USING MULTI-FACTOR AUTHENTICATION (MFA)

Contents

1 WHAT IS MULTI-FACTOR AUTHENTICATION (MFA)

Multi-Factor Authentication (MFA) combines two or more independent credentials when you access an IT system or application: what you know (password), what you have (security token), where you are (geolocation) and (in future) who you are (biometric verification).

The goal of MFA is to create a layered defence to make it more difficult for an unauthorized person to access your account. If one "factor" is compromised or broken (for instance someone managed to get your password through a phishing attack), the attacker still has at least one more barrier to breach before successfully breaking into your account. This is similar to what you might already have for internet banking and other secure online services.
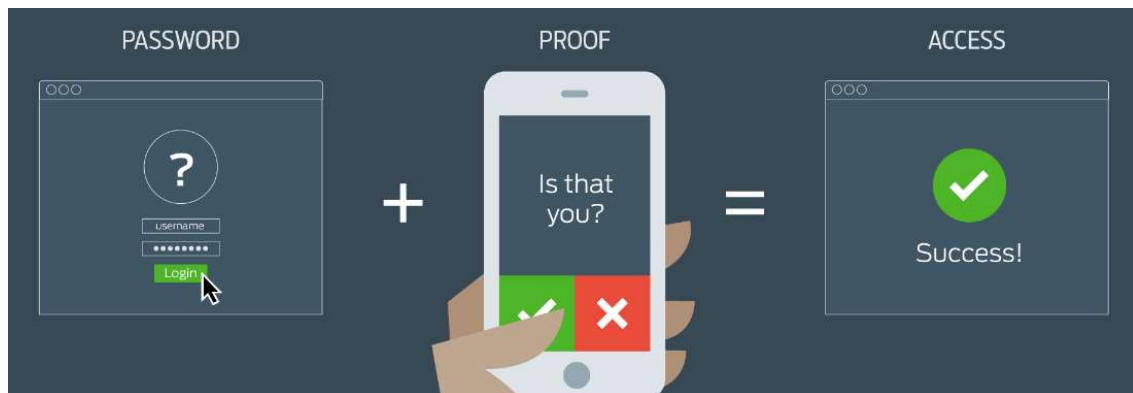
2 HOW DO I LOGIN ONCE MFA HAS BEEN ENABLED?

If you're logging into your work computer, you can log in the exact same way you currently do, however when you connect to an Internet service (such as Outlook Webmail or Microsoft Teams), you'll be prompted for your MFA code.

Enter your MCD Group username and password as you currently do.

Once your password has been accepted, you will be prompted for your authentication code.

Open the Microsoft Authenticator app on your phone (or the text you have been sent), retrieve your unique code and enter it as required to access your MCD Group services.
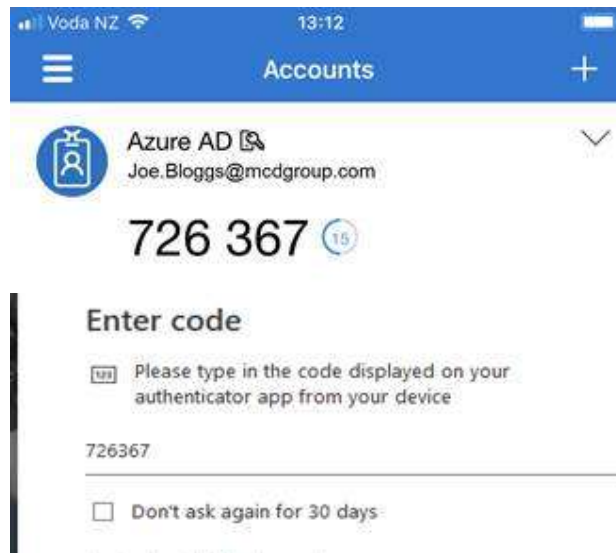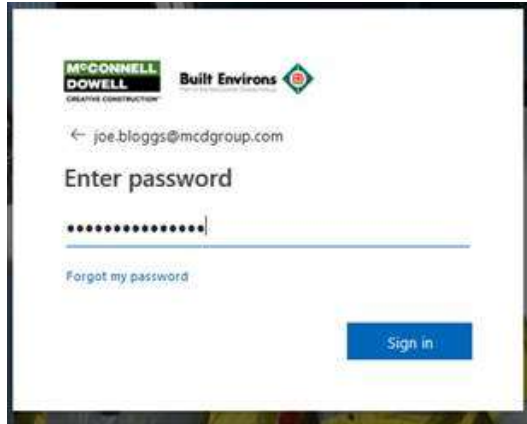
Note: You might experience delays in receiving your code if you are travelling internationally or if there is network congestion. If this is the case, simply select one of the alternate authentication methods (see ALTERNATE METHODS OF NOTIFICATION) or contact the IT department who can temporarily (for 12 hours) remove the need to use MFA.

