



# 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)..... 1

I. Sign in (password reset process) .....2

    1. Sign in to the E-Procurement supplier portal. ....2

    2. “Invalid Username or password” .....2

    3. Reset password .....3

    4. “Forgot password” .....3

    5. Sign in Oracle Applications Cloud webpage .....4

    6. Oracle email 1 - Password Reset Request .....5

    7. Reset password window .....5

    8. Oracle email 2 - password reset request .....5

II. Two-factor authentication set up ..... 7

    1. Enabling the “Mobile App” Option (recommended) .....7

    2. Enabling the Passkey Option ..... 14

## 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](mailto:Procurement.Web@kingcounty.gov) if you do not have a smart device to enable MFA.

## I. Sign in (password reset process)

### 1. Sign in to the E-Procurement supplier portal.



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

Do not use the “Sign in with KC Identity...” option.

A screenshot of the Oracle Cloud sign-in page. At the top left is the 'ORACLE Cloud' logo. To its right is a language dropdown menu set to 'English'. Below the logo is the heading 'Sign in'. There are two input fields: 'Username' and 'Password'. Below the password field is a link for 'Forgot Password?'. A dark grey 'Next' button is positioned below the fields. A horizontal line with 'Or' in the center separates the main sign-in area from a 'Sign in with KC Identity...' button. Below this button is a link for 'Need help signing in?'. At the bottom, there is a link for '> Cloud account details'.

### 2. “Invalid Username or password”

As an existing supplier in the E-Procurement Supplier Portal, you will receive an “Invalid username or password” error message when attempting to sign in using your existing username and password. To access your account, you will need to reset your password. After resetting it, you will be prompted to enable MFA to your E-Procurement Supplier Portal account.

ORACLE Cloud English

Invalid username or password.

### Sign in

Username: [redacted]@gmail.com

Password: [redacted]

Forgot Password?

Next

Or

Sign in with KC\_Identity...

Need help signing in?

> Cloud account details

### 3. Reset password

To reset your password, select “Forgot Password.”

ORACLE Cloud English

### Sign in

Username

Password

Forgot Password?

Next

Or

Sign in with KC\_Identity...

Need help signing in?

