

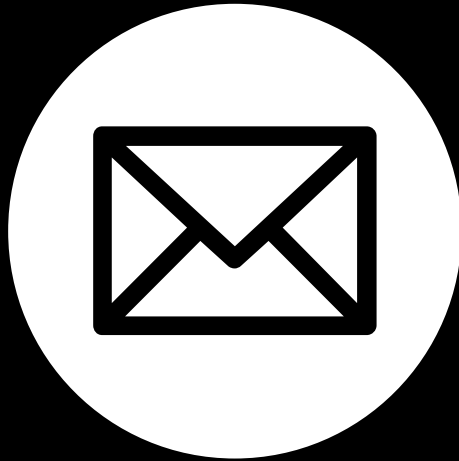


MFA Enrollment overview

Multi Factor Authentication

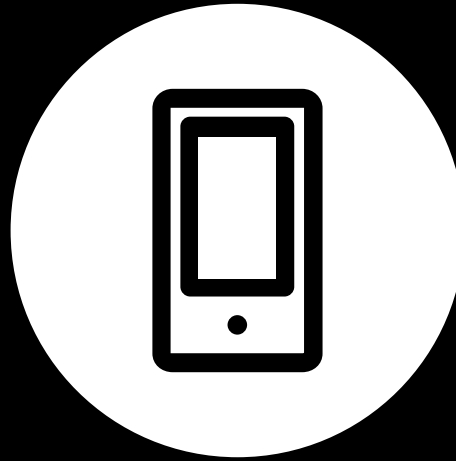
Deloitte Luxembourg

3 enrollment authentication methods



SMS

(You will receive a code by SMS)



Mobile app

(You will receive a notification on the app)



Phone call

(You will receive instructions by phone call)

Please choose your authentication method and click on the icon to discover the enrollment process

** We recommend to use the SMS authentication method*

Enrollment #1

SMS

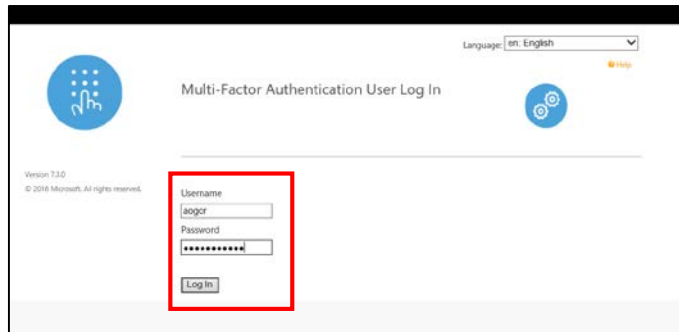
authentication method



Enrollment by SMS

1 Connect to the MFA enrollment page: [link](#)

2 Enter your application login & password



Multi-Factor Authentication User Log In

Language: en: English

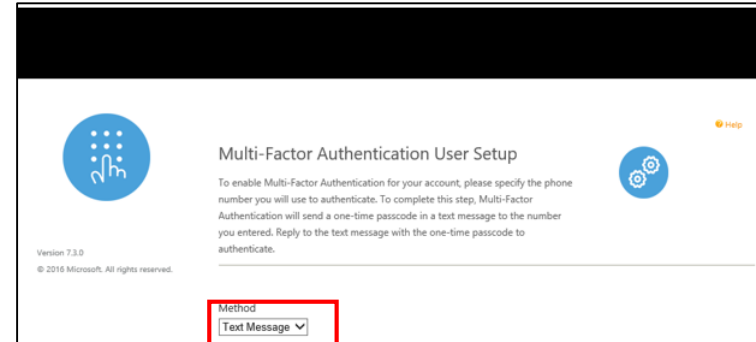
Version 7.3.0
© 2016 Microsoft. All rights reserved.

