

## Multifactor authentication

U uputi su postavke kako postaviti višefaktorska autentifikaciju(Multifactor authentication) za korisnike.

Višefaktorska provjera autentičnosti je proces u kojem se od korisnika traže dodatni oblici identifikacije tijekom prijave. Na primjer, unos jedinstvenog koda na njihov mobilni telefon ili skeniranje otiska prsta. Drugim oblikom autentifikacije sigurnost se povećava jer napadaču nije lako dobiti ili duplicirati ovaj dodatni faktor.

Microsoft Entra višefaktorska provjera autentičnosti i Microsoft Entra multifactor authentication and Conditional Access policies pružaju fleksibilnost zahtjeva MFA od korisnika za određene događaje prijave.

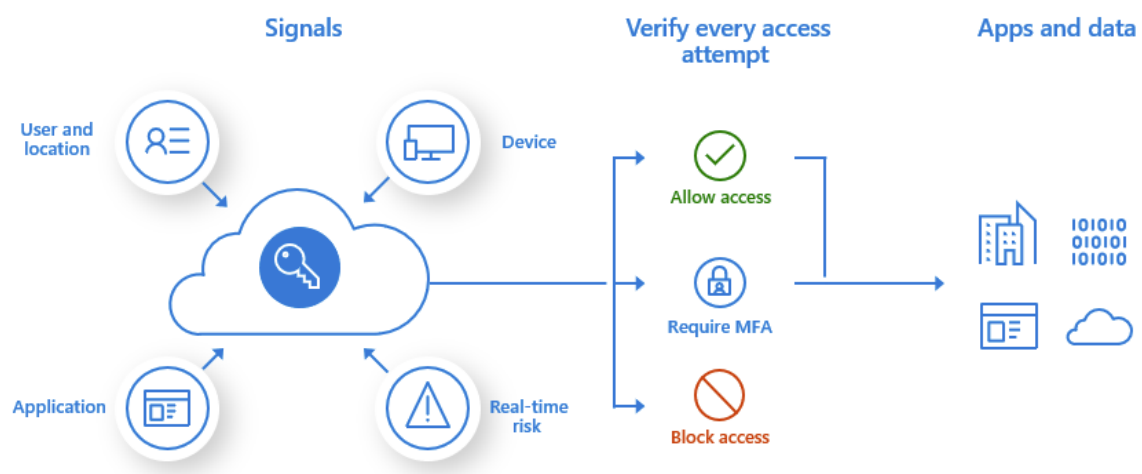
### Prerequisites

Microsoft Entra tenant sa Microsoft Entra ID P1 licencijom.

Korisnički račun s dodijeljenom minimalnom rolom Conditional Access Administrator ili Global administrator.

### Conditional Access policy za MFA

Preporučeni način za omogućavanje i korištenje višefaktorske provjere autentičnosti Microsoft Entra je koristeći Conditional Access policies. Conditional Access policies omogućuje stvaranje i definiranje pravila koja reagiraju na događaje prijave i koje zahtijevaju dodatne radnje prije nego što se korisniku odobri pristup aplikaciji ili usluzi.

