

New User Password and Two Factor Authentication (2FA): Set Up Guide for End Users

(October 2023)

In addition to a username and password, all SAP Concur profiles for concursolutions.com are required to enroll in 2FA. By setting up 2FA, you add an extra layer of security to your SAP Concur account sign in. For example, you first enter your login and password, and when prompted, you then type a dynamically generated verification code provided by an authenticator app or sent to your phone. If a user has multiple username and password sign-in credentials for SAP Concur solutions, the enrollment process must be completed for each set of credentials. Each account will have a unique 2FA associated with it.

- I. **Download An Authenticator App**
- II. **Set Your Password**
- III. **Set Up 2FA**
 - A. **Complete 2FA Setup With QR Code**
 - B. **Complete 2FA Setup Manually (Without Using QR Code)**
- IV. **Troubleshooting**
- V. **Appendix**

I. Download An Authenticator App

Users must have an authenticator app installed on a mobile device, or as a browser plug-in, to set up and use 2FA. It is recommended to have this ready before logging into SAP Concur for the first time.

You are free to use most authenticator apps. Two apps that are known to work well are [Microsoft Authenticator](#) and [Google Authenticator](#). We have found that the iOS Authenticator does **not** work well with Concur.

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. Examples: [Google Chrome Authenticator](#) or [Microsoft Edge Authenticator](#).

NOTE: Some companies have restrictions or guidance about which applications (including third-party authenticator apps) their users can install on company devices. You might need to confirm which authenticator apps are approved for your company by checking with your company's IT department. SAP Concur does not have access to information about your company's specific authenticator app requirements. (If you are using a personal device, this should not be an issue.)

II. Set Your Password

When logging in for the first time, enter the username you have been given, click **Next**, and utilize **Forgot Password**.

The image displays two sequential screenshots of the SAP Concur sign-in interface. The first screenshot shows the 'Sign In' page where the user has entered the email address 'hubadmin@tlhub.com' in the 'Username, verified email address, or SSO code' field. A blue 'Next' button is visible below the field. There is also a 'Remember me' toggle, a 'Forgot username' link, and a 'Need help signing in' link. The second screenshot shows the 'Sign In' page where the password field is empty and the 'Next' button is visible. It also includes 'Forgot password' and 'Need help signing in' links. Both screenshots have a footer link: 'Learn about SAP Concur for your business'.

An email will be sent to the email address associated with the user account with a link to set the password. Click the link and follow the steps to set your password.

NOTE: The email will come directly from **@concursolutions.com**. If you did not receive the email, check your spam folder or, for company email addresses, contact your company's IT department.

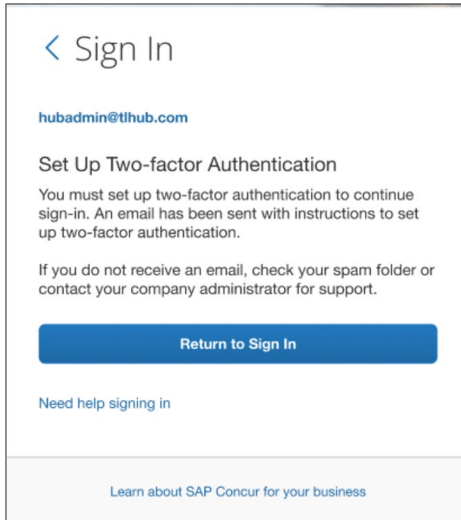
III. Set Up 2FA

1. Log in with the newly set password.
2. The following message is presented:

"You must set up two-factor authentication to continue sign-in. An email has been sent with instructions to set up two-factor authentication.

