

# **Shared: SAP Concur Two-Factor Authentication**

## **Setup Guide**

**Last Updated: November 3, 2023**

Applies to these SAP Concur solutions:

- ☒ Expense
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Travel
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Invoice
  - ☒ Professional/Premium edition
  - ☒ Standard edition
- ☒ Request
  - ☒ Professional/Premium edition
  - ☒ Standard edition

# Table of Contents

<b>Section 1: Overview .....</b>	<b>1</b>
Shared Sign In Credentials and 2FA .....	1
<b>Section 2: Phase 1: October 18, 2023 – November 15, 2023 .....</b>	<b>2</b>
User Enrollment in 2FA .....	2
Enrollment Process .....	3
Enrollment Process using a Manual Key .....	6
User Experience After Enrollment.....	9
User-initiated Reset for 2FA .....	10
Administrator Reset for 2FA .....	14
<b>Section 3: Phase 2: Beginning November 16, 2023 .....</b>	<b>14</b>
Prerequisites and Options .....	14
User Enrollment in 2FA .....	16
Enrollment Process via QR code with email requirement .....	16
Enrollment Process with email requirement using a Manual Key .....	20
Enrollment Process via QR code without the email requirement .....	23
Enrollment Process without email requirement using a Manual Key .....	26
User Experience After Enrollment.....	28
User-initiated Reset for 2FA .....	30
Administrator Reset for 2FA .....	33
Professional Edition.....	33
Standard Edition (Available after November 15, 2023) .....	34
Administrator Opt-Out of Email Requirement.....	34



## Revision History

Date	Notes/Comments/Changes
November 3, 2023	Updated throughout.
October 30, 2023	Initial publication out of DRAFT status.
October 27, 2023	Updated draft.
October 17, 2023	New setup guide published in DRAFT.

# SAP Concur Two-Factor Authentication Setup Guide

---

## Section 1: Overview

To enhance the security of all SAP Concur users, two-factor authentication (2FA) is mandatory for users who sign in to SAP Concur solutions with a Concur username and password.

When an SAP Concur user signs in to SAP Concur using their username and password for the first time, they will be prompted to setup 2FA.

After they have set up 2FA, users who sign in to SAP Concur solutions with a username and password must use 2FA when they sign in. This typically means that the user will be prompted to enter a one-time 6-digit code generated by an authenticator app each time they sign in to SAP Concur solutions.

This document describes the process and requirements for setting up 2FA, resetting 2FA if needed, and the process of signing in to SAP Concur solutions with 2FA after it has been set up.

---

**NOTE:** 2FA typically requires the use of a third-party authenticator app. SAP Concur cannot provide details about setting up a third-party application. Refer to the documentation for the authenticator app you are using for information about your chosen authenticator app.

---

## Shared Sign In Credentials and 2FA

For security reasons, SAP Concur does not recommend sharing sign in credentials between users.

If you choose to share credentials against recommendations, you must also consider the following:

- To share credentials that require 2FA, every user who shares the credentials must set up their authenticator app using the same QR code or manual key.
- If a user who shares credentials must reset 2FA, then all users who share those credentials must also reset 2FA using the same QR code or manual key.
- If a new user is added to a group that shares credentials, that user must use the same QR code or manual key that was used by the other members of the group to setup their authenticator app. If that QR code or manual key is no longer available, all members of the group must reset or set up 2FA using a new, identical QR code or manual key.

## Section 2: Phase 1: October 18, 2023 – November 15, 2023

Phase 1 of the implementation of mandatory 2FA for SAP Concur solutions began on October 18, 2023, and ends on November 15, 2023.



For more information about phase 1 and phase 2 of this release, refer to the [October Shared Changes release notes](#).

During phase 1 (October 18 – November 15, 2023):

- All users can set up 2FA without a valid email address in the **Email Address** section of their **Profile Settings > Personal Information** page.

### **Valid Email Address.**

A valid email address is an email address that can send and receive email messages.

---

**NOTE:** Although a valid email address is not required during phase 1, it is required by default when phase 2 begins. Beginning on October 18, 2023, client admins can opt-out of the phase 2 email requirement through a setting on the **Sign In Settings** page. For information about this setting, see the *Administrator Opt-Out of Email Requirement* section in this document.

---

- Although a valid email address is not required during this phase, SAP Concur recommends that users add a valid email address before phase 2 begins on November 15, 2023.
- Although a valid email address is not required for 2FA setup, it is required for user-initiated 2FA reset. User-initiated 2FA reset sends an email with a reset link to the **Email 1** and/or **Email 2** email addresses configured in the **Email Address** section of their **Profile Settings > Personal Information**.

---

**NOTE:** For users who do not have access to the **Email Address** section of their **Profile Settings > Personal Information** page, the reset email is sent to the email address associated with their user account.

---

- Beginning on October 18, if it is not already setup, after a user enters their SAP Concur sign in credentials (username and password) on the Concur sign in page, they will be prompted to setup 2FA.

## User Enrollment in 2FA

The first time a user signs in to SAP Concur solutions with a Concur username and password, they are prompted to enroll in 2FA.

If they do not already have an authenticator app installed on their mobile device or as a browser plug-in, they must download one to complete the enrollment.

The user can enroll either by scanning a QR code, or by manually entering a key.

**NOTE:** Some companies have restrictions or guidance about which applications (including third-party authenticator apps) their users can install on their 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 a user has multiple username and password word sign in credentials for SAP Concur solutions, they must follow the enrollment process for each set of credentials.

## Enrollment Process

### ► To enroll in 2FA by scanning a QR code

1. On the Concur mobile or web sign in page, enter your SAP Concur username and password.

### Sign In

Username, verified email address, or SSO code

Next

☐ Remember me  
[Forgot username](#)  
[Need help signing in](#)

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

### < Sign In

InvoiceUser@Test\_CA.com

Password

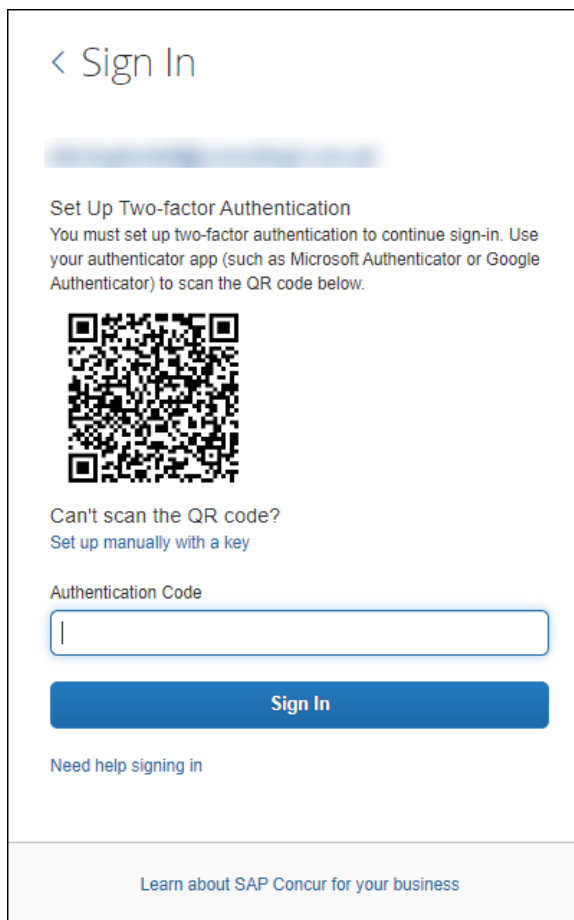
Sign In

[Forgot password](#)  
[Need help signing in](#)

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

2. The following message is presented:

"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."



The screenshot shows a 'Sign In' page with a heading '< Sign In'. Below it is a blurred area. The main heading is 'Set Up Two-factor Authentication'. The text below reads: '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.' A QR code is displayed in the center. Below the QR code, it says 'Can't scan the QR code?' and 'Set up manually with a key'. There is an input field labeled 'Authentication Code' with a blue border. Below the input field is a blue button labeled 'Sign In'. At the bottom, there is a link 'Need help signing in' and a footer link 'Learn about SAP Concur for your business'.

