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

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.

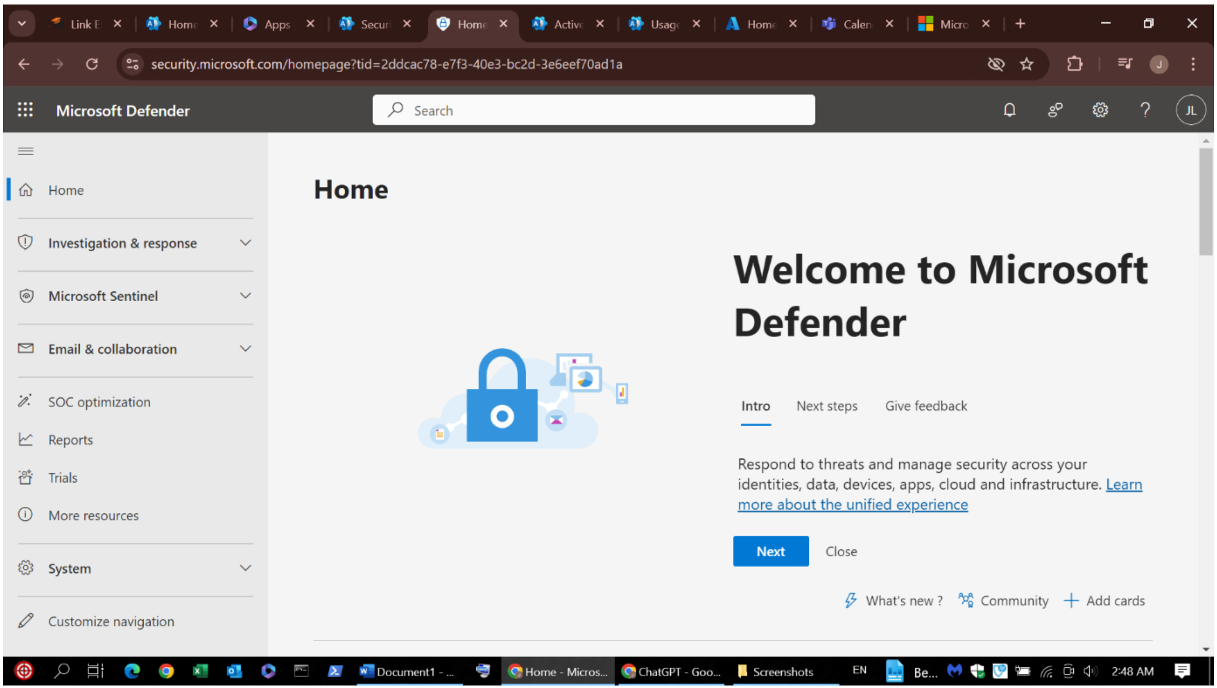
The structured approach ensures that each step is clearly defined, making the process easy to follow and implement in professional environments.

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.

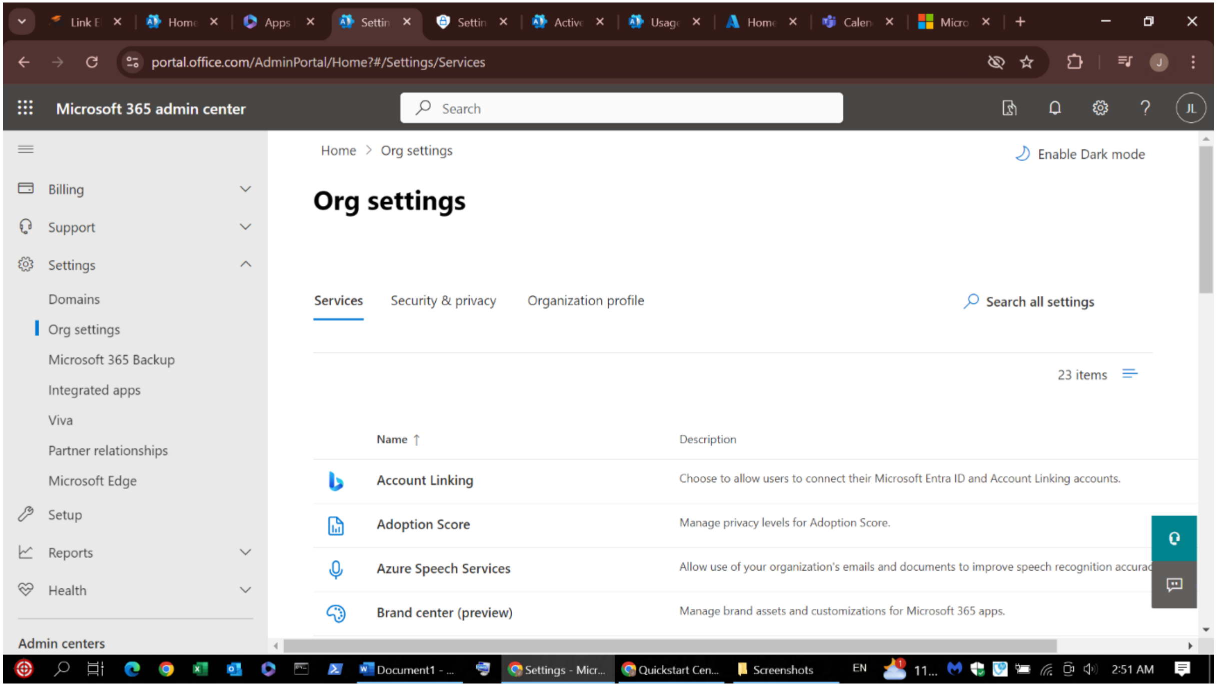
1. Multi-factor authentication (multi-factor)



