



Frequently Asked Questions

Contents

1. What is multi-factor authentication, and how does it impact the way I sign into my account or applications?	2
2. What are the benefits of MFA?	2
3. Who is required to enroll in MFA?	3
4. How do I enroll in MFA?	3
5. Do we enforce MFA for external client logins as well?	3
6. How do I authenticate using MFA?	3
7. What authentication options do I have?	3
8. In which situations will I be required to authenticate through MFA?	4
9. How do I change my preferred MFA authentication method?	4
10. Will I be required to authenticate each time I log-on to an MFA-enabled CMT application?	4
11. Does MFA replace my Deloitte password?	4
12. Does having MFA mean that I will no longer need to change my password?	4
13. If I need assistance with MFA-related matters, who can I talk to?	4
14. What call-back languages are supported when using Voice Call MFA authentication?	5
15. How can I determine if I am configured for MFA (I can't remember)?	5
16. What if I change my mobile device, used for MFA authentication, do I need to reconfigure or update my MFA Profile?	5
17. Why would a user receive a Multi-Factor Authentication call from an anonymous caller when using caller ID?	5
18. What options are available to complete MFA process if I cannot get to authentication request fast enough (~60 seconds)?	6
19. What languages are supported in Azure MFA Profile Page?	6

1. What is multi-factor authentication, and how does it impact the way I sign into my account or applications?

Multi-factor authentication (MFA) is a new security process for Deloitte applications to provide an additional level of identity verification. Two-step identity verification 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 MFA to access any of the Consulting Methods & Tools (CMT) applications listed below, a one-time enrollment is necessary.

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

When enrolling, you will select your MFA authentication method. Until enrollment is completed, access will be denied on applications enabled to require a second authentication factor through MFA.

Note:

- If you access multiple Deloitte CMT applications, you will only need to go through the enrollment process once. After successfully enrolling, you will be able to access any Deloitte CMT application for which you are authorized that has been enabled for MFA. However, you may need to enroll in MFA more than once if you access any other Deloitte applications that use an alternative MFA solution.

You will be able to use your mobile device to enroll in and authenticate to MFA.

2. What are the benefits of MFA?

Deloitte is increasing its focus on information and network security, and MFA is a technology proven to be a successful measure in helping to prevent against the evolving landscape of cyber security threats such as network breaches, hacking, and credentials compromise.

3. Who is required to enroll in MFA?

All Deloitte employees, Deloitte contractors, and client personal must enroll in MFA when communicated to do so. If you choose not to enroll in MFA, you will not have access to the following MFA-enabled CMT applications post MFA rollout:

- Agile Manager (AGM)
- Application Management - Process Manager (AM-PM)
- Application Lifecycle Management (ALM)
- Deloitte Online (DOL)
- Deloitte System Access (DSA)
- IndustryPrint 5 (IP5)
- Octane
- Performance Center (PC)
- Project Management Center (PMC)
- SonarQube

4. How do I enroll in MFA?

To enroll in MFA, go to [Deloitte MFA Profile website](#) and enter your Deloitte credentials to login. Post login, you will be prompted to setup your MFA Profile.

5. Do we enforce MFA for external client logins as well?

Yes. Any application that is accessed by clients is deemed high risk (as it is also presumably Internet facing). As a result, such apps will need to have MFA enabled by December 31, 2017.

6. How do I authenticate using MFA?

When accessing an MFA-enabled application, you will be prompted for your user id and password as usual, and then you receive a second prompt to further verify your identity through the preferred authentication method (phone call, mobile app or text message (available only in certain cases)) selected during the MFA enrollment process. Upon successful verification, you will be able to access the MFA-enabled application.

7. What authentication options do I have?

The following options are available to authenticate using MFA:

Option #	Option Description	Device Required
1	Notify me through app (must first download the <i>Microsoft Authenticator</i> app through your phone's app store)	Mobile
2	Call my authentication phone	Mobile
3	Text my authentication phone (only available for DPASS MFA)	Mobile

You are able to select one of the above options as your preferred method to authenticate.

8. In which situations will I be required to authenticate through MFA?

Once an application becomes MFA-enabled, you will be required to authenticate through MFA to access and use the application. Once you are authenticated through MFA, you can access any of the MFA enabled CMT tools you are authorized to use without authenticating through MFA again for 8 hours.

9. How do I change my preferred MFA authentication method?

You can change your preferred settings, such as your preferred authentication method or your registered phone number through the [Deloitte MFA Profile website](#).

10. Will I be required to authenticate each time I log-on to an MFA-enabled CMT application?

All the MFA enabled CMT applications will require MFA authentication, with each authentication session lasting 8-hours*, in which you will not be asked to authenticate again during the 8-hour timeframe.

11. Does MFA replace my Deloitte password?

No, your Deloitte password is your first factor of authentication when logging into all Deloitte applications, and MFA provides the second factor of authentication when logging into web-based applications.

12. Does having MFA mean that I will no longer need to change my password?

No, you will still have to change your password every 84 days. MFA is an additional security measure in addition to having a strong password that is frequently reset. These multiple layers of security will provide extra protection against potential cyber security threats.

13. If I need assistance with MFA-related matters, who can I talk to?

If you are experiencing issues with MFA enrollment or authentication, try closing out the browser and clearing your web browser's cookies and cache. If your issue is still not resolved, and you need immediate assistance, please contact [CMT support](#).

14. **What call-back languages are supported when using Voice Call MFA authentication?**

Deloitte has configured English as the language for telephone call MFA authentication.

