

User Guide: Activate Your Account

Table of Contents

1 Overview	2
2 Set up Oracle Account and Password	2
2.1 Activate account	2
2.2 Create Password.....	3
2.3 Confirmation.....	3
2.4 Access Oracle.....	4
2.5 Enter Username & Password	4
2.6 Configure Multi-Factor Authentication	5
2.7 Select MFA Option.....	6
2.7.1 Configure Email for MFA.....	7
2.7.2 Configure Mobile App for MFA.....	9
2.8 Access Oracle.....	10
2.9 Next time.....	10

Definitions/Terminology

Oracle – The name of the system this guide is to support you using.

MFA - Multi-Factor Authentication, a common method for protecting accounts when username and password is insufficient.

IDCS - Identity Cloud Service - the old name for IAM

IAM - Identity and Access Management - The IdP for SSO

IdP - Identity Provider - the system that handles authentication.

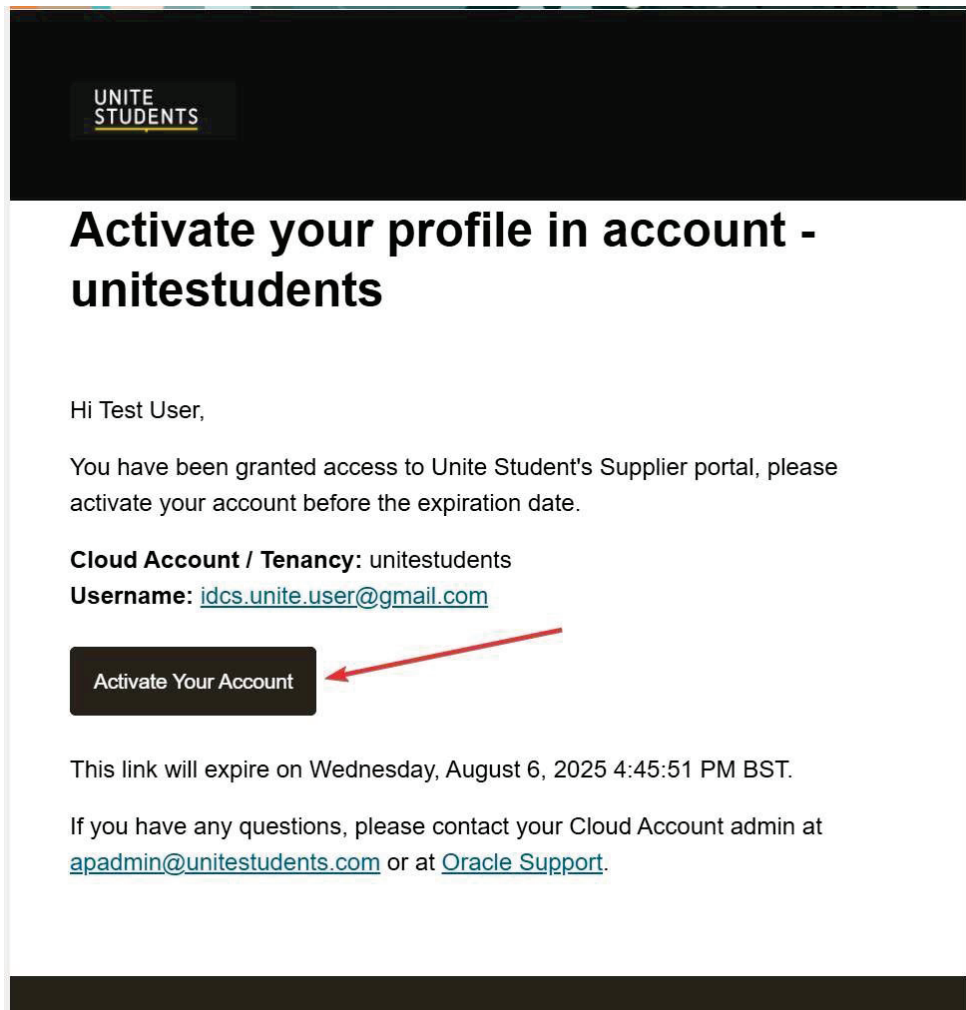
1 Overview

As a Unite Students Supplier, you will receive an Activation email to access our system. This user guide will show you what email to expect and how to access your account.

