2026

King County

Supplier Multifactor Authentication (MFA) Enablement User Guide

This guide will cover how to enable Multifactor Authentication (MFA) in the E-Procurement Supplier Portal as an existing supplier.

Contents

Enable Multifactor Authentication (MFA)

King County Suppliers will be required to enable MFA on their King County E-Procurement supplier accounts as of May 23, 2026.

- MFA is a security measure that requires an additional form of verification besides your password to access a digital account, such as a one-time code sent to your phone, email, or authenticator app.
- Setting up MFA is a one-time action. Once MFA is set up, you’ll be asked to verify your identity every time you sign in to the King County Supplier Portal.

Please email Procurement.Web@kingcounty.gov if you do not have a smart device to enable MFA.

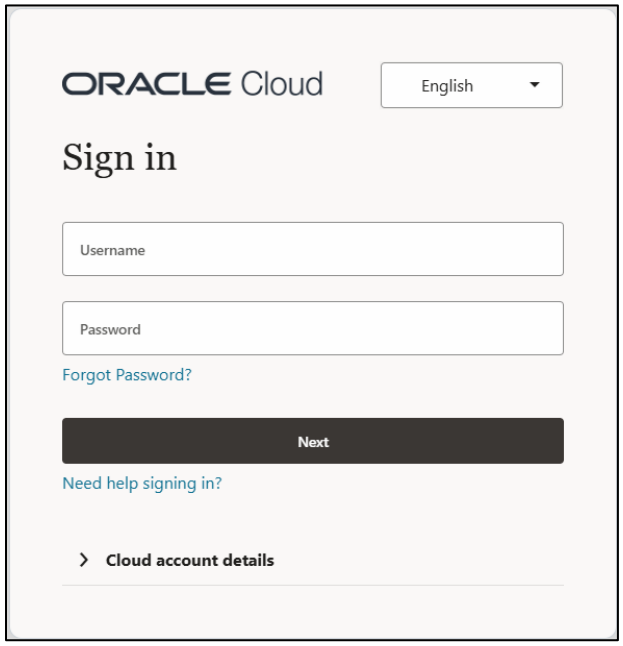
I. Sign in

1. Sign in

Sign in to the E-Procurement Supplier Portal using your Username and Password, then select "Next."

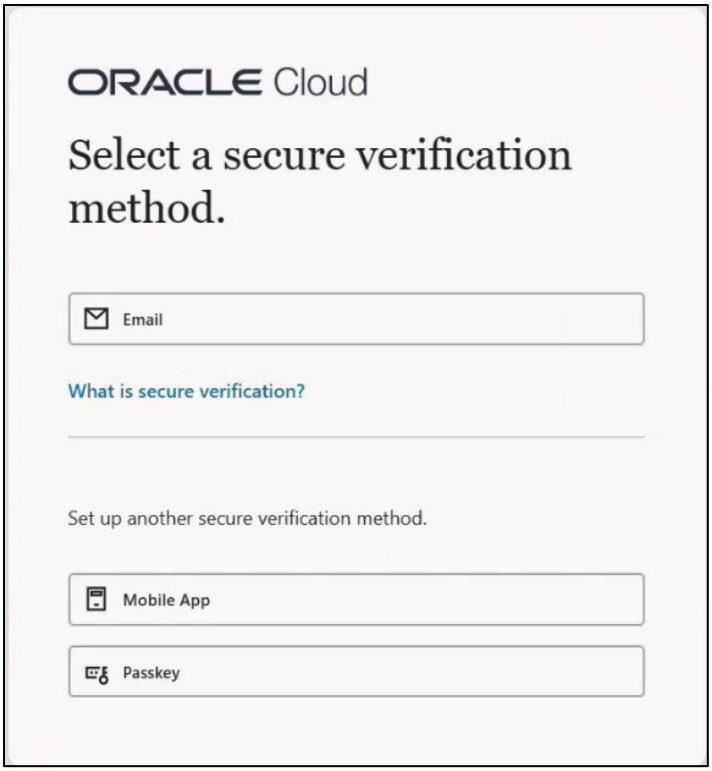
Note: use supporting web browsers: Mozilla Firefox, Google Chrome, Microsoft Edge, and Apple Safari.

Do not use the "Sign in with KC Identity…" option.



2. Enable MFA

You will be redirected to enable MFA if your username and password are entered correctly and the password is active. You will have the option to enable **one** of **three** available methods to set up two-factor authentication: **Email**, **Mobile App** or **Passkey**. Follow the instructions under part **III. Two-factor authentication set up.**



3. Reset password

Reset your expired password if prompted. Enter your current password, then create and confirm a new one. Select **"Reset Password."**

Password requirements:

- The password must have at least 8 characters
- The password must have at least 1 uppercase character
- The password must have at least 1 numeric characters
- The password must have at least 1 special characters
- Cannot repeat the current password

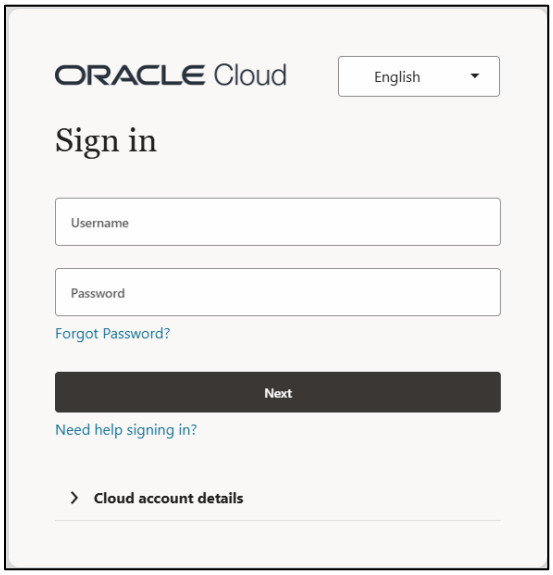
After resetting your password, you can enable **one** of **three** two-factor authentication methods: **Email, Mobile App** or **Passkey**. Follow the instructions under part **III. Two-factor authentication setup.**

