McGraw Hill
Supplier Portal MFA User Guide

Setting up and managing multi-factor authentication

Available MFA methods: Email, Oracle Mobile Authenticator, or Google Authenticator. SMS/text message and Microsoft Authenticator are not available options.

Use this guide the first time you are prompted to enroll in MFA and whenever you want to configure another verification method. You will continue to use your existing Supplier Portal username and password. MFA adds a second verification step.

Before you begin

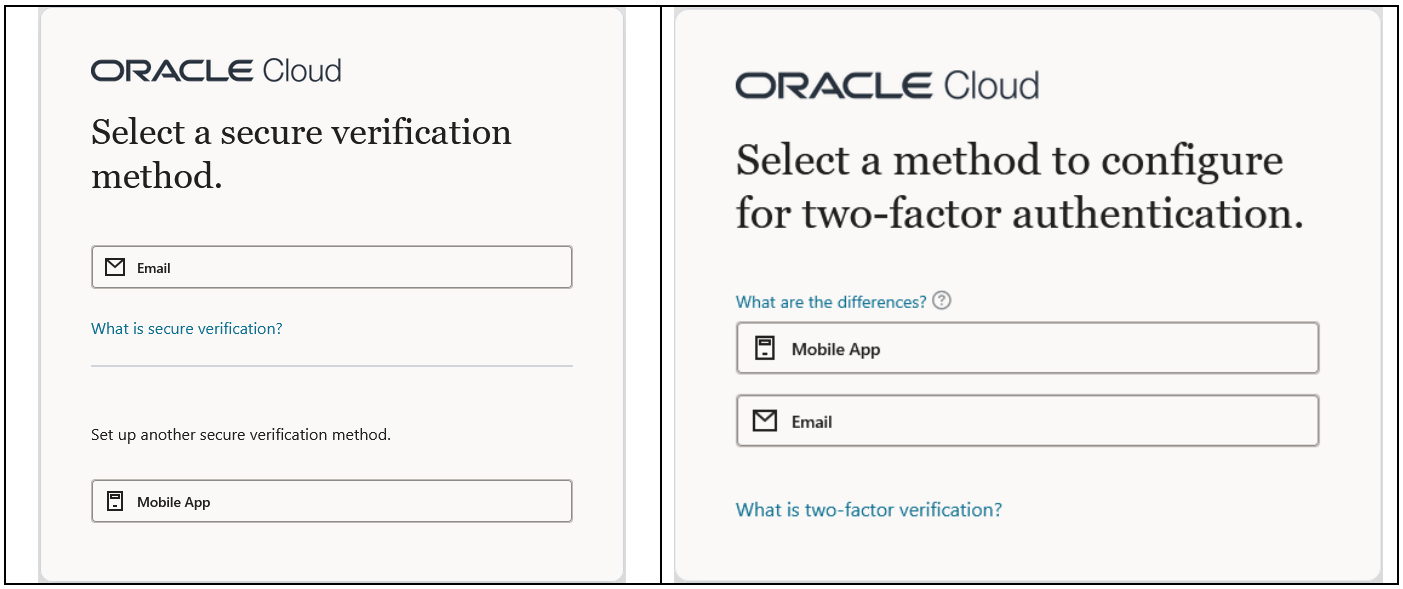
- Make sure you can access the email address associated with your Supplier Portal account.
- If using an authenticator app, install Oracle Mobile Authenticator or Google Authenticator on your mobile device before starting.
- Allow a few extra minutes for the initial setup. Email passcodes are valid for 10 minutes.

Security reminder: The screenshots in this guide are examples. Never share your verification code, QR code, or authenticator setup key with anyone.

Part 1: Select an MFA method

1 Choose a secure verification method

After signing in with your Supplier Portal username and password, you will be prompted with one of the below screens; select either Email or Mobile App.



