SAP Concur

Concur Sign In Security Changes -
Two-Factor Authentication (2FA)
and New Password Policy UI (Sign In Settings UI)

External FAQs

Updated October 13, 2023

What is happening on October 18?

To enhance the sign in security of all SAP Concur users, two-factor authentication (2FA) will be required on concursolutions.com. **All users who are using basic authentication (Concur username and password) on web or mobile will need to set up 2FA at that time.**

In addition to 2FA, there will be a new password policy enhancement; any company whose password policies don't meet the minimum standard will automatically be updated to the new minimum standard on October 18. **At that time company Admins will have access to the new password policy UI (this is found in the "Sign In Settings" under Authentication Admin menu) but Users will NOT have to take any action.** Beginning November 15, all users' password policy will be checked at the time of sign in and Concur will enforce them to reset with the new policies provided in the new UI.

Both 2FA and the New Password Policy UI will occur in phases on the same date.

2FA

Phase 1 (no email required) – **October 18 through November 14**

- All users will be able to setup 2FA without an email address.
- Although a valid email address will not be required, it is highly recommended that during this time each user works on ensuring they have a valid email address. This will be critical to have November 15 in Phase 2.
- Once valid credentials are entered, a prompt will occur to start the setup process for 2FA.

Phase 2 (email enrollment) – **November 15**

- Unless disabled by the company admin via the password policy user interface*, all users must have a valid email address on file in order to ensure they can receive a link to set up 2FA in their email. **(This means that email verification is preferred and optional, but it is NOT required for 2FA to work.)**
- *Company Admins can disable the email requirement at their discretion through the password policy user interface.

- If there is no valid email address on file, the user must reach out to their admin or Concur Support.
- Email address does not need to be verified. Any valid email address entered will suffice.
- There will be an option for Admins to opt out of the email requirement, but 2FA will still be required for all users. Please use this option at your own discretion as you are disabling the additional layer of security for your user accounts. The ability to opt out of the email requirement will be available November 8.

New Password Policy UI (Sign In Settings UI)

Phase 1 – October 18

- The new password policies will launch with defaults in place. Please note that this has NO impact to the users but Admins will now have access to the UI so they can be prepared for enforcement of new policies in Phase 2, beginning November 15.

Phase 2 – November 15

- The password policy for all users will be checked at the time of sign in and Concur will enforce a reset with the new policies provided in the UI.

What is Two-factor Authentication (2FA)?

Two-factor Authentication is an authentication process that requires two different authentication factors to establish identity. This means the user will have to prove their identity in two different ways in order to establish access. To increase security, more software websites are requiring their users to use 2FA in order to sign in. 2FA gives your organization the ability to help safeguard your information.

Why is 2FA being required in order to sign in to Concur?

2FA is a layered approach to securing your users accounts and the data they contain. When 2FA is enabled, after entering the correct password, the user is prompted to provide the second factor of authentication, which could be a one-time code generated by a mobile authenticator app. This second step verifies the user’s identity before the service grants the user access. 2FA greatly enhances the security of online accounts and is a core component of a strong identity and access management policy. While important, usernames and passwords are vulnerable to credential stuffing, password breaches and can be stolen by third parties. Enforcing the use of an 2FA significantly reduces the risk of unauthorized access and increases confidence that your accounts will stay safe from cyber criminals.

Is there an option to disable the 2FA feature?

No, there is no option to disable the 2FA feature. If you attempt to sign in using a Concur username/password on Web or Mobile, you are required to use 2FA.

Will there be any in product messaging on 2FA?

Yes, on September 19, when Admins sign in, they will see a pop-up message about the 2FA requirement and the FAQs will be referenced for more information. End users will see a similar message in early October when they sign in.

What will the end-user experience when signing in to Concur under 2FA?