3. If you are using a mobile device to setup 2FA and have already downloaded an authenticator app, launch the authenticator app.
  - ◆ If you do not yet have an authenticator app, download one and then proceed to setup 2FA.
  - ◆ If you do not have a mobile device or prefer not to use one for this process, you can use an authenticator app in a web browser.
4. Follow the steps or prompts from the authenticator app to scan the QR code on the **Set Up Two-factor Authentication** page and generate a 6-digit code.

The steps vary depending on which authenticator app you are using.

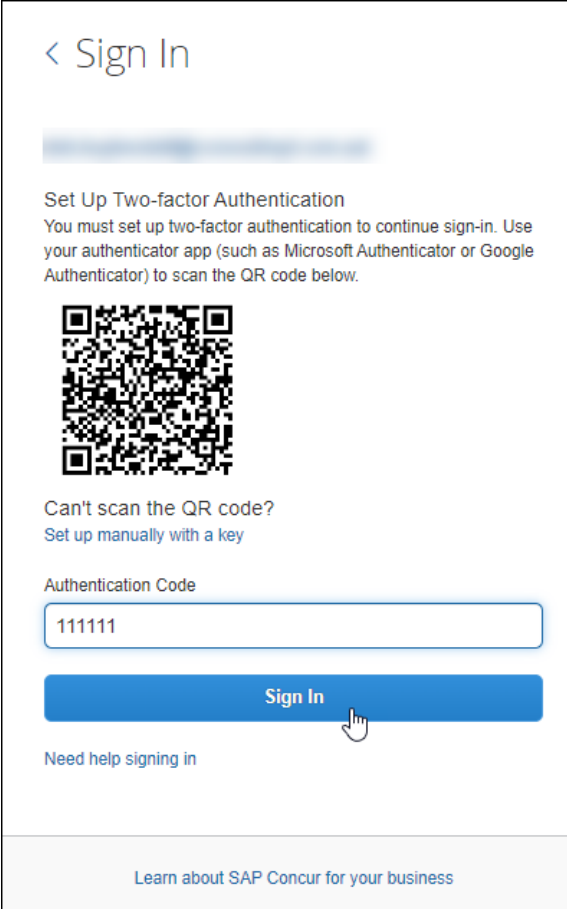


---

**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.

---

5. On the SAP Concur **Sign In** page, enter the 6-digit code into the **Authentication Code** field in the **Set Up Two-Factor Authentication** section and then click **Sign In**.



The screenshot shows the SAP Concur Sign In page. At the top, there is a back arrow and the text "Sign In". Below this is a blurred header area. The main section is titled "Set Up Two-factor Authentication" and contains the text: "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." A QR code is displayed in the center. Below the QR code, there is a link "Can't scan the QR code?" and a sub-link "Set up manually with a key". Underneath, there is a label "Authentication Code" and a text input field containing the number "111111". A blue "Sign In" button is positioned below the input field, with a mouse cursor hovering over it. At the bottom of the main section, there is a link "Need help signing in". The footer of the page contains the link "Learn about SAP Concur for your business".

## ***Enrollment Process using a Manual Key***


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.

1. Click the **Set up manually with a key** link.



< 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?  
[Set up manually with a key](#)

Authentication Code

**Sign In**

[Need help signing in](#)

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

2. 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: 7MHHZN6RZET7007Y2BELQVAP4DTQ2KG 

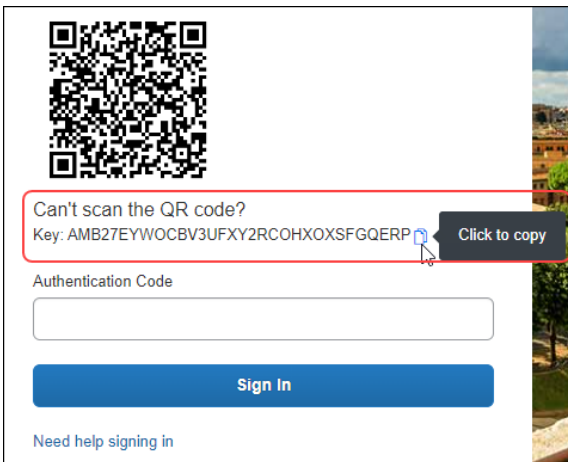
Authentication Code


**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: AMB27EYWOCBV3UFXY2RCOHXOXSFQGERP  Click to copy

Authentication Code

**Sign In**

[Need help signing in](#)

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

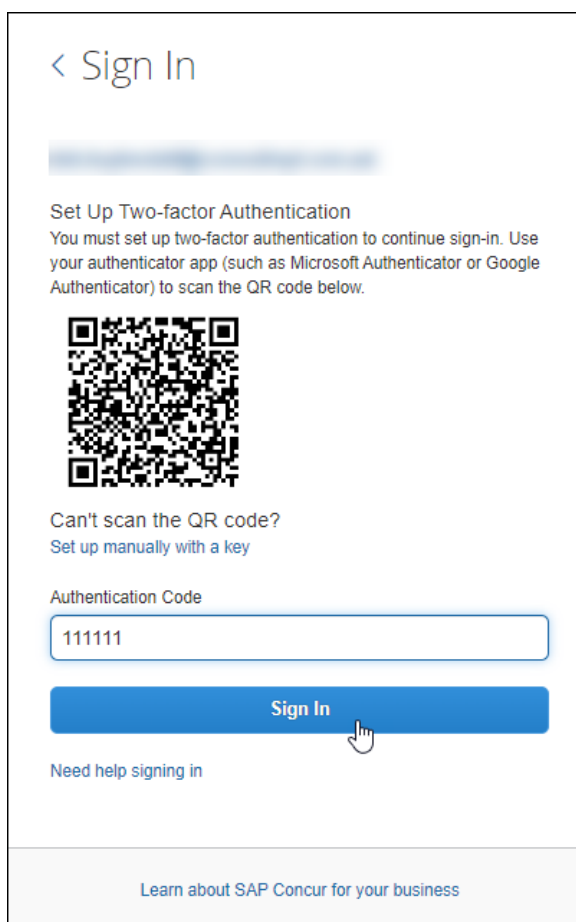
- ♦ Typically, you will need to add a name or other identifier for the account the key is associated with, for example "SAP Concur".
- ♦ If you are using Google Authenticator, choose the Time Based option.

---

**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.

---


4. 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.



< 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?  
[Set up manually with a key](#)

Authentication Code

[Sign In](#)

[Need help signing in](#)

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

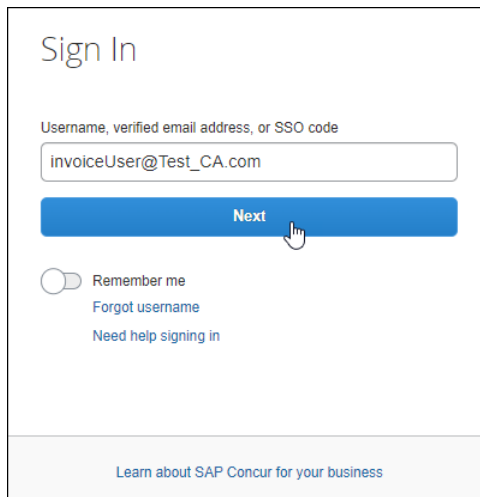
5. Click **Sign In**.

## User Experience After Enrollment

After a user has enrolled in 2FA for SAP Concur, after entering their username and password to sign in to SAP Concur solutions, they are prompted to enter the 6-digit authentication code generated by their authenticator app.

