

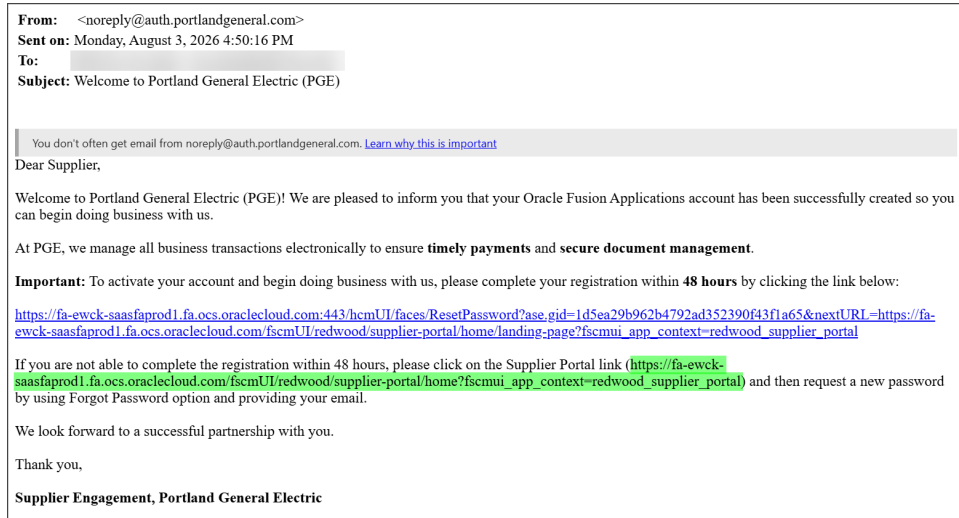
Oracle Supplier Portal: User Access Guide

1. Initial Account Setup (New Users)

Upon approval of your company's supplier profile, the supplier contact will receive a Welcome Email.

Step 1: Open the Welcome Email

Find the email from **portlandgeneral.com** domain in your registered company inbox. In the message, click the **Reset Password** link to create your password and access the Oracle Supplier Portal.



Step 2: Define System Password

In the web window, complete the text credentials fields as instructed:

- Type your chosen combination into the **Password** field.
- Duplicate the exact characters into the **Confirm Password** field, then click **Submit**.

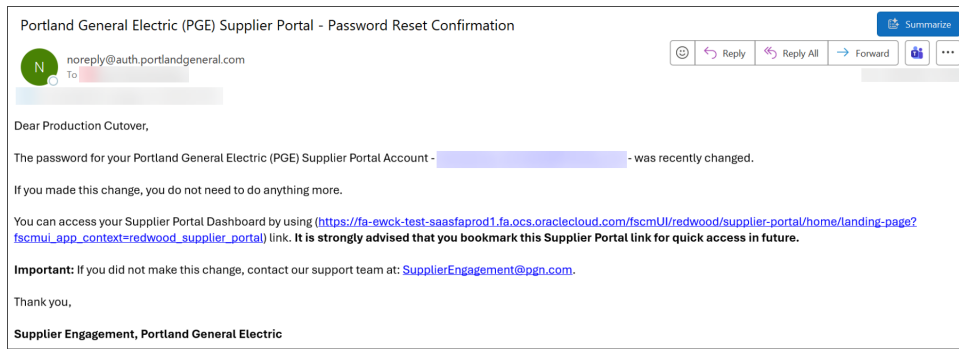
CRITICAL PASSWORD PARAMETERS

The password sequence must meet the following structural rules:

- a. Length Criteria: Must consist of at least 8 alphanumeric characters.
- b. Structural Token: Must feature at least one unique numeric character (0-9).

The screenshot shows the 'Sign In Oracle Applications Cloud' header. Below it, there is a 'Reset Password' section with two input fields for password and confirm password, both masked with asterisks. A 'Submit' button is located at the bottom of the form.

Upon successfully resetting the password, the supplier contact receives a confirmation email containing the **User Account Name**, as shown below.



2. Multi-Factor Authentication (MFA) Setup

Identity integrity validation mandates a dual-factor identity enrollment process. On the **Sign In** page, enter the Supplier Portal Account ID provided in the Password Reset Confirmation email in the **Account** field. Enter the newly created password in the **Password** field, then click **Next**.

ORACLE Cloud English

Sign in

Username

Password

[Forgot Password?](#)

Next

[Need help signing in?](#)

> Cloud account details

Method A: Registered Email Tokenization

1. On the secure verification screen prompt, click the **Email** panel component.
2. The interface will refresh, verifying that your designated account email has been registered as the identity validator.
3. Choose **Continue** or configure alternative options via *Configure another factor*.

ORACLE Cloud

Email successfully set as your default.

Your email address, [Redacted] has been set as your default.