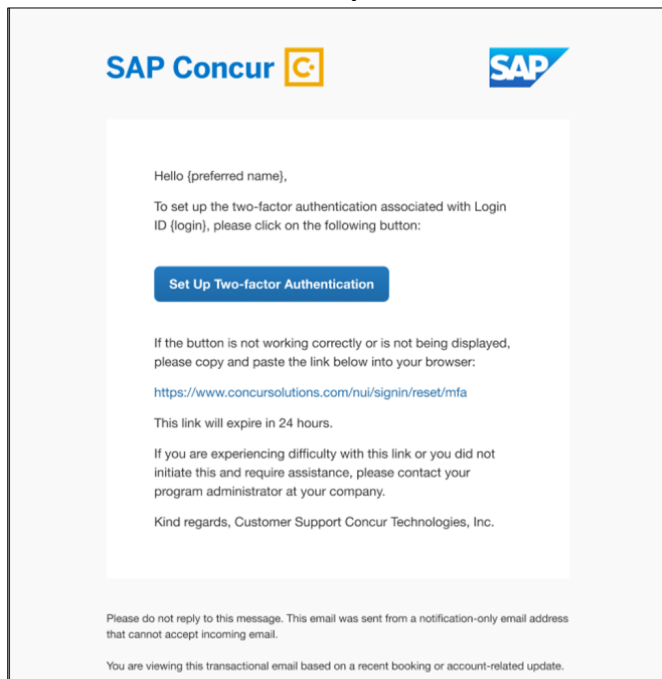
If you do not receive an email, check your spam folder, or contact your company administrator for support."

Click **Return to Sign In**.



NOTE: The email will come directly from @concursolutions.com. If you did not receive the email, check your spam folder, or contact your company's IT department.

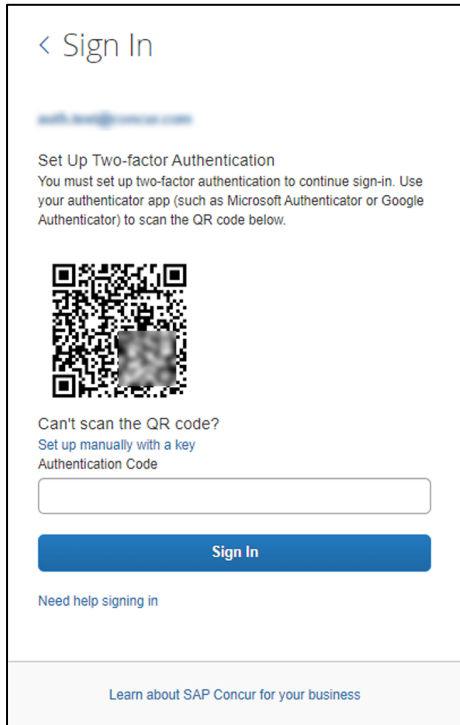
3. In that email, click **Set Up Two-Factor Authentication**.



4. On the SAP Concur sign-in page, enter your username and password again and click **Next**.

A. Complete 2FA Setup with QR Code

5. The **Set Up Two-Factor Authentication** page is presented.



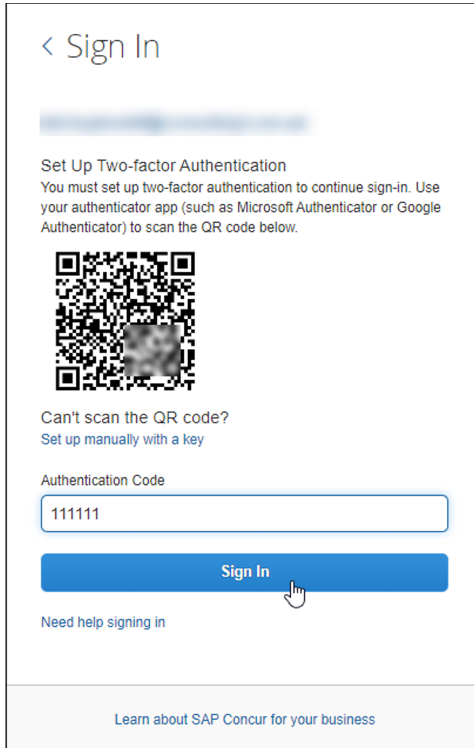
Open the authenticator app on your mobile device now and use that to scan the QR code on the **Set Up Two-Factor Authentication** page to begin setting up 2FA for SAP Concur solutions. If you have chosen to use an authenticator app in a web browser instead, you will use that now.