Username
laocr

Password

Log In

3 Choose the authentication method: "Text message"



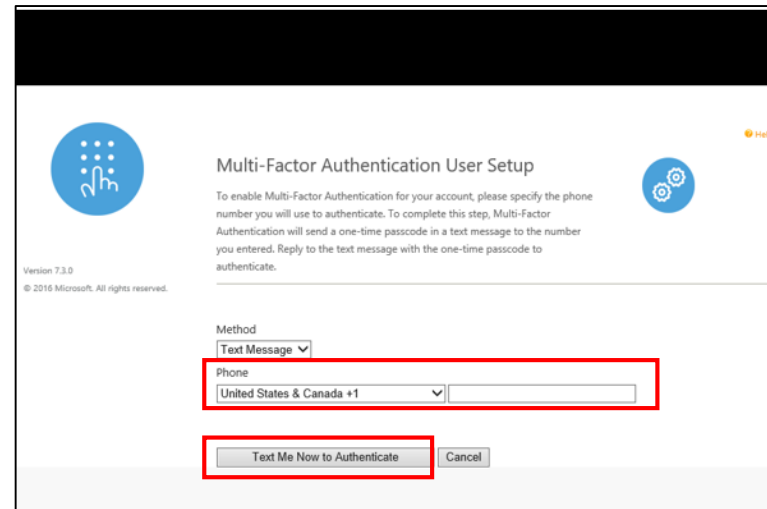
Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account, please specify the phone number you will use to authenticate. To complete this step, Multi-Factor Authentication will send a one-time passcode in a text message to the number you entered. Reply to the text message with the one-time passcode to authenticate.

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Method
Text Message

4 Enter your mobile number and click "Text me Now to Authenticate"



Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account, please specify the phone number you will use to authenticate. To complete this step, Multi-Factor Authentication will send a one-time passcode in a text message to the number you entered. Reply to the text message with the one-time passcode to authenticate.

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Method
Text Message

Phone
United States & Canada +1

Text Me Now to Authenticate Cancel

You will receive a text message with a code that you will need to enter

Enrollment by SMS

5 Choose your security questions and provide answers to them

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Security Questions

Please choose security questions and answers before continuing. These questions will be used to validate your identity should you need support using Multi-Factor Authentication.

Question 1
What is your favorite sports team?
Answer

Question 2
What is your favorite meal?
Answer

Question 3
Who is your favorite actor, musician, or artist?
Answer

Question 4
What is your favorite movie?
Answer

[Continue](#) [Cancel](#)

Men | Log Out

Welcome

Account Configuration Complete
Your account has been configured to use Multi-Factor Authentication.

When you sign on, you will continue to use the same username and password. Before your verification is complete, you will receive a notification asking you to launch the Microsoft Authenticator mobile app and press the Authenticate button to complete your sign on. If you don't confirm the sign on by pressing Authenticate, the sign on will be denied.

You should only press the Authenticate button when you receive the Microsoft Authenticator mobile app notification if you are actually signing on to the application. Otherwise, someone may be trying to sign on with your username and password and you should report this potential fraud to your IT administrator.

Manage your Multi-Factor Authentication account by selecting an option below. Select the Help icon (top right) for assistance.

[Change Phone](#)

FAQs

How does Multi-Factor Authentication™ work?
Multi-Factor Authentication works by sending a notification to your Microsoft Authenticator mobile app during login.

Step 1:
Enter your usual username and password.

Step 2:
Instantly, you receive a Microsoft Authenticator mobile app notification. Launch the app and press the Authenticate button.

That's It!

This simple process provides two separate factors of authentication through two separate channels (your computer and your smart phone).

What happens if I lose my phone?
Select the Change Phone Number option to enter a new phone number. An alternate number can also be set up by calling the support help desk, once your identity is strongly established.

What happens if I lose cell phone coverage in a certain area?
The Microsoft Authenticator mobile app works equally well over Wi-Fi.

What if I receive a Microsoft Authenticator mobile app notification when I'm not trying to log in?
This would only happen if someone else were trying to log into your account, and they already knew your password. Remember, Microsoft Authenticator mobile app notifications are only sent after the username and password are verified. So, if this happens, Multi-Factor Authentication has just saved your account from illicit access! To report the incident, press the Copy and Report Fraud button in the Microsoft Authenticator mobile app. This will alert your company's IT security team. Future authentication attempts will be blocked until the issue has been resolved.

