Shared: Single Sign-On Overview

Last Revised: November 14, 2020

Applies to these SAP Concur solutions:

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

Table of Contents

Revision History

Date	Notes/Comments/Changes
January 21, 2022	Updated the copyright year; no other changes; cover date not updated
November 14, 2020	Initial publication

SSO Service – Overview

Section 1: Access to the SAP Concur Services

SAP Concur services are web-based applications. As such, there is no software or hardware that a company needs to buy, install, or maintain. To access the services, users navigate to https://www.concursolutions.com through a web browser.

Users can also access SAP Concur services on their iOS and Android devices using the SAP Concur mobile app.

📖 For more information about supported devices, browsers, and best-practice configurations, refer to the *Concur Travel & Expense Supported Configurations* guide.

Section 2: Authentication

By default, SAP Concur services use an SAP Concur login ID and password. The password complexity rules can be configured during implementation or by contacting SAP Concur support.

SAP Concur also supports Single Sign-On (SSO) via the **SAML 2.0** standard.

📖 For more information about SAML 2.0 standard, please visit OASIS SAML Wiki.

NOTE: SAP Concur does ***not*** currently support OIDC (OpenID Connect) for web-based single sign-on.

Section 3: SSO with SAP Concur

SAML SSO involves two parties: an identity provider (IdP) and a service provider (SP). SAP Concur is the service provider. SAP Concur supports any identity provider that complies with the SAML 2.0 standard. For example, the SAP Concur SSO service supports various identity providers such as SAP IAS, Microsoft Azure AD, Okta, Ping Identity, OneLogin, JumpCloud, Idaptive, Google G Suite, ADFS, Shibboleth, VMWare Workspace One, Siteminder – and more.

Unlike previous SAP Concur SSO support, which required the intervention of an SAP Concur technician to activate and configure the service, SAP Concur now provides a Single Sign-On self-service option that has no setup fee associated with it. Customers have access to the Single Sign-On self-service option along with the *Shared: Single Sign-On Setup Guide* which includes step-by-step instructions for activation.

NOTE: While there is no fee associated with the Single Sign-On self-service option, clients can choose the Single Sign-On assisted service option, which provides support for an additional fee.

The activation steps are fully described in the setup guide and recapped below:

1. The company identifies a company admin to act as the SSO admin.
2. The SSO admin accesses the **Manage Single Sign-On** page and obtains the SAP Concur SP metadata.
3. The SSO admin configures the SSO settings at the IdP based on information from the SP metadata.
4. The SSO admin retrieves IdP metadata from the IdP and uploads it to the **Manage Single Sign-On** page.
5. The SSO admin adds a few test users and tests the new SSO connection.
6. After successful testing, the company rolls out SSO to all SAP Concur users.

Section 4: Features

The SSO service provides the features listed below.

Self-Contained SSO Service

The SSO service has been designed for full SAML 2.0 compliance and self-service configuration. It is separate from the legacy SAP Concur SSO stack and can safely be used in parallel to any 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.

Single Sign-On Self-Service Tool

To fast-track the SSO onboarding process and to make long-term SSO management easy and secure, customers can manage their own SSO configuration using the **Manage Single Sign-On** page.

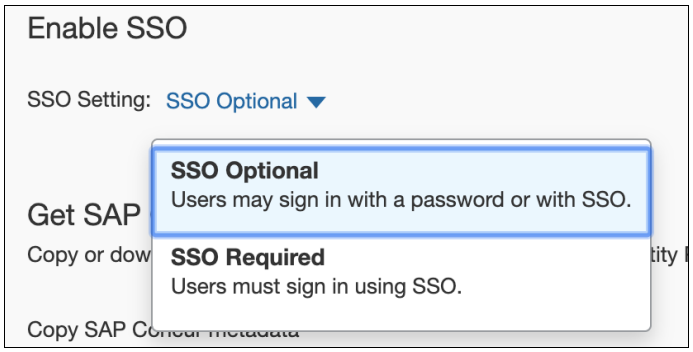
As described in the *Shared: Single Sign-On Setup Guide*, the **Manage Single Sign-On** page is used to:

- Enforce SSO-only sign-in policy for the entire company
- Obtain SAP Concur SP metadata
- Upload IdP metadata to SAP Concur
- Specify the name of each SSO sign-in option
- Specify the URL where users are taken when they sign out of SAP Concur

NOTE: Configuring SSO is a two-part process: uploading SAP Concur SP metadata to IdP and uploading IdP metadata to SAP Concur. The Single Sign-On self-service tool is used only for the second part of the process – uploading IdP metadata to SAP Concur.

SSO Sign-in Policy

The company's SSO admin can manage the SSO sign-in policy on the **Manage Single Sign-On** page using the **SSO Setting** field:



⚠ **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. Users—including TMCs, admins, web services, and test user accounts—will be blocked from signing in to concursolutions.com with their username and password.