Home

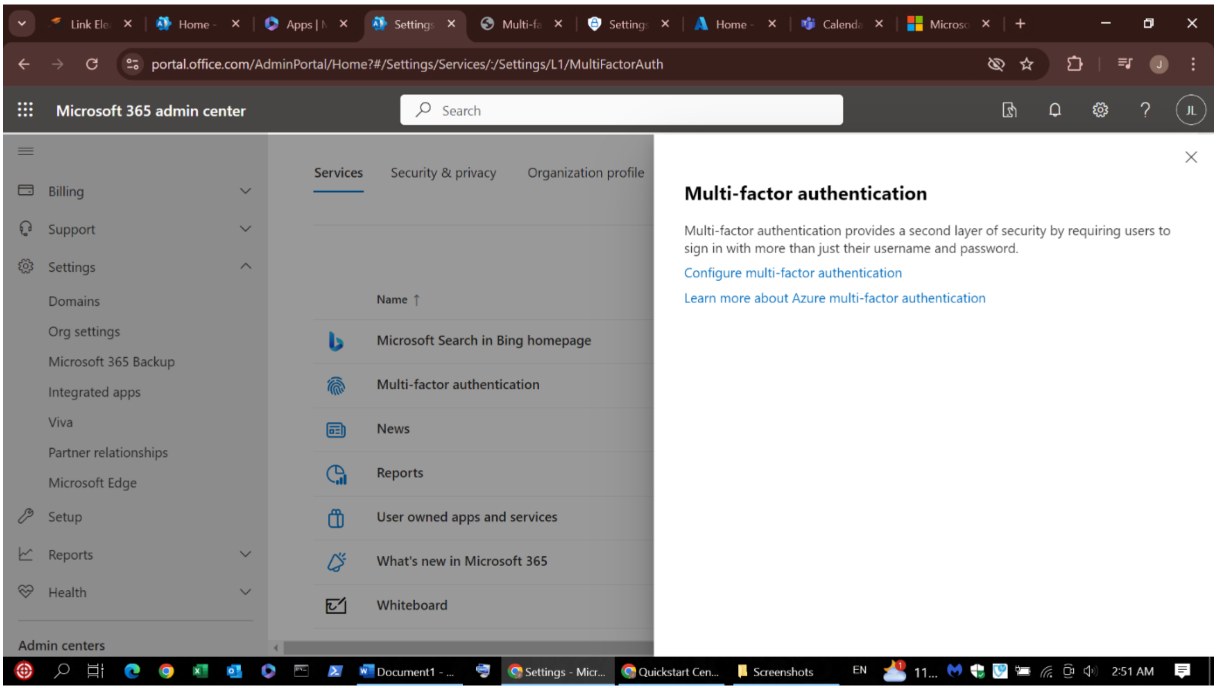
Welcome to Microsoft Defender

Respond to threats and manage security across your identities, data, devices, apps, cloud and infrastructure. Learn more about the unified experience



Org settings

Name ↑	Description
Account Linking	Choose to allow users to connect their Microsoft Entra ID and Account Linking accounts.
Adoption Score	Manage privacy levels for Adoption Score.
Azure Speech Services	Allow use of your organization's emails and documents to improve speech recognition accurac
Brand center (preview)	Manage brand assets and customizations for Microsoft 365 apps.

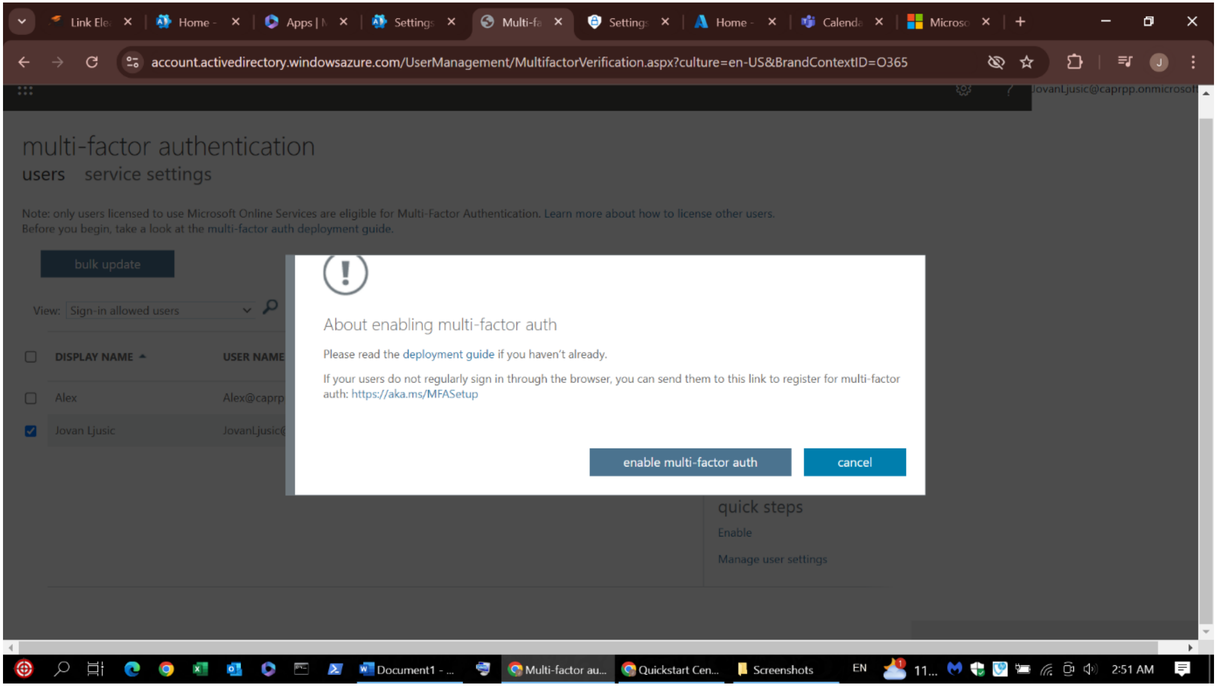

portal.office.com/AdminPortal/Home?#/Settings/Services/:/Settings/L1/MultiFactorAuth

Multi-factor authentication

Multi-factor authentication provides a second layer of security by requiring users to sign in with more than just their username and password.

