useful background information abou your app. Thank you for your help—
• The optional questions bel	ow assist Okta Support in understanding your app integration.	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**.

Settings	Edit About SAML 2.0 streamlines the end user experience by not requiring the user know their credentials. Users cannol
Sign on methods The sign-on method determines how a user signs into and manages their creder application. Some sign-on methods require additional configuration in the 3 rd pa Application username is determined by the user profile mapping. Configure prof	edit their credentials when SAML 2. configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.
SAML 2.0	Application Username
Default Relay State	Choose a format to use as the defau username value when assigning the application to users.
	If you select None you will be promp to enter the username manually whe nl-prod.concur.cor assigning an application with passw
	nl-prod.concur.cor assigning an application with pass

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: <u>https://www.concursolutions.com/nui/signin</u>), 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]".

0	
Userna	ame, verified email address, or SSO code
	Next
For	rgot username?
.	Need support or not yet a Concur customer?
< !	Sign In
	l.anderson@p0073567hq3z.com
paul	
paul	Sign in with Okta SSO [Encrypted]
	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.

additional help.

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.



OK

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

xpense Rep	ort Pending Your Approval	
A AutoNo	tification@concursolutions.com	
If there are proble	ems with how this message is displayed, click here to view it	in a web browser.
SAP Conc	ur C	SAP
	Expense Report Pending Your App	roval
You have a	https://www.concursolutions.com/mobile/ concurmobileredirect.asp?	·
Report From	type=exp_rpt_appr&ts=1620906285415&token=cca9f 9f189d11129036376513ea543f1479c0a540cdffc2525 6acf445c770f668/ctadeenurl=https://dewdfiac136.wdf	
Report Name	sap.corp:50201/saml2/idp/sso?saml2sp=https://us.api.	
Report Purpose	concursolutions.com/ saml2&hpo=4&cte=ugvikhkys6zixinpytofekut3ye9ceda	
Requested Am	hvjkhnzq2e5ndii8oj7mfqv8tpfpnd9y8481wmp3cdgmi0 kp8lqrwa%253d%253d%253a1%253aoazmx4wm Click or tap to follow link.	
View Report		
i nis en	nail was sent by: SAP Concur - 601 108th Ave NE. Bellevu	e. WA 98004. USA

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.

Mana	ge Single Sign-On	
Enable S	50	
SSO Setting:	SSO Optional	_
	SSO Optional	
Get SAP	Users may sign in with a password or with SSO.	
Copy or dowr	SSO Required	ty Provider (IdP).
CODY SAD CO	Users must sign in using SSO.	
Copy SAP CO	mour motadata	
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**.

IP M	etadata dd Edit Delete View Metadata					
	Entity ID	Name	Hidden	Active From		Logout URL
	https://us2.api.concursolutions.com/saml2	SAML Monitor		09/30/2016	09/30/2026	
	http://www.okta.com/exkbkvgvnzjismmfx2p7	muttals okta		02/27/2018	02/27/2028	
	http://www.okta.com/exk8bjsi41SiSaXyM2p7	Concur Okta	~	02/27/2018	02/27/2028	
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**.

	Administration -
Expense Settings	_Ռո
Company	
Expense User Exp	perience 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. <u>Go to Administration > Company > Authentication Admin</u>.

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

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.

One"		DASHBOARD	APPLICATIONS	USERS SETUP	ACCOUNT			?	2	Sign C
My Applications	Application Catalog	PingID SDK #	Applications	OAuth Settings						
My Applicat	ions									
SAML OIDC										
—										
						tion or optituld				
Applications you'v	e added to your account	are listed here.	You can search	h by application na	ime, descrip	tion of entityid				
Applications you'v Active application	e added to your account tions are enabled for sing	are listed here. ' gle sign-on (SSC	You can search)).	n by application na	ime, descrip	tion of entityid				
Applications you'v Active applica Details display 	e added to your account tions are enabled for sing /s the application details.	are listed here. ` gle sign-on (SSC	You can search)).	n by application na	ime, descrip	uon or enutyra				
Applications you'v Active applica Details display Applica	e added to your account tions are enabled for sing /s the application details. tion Name	are listed here. ` gle sign-on (SSC Type	You can search)). e	h by application na Status	ime, descrip	Enabled				
Applications you'v Active applica Details display Applica SAP C	e added to your account tions are enabled for sing /s the application details. tion Name Concur Test	are listed here. ` gle sign-on (SSC Type SA	You can search)). e AML	Status Active	ime, descrip	Enabled	Re	emove	•	
Applications you'v Active applica Details display Applica SAP C	e added to your account tions are enabled for sing rs the application details. tion Name Concur Test	are listed here. ` jle sign-on (SSC Type SA	You can search)). e AML	Status Active	ime, descrip	Enabled Yes	Re	emove	•	
Applications you'v Active applica Details display Applica SAP C Add Application	e added to your account tions are enabled for sing rs the application details. tion Name Concur Test	are listed here. ' gle sign-on (SSC Type SA	You can search)). e MML	Status Active	ime, descrip	Enabled Yes	Re	emove Pause A		
Applications you'v Active applica Details display Applica Applica Add Application	e added to your account tions are enabled for sing rs the application details. tion Name Concur Test	are listed here. ' Jle sign-on (SSC Type SA	You can search)). e AML	Status Active	ime, descrip	Enabled Yes	Re	emove Pause A		
Applications you'v Active applica Details display Applica Applica Application Search Application New SAM Application	e added to your account tions are enabled for sing rs the application details. tion Name Concur Test	are listed here. ' Jle sign-on (SSC Type SA	You can search)). e AML	Status Active	ime, descrip	Enabled Yes	Re	emove Pause A	► II SSO @	
Applications you'v Active applica Details display Applica SAP (Add Application Search Applicat New SAML Application	e added to your account tions are enabled for sing rs the application details. tion Name Concur Test tion Catalog plication	are listed here. ' Jle sign-on (SSC Type SA	You can search)). e	Status Active	ine, descrip	Enabled Yes	Re	Pause A	► II SSO @	
Applications you'v Active applica Details display Applica SAP C Add Application Search Applica New SAML Application Request Ping I	e added to your account tions are enabled for sing rs the application details. tion Name Concur Test tion Catalog plication dentity add a new applic:	are listed here. ' Jle sign-on (SSC Type SA ation to the appli	You can search)). e AML ication catalog	Status Active	ine, descrip	Enabled Yes	Re	emove Pause A	► II SSO @	

