How to set up Multi-Factor Authentication Methods?

Article ID: KB0039491
Created: 2024-12-19 14:01:54
Updated: 2024-12-19 14:01:54
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/8c16c448c3821a100acd3300150131c4', 'value': '8c16c448c3821a100acd3300150131c4'}

This article provides an overview of the Multi-Factor Authentication (MFA) methods available at Fresenius and guidance on how to set them up. MFA protects an account by requiring individuals to present multiple forms of identification, such as a password and a verification prompt sent to a second device, before gaining access to an account or system.

Please set up two different MFA methods to have a backup in case one of your devices is lost. One of them should be a MFA method that provide a high level of security (the Microsoft Authenticator app or One Time Password (OTP) Manager). The most secure authentication method will be used automatically each time you are accessing Microsoft 365 applications outside the office.

1. Set up one of the two strong MFA methods

Choose one of the two MFA options available at Fresenius that provide a high level of security: the Microsoft Authenticator or the OTP Manager.

Option 1: The Microsoft Authenticator

The Microsoft Authenticator must be installed on a mobile phone or tablet and stands out as secure and convenient MFA option because it provides #Passwordless login to many applications that use your Windows password and enables you to use the Self Service Password Reset (SSPR).

Check this ServiceNow Knowledge Article on how to set up the Microsoft Authenticator: https://fnc.service-now.com/sp?id=kb_article_view&sysparm;_article=KB0016999

Note: Find out which applications currently allow #passwordless login here. The list will continue to grow.

Option 2: The OTP Manager

The OTP Manager must be installed on your Fresenius computer. It requires you to enter both, your password and a 6 digit code generated by the OTP Manager to login.

Check this ServiceNow Knowledge Article on how to set up the OTP Manager: https://fnc.service-now.com/sp?id=kb_article_view&sysparm;_article=KB0017268

2. Set up a backup MFA method

After setting up one of the two strong MFA methods, it is recommended to set up a second MFA method as backup in case one of your devices gets lost. SMS, voice call or email verification is recommended as second MFA method.

2.1 Add a sign-in method to your Microsoft Account

2.1.1 Go to the Microsoft Security Information page: My Sign-Ins | Security Info | Microsoft.com

2.1.2 Click on "Add sign-in method".

The next step is to set up one of the following 3 MFA methods as backup.

Option 1: SMS

2.2 SMS as MFA method requires a phone number (business or private) to approve a login attempt after the password was entered. You will receive a unique code via SMS when you attempt to log in to your account after entering your password.

2.2.1 After you have completed step 2.1 as described above, select "Phone" from the drop-down menu. Click on "Add".

2.2.2 Select your phone number area code in the drop down menu and enter your phone number. Select "Receive a code". Then click on "Next".

2.2.3 Enter the 6-digit code you received by SMS on your mobile device and click on "Next".

The SMS MFA method has been set up successfully.

Option 2: Voice Call

2.3 Voice Call as MFA method requires a phone number (business or private) to approve a login attempt after the password was entered. You will receive a unique code via an automated voice call when you attempt to log in to your account after entering your password.

2.3.1 After you have completed step 2.1 as described above, select "Phone" from the drop-down menu. Click on "Add".

2.3.2 Select your phone number area code in the drop down menu and enter your phone number. Select "Call me". Then click on "Next".

2.3.3 You will be called on your mobile device, please follow the instructions. Click on "#" on your mobile device.

The voice call MFA method has been set up successfully.

Option 3: Email

2.4 Email as MFA method requires a email address to approve a login attempt after the password was entered. You will receive a unique code via email when you attempt to log in to your account after entering your password.

2.4.1 After you have completed step 2.1 as described above, select "Email" from the drop-down menu. Click on "Add".

2.4.2 Enter an email address which will be used for authentication. Then click on "Next".

Note: The email address must be different from the current account email address.

2.4.3 Enter the 6-digit code that was sent to your email address and click on "Next".

The email MFA method has been set up successfully.

Data Protection Notice

It is your choice to use your business or private contact details (mobile phone number and email address) for configuring MFA. If you voluntarily decide to enter your private contact details, you give your consent to Fresenius allowing the use of these personal data for the MFA process.

You can withdraw your consent at any time and remove your private details here. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

For further information, please refer to the data protection notice for employees. If you have any questions regarding the processing of your personal data, please contact dataprotection@fresenius.com.