If you do not remember your password, follow the steps under **"Sign in (Invalid username or password)."**

II. Sign in (Invalid username or password)

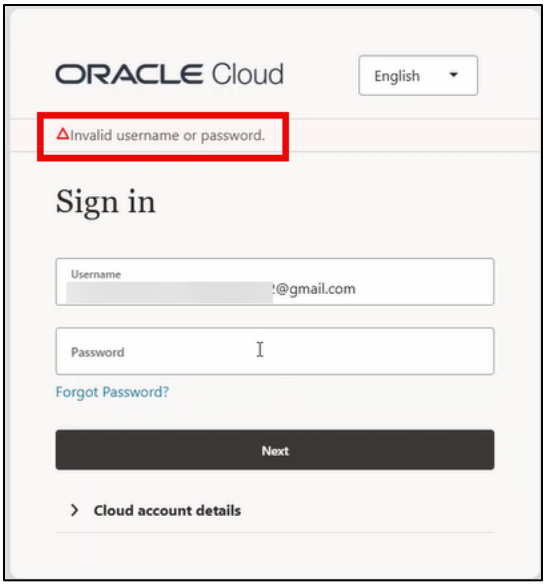
1. Sign in

Sign in to the E-Procurement Supplier Portal using your Username and Password.



2. "Invalid username or password" Error

If your username or password is entered incorrectly, you will receive an "Invalid username or password" error when attempting to sign in. To regain access to your account, reset your password using the "Forgot Password?" option. After completing the reset, you will receive an Oracle kcbrcps email prompting you to enable MFA for your E-Procurement Supplier Portal.



3. Reset password

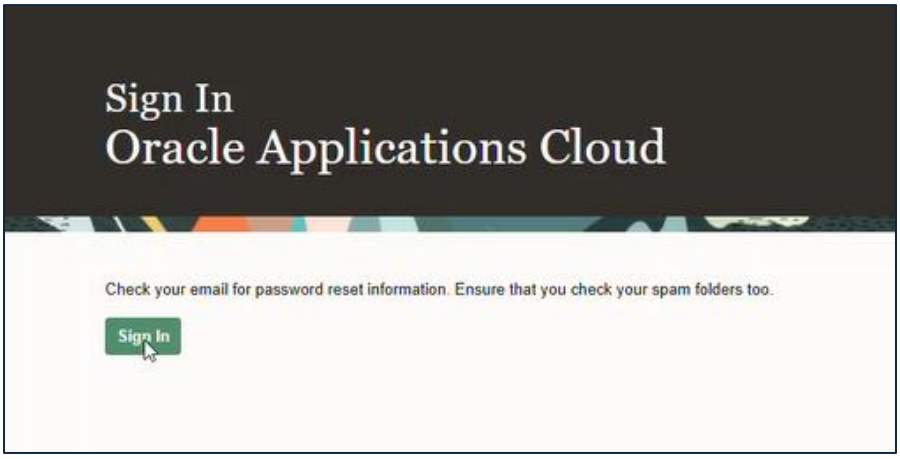
To reset your password, select “Forgot Password?”

4. “Forgot password”

Enter your “User ID” (the email used to register), select the “Forgot Password” option, and select “Submit.”

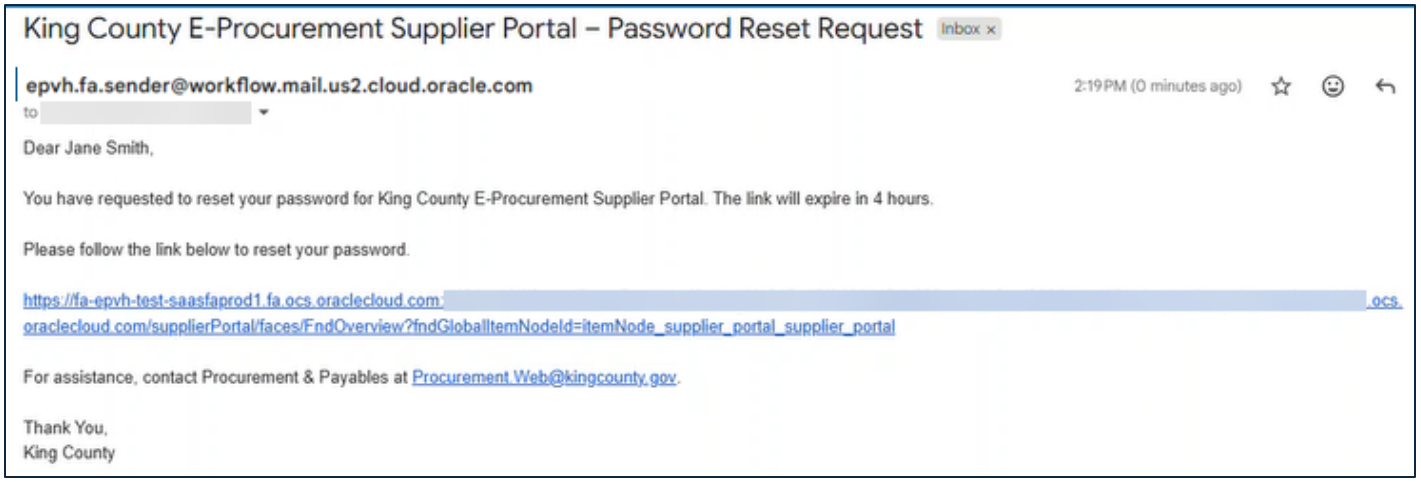
5. Sign in Oracle Applications Cloud webpage

   The Sign In Oracle Applications Cloud webpage will appear, instructing you to check your email for password reset information. **Do not select "Sign In" until you've reset your password and enabled MFA.**



6. Oracle email 1 - Password Reset Request

Email 1 of 2 (Action Required): You will receive an email from ***epvh.fa.sender@workflow.mail.us2.cloud.oracle.com*** with instructions to reset your password. Select the link in the email to begin the password reset process.