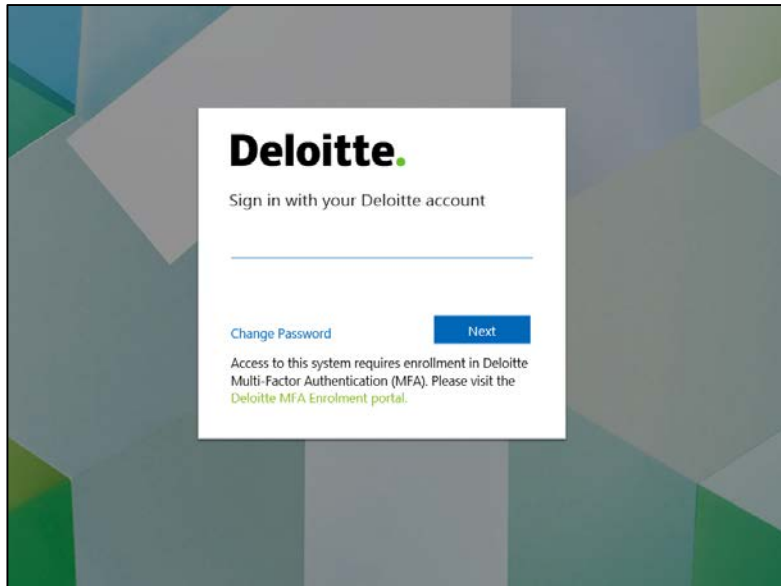


Congratulations!
You are now enrolled

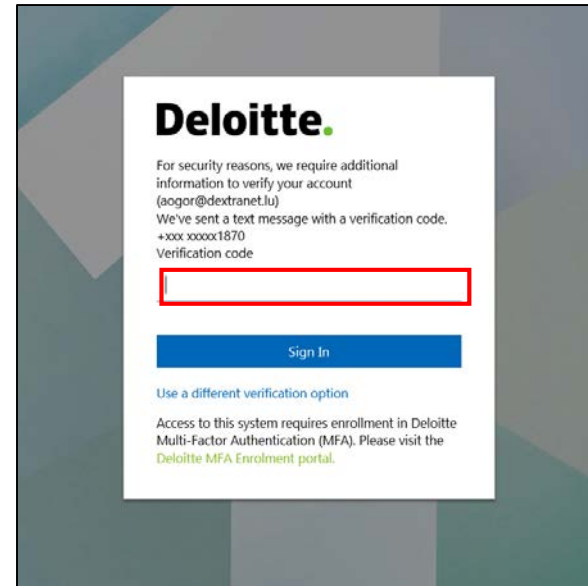
NB: You can select the security questions by using the dropdown lists

