

Aspire Portal

Multifactor Authentication User Guide

October 2026

WAPHA.ORG.AU

Contents

Aspire Portal & MFA	P3
New MFA process	P4
MFA methods available	P5
New Login process	P6
MFA Configuration – Step-by-step overview	P7-9
MFA Configuration – Visual overview	P10-13
Support	P14



Aspire Portal & MFA

What is MFA?

Aspire is WAPHA's online supplier platform used for activities such as tendering, supplier management, contracts, invoicing and payments.

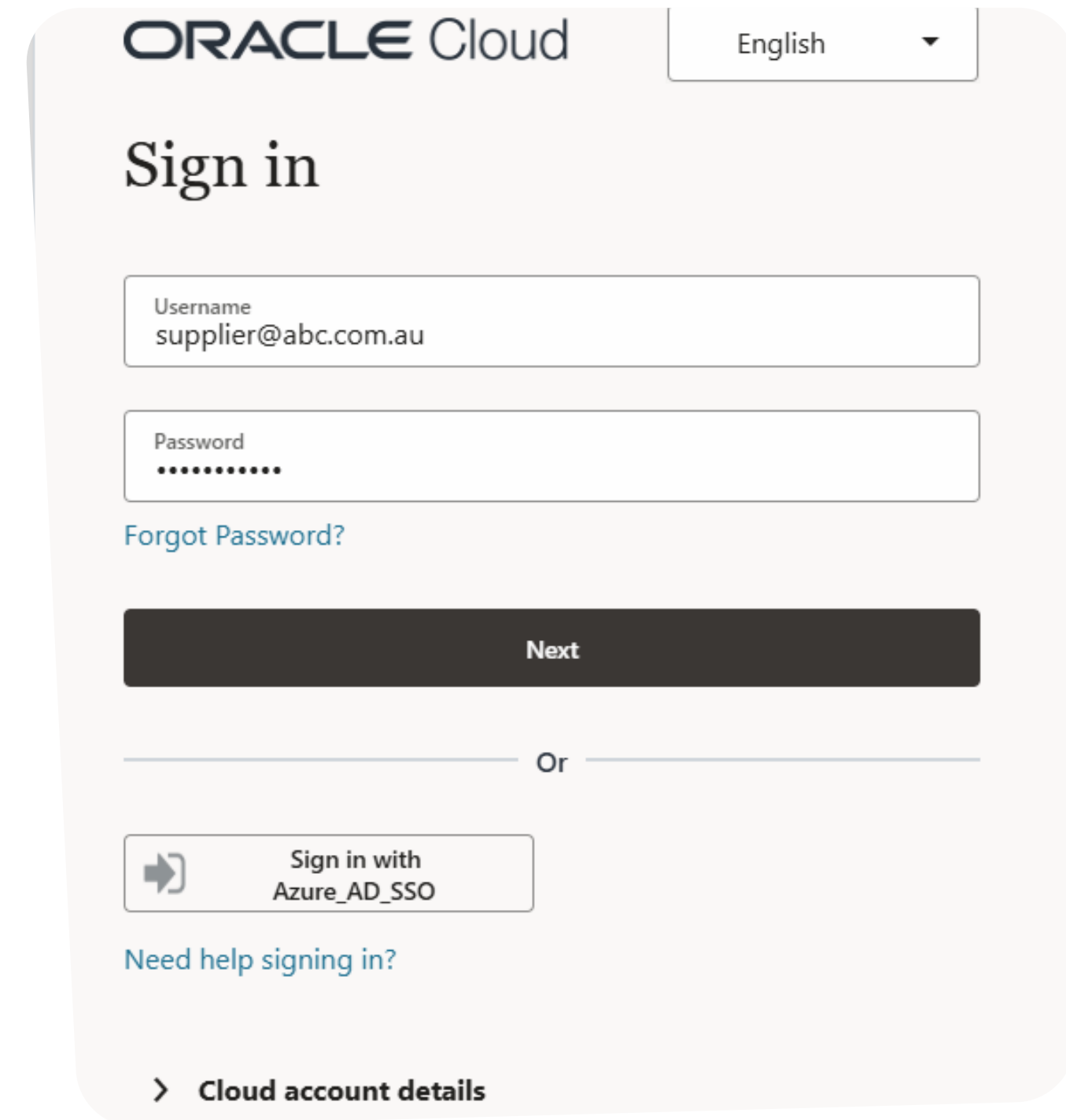
Multi-Factor Authentication (MFA) is an additional security step used when signing in to the Aspire Portal.

