SAP Concur |C·|

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. For example, you first enter your password and, when prompted, you also type a dynamically generated verification code provided 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 an SAP 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.
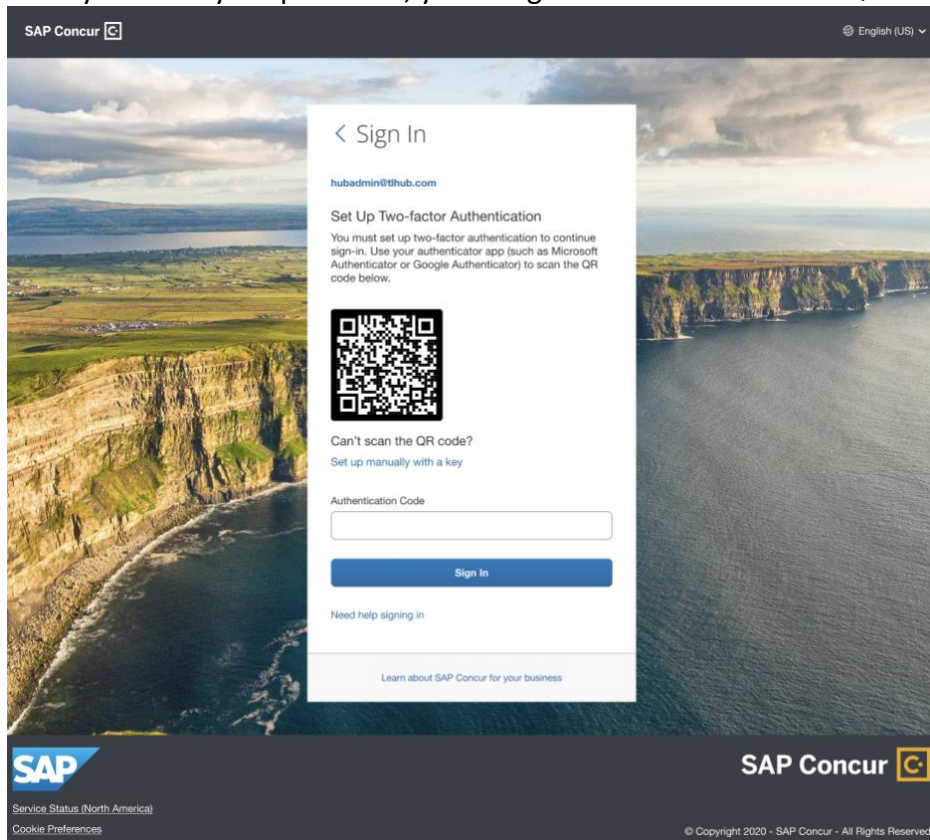
2. Enter your username and password as usual

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

4. Download an authenticator app of your choice in your mobile phone. You can use a corporate phone or also use your personal device. You are free to use any authenticator app- like Microsoft , Google, etc. Eg : https://support.microsoft.com/en-us/account-billing/add-non-microsoft-accounts-to-the-microsoft-authenticator-app-7a92b5d4-d6e5-4474-9ac6-be0b6773f574, https://apps.apple.com/us/app/google-authenticator/id388497605, https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US&gl=US. You generally go into the App Store or Play Store and search/download the authenticator app you wish to use.

   Or, you can choose from the following list:
   Twilio Authy Authenticator, Duo Mobile, Microsoft Authenticator, Google Authenticator

5. 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/bhghoamapcdpbohphigooo addinpkbai. For Microsoft Edge,