Sign in by SMS

1 Enter your application login & password



2 SMS : please enter the passcode received on your mobile phone



Enrollment #2

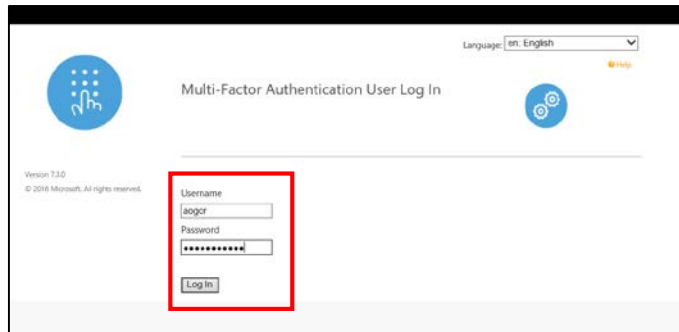
mobile app
authentication method



Enrollment by mobile app

1 Connect to the MFA enrollment page: [link](#)

2 Enter your application login & password



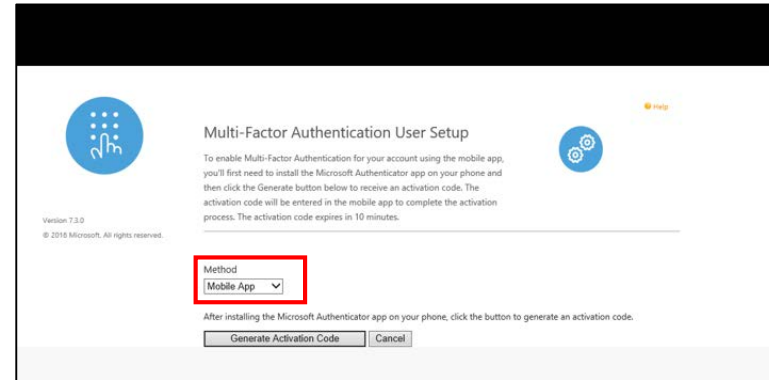
Multi-Factor Authentication User Log In

Username
laocr

Password

Log In

3 Choose the authentication method : "Mobile app"



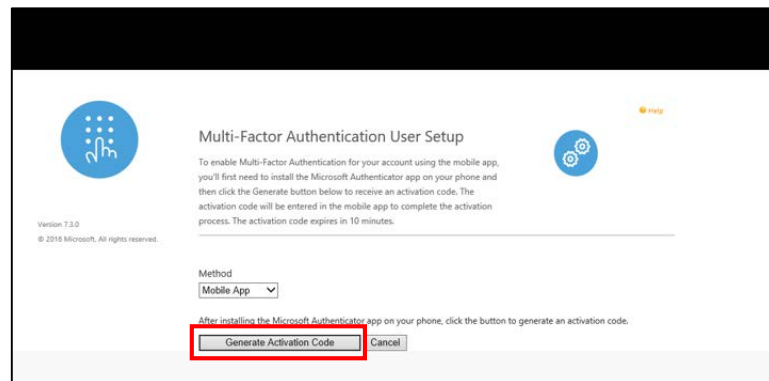
Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account using the mobile app, you'll first need to install the Microsoft Authenticator app on your phone and then click the Generate button below to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes.

Method
Mobile App

Generate Activation Code Cancel

4 Click on "Generate activation code"



Multi-Factor Authentication User Setup

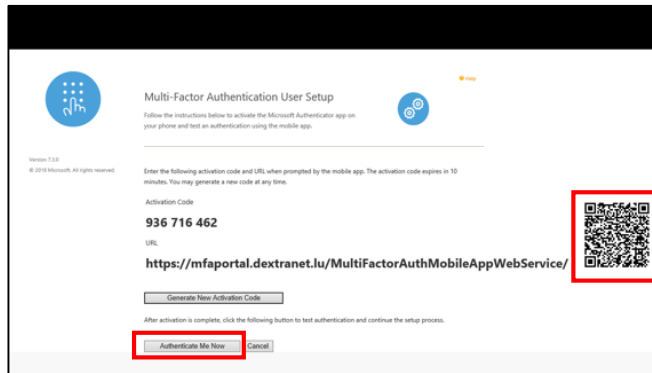
To enable Multi-Factor Authentication for your account using the mobile app, you'll first need to install the Microsoft Authenticator app on your phone and then click the Generate button below to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes.