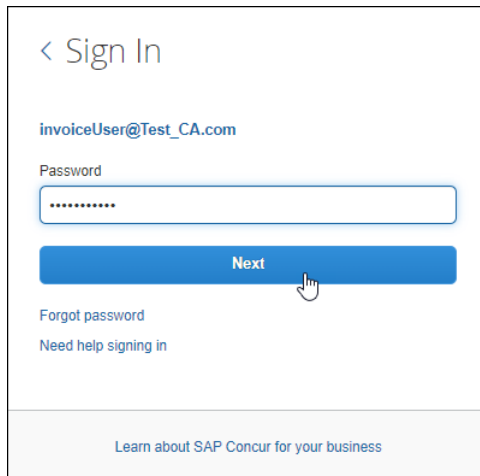
► **To sign in to SAP Concur solutions with 2FA**

1. Navigate to concursolutions.com or open Concur Mobile.
2. Enter your username.



The screenshot shows the 'Sign In' page. At the top, it says 'Sign In'. Below that, a label reads 'Username, verified email address, or SSO code'. A text input field contains 'invoiceUser@Test\_CA.com'. A blue 'Next' button is below the field, with a mouse cursor hovering over it. Below the button, there is a 'Remember me' toggle switch (currently off), a link for 'Forgot username', and a link for 'Need help signing in'. At the bottom, there is a link that says 'Learn about SAP Concur for your business'.

3. Enter your password.



The screenshot shows the 'Sign In' page with a back arrow. The username 'invoiceUser@Test\_CA.com' is displayed above the password field. The label 'Password' is above a text input field containing eight dots. A blue 'Next' button is below the field, with a mouse cursor hovering over it. Below the button, there is a link for 'Forgot password' and a link for 'Need help signing in'. At the bottom, there is a link that says 'Learn about SAP Concur for your business'.

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

The screenshot shows the SAP Concur Sign In page. At the top, there is a back arrow and the text "< Sign In". Below this, the email address "invoiceUser@Test\_CA.com" is displayed. The section is titled "Two-factor Authentication" and instructs the user to "Enter the authentication code generated by the authenticator app on your mobile device or browser." There is a text input field for the "Authentication Code" containing the value "111111". Below the input field is a blue "Sign In" button. A mouse cursor is hovering over the button. Under the button, there is a message "Unable to enter authentication code" and a link "Need help signing in". At the bottom of the page, there is a link "Learn about SAP Concur for your business".

## User-initiated Reset for 2FA

You might need to reset and re-enable 2FA for Concur sign in. For example, you might replace the mobile device you initially used to set up 2FA, or you might want to change your authenticator app.

Resetting 2FA has the following prerequisites:

- User-initiated 2FA reset cannot be completed in Concur Mobile. You must reset 2FA by signing in to concursolutions.com via a web browser.
- You must have a valid **Email 1** or **Email 2** address configured in the **Email Addresses** section of the **My Profile – Personal Information** page in SAP Concur solutions.

The screenshot shows the SAP Concur Profile page. The top navigation bar includes "SAP Concur", "Profile", and several tabs: "Profile", "Personal Information", "Change Password", "System Settings", and "Concur Mobile Registration". The "Personal Information" tab is selected. On the left, there is a sidebar with "Other Settings" and links for "System Settings", "Concur Connect", "Change Password", and "Concur Mobile Registration". The main content area is titled "Email Addresses" and includes a "Go to top" link. It contains instructions to "Please add at least one email address." and several links: "How do I add an email address?", "How do I verify my email address?", "Why should I verify my email address?", and "Travel Arrangers / Delegates". Below this, there is a table with one row for "Email 1" with the address "test\_user@test\_entity.com". The table has columns for "Email Address", "Verify", "Contact?", and "Actions". The "Verify" column shows a "Not Verified" status. The "Actions" column has a "Verify" link. A red box highlights the "Email Address" column. At the bottom right, there is a link "Add an email address".

Some users do not have access to the **Email Addresses** section of the **My Profile – Personal Information** page—for example, Concur Invoice-only users.

If you do not have access the **Email Addresses** section of the **My Profile – Personal Information** page, you can contact your company's Concur administrator to confirm you have a valid email address associated with your Concur user account.

The screenshot shows the SAP Concur Administration interface. On the left, there's a sidebar with 'User Administration' and 'Travel Administration' sections. The main area is titled 'General Settings' and contains fields for 'CTE Login Name\*' (InvoiceUser@Test\_CA.com), 'Password\*', 'Verify Password\*', 'Title', 'First Name\*' (Invoice), 'Middle Name', 'Preferred Name', 'Last Name\*' (User), 'Suffix', 'Account Activation Date' (10/25/2023), 'Employee ID', 'Account Termination Date', and 'Email Address' (InvoiceUser@Test\_CA.com). A mouse cursor is pointing at the 'Email Address' field.

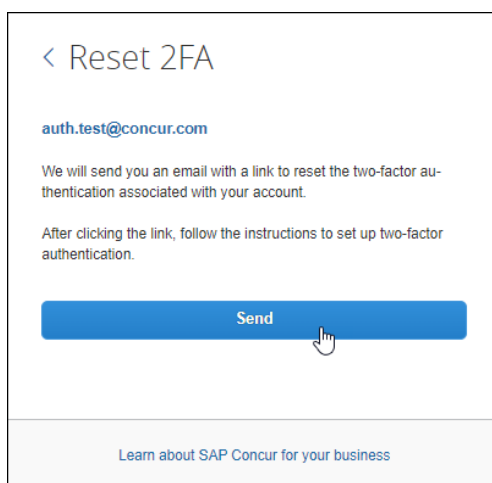
- You must be able to access email sent to the configured **Email 1** or **Email 2 address**. Or, in the case of users who do not have access to the **Email Addresses** section of the **My Profile – Personal Information** page, access to email sent to the email address configured in your user account.

► **To reset 2FA**

1. On the SAP Concur sign in page, enter your username and password.
2. On the **Two-factor Authentication** page, click **Unable to enter authentication code**.

The screenshot shows the 'Two-factor Authentication' page. It has a header '< Sign In' and a username 'auth.test@concur.com'. Below the username, it says 'Two-factor Authentication' and 'Enter the authentication code generated by the authenticator app on your mobile device or browser.' There's a text input field for 'Authentication Code'. Below the field is a blue 'Sign In' button. Under the button, there's a link 'Unable to enter authentication code' with a mouse cursor pointing at it, and a link 'Need help signing in'. At the bottom, there's a link 'Learn about SAP Concur for your business'.

3. On the **Reset 2FA** page, click **Send**.



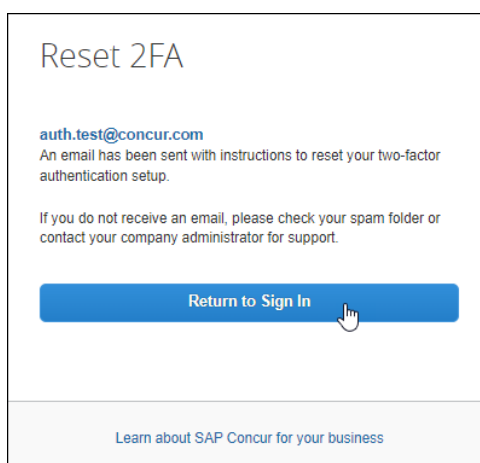
A reset email is sent to the **Email 1** and/or **Email 2** addresses configured in the **Email Addresses** section of the **My Profile – Personal Information** page in SAP Concur solutions. For users who don't have access to the **Email Addresses** section of the **My Profile – Personal Information** page, an email is sent to the email address associated with their Concur user account.