> Cloud account details

### 4. “Forgot password”

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

Sign In  
Oracle Applications Cloud

Forgot Password

\* User Name or Email  
User Name or Email

\* Options

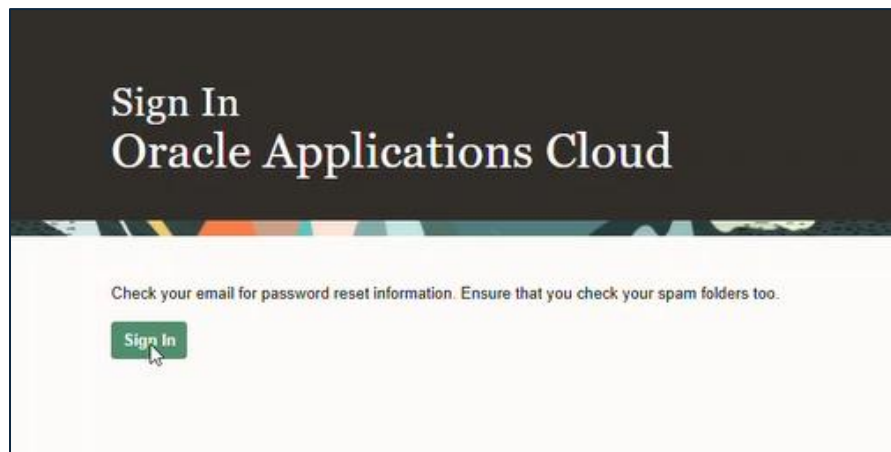
Forgot user name

Forgot password

Submit Cancel

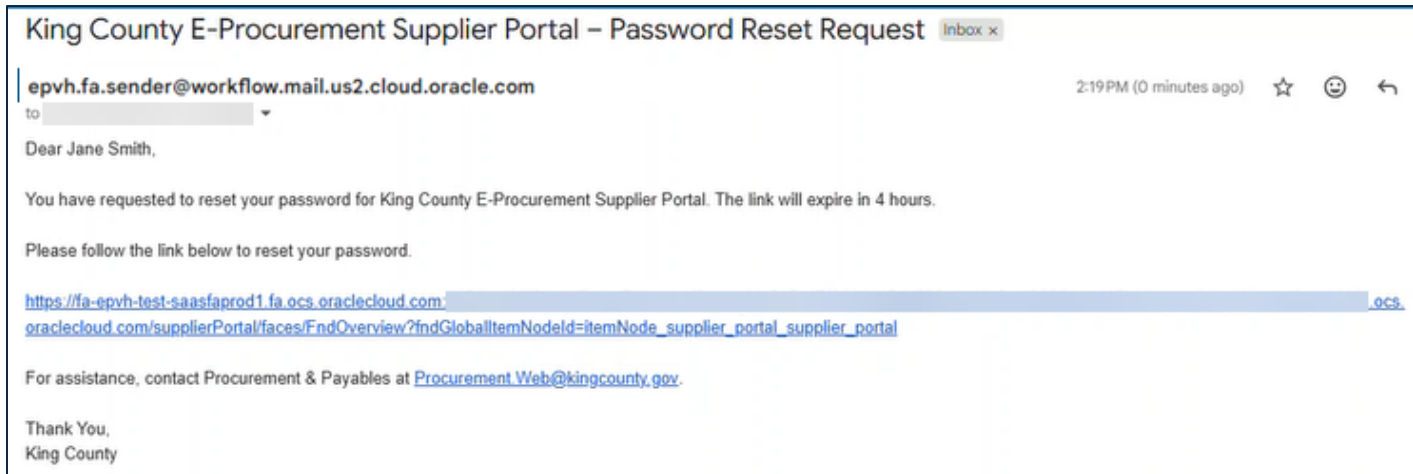
## 5. Sign in Oracle Applications Cloud webpage

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



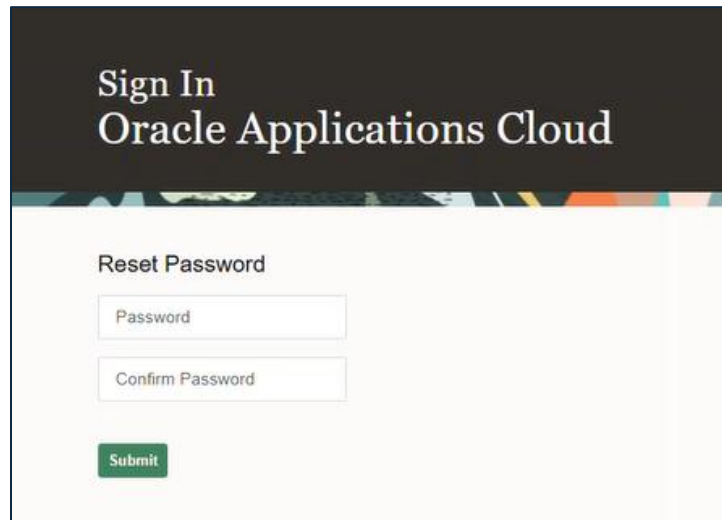
## 6. Oracle email 1 - Password Reset Request

