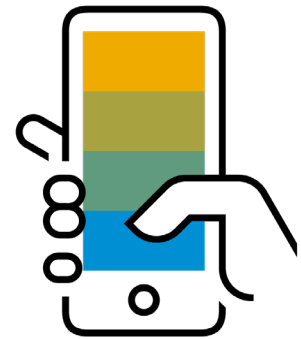


Mobile Authentication Update & Mobile PIN Retirement

Updated: July 2021

As we have been investing to improve the sign-in experience on our web-based solutions, we want to bring those same improvements to the SAP® Concur® mobile app so that users have a consistent, streamlined sign-in experience both at their desk and on the go. Combined, the improvements we're making bring increased reliability, a better user experience, an even stronger security posture, and a consolidated, simpler set of authentication policies.



These enhancements include a two-stage sign-in process to guide users through their options. In addition, we're planning to retire the mobile personal identification number (mobile PIN) sign-in option for the SAP Concur mobile app.

We are extending the release date from the May 2021 mobile release (version 9.91) to the October 2021 mobile release (version 9.96) for our planned changes relating to mobile authentication and retirement of the mobile PIN. We want to provide our customers with more time and for us to make additional improvements to the sign-in experience for users, based on the feedback we have received.

This document and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or noninfringement.

Legal disclaimer

The information in this document is confidential and proprietary to SAP SE or an SAP affiliate company and may not be disclosed without the permission of SAP SE or the respective SAP affiliate company. This document is not subject to your license agreement or any other service or subscription agreement with SAP SE or its affiliated companies. SAP SE and its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation and SAP SE or an SAP affiliate company's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP SE and its affiliated companies at any time for any reason without notice.

The information in this document is not a commitment, promise or legal obligation to deliver any material, code or functionality. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This document is for informational purposes and may not be incorporated into a contract. SAP SE and its affiliated companies assume no responsibility for errors or omissions in this document, except if such damages were caused by SAP SE or an SAP affiliate company's willful misconduct or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Table of Contents

FREQUENTLY ASKED QUESTIONS 4

What is changing?4

Why have you further extended the timeline for when these changes will be made permanent?5

Why are we making these changes?5

What are some of the improvements that have been made to the web experience?6

What actions do I have to take as an administrator?6

What actions will users have to take, and what are a user’s sign-in options?6

What is the auto sign-in policy and new mobile authentication lifetime policy?7

How can we set up biometrics so that it allows our users to sign in more easily?8

Can we turn off mobile PIN earlier?8

How are we communicating to users?8

How does a mobile release work?8

What is the mobile deprecation policy?8

How do I find out which of my users are using the mobile PIN?9

Does this impact the web user experience?9

How might this impact my SSO set up?9

What if our organization enforces SSO on the web, has mobile enabled, but has not set up SSO on mobile?9

Does this change have any impact on backend processes, reporting, and similar areas?9

Will the changes be localized into my users’ languages?9

What will happen to the “Forgot Concur Mobile PIN” page in the Profile?10

What materials can help my users reset their password, troubleshoot sign-in, and more?10

How can I drive more adoption of the SAP Concur mobile app?10

Does this impact the Triplt® mobile app?10

APPENDIX: Single Sign-On (SSO) Options..... 11

SSO Overview 11

SAML 11

SSO Flow 11

Current Mobile Sign-In Options..... 13

Upcoming Mobile Sign-In Changes..... 14

FREQUENTLY ASKED QUESTIONS

What is changing?

We are improving our sign-in experience for users, bringing recent enhancements from the web experience to the SAP Concur mobile app. These enhancements include a two-stage sign-in process to guide users through their options.

In addition to these enhancements, we're retiring the mobile personal identification number (mobile PIN) sign-in option for users to sign in to the SAP Concur mobile app. Users who use mobile PIN should be prepared in advance to use an alternative sign-in method, such as username and password or single sign-on (SSO). Any user has the ability to set up mobile PIN, and so we are communicating to all customers in advance of this change.

As part of this effort, we plan to bring verified e-mail address and company SSO code as sign-in options to the web experience, and this is planned to be implemented in two releases, separated by a period of time to allow customers to make any required changes and conduct change management.

For detailed screenshots, please view the release notes: [Professional](#) | [Standard](#).