Step 2: Application details

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

New Application	SAML Incomplete No
1. Application Details	
Application Name	SAP Concur *
Application Description	test application *
	Max 500 characters
Category	Travel •
Graphics	Application Icon
	For use on the dock Image Change Max Size: 256px x 256px
NEXT: Application Configuration	Cancel 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.

 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).

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

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.

2. Application Configuration	
I have the SAML configuration	I have the SSO URL
You will need to download this SAML metad	data to configure the application:
Signing Certificate	PingOne Account Origination Certificate 🔹
SAML Metadata	Download
Provide SAML details about the application Protocol Version	e you are connecting to: ● SAML v 2.0 ○ SAML v 1.1
Upload Metadata 🧔	Select File Or use 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)

Upload Metadata 🛛 😡	Uploaded file:metadata(1).xml Select File Or use URL
Assertion Consumer Service (ACS)	https://www-us.api.concursolutions.con *
Entity ID	https://us.api.concursolutions.com/sam *
Application URL	
Single Logout Endpoint @	
Single Logout Response Endpoint @	
Single Logout Binding Type	Redirect OPost
Primary Verification Certificate a	Escolher arquivo Nenhum arquivo selecionado saml20metadata.cer
Secondary Verification Certificate @	Escolher arquivo Nenhum arquivo selecionado
Encrypt Assertion @	2
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**.

Application Name	Туре	Status	Enabled	
SAP Concur	SAML	Active	Yes	Remove
3. SSO Attribute Mapping				
Map the necessary application	n provider (AP) attributes to	attributes used by	your identity provider (IdP).	
Map the necessary application Application Attribute	n provider (AP) attributes to Identity Bridge Attribute or	attributes used by Literal Value	your identity provider (IdP).	Required
Map the necessary application Application Attribute	n provider (AP) attributes to Identity Bridge Attribute or	attributes used by Literal Value	your identity provider (IdP).	Required

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

	Application Attribute	Identity Bridge Attribute or Literal Valu	ie		Required	
1	SAML_SUBJECT	Email	As Literal	Advanced	•	•

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 <u>an article</u> 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**.

	Search	
Group Name		
Jsers@directory		Remove
Domain Administrators@directory		Add
est Users		Add

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- Single Sign-On	-On page: 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.

,	
Initiate Single Sign-On (SSO) URL @	https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=9c9fc5fd-81c8-4696-b57e-707 9fea1a0ae&idpid=d5cbc67c-eb2d-4e99-80bb-6dba9d6e8c05
Single Sign-On (SSO) Relay State @	https://pingone.com/1.0/9c9fc5fd-81c8-4696-b57e-7079fea1a0ae
Signing Certificate	Download
SAML Metadata	Download
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 Single Sign-On	-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: <u>https://www.concursolutions.com/</u>
 - US DC Test: <u>https://implementation.concursolutions.com/</u>
 - EMEA DC Prod: <u>https://eu1.concursolutions.com/</u>
 - EMEA DC Test: <u>https://eu1imp.concursolutions.com/</u>
 - CN DC Prod: <u>https://www.concurcdc.cn/</u>
- 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 wih 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.

Manag	Manage Single Sign-On					
Enable SS	60					
SSO Setting:	SSO Optional					
· · · · · ·	SSO Optional					
Get SAP	Get SAP Users may sign in with a password or with SSO.					
Copy or dowr	Copy or dowr SSO Required ty Provider (IdP).					
Copy SAP Co						

Log examples:

Date Changed	06/07/2022
Change	Add
Company	
Change By	
Entity ID	
Name	
Logout URL	
Hidden	\checkmark
Metadata	1.5° amending-"000-4"to iptos anticple-"bogo."see.obto.com/webBcjcccccccom/pBg/" adosced+"or sciptos Mechanisheguartaligned-"Talas" protonolloggeridoumscation-"us ciptos amer"signing's
Metadata	1.1° annocimpe "100-4" " iptes anticipite" bogs ("ema sites conclusible)contributydig" anisocade" or copies Annocimpantalipad" "bogs" protectinggerilleancesion" o copies and "togoing" to anisocade" togoing" to anisocade" togoing " The anisocade" togoing " The anisocade" togoing " togoing and an anisotation of the second togoing to the second togoing togoing to the second togoing to the second togoing to the second to the second togoing togoing togoing to the second togoing togoing togoing togoing to the second togoing togoing to the second togoing togoin
Metadata	1.3' mereding-'NUE-4''s iptor molicylor''scopicates, and conclusible point distributed by "meredination" or copies Meridiation participant''faims' protocollogue of the meridian ciptor mer''scopical'' fo melander''scopical'' Mana Ministra Complete and complete by the set of the set of the set of the set of the set of t
Metadata	<pre>1.5' mechanizage'200-4''s iptor methodology'200-4''s iptor methodology'200-4''s iptor methodology'200-4''s iptor mechanizations and any 'to's iptor mechanizations' methodology'' iptor mechanizations''s iptor mechaniza</pre>
Metadata	<pre>1.5' meendings'100-4'10 ipton metricpic''scap.''mee.stra.rem'sattlejoiriidiadpHip'' meine.metr'sc cripton Meendor'trip.''mee.stra.rem'sattlejoiri'scap.''meine.metr'sc cripton Meendor'trip.''mee.stra.reg'1000.'00'meine.g#'' fa meine.metr'trip.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#''' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#''' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#''' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#'''' fa.meine.metr'scap.''mee.stra.reg'1000.'00'meine.g#''''''''''''''''''''''''''''''''''''</pre>
Metadata	<pre>1.5" mercedings"1000-8"10 iptor mercipite "terms into conclusibly provided provided provide mercedings" iptor mercipite "terms into conclusion" into copies mercipite "terms into conclusion" into conclusion into conclusion into copies mercipite "terms into conclusion" into conclusion into copies mercipite "terms into conclusion" into conclusion into conclusion" into</pre>
Metadata	<pre> 1.5' mechanizary 'NEE-4''E prove metricipite''Ecopy.''email and a new 'needed prove thinkey Might'' metrics and 'ne rights Mechanizary Temp .''email peet''Ecom' prove thinkey Might' is metric and "'ecopy.''email and any 'Ecol and any "' Markar Michael Content of this thickey and any 'Ecol and and any 'Ecol and any '' Markar Michael Content of this thickey and any 'Ecol and any 'Ecol and any '' Michael Content of this thickey and any 'Ecol and any 'Ecol and any '' Michael Content of this thickey and any 'Ecol and any '' Michael Content of this thickey and any 'Ecol and any '' Michael Content of this thickey and any 'Ecol and any '' Michael Content of this thickey and '' Michael Content of this this this this this this this this</pre>

iew Previous Ch	langes
Date Changed Change Company Change By	06/08/2022 Edit
Entity ID	
Name	Concur Okta
Logout URL Hidden	
- Industr	
Previous Values	
Entity ID	
Name	Concur Okta
Hidden	
Metadata	
motudud	C and the little state
real-don crighteener	pror antitally "bright" and a seal and the seal of the seal of the seal " or
real contentions	rights Mariketholmagnetaligent/falm" protortilogaridisamention" et
real despires	China men, Arderoed, -
	ta antina dari tergeri tana ati ang terti teranange i
1000-00	Contract of Contracted Contractional Action (Contraction Contraction Contracti
100	Charles and the second s
	ОК

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.

Date Changed	05/24/2022
Change	Delete
Company	
Change By	
Entity ID	
Name	
Logout URL	https://logout.com
Hidden	
Metadata	
Metadata	
Metadata	1.7" accordings"100-6"15
Metadata	1.5° amondioup'''EM-4'''' Aphon anti-igito''''organi'''eme antis contraction''y second by '' action with ''w
Metadata	1.5" meneting-"100-0"15 igter meningto-"tong-lines.stor.com/unitedistrictions.stor."menetication contact Manifestications.stor.com/ tong-lines.stor.com/ contact Manifestications.stor.com/
Metadata	1.5° menelogy'900-6's gene metrigde 'nogenieme and and encoder the semicorrelation of the second 'n cogne Metrical Magnetic System 'nogenie's comments and 'nogenie's comments and 'nogenie's
Metadata	1.2° menodings'100-2°) gene meligite'lengel'emme atta omelmettilligemettalige" melesamet'e cigne Meridelendegeneratigemet'leism' protociliggeritemmetalism''e cigne ame'rigeing'' 1 melesato''leging'' 1 melesato''leigel'men at org'1000-001melesig"'
Metadata	1.5° annohimp"100.5°1 apino antiquit" "org.:"see antis.com/settir/"pametricity" antiscent "s cigina Macidatichequaristignet" "bias" protectinggeritheamouties" "s cigina Amerikanistigning" Cigina Amerikanisti (see at org.)tettiri antiscig"" Sanat Macar
Metadata	<pre>1.5" monthings''100.6"'1 apter monthings''100.6"'1 apter monthingst''100.6"'1 apter monthingst''100.6"'1 apter monthingst''100.8"' apper monthingst'' apper monthingst'' apper monthingst'' apper monthingst''' apper monthingst''' apper monthingst''' apper monthingst''' apper monthingst''' apper monthi</pre>
Metadata	<pre></pre>
Metadata	

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 <u>Viewing</u> <u>Assigned Tenants and Administrators</u> 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 <u>SAP Concur Integration Scenario</u> 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**.

Administration -
Expense Settings
Company
Expense User Experience Settings

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

	Access To Concur	
User Acc Set up ar	counts nd manage your Concur users and their permissions.	
	Show 1 Advanced Setting	

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



For the SAP Concur **Professional** edition:

1. <u>Go to Administration > Company > Authentication Admin</u>.

	Administra	ition 🗸
Company Admin	Company	•
Tools	Request	•
Web Services	Travel Admin	
Report Admin	Expense	•
Authentication Admin	Invoice	

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

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:

 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.

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

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**.