2 Set up Oracle Account and Password

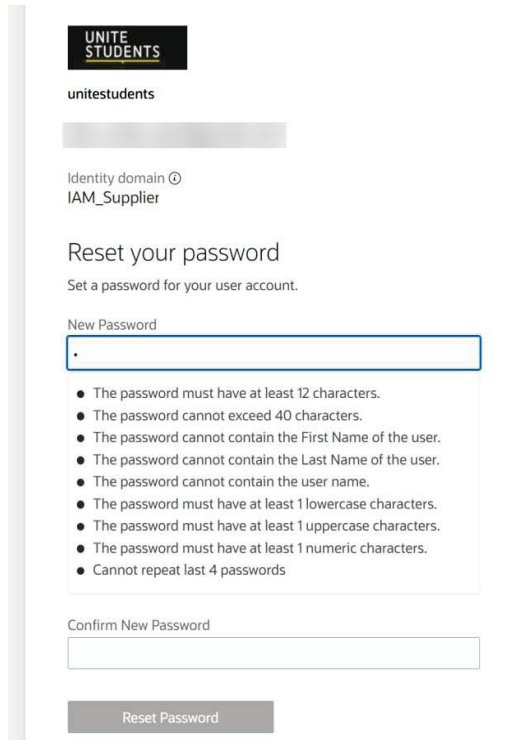
2.1 Activate account

When activated, you'll receive an email like the one below. Please follow the link from this activation email:



2.2 Create Password

On the next page, create a new password following the instructions on screen:



The screenshot shows the UNITE STUDENTS login interface. At the top is the UNITE STUDENTS logo. Below it, the text 'unitestudents' is displayed. A grey bar represents the username field. Below that, the 'Identity domain' is set to 'IAM_Supplier'. The main heading is 'Reset your password', followed by the instruction 'Set a password for your user account.' The 'New Password' field is highlighted with a blue border and contains a single asterisk. Below this field is a list of password requirements: at least 12 characters, not exceeding 40 characters, not containing the first or last name or user name, at least 1 lowercase and uppercase character, at least 1 numeric character, and not repeating the last 4 passwords. A 'Confirm New Password' field is located below the requirements. At the bottom is a 'Reset Password' button.

UNITE
STUDENTS

unitestudents

Identity domain ⓘ
IAM_Supplier

Reset your password

Set a password for your user account.

New Password

*

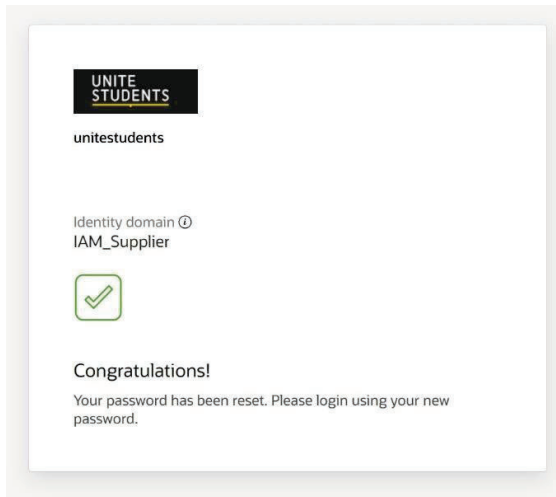
- The password must have at least 12 characters.
- The password cannot exceed 40 characters.
- The password cannot contain the First Name of the user.
- The password cannot contain the Last Name of the user.
- The password cannot contain the user name.
- The password must have at least 1 lowercase characters.
- The password must have at least 1 uppercase characters.
- The password must have at least 1 numeric characters.
- Cannot repeat last 4 passwords

Confirm New Password

Reset Password

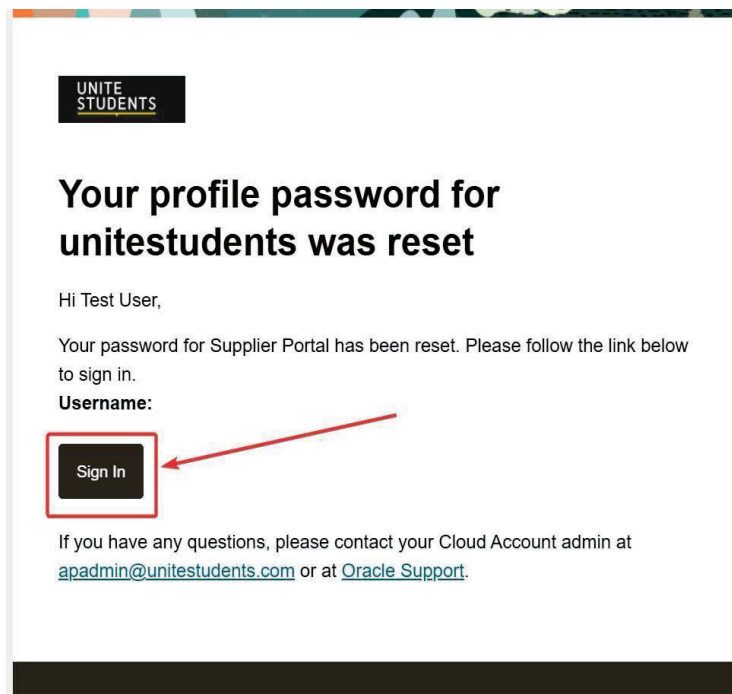
2.3 Confirmation

Once your password is created, this window will pop up:



2.4 Access Oracle

You'll receive a second email confirming your password has been reset. This email includes the link to sign in to the Supplier Portal:



2.5 Enter Username & Password

Enter your username and the password you chose in step "2.2 - Create Password"

The screenshot shows the Oracle Cloud Account Sign In page for UNITE STUDENTS. At the top left is the UNITE STUDENTS logo. Below it, the text "unitestudents" is displayed. The main heading is "Oracle Cloud Account Sign In". Underneath, the "Identity domain" is set to "IAM_Supplier". There are two input fields: "User Name" and "Password". The "User Name" field is empty, and the "Password" field contains masked characters (dots). To the right of the password field are icons for password visibility and strength. Below the password field is a link for "Forgot Password?". At the bottom of the form is a black "Sign In" button. Below the button is a link for "Need help signing in?".

2.6 Configure Multi-Factor Authentication

Multi-Factor Authentication (MFA) will protect your account by ensuring that only a user with access to both your password and another factor will be able to access your account. The additional factor may be one or more of the following two options:

- 1) *Approval within Authenticator App*
- 2) *Access code sent by email message*

On the below screen, please click "Enable Secure Verification"



unitestudents

Identity domain ⓘ
IAM_Supplier

Enable Secure Verification

Secure verification methods prove who you are. Two types of verification methods are passwordless and multi-factor authentication (MFA). Passwordless verification allows you to verify your identity without requiring you to remember a password. MFA is an extra security step to the authentication process. Your administrator might have set up one or both verification methods and require that you enroll in them before accessing your account.

Password

+

Proof

=

Secure Access

Click below to enable secure verification methods for your account.

Enable Secure Verification

2.7 Select MFA Option

For the most secure option, we recommend the Mobile App.



unitestudents

Identity domain ⓘ

Select Your Default Secure Verification Method

You have already set up one or more recovery methods. We will use these same methods for Secure Verification.

☐ Email

Or, setup a new Secure Verification method to be added as a default method.

☐ Mobile App

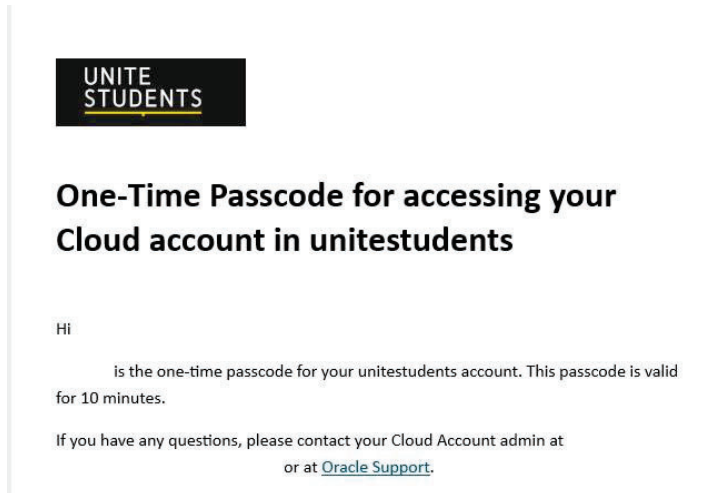
[What is Secure Verification?](#)

If you select "Email", please continue to section 2.7.1

If you select "Mobile App", please skip to section 2.7.2

2.7.1 Configure Email for MFA

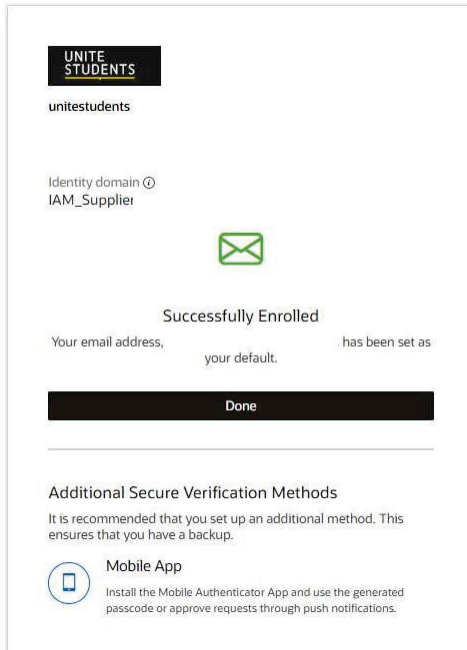
When you select this option, you'll automatically receive an email that looks like this:



Enter the code into the box shown below to verify your email:

The screenshot shows the unitestudents verification page. It includes the UNITE STUDENTS logo, the text "unitestudents", and "Identity domain IAM_Supplier". Under "Select Your Default Secure Verification Method", it says "You have already set up one or more recovery methods. We will use these same methods for Secure Verification." There is a blue button labeled "Email" with an envelope icon. Below this, it says "An email that contains a verification code has been sent to [redacted]". There is a text input field labeled "Code" with a red arrow pointing to it from the text above. Below the input field is a "Resend code" link. At the bottom is a black button labeled "Verify Email Address".

