GSD. General - How to Set-Up Multi-Factor Authentication Method

Article ID: KB0039739
Created: 2024-12-19 14:03:31
Updated: 2024-12-19 14:03:31
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/acaf843397d74958f7e3bb8fe153afe3', 'value': 'acaf843397d74958f7e3bb8fe153afe3'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/a9925c08c38a1a100acd3300150131f8', 'value': 'a9925c08c38a1a100acd3300150131f8'}

General Information:

Possible symptoms/errors:

User wants to Set-Up their Multi-Factor Authentication Method.

Alternative names of the system:

MFA

IMPORTANT NOTICE:

N/A

Solution:

Multi-factor authentication is an authentication method that requires the use of more than one verification method and adds a second layer of security to user sign-ins and transactions. The following process provides instructions how to setup multi-factor authentication.

Note: Once user has chosen their authentication method, this will be used automatically each time they are accessing O365 outside the office. Advise the user to set up two different MFA channels for themselves to have a back-up in case one of their devices gets lost. User can choose which of these options they want to use as default. Details:

1) Advise the user to go to https://aka.ms/mfasetup

2) Guide the user to logon with their Fresenius corporate email address

2b) If the user is performing these steps while connected to the Fresenius network, an additional prompt will ask for the user’s Windows credentials. If so, advise the user to login with DOMAIN\Username.

If the user receives the following error message at this point, that the account is locked out and unable to configure MFA from outside the corporate network. This can be solved by either

Connecting to the Fresenius Global Network via VPN. This counts as a valid second factor for authentication to AzureIf the user has access via Fresenius VPN to our global network, he/she can continue with this guide after connecting.Requesting the user to add mobile phone number to their AAD account to enable MFA by SMSThe user needs to get in touch with his/her Fresenius internal counterpart (Onboarder) to provide them with the mobile phone number. They can open a ticket with the support groupto get their account updated. Please be aware that for compliance reasons this ticket must be opened by a Fresenius employee.Once this is complete, SMS will be automatically used for MFA at your next logon. You still can configure additional MFA options via the link above.

2) The user will be prompted to set up MFA. NOTE: While the user may skip this step for up to 14 days, it is recommend to set up MFA as soon as possibleto prevent being locked out of the service

3) In order to setup authentication with Microsoft Authenticator app, click next button.Otherwise click on "I want to set up a different method" at the bottom. Follow the appropriate section in this guide to continue.

Setup the Microsoft Authenticator app

To set up the Microsoft Authenticator app select the appropriate option on the Microsoft website. This will lead the user to a page that presents a QR code that the user will have to scan with the app

For the next step, request the user to download the app from the app store from their mobile device. Make sure that they install the original Microsoft app, as there are many third party authenticator apps that cannot be used for this MFA method.

1) Download the Microsoft Authenticator App

2) Add a new account

3) Select "Work or school account" and choose"Scan QR code". Scan the code from theMicrosoft website with the camera.

4) Account is registered successfully

After the user has registered their account in the Microsoft Authenticator app, the Microsoft website will trigger one MFA prompt. Guide the user to approve this request on their device to complete the MFA setup.

Setup another Authenticator app

If the user is unable to use the Microsoft Authenticator app, they may use another app that provides support for time-based verification codes. To set this up, please click on the "I want to use a different authenticator app" link during the MFA setup. This will generate a QR code that the user can scan with your app. If the app does not support scanning of QR codes, please click on the "Can't scan image?" button to show the account name and secret key that the user will have to enter manually into your authenticator app.

For the next step, advise the user install the authenticator app on the user’s mobile device.

1) Download the authenticator app

2) Either scan the QR code or select"Enter a setup key" to set up manually

3) Enter the account details from theMicrosoft website

4) The account is added and a time-basedverification code is displayed

Enter the current verification code from the authenticator app on the Microsoft website to complete the MFA setup.

Setup SMS

If the user cannot use the Microsoft Authenticator or another MFA app he/she may also configure the service to send you an SMS with an one time code(OTP). To set up this option please click on the "I want to set up a different method" link during MFA setup and choose the "Phone" option.

On the next dialog enter the (mobile) phone number and select the "Text me a code" checkbox.

The user will receive a SMS with an one-time verification code. Enter this code on the Microsoft website to complete the setup.

Setup Phone call

The user may also configure the service to call with an one time code. To set up this option please click on the "I want to set up a different method" link during MFA setup and choose the "Phone" option.

On the next dialog enter the (mobile) phone number and select the "Call me" checkbox.

The user will receive a phone call that he/she must approve with the dial-tone enabled (mobile) phone. After the user have done so, MFA configuration is complete.

Change Azure MFA options

If the user wants to change your Azure MFA options he/she can do so anytime via the https://aka.ms/MFASetup Microsoft account website.

NOTE: System-preferred multifactor authentication (MFA) has been implemented which prompts users to sign in by using the most secure method they registered.

For example, if a user registered both SMS and Microsoft Authenticator push notifications as methods for MFA, system-preferred MFA prompts the user tosign in by using the more secure push notification method. The user can still choose to sign in by using another method, but they're first prompted to try themost secure method they registered.

How does system-preferred MFA determine the most secure method?

When a user signs in, the authentication process checks which authentication methods are registered for the user. The user is prompted to sign-in with themost secure method according to the following order. The order of authentication methods is dynamic. It's updated as the security landscape changes, andas better authentication methods emerge.

1. Temporary Access Pass2. Certificate-based authentication3. FIDO2 security key4. Microsoft Authenticator push n...