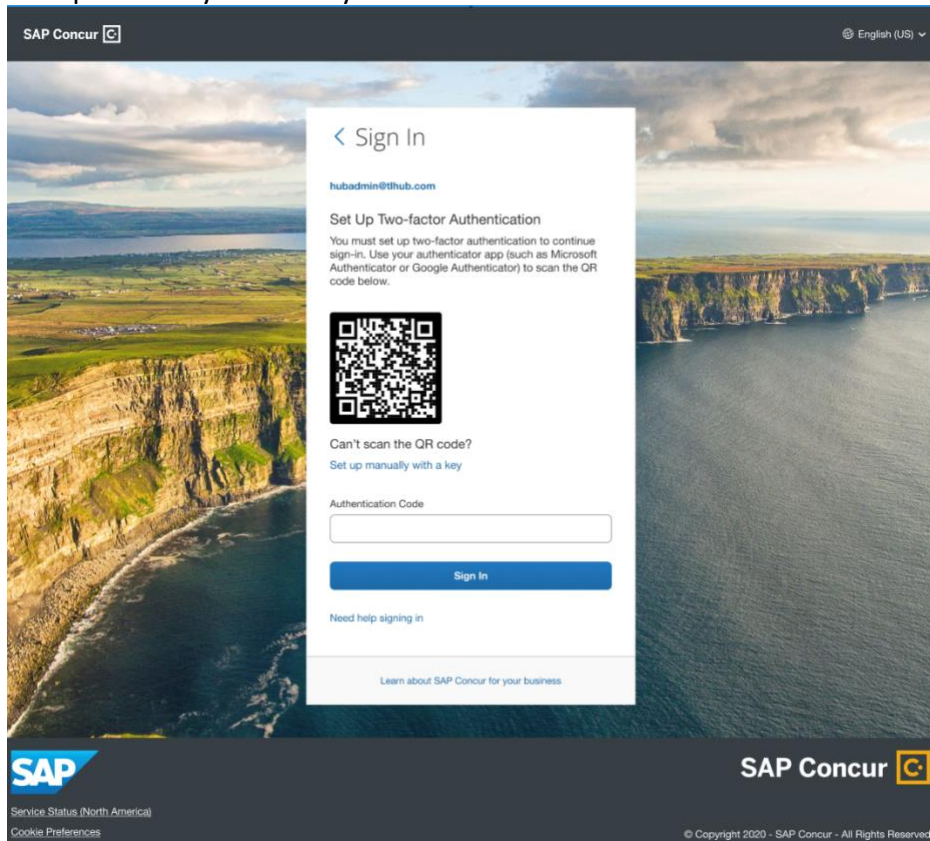https://microsoftedge.microsoft.com/addons/detail/authenticator-2fa-client/ocglkepbibnalbgmbachknglpdipeoio

To better understand how your browser will scan the QR code, please reference this YouTube video of how web browser authenticator works https://www.youtube.com/watch?v=x14KazisIAQ

6. Click on ' Add account' or '+' sign or whatever button is available in the authenticator app for you to add a new account

7. Once the QR code scanner starts on the app, scan the QR code shown on the Concur sign in page. This will add your Concur account to the authenticator app.

8. Once this is done, For example purpose- if your account username is hubadmin@concur.com- right below this account on the authenticator app- a 6-digit code will be generated

9. Before the 6-digit code expires- please copy that code into the ' Authentication Code' field on the Concur sign in page and hit Sign In

10. You are now successfully logged 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 on the '
   Set up manually with a key'