---

**NOTE:** The reset link will not be sent to addresses after **Email 2**.

---

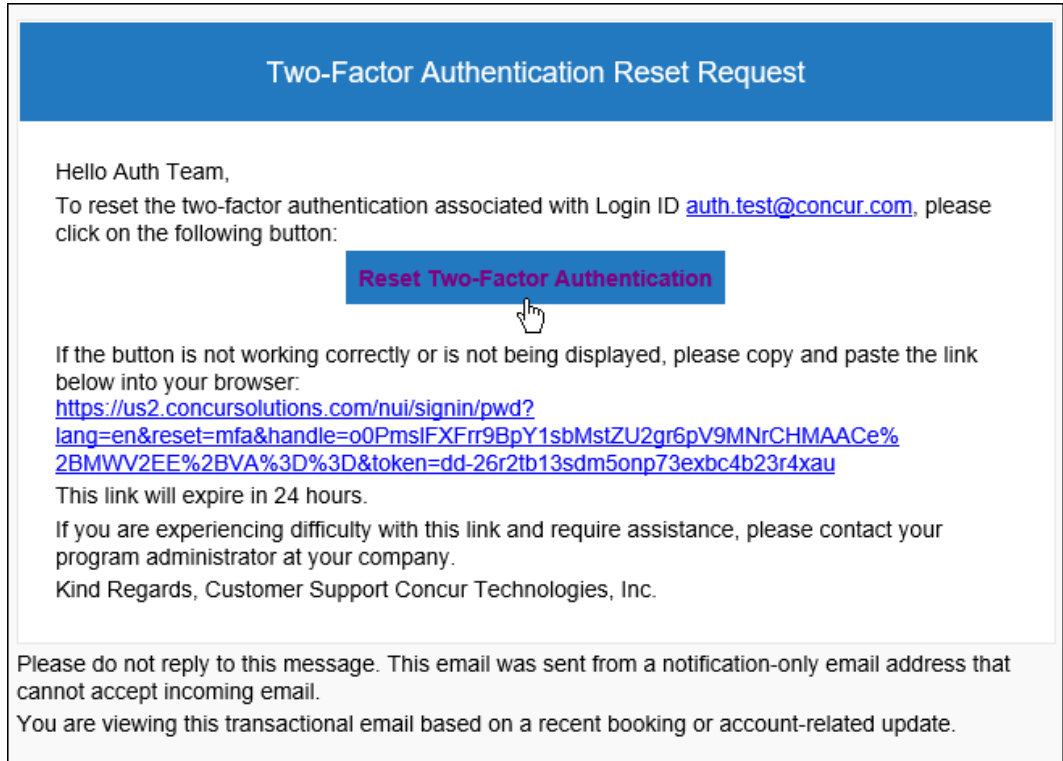
4. Click **Return to Sign In**.



5. Before attempting to sign in on the **Sign In** page, open the **Two-Factor Authentication Reset Request** that was sent from noreply@concur.com to the configured email address.

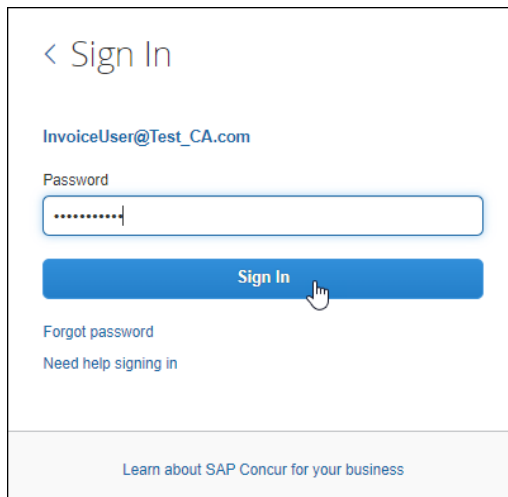


6. In the email, click **Reset Two-Factor Authentication**.



7. On the SAP Concur **Sign In** page, enter your password.

**NOTE:** You will not be prompted to enter your username. The username associated with the configured email address is automatically used to sign in.




8. On the **Set Up Two-factor Authentication** page, follow the steps in the preceding *Enrollment Process* section to re-enroll in 2FA for SAP Concur.

## Administrator Reset for 2FA

If a user is unable to reset 2FA, a company administrator with the permission to administer users can reset 2FA for the affected user.

► **To reset 2FA for a user in Professional Edition**

1. Sign in to SAP Concur solutions as an administrator with permission to administer users. For example, **User Administration** or **Company Administration**.
2. Open the user account page for the user who needs 2FA to be reset.
3. In the **MFA Reset** section of the user's account page, click **Reset**.



**MFA Reset**

**Reset**

This resets the user's MFA details, and they must now re-register their MFA methods upon their next sign-in.

---

**General Settings**

CTE Login Name* <small>(must be suffixed with a valid domain)</small>	Password* <small>(Blank to leave unchanged)</small>	Verify Password*
<input type="text"/>	<input type="text"/>	<input type="text"/>

---

**NOTE:** The option for administrators to reset MFA for their users in **Concur Standard Edition** will not be available until phase 2 (November 15, 2023).

---

After the administrator resets 2FA the user must go through the 2FA enrollment process either by scanning the QR code or by manually entering a key as described in the preceding *Enrollment Process* section.

## Section 3: Phase 2: Beginning November 16, 2023

### Prerequisites and Options

Depending on your company's configuration, users must meet some requirements to complete 2FA setup or reset 2FA.

- **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.
- **Valid Email Address:**  
By default, users must have an **Email 1** or **Email 2** email address configured in the **Email Addresses** section of the **My Profile – Personal Information** page.

## Email Addresses

Users who do not have access to the **Email Addresses** section of the **My Profile – Personal Information**—for example, invoice-only users—must have a valid email address associated with their user account. The email address associated with their account can be confirmed by their company's Concur user administrator.

During the initial setup process, after the user enters their sign-in credentials for the first time, an email containing a link to set up 2FA is sent to the configured email address(es).

- ◆ A Concur company administrator can disable the option to require a valid email address.



For more information, refer to the *Administrator Opt-Out of Email Requirement* section of this document.

---

**NOTE:** Disabling the email requirement is not recommended as this requirement adds an additional level of security to the enrollment process.

---

- ◆ If the required email address option is disabled, users can set up 2FA without using an email link.
- ◆ If a user has a valid **Email 1** or **Email 2** address set up in the **Email Addresses** section of the **My Profile – Personal Information** page, they can initiate the 2FA reset process. The reset link will be sent to the configured email address(es).

However, if the option requiring a valid email address is disabled and the user does not have a valid email address set up, the user must contact their company administrator or IT department to reset 2FA.

An SAP Concur user administrator can reset 2FA for the user through an option on the user's **User Account** page.



For more information, refer the *Administrator Reset for 2FA* procedures.

## User Enrollment in 2FA

The first time a user signs in to SAP Concur solutions with a Concur username and password, they are prompted to enroll in 2FA.

If they do not already have an authenticator app installed on their mobile device or as a browser plug-in, they must download one to complete the enrollment.

The user can enroll either by scanning a QR code, or by manually entering a key.

---

**NOTE:** Some companies have restrictions or guidance about which applications (including third-party authenticator apps) their users can install on their 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 a user has multiple username and password word sign in credentials for SAP Concur solutions, they must complete the enrollment process for each set of credentials.

### ***Enrollment Process via QR code with email requirement***

By default, the 2FA enrollment process requires that users have a valid **Email 1** or **Email 2** address configured in the **Email Addresses** section of the **My Profile – Personal Information** page in SAP Concur solutions. Users who do not have access to the **Email Addresses** section of the **My Profile – Personal Information**—for example, invoice-only users—must have a valid email address associated with their user account.

---

**NOTE:** A Concur company administrator can disable the option to require a valid email address. For more information, refer to the *Administrator Opt-Out of Email Requirement* section of this document.