≡	SAP Identity Authentical	tion Service [US/Car	ada]						Concur Test	- adg0duqpi
ଜ	Home									
8ª	Users & Authorizations	Users & Authorizations								
Ē	Applications & Resources $~\checkmark~$	_ =	0	- 0	0	0	F			
	Applications	8	8	22	0	<u>Å</u>	5	Z +		Z
	Tenant Settings									
	Terms of Use Documents	User Manager	ment	User Groups		Administrat	tors	Import Users		Export Us
	Privacy Policy Documents									
	E-Mail Template Sets									Export the
	Password Policies	Manage us	er accounts	Manage	user groups	Configure	Authorizations	import new users exis	or update sting users	Authe
	Custom CSS									
	Tenant Texts	Application	is & Res	ources						
2	Identity Providers	Application		ources						
	Monitoring & Reporting		Λ	0		6	0	ค	0	
		·	4	*		نگ	0	6	0	
		Applications		Topont Sotting	10	Torms of U		Brivery Policy		E Mail Tar
		Applications		Tenanic Setting	5	Documents	se .	Documents		E-Mait Ter
		Set custom featu	res for your applications	Configure ten	ant settings	Configure c use for yc	sustom terms of our applications	Configure custo policies for your ap	om privacy oplications	Configu template

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

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

≡	SAP Identity Auther	ntica	ation Service [US/Canada]	
බ	Home		Applications	
8ª	Users & Authorizations	>	Search	Q
	Applications & Resources	~		
	Applications		Bundled Applications	
	Tenant Settings		Concur SAML2 -CN	>
	Terms of Use Documents		https://cn.api.concurcdc.cn/saml2	
	Privacy Policy Documents		test	>
	E-Mail Template Sets		https://us.api.concursolutions.com/saml2	
	Password Policies		System Applications	
	Custom CSS		Administration Console	
	Tenant Texts		oac.accounts.sap.com	>
2	Identity Providers	>	User Profile	
ď	Monitoring & Reporting	>	sp.accounts.sap.com	>
				Add

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

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

Application	
Concur SSO - TEST	
This application name appears on the logon and registration pages. Home URI	Home URL not configured
Trust Authentication and Access Branding and Layout	
Single Sign-On	
Type Choose SAML 2.0 or OpenID Connect.	SAML 2.0 >
SAML 2.0 Configuration Configure trust with a service provider by uploading metadata for web-based authentication.	Not Configured >
Subject Name Identifier Configure the attribute which the application uses to identify the users. The attribute is sent as name ID in SAML 2.0 authentication requests to Identify Provider.	User ID >

5. 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**.

SAML 2	0 Configuration	Save Cancel
Define from I	Metadata	
Configure trust with	a service provider by uploading metadata for web-based authentication.	
Metadata File:	Enter .xml file	Browse
Configure trust with	a service provider via metadata URL for web-based authentication.	
Metadata URL:		Load

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

K	SAML 2.0 Configuration	
Define from Meta	adata	
Configure trust with a	service provider by uploading metadata for web-based authentication.	
Metadata File:	SAP Concur Metada (implementation).xml	- 1
Configure Manua	ally	- 1
*Name:	https://us-impl.api.concursolutions.com/saml2	
Assertion Consur	mer Service Endpoint	
The URLs of the servious service.	ice provider assertion consumer service endpoint that receives responses from Identity Authentication	
+ Add URL	Reply URL (AOS)	
Default	URL Index	
\bigcirc	https://www-us-impl.api.concursolutions.com/sso/saml2/V1/acs/	W
	() Save	⊗ Cancel

Step 3: Change Subject Name Identifier

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

gle Sign-On	
SAML 2.0 Configuration Configure trust with a service provider by uploading metadata for web-based authentication.	https://us.api.concursolutions.c
Subject Name Identifier	1110
Configure the attribute which the application uses to identify the users. Identity Authentication sends the attribute to the application as name ID in SAML 2.0 assertions.	User ID
Default Name ID Format	
Configure the default Name ID format. The attribute is sent as name ID format in SAML 2.0 authentication requests to Identity Provider.	Unspecified
Apply Function to Subject Name Identifier	None
Convert the subject name identifier to uppercase or lowercase.	None
Attributes	

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.

Global User ID, User ID, Logir	Name and Email are unique for the tenant.
 Basic Configuration Set a basic attribute from When Identity Authenticat the advanced configuration Select a basic attribute: Select a fallback attribute: 	the list below. ion acts as proxy IdP, and the users have no profile in Identity Authentication, choose n option. Email None
Advanced Configuration	n

• 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.

Global User ID, User ID, Login N	ame and Email are unique for th	e tenant.	
 Basic Configuration 			
Set a basic attribute from the When Identity Authentication the advanced configuration of	e list below. n acts as proxy IdP, and the user: option.	s have no profile in Identity	Authentication, choose
Select a basic attribute:	Login Name	~	
Select a fallback attribute:	None	~	

• 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 <u>Configure the Subject Name Identifier Sent</u> to the Application procedure.

Global User ID, User ID, Login Nam	e and Email are unique for the tenant.	
Basic Configuration		
Advanced Configuration		
Set an attribute with dynamic va When Identity Authentication ac attribute with the following dyna	alue in the following pattern: <prefix> \${attribute_techni :ts as proxy IdP, and the users have no profile in Identity amic value: <prefix> \${corporateIdP.<corporateidp attrik<="" td=""><td>cal_name} <suffix>. / Authentication, set an pute>} <suffix>.</suffix></suffix></td></corporateidp></prefix></prefix>	cal_name} <suffix>. / Authentication, set an pute>} <suffix>.</suffix></suffix>
Dynamic subject name identifier valu	e: \${loginName}@sap.com	
Select a fallback attribute:	None 🗸	

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.