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

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

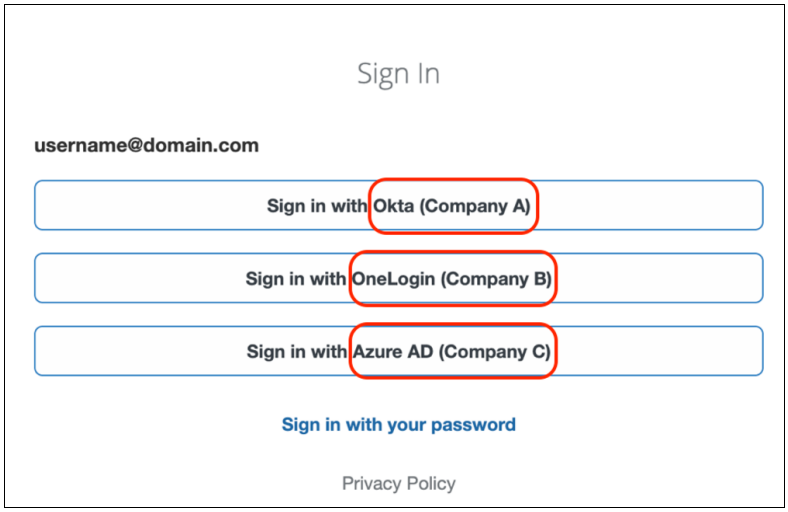
NOTE: Supporting SSO enforcement by user group is targeted as a future enhancement. Currently, a company cannot enforce SSO only a specific group. For example, a company might only want to enforce SSO for "FTE (full-time employee)" group but not "Contractor" group. Currently, if that is the desired outcome, best practice is to add all users to the IdP and use the IdP to manage their access to SAP Concur.

Multiple IdP Support

A company can upload an unlimited number of IdP metadata to SAP Concur through the Single Sign-On self-service tool. That means a company can connect an unlimited number of IdP apps or connectors to a single SAP Concur entity. The SSO

admin can give each IdP a user-friendly name such as "Okta (Company A)" so that users know which one to choose during SP-Initiated SSO sign-in.

EXAMPLE



Encrypted SAML

SAP Concur supports encrypted SAML assertion; the encryption key is available in the SAP Concur SP metadata.

📖 For more information, refer to the *Shared: Single Sign-On Setup Guide*.

IdP-Initiated SSO

IdP-Initiated SSO is supported. With IdP-Initiated SSO, the user signs in to the IdP and then typically clicks a link or tile on the IdP page to access SAP Concur. Optionally, SSO HTTP-Redirect URL (provided by the IdP) can also be used to initiate the sign in.

SP-Initiated SSO

SP-Initiated SSO is supported. With SP-Initiated SSO, the user navigates to concursolutions.com, enters their username, verified email address, or company SSO code, and selects the appropriate SSO option.

The SP-Initiated SSO flow is used by the SAP Concur mobile app to sign in to that platform using SSO.

Mobile SSO

SSO is supported on the SAP Concur mobile app on iOS and Android platforms.

The SP-Initiated SSO flow is used by the SAP Concur mobile app to sign in to that platform using SSO.

📖 For more information on mobile SSO, refer to the *Shared: Single Sign-On Setup Guide*.

Section 5: Implementation Roles and Responsibilities

Roles and responsibilities are shown in the following table.

SAP Concur	Identity Provider	Customer
Provides documentation	Provides documentation on how to set up SSO on the IdP side	Acquires or develops SSO solution that supports the SAML 2.0 standard
Q&A	Q&A	Sets up and self-manages SSO configurations
Troubleshoots if errors are on the SAP Concur side	Troubleshoots if errors are on the IdP side	Finds the correct owner of the problem

Section 6: FAQ

Q: Is "self-signed" certificate permissible in IdP metadata?

A: A public X509 (SSL) key from a certificate issued by a trusted certificate authority must be provided. You should not have this problem if you use one of the commercial identity providers. If you build an in-house SSO, a "self-signed" certificate is permissible if it is within the chain of certificates—for example, if the root certificate generates several sub-certificates that are self-signed.

Q: Does SAP Concur support IP restrictions?

A: While SAP Concur currently provides options for restricting access to the platform to certain IP gateways, it is recommended that you use the IP limiting features of the company's chosen IdP. In this case, users should be required to connect via a VPN to the company network to reach the IdP; server split tunneling should be disabled on the VPN client. It should be noted that restricting access to certain IP gateways can impact performance as users will first be routed to the corporate network and then to the internet rather than via SAP Concur content delivery and acceleration partner.

Q: Does SAP Concur support multi-factor authentication (MFA)?

A: SAP Concur does not provide direct support for MFA. However, most identity providers provide support for MFA, and that functionality can be configured for signing in to SAP Concur using SSO.

Q: Is the SSO service supported in all regions?

A: The SSO service is supported in all data centers: North America (US), EMEA, and China.

Q: Is HMAC-based SSO still supported?

A: It is no longer supported and customers who use HMAC today should be prepared to migrate from HMAC to SAML SSO.

Q: How does SSO enforcement work on the mobile app?

A: The SAP Concur mobile app uses the SP-Initiated SSO flow to sign in using SSO. When the SSO Setting is set to **SSO Required**, as described in the *SSO Sign-in Policy* section above, or when a mobile-specific policy requires SSO, users must use SSO to sign in to the mobile app.

Q: Can I set up multiple IdPs for mobile SSO?

A: Yes. A company can upload an unlimited number of IdP metadata to SAP Concur through the Single Sign-On self-service tool. Each of these configurations will be available from the mobile app.

Q: Does the SAP Concur mobile app support SP-Initiated SSO?

A: Yes. The SP-Initiated SSO flow is used by the SAP Concur mobile app to sign in to that platform using SSO.

 For information, refer to the *Shared: Single Sign-On Setup Guide*.