Example: secure verification method screen

Both screen versions provide the same two choices; Mobile App or Email

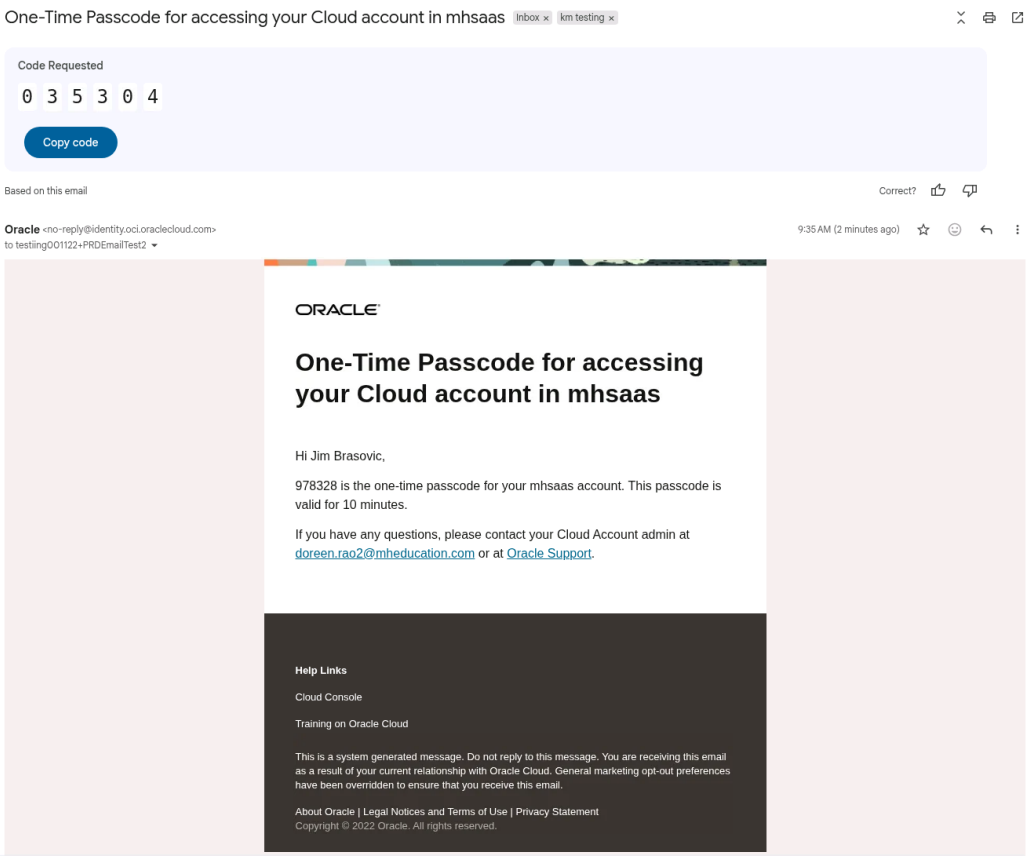
Part 2: Set up email verification

2 Select Email

Select Email and follow the on-screen instructions. Oracle sends a one-time passcode to the email address associated with your Supplier Portal account.

3 Retrieve the one-time passcode

Open the email from Oracle (no-reply@identity.oci.oraclecloud.com). Make note of the six-digit code and enter it in the verification screen. The passcode is valid for 10 minutes.