After you choose an authenticator allowed by your company IT policy, you will be asked to enter the 6-digit code generated by the authenticator app. This will be required for every subsequent login. Please note that a browser version is available for users on corporate phones with security limitations on downloading new authenticator apps. If downloading authenticator apps on the corporate phone are not permitted, user is free to download an authenticator app on their personal mobile device as well. The following is a list of authenticator apps: Google, Microsoft, Twilio, Duo,

Why is 2FA being required in order to sign in to Concur?

2FA is a layered approach to securing your users accounts and the data they contain. When 2FA is enabled, after entering the correct password, the user is prompted to provide the second factor of authentication, which could be a one-time code generated by a mobile authenticator app. This second step verifies the user’s identity before the service grants the user access. 2FA greatly enhances the security of online accounts and is a core component of a strong identity and access management policy. While important, usernames and passwords are vulnerable to credential stuffing, password breaches and can be stolen by third parties. Enforcing the use of an 2FA significantly reduces the risk of unauthorized access and increases confidence that your accounts will stay safe from cyber criminals.

Why will SAP Concur be enforcing new password policies ?

We are raising the benchmark on minimum password requirements and setting new baseline to ensures your company have the best security posture against cyberattacks.

What will the new password policies include?

The following are the new SAP Concur minimum, maximum, and default values for passwords. Admins will be able to see these details in the Sign In Settings UI on October 18. Enforcement of these new password policies will begin November 15.

Password Strength (required password elements)	Minimum	**Maximum**	**Default**
Password length	8	255	8
Upper (A-Z) and lower (a-z) case letters required	True/False	True/False	True
Number (0-9) required	True/False	True/False	False
Number or special (non-alphabetic) character required	True/False	True/False	True

Special (non-alphanumeric) character required	True/False	True/False	False
Password Change (password reset and expiration)	**Minimum**	**Maximum**	**Default**
How often users are allowed to change their password	Never	Anytime	Anytime
Password reset allowed once per day	True/False	True/False	True
Number of password changes required before reusing a password	0	20	5
Passwords expire	True/False	True/False	True
Period after which password expires	1 month	1 year	6 months
Account Lockout (criteria for locking an account after failed attempt(s))	**Minimum**	**Maximum**	**Default**
Number of failed sign in attempts allowed before an account is locked	3	20	5
Sign in failure window (elapsed time before restarting the failure count)	10 min	240 min	10 min
Permanent lockout	True/False	True/False	False
Duration of account lockout	30 min	1440 min	120 min
Session Timeout (sign users out after a period of inactivity)	**Minimum**	**Maximum**	**Default**
Display sign out warning (display a warning x minutes before user is signed out due to inactivity)	0	15	15
Sign out an idle user (number of minutes a user can be idle before being automatically signed out)	10	120	30
Other settings	**Minimum**	**Maximum**	**Default**
Hide the "Forgot Username" link	True/False	True/False	False
Hide the "Forgot Password" link	True/False	True/False	False
User must change their password on first sign in	True/False	True/False	True

Why has SAP Concur decided to roll this out in such an urgent fashion with little notice?

SAP Concur is releasing 2FA in October as that is when it will be technically ready and to ensure we are adding additional security to our customer's accounts. Security is one of SAP's top concerns and we want to ensure our customer data is safe.

There are more than 24 billion username and passwords on the dark web as of June 2022. Hackers are getting smarter every day and username/passwords are vulnerable to risk of unauthorized access, brute force attacks, and various cyber threats, such as phishing, credential stuffing, and password breaches. This can lead to sign in credentials being stolen by third parties. Enforcing the use of a 2FA significantly reduces the risk of unauthorized access and increases confidence that your accounts will stay safe from cyber criminals.

Our rollout may be fast, and while not perfect, slowing down the release is not an option. We are an agile company and are still working through the rollout pieces based on customer feedback. It costs SAP millions of euros to deal with 1 security incident and per the ISBN Security team we need to lower the risk of the incidents. Our reputation is a valuable asset, and if a security incident happens, it can tarnish our image in the eyes of our customers, partners, and the general public. We know that your confidence in our ability to safeguard your data is crucial. We want to reassure you that we are investing in stronger security measures and continuously monitoring and improving our systems.