**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.



## 7. Reset password window

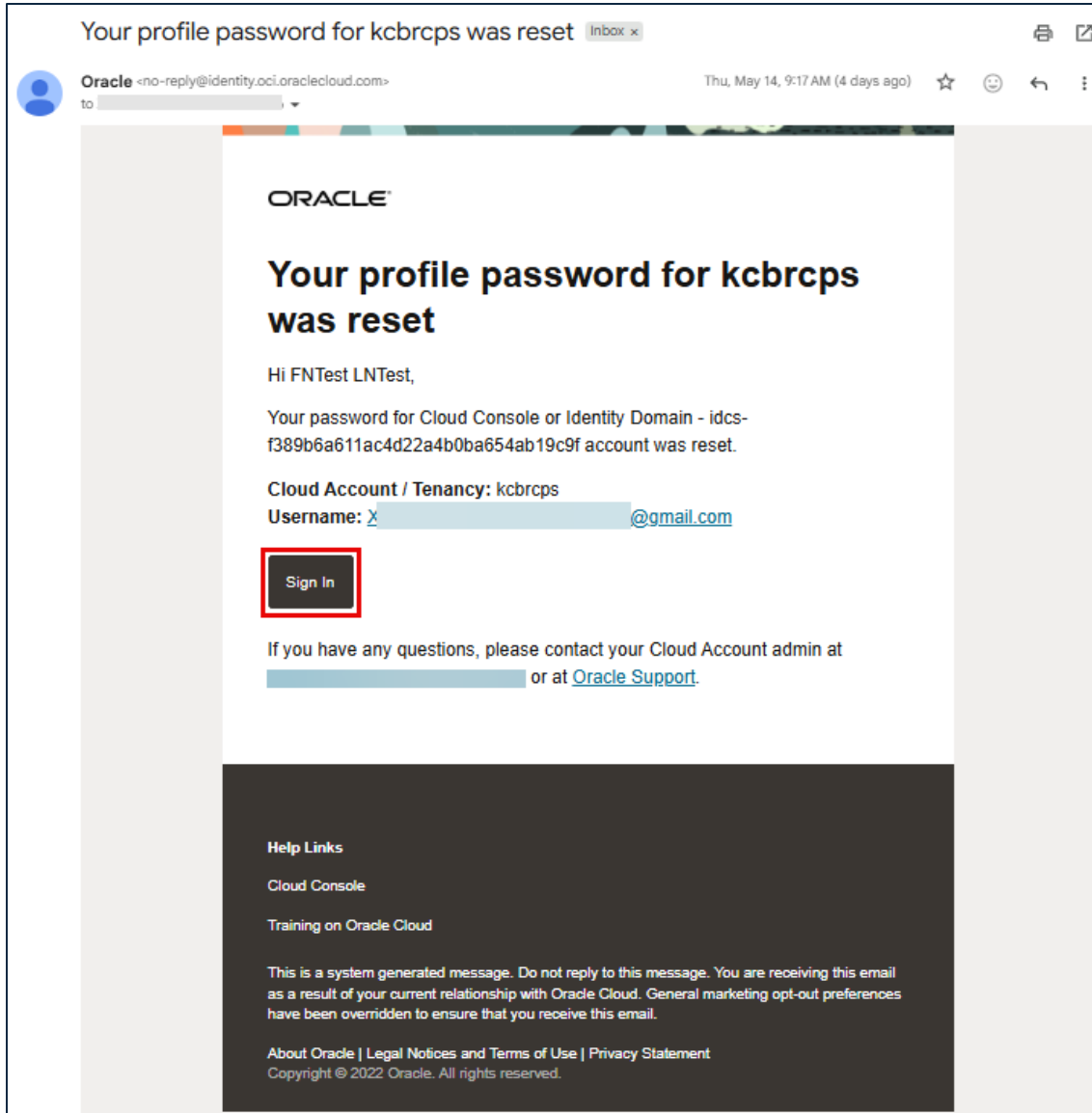
A reset password window will appear. Enter a new password, confirm it, then select “Submit.” Navigate back to your email inbox.

A screenshot of a web-based "Reset Password" form. The header reads "Sign In Oracle Applications Cloud". The form has a title "Reset Password" and two input fields: "Password" and "Confirm Password". Below the fields is a green "Submit" button.

## 8. Oracle email 2 - password reset request

**Email 2 of 2 (Action Required):** A second email will come from Oracle [reply@identity.oci.oraclecloud.com](mailto:reply@identity.oci.oraclecloud.com) confirming your password for kbcrcps 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](mailto:Procurement.Web@kingcounty.gov) for assistance.



## II. Two-factor authentication set up

The Oracle Cloud window will appear. Choose one of two available methods to set up two-factor authentication: Mobile App **or** Passkey.

- **RECOMMENDED: The Mobile App** option enables you to use your mobile device during the login process to verify your identity.
  - Your mobile app generates a passcode. Enter this passcode on the login screen to verify your identity.
  - A push notification is sent to your device. To approve the login request, tap Allow.
- The **Passkey** option uses a security key into your device to sign in.



### 1. Enabling the “Mobile App” Option (recommended)

- i. *Select the "Mobile App" option.*

On the Oracle Cloud Window, select “Mobile App” option.