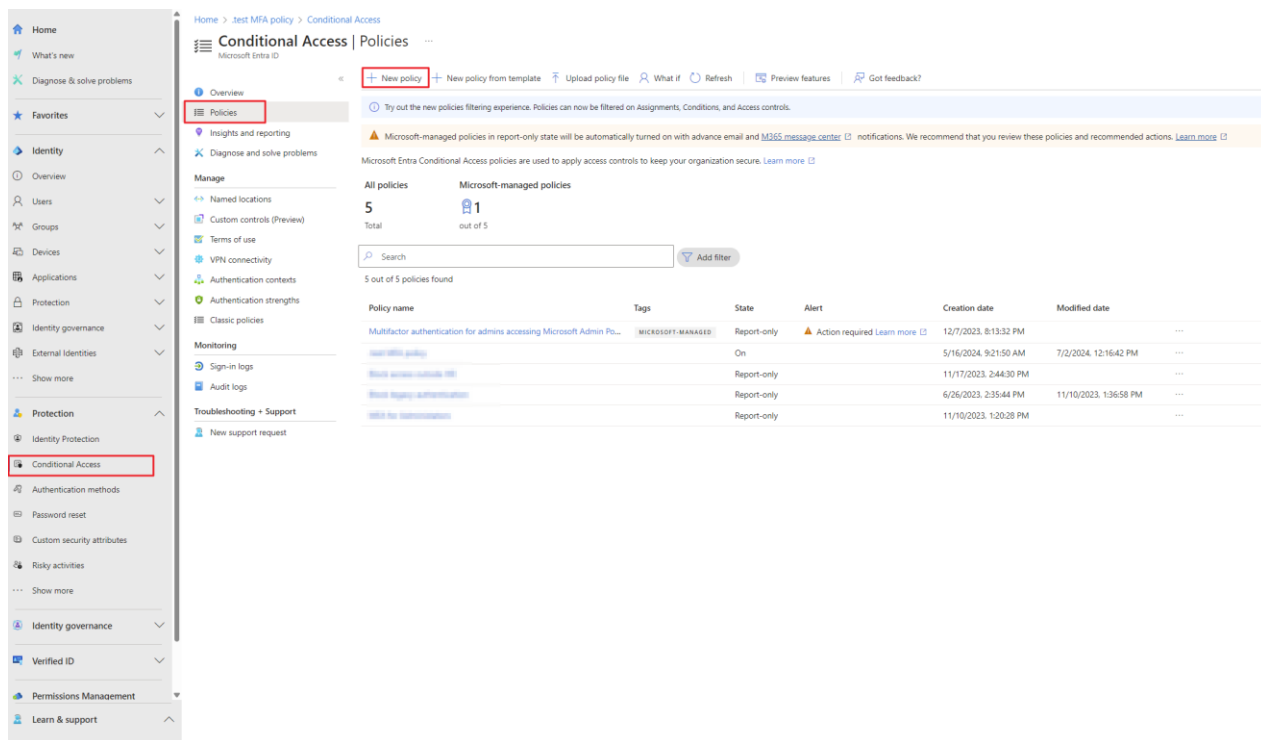


Conditional Access policies mogu se primijeniti na određene korisnike, grupe i aplikacije.

Uputa

Potrebno se prijaviti na portal Microsoft Entra (<https://entra.microsoft.com/>) te odabrati:

**Protection -> Conditional Access -> Policies -> New Policy**



Nakon odabira prikazuju se postavke kao sa slike.

U polje „name“ upisao sam ime police koju kreiram.

Pod selekciju User, na desnu stranu prikazale su se postavke Include gdje sam selektirao opciju „Select users and groups“ u koju sam dodao prethodno kreiranu grupu \_MFA Enabled Users, u grupu se mogu dodavati korisnici pojedinačno ili dodavati sigurnosne grupe npr. Sigurnosne grupe po odjelima.

Home > .test MFA policy > Conditional Access | Policies >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more >](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.  
[Learn more >](#)

Name \*

MFA policy

Assignments

Users

Specific users included

Select users and groups must be configured

Target resources

No target resources selected

Network

NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Include

Exclude

☐ None

☐ All users

☒ Select users and groups

☐ Guest or external users

☐ Directory roles

☒ Users and groups

Select

0 users and groups selected

Select at least one user or group

Enable policy

Report only

On

Off

Create

Select users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

mfa

1 result found

All

Users


Groups

Name

Type

Details


☒

 -MFA Enabled Users

Group

Selected (1)

Reset

 -MFA Enabled Users

Select

## Target Resources - Include

Ova postavka služi za postavljanje pristupa aplikacijama. Pod **Include** Odabrao sam opciju „All cloud Apps“ opcija će implementirati multifaktorsku autentifikaciju za sve cloud aplikacije.