King County E-Procurement Supplier Portal – Password Reset Request Inbox ×

epvh.fa.sender@workflow.mail.us2.cloud.oracle.com 2:19 PM (0 minutes ago)

to

Dear Jane Smith,

You have requested to reset your password for King County E-Procurement Supplier Portal. The link will expire in 4 hours.

Please follow the link below to reset your password.

https://fa-epvh-test-saasfaprod1.fa.ocs.oraclecloud.com ocs.oraclecloud.com/supplierPortal/faces/FndOverview?fndGlobalItemNodeId=itemNode_supplier_portal_supplier_portal

For assistance, contact Procurement & Payables at Procurement.Web@kingcounty.gov.

Thank You,
King County

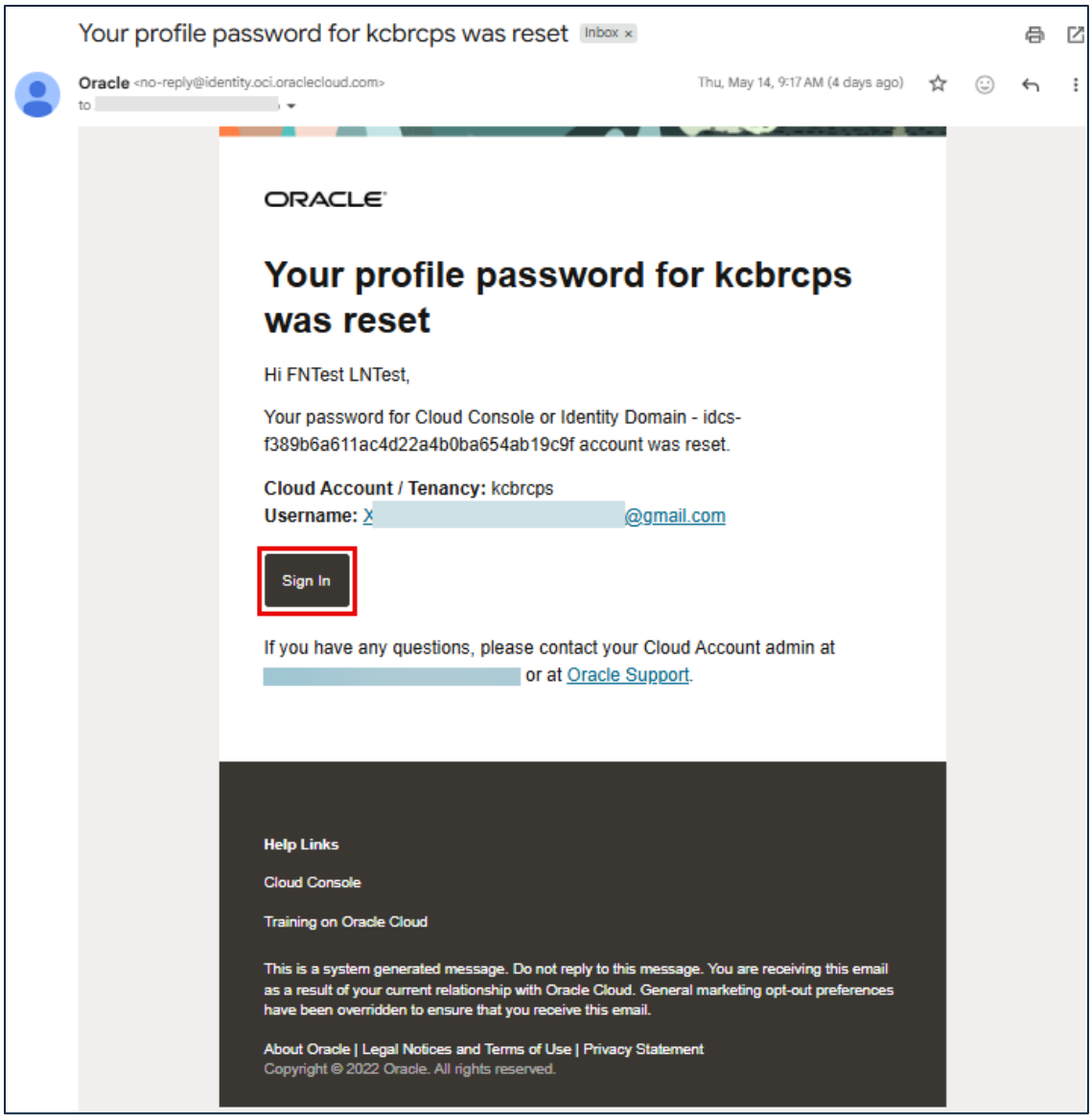
7. Reset password

A reset password webpage will appear. Enter a new password, confirm it, and select "Submit." Then return to your email inbox.

8. Oracle email 2 - password reset confirmation

Email 2 of 2 (Action Required): A second email will come from Oracle (*no-reply@identity.oci.oraclecloud.com*) confirming your password for kcbrcps was reset. Select "**Sign In**" in the email to begin enabling MFA for your user account.

- Each contact with a user account will receive an email to enable their own MFA. **All users must enable MFA** to sign in.
- If this email is missing, please check your spam, junk, and quarantine folders. If the email never arrives, please email Procurement.Web@kingcounty.gov for assistance.



