Multi-Factor Authentication (MFA)
Enrollment guide
December 2017
Table of Contents

What is MFA and how does it impact the way I sign into applications? 2
MFA Enrollment Log-in 3
Setup your preferred method of authentication 4
Mobile App option 5
Phone Call option 10
Security questions 11
Welcome page 12
Updating your MFA preferences 13
Authentication failure resolution 14
What is MFA and how does it impact the way I sign into applications?

Multi-Factor Authentication (MFA) is a new security process for Deloitte applications that provides an additional level of identity verification. It is a method of authentication that requires more than one verification method and adds a critical second layer of security to user sign-ins and transactions. Deloitte is enabling MFA for all client-facing applications.

Before using any of the Deloitte applications listed below, a one-time MFA enrollment is necessary.

- Agile Manager (AGM)
- Application Management - Process Manager (AM-PM)
- Application Lifecycle Management (ALM)
- IndustryPrint 5 (IP5)
- Octane
- Performance Center (PC)
- Project Management Center (PMC)
- SonarQube

NOTES:

- Access to all the applications listed above involves a single MFA enrollment process and related account. You may need to enroll in a separate MFA for other Deloitte applications (e.g. Deloitte Online).
- Until enrollment is completed, access will be denied to the above applications.
MFA Enrollment Log-in

1. From a web browser, enter https://consultingmfa.deloitte.com/portal/ to access the MFA enrollment portal and to reach the Multi-Factor Authentication User Login screen.

2. If you are directed to the following landing page:
   
   a. **Deloitte** users, click the **Deloitte professional**
   
   b. **Client** users, click **Client or business partner**, do NOT check **Select if this is your Deloitte laptop**

3. Enter your username and password and click **Log-in**
   
   a. **Deloitte** users, enter your Deloitte alias ID and password
   
   b. **Client** users, enter your email address and Deloitte password you use for tools listed above.
Setup your preferred method of authentication

You have the option to choose one of two options to verify MFA

- **Mobile App** – use an App on your mobile device to authenticate MFA. You receive a notification on your mobile device and confirm MFA by clicking Approve.
- **Phone Call** – receive a phone call at a primary number, answer the call and confirm MFA by entering ‘#’.

Perform the following steps to choose which option you prefer:

1. Use the drop-down to select your preferred method of authentication. Available options include **Phone Call** (default selection) or **Mobile App**.

2. If you chose **Mobile App** proceed to the next section for further detailed instructions to complete registration.

3. If you chose **Phone Call** proceed to the **Phone Call option** section to complete registration.
Mobile App option

If you chose Mobile App in Setup your preferred method of authentication, perform the following steps to complete registration.

1. From your mobile device, search and download the Microsoft Authenticator mobile app from the (i) App Store®, Microsoft Store, or (ii) on Google Play. If already installed, go to step 2.

NOTE: If your mobile device is unable to download the Microsoft Authenticator app, please use the Phone Call option.
2. Once the Authenticator app is installed, open it. Click the ‘➕’ icon to add a new account.

3. Select **Work or school account**
4. From the MFA portal website, click **Generate Activation Code** on the MFA enrollment page to continue.

6. You can authenticate using one of the two options below:

<table>
<thead>
<tr>
<th><strong>Option 1: Scan QR code (Preferred):</strong></th>
<th><strong>Option 2: Enter manually</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the camera on your mobile device, scan the QR code to complete the enrollment and synchronization of the mobile app. If you are asked to allow the Microsoft Authenticator app to access your camera, tap <strong>Allow</strong>.</td>
<td>Enter the <strong>URL</strong> and <strong>Activation Code</strong> in the fields highlighted below and tap <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>

**NOTE:** If the QR code expires before you are able to scan, you can click the **Generate New Activation Code** button to generate a new one. There is no need to refresh the page.
7. From your mobile device, you should now see a new account named **Deloitte Project Delivery Solutions** in the Authenticator app.

![Authenticator App](image.png)

**NOTE: Deloitte users only** – Since this MFA account only allows Mobile Device App or Phone Call MFA verification, you will not see the 6-digit code under the account name like you do with the account you use to access VPN, DeloitteNet and DeloitteOnline.

8. From the MFA portal website, click **Authenticate Me Now**.

![MFA Portal Website](image.png)

9. From your mobile device **Authenticator App**, click **Approve**.

![Approve Sign-in](image.png)

10. Proceed to the **Security Questions** section to complete registration.
Phone Call option

If you choose the Phone Call option:

1. From the MFA portal website, for your PRIMARY and BACKUP phone numbers perform the following steps:
   a. Select your Country Code from the drop down box under Phone
   b. Enter the phone number (minus the country code) in the field to the right

2. Click Call Me Now to Authenticate.

3. You will receive a phone call at the primary number entered and be asked to tap “#” to authenticate.

4. Answer the call and press # to authenticate.

5. After authenticating, proceed to the Security Questions section to complete registration.

NOTE: It is highly recommended you include a Backup number. In the event you cannot respond to your Primary number (e.g., lost mobile device), the MFA system will attempt to call you at your Backup number to authenticate. If you do not have a Backup number, you will need to answer your security questions to authenticate. See the Authentication failure resolution section for more information.
Security questions

After selecting your preferred method of authentication, you will update your security questions on the Security Questions page. The security questions are used in the event you are unable to authenticate via your preferred authentication method (e.g., your mobile device is unavailable).

1. Enter the answer to all five security questions. You can select the down arrow for each question to choose a different question.

2. Once complete answering all five questions, click Continue

3. You will be directed to the Welcome page on the MFA website.

MFA registration is now complete!
Welcome page

After successfully enrolling in MFA, you will be directed to the Welcome page where you can update your preferences and review the MFA FAQs.

You can now access the applications via the URL you normally use and log in.

When you log in, you will be required to authenticate via the MFA method you selected.
Updating your MFA preferences

To update your MFA preferences, navigate to the MFA enrollment portal. After authenticating, you will be directed to the Welcome page and will be able to change your authentication method, update your phone number, change the language used in the MFA portal, activate the mobile app (as shown in the Mobile App option section), or change your security questions.

**Change authentication method**

**Change phone number**

**Change language**

**Change security questions**
Authentication failure resolution

If you are unable to authenticate to your application via MFA (e.g., you don’t have access
to your mobile device and cannot be reached at your backup number if you use the phone
call option), perform the following steps to update your authentication method:

1. Access the MFA enrollment portal and log in with your credentials.

2. Upon authentication failure (this could take up to a minute or two), you will be
prompted to answer your security questions to log-in and change your settings.

3. Answer all security questions and click Log In

4. If you do not remember your security question answers and/or unable to log in, please
contact MFA Support for assistance.