Multi-Factor Authentication Enrolment Guide

How to set up the service and authenticate successfully

What is MFA and how does it impact the way I sign into my account or applications?

Multi-Factor Authentication (MFA) is a new security feature to provide an additional level of identity verification to help prevent unauthorised access to Deloitte’s applications. When an application is enabled for MFA, a second authentication process is required to access the application.

Deloitte is utilising Microsoft Azure AD and Azure B2B for MFA services.

Before using MFA to access Deloitte applications, a one-time enrolment is necessary. When enrolling, you will select your MFA authentication method. Until enrolment in MFA is completed, you will be unable to access the applications that have MFA enabled.

Note:
- If you access multiple Deloitte applications, you will only need to go through the Azure AD enrolment process once. After successfully enrolling, you will be able to access any Deloitte application that has been enabled for Microsoft Azure AD and Azure B2B MFA for which you have an account and received and accepted an e-mail invitation. However, you may need to enrol in MFA more than once if you access any Deloitte applications that use an alternative MFA solution.
- There are a number of options you can use to enrol and authenticate in to MFA, including your smart phone

Contents

1 Enrolling in Multi-Factor Authentication (MFA) 2
  1.1 Enrolling in MFA with the Mobile App 3
  1.2 Enrolling in MFA with Authentication phone text message or phone call option 7
    1.2.1 Text Message 7
    1.2.2 Phone call 10
  1.3 Enrolling in MFA: Creating a Microsoft authentication account 13
2 Managing your authentication options 15
  2.1 Setting up your backup authentication method 15
  2.2 Using your backup authentication method 16
  2.3 Changing your preferred authentication method 17
1 Enrolling in Multi-Factor Authentication (MFA)

There are a number of easy verification options, and the first step in the enrolment process is to decide how you would like to be contacted to verify your account.

The contact methods are listed in the table below, click on the links to go to the set-up steps for each method.

<table>
<thead>
<tr>
<th>Contact method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Mobile app              | • **Receive notifications for verification.** This option pushes a notification to the authenticator app on your smartphone. View the notification and, if it is legitimate, select **Authenticate** in the app.  
                          | • **Use verification code.** In this mode, the authenticator app generates a verification code that updates every 30 seconds. Enter the most current verification code in the sign-in interface.  
                          | • The Microsoft Authenticator app is available for **Windows Phone**, **Android**, and **iOS**. |
| Mobile phone call or text| • **Phone call** places an automated voice call to the phone number you provide. Answer the call and press # in the phone keypad to authenticate.  
                          | • **Text message** sends a text message containing a verification code. Enter the verification code provided into the sign-in interface. |
| Authentication phone call| • Places an automated voice call to the phone number you provide. Answer the call and press # in the phone keypad to authenticate. |

Note: The mobile app verification code option is the only authentication option that allows MFA verification at all times, even without network coverage service (i.e. on a flight). Therefore, you are encouraged to select this method as your preferred authentication method.
1.1 Enrolling in MFA with the Mobile App

1. When the Deloitte application you access has enabled MFA, you will receive an e-mail invitation to enrol, with a unique link. Click the link to Get Started.

2. If your organisation already uses Microsoft Azure B2B MFA, or if your organisation/corporate email is already registered with Microsoft (for example, through the use of Office365 or Skype) and you are enrolling with this e-mail address, you will see a consent screen to utilise your organisation’s MFA to access the Deloitte application.

   **Note:** If you do not see a consent screen, skip to the Creating a Microsoft authentication account section.

3. To continue, please enter your existing Microsoft login credentials (username and password). After authenticating, you will see a screen asking you to set up MFA.

   **Note:** In this example, your organisation’s name is Cherno Alpha.
4. Select the additional security verification option from the drop-down. The **Mobile App** option is recommended.

![Additional security verification](image1)

5. On your mobile device, access the **Microsoft Authenticator** mobile app on the (i) App Store®, Microsoft Store, or (ii) on Google Play.

A QR code scanner will appear using the camera on your mobile device. If you are asked to allow the Microsoft Authenticator app to access your camera, click **Allow**.

**Note:** If your mobile device is unable to download the Microsoft Authenticator app, please select one of the alternate authentication options.

6. Once the app is installed, open the app and click **Add account** or tap the + icon to add a new account. Select **Work or school account**.

![Add account](image2)
7. Scan the QR code on your PC/laptop screen.

8. If you are unable to scan the QR code, tap the **Or enter code manually** link on your screen, and enter the code and URL displayed below the QR code. Click **Done** (below the QR code) if you see a 6-digit code on your mobile app screen.

9. Click the **Set up** button to continue.

10. Click **Contact me** to continue.
11. Add your mobile phone number as a secondary contact option (in case you lose access to the mobile app) and click **Done**.

![Multi-Factor Authentication Enrolment Guide](image)

12. After enrolment is complete, you will be logged in to the Deloitte application

**Subsequent log-in process**

1. When you next log-in to the Deloitte application after setting up MFA, you will be directed to a Microsoft log-in screen.

2. Enter your login credentials and click **Sign in**. You will receive an authentication code from the mobile app to verify your credentials as part of the MFA process.