Application		
Home URL	Home URL not configured	ł
Trust Authentication and Access Branding and Layout		
Single Sign-On		
Type Choose SAML 2.0 or OpenID Connect.	SAML 2.0	>
SAML 2.0 Configuration Configure trust with a service provider by uploading metadata for web-based authentication.	https://us-impl.api.concursolutions	>
Subject Name Identifier Configure the attribute which the application uses to identify the users. The attribute is sent as name ID in SAML 2.0 authentication requests to Identity Provider.	Login Name	>
Default Name ID Format Configure the default Name ID format. The attribute is sent as name ID format in SAML 2.0 authentication requests to Identity Provider.	Unspecified	>
Apply Function to Subject Name Identifier Convert the subject name identifier to uppercase or lowercase.	None	>
		elete

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

<	Default Name ID Format
0	Unspecified urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
۲	E-Mail urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
For	r more information about Default Name ID Formats, see Identity Authentication Documentation.
	Save Scancel

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 Provide	r Settings		
	Name: https://adg0duqpi.accounts400.ondemand.com		
Single Sign-On I	Endpoint		
The URLs of the ider	ntity 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/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/idp/sso/saml2/		
Assertion Consu	Imer Service Endpoint ntity 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/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondemand.com/saml2/idp/acs/adg0duqpi.accounts400.ondem		
Single Logout E	ndpoint ntity provider single logout endpoint that receive logout messages		
Binding	URL		
HTTP-Redirect	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.saml2/idp/slo/adg0duqpi.saml2/idp/slo/adg0duqpi.saml2/idp/slo/adg0duqpi.saml2/idp/slo/adg0duqpi.saml2/idp/slo/adg0duqpi.saml2/idp/slo/adg0duqpi.saml2/idp/slo/adg0du		
HTTP-POST	https://adg0duqpi.accounts400.ondemand.com/saml2/idp/slo/adg0duqpi.accounts400.ondemand.com		
Signing Certifica A certificate used by	the identity provider to digitally sign the messages for the applications		
Develo 111 - 11	Certificate File: Enter a file with extension .crt or .cer		
Vownload Metadata	arile		

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: <u>https://www.concursolutions.com/nui/signin</u>), 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.

ଜ	Home	SAML
8	Users & Authorizations	
	Applications & Resources $~\checkmark~$	Identity Provider Settings
	Applications	
	Tenant Settings	Name: https://adg0duqpi.accounts400.ondemand.com
	Terms of Use Documents	
	Privacy Policy Documents	Single Sign-On Endpoint
	E-Mail Template Sets	The URLs of the identity provider single sign-on endpoint that receive authentication requests
	Password Policies	Binding URL
	Custom CSS	HTTP-Redirect https://adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com
	Tenant Texts	HTTP-POST https://adg0duqpi.accounts400.ondemand.com/saml2/idp/sso/adg0duqpi.accounts400.ondemand.com
2	Identity Providers	
	Monitoring & Reporting	Assertion Consumer Service Endpoint
		The URLs of the identity provider assertion consumer service endpoint that receive authentication responses

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

SAP C	Sign In	SAP Concur C Sign In
Username, verified email	address, or SSO code	ssoadmin@t00653928tex.com
ssoadmin@t006539	928tex.com	Sign in with Mobile SSO
	Next	Sign in with SAP IAS
Remember me		
Forgot username?		Sign in with your password
Forgot username?	Done	sign in with your password
Forgot username?	Done	sign in with your password
Forgot username?	Passwords t y u i o p	sign in with your password
Forgot username?	Passwords t y u i o p g h j k l	sign in with your password
Forgot username?	Passwords t y u i o p g h j k l v b n m ≪	sign in with your password

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 wih 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.

Expense Report Pending	Your Approval
AutoNotification@co	ncursolutions.com
If there are problems with how this	message is displayed, click here to view it in a web browser.
SAP Concur 🖸	SAP
Expense	Report Pending Your Approval
You have a report pend	Report Pending Your Approval
You have a report pend Report From	ing your approval.
You have a report pend Report From Report Name	ing your approval. SSO Admin SSO TEST
You have a report pend Report From Report Name Report Purpose	ing your approval. SSO Admin SSO TEST
You have a report pend Report From Report Name Report Purpose Requested Amount	Report Pending Your Approval
You have a report pend Report From Report Name Report Purpose Requested Amount View Report	Ing your approval. SSO Admin SSO TEST 2,000.00 USD

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.

Expense Report Pending Your Approval
AutoNotification@concursolutions.com
) If there are problems with how this message is displayed, click here to view it in a web browser.
SAP Concur 🖸
Expense Report Pending Your Approval
You have a https://www.concursolutions.com/mobile/ concurnobileredirect.asp?
Report From 9f189d11129036376513ea543f1479c0a540cdffc2525
Report Name sap.corp:50201/saml2/idp/sso?saml2sp=https://us.api.
concursolutions.com/ Report Purpose sam28/hpp=48/cte=ugvikhkysfiziving/tofekut3ye9ceda
Requested Amc kp8lqrva%253d%253d%253a1%253aoazmx4wm Click or tap to follow link.
View Report

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.

Manage Single Sign-On					
Enable SS	60				
SSO Setting:	SSO Optional				
Get SAP	SSO Optional Users may sign in with a password or with S	:50.			
Copy or dowr	SSO Required Users must sign in using SSO.	ty Provider (IdP).			
Copy SAP Co	nour motadata				

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 C	ious 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.

