Assignment

Configuring Organizational Settings

*Task*

*At the organization level, select at least three authentication methods and define that at least two are required to reset. Explain the choice of authentication method.*

*Submit the task in Word with screenshots.*

*View multimedia with Module 4.*

Course: Microsoft 365 Messaging

Module: Managing a Microsoft 365 messaging environment

Student: Jovan Ljušić

CONTENT

[SELECTION OF AUTHENTICATION METHODS 2](#_Toc178043476)

# SELECTION OF AUTHENTICATION METHODS

This document presents a step-by-step approach to solving a specific task, outlining the methodology, execution, and expected outcomes. By following the instructions, the reader will gain hands-on experience in applying technical concepts to practical situations, reinforcing both theoretical knowledge and problem-solving abilities.

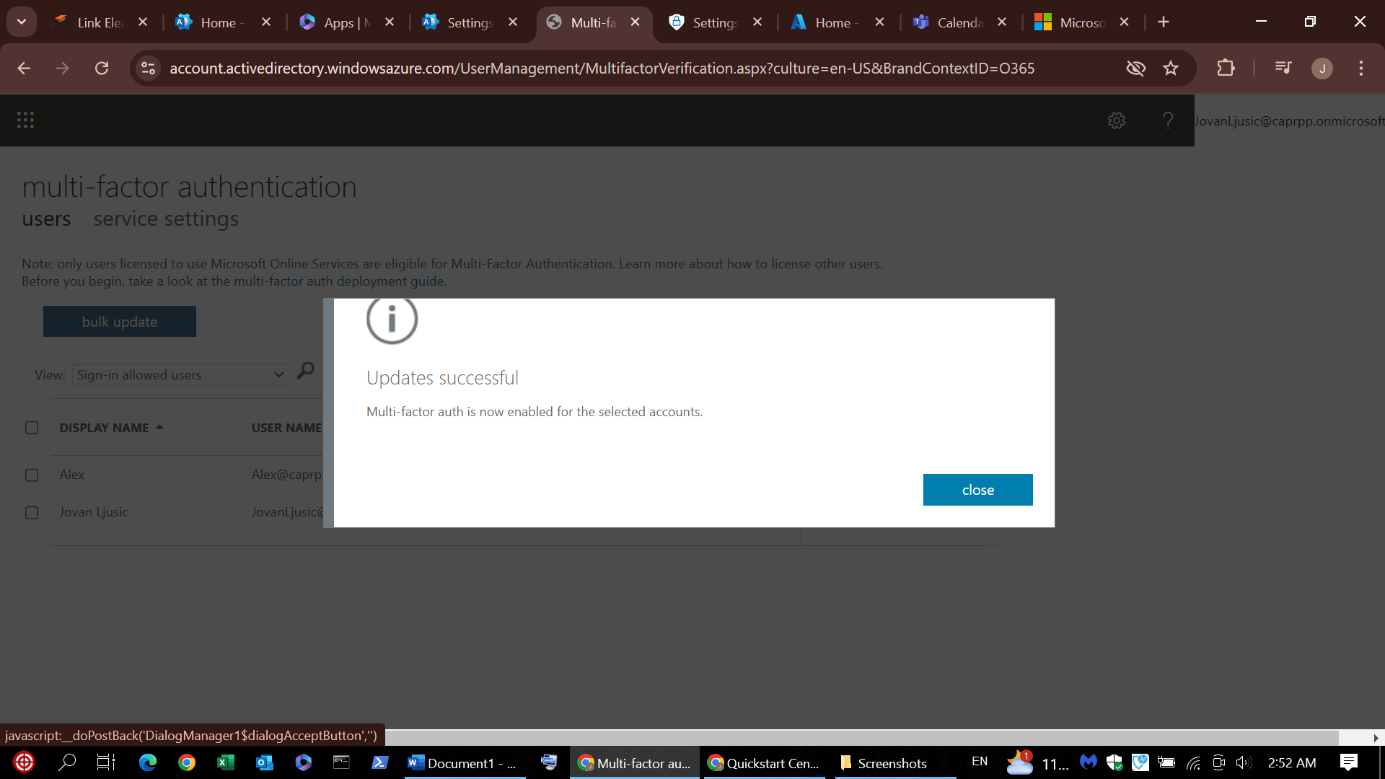
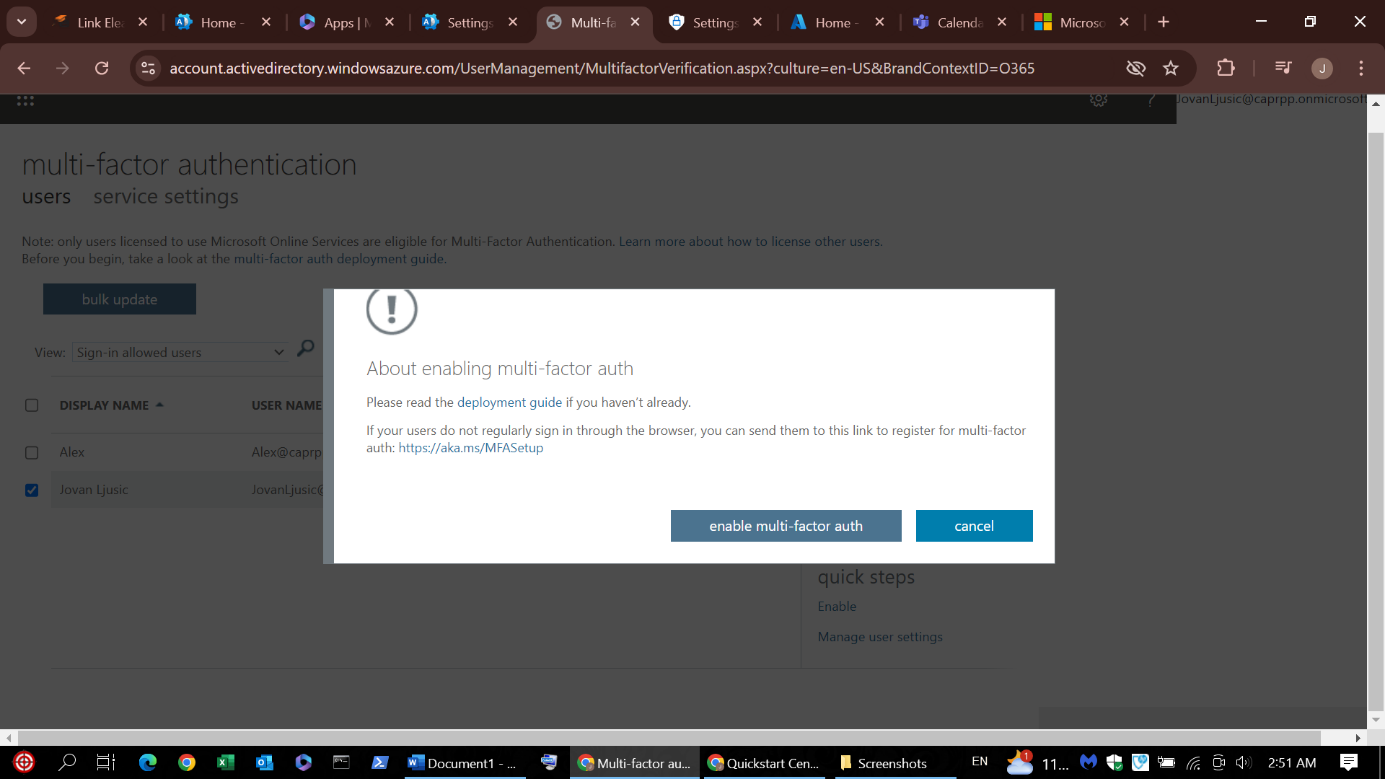
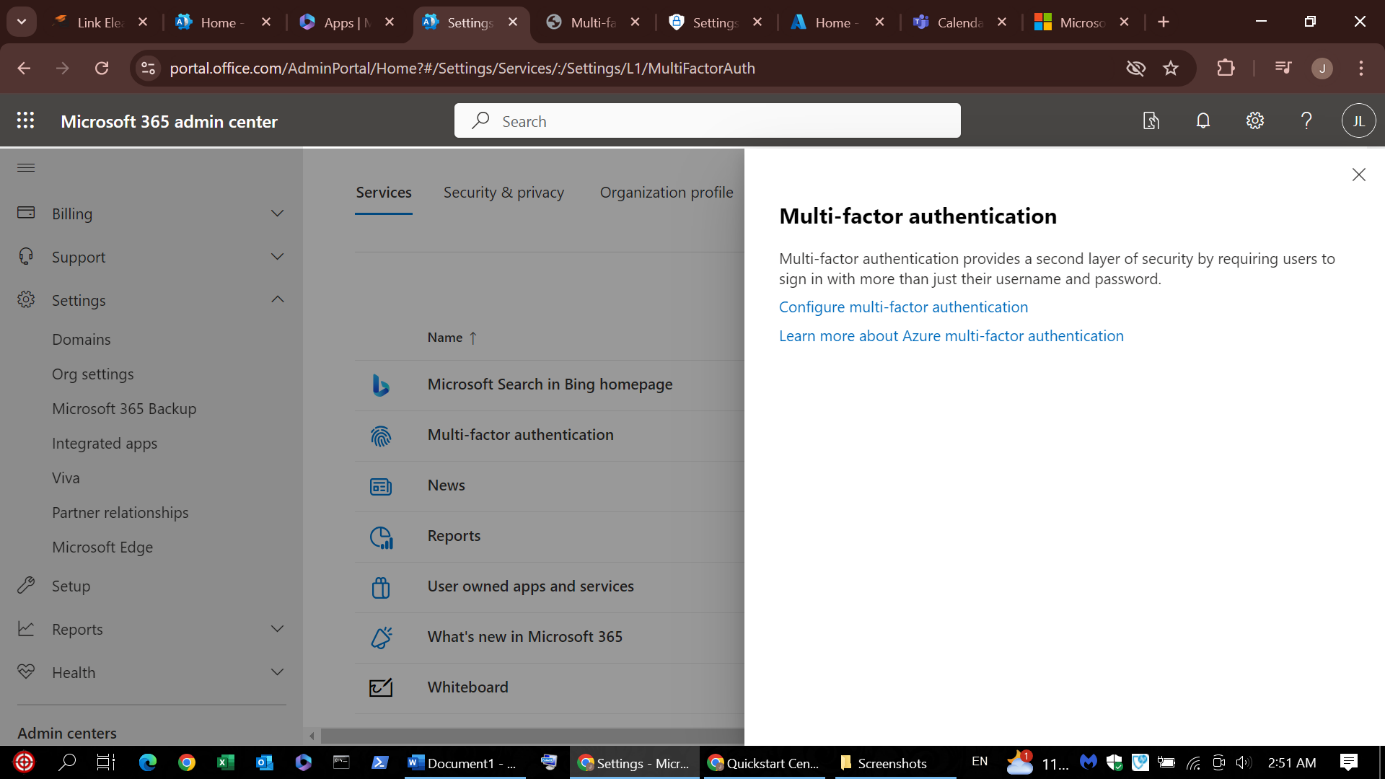
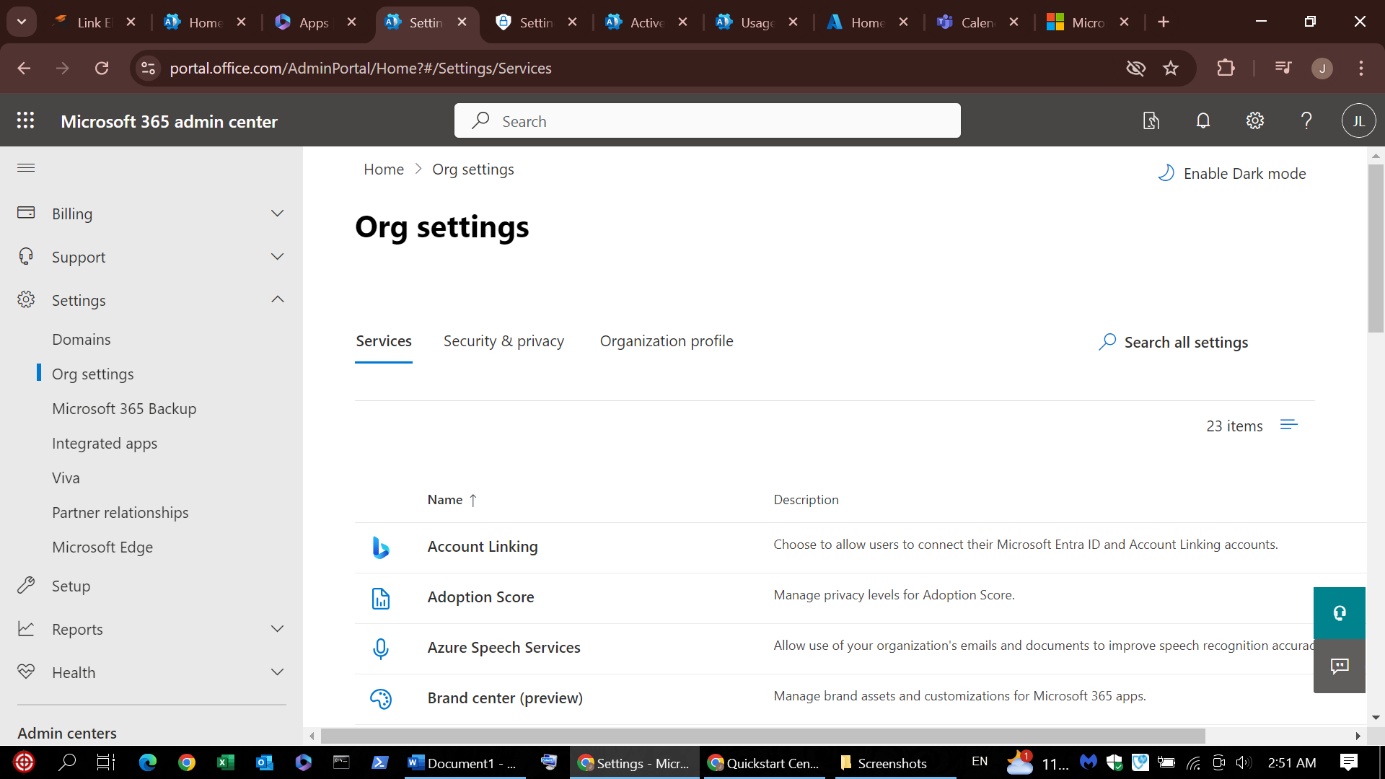
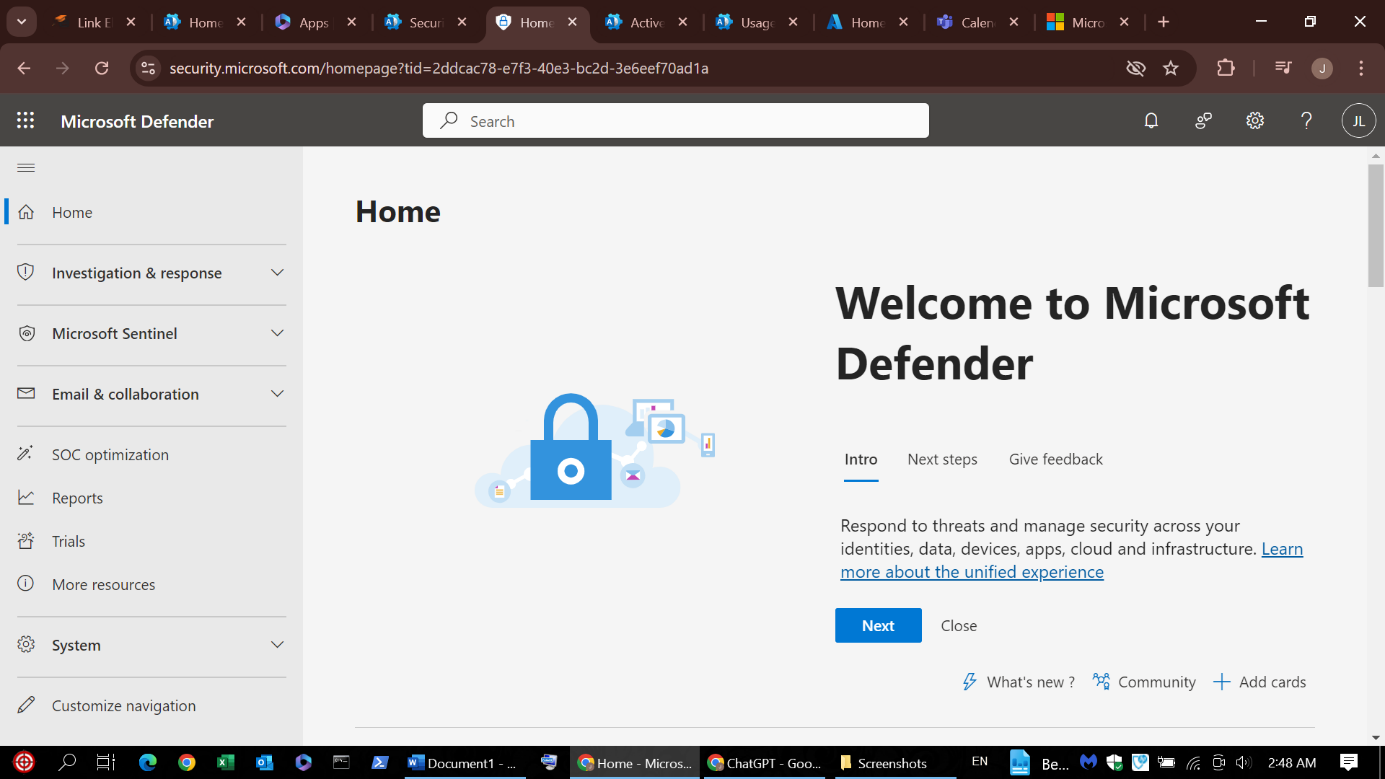
The structured approach ensures that each step is clearly defined, making the process easy to follow and implement in professional environments.