MFA helps protect your account by requiring two forms of verification:

1. **Something you know** – your username and password
2. **Something you have** – a verification code sent to you

This additional step helps prevent unauthorised access to your account, even if your password becomes known to someone else.

MFA is widely used by banks, government agencies, and online services to improve security and help protect personal and business information.



The screenshot shows the Oracle Cloud Sign in interface. At the top left is the 'ORACLE Cloud' logo, and at the top right is a language dropdown menu set to 'English'. The main heading is 'Sign in'. Below this are two input fields: 'Username' with the value 'supplier@abc.com.au' and 'Password' with masked characters. A blue link 'Forgot Password?' is positioned below the password field. A dark grey 'Next' button is centered below the inputs. A horizontal line with the word 'Or' in the center separates this from the 'Sign in with Azure_AD_SSO' option, which includes a right-pointing arrow icon. Below this is another blue link 'Need help signing in?'. At the bottom, there is a link '> Cloud account details'.



New MFA process

What to expect when you log in?

If you have not previously configured MFA, you will be prompted to complete a one-time setup process when you next sign in.

Each time you sign in to the Aspire Supplier Portal, you will be required to verify your identity using an additional authentication method after entering your username and password.

This additional security step helps protect your account and organisational information from unauthorised access.

You can choose to receive verification codes via:

- Mobile App
- Phone Number (SMS)*
- Email

Once configured, MFA will be used to verify your identity when required.

* Note: The Phone Number option will only appear if a mobile phone number is recorded in your user account in Aspire.



The screenshot shows the 'ORACLE Cloud' login interface. At the top, it says 'ORACLE Cloud'. Below that, a large heading reads 'Select a method to configure for two-factor authentication.' Underneath this heading is a link that says 'What are the differences?' followed by a question mark icon. There are three selectable options, each in a light gray box with a dark gray border: 'Mobile App' with a mobile phone icon, 'Phone Number' with a speech bubble icon, and 'Email' with an envelope icon. At the bottom of the screen, there is another link that says 'What is two-factor verification?'.



MFA methods available

Verify via Email

- A verification code is sent to the **email address associated with the user account**.
- Users enter the code received via email to complete the sign-in process.
- This option is the simplest and suitable for users who have reliable access to their registered email account.

Verify via Phone Number

- A verification code is sent via **text message (SMS)** to the mobile phone number recorded in the user account.
- This option will **only be available if a mobile phone number has already been recorded** against the user's account.
- If the option is not visible and the user wishes to use SMS verification, they should contact Procurement Support to have their mobile number added or updated.

Verify via Mobile App

- Users can verify their identity using an **authentication app** installed on their mobile device.
- Any compatible authenticator application can be used (for example, Microsoft Authenticator, Google Authenticator, or similar apps).
- The authenticator app must be **installed and configured on the mobile device before it can be used** for MFA.
- During setup, users will link their account to the authenticator app by following the on-screen instructions, typically by scanning a QR code.



New login process

Users only need to set up their chosen MFA verification method once*.

After setup, each sign-in to the Aspire Portal will require two steps:

1. Enter username and password.
2. Complete MFA verification using the selected method (Email, SMS, or Authenticator App).

This additional verification step helps protect user accounts and supplier information, even if a password is compromised.

* For each user account

The diagram illustrates the new login process in two steps, set against a green background. Step 1, 'Sign in', shows a form with 'Username' (supplier@abc.com.au) and 'Password' (masked with dots), a 'Forgot Password?' link, and a 'Next' button. Step 2 shows the 'ORACLE Cloud' logo, a verification instruction, the email address 'supplier@abc.com.au', a six-digit code input field, and a 'Resend code' link.

1 Sign in

supplier@abc.com.au

.....

[Forgot Password?](#)

Next

2

ORACLE Cloud

Verify your email address by
entering the verification code
sent to supplier@abc.com.au

[Resend code](#)



MFA Configuration

Step-by-Step Overview



Detailed configuration instructions

Verify via Email

1. Sign in to Aspire using your existing username and password.
2. Select email as your authentication method.
3. A verification code will be sent to your email.
4. Enter the code when prompted.
5. MFA setup is complete.

Verify via Phone number

1. Sign in to Aspire using your username and password.
2. Select phone number as your authentication method.
3. A verification code will be sent to your phone via SMS.
4. Enter the code when prompted.
5. MFA setup is complete.