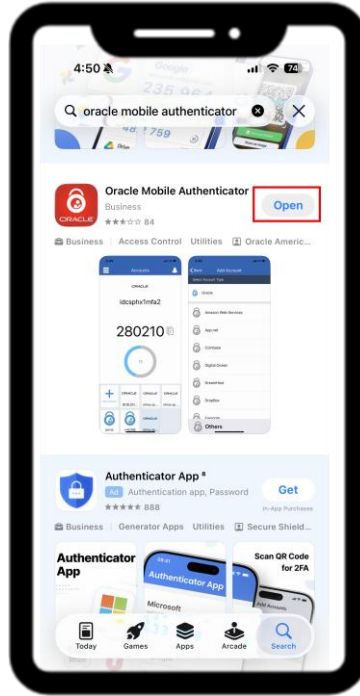
ii. *Configure authenticator app*

The Oracle Cloud Configure Authenticator App webpage will appear.



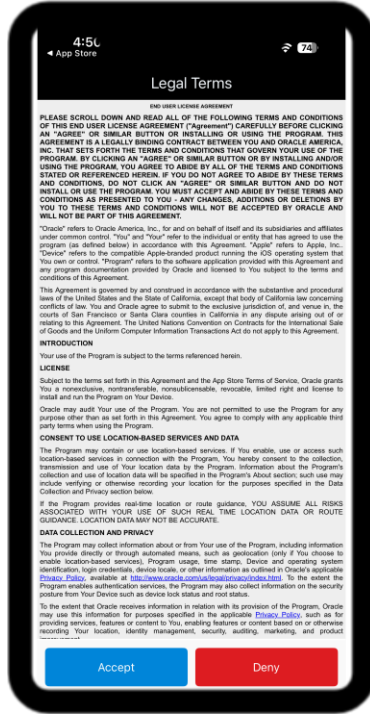
iii. *Download the Oracle Mobile Authenticator App*

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.



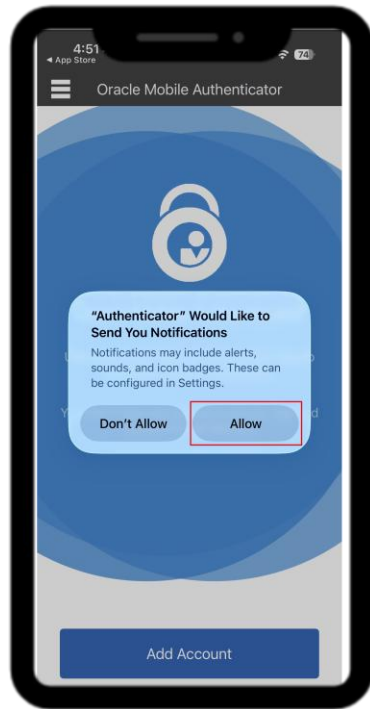
iv. *Oracle Mobile Authenticator's Terms and Conditions*

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.”



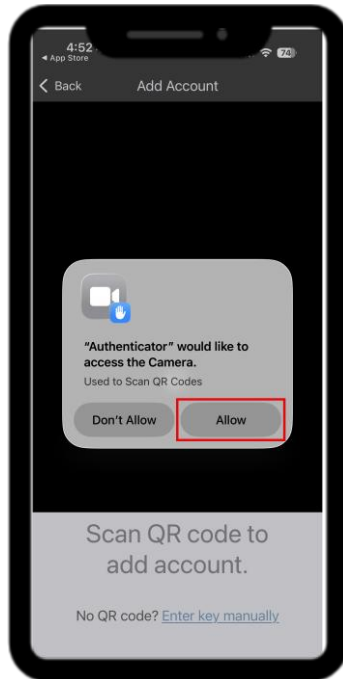
vi. *“Add Account”*

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.”