Through this approach, several methods will be shown, including textual and visual access using a screenshot:

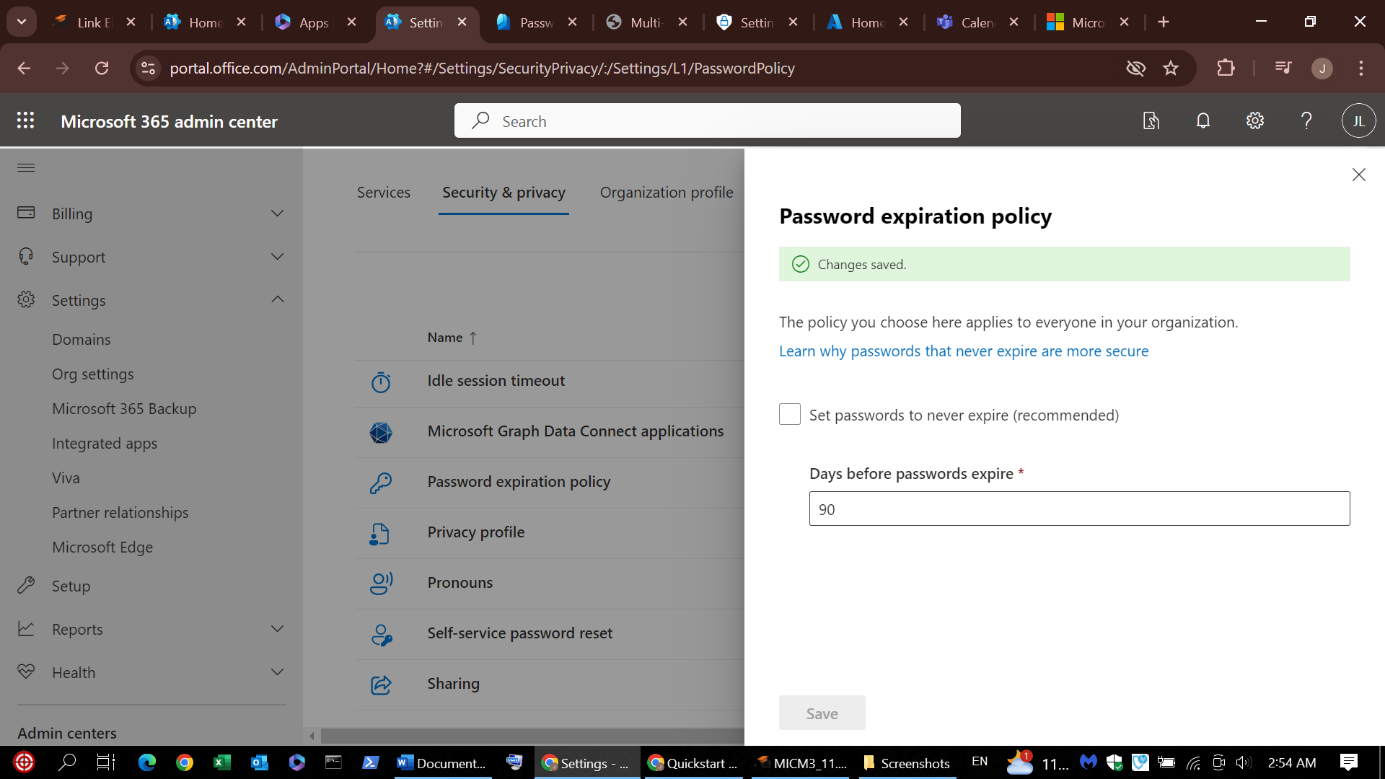
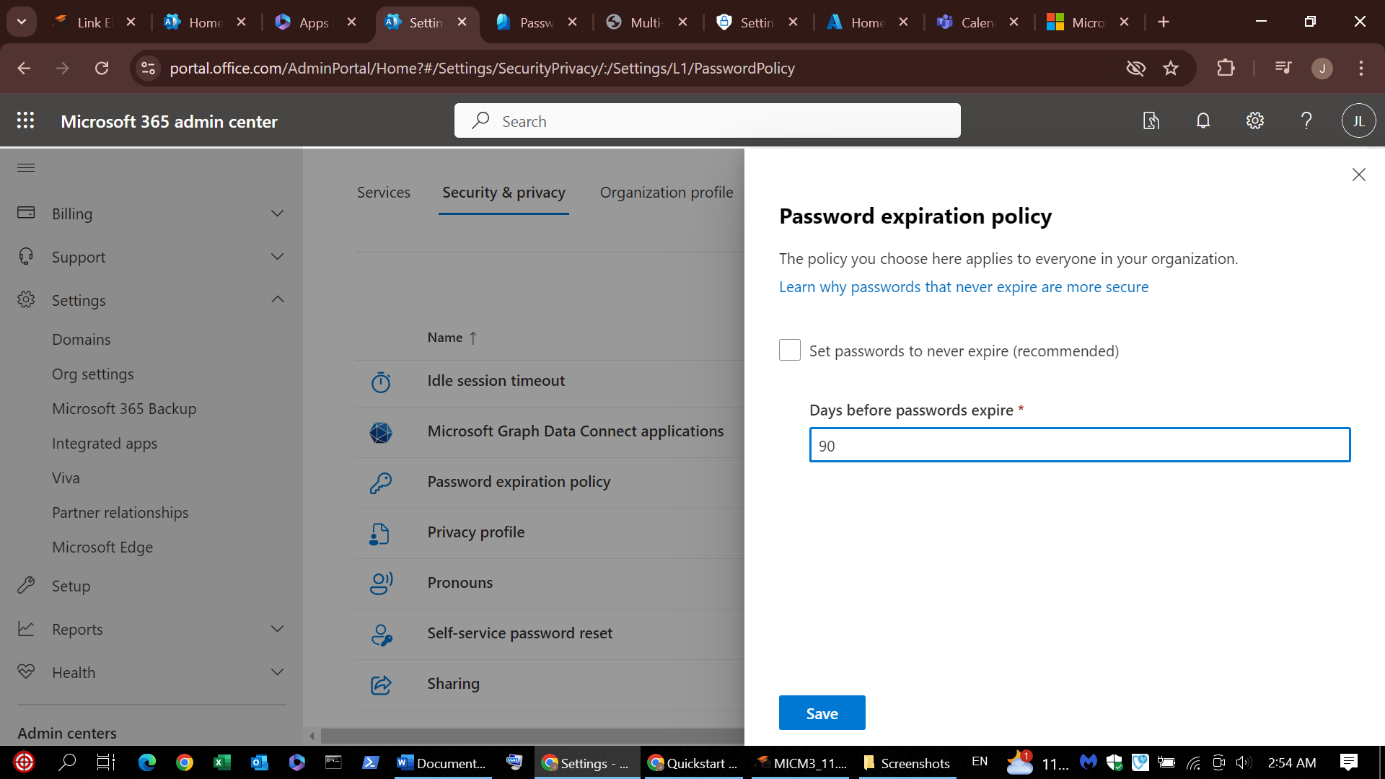
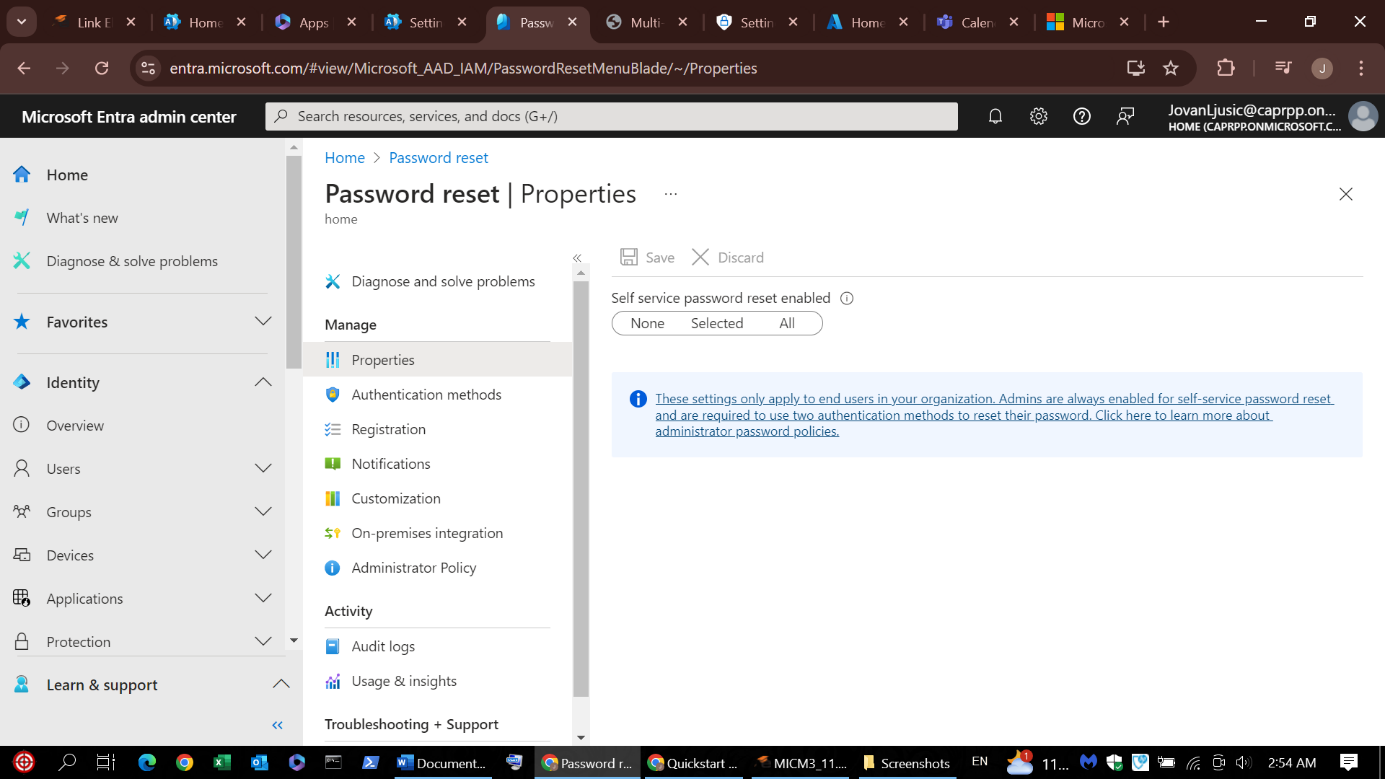
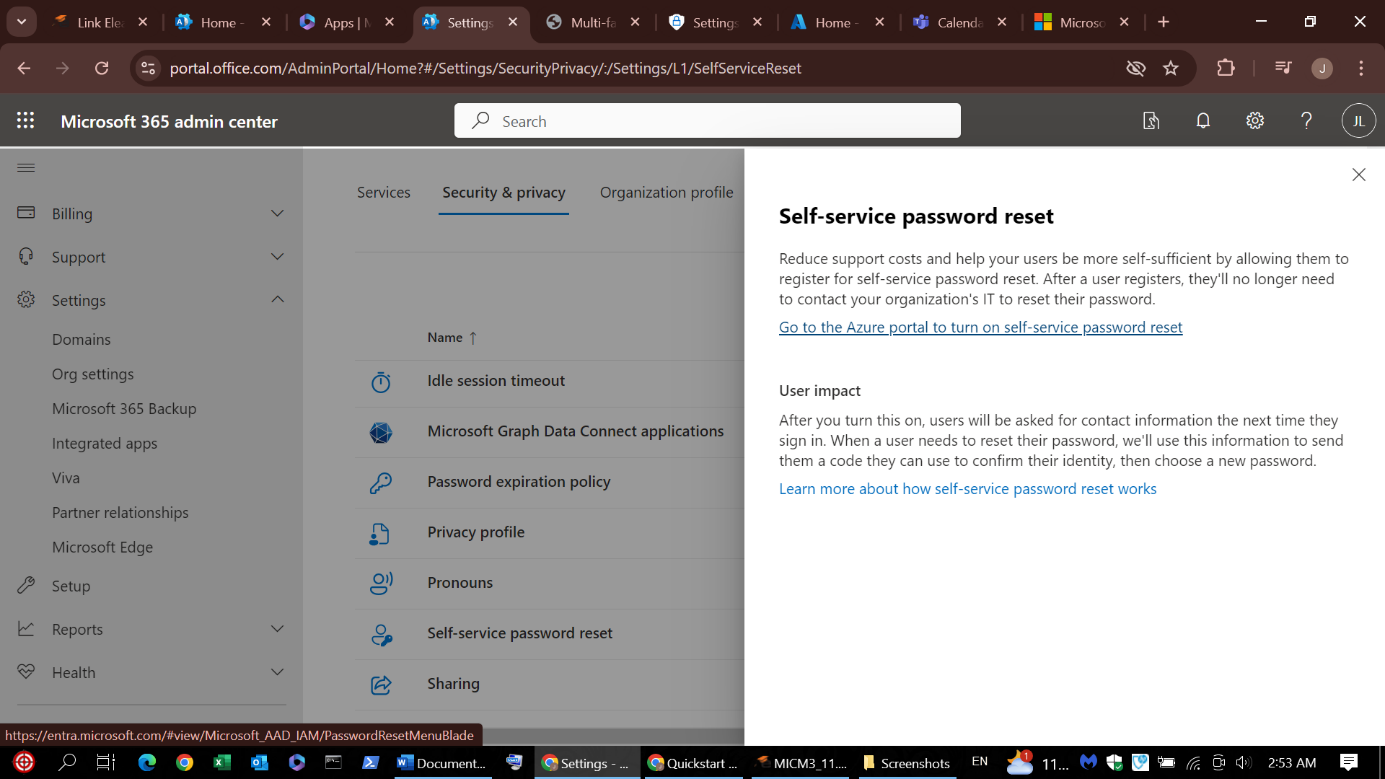
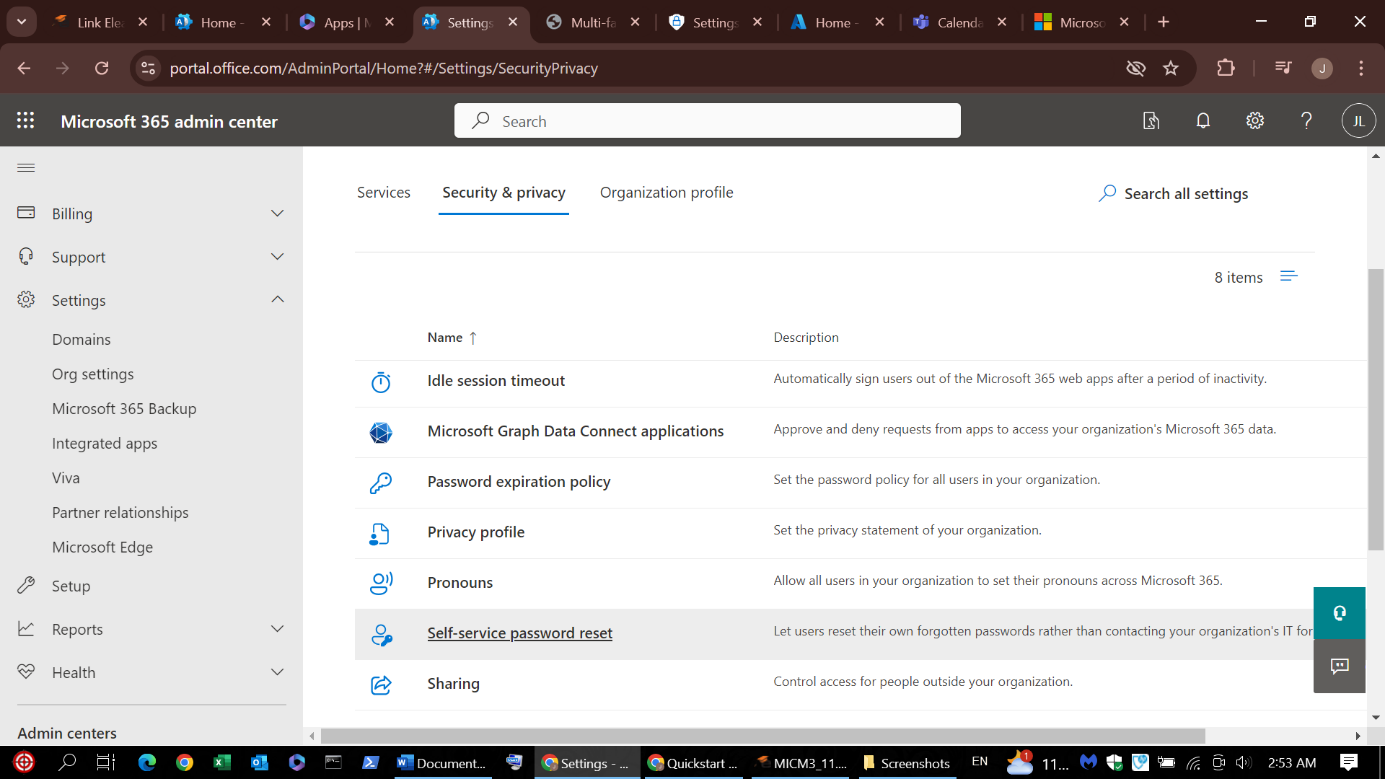
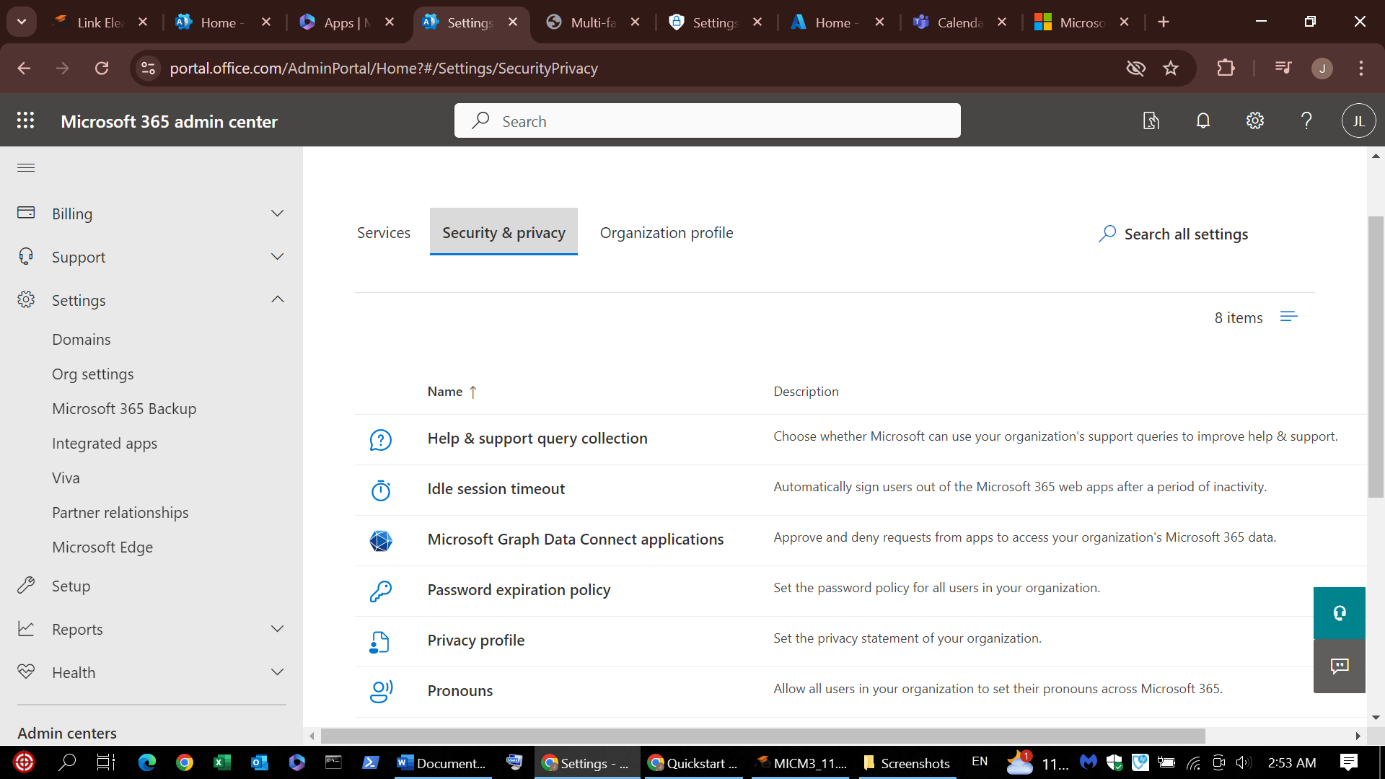
* **Password-based Authentication**: The most common authentication method, but we always recommend using it in conjunction with other methods for security reasons.
* **Two-factor authentication (2FA):** It uses a combination of two factors, usually something that the user knows (such as a password) and something that the user owns (such as a mobile device or an authentication app such as Google Authenticator or Microsoft Authenticator).
* **Biometric Authentication** : A fingerprint scanner, facial or iris recognition. This method is very safe and difficult to counterfeit.
* **E-mail or SMS** Authentication: A code is sent to an e-mail or SMS that the user must enter to verify their identity.
* **Tokens or smart cards** (Hardware Token Authentication): Physical devices owned by a user that generate one-time codes.