2. Once you click, a secret key should be visible on your screen
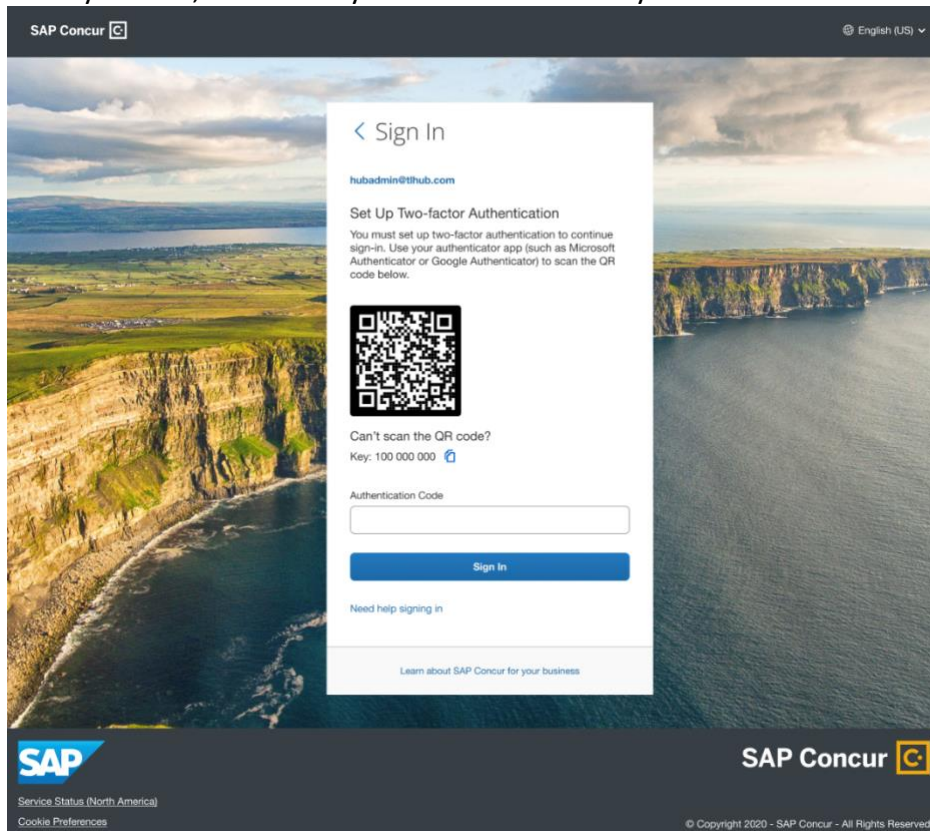
3. Now, go into your authenticator app on your phone or web. Based upon what authenticator app you are using- there should be an option like ' Enter a setup key' for example in Google Authenticator or if you are using MSFT Authenticator - Click on ' Add account' → Other account→ ' Enter code manually'.
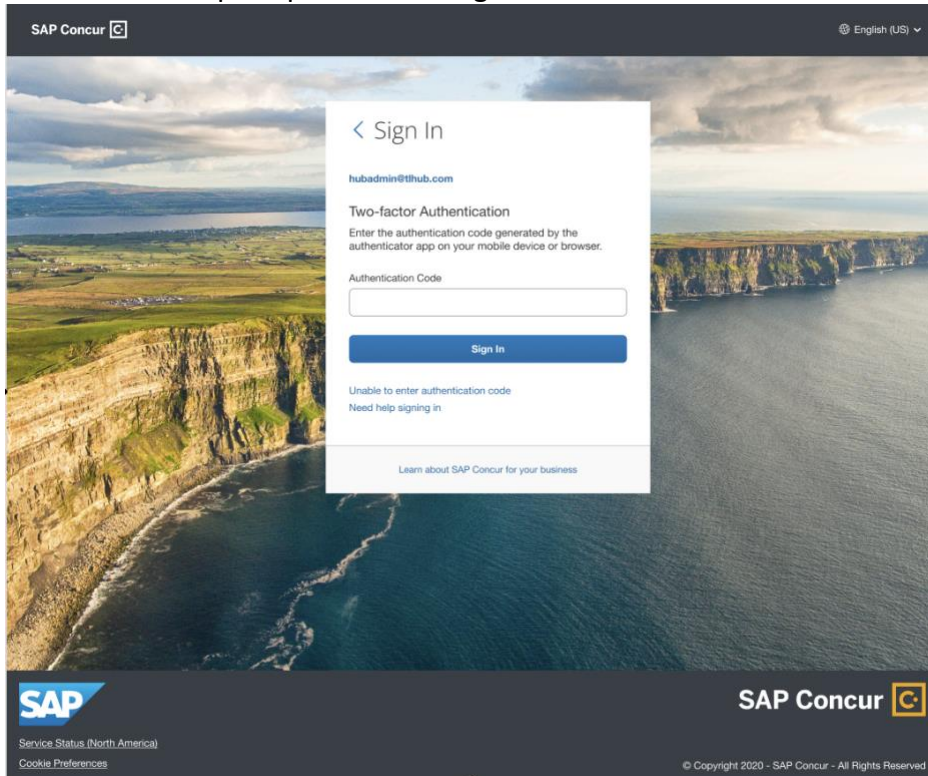
4. There will be two fields visible on the Authenticator app- account and secret key. In the account- add your Concur account username shown on your Concur screen . For e.g.: hubadmin@concur.com and in secret key enter the secret key shown on the Concur page- for e.g.: 100 000 000.

5. Once the account is added, beneath the Concur account in your authenticator app, a 6-digit code will be generated.

6. 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 and need to reset MFA? Did you lose your device and want to reset your 2FA? Do you want to switch your Authenticator app and use a different one?