6. Follow the steps or prompts from the authenticator app to generate a 6-digit code. These steps will vary depending on which authenticator app you are using.

- Typically, you will need to add a name or other identifier for the account the key is associated with, for example "SAP Concur". Remember, if you have multiple SAP Concur accounts - perhaps through multiple organizations - you should include something in the name to differentiate them, for example "SAP Concur ABC Company".
- If you are using Google Authenticator, choose the Time Based option.

NOTE: SAP Concur does not have information about which authenticator app you use and cannot provide steps for this process. Consult the authenticator app user guide or your company's IT department if you require assistance setting up the authenticator app or generating the 6-digit code.

7. Enter the 6-digit authentication code generated by your authenticator app and then click **Sign In**.



B. Complete 2FA Setup Manually (without scanning QR Code)

If you are unable to scan the QR code on the Set Up Two-Factor Authentication page - for example, if you are unable to use the camera on your device to scan the QR code - you can use the manual process.

Follow **Set Up 2FA - steps 1 through 4** laid out above first.

5. The **Set Up Two-Factor Authentication** page is presented. Click **Set up manually with a key**.



6. Record the key.

< Sign In

Set Up Two-factor Authentication
You must set up two-factor authentication to continue sign-in. Use your authenticator app (such as Microsoft Authenticator or Google Authenticator) to scan the QR code below.

Can't scan the QR code?
Key: [REDACTED] 07Y2BELQVAP4DTQ2KG

Authentication Code

[Sign In](#)

[Need help signing in](#)

[Learn about SAP Concur for your business](#)

NOTE: If you are setting up 2FA on your mobile device or in a web browser, you can use the icon to the right of the key to copy the key.

Can't scan the QR code?
Key: A [REDACTED] Y2RCOHX0XSFGQERP Click to copy

Authentication Code

[Sign In](#)

[Need help signing in](#)

7. Follow the steps in your authenticator app to enter the key manually. These steps vary depending on which authenticator app you are using.

- Typically, you will need to add a name or other identifier for the account the key is associated with, for example "SAP Concur". Remember, if you have multiple SAP Concur accounts -

perhaps through multiple organizations - you should include something in the name to differentiate them, for example "SAP Concur ABC Company".

- If you are using Google Authenticator, choose the Time Based option.

NOTE: SAP Concur does not have information about which authenticator app you use and cannot provide steps for this process. Consult the authenticator app user guide or your company's IT department if you require assistance setting up the authenticator app.

8. After you enter the key manually and follow the steps in your authenticator app, the authenticator app will generate a 6-digit code. Enter the code into the **Authentication Code** field on the **Set Up Two-Factor Authentication** page.

9. Click **Sign In**.

IV. Troubleshooting

Most Frequent Issues

Issue 1: I tried to reset my password, but never received an email

This could be, but not limited to, the following reasons:

- The email went to your Junk or Spam folder
- Your company has not added **@concursolutions.com** to the allowed list of email domains*
- You entered an incorrect username/log in ID
- Your email was added to a suppression list, likely due to an out of office setting/automatic reply*

*If you suspect either of these is the issue, contact your IT department.

Issue 2: I'm receiving the error: "The authentication code you entered is incorrect" when using 2FA

There are a few potential reasons why you might receive the error: "The authentication code you entered is incorrect" when setting up two-factor authentication (2FA). Below are a few of the most common scenarios that might cause this error.

Scenario 1: User has not added their SAP Concur account on an authenticator app or browser extension and is entering the manual key in the Authentication Code field.

The **Authentication Code** field is where you should enter the six-digit code generated by the Authenticator app AFTER you have added the account in the authenticator app using the key provided by SAP Concur.

To set up 2FA, you should download an authenticator app (if you don't have one already) and add an account within the authenticator app, using either the QR code or the manual key. After the account is added, the authenticator app will display a six-digit code that you should copy and enter in the **Authentication Code** field in the SAP Concur Sign In page.