Who is NOT impacted by the Two-factor Authentication (2FA) change?

Users that authenticate via Single Sign On (SSO) will not be impacted. More information on SSO can be found here: https://www.concurtraining.com/customers/tech_pubs/Docs/_Current/SG_Shr/Shr_SG_SSO_Mgmt.pdf

Is ConcurGov impacted by 2FA?

No, ConcurGov will not be impacted until they move to their new UI.

Is there any configuration the end user needs to activate in order to set up 2FA?

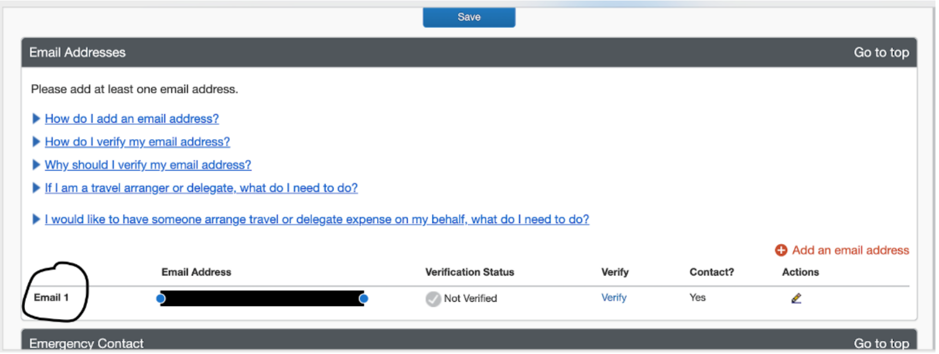
No configuration/activation is required prior to the 2FA rollout feature on October 18. When the end user signs in for the first time after the 2FA rollout feature using a Concur username/password, they will be automatically asked to enroll in 2FA and set up an authenticator app to generate the 6-digit authentication code needed. Once they are set up for 2FA, all subsequent sign ins will require them to enter the 6-digit authentication code generated by their authenticator app. (The authenticator app should be one in line with direction from your IT department.)

Is this also applicable to test entities (Production Sandbox Environments)?

If you are using Concur username and password to sign in to a Production Sandbox Environment then yes, you will be required to enroll in 2FA. Each 2FA is unique to each unique account. So, if you have 2 separate accounts - you will be required to enroll in 2FA for both the accounts.

What action do I need to take to ensure smooth onboarding onto 2FA?

During Phase 2 (November 15) a valid email address will be required (unless disabled as noted in Question 1 of this FAQ) . You may verify now (**before** November 15) if you have an up-to-date EMAIL1 in your Profile Settings, preferably with "Verification Status" of "Verified". To check this – sign in to Concur → Profile Settings→ Email Addresses.



Please add at least one email address.

- How do I add an email address?
- How do I verify my email address?
- Why should I verify my email address?
- If I am a travel arranger or delegate, what do I need to do?
- I would like to have someone arrange travel or delegate expense on my behalf, what do I need to do?

	Email Address	Verification Status	Verify	Contact?	Actions
Email 1	[redacted]	Not Verified	Verify	Yes	✎

Will I be required to enroll in 2FA for Mobile login?

Mobile sign-in using a username and password will also require 2FA. If you have already enrolled in 2FA while signing in with a username/password on Web, you do not need to set up 2FA again. Instead, you will use the same authenticator app to generate the 6-digit code necessary to sign in to the Concur Mobile App. If you have not yet enrolled in 2FA, you will be required to set up 2FA as part of the sign in to the Concur Mobile App.

Will push Notifications be supported?

At this point in time, push notifications and SMS are not supported. You will need to download an Authenticator app and copy the 6-digit code generated in the app into the Concur sign in screen.

Do I need to have a corporate phone to set up 2FA?