Prerequisite: You have already enrolled in 2FA before

1. Enter your username and password.
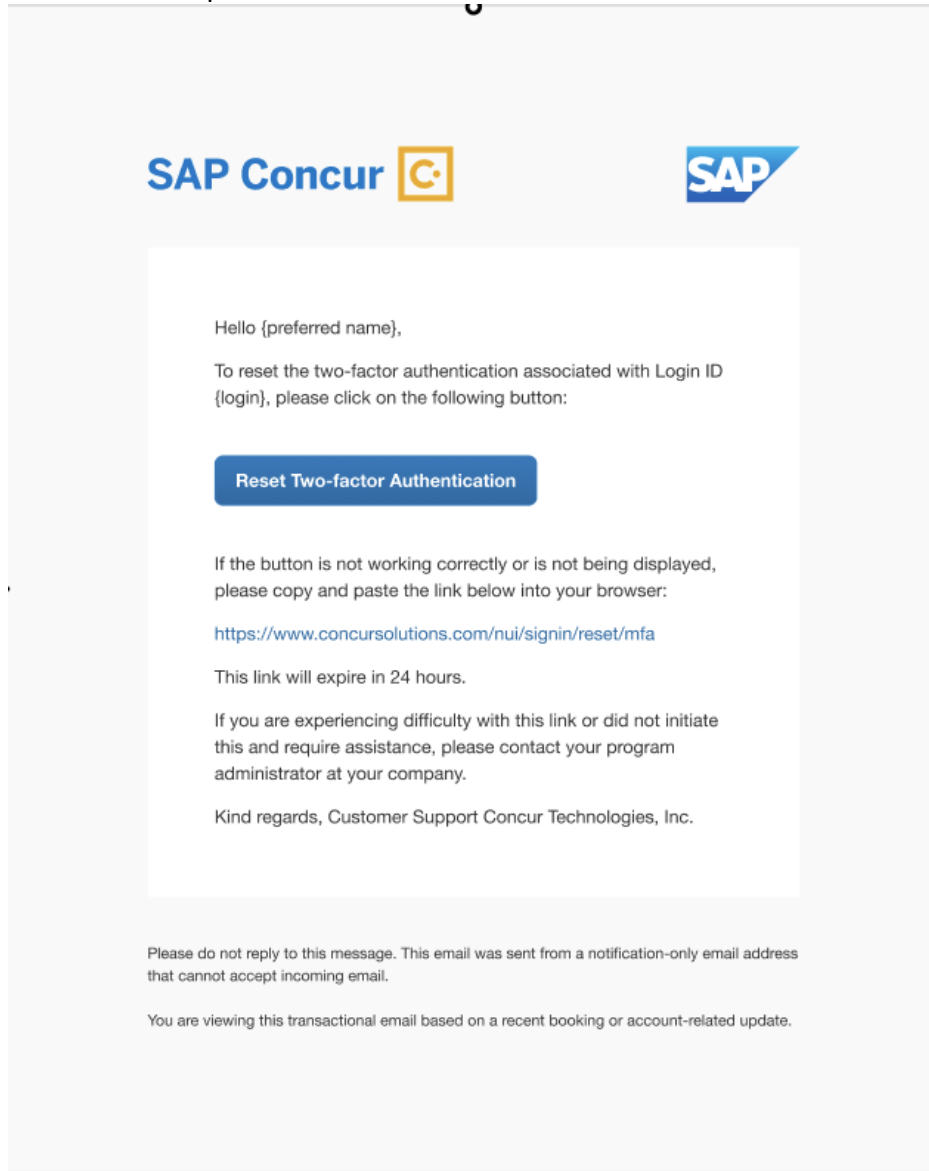2. You will be now prompted for a 6-digit authentication code