Configure multi-factor authentication

Learn more about Azure multi-factor authentication


account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?culture=en-US&BrandContextID=O365

multi-factor authentication

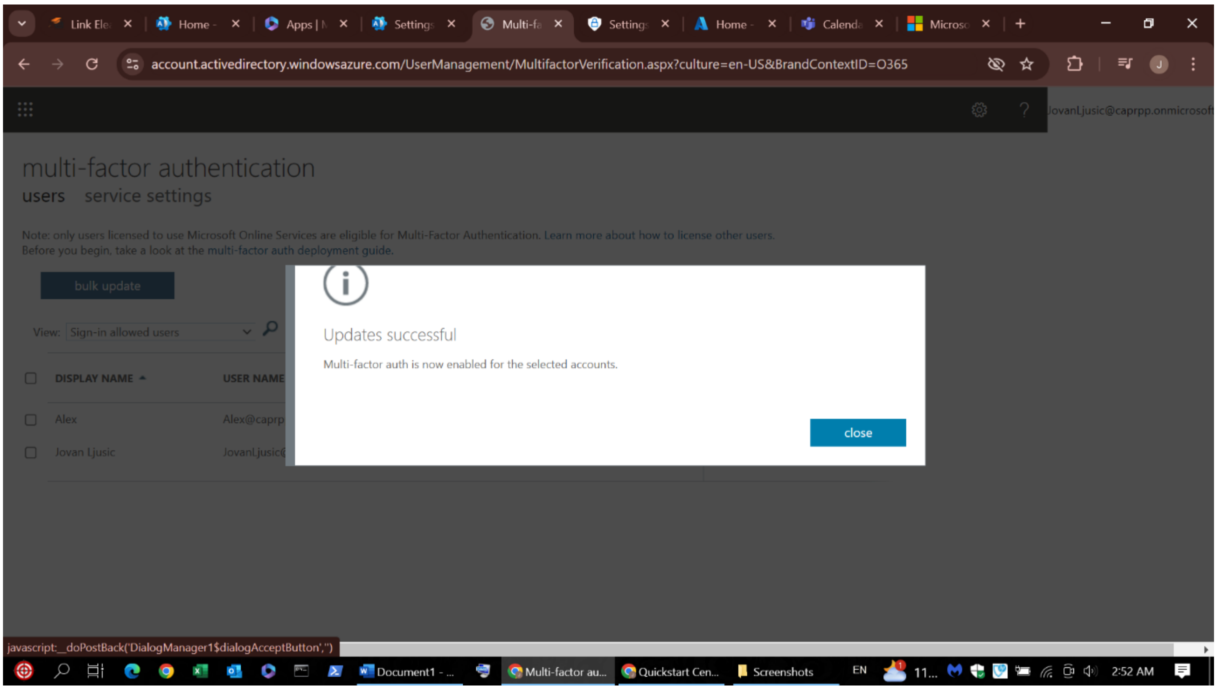
Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

□	DISPLAY NAME ▲	USER NAME
□	Alex	Alex@caprp
☑	Jovan Ljusic	JovanLjusic@

About enabling multi-factor auth

Please read the deployment guide if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup



account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?culture=en-US&BrandContextID=O365

