

Two Factor Authentication (2FA) - Setup Guide for End Users

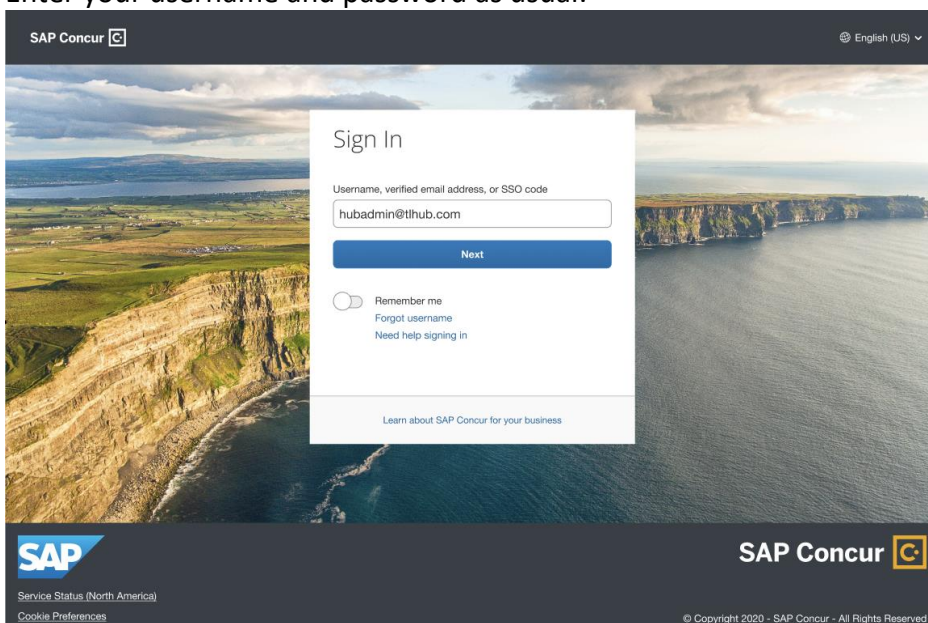
By setting up 2FA, you add an extra layer of security to your SAP Concur account sign in. Once 2FA has been set up, you will first enter your SAP Concur password. When prompted, you will provide a verification code that is dynamically generated by an authenticator app or sent to your phone.

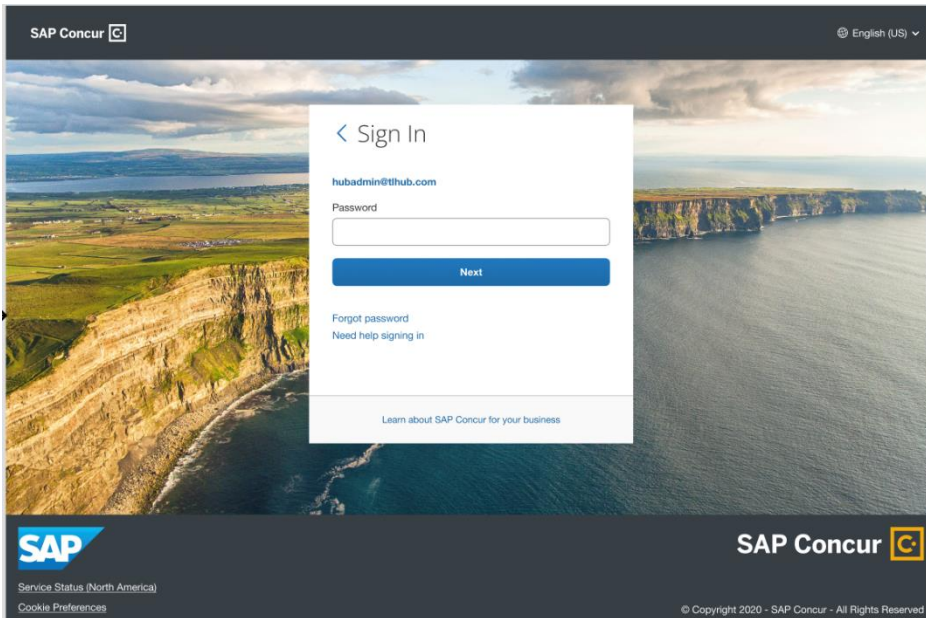
This Setup Guide is divided into 4 sections:

1. Enrollment
2. Trouble with Scanning QR Code
3. Reset 2FA
4. Phase 2 Enrollment (includes how to disable email requirement)