There is no limitation on using a corporate device or your personal device. It is up to you where you want to download the authenticator app and add your SAP Concur account for 2FA.
If you do not have a phone or do not want to download an authenticator app to your mobile phone, you can also use authenticator apps on your browser. For example: For Google Chrome, https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai. For Microsoft Edge, https://microsoftedge.microsoft.com/addons/detail/authenticator-2fa-client/ocglkepbibnalbgmbachknglpdipeoio

If I do not choose to use my corporate or personal phone for 2FA, How do I use the browser option?

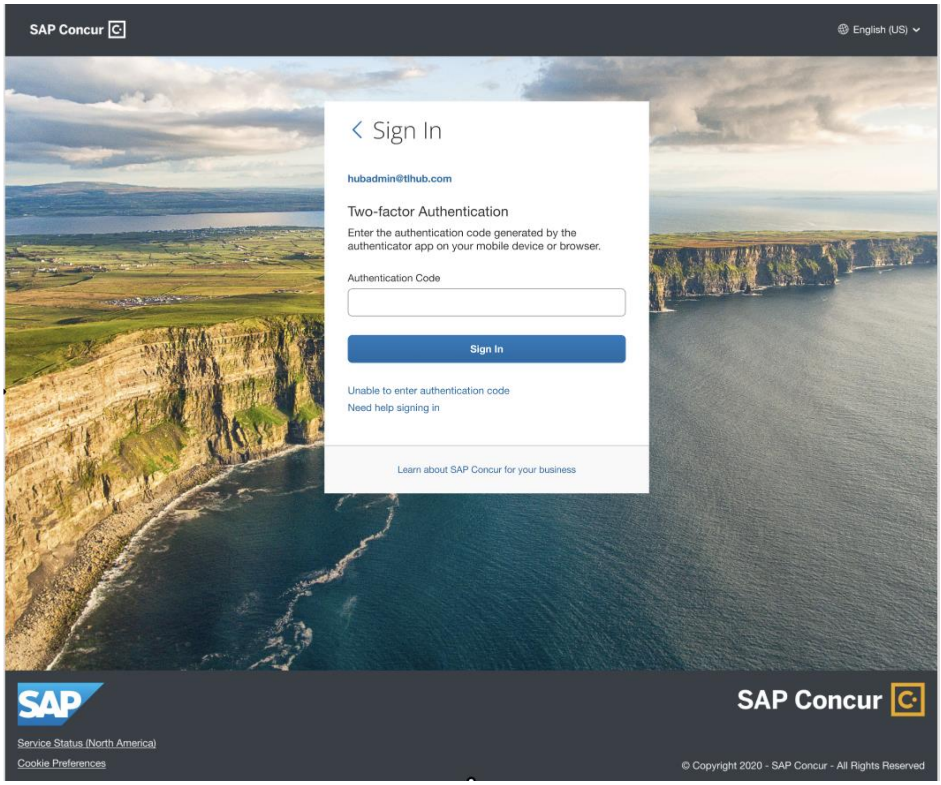
Details will be given in the setup guide available on Oct 18 on
https://help.sap.com/docs/SAP_CONCUR_SECURITY/b92b8c7fc75a4c8faf62a6584077b022/26c1f2d1d2d34f2d8cf8099ffc9aa965.html
but if you do not have a phone or cannot download an authenticator app to your mobile phone, you can also use authenticator apps on your browser. For example: For Google Chrome, https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai. For Microsoft Edge, https://microsoftedge.microsoft.com/addons/detail/authenticator-2fa-client/ocglkepbibnalbgmbachknglpdipeoio

Which authenticator apps can I use for 2FA?

Any authenticator app using a TOTP algorithm will work. The following are some examples of authenticator apps that can be used for 2FA. Please choose one that is approved by your IT department.
Twilio Authy Authenticator, Duo Mobile, Microsoft Authenticator, Google Authenticator

What if I lose my phone or change phones?