Jovanl.jusic@caprpp.onmicrosoft

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

View: Sign-in allowed users

□ DISPLAY NAME ▲	USER NAME
□ Alex	Alex@caprp
□ Jovan Ljusic	Jovanl.jusic(

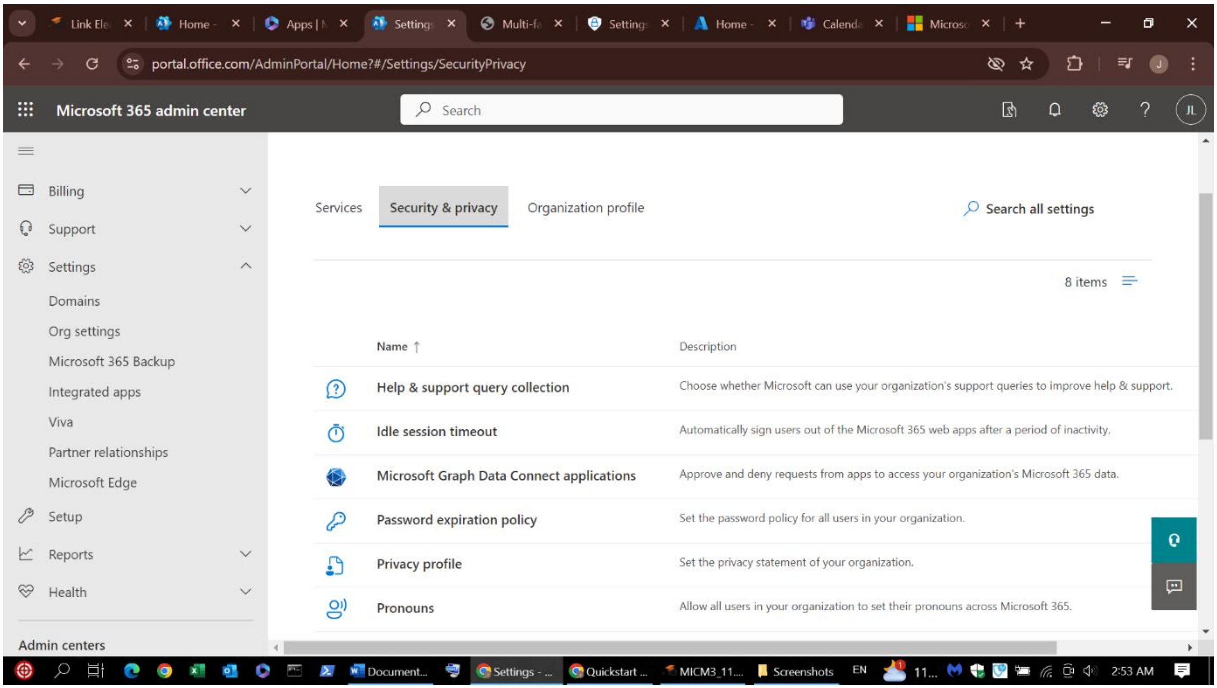
Updates successful

Multi-factor auth is now enabled for the selected accounts.

close

javascript:__doPostBack('DialogManager1$dialogAcceptButton','')