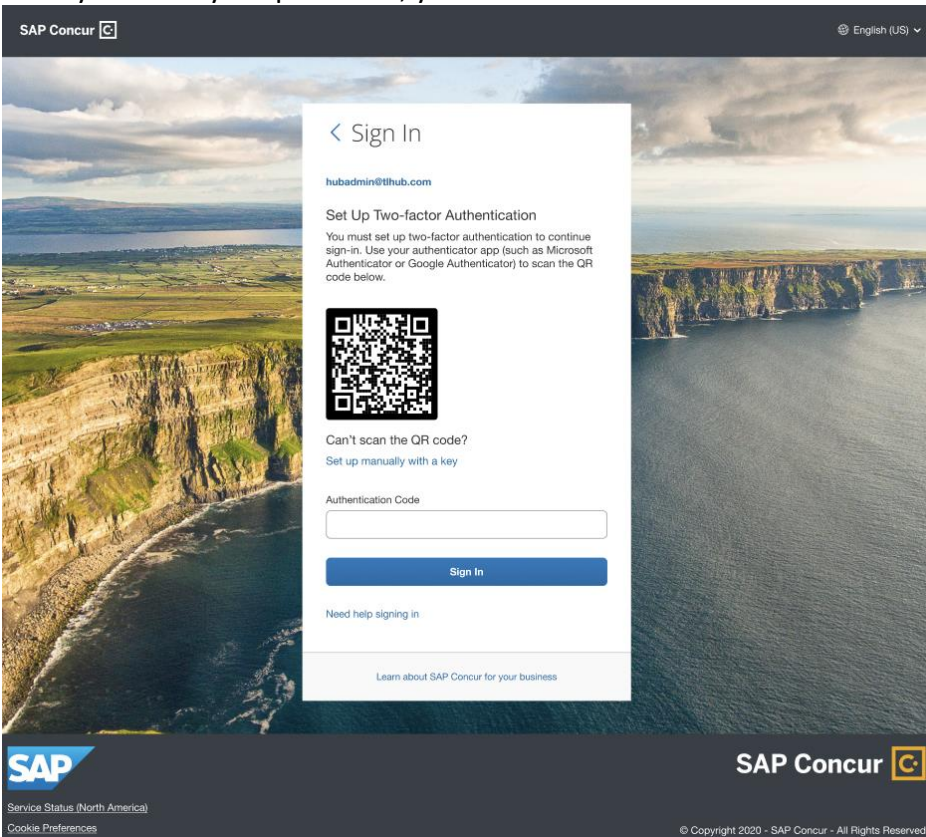
Section 1: Enrollment

1. If you are using Concur username and password to login into concursolutions.com for your account via Web or Concur Mobile- you are required to enroll in 2FA. This is applicable to both Production and Test accounts. Each account will have a unique 2FA associated. Therefore, if you use multiple different Concur accounts to login using username/password- you are required to set up 2FA for all these accounts.
2. Enter your username and password as usual.





3. After you enter your password, you will see a new screen with a QR code presented.



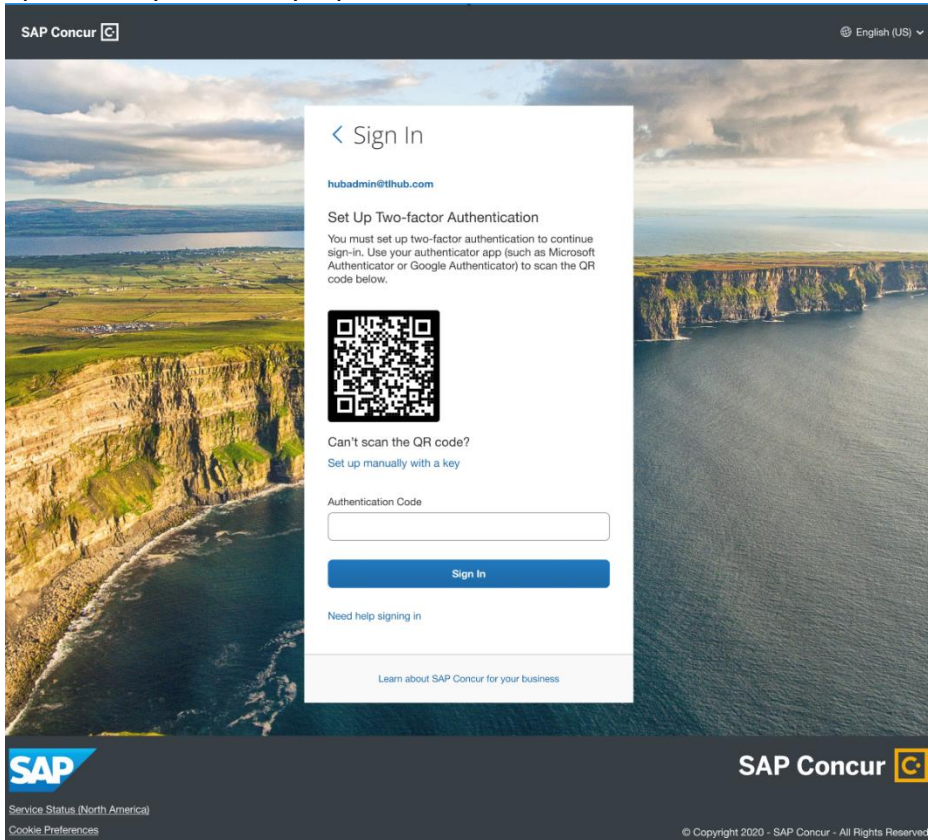
4. Download an authenticator app of your choice to your mobile phone. You can use a corporate phone or use your personal device. You are free to use any authenticator app, such as [Twilio Authy Authenticator](#), [Duo Mobile](#), [Microsoft Authenticator](#), [Google Authenticator](#).
5. Go to the App Store or Google Play Store and search/download the authenticator app you wish to use.
6. If you do not have a phone or do not want to download an authenticator app to your mobile phone, you can use an authenticator app on your browser such as [Google Chrome](#) and [Microsoft Edge](#).

To better understand how your browser will scan the QR code, please reference this [YouTube video](#) to see how the web browser authenticator works.

7. Click on 'Add account' or '+' sign or whichever button is available in the authenticator app for you to add a new account.
8. Once the QR code scanner starts on the app, scan the QR code shown on the Concur sign in page. This will add your SAP Concur account to the authenticator app.
9. Once this is done, right below the account, a 6-digit code will be generated.
10. Before the six-digit code expires, please copy that code into the 'Authentication Code' field on the SAP Concur sign in page and hit Sign In.
11. You are now successfully signed in.