Verify via Mobile App

1. Install an Authenticator App such as Microsoft Authenticator or Google Authenticator.
2. Sign in to Aspire using your username and password.
3. Select mobile app as your authentication method.
4. The screen will display a QR code.
5. Click to toggle on "Use Offline Mode or another Authenticator App".
6. Open the Authenticator app on your mobile phone.
7. Select add account and choose the account type if prompted.
8. Use your phone's camera to scan the QR code shown on Aspire.
9. The Authenticator app will display a verification code on your phone.
10. Enter the code when prompted & click Verify.
11. MFA setup is complete.



Information for users with multiple accounts

Multiple accounts

Some providers currently access Aspire using usernames rather than email addresses, particularly where multiple user accounts exist.

If you have multiple Aspire accounts.

Each Aspire account is treated as a separate user profile. This means:

- MFA must be configured for each account individually.
- The same email address or mobile phone number can typically be used for multiple accounts, subject to system configuration.
- You may be prompted to complete MFA setup separately when signing into different accounts.

Using a username Instead of an email address

If your Aspire login uses a username (for example, *jsmith_provider*) rather than an email address:

- You can continue to use your existing username to sign in.
- MFA verification will be linked to the email address or phone number recorded against your account during setup.
- Your username itself does not need to change.

Recommended Approach

If you have multiple Aspire accounts linked to different supplier organisations, we recommend:

- Using the same business email address for MFA where appropriate.
- Keeping your mobile number and email address up to date.
- Contacting us if you are unsure which account you should use.



MFA Configuration

Visual Overview



Method 1: Verify via Email

1. Sign in using your existing username and password

Sign in

Username
supplier@abc.com.au

Password
••••••••

[Forgot Password?](#)

Next

2. Select Email as the method

Select a method to configure for two-factor authentication.

[What are the differences? ?](#)

Mobile App

Phone Number

Email

3. Access and enter the verification code

ORACLE Cloud

Verify your email address by entering the verification code sent to **supplier@abc.com.au**

[Resend code](#)

4. MFA set up is complete, click Continue

ORACLE Cloud

Email successfully enrolled.

Next time you sign in, enter the verification code sent to your email **WAPHA3_Supplier@yopmail.com** to authenticate.

Continue

[Configure another factor](#)



Method 1: Verify via Phone Number

1. Sign in using your existing username and password

Sign in

Username

supplier@abc.com.au

Password

.....

Forgot Password?

Next

2. Select Phone Number as the method

Select a method to configure for two-factor authentication.

What are the differences? ?

Mobile App

Phone Number

Email

3. Send verification to registered number

ORACLE Cloud

+61 455555555

Standard rates may apply.

Send

Choose another method

4. Access and enter the verification code

ORACLE Cloud

A passcode has been sent to +61XXXXXX555

Complete verification by entering the verification code sent to phone number +61XXXXXXX555.

5. MFA set up is complete, click Continue

ORACLE Cloud

Phone successfully enrolled.

Next time you sign in, enter the verification code sent to your phone at +61XXXXXXX775 to authenticate.

Continue

Configure another factor

12

Method 1: Verify via Mobile App

1. Sign in using your existing username and password

Sign in

Username

supplier@abc.com.au

Password

••••••••

Forgot Password?

Next

2. Select Mobile App as the method

Select a method to configure for two-factor authentication.

What are the differences? ?

Mobile App

Phone Number

Email

3. Follow the on-screen instructions, enter the verification code and click Verify

Configure Authenticator App

Step 1: Download the Oracle Mobile Authenticator App from your phone's app store.

Step 2: Open the App, tap Add Account, then scan the QR code below.

Use Offline Mode or another Authenticator App.

?



I can't scan the QR code.

Step 3: Enter the passcode generated by the app.

080703

Verify

Download and install your preferred Authenticator App, such as Microsoft Authenticator or Google Authenticator.

To use an alternative Authenticator App as per above, ensure the 'Use Offline Mode or another Authenticator App.' toggle is turned on (blue), as per Step 2 in the image on the left.

4. MFA set up is complete, click Continue

ORACLE Cloud

Mobile app successfully enrolled.

Next time you sign in, tap **Allow** in the Authenticator app to authenticate.

Continue

Configure another factor

13

Support

If you experience any difficulties setting up MFA or accessing the Aspire Supplier Portal, please contact procurementsupport@wapha.org.au