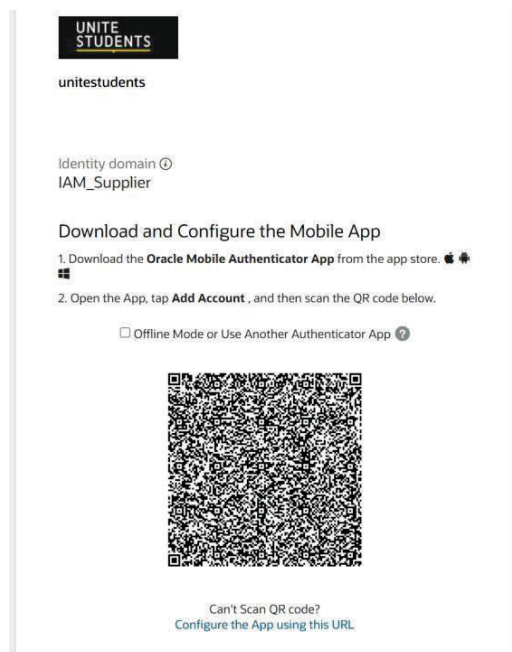
You'll receive the following message as confirmation:



Click Done, or you may choose to configure additional factors.
Continue to Section 2.8.

2.7.2 Configure Mobile App for MFA

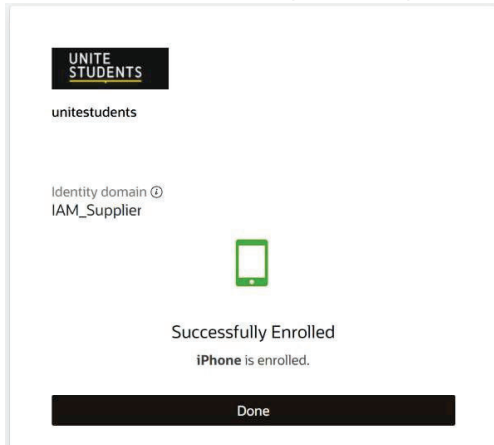
You'll be shown this page:



Please download the Oracle Mobile Authenticator App from the app store and scan the QR code on the screen. The app looks like this:



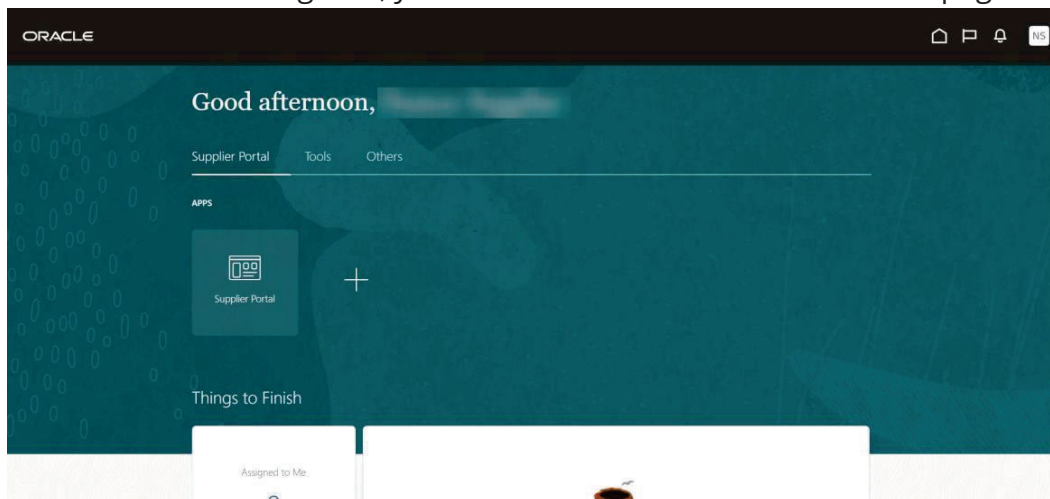
You'll receive the following message as confirmation.



Click Done, or you may choose to configure additional factors.

2.8 Access Oracle

Once MFA has been configured, you'll be redirected to the Oracle home page:



2.9 Next time

Now that your password and MFA is configured, next time you want to sign into the Supplier Portal, you simply need to access it via this link (you may need to press ctrl whilst clicking the link):

supplierportal.unitestudents.com

Please note, it is a good idea to bookmark this link, so that you can easily access the system in the future.