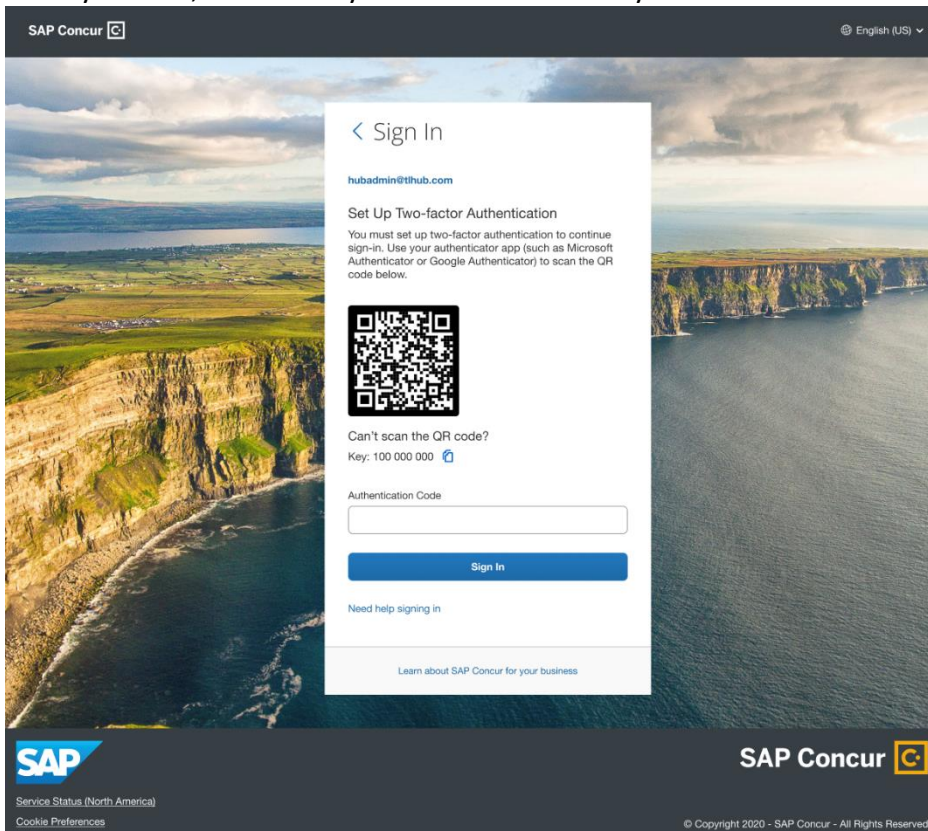
Section 2: Having trouble with scanning QR code?

1. If you are unable to scan the QR code, you can manually add your account. Click the 'Set up manually with a key' option.



The screenshot displays the SAP Concur Sign In interface. At the top left, the SAP Concur logo is visible, and at the top right, the language is set to English (US). The main content area features a white sign-in card with a back arrow and the text '< Sign In'. Below this, the email address 'hubadmin@thub.com' is displayed. The card prompts the user to 'Set Up Two-factor Authentication' and explains that they must use an authenticator app to scan a QR code. A QR code is provided for scanning. Below the QR code, there is a link that says 'Can't scan the QR code? Set up manually with a key'. Underneath, there is an 'Authentication Code' input field and a blue 'Sign In' button. At the bottom of the card, there is a link for 'Need help signing in' and a footer link for 'Learn about SAP Concur for your business'. The background of the page is a scenic image of a coastline with cliffs and a body of water. The bottom of the page contains the SAP logo, 'Service Status (North America)', 'Cookie Preferences', the SAP Concur logo, and the copyright notice '© Copyright 2020 - SAP Concur - All Rights Reserved'.

2. Once you click, a secret key should be visible on your screen.



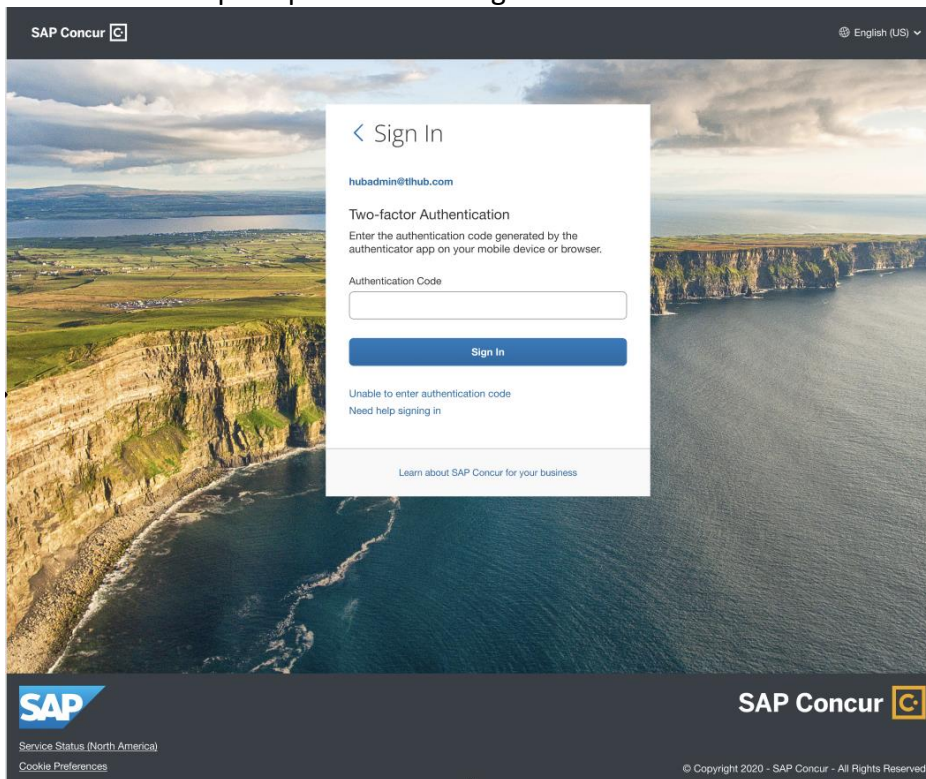
3. Next, go into your authenticator app on your phone or browser. Based upon what authenticator app you are using, there should be the option 'Enter a setup key' for Google Authenticator or 'Add account' for MSFT Authenticator - Click 'Add account' → Other account → 'Enter code manually'.
4. There will be two fields visible on the Authenticator app: Account and Secret Key. In the Account field enter your SAP Concur account username shown on your SAP Concur screen (i.e., hubadmin@concur.com).
5. In the Secret Key field, enter the secret key shown on the SAP Concur page. For example: 123 456 789.
6. Once the account is added, beneath the SAP Concur account in your authenticator app, a six-digit code will be generated.
7. Before the code expires, enter the code into the 'Authenticator Code' field on your Concur screen.

