Implementacijom novog firewall uređaja ukida se postojeća FortiToken višefaktorska autentifikacija (MFA), a uvodi se novi MFA mehanizam koji koristi Microsoft Mobile Authenticator aplikaciju za generiranje jednokratnih lozinki.

Novi sustav autentifikacije koristi sljedeće podatke za prijavu:

- domenski username (ime.prezime@login.hr)
- domenski password
- jednokratna lozinka generirana putem Microsoft Mobile Authenticator aplikacije

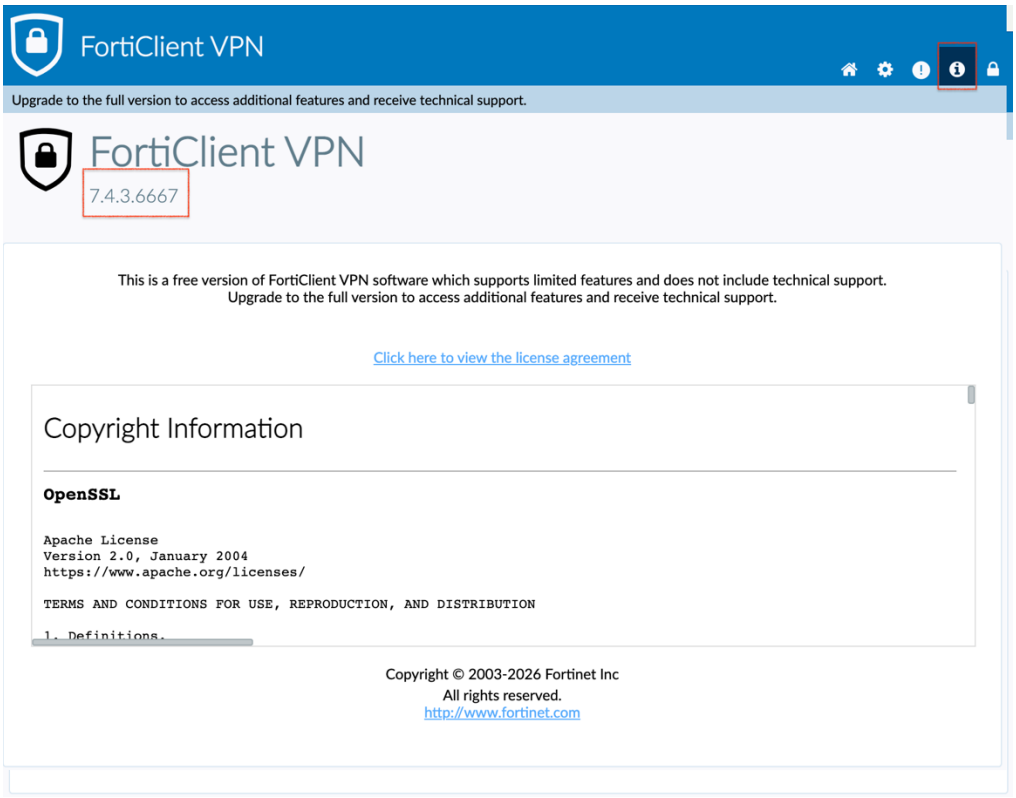
Na FortiClient VPN klijentu potrebno je kreirati novi konfiguracijski profil, koji možete podesiti već tijekom ovog tjedna - prije zamjene firewall uređaja - prateći upute u nastavku.

Napomena:

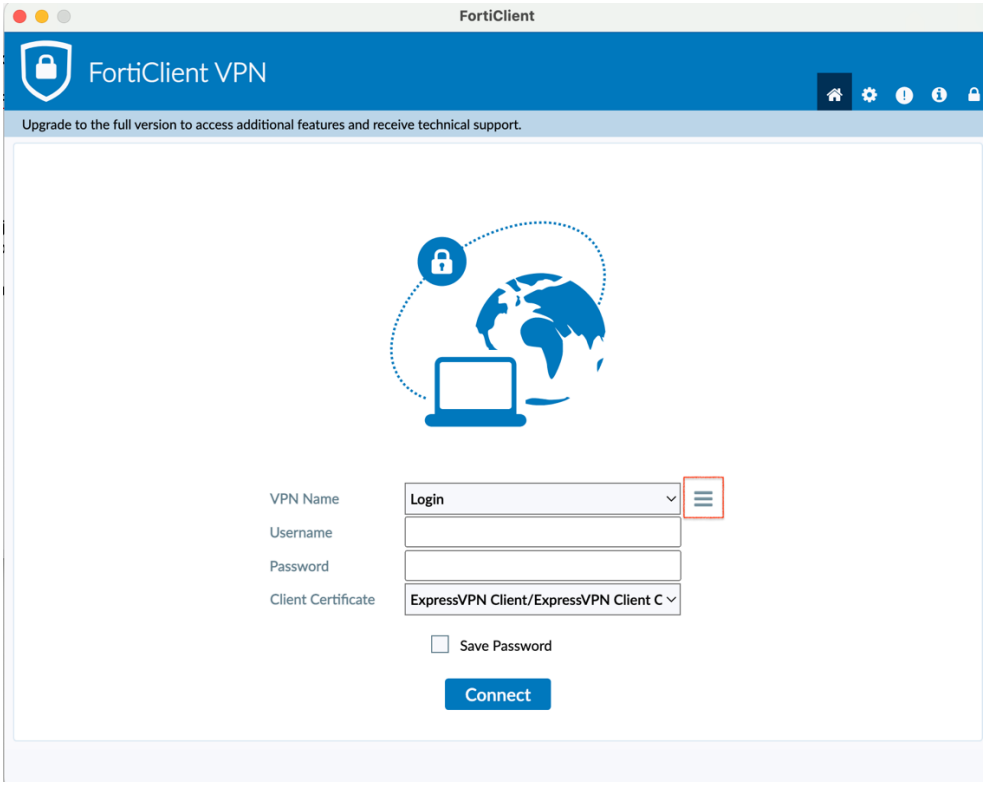
Nemojte brisati postojeći FortiClient VPN konfiguracijski profil za spajanje u Login mrežu dok ne potvrdite idući tjedan da novi profil radi ispravno. Također, u slučaju nadogradnje klijenta molimo Vas da napravite backup postojećih konekcija na FortiClient VPN-u (odabrati kotačić u gornjem desnom kutu aplikacije, Backup, unijeti password da enkripciju backupa i pohraniti backup konekcija ukoliko se iste pobrišu prilikom nadogradnje). Za import konekcija potrebno je odabrati lokot u gornjem desnom kutu VPN aplikacije, potom odabrati kotačić, pa Restore, odabrati backup datoteku i unijeti password koji ste ranije unijeli za enkripciju backupa)

1. Provjeriti verziju Forticlient VPN klijenta - ukoliko imate instaliranu bitno stariju verziju od 7.4.3, moguće je da nećete moći odabrati ili unijeti pojedine konfiguracijske opcije opisane u nastavku. (preuyimanje nove verzije FortiClient VPN aplikacije za sve platforme moguće je sa adrese : https://www.fortinet.com/support/product-downloads (Napomena **FortiClient VPN-only** verzija)

   Alternativno za Windows platformu moguće je preuzeti off-line instaler klijenta sa adrese : https://logindoo-my.sharepoint.com/:u:/g/personal/bruno_smiljanic_login_hr/IQAvcDsakmkgRrOeehjVwRyFAeCn2Z83k4S4Wwh6ag_0Gkg?e=7MOuL1