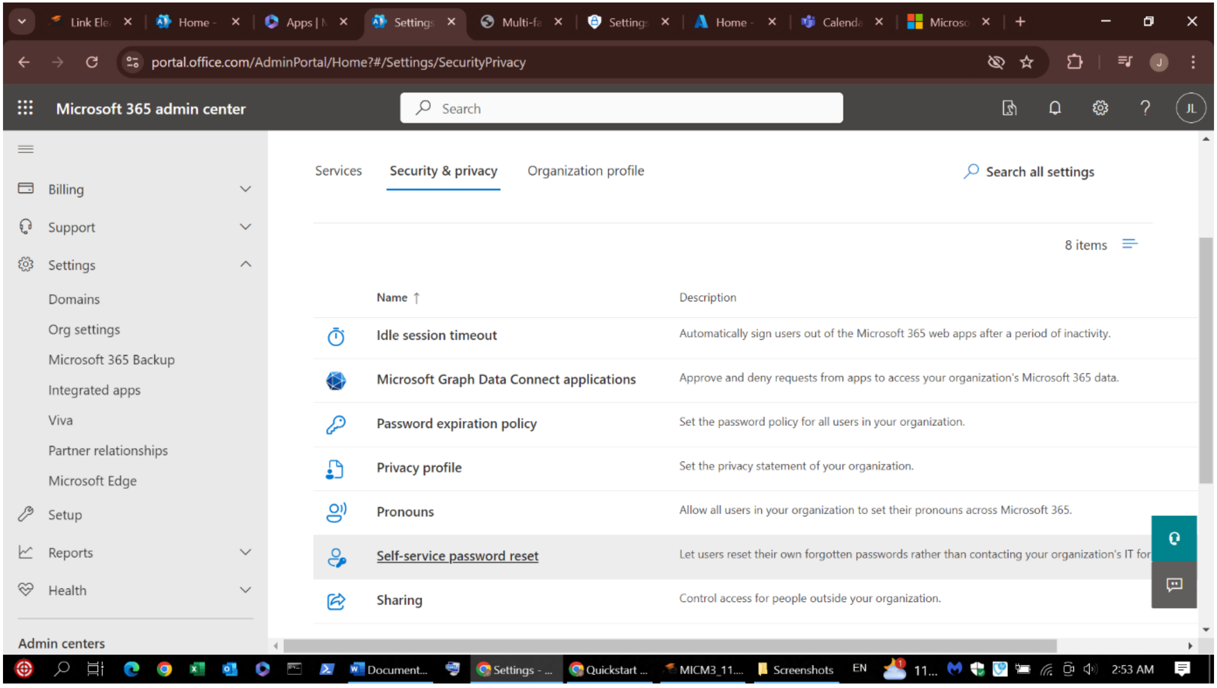
2. Method Self-service password reset



portal.office.com/AdminPortal/Home?#/Settings/SecurityPrivacy

Microsoft 365 admin center

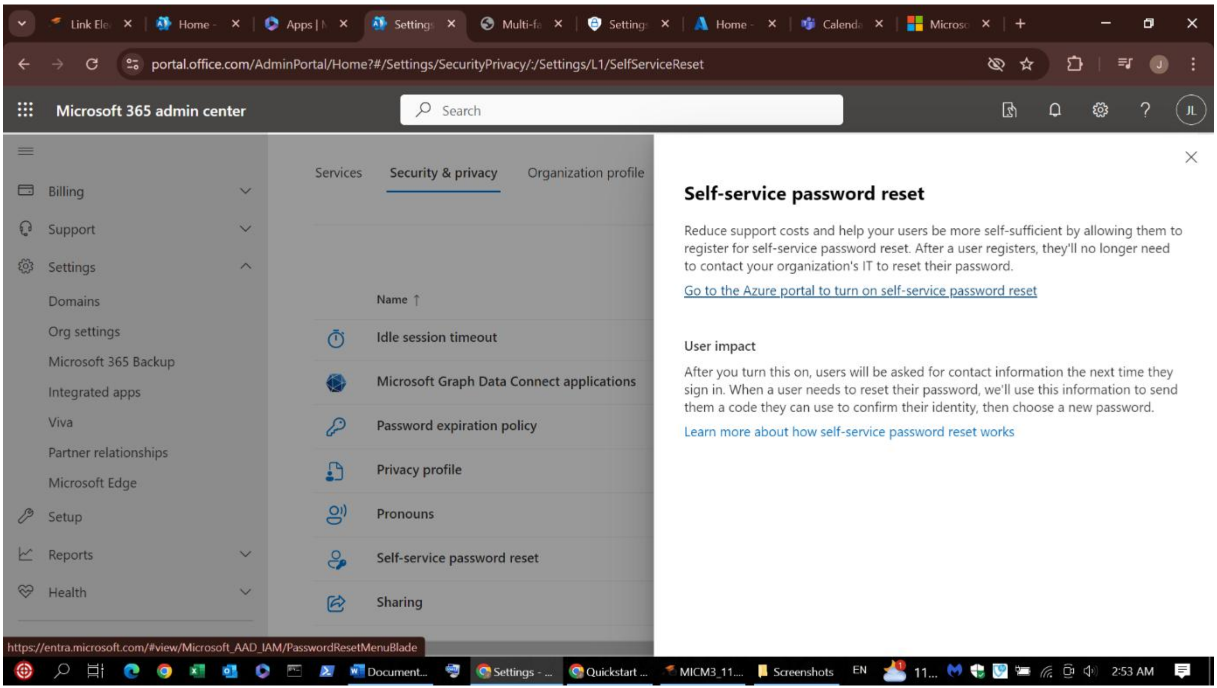
Name ↑	Description
Help & support query collection	Choose whether Microsoft can use your organization's support queries to improve help & support.
Idle session timeout	Automatically sign users out of the Microsoft 365 web apps after a period of inactivity.
Microsoft Graph Data Connect applications	Approve and deny requests from apps to access your organization's Microsoft 365 data.
Password expiration policy	Set the password policy for all users in your organization.
Privacy profile	Set the privacy statement of your organization.
Pronouns	Allow all users in your organization to set their pronouns across Microsoft 365.



portal.office.com/AdminPortal/Home?#/Settings/SecurityPrivacy

Microsoft 365 admin center

Name ↑	Description
Idle session timeout	Automatically sign users out of the Microsoft 365 web apps after a period of inactivity.
Microsoft Graph Data Connect applications	Approve and deny requests from apps to access your organization's Microsoft 365 data.
Password expiration policy	Set the password policy for all users in your organization.
Privacy profile	Set the privacy statement of your organization.
Pronouns	Allow all users in your organization to set their pronouns across Microsoft 365.
Self-service password reset	Let users reset their own forgotten passwords rather than contacting your organization's IT for
Sharing	Control access for people outside your organization.



portal.office.com/AdminPortal/Home?#/Settings/SecurityPrivacy/:/Settings/L1/SelfServiceReset

Self-service password reset

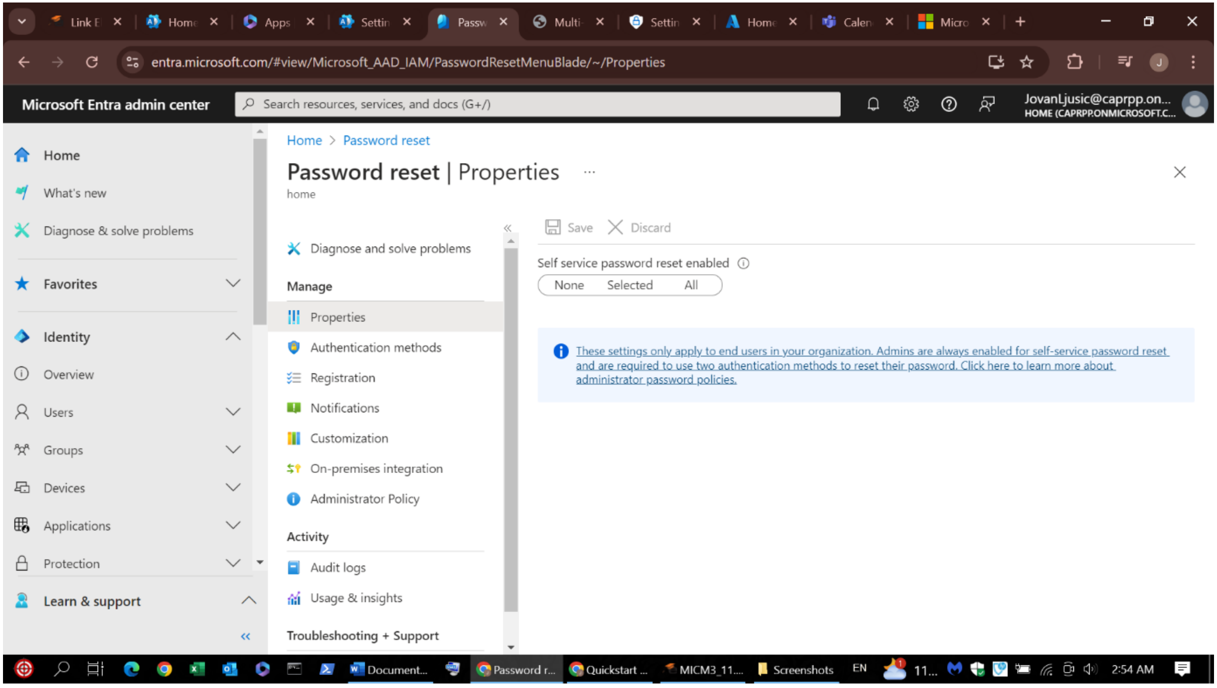
Reduce support costs and help your users be more self-sufficient by allowing them to register for self-service password reset. After a user registers, they'll no longer need to contact your organization's IT to reset their password.

Go to the Azure portal to turn on self-service password reset

User impact

After you turn this on, users will be asked for contact information the next time they sign in. When a user needs to reset their password, we'll use this information to send them a code they can use to confirm their identity, then choose a new password.