Initial Release November 2020 mobile release (Version 9.86)	Final Release October 2021 mobile release (Version 9.96)
<ul style="list-style-type: none">• Users are now presented with the same sign-in screens (formatted for mobile) as those currently presented to users when signing in to the web experience• Mobile PIN will not be a sign-in option• When available by policy / device, Android supports biometric options (already supported on iOS)• Auto sign-in policy replaced with mobile authentication lifetime policy• Users will have an option to use the old sign-in experience, which will continue to support mobile PIN	<ul style="list-style-type: none">• Extended from May 2021 mobile release (Version 9.91)• The option to use the old sign-in experience will no longer be available in this version, and users must sign in using one of the supported options:<ul style="list-style-type: none">○ Username and password○ Mobile SSO○ SAP Concur SAMLv2 SSO• Remember, starting with mobile version 9.87, our mobile deprecation policy, will require users to upgrade to at least the third most recent version.

Why have you further extended the timeline for when these changes will be made permanent?

We are extending the release date from the May 2021 mobile release (version 9.91) to the October 2021 mobile release (version 9.96) for our planned changes relating to mobile authentication and retirement of the mobile PIN. We want to provide our customers with more time and for us to make additional improvements to the sign-in experience for users, based on the feedback we have received. The improvements that we are planning include:

- Helping users learn what options they have to sign in to the mobile app, how to sign in, and how often their organization requires them to sign in
- Keeping users signed in by encouraging use of biometrics such as fingerprint TouchID and face recognition integration*
- Updating our existing documentation and training materials available to users
- Improving responses to user questions and feedback in the app stores

We understand the impacts of adjusting our timeline, but we have listened to our customers and users and this extension will allow us to create a better sign-in experience in preparation for mobile PIN retirement. If you have already communicated these changes to your users, that is fine. Users who are already using the updated experience are all set! Throughout this time, you should continue to encourage users to only use the updated sign-in experience.

* Where supported by device, user settings, and company phone policy. These are now supported by iOS and Android.

Why are we making these changes?

As we have been investing to improve the sign-in experience on our web-based solutions, we have brought those same improvements to the SAP Concur mobile app so that users have a consistent, streamlined sign-in experience both at their desk and on the go.

Combined, the improvements we have made bring increased reliability, a better user experience, an even stronger security posture, and a consolidated, simpler set of authentication policies both for our customers and for our development teams.

The mobile PIN functionality and its associated policy settings are redundant with the standard SAP Concur solutions password. We are retiring the mobile PIN to provide a single sign-in experience, reducing sign-in issues, and making resetting passwords simpler. That means fewer questions around sign-in issues to administrators.

Additionally, with innovations around biometrics such as fingerprint TouchID and face recognition integration, our users gain even more convenience in the sign-in experience along with improved security for our customers. The SAP Concur mobile app now uses the same reset flow as in the web experience of SAP Concur solutions and follows the same troubleshooting tools.

What are some of the improvements that have been made to the web experience?

Our unified sign-in experience will add support to sign in with not only a username, but also a verified e-mail address or SSO code, as is supported by the SAP Concur mobile app.

Other recent changes in the web sign-in experience have added a two-stage sign-in process, to help guide the user through their available sign-in options. Additionally, customers may set up multiple SSO options for their users.

What actions do I have to take as an administrator?

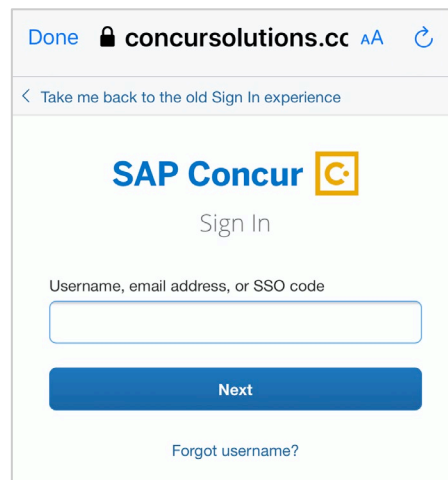
These changes will happen automatically, and no action is required. Customers do not need to make any configuration changes as a result of these enhancements unless you only use mobile PIN. This will have no impact on a customer's SSO set up, but users may see two SSO options if you have both SAP Concur SAML v2 (SAML v2) and Mobile SSO set up. You may want to remove one of those options.