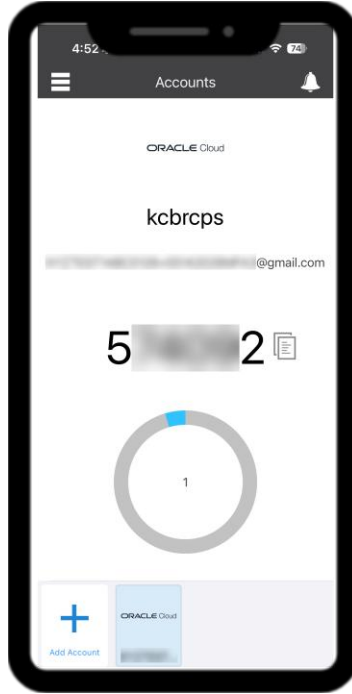
*viii. Scan the QR code*

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



ix. *Authenticator app*

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



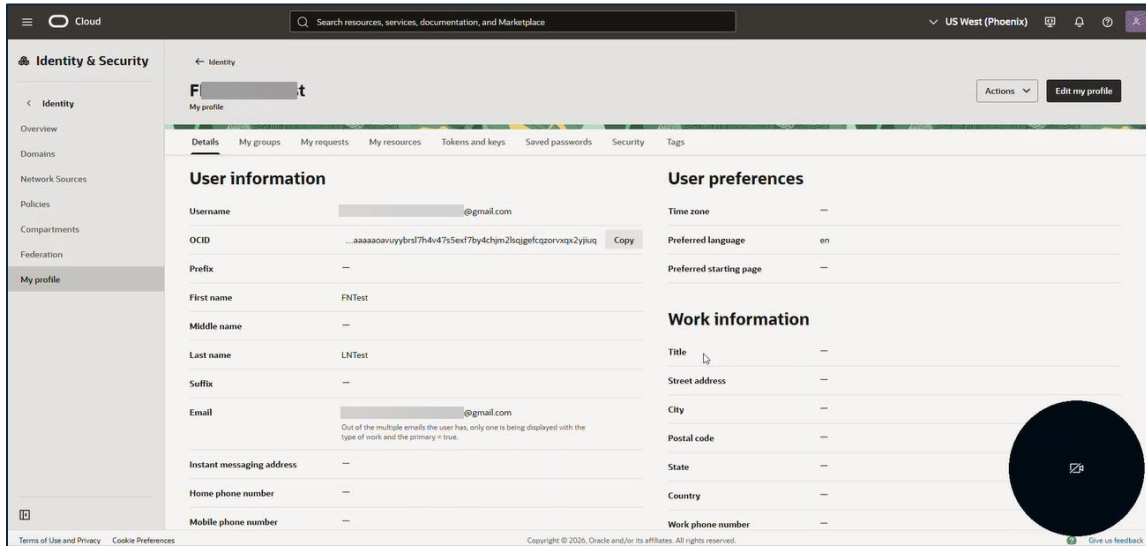
x. *Mobile app enrollment confirmation*

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 page*

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



xii. *E-Procurement supplier portal*

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

## 2. Enabling the Passkey Option

i. *“Passkey” Option*

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



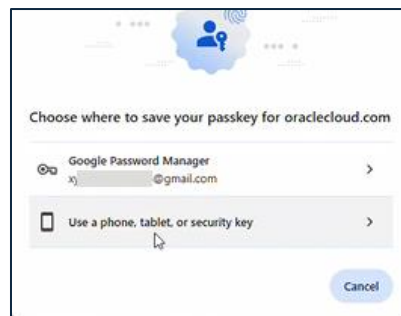
ii. *Configure a passkey*

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



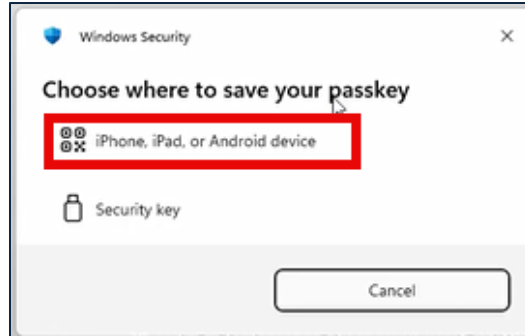
iii. *Saving your passkey for Oracle Cloud*