Learn more about how self-service password reset works



entra.microsoft.com/#view/Microsoft_AAD_IAM/PasswordResetMenuBlade/~/Properties

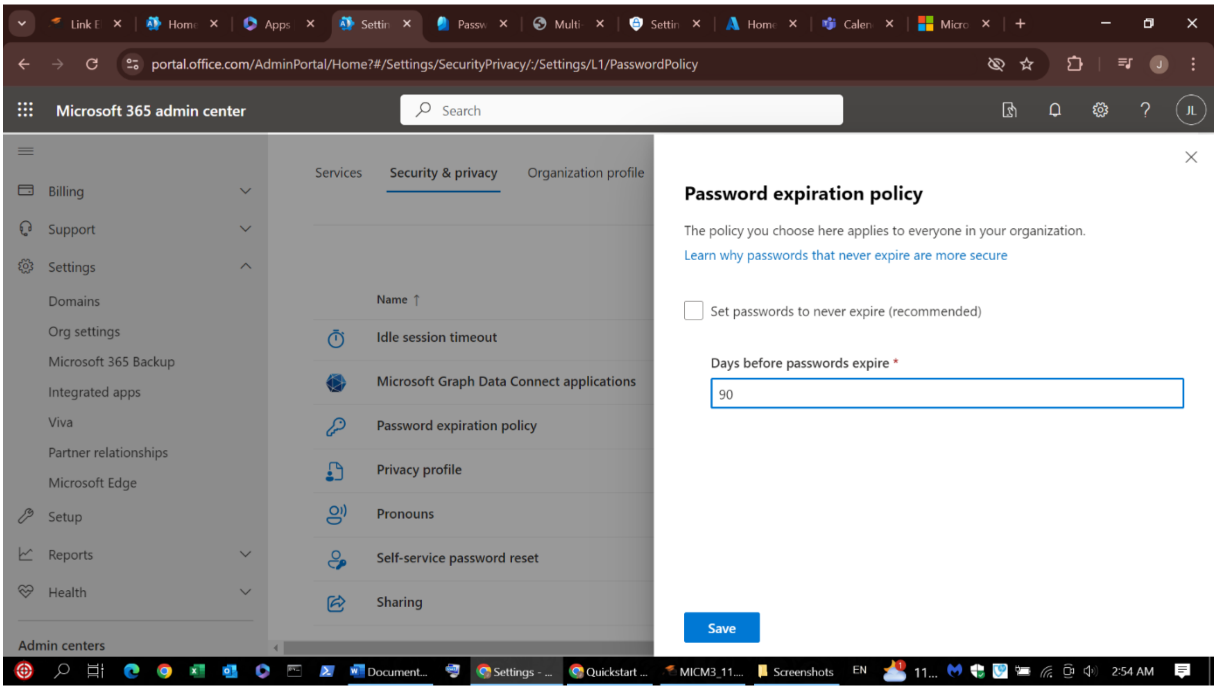
Password reset | Properties

home

Self service password reset enabled ⓘ

None | Selected | All

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.



Password expiration policy

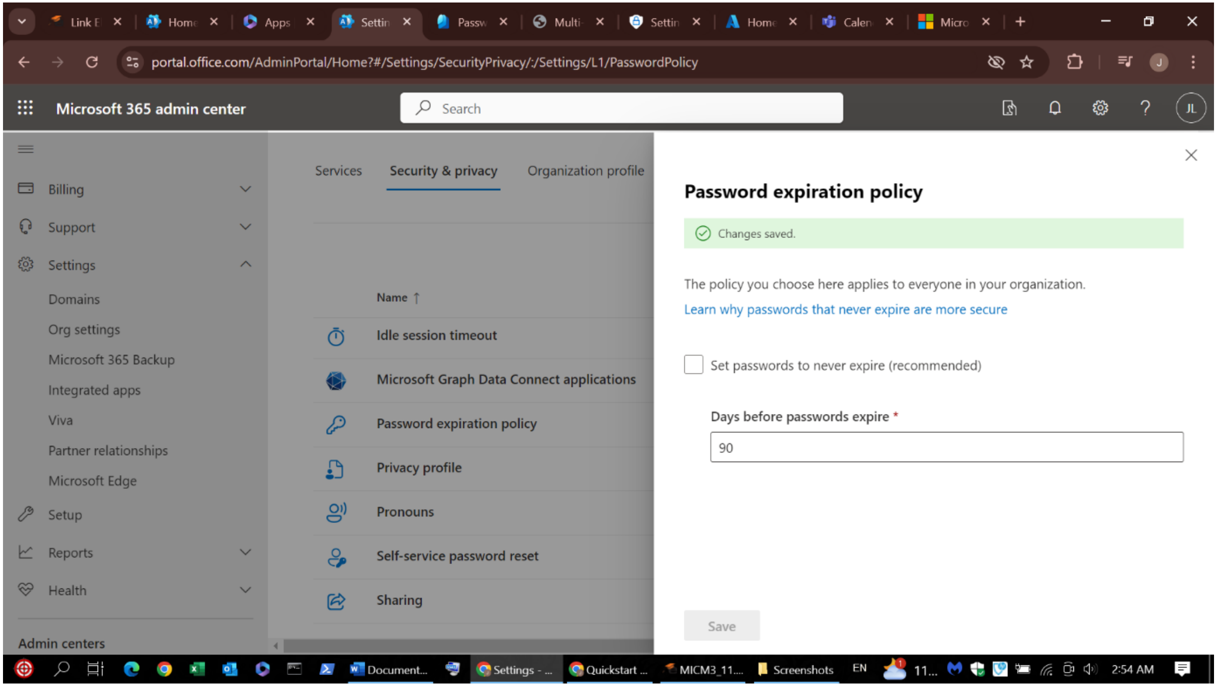
The policy you choose here applies to everyone in your organization.