Method
Mobile App

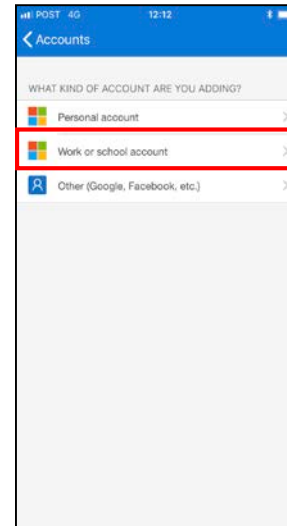
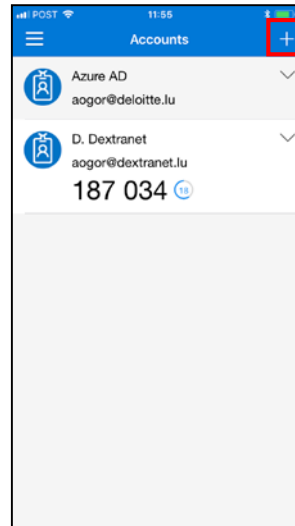
Generate Activation Code Cancel

Enrollment by mobile app

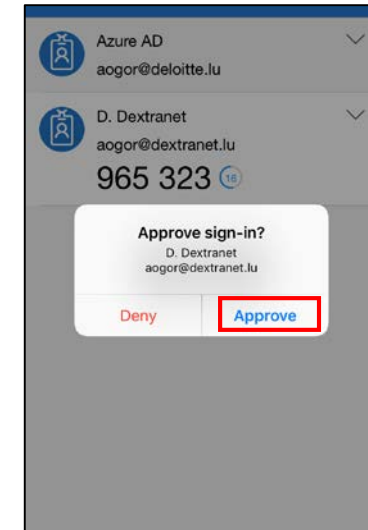
5 Scan the QR code on your mobile through the App “**Microsoft Authenticator**” (you can download it in the App Store)



6 In the App, after clicking on the widget “+”, please click on “Work or school account” to be able to scan the QR code and register a new account



8 Click on “Approve” on the App



7 Once the account is added in the App, please click on “Authenticate Me Now” in the portal

Enrolment by mobile app

8

Choose your security questions and provide answers to them

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Security Questions

Please choose security questions and answers before continuing. These questions will be used to validate your identity should you need support using Multi-Factor Authentication.

Question 1
What is your favorite sports team?
Answer

Question 2
What is your favorite meal?
Answer

Question 3
Who is your favorite actor, musician, or artist?
Answer

Question 4
What is your favorite movie?
Answer

Continue Cancel

Welcome

Account Configuration Complete
Your account has been configured to use Multi-Factor Authentication.

When you sign on, you will continue to use the same username and password. Before your verification is complete, you will receive a notification asking you to search for the Microsoft Authenticator mobile app and press the Authenticate button to complete your sign on. If you don't confirm the sign on by pressing Authenticate, the sign on will be denied.

You should only press the Authenticate button when you receive the Microsoft Authenticator mobile app notification if you are actually signing on to the application. Otherwise, someone may be trying to sign on with your username and password and you should report this potential threat to your IT administrator.

Manage your Multi-Factor Authentication account by selecting an option below. Select the Help icon (top right) for assistance.

Change Phone

FAQs

How does Multi-Factor Authentication work?
Multi-Factor Authentication works by sending a notification to your Microsoft Authenticator mobile app during login.

Step 1:
Enter your usual username and password.

Step 2:
Instantly, you receive a Microsoft Authenticator mobile app notification. Launch the app and press the Authenticate button.

That's it!

This simple process provides two separate factors of authentication through two separate channels (your computer and your smart phone).

What happens if I lose my phone?
Select the Change Phone Number option to enter a new phone number. An alternate number can also be set up by calling the support help desk, once your identity is strongly established.

What happens if I lose cell phone coverage in a certain area?
The Microsoft Authenticator mobile app works equally well over WiFi.

What if I receive a Microsoft Authenticator mobile app notification when I'm not trying to log in?
This would only happen if someone else were trying to log into your account, and they already knew your password. Remember, Microsoft Authenticator mobile app notifications are only sent after the username and password are verified. So if this happens, Multi-Factor Authentication has just saved your account from being accessed! To report the incident, press the Deny and Report Fraud button in the Microsoft Authenticator mobile app. This will alert your company's IT security team. Future authentication attempts will be blocked until the issue has been resolved.

