

Multi-factor authentication enrollment guide for Deloitte practitioners

What is multi-factor authentication (MFA) and how does it impact the way I sign into my account or applications?

MFA is a security feature to provide an additional level of identity verification to help prevent unauthorized access to Deloitte's applications. When an application is enabled with MFA, a second authentication process is required to access the application.

Before using MFA to access DOL eRoom, a one-time enrollment is necessary. When enrolling, you will select your authentication method. Until enrollment is completed, access will be denied to your eRooms.

DOL eRoom will be using a customized MFA solution that requires all users to enroll in MFA, even if you have already enrolled in MFA for another application (i.e., VPN) as it uses a separate underlying technology to manage internal user credentials. You may use your mobile device to enroll in MFA and to authenticate when accessing eRooms.

If you are a newly added user to DOL eRoom, please allow at least 30 minutes for your login credentials to be synchronized with MFA.

This document provides information on:

- [Enrolling in MFA](#) and selecting an authentication method
 - Receiving a prompt to authenticate via mobile application
 - Receiving a phone call to a number of your choosing
- [Adding or updating security questions](#) to be used for authentication if you are unable to authenticate via mobile application or phone call
- [Updating your MFA preferences](#)
- [Authentication failure resolution](#)

Enrolling in MFA

1. On the eRoom login page, select **Deloitte practitioners**.

Welcome to Deloitte OnLine Classic
Collaborate. Share. Know.

Deloitte OnLine is a client-focused website aimed at enhancing your communication and collaboration with the people of Deloitte. Designed to increase your visibility into how we can best solve your business challenges, Deloitte OnLine enriches the interaction between your team and ours.

Please note: Deloitte is moving from this classic eRoom platform to Microsoft SharePoint. Contact your eRoom owner or Deloitte representative for information about the transition.

As part of our continuous improvements to protect your data, multi-factor authentication (MFA) will be implemented for this application on 16 December 2017. MFA requires an additional authentication after you enter your user name and password. On 16 December 2017, all users will be required to enroll before accessing the system. The MFA enrollment and quick reference guides are available on the [Need help logging in?](#) page. You may pre-enroll now by clicking the appropriate link below.

[Deloitte practitioners](#) / [Client or business partners](#)

To access Deloitte OnLine, login below with your User name and password. If you need an account or would like more information about how Deloitte OnLine can start to work for you, contact your Deloitte client service team.

2. On the resulting **Multi-Factor Authentication User Log In** page, enter your eRoom **Username** and **Password** into the appropriate fields and select **Log In**. *The **Multi-Factor Authentication Set-up** page will appear next.*

Selecting an authentication method

From the **Method** dropdown menu, select your preferred method of authentication.

- **Phone Call** – the system will authenticate your identity via a phone call to the number you provide
- **Mobile App** – you will authenticate using the **Microsoft Authenticator app**. The **Microsoft Authenticator app** is the recommended method for frequent travelers and allows for users to authenticate via Wi-Fi when traveling on an aircraft without cellular service.

Authenticating via Phone Call

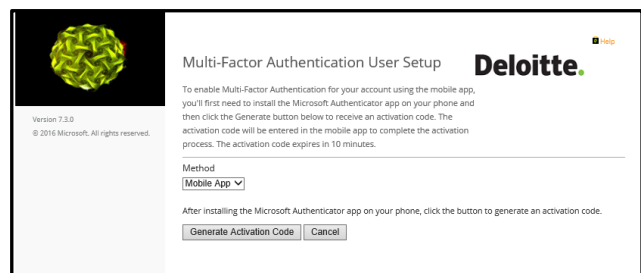
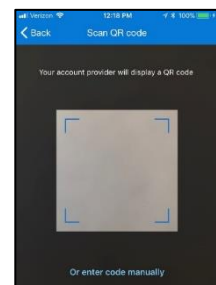
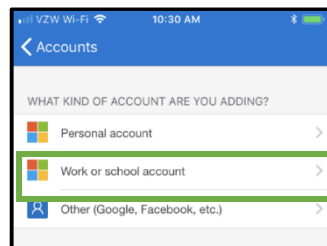
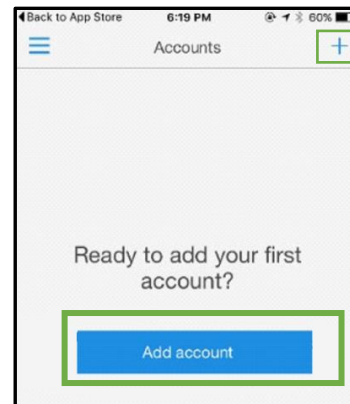
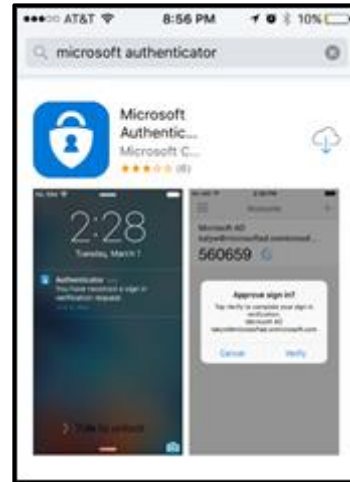
If you choose **Phone Call**, enter your phone number and any needed office extension number (office extension number is not required). Select **Call Me Now to Authenticate**. You will receive a phone call to the number you provided and to authenticate by pressing the pound/hashtag key (#).