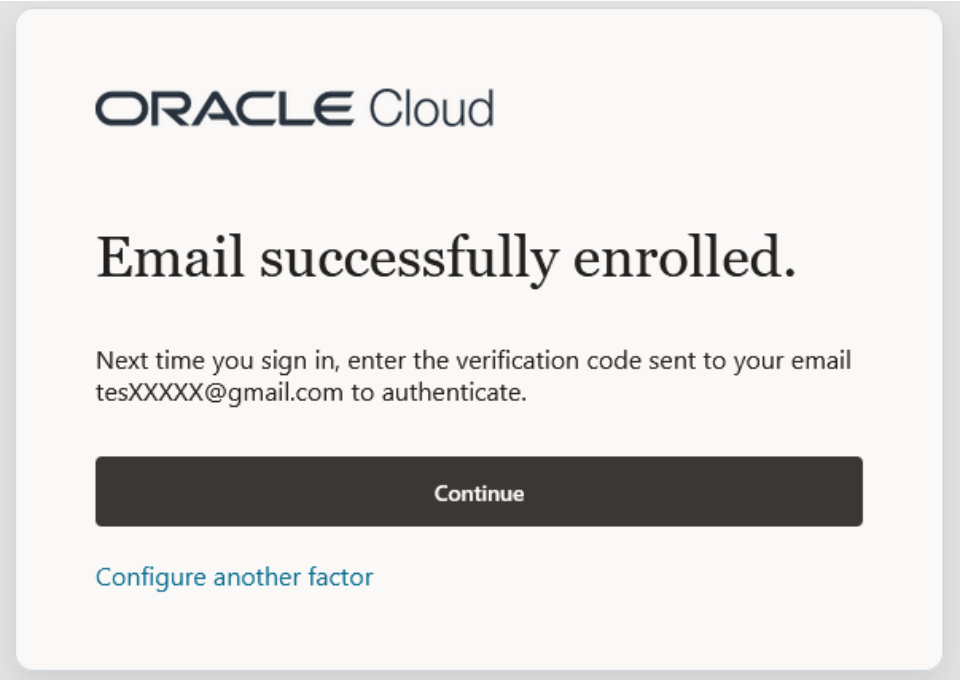


Example Oracle one-time passcode email

If the email does not arrive: Check your spam or junk folder, confirm you are checking the correct mailbox, and request a new code if the original code expires.

4 Confirm email enrollment

After the code is accepted, the Email successfully enrolled message appears. Select Continue.



Email enrollment confirmation

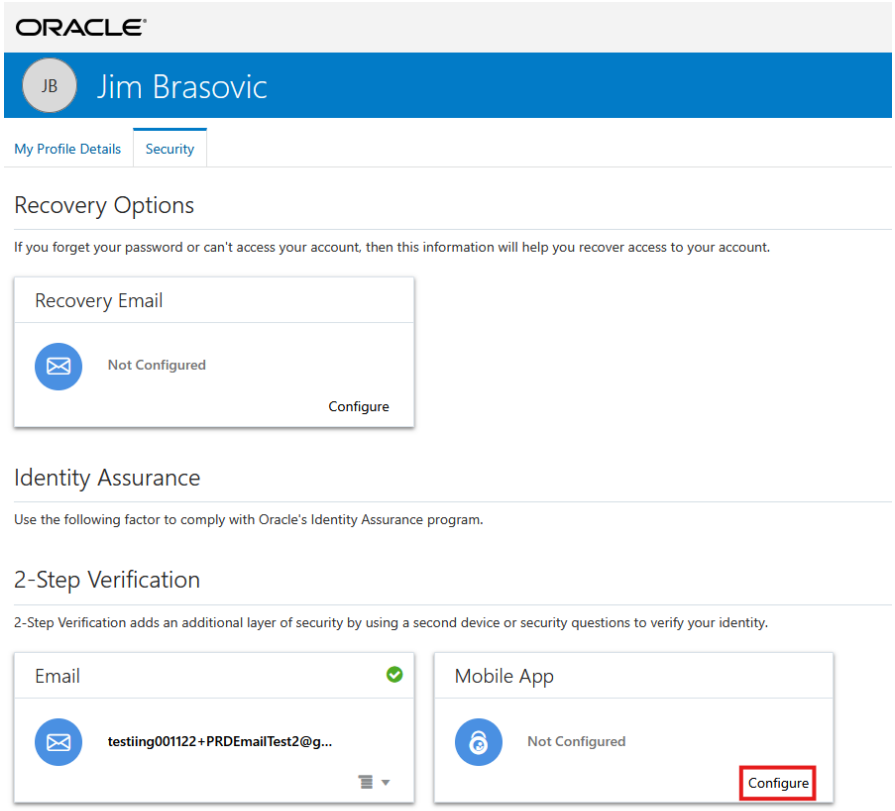
Future sign-ins: Oracle will email a new verification code when email is selected as your MFA method.