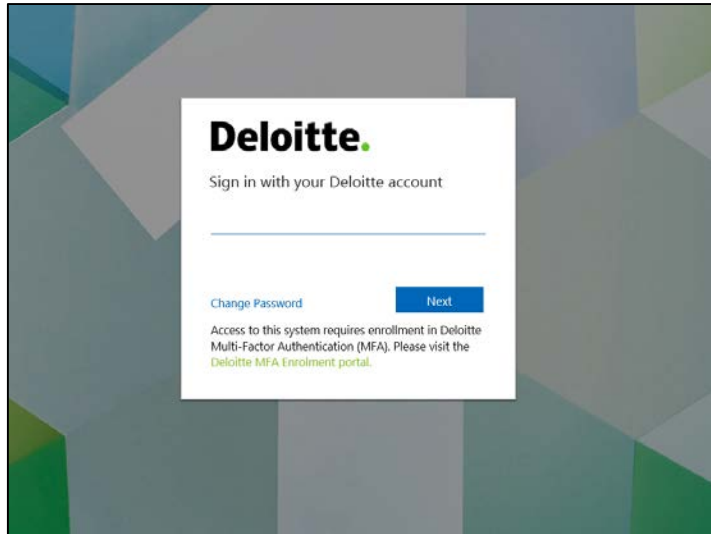


Congratulations!
You are now enrolled

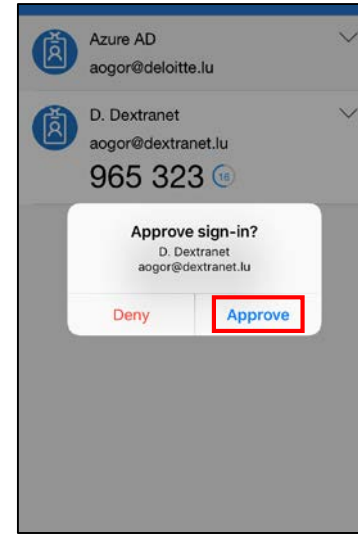
NB: You can select the security questions by using the dropdown lists

Sign in by mobile app

1 Enter your application login & password



2 **Mobile app:** open it and click on "Approve"



Enrollment #3

phone call
authentication method



Enrollment by phone call

1 Connect to the MFA enrollment page: [link](#)

2 Enter your application login & password

Multi-Factor Authentication User Log In

Language: en: English

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Username
laogor

Password

Log In

3 Choose the authentication method: "Phone Call"

Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account, please specify the phone number you will use to authenticate. To complete this step, Multi-Factor Authentication will call the number you entered. Answer and press # to authenticate.

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Method
Phone Call

4 Enter your mobile number and click "Call me Now to Authenticate"

Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account, please specify the phone number you will use to authenticate. To complete this step, Multi-Factor Authentication will call the number you entered. Answer and press # to authenticate.

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Method
Phone Call

Phone
United States & Canada +1

Extension

Call Me Now to Authenticate Cancel

Enrollment by phone call

5 Choose your security questions and provide answers to them

Version 7.3.0
© 2016 Microsoft. All rights reserved.

Security Questions

Please choose security questions and answers before continuing. These questions will be used to validate your identity should you need support using Multi-Factor Authentication.

Question 1
What is your favorite sports team?
Answer

Question 2
What is your favorite meal?
Answer

Question 3
Who is your favorite actor, musician, or artist?
Answer

Question 4
What is your favorite movie?
Answer

[Continue](#) [Cancel](#)

Men | Log Out

Welcome

Account Configuration Complete
Your account has been configured to use Multi-Factor Authentication.

My Account
[Change Method](#)
[Change Phone](#)
[Activate Mobile App](#)
[Change Security Questions](#)

Version 7.3.0
© 2016 Microsoft. All rights reserved.

[Change Phone](#)

FAQs

How does Multi-Factor Authentication work?
Multi-Factor Authentication works by sending a notification to your Microsoft Authenticator mobile app during login.

Step 1:
Enter your usual username and password.

Step 2:
Instantly, you receive a Microsoft Authenticator mobile app notification. Launch the app and press the Authenticate button.