2. Otvoriti FortiClient VPN konzolu, na hamburger izborniku odabrai Add a new connection



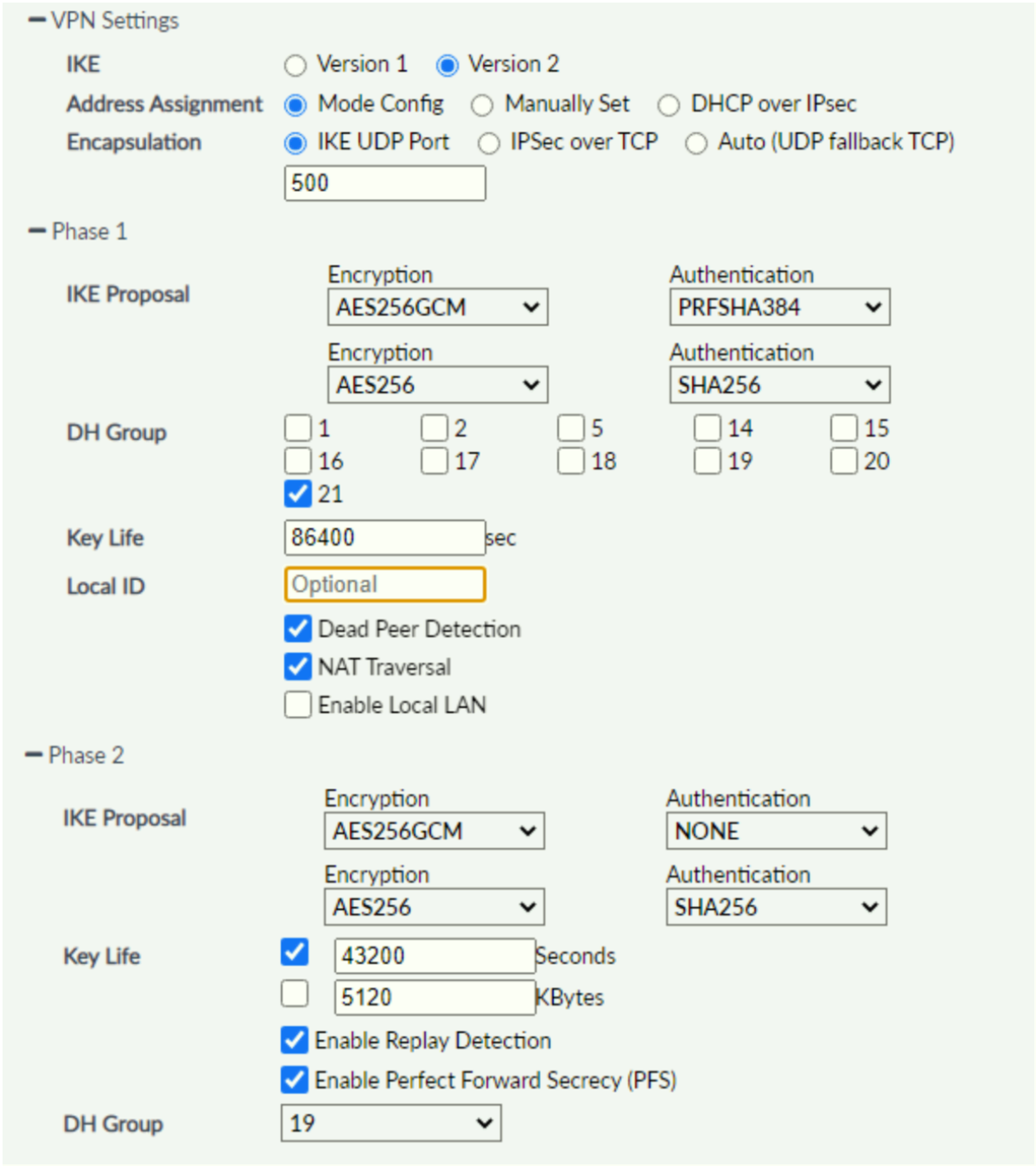
1. Unijeti podatke za kreiranje novog konfiguracijskog profila kako slijedi:

U polje prazno polje Pre-shared key upisati: c4NUVBt46fN0zmwvecG8

Provjeriti da su ostale crveno označene postavke odabrane, te da je u polje SSO port upisano 11001

2. Kliknuti na znak + pored Advanced Settings i upisati podatke u sekcije VPN Settings, Phase 1 i Phase 2 kako slijedi:

Local ID: Istratech


VPN Settings
IKE
Version 1
Version 2
Address Assignment
Mode Config
Manually Set
DHCP over IPsec
Encapsulation
IKE UDP Port
IPSec over TCP
Auto (UDP fallback TCP)
500
Phase 1
IKE Proposal
Encryption
AES256GCM
Authentication
PRFSHA384
Encryption
AES256
Authentication
SHA256
DH Group
1
2
5
14
15
16
17
18
19
20
21
Key Life
86400
sec
Local ID
Optional
Dead Peer Detection
NAT Traversal
Enable Local LAN
Phase 2
IKE Proposal
Encryption
AES256GCM
Authentication
NONE
Encryption
AES256
Authentication
SHA256
Key Life
43200
Seconds
5120
KBytes
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)
DH Group
19