## New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

MFA policy ✓

### Assignments

Users ⓘ

[Specific users included](#)

Target resources ⓘ

All cloud apps

Network **NEW** ⓘ

[Not configured](#)

Conditions ⓘ

[0 conditions selected](#)

### Access controls

Grant ⓘ

[0 controls selected](#)

Session ⓘ

[0 controls selected](#)

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps ▾

**Include** Exclude

☐ None

☒ All cloud apps

☐ Select apps

⚠ Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected. [Learn more](#)

## Target resources – Exclude

Kako bi računala mogao dodati u Intune, obilježim da je Microsoft Intune Enrollment cloud aplikacija postavio sam ju na listu „Exclude“

[Home](#) > [.test MFA policy](#) > [Conditional Access | Policies](#) >

## New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*

MFA policy ✓

### Assignments

Users ⓘ

[Specific users included](#)

Target resources ⓘ

All cloud apps included and 1 app excluded

Network **NEW** ⓘ

[Not configured](#)

Conditions ⓘ

[0 conditions selected](#)

### Access controls

Grant ⓘ

[0 controls selected](#)

Session ⓘ

[0 controls selected](#)

Control access based on all or specific network access traffic, cloud apps or actions.

[Learn more](#)

Select what this policy applies to

Cloud apps ▾

Include **Exclude**

Select the cloud apps to exempt from the policy

Edit filter

[None](#)

Select excluded cloud apps

[Microsoft Intune Enrollment](#)

MI

Microsoft Intune Enrollment  
d4ebce55-015a-49b5-a083-c84d1797ae8c ...

## Grant

Za odobrenje ili onemogućavanje pristupa ovisno o preferencijama postavio sam *Grant access* - > „*Require multifactor authentication*“ te odabrao opciju „*Require one of the selected controls*“

Home > .test MFA policy > Conditional Access | Policies >

## New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
MFA policy ✓

Assignments

Users ⓘ  
Specific users included

Target resources ⓘ  
All cloud apps included and 1 app excluded

Network | NEW ⓘ  
Not configured

Conditions ⓘ  
0 conditions selected

Access controls

Grant ⓘ  
0 controls selected

Session ⓘ  
0 controls selected

Enable policy  
Report-only On Off

Create

## Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access  
☒ Grant access

☒ Require multifactor authentication ⓘ

Consider testing the new "Require authentication strength". [Learn more](#)

☐ Require authentication strength ⓘ

\*"Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

☐ Require device to be marked as compliant ⓘ

☐ Require Microsoft Entra hybrid joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)


☐ Require app protection policy ⓘ  
[See list of policy protected client apps](#)

For multiple controls  
☐ Require all the selected controls  
☒ Require one of the selected controls

Select

## Test multifaktor autentifikacije

Ss

 Microsoft

Sign in


test2@gmail.com

No account? [Create one!](#)

[Can't access your account?](#)

Back

Next

 Sign-in options

Ss

test2@gmail.com

## More information required

Your organization needs more information to keep your account secure

[Use a different account](#)


[Learn more](#)

Next

Sss

## Keep your account secure

### Microsoft Authenticator



#### Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

Next

[I want to set up a different method](#)

Ss

## Keep your account secure

### Microsoft Authenticator



#### Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

[Back](#)[Next](#)

[I want to set up a different method](#)