That's it!

This simple process provides two separate factors of authentication through two separate channels (your computer and your smart phone).

What happens if I lose my phone?
Select the Change Phone Number option to enter a new phone number. An alternate number can also be set up by calling the support help desk, once your identity is strongly established.

What happens if I lose cell phone coverage in a certain area?
The Microsoft Authenticator mobile app works equally well over Wi-Fi.

What if I receive a Microsoft Authenticator mobile app notification when I'm not trying to log in?
This would only happen if someone else were trying to log into your account, and they already knew your password. Remember, Microsoft Authenticator mobile app notifications are only sent after the username and password are verified. So, if this happens, Multi-Factor Authentication has just saved your account from illicit access! To report the incident, press the Copy and Report Fraud button in the Microsoft Authenticator mobile app. This will alert your company's IT security team. Future authentication attempts will be blocked until the issue has been resolved.

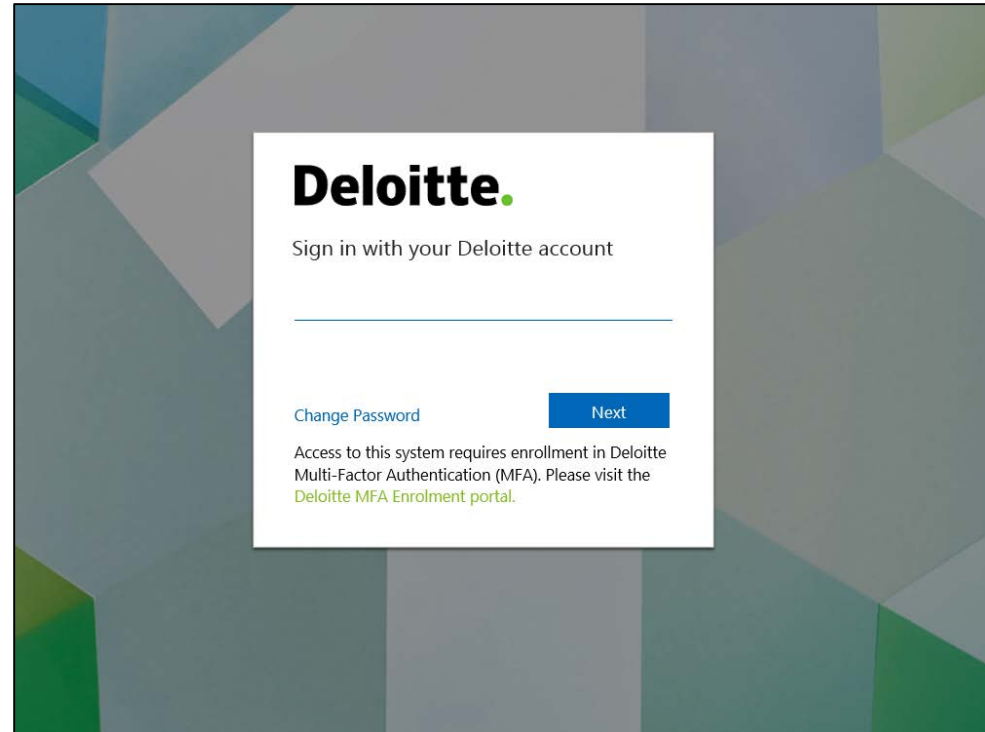


Congratulations!
You are now enrolled

NB: You can select the security questions by using the dropdown lists

Sign in by phone call

- 1 Enter your application login & password
- 2 **Phone call** : pick up and wait the instructions



Manage your account

SMS / App / Phone call

Manage your account

Change your authentication method

1 Access the enrollment portal [link](#)

2 Enter your application login and password + identify yourself with App / Phone call / SMS

3 Change your authentication method: My account > Change method



Deloitte is a multidisciplinary service organization which is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals make an impact that matters, please connect with us on [Facebook](#), [LinkedIn](#), or [Twitter](#).