3. If you need to reset your 2FA for your new device OR you lost your phone and need to enroll in 2FA again for your new device OR you wish to switch to a different Authenticator App, click on ' Unable to enter authentication code'.
4. You will now receive an email with a link to reset 2FA. Please note : This email will be sent to the email1 or email2 set up in your Profile settings
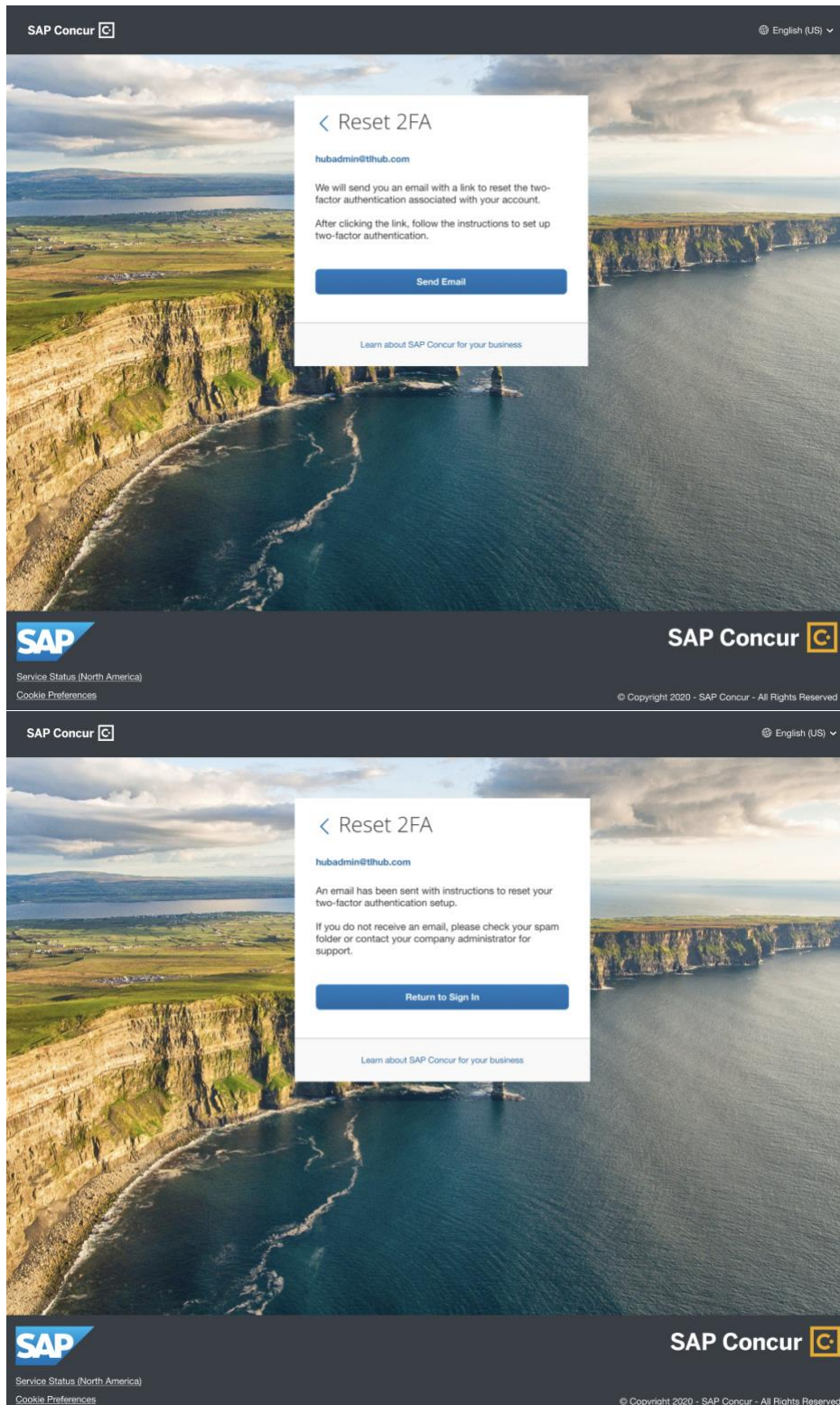
5. To check whether your email is updated in Profile . You need to login to Concur - Profile-Profile Settings- Personal Information-Email addresses.