By resetting your password and signing in using the Oracle kcbrcps email, you will be able to enable **one** of **two** two-factor authentication methods: **Mobile App** or **Passkey**. Follow the instructions under **part III. Two-factor authentication set up.**

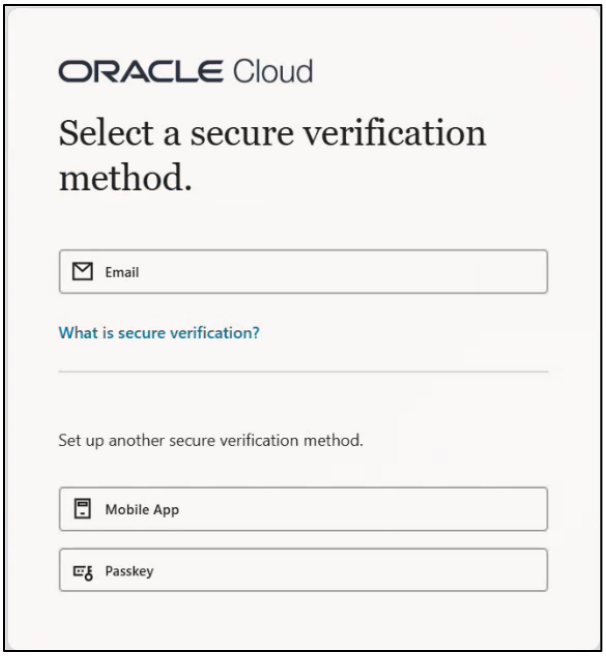
III. Two-factor authentication set up

The "Oracle Cloud – Select a secure verification method" webpage will appear. Choose one of three available methods to set up two-factor authentication: **Email**, **Mobile App** or **Passkey**. King County recommends the **Mobile App** for the most secure option.

- The **Email** option sends a verification code to your established email address to confirm your identity.
- **RECOMMENDED: The Mobile App** option enables you to use your mobile device during the login process to verify your identity.
- The **Passkey** option uses a security key into your device to sign in.

Important Reminder: The MFA options available to you will depend on how you sign in to the Supplier Portal—either through the existing Supplier Portal URL or using the Oracle **kcbrcps** email.

- **Using the existing Supplier Portal URL**: If your Username and Password are entered correctly and the Password is active, you will have access to all three two-factor authentication methods: **Email**, **Mobile App** or **Passkey**:

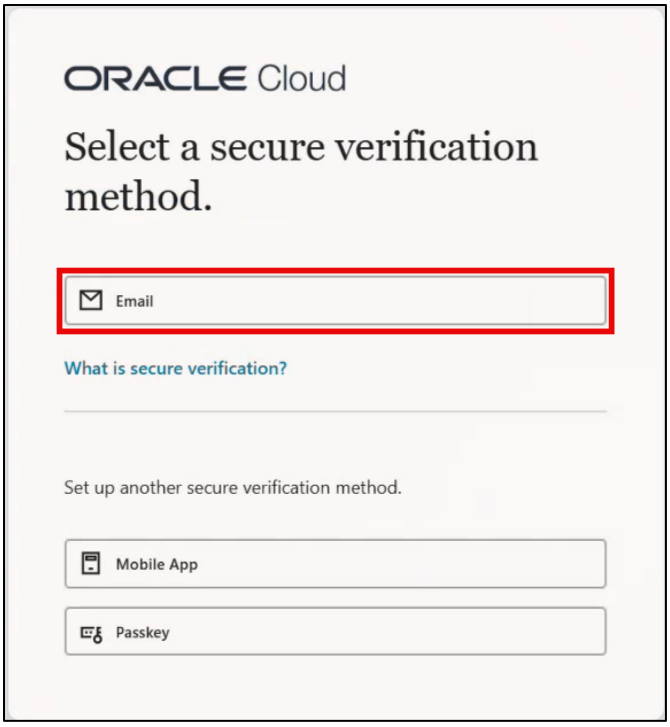


- **Oracle kcbrcps email**: If you sign in using the Oracle **kcbrcps** email, you will have access to only two two-factor authentication methods: **Mobile App** or **Passkey**:

1. Enabling the "Email" Option

i. Select the "Email" option.

On the Oracle Cloud webpage, select "Email" option.

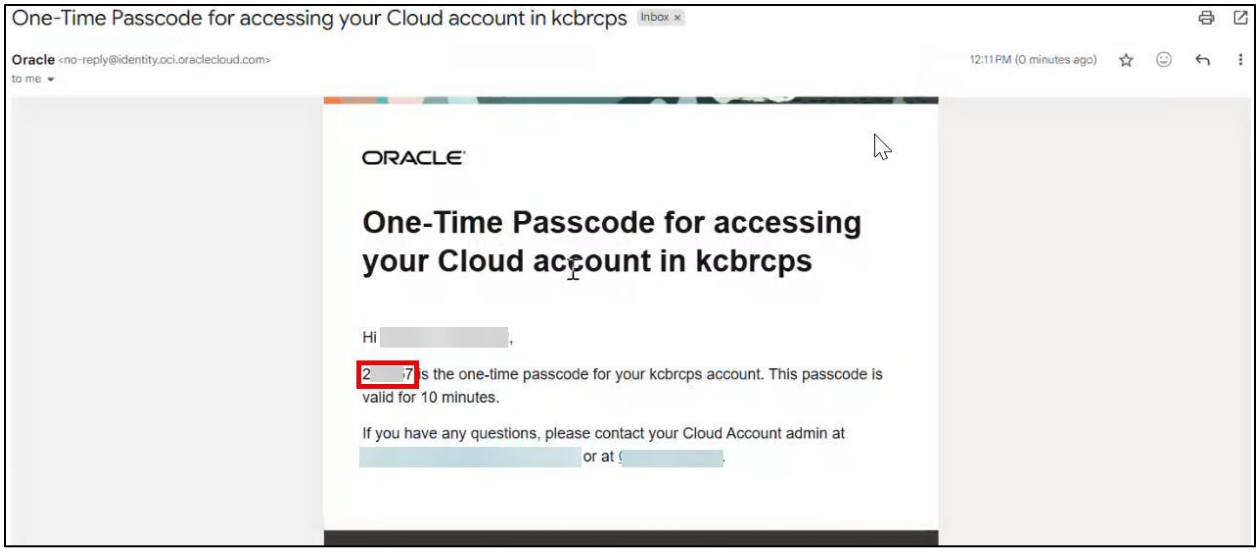


ii. *Oracle Cloud Email Verification*

The Oracle Cloud Email Verification webpage will appear.