Konfiguracija MFA tokena

Prilikom prvog korištenja VPN-a potrebno je izvršiti aktivaciju multi-faktorske autentikacije putem M365 servisa te povezati korisnički račun sa MFA aplikacijom (Microsoft Authenticator aplikacija je dostupna preko Gogole Play Store-a ili Apple App Store-a)

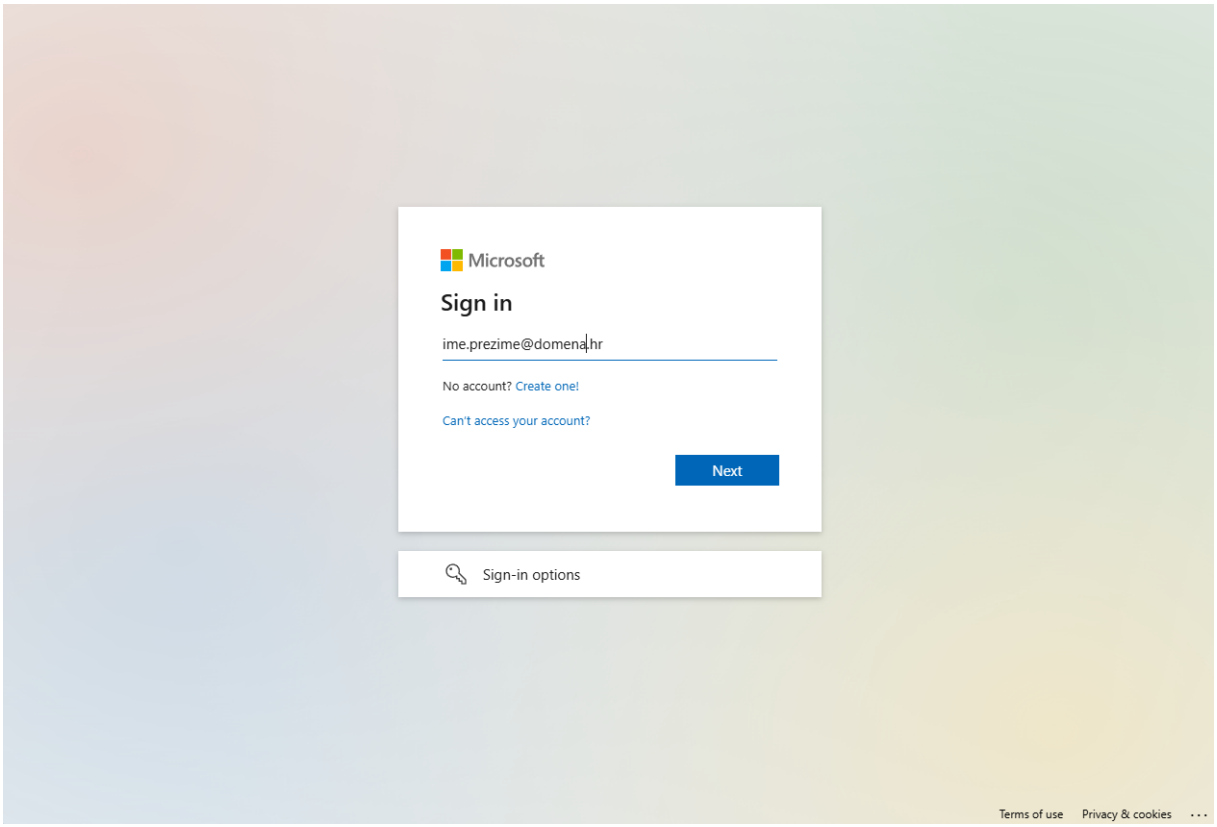
Napomena : pripaziti prilikom preuzimanja aplikacije da se odabere ispravna. Ikona ili logo ispravne aplikacije je :

Za navedeno korisnik se mora prijaviti na M365 račun, dok korisničko iskustvo može minimalno varirati ovisno o platformi:

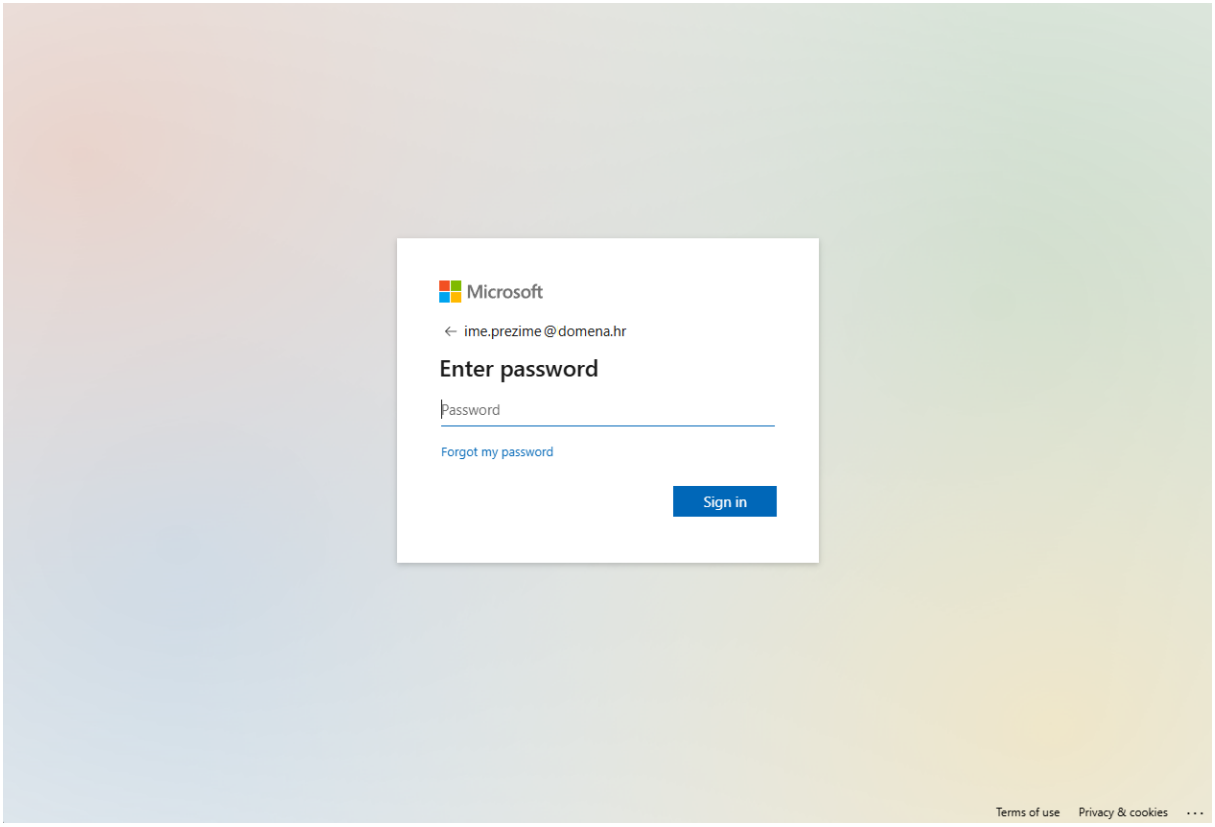
- Putem M365 portala – portal.office.com

Primjer prijave putem portal.office.com :