Authenticating via Mobile App

In order to select **Mobile App** as your method, first download the **Microsoft Authenticator app** onto your mobile device. The app is available from Apple, Google, and Windows application stores.

Note: If your mobile device does not support the **Microsoft Authenticator app**, you must select the **Phone Call** method.

1. Once you have installed the Microsoft Authenticator app, open it and add a new account by selecting either **Add account** or the **+** icon.
2. Select **Work or school account**.
*The **Scan QR code** screen displays on your mobile device.*
3. On the **Multi-Factor Authentication User Setup** page on your device, select **Mobile app** from the **Method** dropdown list, and select **Generate Activation Code** to generate an activation code, URL, and QR code.



- Using your mobile device, authenticate by scanning the QR code. If, for any reason, you cannot scan the QR code, select the **Or enter code manually** option and enter the activation code and URL.

After configuring your preferred authentication method, you will be directed to the **Security Questions** setup page.

Setting up security questions

Security questions allow users to authenticate when unable to use their preferred authentication method.

- For each security question, select a question from the dropdown menu and provide your answer. All questions must be completed. Select **Continue**. The **Welcome** screen displays to indicate successful MFA enrollment.

Updating your MFA preferences

After enrolling and successfully authenticating via MFA, you can update your MFA preferences at any time. Be sure to log out of the MFA site when complete and close your browser window.

To update your settings, select the **Deloitte professionals** link on the DOL eRoom login page. On the MFA **Welcome** screen, you can:

- Update your authentication method
- Update the phone number associated with your MFA account
- Select a different language
- Activate the mobile app on another mobile device
- Update your security questions

Updating your authentication method

To change your authentication method go to **My Account** and select **Change Method**. On the **My Account: Change Method** screen, select your updated method and select **Save**.

Updating phone number

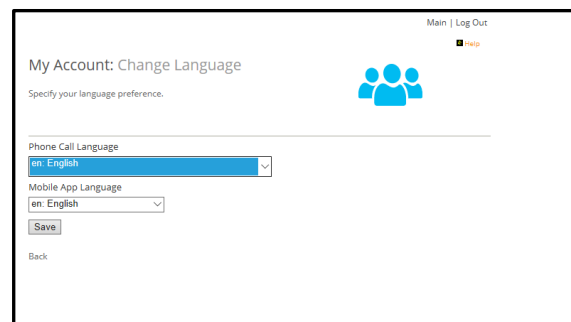
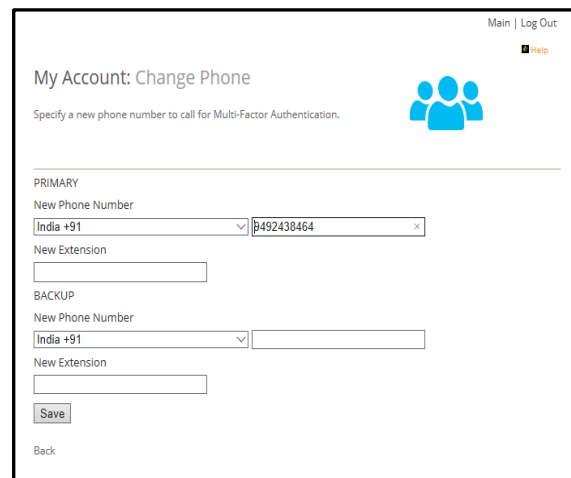
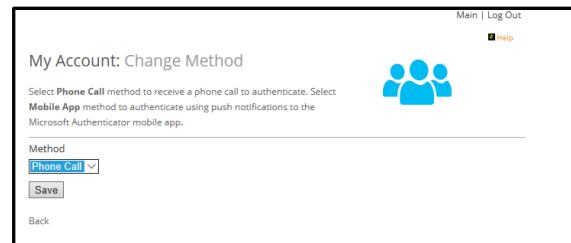
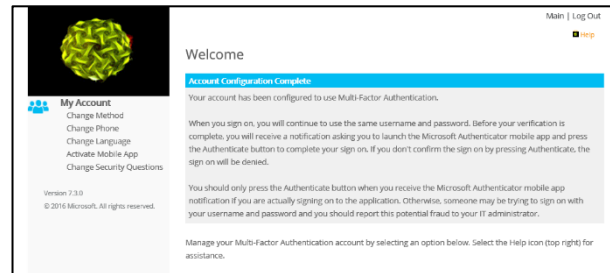
To update the phone number associated with your MFA account, go to **My Account** and select **Change Phone**. On the **My Account: Change Phone** screen, update the phone information and select **Save**.