Log examples:

Date Changed	06/07/2022	
Change	Add	
Company		
Change By		
Entity ID		
Name		
Logout URL		
Hidden	\checkmark	
Metadata	1.1' annulling: '200-8''s	
Metadata	<pre>/'l.d' monodings'100-d'in Ciptor motingthe''sognitives.skts.com/webBigsitelds/pEg/' motion.mdf'so compose Merchantohogueristipeet''lsize' protocolloggerithommerstice''s Ciptor ser'signing's Ciptor ser'signing's Ciptor ser'signing's Ciptor d'international complete to an international decige's Ciptor d'international complete to an international decige's Ciptor d'international complete to an international decige's Ciptor d'international decige to an international decige's Ciptor decige to an international decige to an international decige Ciptor decige to an international decige to an international</pre>	
Metadata	<pre>/'l.f' mecodings'100-d'10 ciptor mecodings'100-d'10 ciptor mecodings:'D00-d'10 ciptor mecodings:'Mongo.'D00-d'10 conciptor Mecodoristicspanetaligned'Talam' protocolloggerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogerillogeril</pre>	
Metadata	<pre>/'l.d' mechaning''net d'in i(j.d' mechaning)''net d'in i(j.d' mechaning)'''''''''''''''''''''''''''''''''''</pre>	
Metadata	<pre>/'l.d' mechaning''net-d'in Lighter metiopic''net-d'in Lighter metiopic''net-d'in Lighter metiopic''net-d'in Lighter metiopic'' lease akte can berekendelige telebagety'' metion met''s Lighter metiopic'' lease at ong 'telebage'' Lighter metiopic'' lease at ong 'telebage''' Lighter metiopic''' Lighter metiopic'''' Lighter metiopic'''''''''''''''''''''''''''''''''''</pre>	

ew Previous Cł	nanges	×
Date Changed Change Company Change By	06/08/2022 Edit	
Entity ID Name	Concur Okta	
Hidden	\checkmark	
Previous Values		
Entity ID		
Name	Concur Okta	
Logout URL		
Metadata		
the second	1.4" annullings" (III-d')s	
real-dot inglessor	pror antipleving. The des calendary contradigity after	
THE CONTRACTOR	score Reclationegestational fairs, house differences	100.000
	Figure and Sector Sector (Sector) and an interview (Sector) and an interview (Sector)	
1000-0010	Natur -	
1000	Children's Provident Concerning and Stage Control of Concerning and Concerning an	
	and the second secon	and a second
	_	

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 <u>SSO Overview Guide</u>
- SAP Help Portal <u>SAP Cloud Identity Services Identity Authentication</u>
- SAP KBA <u>2701851 SAP Cloud Platform Identity Authentication Service</u> (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**.

	Administration -
Expense Settings	լիտ
Company	
Expense User Experience 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. <u>Go to Administration > Company > Authentication Admin</u>.

	Administra	ition -
Company Admin	Company	F
Tools	Request	•
Web Services	Travel Admin	
Report Admin	Expense	•
Authentication Admin	Invoice	

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

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:

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

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**.

SAP NetWeaver Administrator
User: Luft Lucas Active Profile: Complete List System: ID2 On dewdfias136, v.7.50 System Time/Date:
My Workspace Availability and Performance Operations Configuration Troubleshooting SO
Security Infrastructure Scenarios Connectivity
Authentication and Single Sign-On Views
Use the Authen Usion and Single Sign-On service to configure the authentication methods required for your application
Single Sign-On mechanisms such as HTTP-based cross-platform authentication using the Simple and Protected Negotian
Language (SAML) version 2.0, with which you can configure the AS Java to act as an identity provider, a service provide
The User Management Engine (UME) provides centralized user management for all Java applications and can be config
data sources. It is seamlessly integrated into the Application Server Java of the SAP NetWeaver Application Server for J
administered using the administration tools of the AS Java.
Trusted Systems Views
You can use the trusted systems configuration to maintain the relationship between issuing and accepting systems.

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

Authentication and Single Sign-On: Authentication			
Favorites Related Links Go To Support Details			
Authentication SAML 2.0 SPNEGO			
Components Login Modules Properties Logon Policies			
Edit Save Cancel Add Remove			
Policy Configuration Name			
8			

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

Authentication and Single Sign-On: SAML 2.0
Favorites Related Links Go To Support Details
Authentication SAML 2.0 SPNEGO
Local Provide Trusted Primiders Policies Name ID Management Edit Save Cancel Disable Download Metadata Delete Configuration
: Operational Mode:
General Settings Metadata Authentication Contexts User Attributes Identity Provider Settings Service Provider Settings
Signature and Encryption Keystore View: Signing Key Pair: Encryption Key Pair: Trusted CAs Keystore View:

 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.

Authen	tication and Single Sign-O	n: SAML 2.0	
Favorites Rela	ated Links Go To Support Details		
Local Provider	Trusted Providers Policies Name ID Management		
Show: Service F Active	Providers Edit Save Cancel Disable Name	Add Update Remove Manually Specifying Metadata URL Uploading Metadata File	4

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

s#	ML 2.0 Configuration								
	New Trusted Service	Provider							
R	• <u>1</u>	2	3	4	5	6	7	8	9
	Select Metadata	Metadata Verification	Select Providers	Provider Name	Signature and Encryption	Single Sign-On Endpoints	Single Log-Out Endpoints	Artifact Endpoints	Manage Name ID Endpoints
	Previous Next F	inish Cancel							
	Metadata File:* Brows	e metadata (18).xml							

 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.