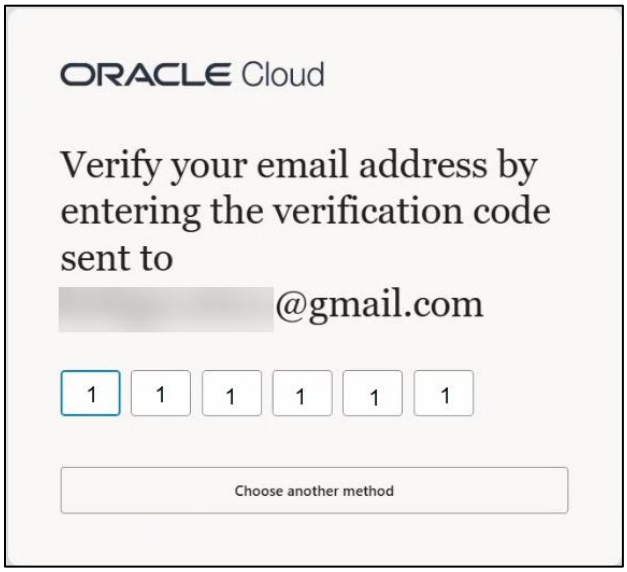
iii. *Oracle One-Time Passcode Email*

Navigate to your email to copy the One-Time Passcode included. The passcode is valid for 10 minutes.



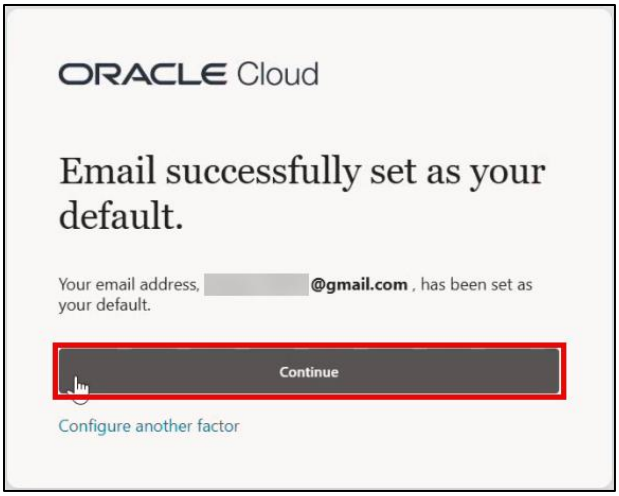
iv. Verify email using one time code

Return to the Oracle cloud webpage to enter the code.



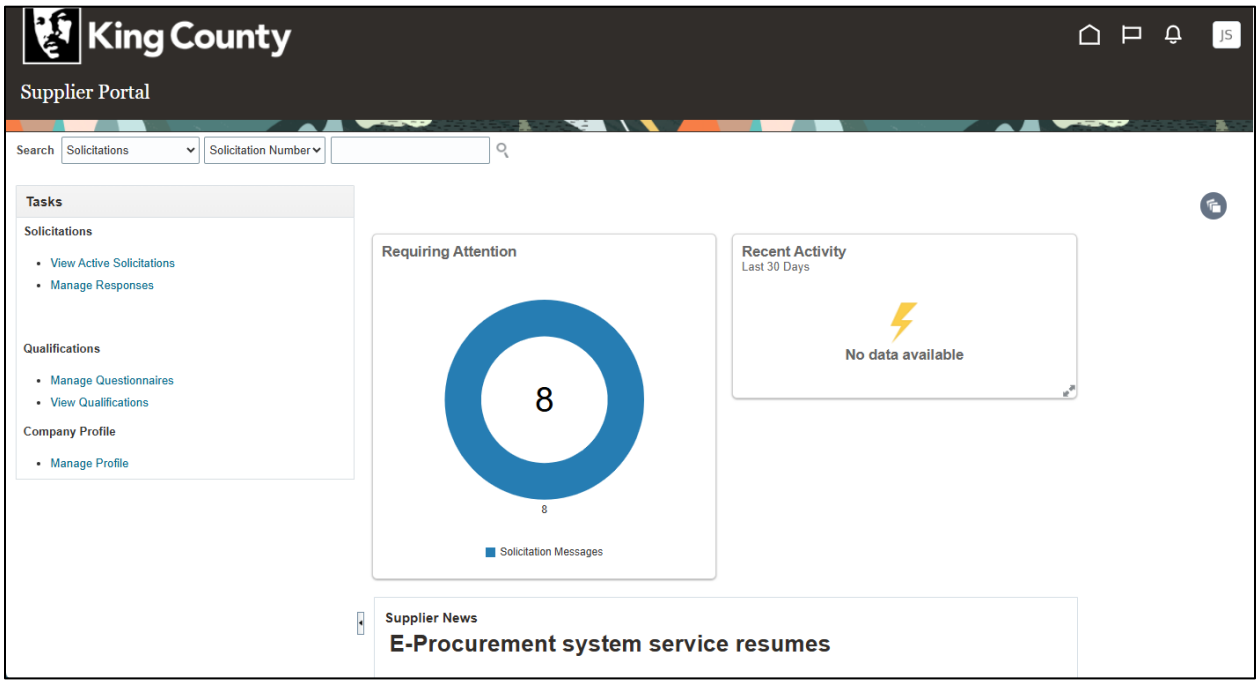
v. "Email" Option Successfully set as default

On the Oracle Cloud webpage, you will receive a confirmation that the "Email" option was successfully set as your default two-factor authentication. Select "Continue" to navigate to the Supplier Portal.



vi. E-Procurement Supplier Portal

You will be redirected to your E-Procurement Supplier Portal account.



2. Enabling the "Mobile App" Option (recommended)

i. Select the "Mobile App" option.