Section 3: Reset 2FA.

Do you have a new device or did you lose your device and need to reset 2FA? Do you want to switch your Authenticator app and use a different one?

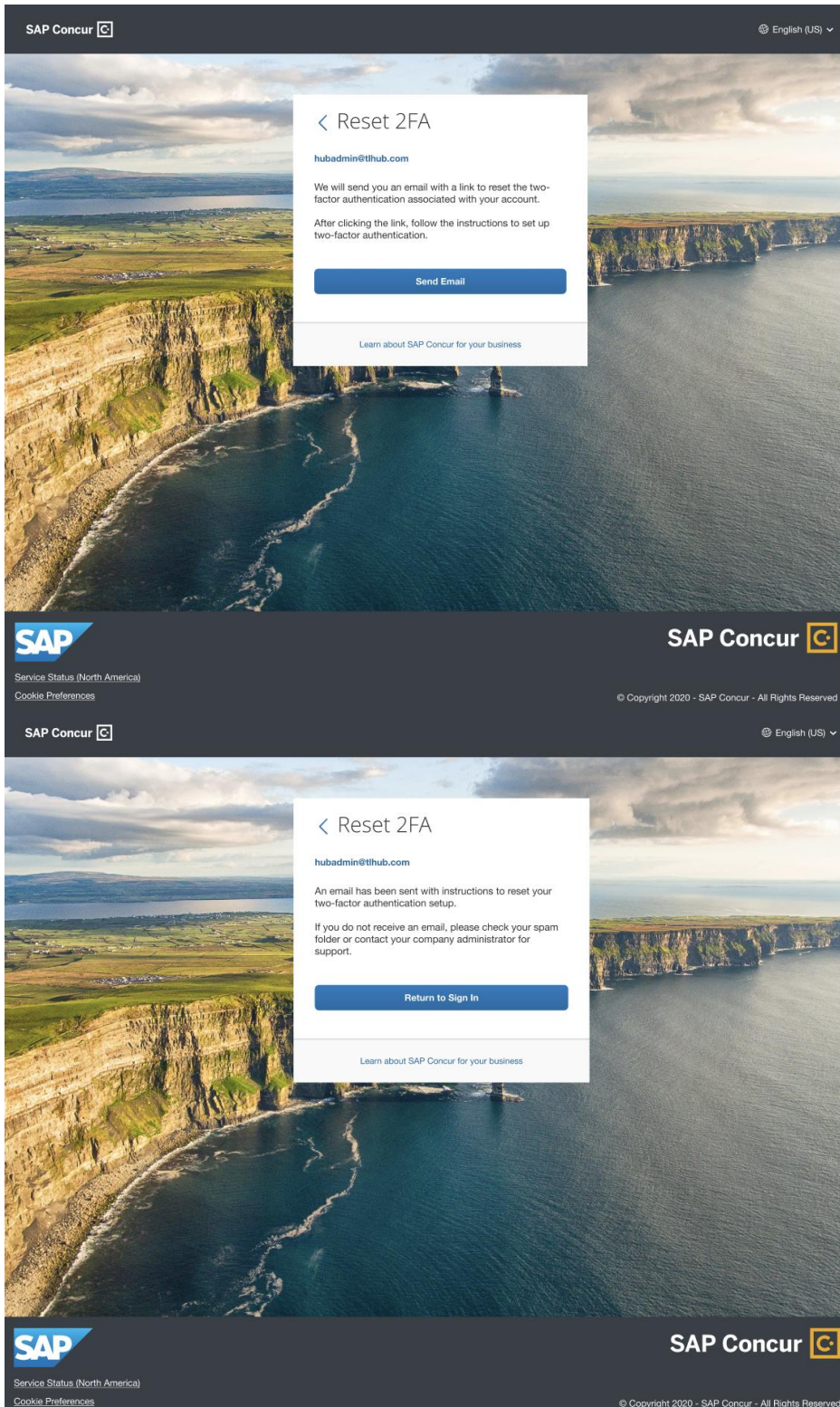
Prerequisite: You have previously enrolled in 2FA.