Part 3: Set up an authenticator app

To use an authenticator app, select Mobile App during initial enrollment or configure it later by following Part 4 of this guide.

5 Open Mobile App configuration

On the Security page, select Configure under Mobile App.

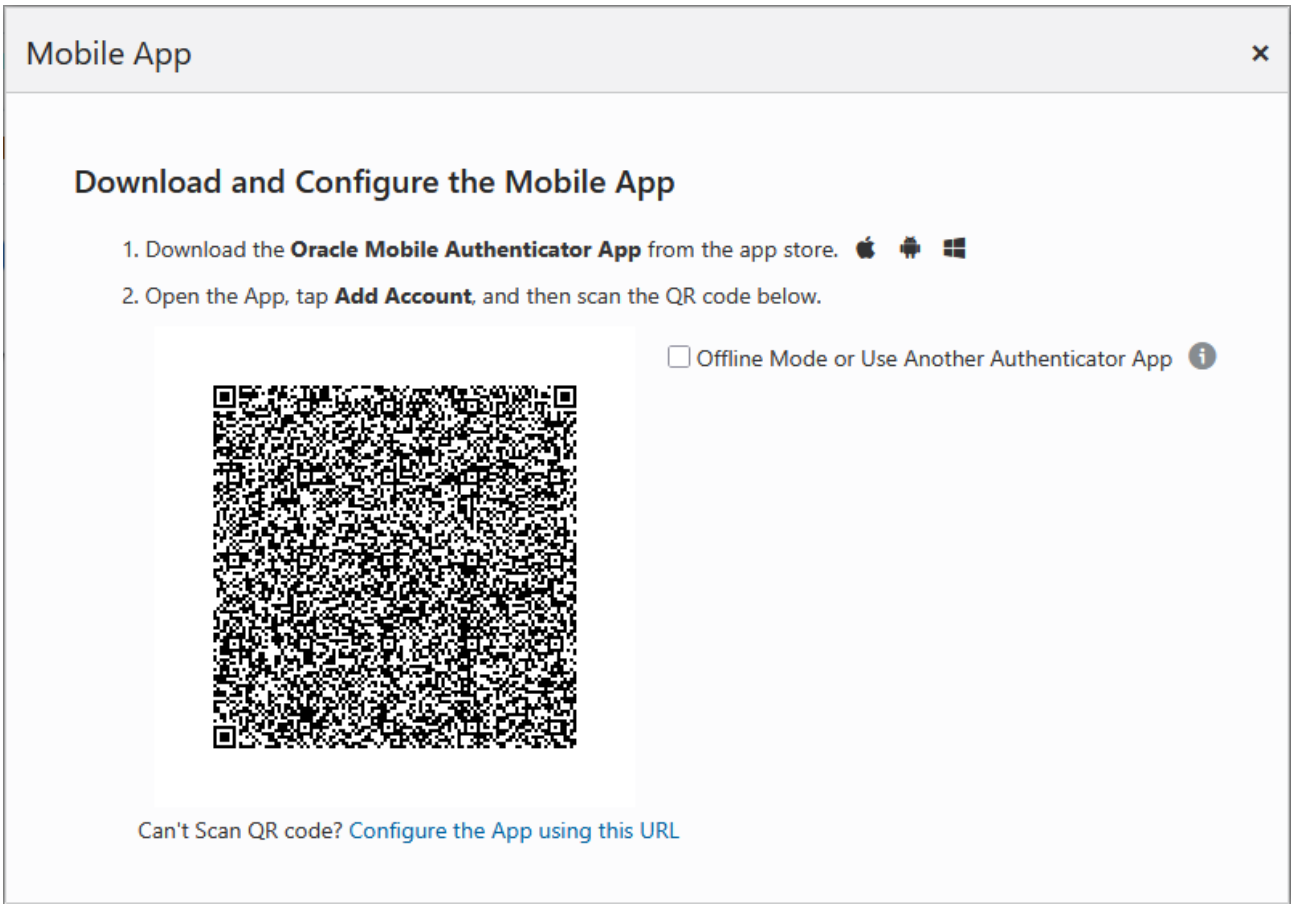


Security page showing the Mobile App Configure option

Option A: Oracle Mobile Authenticator

6 Download and configure Oracle Mobile Authenticator

Install Oracle Mobile Authenticator. Leave “Offline Mode or Use Another Authenticator App” unchecked. In the app, select Add Account and scan the QR code displayed on the screen.