![Microsoft Log-in Screen](image)

3. After successfully authenticating, you will be logged in to the Deloitte application

**Note:**
- Your authentication will remain active for 8 hours.
- The authentication is specific to the browser with which you authenticate. If you try to access the application via a different browser, you will need to re-authenticate.
1.2 Enrolling in MFA with Authentication phone text message or phone call option

1.2.1 Text Message

1. When the Deloitte application you access has enabled MFA, you will receive an e-mail invitation to enrol, with a unique link. Click the link to Get Started.

If your organisation already uses Microsoft Azure B2B MFA, and you are enrolling with your corporate e-mail address account, you will see a consent screen to utilise your organisation’s MFA to access the Deloitte application.

**Note:** If you do not see a consent screen, skip to the Creating a Microsoft authentication account section.

2. Enter your login credentials. After authenticating, you will see a screen asking you to set up MFA. **Note:** In this example, your organisation’s name is Cherno Alpha.
3. Select Authentication phone from the drop-down. Select **Send me a code by text message** and enter Mobile phone details. Select **Contact me** to continue.

4. You will receive a text message from Microsoft with a 6-digit code. Enter the code and click **Verify** to continue.

5. You will receive a verification successful page. Click **Done** to complete the enrolment process.
6. After enrolment is complete, you will be logged into the Deloitte application.

**Subsequent log-in process**

1. When you next log-in to the Deloitte application after setting up MFA, you will be directed to a Microsoft log-in screen.
2. Enter your login credentials and click Sign in. You will receive a text message to your authentication phone to verify your credentials as part of the MFA process.

3. After successfully authenticating, you will be logged in to the Deloitte application

**Note:**
- Your authentication will remain active for 8 hours.
- The authentication is specific to the browser with which you authenticate. If you try to access the application via a different browser, you will need to re-authenticate.
1.2.2 Phone call

1. When the Deloitte application you access has enabled MFA, you will receive an e-mail invitation to enrol, with a unique link. Click the link to Get Started.

2. If your organisation already uses Microsoft Azure B2B MFA, and you are enrolling with your corporate e-mail address account, you will see a consent screen to utilise your organisation’s MFA to access the Deloitte application.

   **Note:** If you do not see a consent screen, skip to the Creating a Microsoft authentication account section.

3. Enter your login credentials. After authenticating, you will see a screen asking you to set up MFA. **Note:** In this example, your organisation’s name is Cherno Alpha.
4. Select Authentication phone from the drop-down menu. Select **Call me** and enter telephone details (this can be a mobile phone number or desk phone number).
   Select **Contact me** to continue.

7. You will receive a telephone call. Answer the call and press # to verify and continue.

8. You will receive a verification successful page. Click **Done** to complete the enrolment process.
9. After enrolment is complete, you will be logged into the Deloitte application.

**Subsequent log-in process**

1. When you next log-in to the Deloitte application after setting up MFA, you will be directed to a Microsoft log-in screen.
2. Enter your login credentials and click Sign in. You will receive a phone call to your authentication phone to verify your credentials as part of the MFA process.

3. After successfully authenticating, you will be logged in to the Deloitte application

**Note:**
- Your authentication will remain active for 8 hours.
- The authentication is specific to the browser with which you authenticate. If you try to access the application via a different browser, you will need to re-authenticate.
1.3 Enrolling in MFA: Creating a Microsoft authentication account

1. When the Deloitte application you access has enabled MFA, you will receive an e-mail invitation to enrol, with a unique link. Click the link provided in the email to Get Started

   Note:

2. You will be directed to a consent page to set up a Microsoft authentication account. Click Next to continue.

3. Enter your e-mail address and create a new password. Please ensure you use an email address to create your account. Deloitte are not able to support account creation with a phone number

   Note: Your password to access the Deloitte application will change to the password you create in this step
4. A verification code will be sent to the e-mail address you entered. When retrieving this code please do not close down the *Enter Code* tab/window (illustrated below).

5. Enter the verification code and click **Next**. Enter the Captcha and click **Next** to continue.

6. After your account is created, click **Set it up now** to continue the enrolment process.

7. Follow the enrolment process for your preferred authentication contact method outlined above (mobile phone call, text message, mobile app or call to your authentication phone – mobile or desk phone)
2 Managing your authentication options

2.1 Setting up your backup authentication method

By setting up backup authentication methods, you can decrease the likelihood of being completely locked out of an MFA-enabled application in the situation that you are unable to access your primary authentication method.

1. To set up your backup authentication methods, navigate to the Additional security verification web page (note: you will have to authenticate via MFA to access the page).
2. Under ‘how would you like to respond?’ select one or more of the additional options available for authentication and provide the necessary information.
3. When you are finished adding additional authentication methods, click Save.
4. When the verification message appears, click Close to complete the process.
2.2 Using your backup authentication method

1. Log-in as you normally would

2. To use a backup authentication method, click the **Sign in another way** on the MFA login page.

3. Select the authentication method you wish to use from the available options and proceed as normal.
2.3 Changing your preferred authentication method

1. To change your preferred authentication method, navigate to the Additional security verification web page (note: you will have to authenticate via MFA to access the page).
2. Select your preferred method of authentication from the dropdown list under ‘what’s your preferred option?’

3. Click Verify preferred option to verify your choice.
4. When the verification message appears, click Close to complete the process.