Sss

## Keep your account secure

### Microsoft Authenticator

#### Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

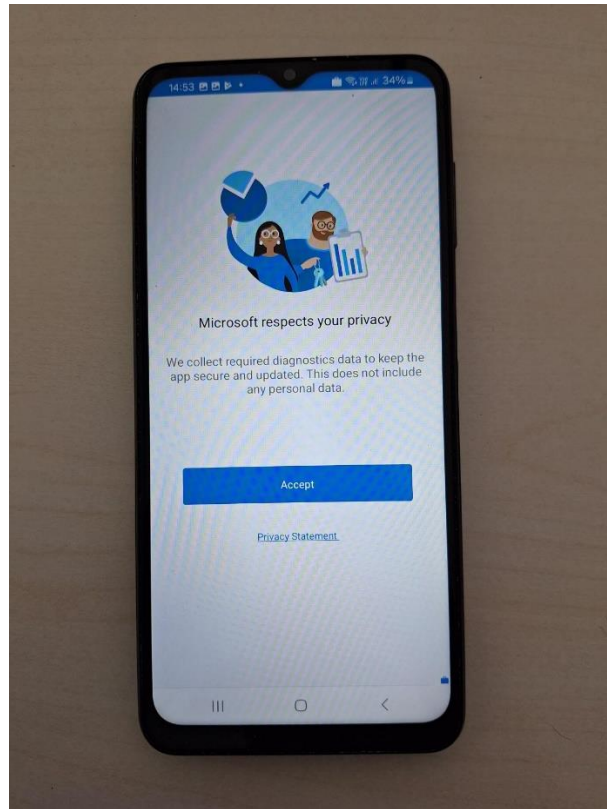
After you scan the QR code, choose "Next".

[Can't scan image?](#)[Back](#)[Next](#)

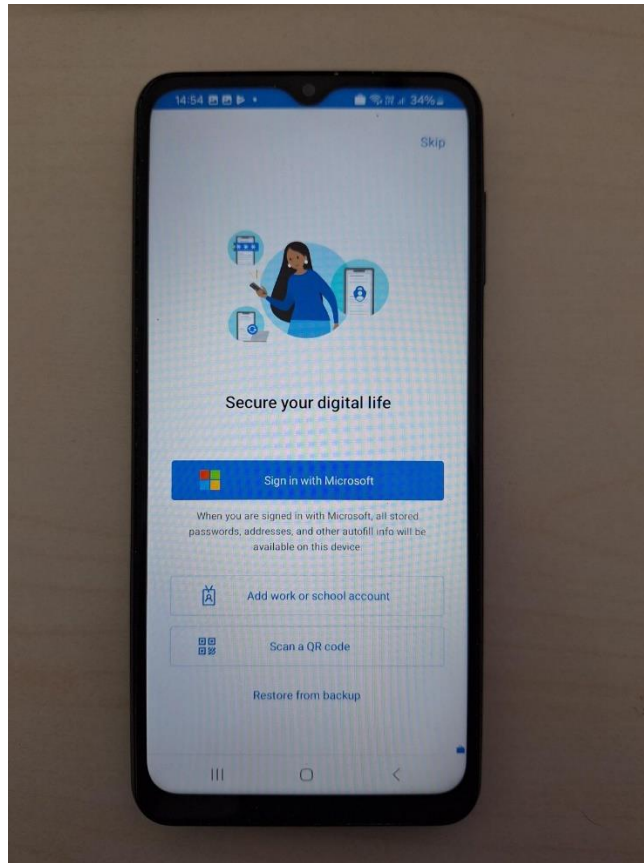
[I want to set up a different method](#)