Section 14: Appendix - SAP NetWeaver Setup

SAML	2.0 Configuration						
Nev	v Trusted Service Provider	r					
-	1	2	3	4	5		6
17	Select Metadata Metada	ta Verification	Select Providers	Provider Name	Signature and E	nervotion	Single Sign-On Endp
	Ocioer motoreau	ita vormouter	001001111111111	Tronad.	0.9	10.) P	onigio oigi: en en-p
	Previous Next 🕨 Finish C	ancel					
							6
	Certificates and algorithms						
	Signing Certificate:	CN=core-saml-proc	d.concur.com,OU=C	ore Services,O=SAP	Conur,L=Bellevue,S	Details	
	Encryption Certificate	CN=core-saml-proc	d.concur.com,OU=C	ore Services,O=SAP	Conur,L=Bellevue,§	Details	
	Encryption Obtaindute:	AES-128			•	bottane	
	Encryption Algorithm.						
	Single sign-on authentication	on request		Manage N	lameID request an	d response	
	Require Signature:	Always	•	Sign:		Always	•
				Require Si	gnature:	Always	•
	Single sign-on assertions			Encrypt Ele	ements:	No	•
	Sign:	Always	•	Require Er	ncrypted Elements:	No	•
	e in 1 in 1			A			
	Single sign-on response	Nevor		Artifact re	solution request a	Alwaye	sponse
	Sign:	Never		Sign:		Always	
	Encrypt Elements:	NO	_	Require Si	gnature:	Always	•

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**.

SAML 2.0 Configuration								
New Trusted Servic	e Provider							
Select Metadata	2 Metadata Verification	3 Select Providers	4 Provider Name	5 Signature and Encryption	6 Single Sign-On Endpoints	7 Single Log-Out Endpoints	8 Artifact Endpoints	9 Manage Name ID Endpoints
Previous Next	Finish Cancel							

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**.

Authentic	cation and Single Sign-On: SAML 2.0
Favorites _ Related	Links Go To Support Details
Authentication	n SAML 2.0 SPNEGO
Local Provider Trus	ted Providers Policies Name ID Management
List of trusted provide Show: Service Provide	ders Edit ave Cancel Enable Add Update Remove
Active	Name 🔔
<u>₹</u>	
\diamond	
	https://us.api.concursolutions.com/saml2

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.

Name ID Format				
Format Name:*		•		
	E-mail	N		
Source Name:*	Kerberos	3		
	Persistent			
	Transient			
	Unspecified			
	Windows Name			
	X509 Subject Name			

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.

Authentic	cation and Single Sign-On: SAML 2.0
Favorites _ Related	Links Go To Support Details
Authenticatio	n SAML 2.0 SPNEGO
Local Provider Trus	ted Providers Policies Name ID Management
List of trusted provid	ers
Show: Service Prov	ders Edit Save Cancel Engle Add Update Remove
Active	Name 🔟
¥ -	
♦	
□ ◇	https://us.api.concursolutions.com/saml2
	10.00.7

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.

Authentication and Single Sign-On: SAML 2.0				
Favorites Related Links Go To Support Details				
Authentication SAML 2.0 SPNEGO				
Cocal Provider Trusted Providers Policies Name ID Management Edit Save Cancel Disable Download Metadata Delete Configuration				

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: <u>https://www.concursolutions.com/nui/signin</u>), 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".

Learnama, varified amail addrocs	a ar SSO cada
testconcur@netweaver	
N	ext
Remember me Forgot username?	

	< Sign In	
	testconcur@netweaver	
	Sign in with SAP NW SSO	
	Sign in with your password	
	Need support or not yet a Concur customer?	
1		

- 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.

Authentication and	Single Sign-On: SAML 2.0
Favorites _ Related Links _ Go To _	Support Details
Authentication SAML 2.0	SPNEGO
Local Provider Trusted Providers Polic	es Name ID Management
Edit Save Cancel Disable	Download Metadata Delete Configuration
: Java_Identity_Provi Operational Mode: Identity Provider an General Settings Metadata	der
Single Sign-On Service (SSO) Supported SSO Types: Supported Bindings:	☑ IdP-Initiated ☑ SP-Initiated ☑ HTTP Redirect ☑ HTTP PoST ☑ HTTP Artifact ☑ SOAP
Endpoint URL:	https://dewdfias136.wdf.sap.corp:50201/saml2/idp/sso
Session Timeout:	3.600 Seconds View Sessions
Cleanup Interval for Expired Sessions:	Include session timeout in assertion (SessionNotOnOrAfter) 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:

- 1. Open the SAP Concur login page according to the environment you want to test.
 - US DC Prod: <u>https://www.concursolutions.com/</u>
 - US DC Test: <u>https://implementation.concursolutions.com/</u>
 - EMEA DC Prod: <u>https://eu1.concursolutions.com/</u>
 - EMEA DC Test: <u>https://eu1imp.concursolutions.com/</u>
 - CN DC Prod: <u>https://www.concurcdc.cn/</u>
- 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:

16:01	a- 2 🗮	15:02			
Done Concursolutions.com	S AA	Done	a concursolut	tions.com	S AA
SAP Concur C Sign In]	<	SAP Con Sign I	cur 🖸	
Username, verified email address, or SSO code		testconc	ur@netweaver		
testconcur@netweaver			Sign in with Mo	obile SSO	
Next			Sign in with S	SAP NW	
Remember me			Sign in with you	r password	
r olgot docimano.					
$\wedge \vee$	Done				
Passwords					
qwertyu i	o p				
asdfghj	k I				
☆ z x c v b n	m 🗵				
123 😄 espaço @ .	retorno				
		<	>	Ċ	Ø