---

#### ► **To enroll in 2FA**

1. On the Concur mobile or web sign in page, enter your SAP Concur username and password.

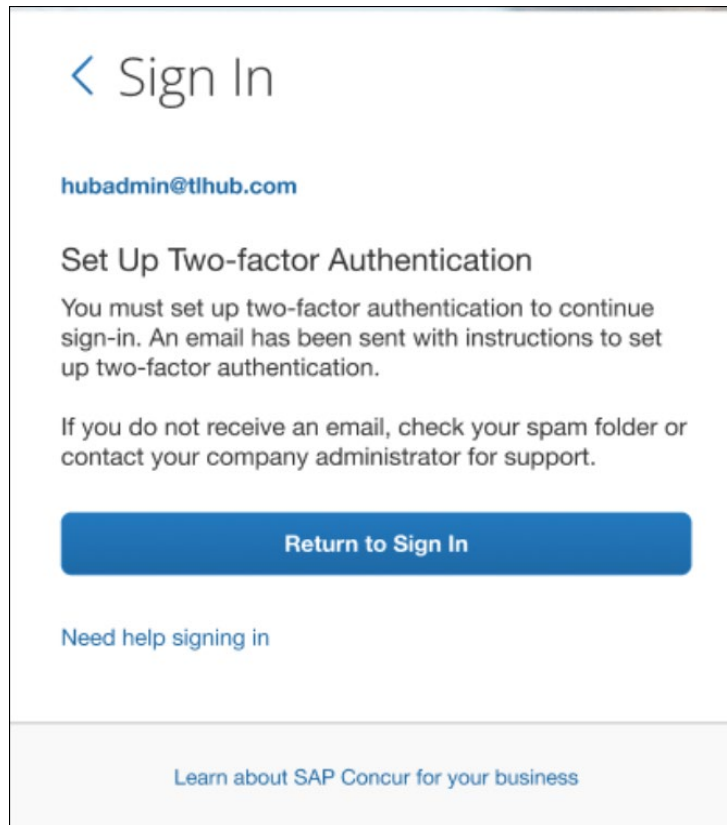
The image displays two sequential screenshots of the SAP Concur sign-in interface. The left screenshot shows the initial 'Sign In' page. It features a text input field labeled 'Username, verified email address, or SSO code' with the value 'InvoiceUser@Test\_CA.com' entered. Below the field is a blue 'Next' button. At the bottom, there are three links: 'Remember me' (with an unchecked toggle), 'Forgot username', and 'Need help signing in'. The right screenshot shows the subsequent step after clicking 'Next'. It has a '< Sign In' header. The email 'InvoiceUser@Test\_CA.com' is displayed above a 'Password' field, which contains masked characters. A blue 'Sign In' button is shown with a cursor clicking it. Below the button are two links: 'Forgot password' and 'Need help signing in'.

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**.



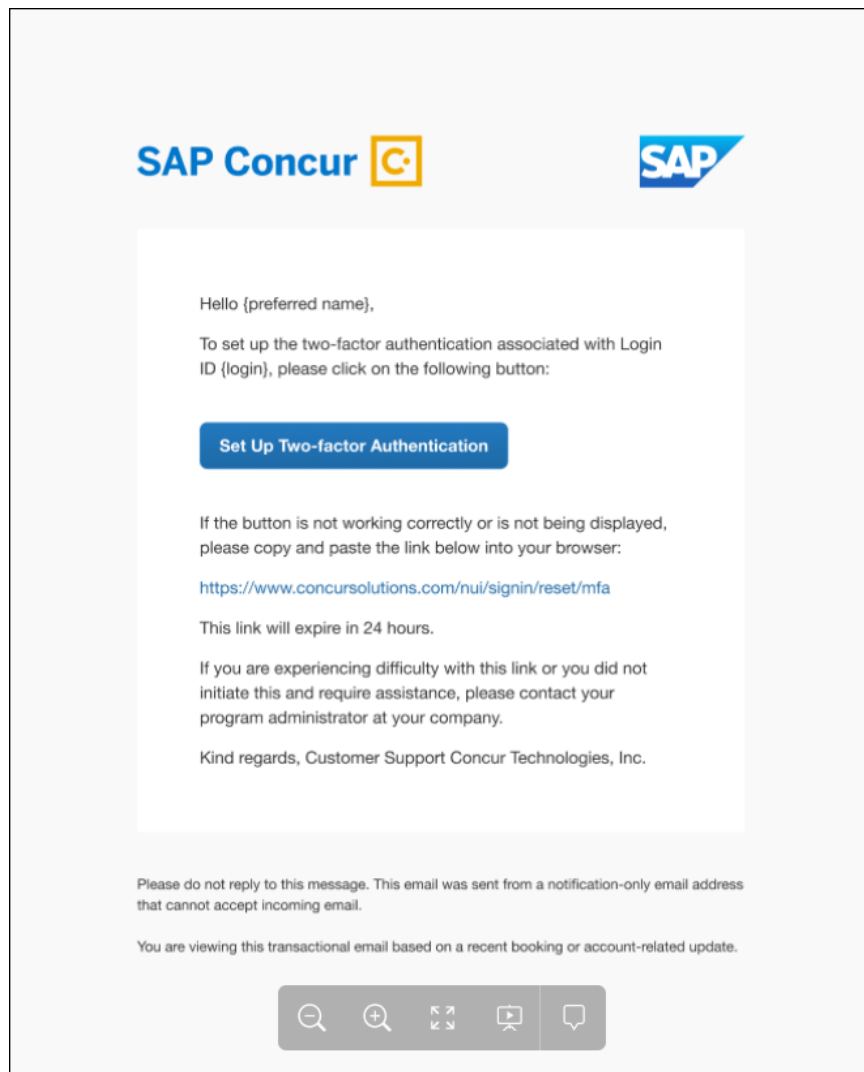
3. Open the email that was sent to the email address(es) configured on the **My Profile – Personal Information** page or to the email address associated with your user account.

---

**NOTE:** If you did not receive the email, check your spam folder or contact your company's Concur administrator or IT department.

---

4. Click **Set Up Two-Factor Authentication**.



5. On the SAP Concur sign in page, enter your password and click **Next**.

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

< Sign In

auth.test@concur.com

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?  
Set up manually with a key  
Authentication Code

Sign In

Need help signing in

Learn about SAP Concur for your business

- ♦ If you are using a mobile device to setup 2FA and have already downloaded an authenticator app, you can scan the QR code on the **Set Up Two-Factor Authentication** page to begin setting up 2FA for SAP Concur solutions.
  - ♦ If you do not yet have an authenticator app setup, you can download one and then proceed to setup 2FA.
  - ♦ If you do not have a mobile device or prefer not to use one for this process, you can use an authenticator app in a web browser.
7. Follow the steps or prompts from the authenticator app to generate a 6-digit code. These steps vary depending on which authenticator app you are using.

---

**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.

---

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



The screenshot shows the 'Sign In' page for SAP Concur. At the top, there is a back arrow and the text 'Sign In'. Below this is a blurred area representing a user's profile. The main heading is 'Set Up Two-factor Authentication', followed by instructions: '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.' A QR code is displayed in the center. Below the QR code, there is a link 'Can't scan the QR code?' and a sub-link 'Set up manually with a key'. An 'Authentication Code' input field contains the text '111111'. A blue 'Sign In' button is at the bottom, with a mouse cursor hovering over it. Below the button is a link 'Need help signing in'. At the very bottom, there is a link 'Learn about SAP Concur for your business'.

### ***Enrollment Process with email requirement using a Manual Key***

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.

1. On the Concur mobile or web sign in page, enter your SAP Concur username and password.

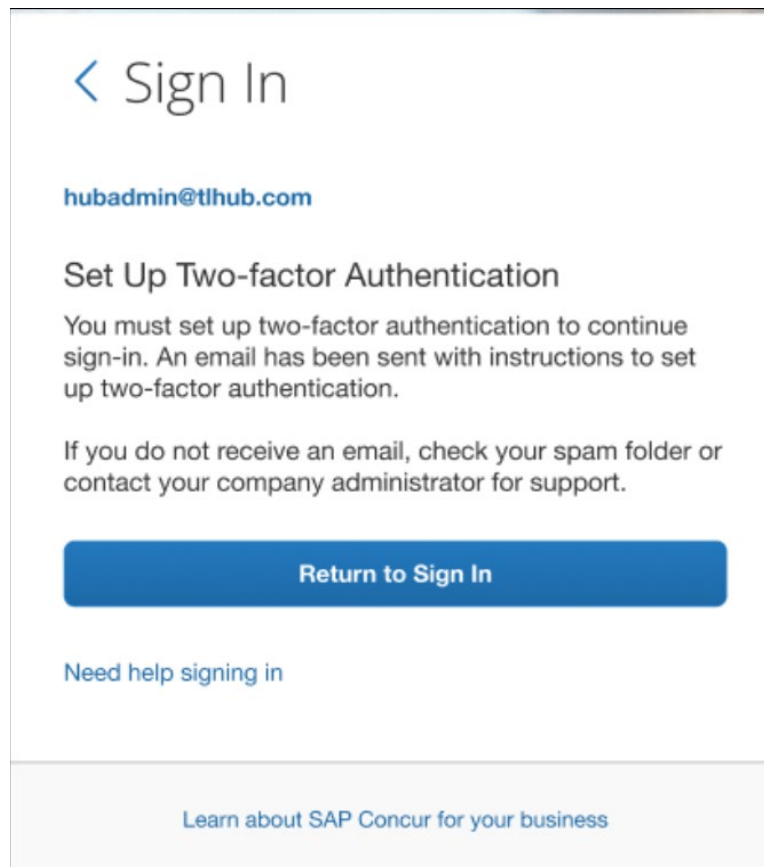


2. The following message is presented:

"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**.