If you haven't already, we recommend that you communicate to your mobile users that they will no longer be able to use their mobile PIN if they have set one up and should use alternative sign-in options. You can use [this e-mail template](#) as a starting point and share [this end user FAQ](#).

What actions will users have to take, and what are a user's sign-in options?

Since updating the SAP Concur mobile app with the initial release, users who use mobile PIN have either chosen an alternative sign-in method or to use the old sign-in experience, which will continue to support mobile PIN until the final release. A user can confirm whether they have a mobile PIN set up by going to Profile > Concur Mobile Registration. If the user sees the "Forgot Concur Mobile PIN" item in the left-hand menu under "Other Settings", a mobile PIN is set up.

With the final release, the only supported SAP Concur mobile app sign-in methods are:



Without SSO:

- **Username/password:** For companies that allow their users to sign in to SAP Concur solutions on the web and mobile using a username and password, after mobile PIN is removed, users may continue to sign in to both web and mobile with their username and password.
 - Admins can verify if employees can "change password" through their profile. If not, create a Support Case to make a configuration change.

With SSO: For more information, [see the appendix](#).

- **Mobile SSO:** For companies configured to support Mobile SSO, after mobile PIN is removed, users may continue to use Mobile SSO to sign in to both mobile and web (through Company SSO code).
 - Users can find your Company SSO code by going to Profile > Profile Settings > Concur Mobile Registration.
 - Admins can verify if you already have Mobile SSO enabled by looking at Mobile Registration in your profile. If you do, then no action is necessary. If you do not, create a Support Case with a Mobile SSO URL to make a configuration change. Also, if desired, you can have the SSO “enforced” on mobile which will eliminate the password option.
- **SAP Concur SAML v2:** For companies configured to support SSO through SAP Concur SAML v2, after mobile PIN is removed, users may continue to use SAP Concur SAML v2 to sign in to both mobile and web.
- **Both Mobile SSO and SAP Concur SAML v2:** For companies configured to support Mobile SSO for mobile sign-ins and SAP Concur SAML v2 for web sign-ins, users may have both options presented to them on both mobile and web.

Note: If possible, the sign-in unification process will try to combine these SSO options into a single option, so that users are presented with only that single option.

Once signed in, and when/where supported, a user can set up biometrics such as fingerprint TouchID and/or face recognition so that they can use these methods to sign in again quickly in the future.

With the final mobile release, all users will be forced to upgrade to at least version 9.89, which contains these changes.

What is the auto sign-in policy and new mobile authentication lifetime policy?

Set per organization, when enabled and after initial authentication, auto sign-in policy kept the user signed in on the SAP Concur mobile app. They were never again prompted for credentials to sign in. In the initial mobile release, this policy was replaced with the mobile authentication lifetime policy, which is disabled by default. This effectively provides the exact same experience users have today, never requiring re-authentication unless the user manually signs out.

If you want to require re-authentication on a more frequent basis to improve security, adjust the mobile authentication lifetime setting to allow your users' authenticated session to continue for a period of time (15 minutes up to 120 days). Customers can adjust this value by submitting a case to SAP Concur Support.

How can we set up biometrics so that it allows our users to sign in more easily?

This feature is on by default, so, in most cases, action is not required. If you want to make adjustments, submit a case to SAP Concur Support requesting to allow users to sign in using biometrics (where/when available by device).

Can we turn off mobile PIN earlier?

If a customer wants to force users to stop using mobile PIN prior to these changes, the only available option is for customers with Mobile SSO to force users to sign in with SSO. Submit a Support Case to get this process started.

How are we communicating to users?

We are planning to have a dialog in the SAP Concur mobile app informing users of the upcoming changes start with the October 2020 mobile release, one month prior to initial launch. We will also post additional messages throughout the period leading up to the final release.

How does a mobile release work?

We release our updated SAP Concur mobile app to the respective app stores at the end of the month. Then each app store processes and approves the app for release. This takes a variable amount of time depending on each app store.

As an example, the November 2020 mobile release (9.86) was released to users in early December 2020.