Learn why passwords that never expire are more secure

□ Set passwords to never expire (recommended)

Days before passwords expire *

90



Password expiration policy

✓ Changes saved.

The policy you choose here applies to everyone in your organization.

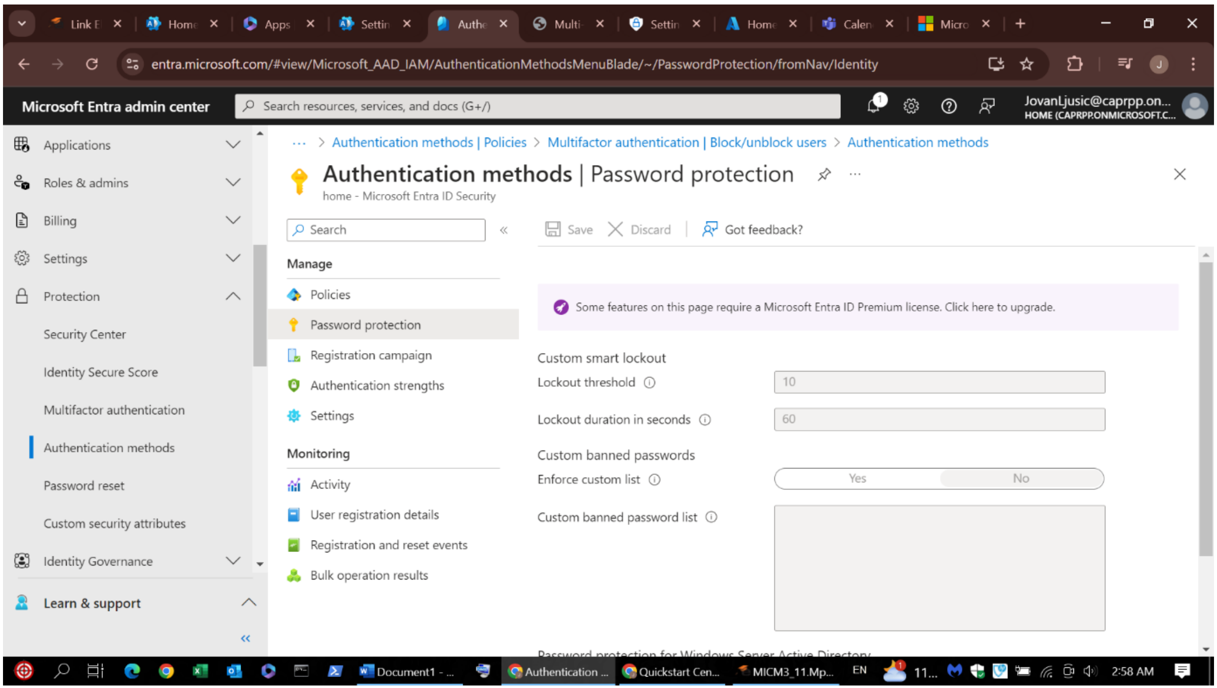
Learn why passwords that never expire are more secure

□ Set passwords to never expire (recommended)

Days before passwords expire *

90

3. Methods provided by Azure


entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtection/fromNav/Identity
Microsoft Entra admin center
Search resources, services, and docs (G+/)
JovanLjusic@caprpp.on...
HOME (CAPRPP.ONMICROSOFT.C...
Applications
Roles & admins
Billing
Settings
Protection
Security Center
Identity Secure Score
Multifactor authentication
Authentication methods
Password reset
Custom security attributes
Identity Governance
Learn & support
... > Authentication methods | Policies > Multifactor authentication | Block/unblock users > Authentication methods
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Save
Discard
Got feedback?
2:58 AM

Authentication methods | Password protection

home - Microsoft Entra ID Security

Some features on this page require a Microsoft Entra ID Premium license. Click here to upgrade.

Custom smart lockout

Lockout threshold: 10

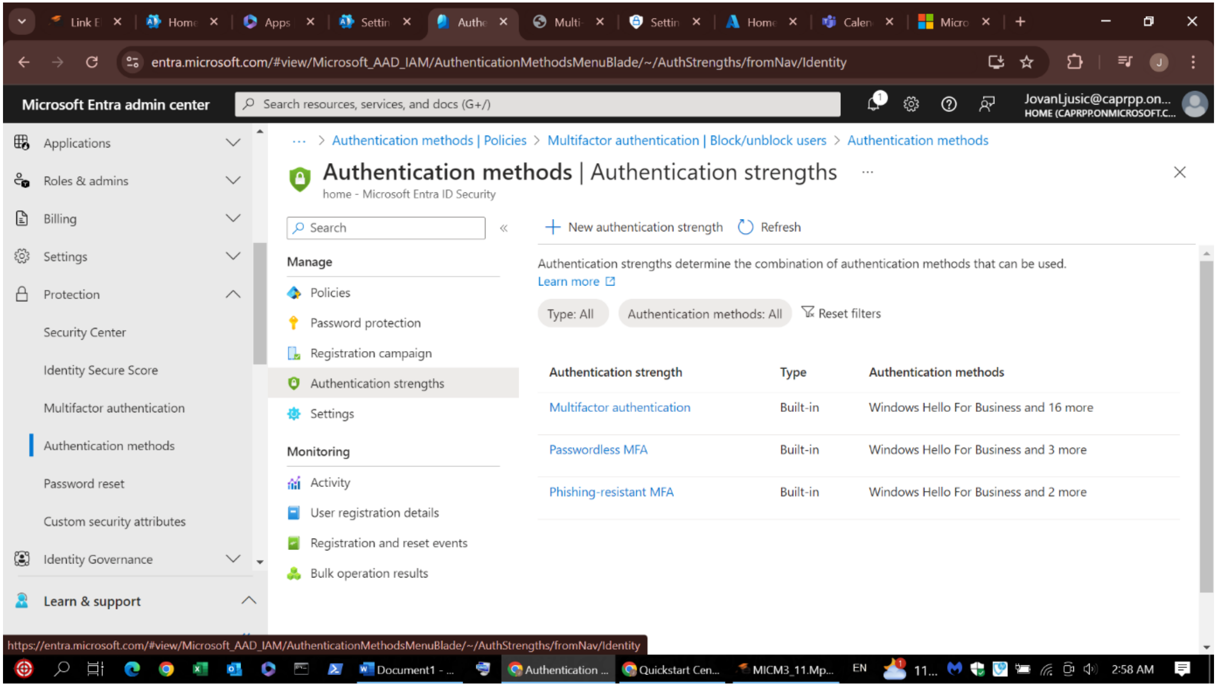
Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: Yes [✓ No]