Also, the first method follows the steps in the Microsoft 365 admin center, followed immediately by the steps in the Azure platform.

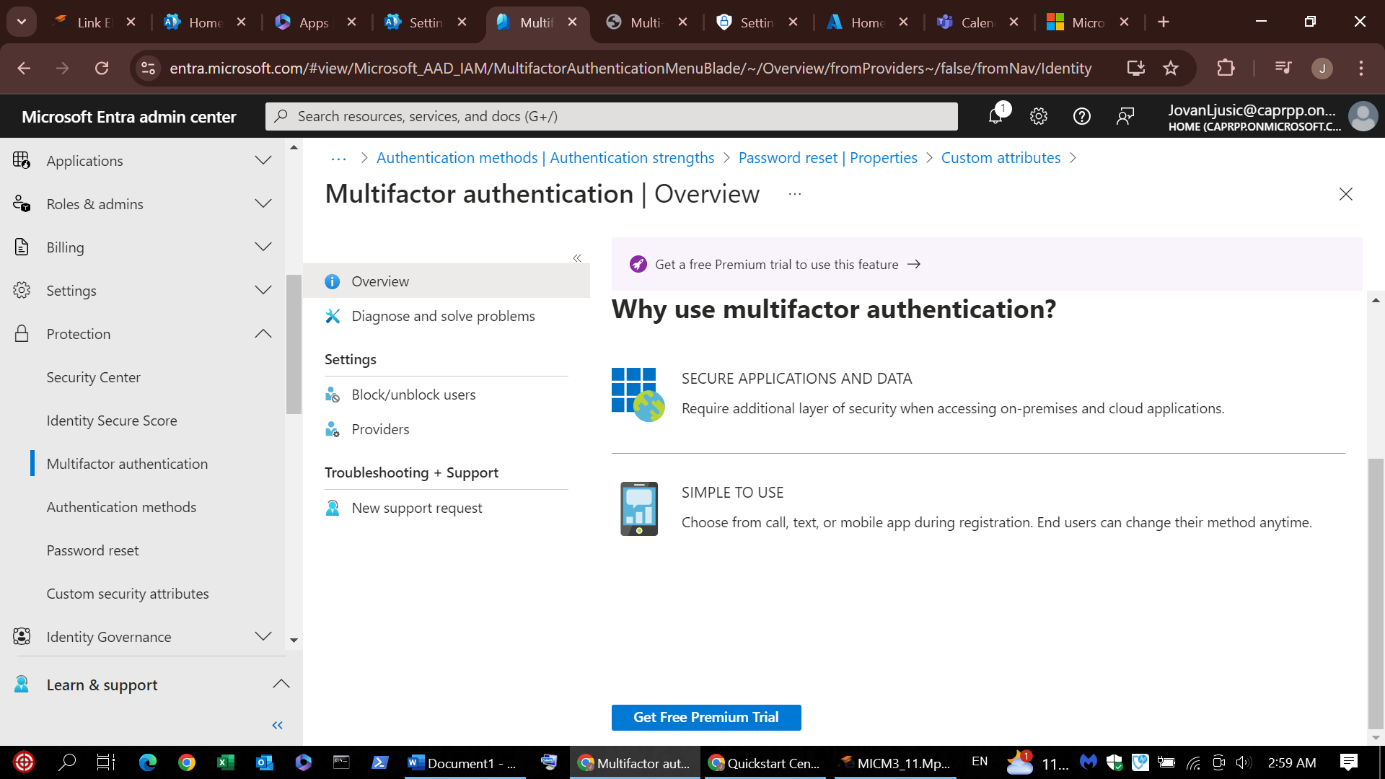
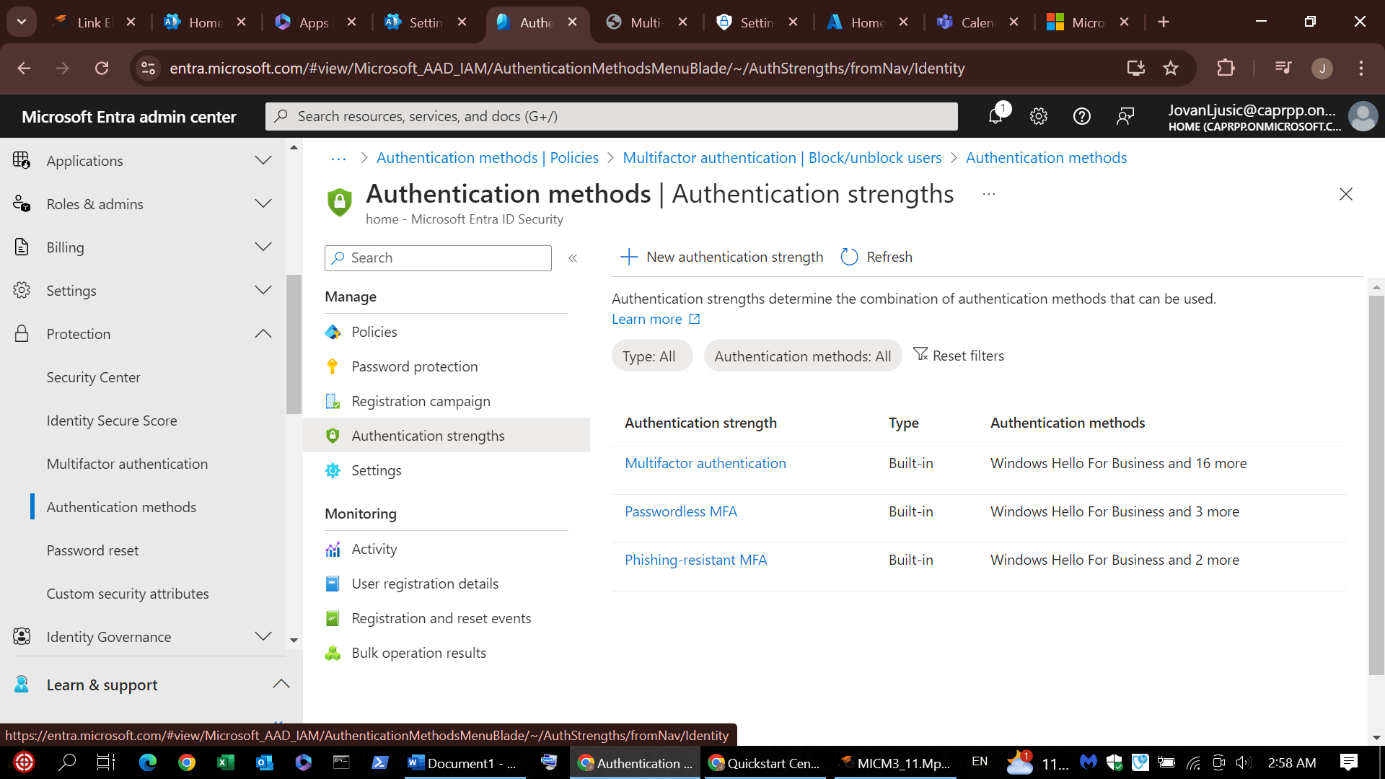
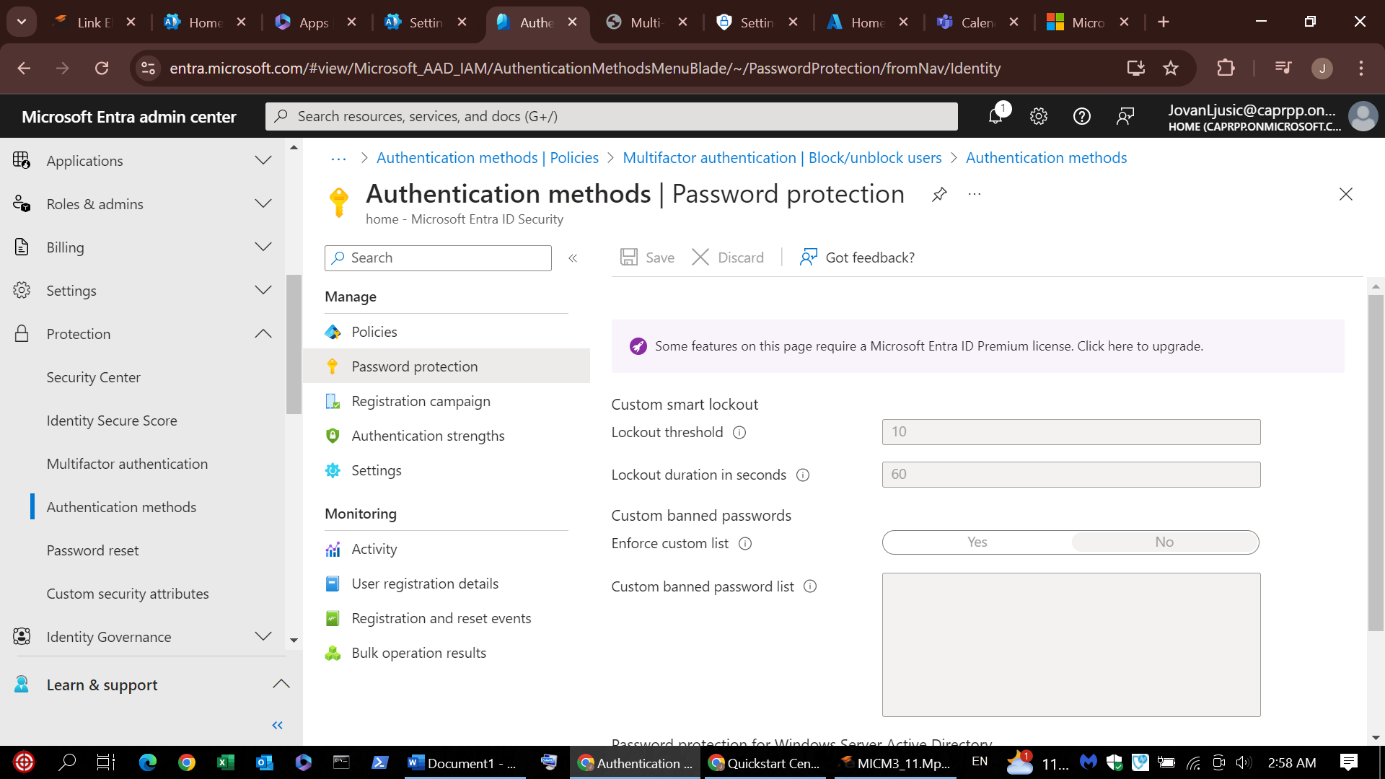
1. **Multi-factor authentication (multi-factor)**



1. **Method Self-service password reset**



1. **Methods provided by Azure**



As shown in the screenshots, although it is about data protection and security, certain restrictions have become imposed through this account because the account in use was not a Premium but a Standard Business account.

The options for protection are varied, and several of them are shown through screenshots. The text display for password setting options follows the following:

**1. Setting Password Reset Rules**

* Method One: The user must enter their password or answer a security question.
* Second method: The user must enter a code sent to their e-mail or mobile phone (SMS) or use biometric authentication (e.g. fingerprint).

This increases security because even if someone learns the user's password, they cannot reset the password without additional authentication.

**2. Setting the conditions for password reset**

The available methods to reset your password include:

* An authenticator app (such as Microsoft Authenticator)
* SMS Message
* E-mail
* Biometric data (if supported)
  1. **Configuration of authentication methods**

In the Security section, select Authentication methods.

Options include:

* Password
* Multi-Factor Authentication (2FA)
* FIDO2 Security Key (Hardware Tokens)
* Phone (SMS/Voice)
* Authenticator App
* Biometrics (if supported on devices)