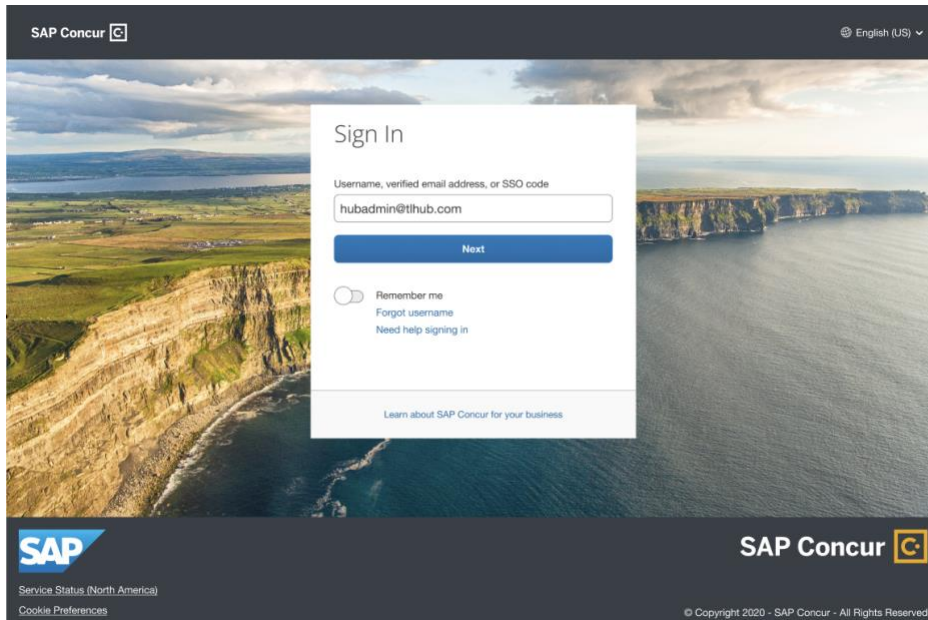
6. If you did not update email1 in Profile and are locked out, please contact the Admin of your company and ask them to update the email for you and then once they update- click on ' Unable to enter authentication code' to trigger the email one more time.
7. If you receive an email, you will receive a link in the email to reset 2FA. Click on the link and you will receive the QR code. Follow the same steps provided in the 2FA Enrollment section to set up 2FA
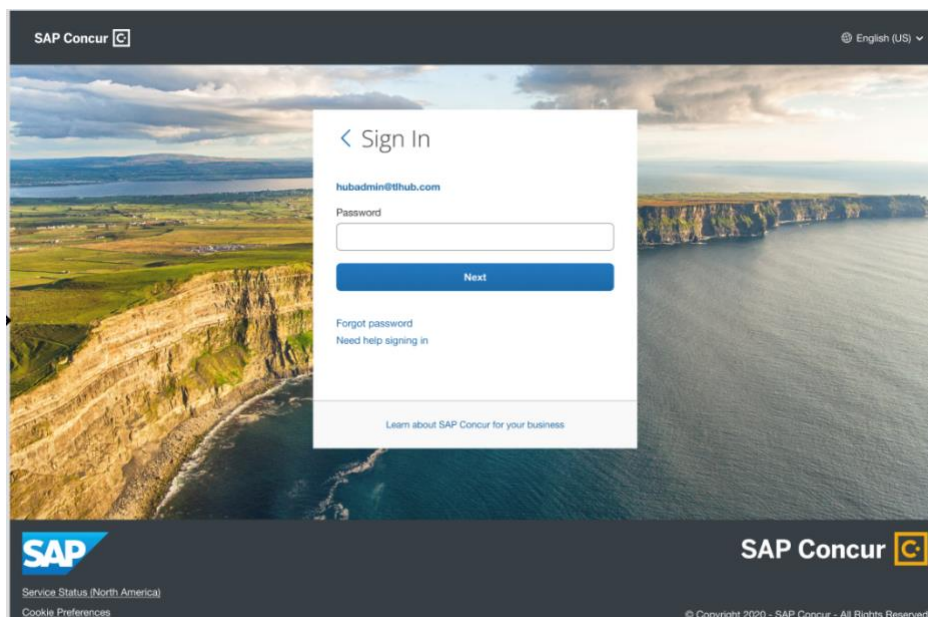
SAP Concur C·   **SAP**