What is the mobile deprecation policy?

We implemented a mobile deprecation policy in April 2020 to improve security for the SAP Concur mobile app and provide additional resources for greater innovation to our customers and users.

Since implementing the policy, we gained greater insights into actual usage and determined that the vast majority of users — approximately 98% — consistently update to the most recent three versions. To further improve security and availability of resources, we updated our policy to support the most recent three versions instead of seven with the first 2021 mobile release (9.87). This change also closer aligns the SAP Concur mobile app with other mobile apps in the SAP family.

We plan to use this policy to enforce the mobile authentication updates.

A deprecation policy for mobile apps is routine for enterprise and personal mobile applications, and users are accustomed to updating their apps on a regular basis. The vast majority of SAP Concur mobile app users update the app frequently and were not be affected by this change in policy.

For full information on this update, [review this FAQ](#).

How do I find out which of my users are using the mobile PIN?

We have no method to provide you which users or how many of your users have set up a mobile PIN. Our authentication process treats a mobile PIN the same as a user's password, which is why it is not possible. There is no standard report that provides this information.

A user can confirm whether they have a mobile PIN set up by going to [Profile > Profile Settings > Concur Mobile Registration](#). If they see the "Forgot Concur Mobile PIN" is in the left-hand menu under "Other Settings", a mobile PIN is set up.

We recommend communicating to all users, noting that this change only impacts users who have set up a mobile PIN. You can use [this e-mail template](#) as a starting point and share [this user FAQ](#).

Does this impact the web user experience?

No. However, users of the web experience will also be able to use either their verified e-mail address or Company SSO code rather than only their username. We are planning to unify the sign-in experience across mobile and web.

How might this impact my SSO set up?

This will have no impact on a customer's SSO set up; however, on mobile, users may see two options if you have both SAP Concur SAML v2 and Mobile SSO set up. You may want to remove one of those options. Where possible, the sign-in unification process will try to combine these SSO options into a single option, so that users are presented with only that single option. For more information, [see the appendix](#) or reach out to SAP Concur Support to make a configuration change.

What if our organization enforces SSO on the web, has mobile enabled, but has not set up SSO on mobile?

In this scenario, your users are only using mobile PIN to sign in to the SAP Concur mobile app. Your organization will have to either enable Mobile SSO or allow your users to sign in on mobile using their username and password. Very few customers have this set up.

Does this change have any impact on backend processes, reporting, and similar areas?

This change is not planned to impact any backend processes or reporting. It is only our backend that handles authentication on mobile that will use the same methods as the web authentication.

Will the changes be localized into my users' languages?

The changes will adhere to the [SAP Concur Supported Languages](#).

What will happen to the “Forgot Concur Mobile PIN” page in the Profile?

Our plan is to remove this page in the profile once we have fully retired support for mobile PIN.

What materials can help my users reset their password, troubleshoot sign-in, and more?

Users can find materials on how to sign in to the SAP Concur mobile app, reset their passwords, and more through [our mobile admin toolkit](#). We recommend the [user FAQ on how to sign in](#). For detailed screenshots of these changes, please view the release notes: [Professional](#) | [Standard](#).

If you have disabled the option for users to reset passwords and would like to re-enable it, please open a case with SAP Concur Support.

How can I drive more adoption of the SAP Concur mobile app?

The SAP Concur mobile app is a simple tool that lets users manage expenses, travel, and invoices right from their mobile device. Road warriors can stay productive from anywhere and managers can easily track spend. [The SAP Concur mobile app admin toolkit](#) will help you learn more about, set up, and drive adoption of the SAP Concur mobile app.

Does this impact the Triplt® mobile app?

No. Triplt app sign-in methods are not impacted as a result of this change.

APPENDIX: Single Sign-On (SSO) Options

SSO Overview

Customers who want to enable users to securely authenticate with multiple applications and websites with just one set of credentials (username and password) use single sign-on (SSO).

SSO can be used to authenticate on the web (concur solutions.com) and on the SAP Concur mobile app.