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.

xpense Rep	ort Pending Your Approval	
A AutoNo	vtification@concursolutions.com	
If there are proble	ems with how this message is displayed, click here to view it in a w	eb browser.
SAP Conc	ur 🖸	SAP
	Expense Report Pending Your Approva	I
You have a	https://www.concursolutions.com/mobile/ concurmobileredirect.asp?	
Report From	type=exp_rpt_appr&ts=1620906285415&ttoken=cca9f 9f189d11129036376513ea543f1479c0a540cdffc2525	
Report Name	6ecf445c770f66&ctedeepurl=https://dewdfias136.wdf. sap.corp:50201/saml2/idp/sso?saml2sp=https://us.api.	
Report Purpose	concursolutions.com/ saml2&hpo=4&cte=ugvikhkys6zixinpytofekut3ye9ceda	
Requested Am	hvjkhnzq2e5ndii8oj7mfqv8tpfpnd9y8481wmp3cdgmi0 kp8lqrwa%253d%253d%253a1%253aoazmx4wm Click or tap to follow link.	
View Report		

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.

Mana	Manage Single Sign-On				
Enable S	50				
SSO Setting:	SSO Optional	_			
	SSO Optional				
Get SAP	Users may sign in with a password or with SSO.				
Copy or dowr	SSO Required Users must sign in using SSO.	ty Provider (IdP).			
Copy SAP Co					

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 C	hanges					
	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.

Log examples:

View Previous Changes					
Date Changed Change Company Change By	06/07/2022 Add				
Entity ID Name Logout URL					
Metadata					
right sections"	.2' annuling-'200.4''s good anti-pite-'ergo.''ann.okta.com/antikipitetikingkipi' anise.ak-'	-			
And Anglese Angles	ignor seer'aigning's h melon-der'higo/imme.el.org/1000/00/amidmig#'s				
10.1	(1) And (1) and (2) (1) (1) have plot they could be a set of a point of a				
100	and a set of a set of the set of t In a set of the set of t In a set of the set of t				
10	Fig. plant optimization in a constraint of the particular constraint in the principle of	2			
	ОК	٢			

iew Previous Ch	anges	×
Date Changed Change Company Change By	06/08/2022 Edit	
Entity ID Name Logout URL Hidden	Concur Okta ✓	
Previous Values		
Entity ID		
Name	Concur Okta	
Logout URL Hidden		
Metadata		
ring sectors's	A" annulings"(NI-A"))	
real does in pleasers in	her muchle, and the survey servey building at a	1001
and the second	rights Marchicheleganishigant faim protonolingporthomous	1000
the design	a second of the	
1000-0000	henar	
100-07	Delays of concerned the probability cannot promote by the regime con-	
A	And in only only "Summa changes" of a 10 and to be the	100 A. 100 A.
		OK
		UK

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 <u>SSO Overview Guide</u>
- SAP Help Portal SAP Single Sign-On
- SAP Help Portal <u>Configuring AS Java as a Service Provider</u>
- SAP Help Portal <u>Identity Provider Implementation Guide (HTML)</u>

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.

-	Administration -
Company Admin	Company ►
Tools	Request •
Web Services	Travel Admin
Report Admin	Expense •
Authentication Admin fm	Invoice
d)	

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.

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

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://wwwus.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.

	Your IdP's Metadata has been successfully added and sa	ved
Č	You may now test the new SSO connection.	
	OF	٢
Erro	r	;
0	Sorry, we were unable to save your IdP metadata. Please again. If the issue persists, please contact Concur Supp	e try ort with
	correlation_id additional belo	for

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: <u>https://www.concursolutions.com/nui/signin</u>), 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/ initsso?idpid=CLIENT_IDP_ID&spid=SERVICE_PROVIDER_ID&forceauthn=fals e

Example: *https://accounts.google.com/o/saml2/ initsso?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:

Done antation.concursolutions.com AA C	Done antation.concursolutions.com AA 🖒
SAP Concur C	SAP Concur C Sign In
Username, verified email address, or SSO code	ssoadmin@t00653928tex.com
ssoadmin@t00653928tex.com	Sign in with Mobile SSO
Next	Sign in with SAP IAS
Forgot username?	Sign in with your password
∧ ∨ Done	
Passwords	
qwertyuiop	
asdfghjkl	
↔ z x c v b n m ⊗	
123 😂 espaço @ . retorno	

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.

Expense Report Pendin	g Your Approval	
AutoNotification@co To I) If there are problems with how thi	oncursolutions.com s message is displayed, click here to view it in a web browser.	
SAP Concur 💽	SAF	2
Expens	e Report Pending Your Approval	
You have a report pen	ding your approval.	
Report From	SSO Admin	
Report Name	SSO TEST	
Report Purpose		
Requested Amount	2,000.00 USD	
View Report		
This email was sent hy:	SAP Concur - 601 108th Ave NE, Bellevue, WA 98004, USA	

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.

Manag	ge Single Sign-On	
Enable SS	SO	
SSO Setting:	SSO Optional	
Get SAP	SSO Optional Users may sign in with a password or with SSO.	
Copy or down	SSO Required Users must sign in using SSO.	ty Provider (IdP).
Copy SAP Co		

View Previous Changes

This featured 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 <u>SAP Single Sign-On</u>

Ф