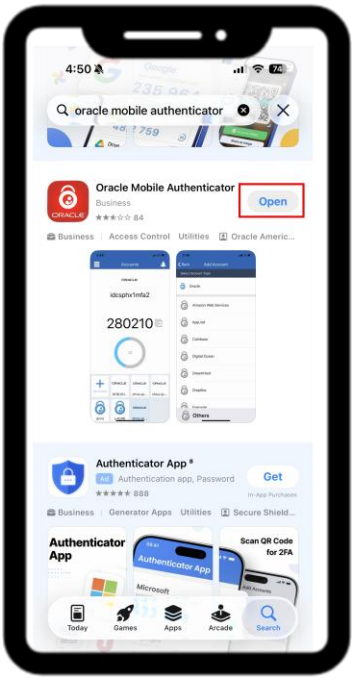
On the Oracle Cloud webpage, select "Mobile App" option.

ii. Configure authenticator app

The Oracle Cloud Configure Authenticator App webpage will appear.

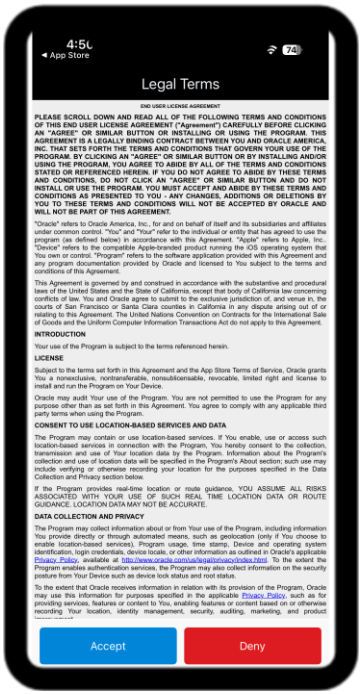
iii. Download the Oracle Mobile Authenticator App

Download and open the Oracle Mobile Authenticator App from your devices' App Store for iPhone or iPad devices or the Google Play Store for Android devices.



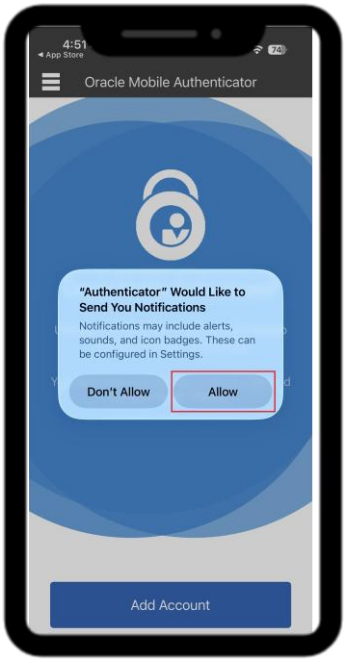
iv. Oracle Mobile Authenticator's Terms and Conditions

Read the Oracle Mobile Authenticator's Terms and Conditions. Select "Accept" to continue the MFA set-up.



v. "Allow" notification

You will be prompted to select the notification settings in the Oracle Mobile Authenticator App. Select "Allow."

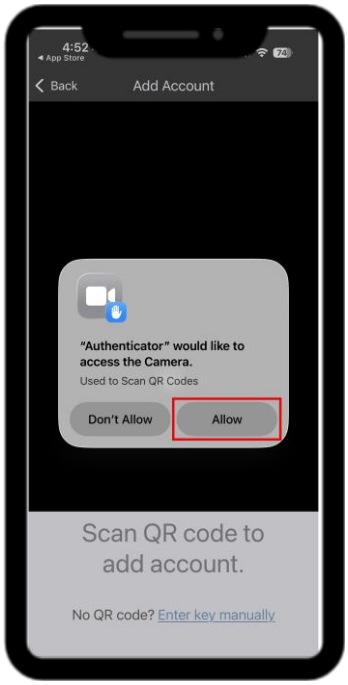


vi. "Add Account"

Select the "Add Account" option to add the King County Supplier Portal user account.

vii. Camera access

You will be prompted to give access to your device's camera to scan the QR code to add account. Select "Allow."

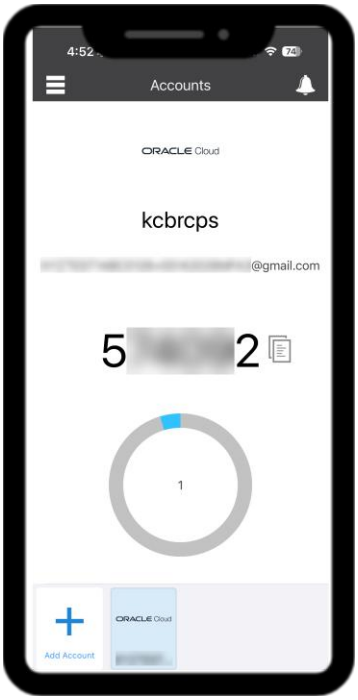


viii. Scan the QR code

Using your device, scan the QR code on the Oracle Cloud webpage.

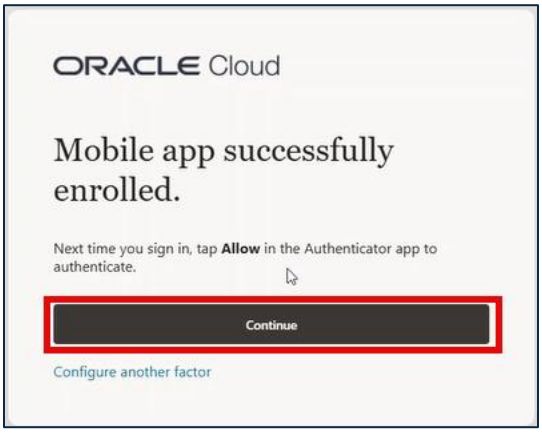
ix. Authenticator app

The Oracle Cloud kcbrcps Company account will be added to your authenticator app.