Oracle Mobile Authenticator setup screen

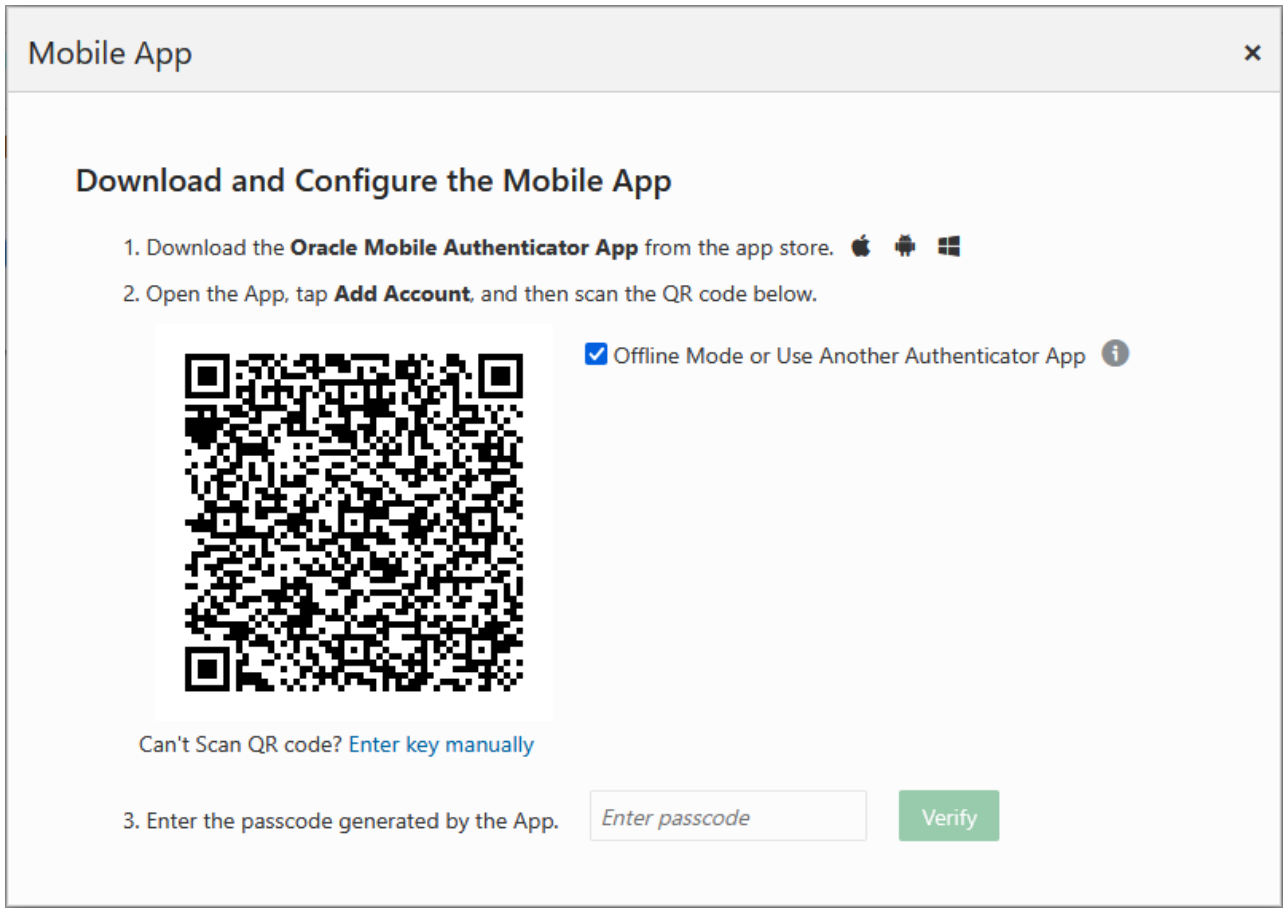
Important: The QR code shown during your setup is unique to your account. Do not use the sample QR code in this guide.