3 HOW DO I REGISTER?

There are a few methods to receive a code:

1. Via the Microsoft Authenticator App
2. A text on your mobile
3. A Call-back to any number

3.1 USING THE MICROSOFT AUTHENTICATOR APP

1. Go to https://mypassword.mcdgroup.com/register

2. From the Security Info screen, select "**+ Add Method"**, choose "**Authenticator App"** and then select "**Add".** Click "next" until a QR code is displayed
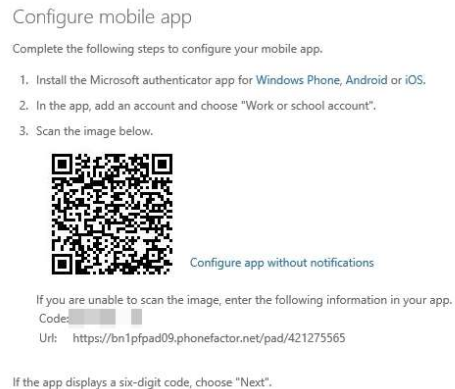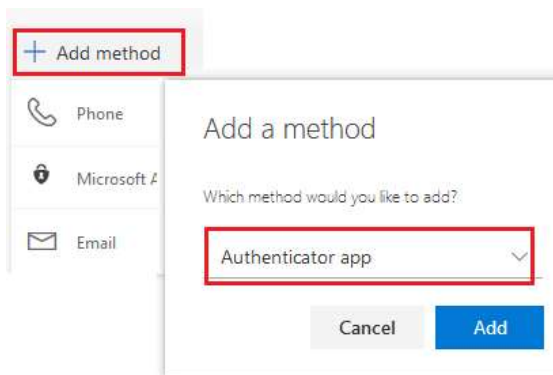
3. Open the Microsoft Authenticator App on your phone

- MCD Group IT have already deployed the app to all company phones
- You can install the app onto a personal phone using one of the links below or search for "Microsoft Authenticator" in the app store:
  - Apple iPhone: https://apps.apple.com/us/app/microsoft-authenticator/id983156458
  - Android:https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en

4. Under Accounts click + and select "work or school" then scan the QR code

5. Enter the 6-digit code on your phone into the browser to Verify the connection

5
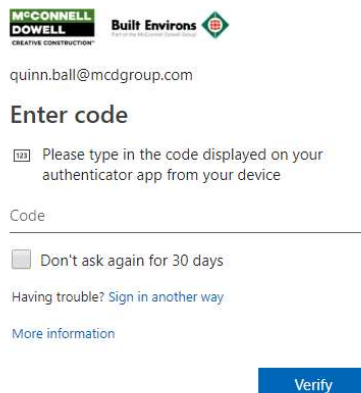
3.2   VIA A TEXT MESSAGE

1. Navigate to https://mypassword.mcdgroup.com/register from your pc browser

2. From the Security Info screen, select "+ **Add Method",** choose "**Phone**" and then select "**Add**"

3. Enter your Phone Number, and select **Text me a code**, and click **Next**.

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.
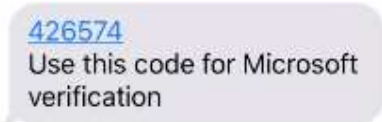
What phone number would you like to use?

| Australia (+61) ⌄ | 04▓▓▓▓▓▓ |

🔘 Text me a code

⚪ Call me

Message and data rates may apply.

Cancel   **Next**

4. You will be prompted for a code, which you will receive via SMS. Please keep in mind this can take up to a few minutes to process depending on network congestion or if you are "roaming".

426574
Use this code for Microsoft verification

Phone

We just sent a 6 digit code to +61 04▓▓▓▓▓▓. Enter the code below.

426574

Resend code

Back   **Next**

5. Once you enter the code and click next you will receive verification.

✅ SMS verified successfully

3.3   BY RECEIVING A CALL

1. Navigate to https://mypassword.mcdgroup.com/register from your pc browser

2. From the Security Info screen, select "+ **Add Method",** choose "**Phone**" and then select "**Add**"

3. Enter your Phone Number, and choose **Call me**, and click **Next**.

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

| Australia (+61) ⌄ | 04░░░░░░ |

○ Text me a code

◉ Call me

Message and data rates may apply.

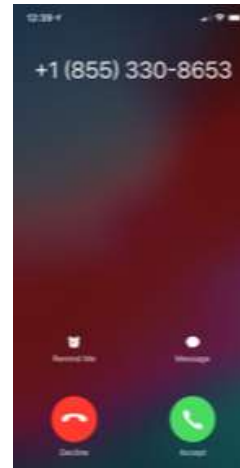| Cancel | **Next** |

+1 (855) 330-8653

4. Once you click next you will receive a call.

Phone

We're calling +61 04░░░░░ now.

| Back |

4. Answer the call and follow the prompts to verify.

✓ Call answered

3.4 ALTERNATE METHODS OF NOTIFICATIONS

It is recommended that you have multiple authentication methods. You can change your default method at any time from the Security Info page as shown below.

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification Change

4 HOW OFTEN WILL I BE REQUIRED TO USE MFA?

If you're on a device you trust (like your work computer), you may wish to select "Don't ask again for 30 days" when you see the login screen. This will reduce the number of times you are prompted for MFA.

It's important that you don't select this on public or shared computers, as this may allow someone else to gain access to your account.

Even after selecting "Don't ask for 30 days" you may receive MFA prompts as the system monitors for changes to networks and other security aspects (i.e. connected to public WiFi etc). This is normal behaviour and designed to help keep your account secure. If you believe you are being requested too frequently to provide MFA confirmation, please contact the MCD Group IT Service Desk.

5 NEED HELP?

If you need assistance, please do not hesitate to contact the IT Service Desk (Servicedesk@mcdgroup.com)