1. Enter your username and password.
2. You will now be prompted for a six-digit authentication code.

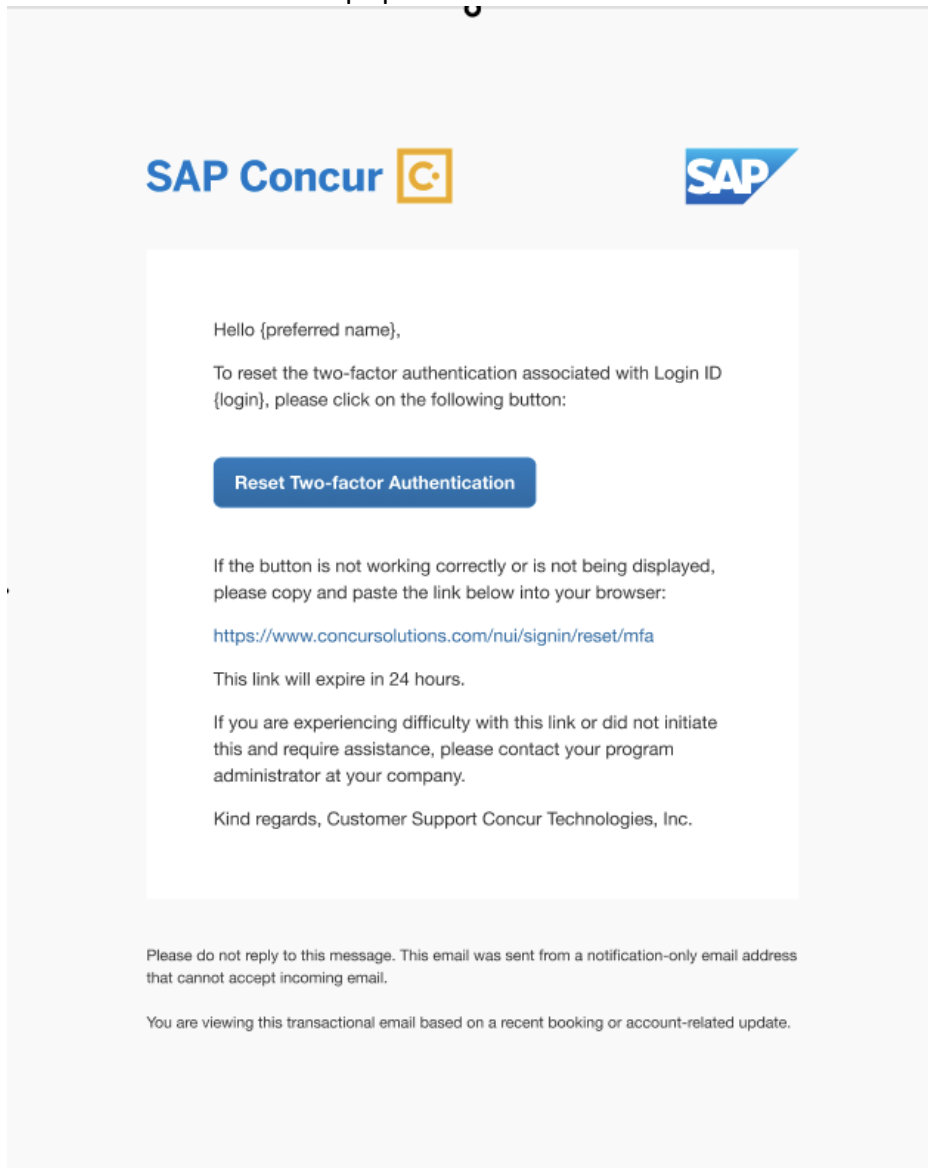


3. If you need to reset your 2FA for a new device OR you lost your phone and need to enroll in 2FA again for your replacement device OR you wish to switch to a different Authenticator App, click ' Unable to enter authentication code'.

4. You will receive an email with a link to reset 2FA. Please note: This email will be sent to



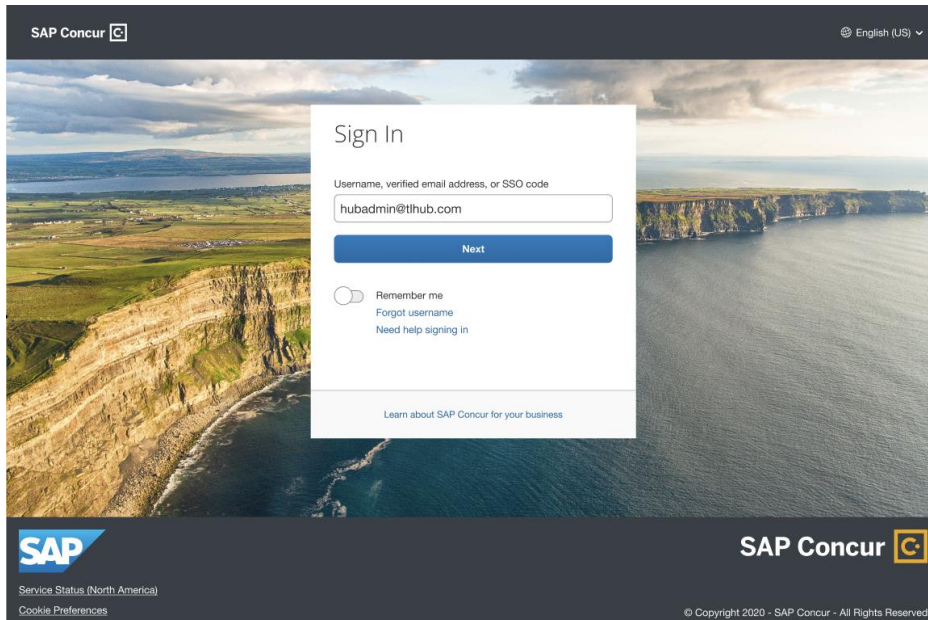
5. To check whether your email is updated in your Profile. You need to sign in to your SAP Concur account and go to: Profile>Profile Settings>Personal Information>Email addresses.
6. If you did not update email1 in your Profile and are locked out, please contact the Admin of your company and ask them to update the email for you. Once updated, click 'Unable to enter authentication code' to trigger the email one more time.
7. If you receive an email, it will contain a link to reset 2FA. Click the link to receive the QR code. Follow the same steps provided in the 2FA Enrollment section to set up 2FA.