- If the QR code cannot be scanned, use the on-screen link to configure the app using a URL.
- Follow the prompts in Oracle Mobile Authenticator to finish enrollment.

Option B: Google Authenticator

7 Configure Google Authenticator

Install Google Authenticator. Check “Offline Mode or Use Another Authenticator App.” Scan the QR code, then enter the passcode generated by Google Authenticator and select Verify.



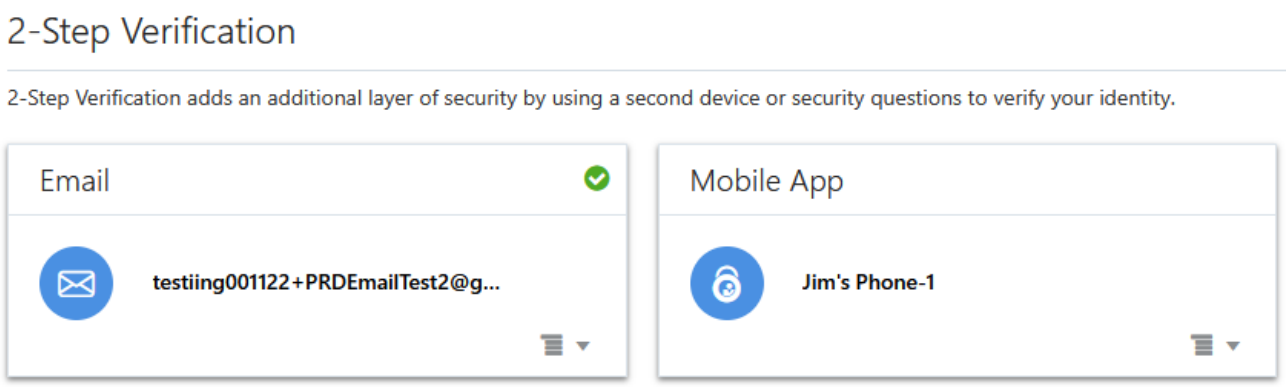
Google Authenticator setup screen

Important: The QR code and manual setup key are sensitive account credentials. Do not share or reuse the sample values shown in this guide.

- If the QR code cannot be scanned, select Enter key manually and follow the on-screen instructions.
- Authenticator passcodes change periodically. Enter the code currently displayed in the app.

8 Confirm both methods are configured

After successful setup, the 2-Step Verification page shows the configured Email and Mobile App methods.