3. Open the email that was sent to the email address configured on the **My Profile – Personal Information** page or to the email address associated with your user account.

---

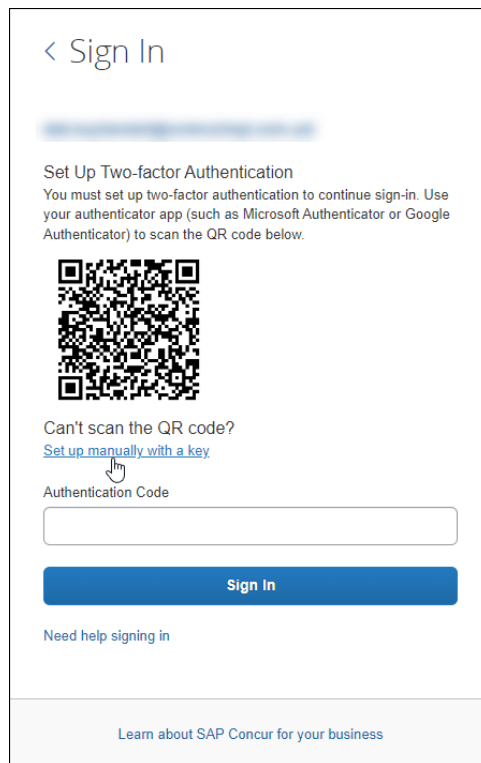
**NOTE:** If you did not receive the email, check your spam folder or contact your company's Concur administrator or IT department.

---

In the body of the email, click **Set Up Two-Factor Authentication**.


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

5. Click **Set up manually with a 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?  
[Set up manually with a key](#)

Authentication Code

Sign In

[Need help signing in](#)

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

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: 7MHHZN6RZET7O07Y2BELQVAP4DTQ2KG

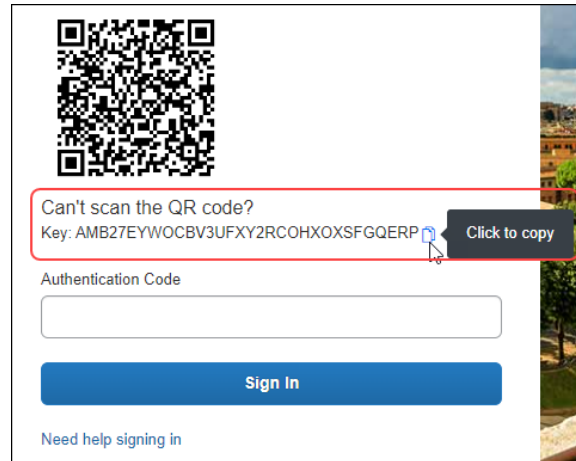
Authentication Code

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.



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".
  - ♦ 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**.

### ***Enrollment Process via QR code without the email requirement***

By default, the 2FA enrollment process requires that users have a valid **Email 1** or **Email 2** address configured in the **Email Addresses** section of the **My Profile – Personal Information** page in SAP Concur solutions.

Although it is not recommended, the default email requirement can be disabled by a company administrator.

► **To enroll in 2FA without an email link**

1. On the Concur mobile or web sign in page, enter your SAP Concur username and password.

The left screenshot shows the 'Sign In' page with a username field containing 'InvoiceUser@Test\_CA.com' and a 'Next' button. The right screenshot shows the 'Sign In' page with a password field containing '.....' and a 'Sign In' button being clicked by a mouse cursor.

2. The following message is presented:

“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.”

The screenshot shows the 'Set Up Two-factor Authentication' page. It displays a QR code for scanning. Below the QR code, there is a link 'Can't scan the QR code? Set up manually with a key' and an 'Authentication Code' input field. A 'Sign In' button is at the bottom.

3. If you are using a mobile device to setup 2FA and have already downloaded an authenticator app, launch the authenticator app.

- ◆ If you do not yet have an authenticator app, download one and then proceed to setup 2FA.
  - ◆ If you do not have a mobile device or prefer not to use one for this process, you can use an authenticator app in a web browser.
4. Follow the steps or prompts from the authenticator app to scan the QR code on the **Set Up Two-factor Authentication** page and generate a 6-digit code.

The steps vary depending on which authenticator app you are using.

---

**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.

---

5. On the SAP Concur **Sign In** page, enter the 6-digit code into the **Authentication Code** field in the **Set Up Two-Factor Authentication** section and then click **Sign In**.



The screenshot shows the SAP Concur Sign In page. At the top, there is a back arrow and the text "Sign In". Below this is a blurred header. The main section is titled "Set Up Two-factor Authentication" and contains the text: "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." A QR code is displayed. Below the QR code, there is a link: "Can't scan the QR code? Set up manually with a key". Underneath is the "Authentication Code" label and a text input field containing "111111". A blue "Sign In" button is below the input field, with a mouse cursor pointing at it. At the bottom left of the form area is a link: "Need help signing in". At the very bottom of the page is a link: "Learn about SAP Concur for your business".

## ***Enrollment Process without email requirement using a Manual Key***

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.

1. On the Concur mobile or web sign in page, enter your SAP Concur username and password.

The image displays two sequential screenshots of the SAP Concur sign-in interface. The left screenshot shows the initial sign-in page with a 'Sign In' header, a text input field for 'Username, verified email address, or SSO code' containing 'InvoiceUser@Test\_CA.com', and a blue 'Next' button. Below the button are links for 'Remember me', 'Forgot username', and 'Need help signing in'. The right screenshot shows the next step where the password is entered. The 'Sign In' button is now highlighted with a cursor, and the password field contains masked characters. The same help links are present at the bottom of both screens.

2. The following message is presented:

“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.”

This screenshot shows the 'Set Up Two-factor Authentication' page. It features a QR code for scanning. Below the QR code, there is a link that reads 'Can't scan the QR code? Set up manually with a key'. Underneath this link is an 'Authentication Code' input field. At the bottom of the page is a blue 'Sign In' button and a link for 'Need help signing in'.

3. Click the **Set up manually with a key** link.

The manual setup key is presented.

4. 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: 7MHHZN6RZET7007Y2BELQVAP4DTQ2KG 

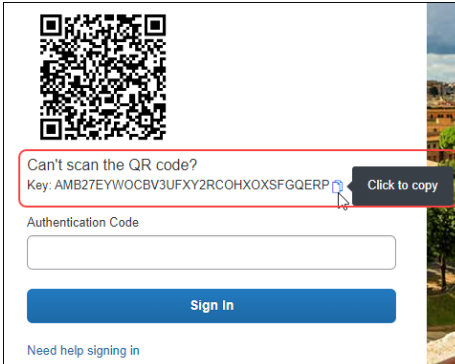
Authentication Code

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: AMB27EYWOCBV3UFXY2RCOHXOXSGQERP  Click to copy

Authentication Code

Sign In

[Need help signing in](#)

5. 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".
  - ♦ 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.

---

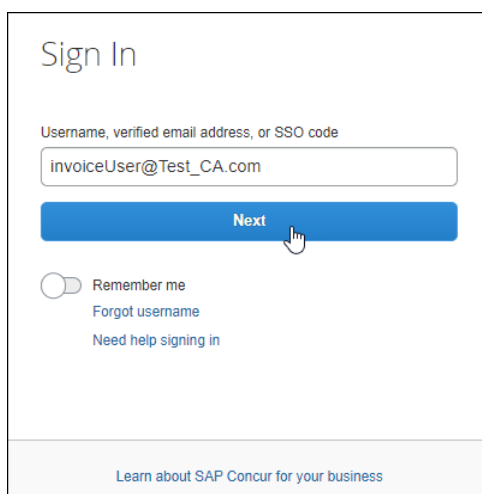
6. After you enter the key manually and follow the steps in your authenticator app, the authenticator app will generate a 6-digit code. Enter the code into the **Authentication Code** field on the **Set Up Two-Factor Authentication** page.
7. Click **Sign In**.