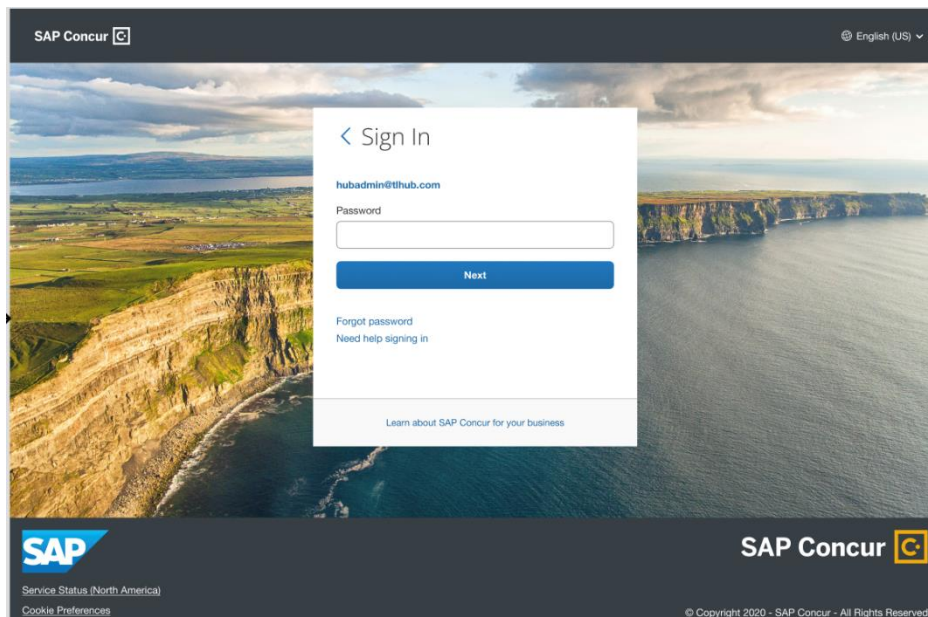
Phase 2 Enrollment starting November 15

Enrollment

1. If you have not enrolled in 2FA for your accounts using an SAP Concur username and password, enter your Concur username and password as usual.

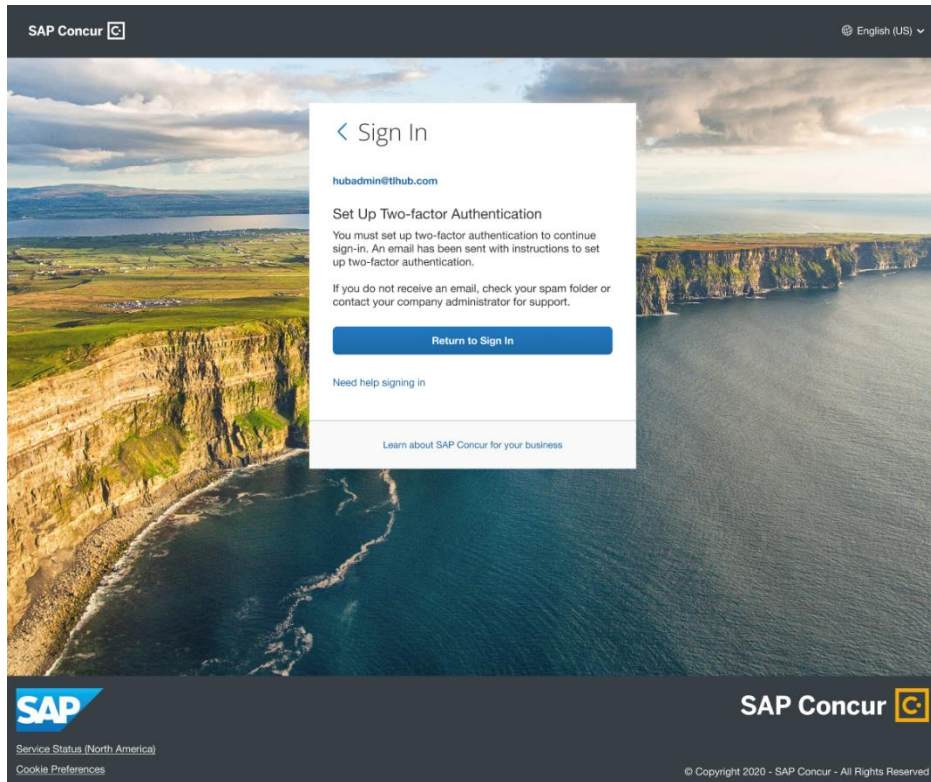


The screenshot shows the SAP Concur Sign In page. The background is a scenic view of a coastline with cliffs and a bay. The page has a dark header with the SAP Concur logo on the left and a language dropdown set to 'English (US)' on the right. The main content area features a white 'Sign In' form. The form title is 'Sign In'. Below the title, it says 'Username, verified email address, or SSO code'. A text input field contains the email 'hubadmin@thub.com'. Below the input field is a blue 'Next' button. Underneath the button is a 'Remember me' checkbox, which is currently unchecked. Below the checkbox are two links: 'Forgot username' and 'Need help signing in'. At the bottom of the form is a link that says 'Learn about SAP Concur for your business'. The footer of the page contains the SAP logo on the left, 'Service Status (North America)' and 'Cookie Preferences' below it, the SAP Concur logo on the right, and '© Copyright 2020 - SAP Concur - All Rights Reserved' at the bottom right.