If you no longer have access to the Authenticator app configured for 2FA with concursolutions.com, you must reset your 2FA configuration. To begin the process of resetting your 2FA configuration, click the "Unable to enter authentication code" during the sign in flow, when you are asked to enter your 6-digit authentication code.


SAP Concur
English (US)
Sign In

hubadmin@tlhub.com

Two-factor Authentication

Enter the authentication code generated by the authenticator app on your mobile device or browser.

Authentication Code

Sign In
Unable to enter authentication code
Need help signing in
Learn about SAP Concur for your business
SAP
SAP Concur
Service Status (North America)
Cookie Preferences

© Copyright 2020 - SAP Concur - All Rights Reserved

Click "Send" on the next dialog. An email will be sent to the email address specified as Email1 in your Profile Settings.

Click “Return to Sign In" to return to the first page of sign in.

Check your inbox for an email with subject "Two-factor Authentication Reset Request". Click the "Reset two-factor authentication" button. Then perform the same steps you followed when first setting up 2FA.

Where can I get step by step instructions on how to enroll in 2FA?

On October 18, an End User Set Up Guide will be available on Concurtraining.com.

Where can I get more help if I have trouble scanning the QR code?

You can find this information in the End User User Set Up Guide, available October 18 on Concurtraining.com.

Where can I get more information on how to reset 2FA?

You can find this information in the End User User Set Up Guide, available October 18 on Concurtraining.com.

Are there other methods of one-time password? (OTP)?

No other OTP methods (SMS/OTP/Push notifications/email) are supported at the moment.

We have a small portion of our user base without a mobile phone. Can OTP also be sent via email?

No. The only supported method is an authentication app via the phone or a browser extension.

How does this impact delegates?

Since delegates sign in as themselves, the impact is the same.

What if I am a delegate, will this impact my ability to switch profiles?

No.

What if the person that delegated to me did not sign up for 2FA yet? Will this impact my ability to log in?

No.

Once I have 2FA, how often do I need to authenticate?

You will need to authenticate every time you sign in. In the event your session timed out, you would need to input your username and password again and will need to provide your authentication code.

What if I experience issues with 2FA?

Please click on ' Need Help Signing in' to use the 2FA set up guide. If you still run into issues, please reach out to Concur Support. For issues with the authenticator app, please reach out to your company IT team or the Authenticator App Support. Concur Support will not be resolving issues with your authenticator app.

Is there a fee associated with your Support in the setup process?

There are no fees specifically related to the setup process for 2FA in Concur.

Can we receive the 6-digit code through email?

No, this is not supported. In case you do not have a mobile phone, you can choose to use the Authenticator App on your browser. See an example of Google Authenticator browser extension- https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai for Google Chrome

For phase 2 of 2FA, my email address is not unique. The same email address is being used in other accounts. Will I run into an issue? How will Concur determine the right account to send the code?

No issues in using the same email for other accounts. As long as you have updated email1 in Profile settings and you have access to that email, you will receive an email.

When will 2FA capability be available for testing?

It won't be made available prior to launch expected on October 18.

Will there be a configuration option to exclude certain accounts from 2FA?

No, there is no user level opt out option.

If the profile is on "Is Test User", will it still require 2FA?

Yes, it will still require 2FA as it is applicable to the entire entity.

Can we enable 2FA for one test user id and have the others disabled?

The answer to this is in line with the previous two questions above. 2FA is required at the organizational level to enhance security for all users uniformly. Enabling 2FA for a single user while keeping it disabled for others is not possible.

My company uses BOTS automation for sign in, how can we comply with this requirement?

Automation BOTS can be used for malicious purposes, such as attempting to gain unauthorized access to user accounts. This can pose a security risk both to the user employing the bot and to SAP Concur. Since BOT automation is being done on the customer end, it is up to the customer to decide /implement how they can work around with 2FA in place for SAP Concur. There may be automation scripts online on how to automate with 2FA in effect though it could prove to be challenging.