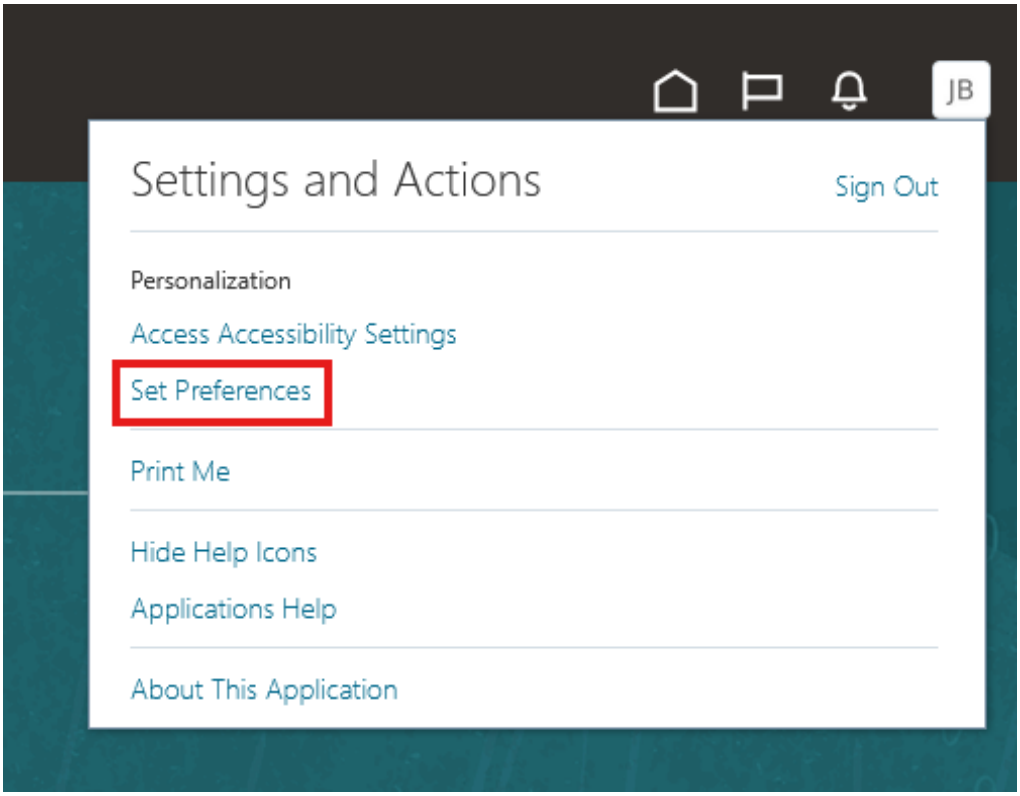


Example showing Email and Mobile App configured

Part 4: Configure another MFA method later

9 Open Settings and Actions

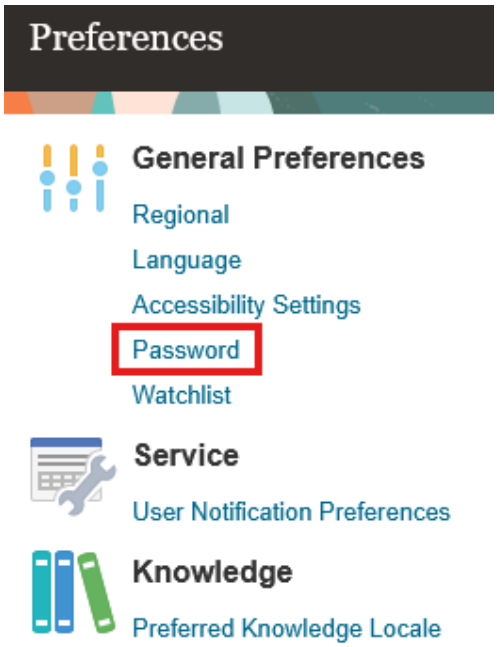
After signing in to the Supplier Portal, open the Settings and Actions menu and select Set Preferences.



Settings and Actions menu with Set Preferences selected

10 Open Password preferences

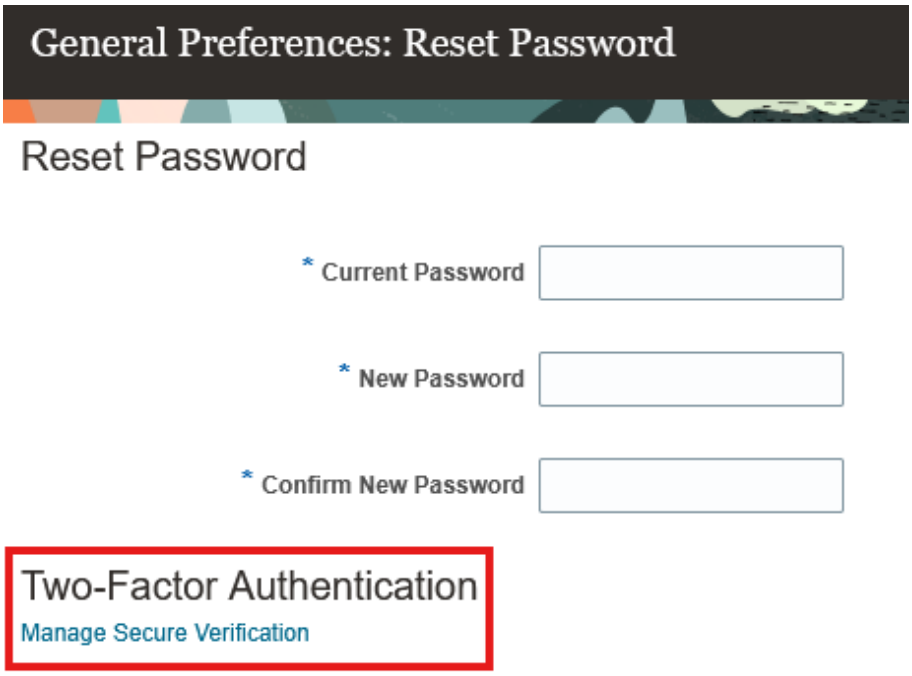
On the Preferences page, select Password under General Preferences.