Scenario 2: The code you are trying to enter has already expired.

The authentication code is time-based and expires every 30 seconds. Please make sure that the authentication code entered is still active in the Authenticator app.

Scenario 3: The user has simultaneously opened the 2FA enrollment page in more than one browser window and added the account using the QR code or secret key from the first window that was opened.

Every time you open the Enroll in 2FA page, we initialize the 2FA secret on the database and a unique QR code and secret key are displayed. However, we only honor the latest initialized secret. Therefore, if you opened the Enroll in 2FA page in two different browsers or in a browser and in the mobile app, the only QR code and manual key that will work will be the ones from the page that was opened last. If that is the case, you should delete the account you had created in the authenticator app or extension, and add a new account using the latest generated QR code or manual key.

Scenario 4: User is entering a space between the first three and last three digits of the six-digit code.

There should not be any space in the six-digit authentication code field. Remove any spaces, then try again. Be sure that the corrected code you are entering is still the active code in the authenticator app and not expired.

Scenario 5: The time on the user's mobile device is not synchronized.

Please follow the steps below to fix this issue:

iOS devices:

1. On your iPhone, go to Settings
2. Scroll down, then select General
3. Scroll down, then select Date & Time
4. Select Set Automatically to true
5. Close and reopen the Authenticator app
6. Enter the authentication code shown on the app

Android devices:

1. Go to the main menu of the Authenticator app
2. Select the three dots in the top right corner
3. Select Settings
4. Select Time correction for codes
5. Press Sync now
6. The message displayed will confirm if the time has been synchronized or if it was already correct
7. Close and reopen the Authenticator App
8. Enter the authentication code shown on the app

If you are using an Android device and the Google Authenticator app, please follow these steps:

1. Go to the main menu of the Google Authenticator app
2. Click the three dots in the upper right corner
3. Select Settings
4. Select Time correction for codes
5. Select sync now
6. The message displayed will confirm if the time has been synchronized or it was already correct
7. Close and reopen the authenticator app
8. Enter the authentication code in to SAP Concur again

Scenario 6: The time on the user's laptop or computer is not synchronized.

When using the Google Authenticator extension for Google Chrome, first be sure you have pinned the Authenticator app so it is more easily accessible. Once pinned, follow these steps:

1. Click the Authenticator icon to open the extension
2. When the Authenticator opens, click the cog wheel icon in the upper-left corner to open settings
3. Click Sync Clock with Google
4. Click Allow to give permission to "Read and change your data on www.google.com on the pop-up if shown (Optional)
5. The message displayed will confirm if the time has been synchronized

Still Receiving Errors

If none of the above scenarios fix your issue, please try to delete the account you had created in the authenticator app or extension and add a new account to troubleshoot the issue. In addition, you can also try to uninstall the authenticator app and install it again.

If the error persists, please create a case with SAP Concur Support, providing the troubleshooting steps you tried, the name of the authenticator app or extension that you are using and a screenshot of the error.

V. Appendix

Why 2FA?

Here at SAP Concur, we are committed to providing a secure and trustworthy platform for all our users.

In today's digital landscape, security is of utmost concern, and we are committed to safeguarding your sensitive information and personal data. Two-Factor Authentication is a robust and proven method that significantly enhances the security of your accounts. Reputations are valuable assets, and if a security incident happens, it can tarnish an image in the eyes of 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 by bring 2FA to your accounts. There are more than 24 billion usernames 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, various cyber

threats, such as phishing, credential stuffing, password breaches and can be 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.

What is 2FA?

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 a 2FA significantly reduces the risk of unauthorized access and increases confidence that your accounts will stay safe from cyber criminals. Two-factor authentication (2FA) is safer than basic authentication (usually just a username and password) because it adds an extra layer of security to the login process. Basic authentication relies solely on something the user knows (the password), while 2FA requires more than that (a second factor) for authentication.