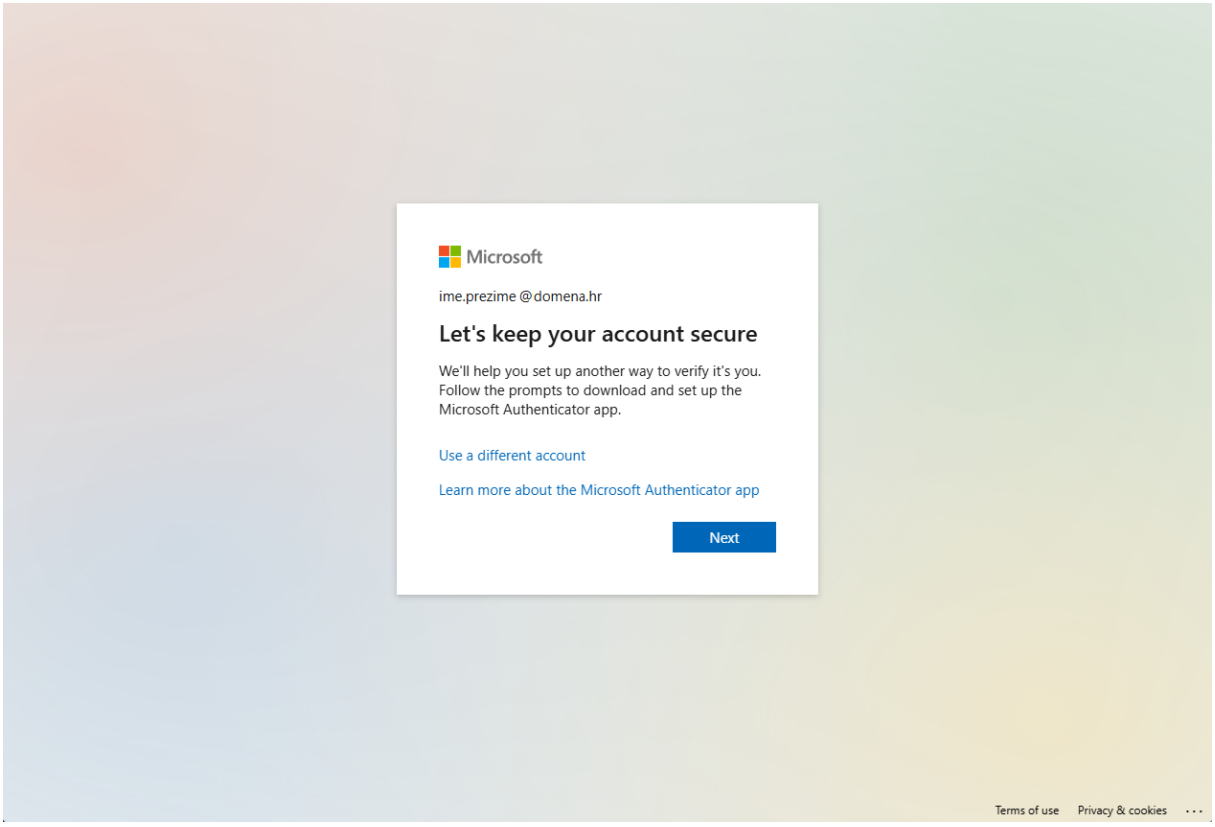
1. Odabrati sign-in na prvom sušelju stranice
2. Unjeti dodjeljeno korisničko ime (ime.prezime@login.hr, odnosno Vaše dosadašnje VPN korisničko ime na login.hr domeni, ime.prezime odgovara dosadašnjem korisničkom imenu) i odabrati next



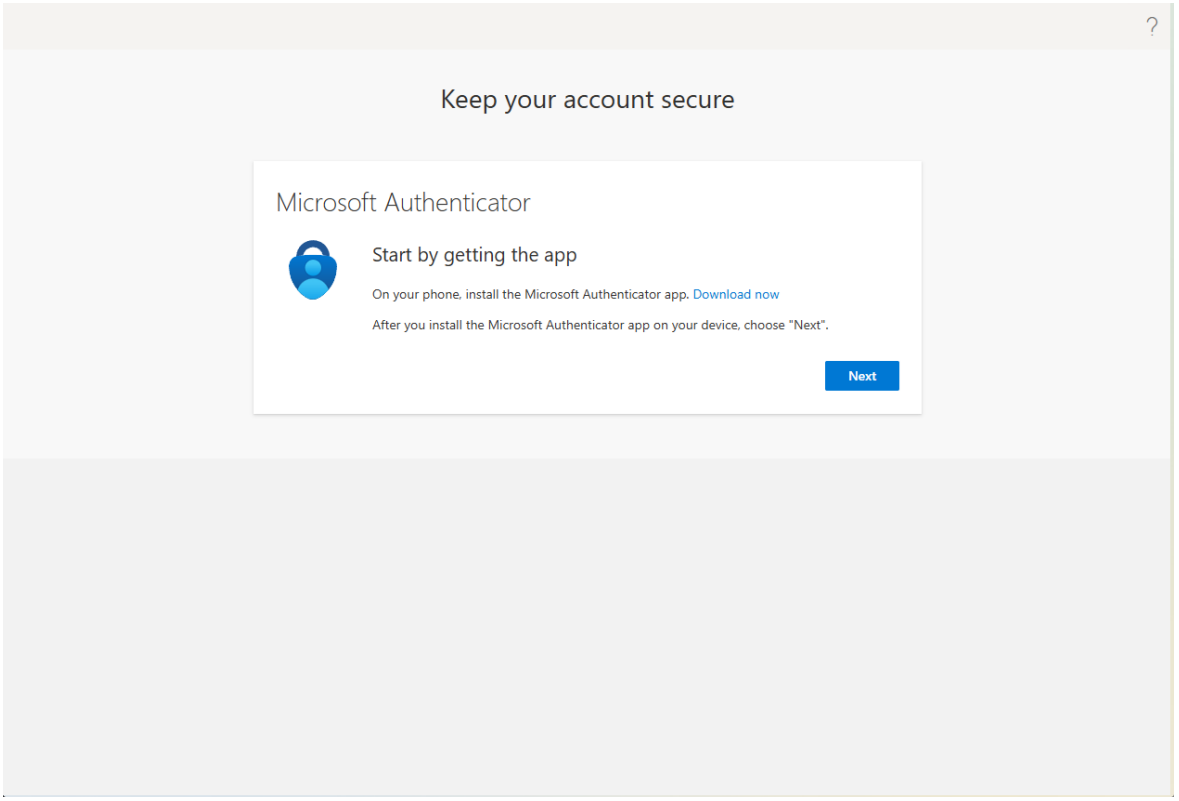
3. Na sljedećem sučelju potrebno je unjeti dodjeljenu lozinku i odabrati sign in