Note: Updates to authentication methods may take up to 15 minutes to take effect.

Changing language

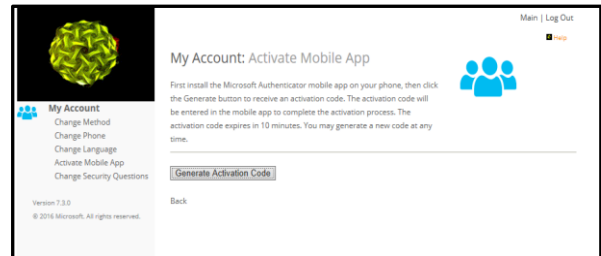
To update the language associated with your MFA account, go to **My Account** and select **Change Language**. On the **My Account: Change Language** screen, select the preferred language from the available options and select **Save**.

Note: Updates to languages may take up to 15 minutes to take effect. At this time, not all languages in the dropdown menu are available.



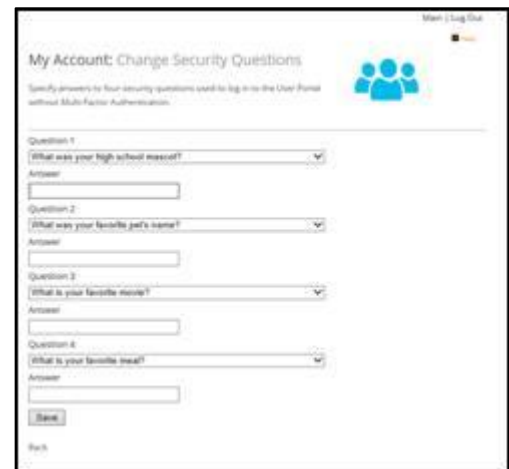
Activating mobile authenticator on another device

To activate the mobile authenticator on another device, select **Activate Mobile App** under **My Account**. Select **Generate Activation Code**. Within the Mobile Authentication app on your mobile device, scan the QR code on the computer screen. If you experience issues scanning the QR code, select **Or enter code manually** and enter the activation code and URL.



Updating security questions

To change the security questions associated with your MFA account, select **Change Security Questions** under **My Account**. On the **Security Questions** screen, select a question from the dropdown menu and provide your answer. All questions must be completed. Select **Save**.

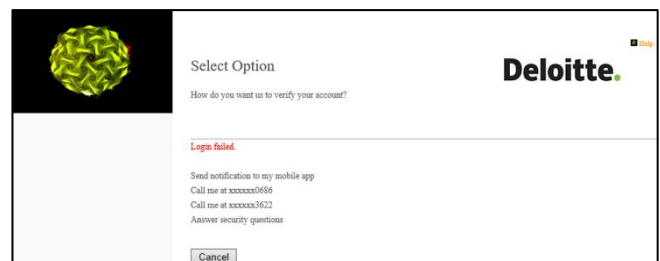


Authentication failure resolution

Mobile App method failure:

If you selected **Mobile App** as your primary method and it fails to authenticate, an error page will appear, and prompt you to use any of your backup methods to authenticate as shown here.

Upon successful verification, you will be directed to the eRoom landing page.



Phone Call method failure:

If you selected **Phone Call** as your primary method and do not have your primary phone

available, the MFA will attempt to reach you on the backup phone as specified in the enrollment process.

If the authentication fails, an error page will appear, and prompt you to answer the security questions created during MFA enrollment.



The screenshot shows a web page titled "Multi-Factor Authentication User Log In" with the Deloitte logo in the top right corner. On the left, there is a green, textured sphere icon. A red error message reads: "Multi-Factor Authentication denied. Please answer your security questions to log on." Below this message is a form with three text input fields. The first field is labeled "What was your high school mascot?", the second "What was your favorite pet's name?", and the third "What was your favorite teacher's name?". At the bottom of the form are two buttons: "Log In" and "Cancel".

Upon successful verification, you will be directed to the eRoom landing page.

Support

For any further questions or support, please open a ticket via [ServiceNow](#).

- **All users:** <https://deloitteglobal.service-now.com/sp>
- **US users:** 1 718 354 1250

This communication is for internal distribution and use only among personnel of Deloitte Touche Tohmatsu Limited, its member firms, and their related entities (collectively, the "Deloitte Network"). None of the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.