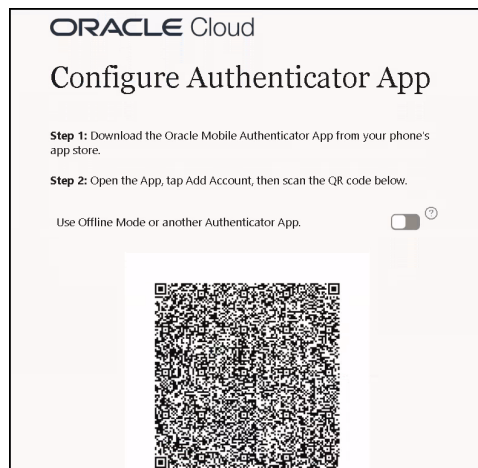
Continue

[Configure another factor](#)

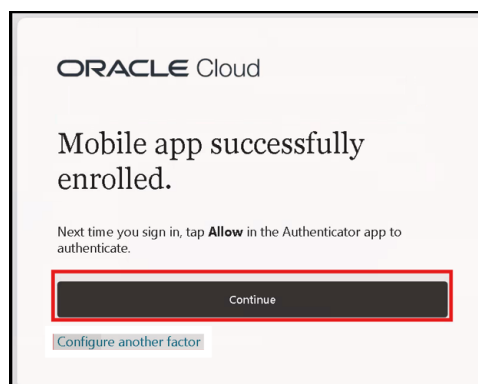
Method B: Mobile App Tokenization



1. Download the commercial **Oracle Mobile Authenticator App** straight from your local device repository (Google Play Store or iOS App Store).
2. Open the App, click **Add Account**, and scan the active **QR Code** displayed on your browser screen.



3. The verification notification window confirming *Mobile app successfully enrolled*. Click on **Continue**.



3. Standard Login Procedure

Execute the following operational guidelines for daily routine access once your security credentials are fixed.

Step 1: Core Authentication

Enter your authorized **Username** and **Password**. Click on **Next**



The Oracle Cloud sign-in interface. At the top, it says 'ORACLE Cloud' with a language dropdown set to 'English'. Below is the 'Sign in' heading. There are two input fields: 'Username' and 'Password'. A link for 'Forgot Password?' is below the password field. A large black button labeled 'Next' is highlighted with a red rectangle. Below the button is a link 'Need help signing in?'. At the bottom, there is a link '> Cloud account details'.

Step 2: Second-Factor Identity Verification

Complete identity processing according to your registered operational selection profile:

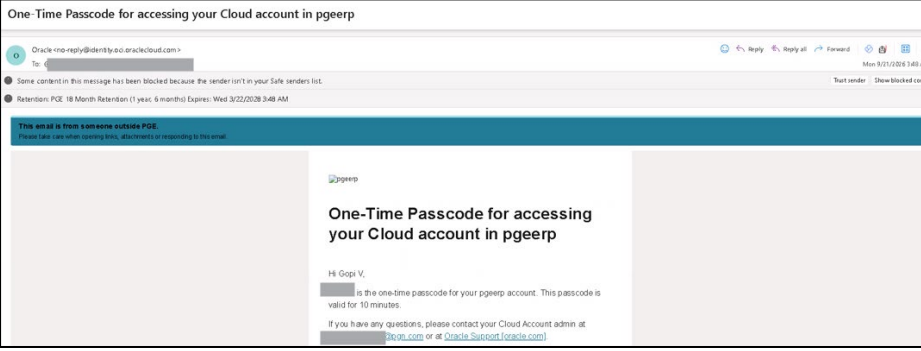
• **Push Notification:** Acknowledge processing validation updates by tapping **Allow** on the security confirmation alert sent directly to your phone.



A push notification screen from Oracle Cloud. It says 'ORACLE Cloud' at the top. The main text reads 'Tap **Allow** on the notification sent to your mobile device to continue.' The word 'Allow' is highlighted with a red rectangle. Below the text is a large circular progress indicator. At the bottom, there is a checkbox labeled 'Trust this device for 15 day(s)'. A button labeled 'Try another way' is highlighted with a red rectangle.

OR

• **Email Passcode:** Access your mail inbox, copy the one-time system token string, input the characters into the verification dashboard boxes



An email interface showing a message from Oracle. The subject is 'One-Time Passcode for accessing your Cloud account in pgeerp'. The email body contains the same subject and a message to 'Hi Gopi V,' stating that a one-time passcode has been sent to the user's mobile device and is valid for 10 minutes. It also provides contact information for support.



A verification screen for the email passcode. It says 'ORACLE Cloud' at the top. The main text reads 'Complete verification by entering the passcode sent to gopXXXXX@pgn.com to continue.' Below the text are six empty boxes for entering the passcode. There are two checkboxes: 'Make this my default method' and 'Trust this device for 15 day(s)'. A button labeled 'Try another way' is at the bottom.

Once you enter the passcode you will be navigated to Supplier Portal landing page.