Custom banned password list:

Password protection for Windows Server Active Directory

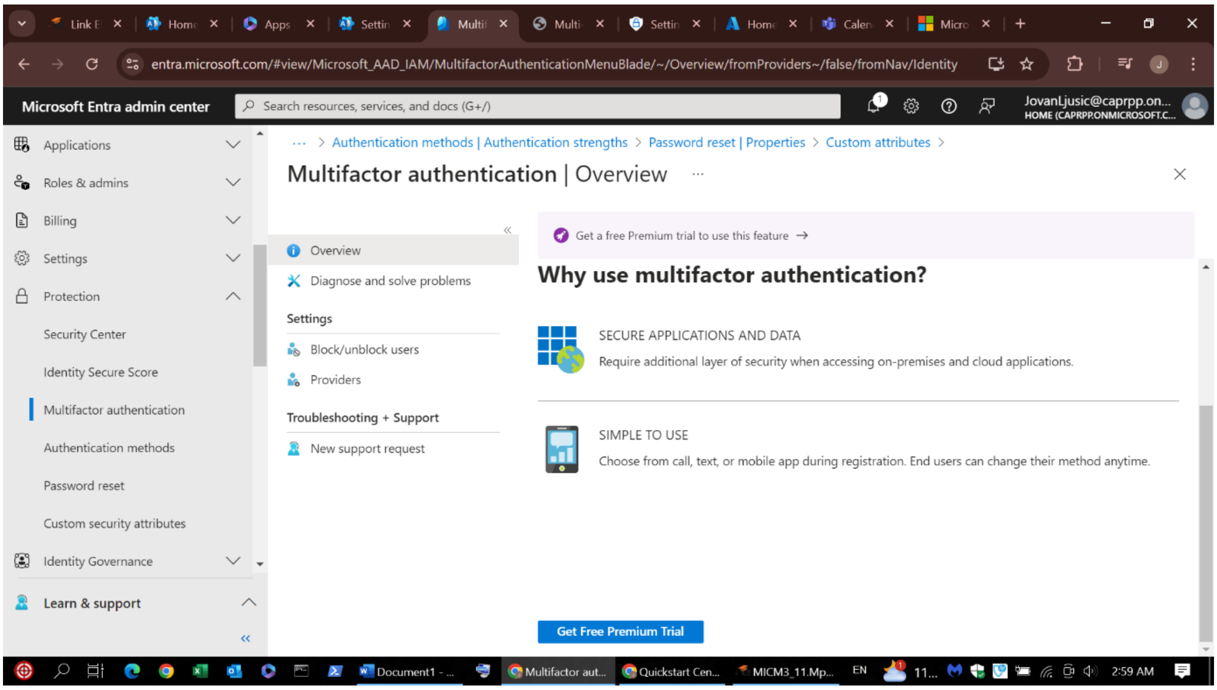

entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AuthStrengths/fromNav/Identity
Microsoft Entra admin center
Search resources, services, and docs (G+/)
JovanLjusic@caprpp.on...
HOME (CAPRPP.ONMICROSOFT.C...
Applications
Roles & admins
Billing
Settings
Protection
Security Center
Identity Secure Score
Multifactor authentication
Authentication methods
Password reset
Custom security attributes
Identity Governance
Learn & support
... > Authentication methods | Policies > Multifactor authentication | Block/unblock users > Authentication methods
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
New authentication strength
Refresh
Type: All
Authentication methods: All
Reset filters
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AuthStrengths/fromNav/Identity
2:58 AM

Authentication methods | Authentication strengths

home - Microsoft Entra ID Security

Authentication strengths determine the combination of authentication methods that can be used.
Learn more

Authentication strength	Type	Authentication methods
Multifactor authentication	Built-in	Windows Hello For Business and 16 more
Passwordless MFA	Built-in	Windows Hello For Business and 3 more
Phishing-resistant MFA	Built-in	Windows Hello For Business and 2 more



entra.microsoft.com/#view/Microsoft_AAD_IAM/MultifactorAuthenticationMenuBlade/~/Overview/fromProviders~/false/fromNav/Identity

Microsoft Entra admin center

Jovan.Ljusic@caprpp.on...
HOME (CAPRPP.ONMICROSOFT.C...

... > Authentication methods | Authentication strengths > Password reset | Properties > Custom attributes >

Multifactor authentication | Overview

Get a free Premium trial to use this feature →

Why use multifactor authentication?

SECURE APPLICATIONS AND DATA
Require additional layer of security when accessing on-premises and cloud applications.

SIMPLE TO USE
Choose from call, text, or mobile app during registration. End users can change their method anytime.

Get Free Premium Trial

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)

3. 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)