There are three key participants in the SSO flow within SAP Concur solutions:

1. The User Agent = the actual end user who tries to sign in on the web (concur solutions.com) or the SAP Concur mobile app.
 - a. The end user is usually an employee of an organization that has integrated with SAP Concur solutions.
2. The Service Provider (SP) = in this case, SAP Concur solutions
3. The Identity Provider (IdP) = in this case the IdP the customer (company) is using; as an example, let's assume the company's IdP is OKTA.

SAML

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers. In this case, SAML is the mechanism on how Company Acme OKTA (IdP) and SAP Concur solutions (Service Provider) communicate to exchange the user credentials in a secure manner.

SSO Flow

At a high level, the way these three participants interact is as follows:

1. The website (concur solutions.com) or the app first checks to see whether the user has already been authenticated with the Service Provider (in this case, SAP Concur solutions), if the user has been authenticated, then the user can access the site or the app.
2. If the user has not been authenticated, then the website (SAP Concur solutions) sends the user to the IdP sign-in page, in this example Company Acme is using OKTA.
3. In the IdP sign-in page, in this example Company Acme OKTA page, the user enters their username/password that they use for corporate access.
4. The service provider requests authentication from the IdP the company uses (in this example OKTA). The IdP verifies the user's identity and notifies the service provider.

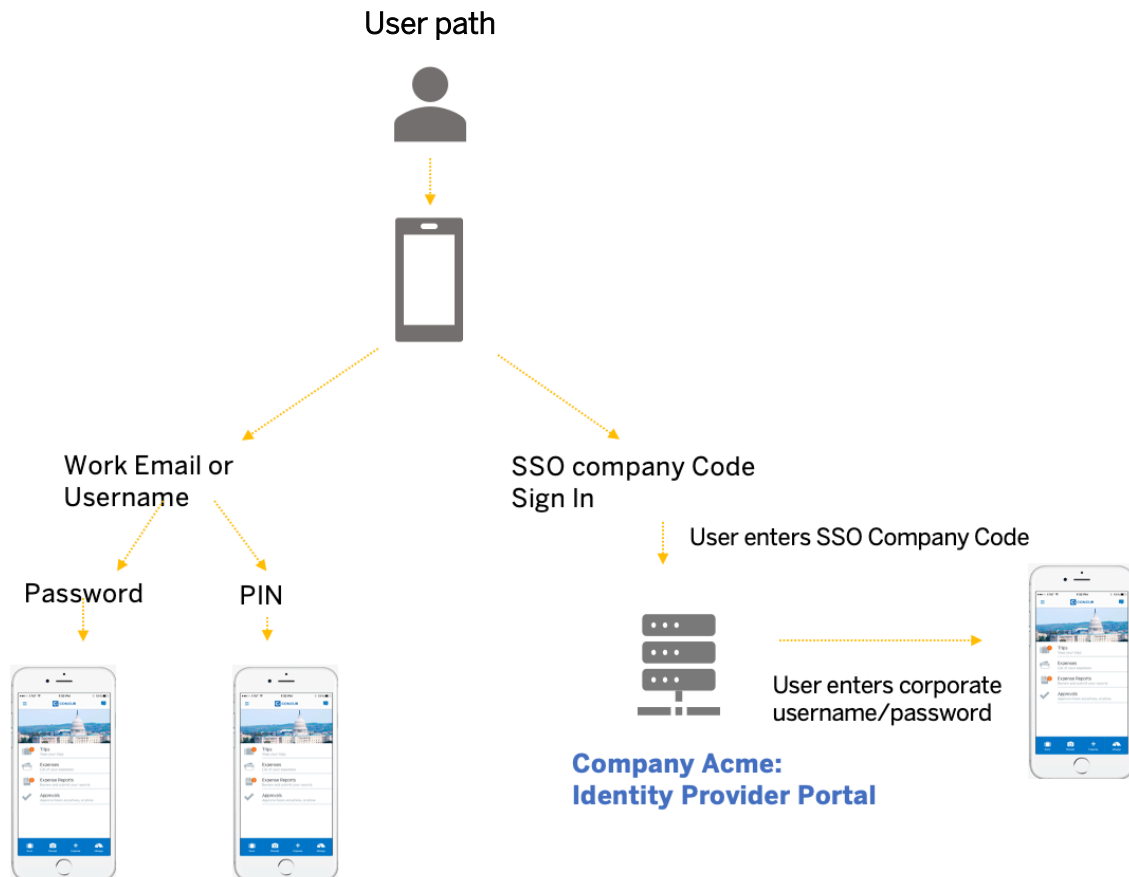
5. SAP Concur solutions (service provider) passes the authentication data to the website (concur solutions.com) and returns the user to that site.