15. **How can I determine if I am configured for MFA (I can't remember)?**

By browsing to the [Deloitte MFA Profile website](#) the service will prompt for your Deloitte credentials and once completed, you will either be prompted to setup your MFA Profile or show your MFA profile (already configured), with configurations options that can be managed/changed as needed.

16. **What if I change my mobile device, used for MFA authentication, do I need to reconfigure or update my MFA Profile?**

Possibly depending on which MFA authentication type you have selected during configuration:

- **Same Phone Number:** If your MFA profile is configured to Call/Text a phone number and the device has changed but the number remains the same, then no changes are needed.
- **Azure Authenticator Application:** If using this authentication option, then your MFA Profile must be updated (Configure Azure Authenticator App), as devices are 'linked' to devices and any device change requires you to go through the Authenticator Application setup/configuration, which will remove the 'service connection' with your old device and be configured for use with your new device. To reconfigure, visit [Deloitte MFA Profile website](#), sign-in with your Deloitte account and click the Configure option and walk through the steps to setup your new device and Authenticator application.

17. **Why would a user receive a Multi-Factor Authentication call from an anonymous caller when using caller ID?**

When Multi-Factor Authentication calls are placed through the public telephone network, sometimes they are routed through a carrier that doesn't support caller ID. Because of this, caller ID is not guaranteed, even though the Multi-Factor Authentication system always sends it.

18. What options are available to complete MFA process if I cannot get to authentication request fast enough (~60 seconds)?

When accessing an MFA secured application, the requestor has **~60 seconds to respond to the MFA request before timing out**. If someone is not able to respond within this time, the following options are available to get through the MFA process:

Web Browser

- Use a different verification option
 - **Note:** This option requires the user to have already configured a secondary authentication option (Authenticator, Mobile Device <Phone Call/Text>, etc.).
- Click the URL in the browser window and hit <Enter> or refresh the webpage, which will force MFA to resend an authentication requires to the user, who can then respond.
- If neither option works, you will need to close your browser and retry access, which should force MFA to send another authentication request.

19. What languages are supported in Azure MFA Profile Page?

Afrikaans - South Africa	Danish – Denmark	Greek - Greece	Slovenian - Slovenia
Albanian - Albania	Dhivehi - Maldives	Gujarati - India	Spanish - Argentina
Arabic - Algeria	Dutch - Belgium	Hebrew - Israel	Spanish - Bolivia
Arabic - Bahrain	Dutch - The Netherlands	Hindi - India	Spanish - Chile
Arabic - Egypt	English - Australia	Hungarian - Hungary	Spanish - Colombia
Arabic - Iraq	English - Belize	Icelandic - Iceland	Spanish - Costa Rica
Arabic - Jordan	English - Canada	Indonesian - Indonesia	Spanish - Dominican Republic
Arabic - Kuwait	English - Caribbean	Italian - Italy	Spanish - Ecuador
Arabic - Lebanon	English - Ireland	Italian - Switzerland	Spanish - El Salvador
Arabic - Libya	English - Jamaica	Japanese - Japan	Spanish - Guatemala
Arabic - Morocco	English - New Zealand	Kannada - India	Spanish - Honduras
Arabic - Oman	English - Philippines	Kazakh - Kazakhstan	Spanish - Mexico
Arabic - Qatar	English - South Africa	Konkani - India	Spanish - Nicaragua
Arabic - Saudi Arabia	English - Trinidad and Tobago	Korean - Korea	Spanish - Panama
Arabic - Syria	English – United Kingdom	Kyrgyz - Kazakhstan	Spanish - Paraguay
Arabic - Tunisia	English - United States	Latvian - Latvia	Spanish - Peru

Arabic - United Arab Emirates	English - Zimbabwe	Lithuanian - Lithuania	Spanish - Puerto Rico
Arabic - Yemen	Estonian - Estonia	Macedonian (FYROM)	Spanish - Spain
Armenian - Armenia	Faroese - Faroe Islands	Malay - Brunei	Spanish - Uruguay
Azeri (Cyrillic) - Azerbaijan	Farsi - Iran	Malay - Malaysia	Spanish - Venezuela
Azeri (Latin) - Azerbaijan	Finnish - Finland	Marathi - India	Swahili - Kenya
Basque - Basque	French - Belgium	Mongolian - Mongolia	Swedish - Finland
Belarusian - Belarus	French - Canada	Norwegian (Bokmål) - Norway	Swedish - Sweden
Bulgarian - Bulgaria	French - France	Norwegian (Nynorsk) - Norway	Syriac - Syria
Catalan - Catalan	French - Luxembourg	Polish - Poland	Tamil - India
Chinese - China	French - Monaco	Portuguese - Brazil	Tatar - Russia
Chinese - Hong Kong SAR	French - Switzerland	Portuguese - Portugal	Telugu - India
Chinese - Macau SAR	Galician - Galician	Punjabi - India	Thai - Thailand
Chinese - Singapore	Georgian - Georgia	Romanian - Romania	Turkish - Turkey
Chinese - Taiwan	German - Austria	Russian - Russia	Ukrainian - Ukraine
Chinese (Simplified)	German - Germany	Sanskrit - India	Urdu - Pakistan
Chinese (Traditional)	German - Liechtenstein	Serbian (Cyrillic) - Serbia	Uzbek (Cyrillic) - Uzbekistan
Croatian - Croatia	German - Luxembourg	Serbian (Latin) - Serbia	Uzbek (Latin) - Uzbekistan
Czech - Czech Republic	German - Switzerland	Slovak - Slovakia	