Preferences page with Password selected

11 Manage secure verification

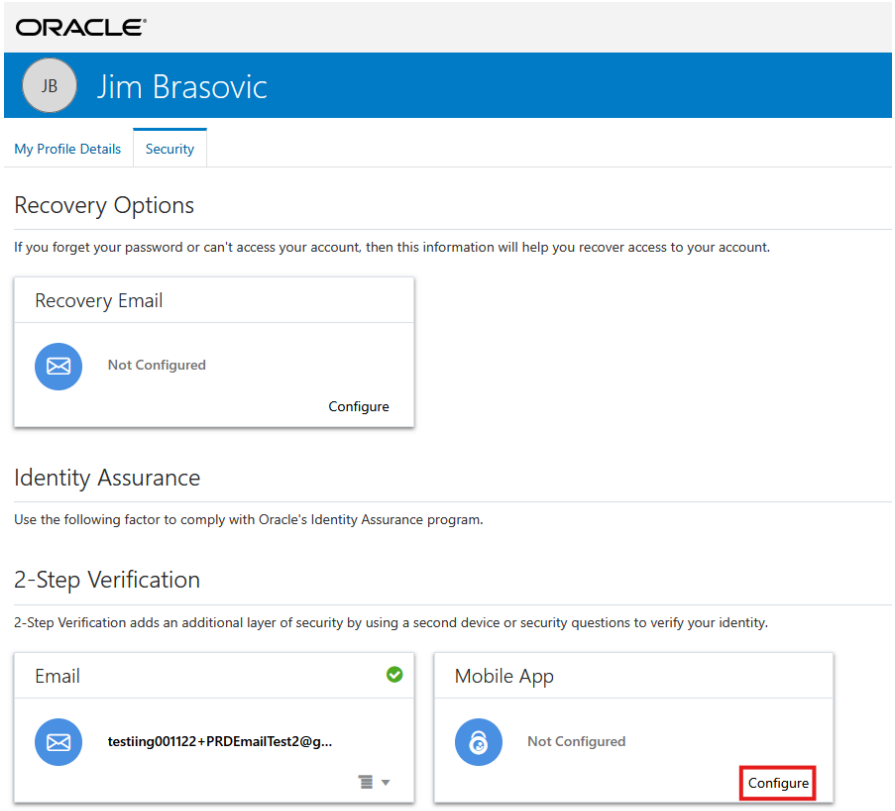
On the Reset Password page, find Two-Factor Authentication and select Manage Secure Verification.



Manage Secure Verification link

12 Configure the additional method

On the Security tab, select Configure for the method that is not yet set up. Follow the corresponding Email or Mobile App instructions in this guide.



Security page for configuring an additional factor

Need help?

If you experience difficulty setting up MFA or accessing the Supplier Portal, please complete our Supplier Support Request form, selecting **Multi-factor Authentication (MFA)** in the ***'I need assistance with:'*** field.

When requesting help: Do not send your password, verification code, QR code, or authenticator setup key.