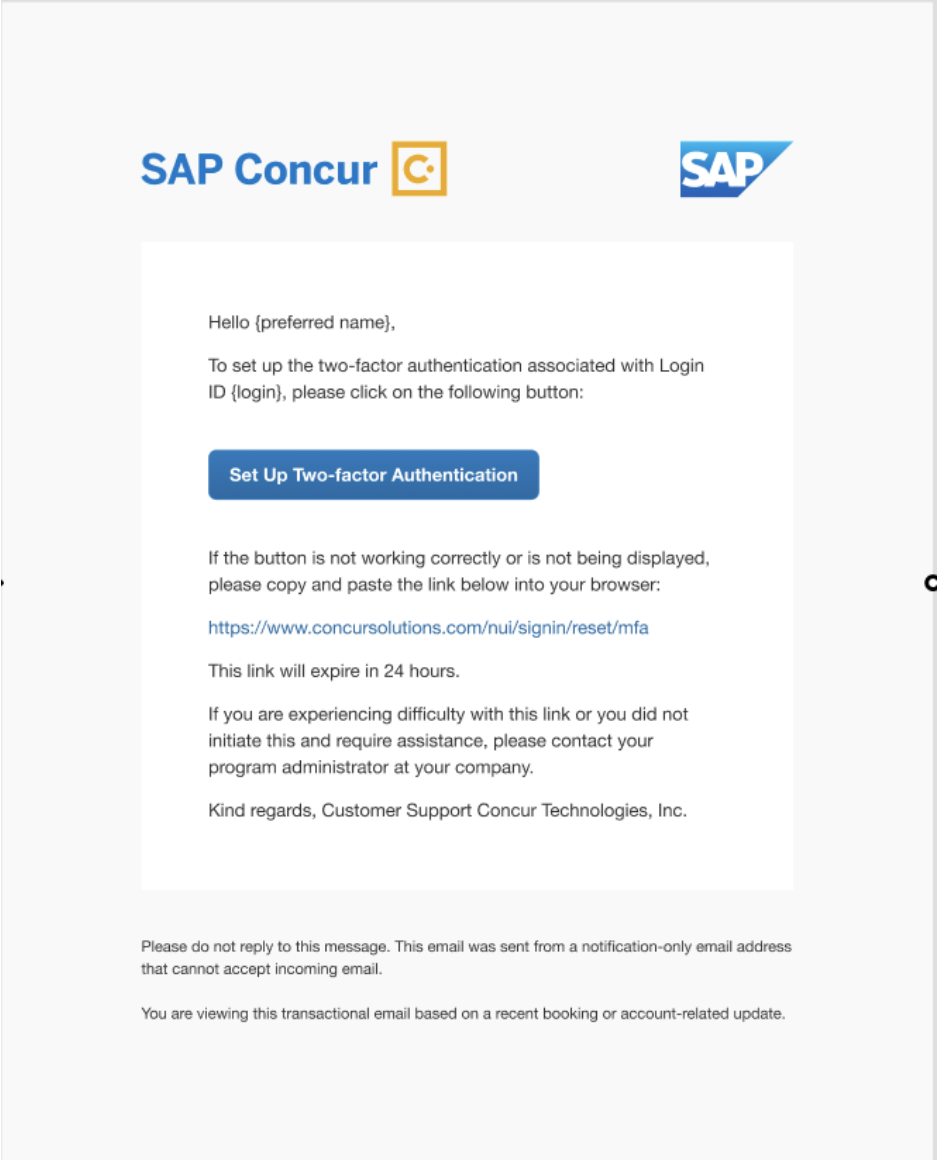


The screenshot shows the SAP Concur Sign In page at the second step. The background and header are the same as in the first screenshot. The main content area features a white 'Sign In' form with a back arrow on the left. The form title is '< Sign In'. Below the title, the email 'hubadmin@thub.com' is displayed. Below the email is a 'Password' label and a text input field. Below the input field is a blue 'Next' button. Underneath the button are two links: 'Forgot password' and 'Need help signing in'. At the bottom of the form is a link that says 'Learn about SAP Concur for your business'. The footer of the page is identical to the first screenshot, containing the SAP logo, service status, cookie preferences, the SAP Concur logo, and the copyright notice.