Ed

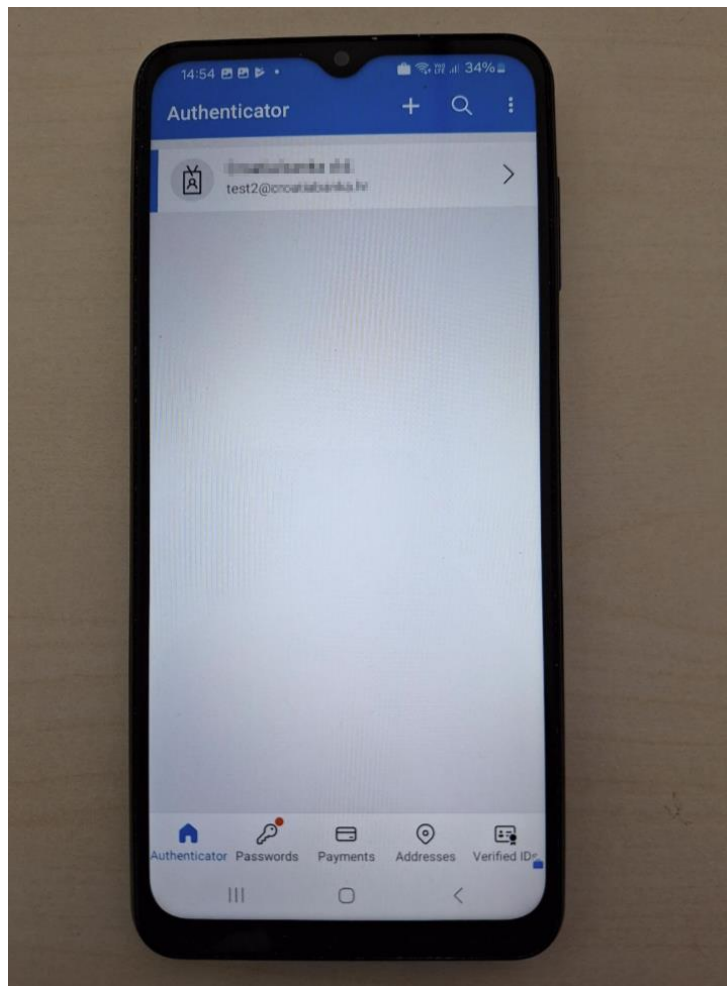




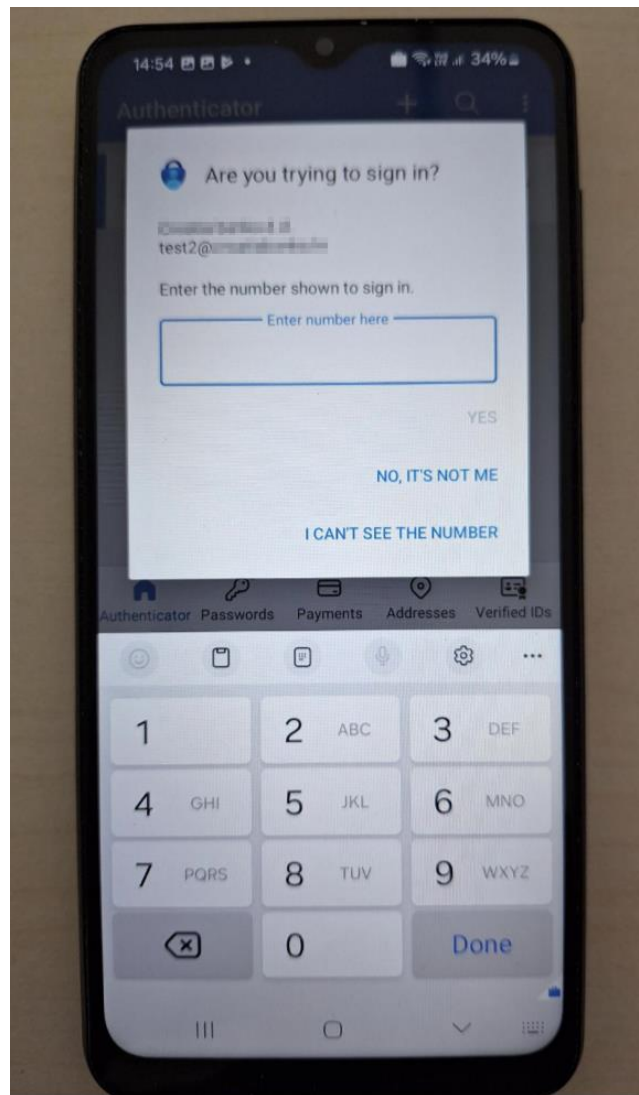
Hhh



LU



Ddd



Ddd

## Keep your account secure

### Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

59

Back

Next

[I want to set up a different method](#)

Gfgg

## Keep your account secure

### Microsoft Authenticator



✓ Notification approved

Back

Next

[I want to set up a different method](#)

Llččl

## Keep your account secure

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in

**Default sign-in method:**



Microsoft Authenticator

Done