## User Experience After Enrollment

After a user has enrolled in 2FA for SAP Concur, after entering their username and password to sign in to SAP Concur solutions, they are prompted to enter the 6-digit authentication code generated by their authenticator app.

### ► *To sign in to SAP Concur solutions with 2FA*

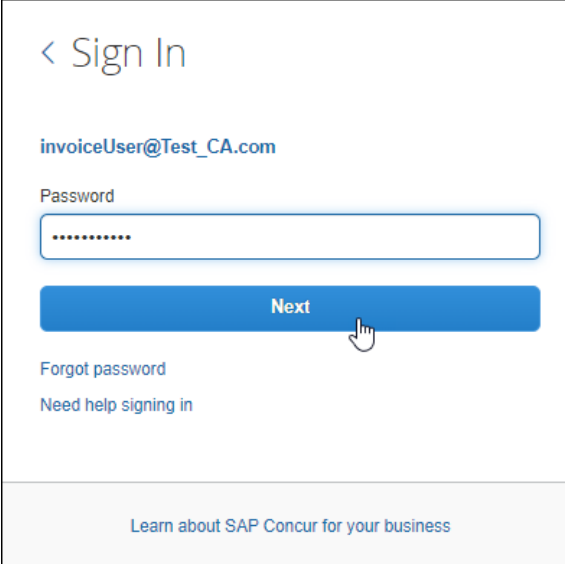
1. Navigate to concursolutions.com or open Concur Mobile.
2. Enter your username.



The screenshot shows the 'Sign In' page of SAP Concur. At the top, the text 'Sign In' is displayed. Below it, a label reads 'Username, verified email address, or SSO code'. A text input field contains the email 'invoiceUser@Test\_CA.com'. A blue 'Next' button is positioned below the input field, with a mouse cursor hovering over it. Underneath the button, there is a 'Remember me' toggle switch (currently off), a link for 'Forgot username', and a link for 'Need help signing in'. At the bottom of the page, there is a link that says 'Learn about SAP Concur for your business'.

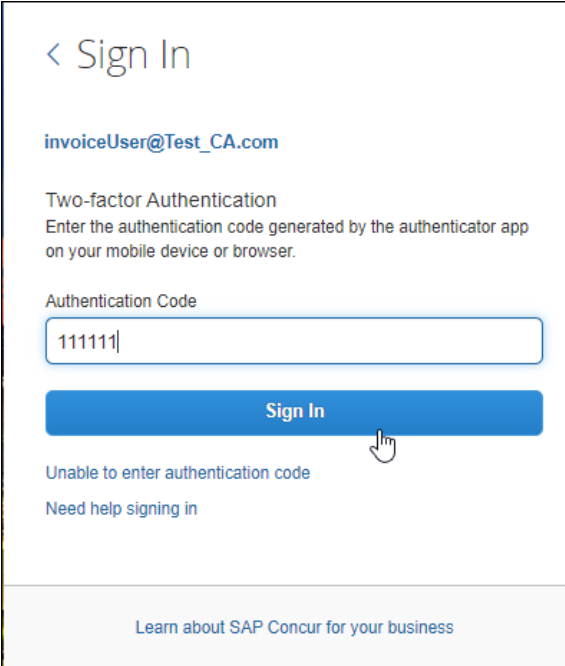


3. Enter your password.



The screenshot shows the 'Sign In' screen for SAP Concur. At the top, there is a back arrow and the text '< Sign In'. Below this, the email address 'invoiceUser@Test\_CA.com' is displayed. Under the email, the label 'Password' is shown above a text input field containing seven dots. A blue button labeled 'Next' is positioned below the password field, with a mouse cursor hovering over it. Below the 'Next' button, there are two links: 'Forgot password' and 'Need help signing in'. At the bottom of the screen, there is a link that says 'Learn about SAP Concur for your business'.

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



The screenshot shows the 'Sign In' screen for SAP Concur, specifically the two-factor authentication step. At the top, there is a back arrow and the text '< Sign In'. Below this, the email address 'invoiceUser@Test\_CA.com' is displayed. Under the email, the text 'Two-factor Authentication' is shown, followed by the instruction 'Enter the authentication code generated by the authenticator app on your mobile device or browser.' Below this instruction, the label 'Authentication Code' is shown above a text input field containing the code '111111'. A blue button labeled 'Sign In' is positioned below the authentication code field, with a mouse cursor hovering over it. Below the 'Sign In' button, there are two links: 'Unable to enter authentication code' and 'Need help signing in'. At the bottom of the screen, there is a link that says 'Learn about SAP Concur for your business'.

## User-initiated Reset for 2FA

You might need to reset and re-enable 2FA for Concur sign in. For example, you might replace the mobile device you initially used to set up 2FA, or you might want to change your authenticator app.

Resetting 2FA has the following prerequisites:

- User-initiated 2FA reset cannot be completed in Concur Mobile. You must reset 2FA by signing in to concursolutions.com via a web browser.
- You must have a valid **Email 1** or **Email 2** address configured in the **Email Addresses** section of the **My Profile – Personal Information** page in SAP Concur solutions.

Some users do not have access to the **Email Addresses** section of the **My Profile – Personal Information** page—for example, Concur Invoice-only users.

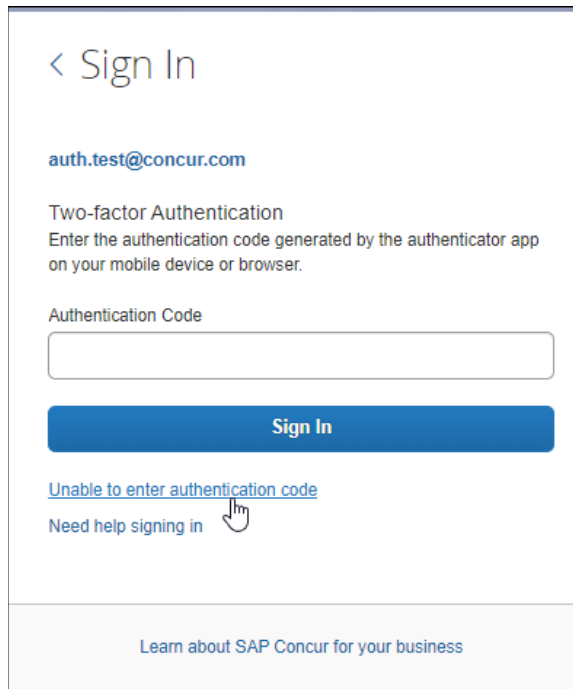
If you do not have access the **Email Addresses** section of the **My Profile – Personal Information** page, you can contact your company's Concur administrator to confirm you have a valid email address associated with your Concur user account.

- You must be able to access email sent to the configured **Email 1** or **Email 2 address**. Or, in the case of users who do not have access to the **Email**

**Addresses** section of the **My Profile – Personal Information** page, access to email sent to the email address configured in your user account.

► **To reset 2FA**

1. On the SAP Concur sign in page, enter your username and password.
2. On the **Two-factor Authentication** page, click **Unable to enter authentication code**.



< Sign In

auth.test@concur.com

Two-factor Authentication  
Enter the authentication code generated by the authenticator app on your mobile device or browser.