Current Mobile Sign-In Options

Based on each company settings, IdP, and SAML version the user experience on how a company employees' sign in to SAP Concur web or app might vary. Currently, users can sign in to the SAP Concur mobile app using:

- Mobile PIN
- Username/Password
- Mobile SSO company code, using their SSO credentials

Here is an overview of how users can sign in to the SAP Concur mobile app today:



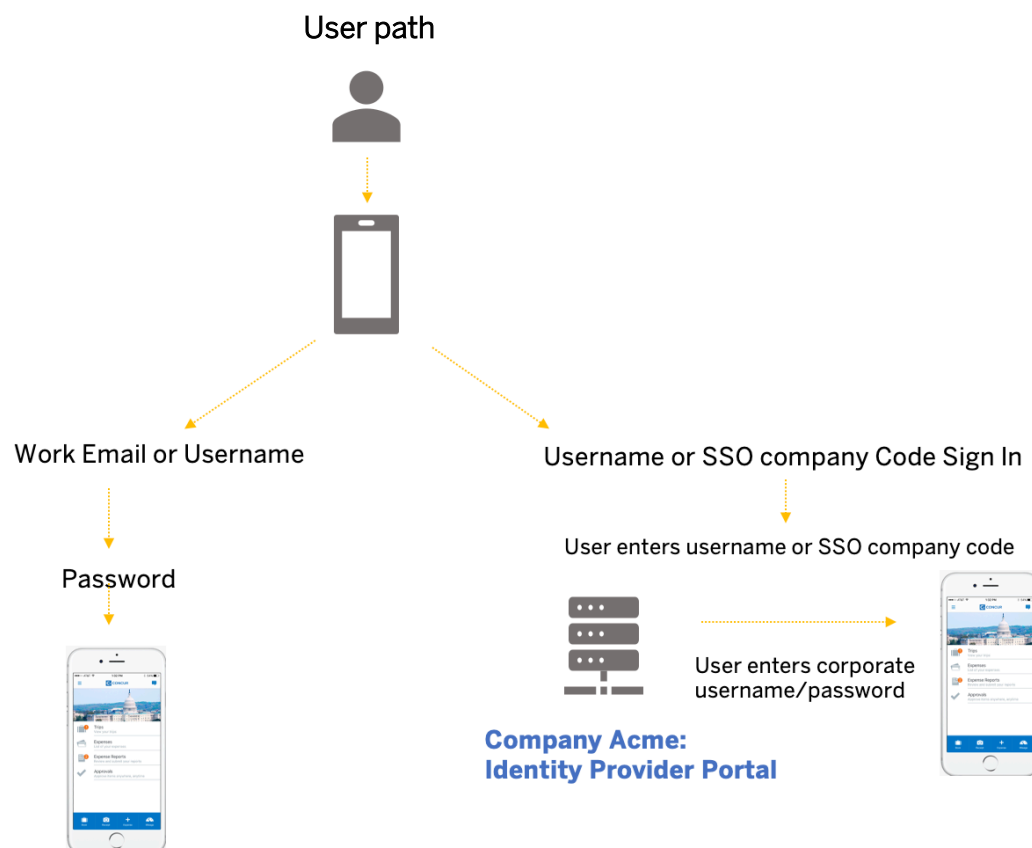
Upcoming Mobile Sign-In Changes

We started to make changes to the way users sign in during 2019. The changes were initially visible on the web (concur solutions.com), and those same changes are now coming to the SAP Concur mobile app.

The process of unifying the web and mobile sign-in experiences also unifies the options for users to sign in. After the deprecation of mobile PIN, users must sign in using one of the supported options. The user impact will vary based on how a company is configured to allow their users to sign in. After these changes are complete, users can sign in to the SAP Concur mobile app using:

- Username/Password
- Mobile SSO company code, using their SSO credentials
- SAMLv2 SSO

Here is an overview of how users would sign in after the changes are complete:



Learn more at concur.com

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.