Hello {preferred name},

To reset the two-factor authentication associated with Login ID {login}, please click on the following button:

Reset Two-factor Authentication

If the button is not working correctly or is not being displayed, please copy and paste the link below into your browser:

https://www.concursolutions.com/nui/signin/reset/mfa

This link will expire in 24 hours.

If you are experiencing difficulty with this link or did not initiate this and require assistance, please contact your program administrator at your company.

Kind regards, Customer Support Concur Technologies, Inc.

Please do not reply to this message. This email was sent from a notification-only email address that cannot accept incoming email.

You are viewing this transactional email based on a recent booking or account-related update.

Phase 2 Enrollment starting November 15

Enrollment

1. If you have not enrolled in 2FA for your accounts using Concur username/password. Enter your Concur username/ password as usual.
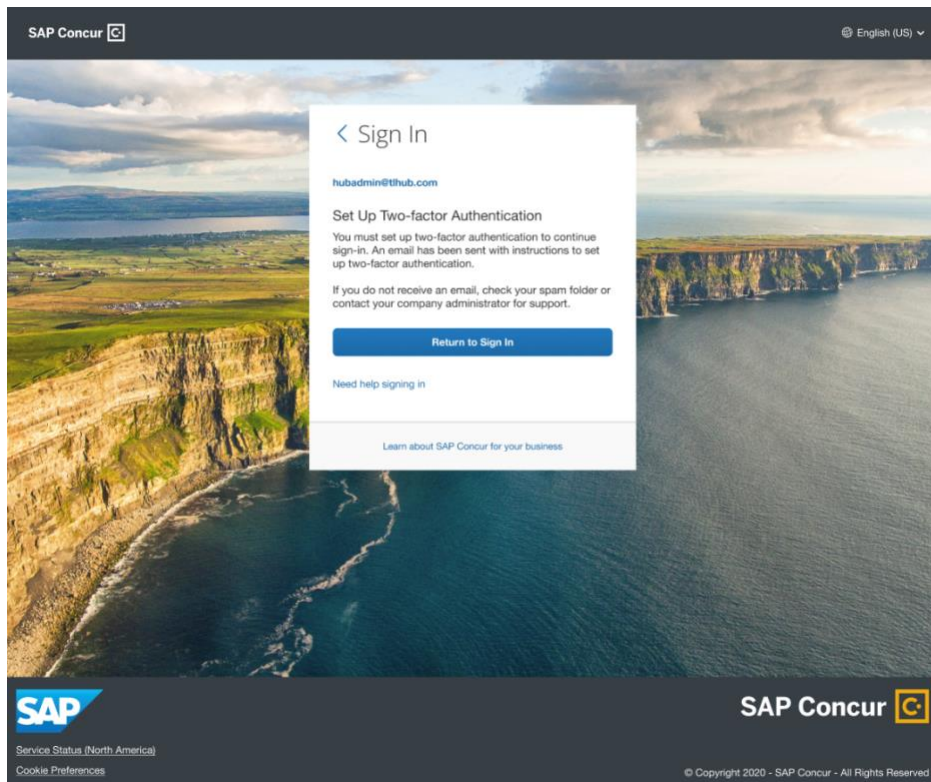

2. You will see on your screen that you will receive an email to enroll in 2FA

3. You will receive an email in the email address you have configured in your Concur Profile settings - email1.

SAP Concur C·   **SAP**

Hello {preferred name},

To set up the two-factor authentication associated with Login ID {login}, please click on the following button:

Set Up Two-factor Authentication

If the button is not working correctly or is not being displayed, please copy and paste the link below into your browser:

https://www.concursolutions.com/nui/signin/reset/mfa

This link will expire in 24 hours.

If you are experiencing difficulty with this link or you did not initiate this and require assistance, please contact your program administrator at your company.

Kind regards, Customer Support Concur Technologies, Inc.

Please do not reply to this message. This email was sent from a notification-only email address that cannot accept incoming email.

You are viewing this transactional email based on a recent booking or account-related update.

4. If you don't know where your email address is configured,

- You can verify if you have an up-to-date EMAIL1 in your Profile Settings. In order to check this- log into Concur → Profile Settings→Email Addresses.

5. From Step 3- click on ' 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 from Section 1 enrollment - Step 4 onwards

8. **For ADMINS ONLY**- If you wish to disable the additional email step required in order to enroll in 2FA during phase 2- you have the option to disable this setting under the new ' Sign In Settings' under Authentication Admin where you can configure login/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
- [x] Contains at least one uppercase (A-Z) and one lowercase letter (a-z)
- [ ] Contains at least one number (0-9)
- [x] 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
- [x] Limit reset to once per day

Expiration
- [x] 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
- [x] Require users to receive an email link to set up Two-factor Authentication ❓

Reset | Save