Authentication Code

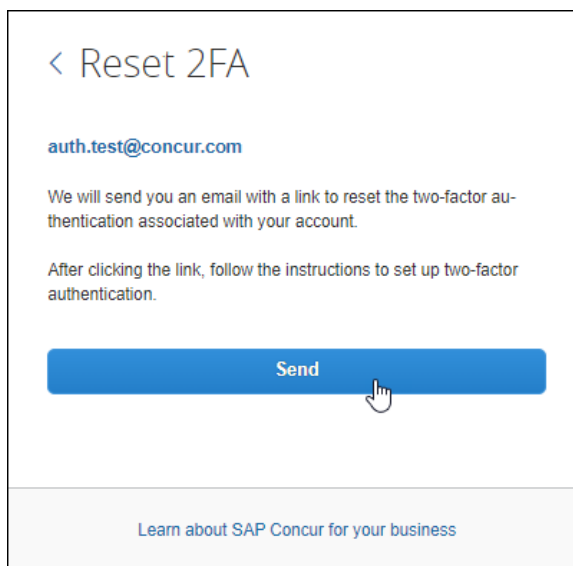
Sign In

[Unable to enter authentication code](#)

Need help signing in

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

3. On the **Reset 2FA** page, click **Send**.



< Reset 2FA

auth.test@concur.com

We will send you an email with a link to reset the two-factor authentication associated with your account.

After clicking the link, follow the instructions to set up two-factor authentication.

Send

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

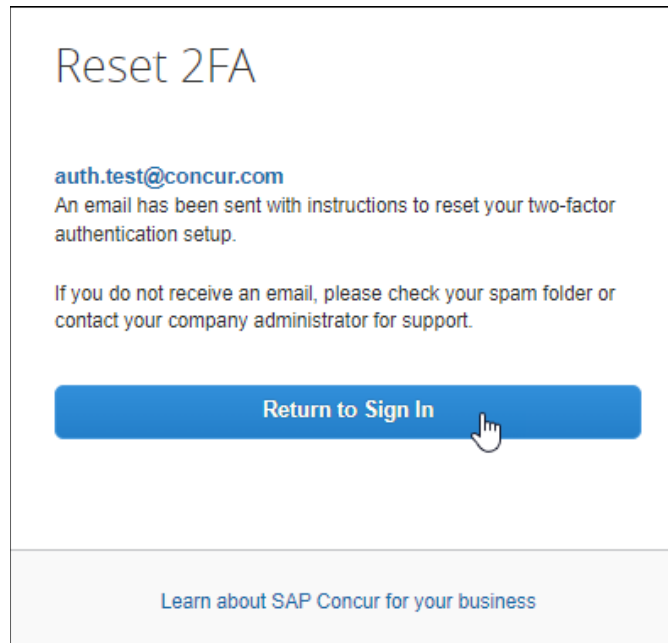
A reset email is sent to the **Email 1** and/or **Email 2** addresses configured in the **Email Addresses** section of the **My Profile – Personal Information** page in SAP Concur solutions.

---

**NOTE:** The reset link will not be sent to addresses after **Email 2**.

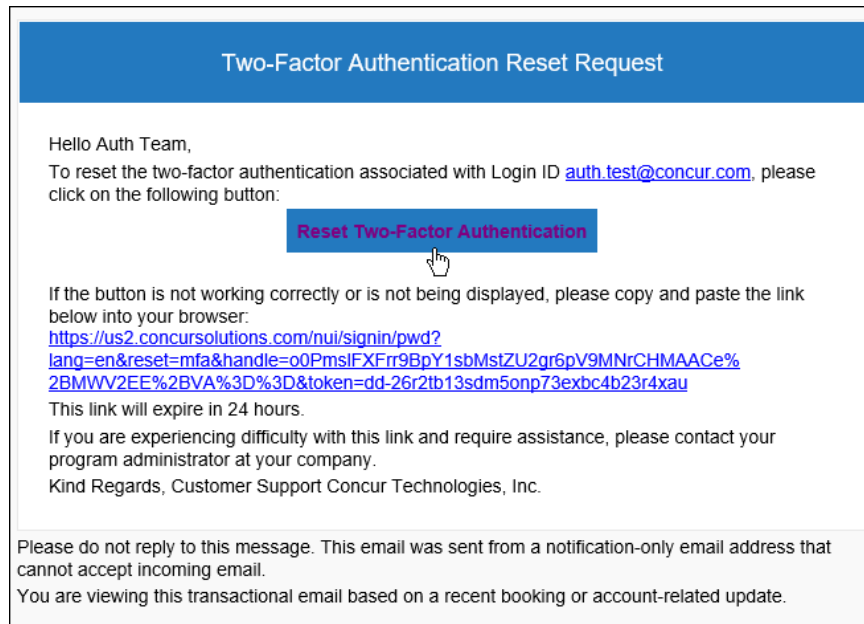
---

4. Click **Return to Sign In**.



5. Open the **Two-Factor Authentication Reset Request** that was sent from noreply@concur.com to the address (**Email 1** and/or **Email 2**) configured on the **My Profile – Personal Information** page in SAP Concur solutions.

6. In the email, click **Reset Two-Factor Authentication**.



7. On the SAP Concur **Sign In** page, enter your password.

---

**NOTE:** You will not be prompted to enter your username. The username associated with the configured email address is automatically used to sign in.

---

8. On the **Set Up Two-factor Authentication** page, follow the steps in *Section 2: Enroll in 2FA* to re-enroll in 2FA for SAP Concur.

## Administrator Reset for 2FA

If a user is unable to reset 2FA, a company administrator with the permission to administer users can reset 2FA for the affected user.

### **Professional Edition**

#### ► **To reset 2FA for a user**

1. Sign in to SAP Concur solutions as an administrator with permission to administer users. For example, **User Administration** or **Company Administration**.
2. Open the user account page for the user who needs 2FA to be reset.
3. In the **MFA Reset** section of the user's account page, click **Reset**.



The screenshot shows a user interface for MFA Reset and General Settings. At the top, there is a section titled "MFA Reset" with a blue "Reset" button. Below the button, a text line states: "This resets the user's MFA details, and they must now re-register their MFA methods upon their next sign-in." Below this is a section titled "General Settings". It contains three input fields: "CTE Login Name\*" with a subtext "(must be suffixed with a valid domain)", "Password\*" with a subtext "(Blank to leave unchanged)", and "Verify Password\*".

### ***Standard Edition (Available after November 15, 2023)***

#### **► To reset 2FA for a user**

1. Sign in to SAP Concur solutions as an administrator with permission to administer users. For example, **Travel and Expense Administrator**.
2. Open the **User Details** page for the user who needs 2FA to be reset.
3. In the **MFA Reset** section of the user's account page, click **Reset**.

## **Administrator Opt-Out of Email Requirement**

A company administrator can opt-out of the email requirement on the **Sign In Settings** page.

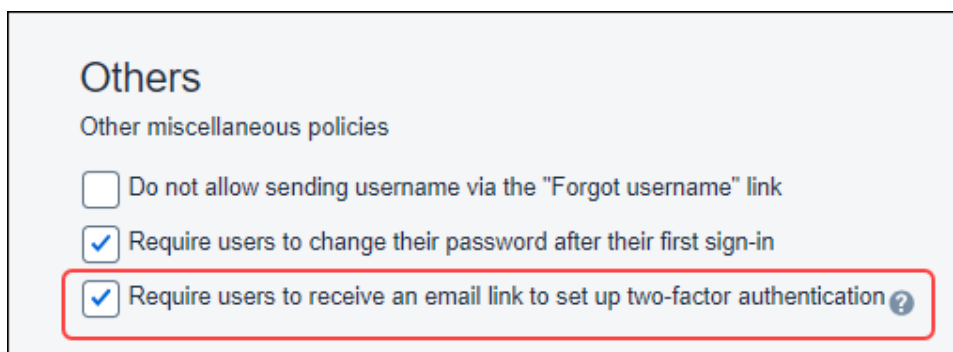
---

**NOTE:** Disabling the email requirement is not recommended as this requirement adds an additional level of security to the enrollment process.

---

#### **► To disable the email requirement for 2FA**

1. In SAP Concur solutions, navigate to **Administration > Authentication Admin > Sign In Settings**.
2. In the **Others** section of the **Sign In Settings** page, uncheck Require users to receive an email link to set up two-factor authentication.



The screenshot shows the "Others" section of the "Sign In Settings" page. It is titled "Others" with a subtitle "Other miscellaneous policies". There are three checkboxes: "Do not allow sending username via the 'Forgot username' link" (unchecked), "Require users to change their password after their first sign-in" (checked), and "Require users to receive an email link to set up two-factor authentication ?" (checked). The third checkbox is highlighted with a red rectangular border.