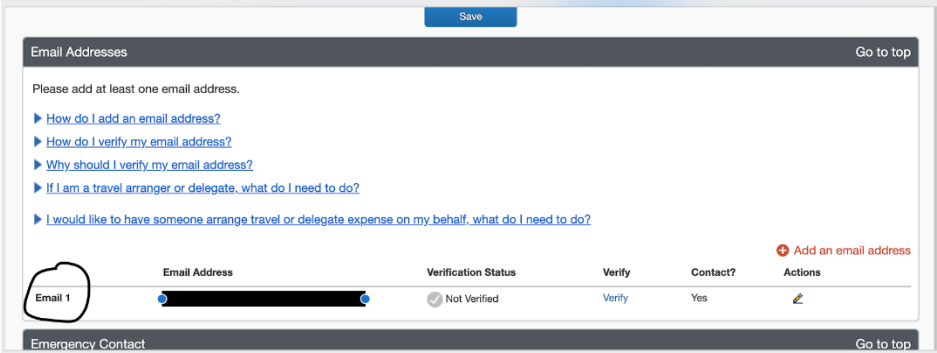
2. You will see an on-screen message stating that you will receive an email to enroll in 2FA.



3. You will receive an email in the email address you have configured in your SAP Concur Profile settings: Email1.

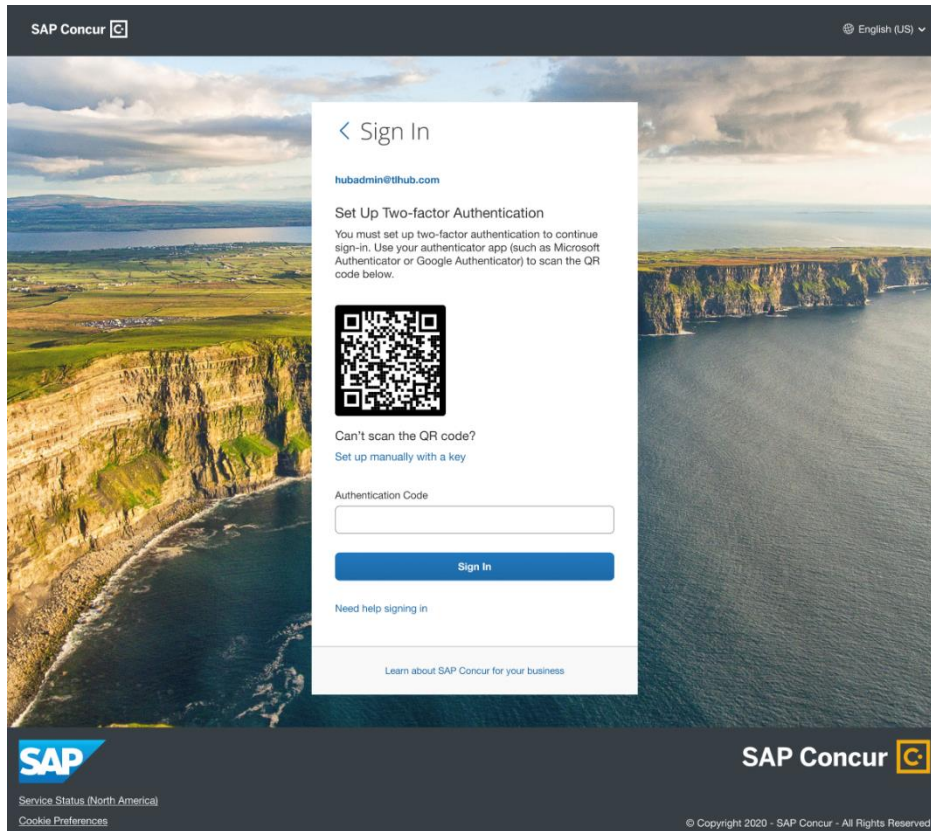


4. If you don't know where your email address is configured, check by signing in to your SAP Concur account and navigating to: Profile>Profile Settings. Under "Your Information", click Email Addresses.



5. From Step three, click the ' Set up Two-factor authentication' link in your email.

6. You will be redirected to scan your QR code.



7. Follow the same instructions for enrollment found in Section 1: Enrollment, starting at Step four.

8. **For ADMINS ONLY-** If you wish to disable the additional email step required in order to enroll in 2FA during phase two, you have the option to disable this setting under the new ' Sign In Settings' found on the Authentication Admin screen. Here you can configure sign in and password policies. Please do so at your own discretion. By disabling this setting, you are removing the additional layer of security for your user accounts.

Sign-In Settings * Required

Password Strength
Password requirements for all users in your organization. The maximum password length is 255 characters.

Minimum password length *
8 Characters
Minimum 8 characters

Characters Requirements

- Contains at least one uppercase (A-Z) and one lowercase letter (a-z)
- Contains at least one number (0-9)
- Contains at least one non-alphabetical character, such as a number or special character
- Contains at least one special (non-alphanumeric) character

Password Change
Set requirements for password reset restrictions and expiration.

Reset Restrictions

After how many changes are users allowed to reuse a password? *
5

How often are users allowed to change passwords?

- Anytime
- After one successful sign in
- Never
- Limit reset to once per day

Expiration

- Enable password expiration

When should passwords expire after renewal or creation?
1 month

Account Lockout
Lock user accounts after failed sign in attempts.

After how many failed attempts should a user be locked out? *
5

Within what timeframe should the failed attempts trigger an account lockout? *
10 Minutes

How would you like to lock the account?

- Permanently
- Temporarily

After how much time should a locked account be unlocked? *
120 Minutes

Session Timeout
Sign users out automatically after a period of inactivity.

Sign out inactive user
After 30 minutes

Show sign out warning
15 minutes before timeout

Others
Other miscellaneous policies

- Hide "Forgot Username" link
- Hide "Forgot Password" link
- Require users to change their password after their first sign in
- Require users to receive an email link to set up Two-factor Authentication

Reset **Save**