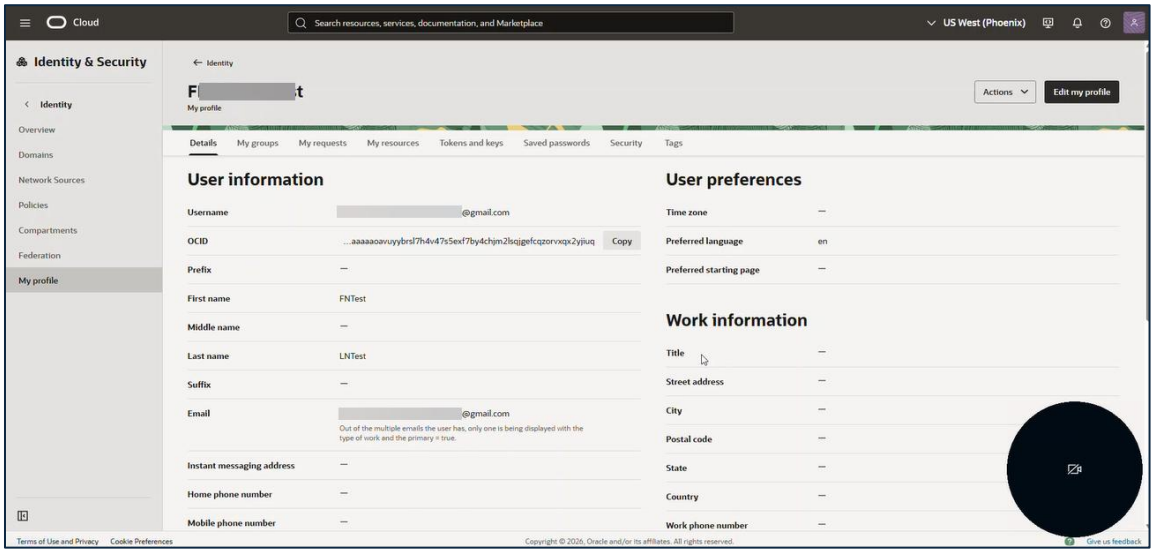
x. Mobile app enrollment confirmation

After enabling MFA using the mobile app, you will receive the "Oracle Cloud Mobile app successfully enrolled" confirmation on your web browser. Select "Continue."



xi. Oracle Cloud Identity & Security webpage

You will be redirected to the Oracle Cloud Identity & Security webpage. **No action is needed on this webpage. Close the webpage.**



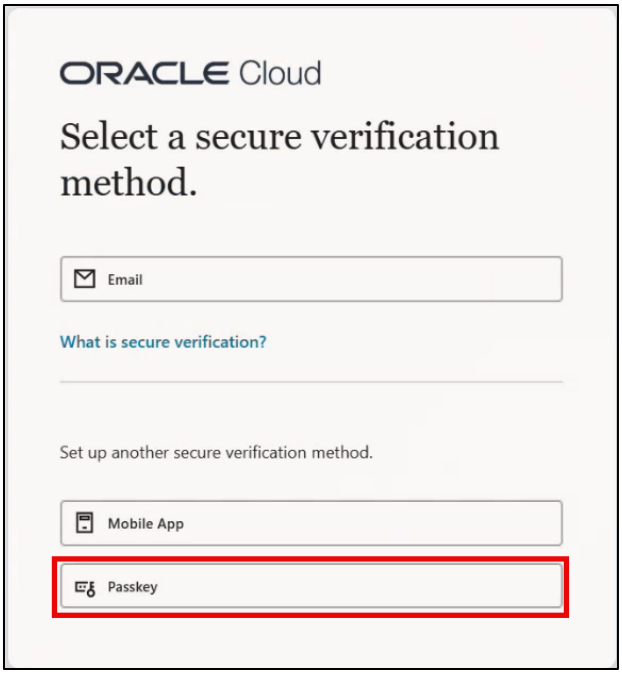
xii. Sign in to E-Procurement Supplier Portal

Sign in to the E-Procurement Supplier Portal. The “Sign In” webpage will display. Enter your “User ID” and “Password” then select “Sign In.” You will then be asked to approve your established MFA.

3. Enabling the “Passkey” Option

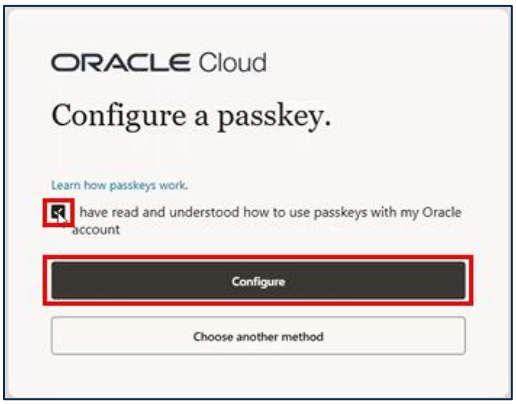
i. “Passkey” Option

On the Oracle Cloud webpage, select the "Passkey" option.



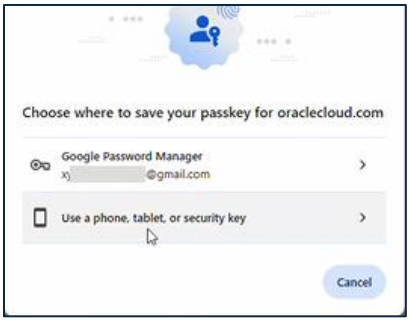
ii. Configure a passkey

The Configure a passkey webpage will appear. Select the checkbox indicating you have read and understand how to use passkeys with your Oracle account. Select "Configure."