**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. *Window 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.



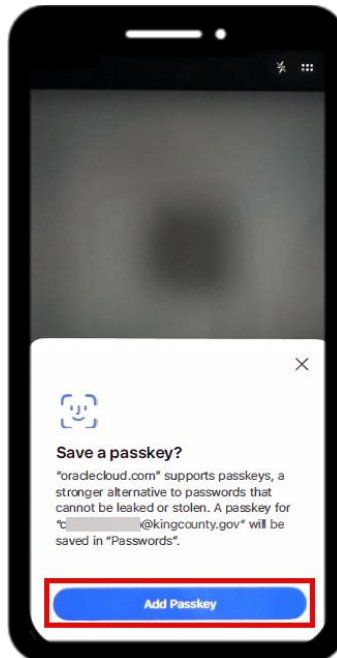
vi. *Scan the QR code on your device camera*

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.



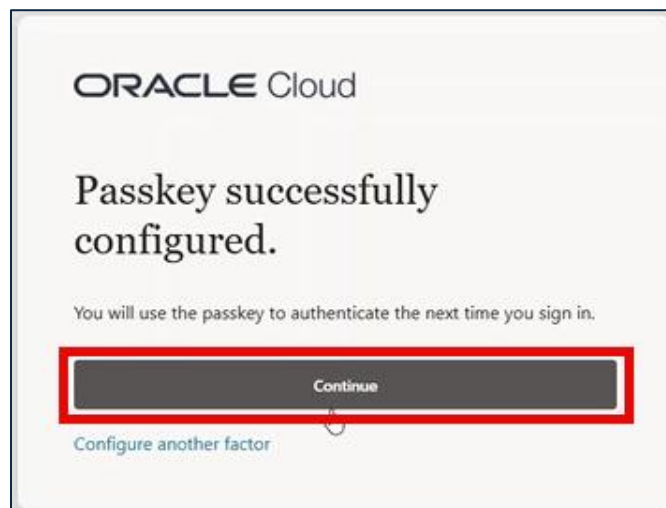
*viii. Device connection confirmation*

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



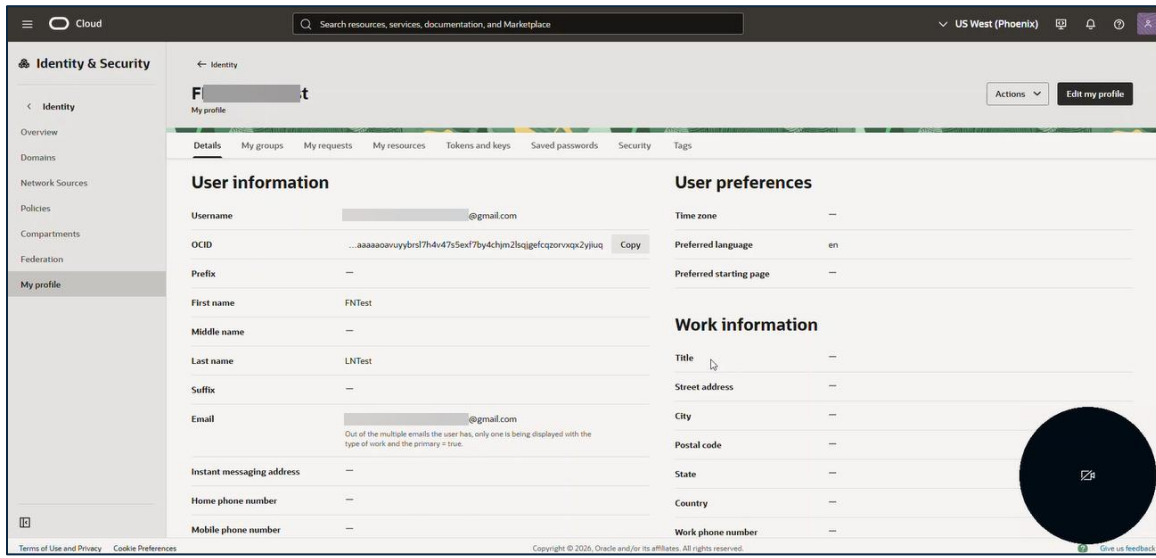
ix. *Passkey successful confirmation*

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 page. Close the web browser.



xi. *Sign in to [E-Procurement Supplier Portal](#)*

Sign in to the [E-Procurement Supplier Portal](#). The “Sign In” page 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