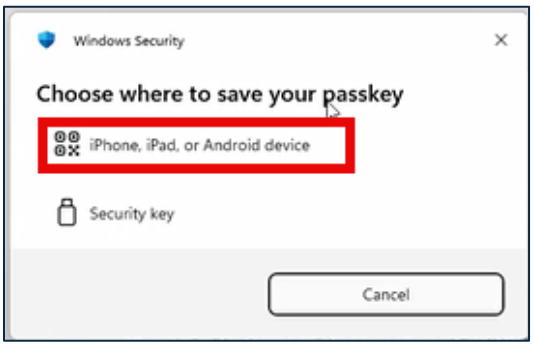
iii. Saving your passkey for Oracle Cloud

Important note: if using the Google web browser, you will be prompted to choose where to save your passkey for oraclecloud.com: Select the "Use a phone, tablet, or security key option."



iv. Windows security pop-up

You will see a Windows security pop-up. Select the "iPhone, iPad or Android device" option **or** the "Security key" option.



v. Select "iPhone, iPad, or Android device"

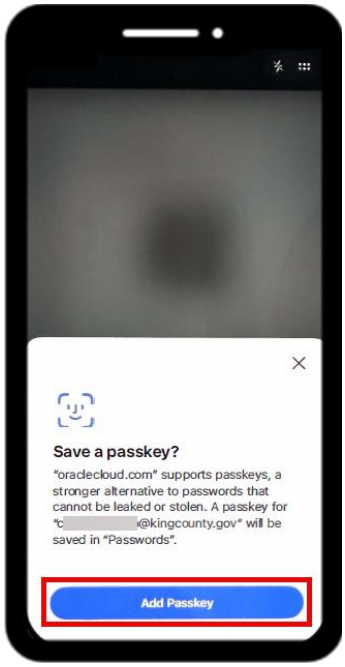
It's recommended you select the "iPhone, iPad or Android device" option. You will be prompted to save your passkey by scanning the QR code with your device camera.

vi. Scan the QR code on your device camera

When you scan the QR Code on your device, select the “Save a passkey” option that appears at the bottom of the image.

vii. Save a passkey using Face ID

Your device will prompt you to Save a passkey using Face ID. Select “Add Passkey” to enable passkey on your device.

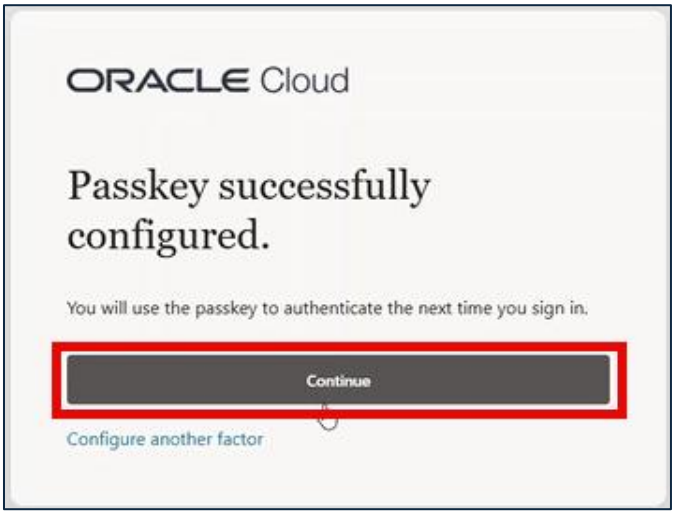


viii. *Device connection confirmation*

A Windows Security pop-up window will appear confirming that your device is connected.

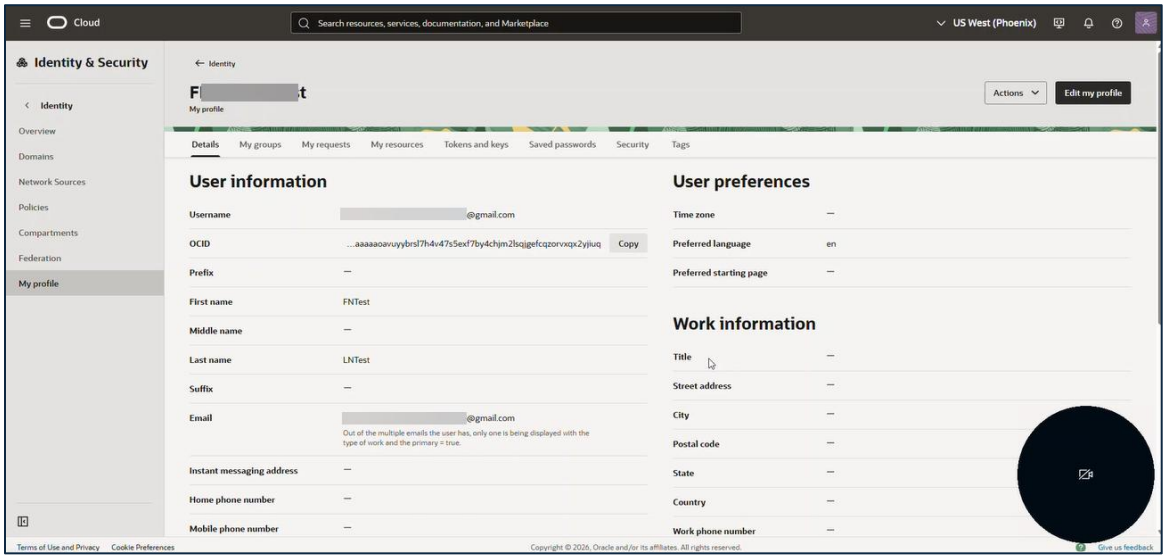
ix. Passkey *successful confirmation*

You will also see the Oracle Cloud message on your web browser, "Passkey successfully configured." Select "Continue."



x. The Oracle Cloud identity & security webpage

You will be redirected to the Oracle Cloud Identity & Security webpage. No action is needed on this webpage. Close the webpage.



xi. Sign in to E-Procurement Supplier Portal

Sign in to the E-Procurement Supplier Portal. The “Sign In” webpage will display. Enter your “User ID” and “Password” then select “Sign In.” You will then be asked to approve your established MFA.

End of Process