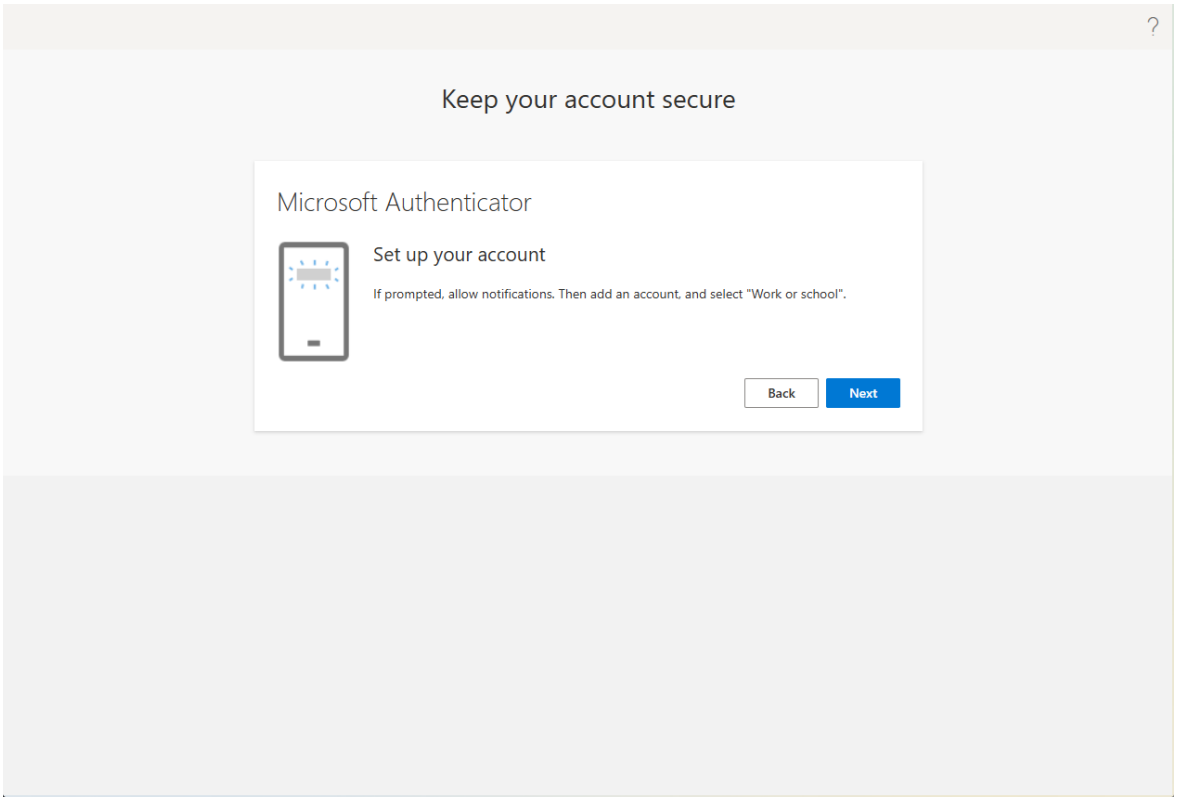
4. Odabrati next



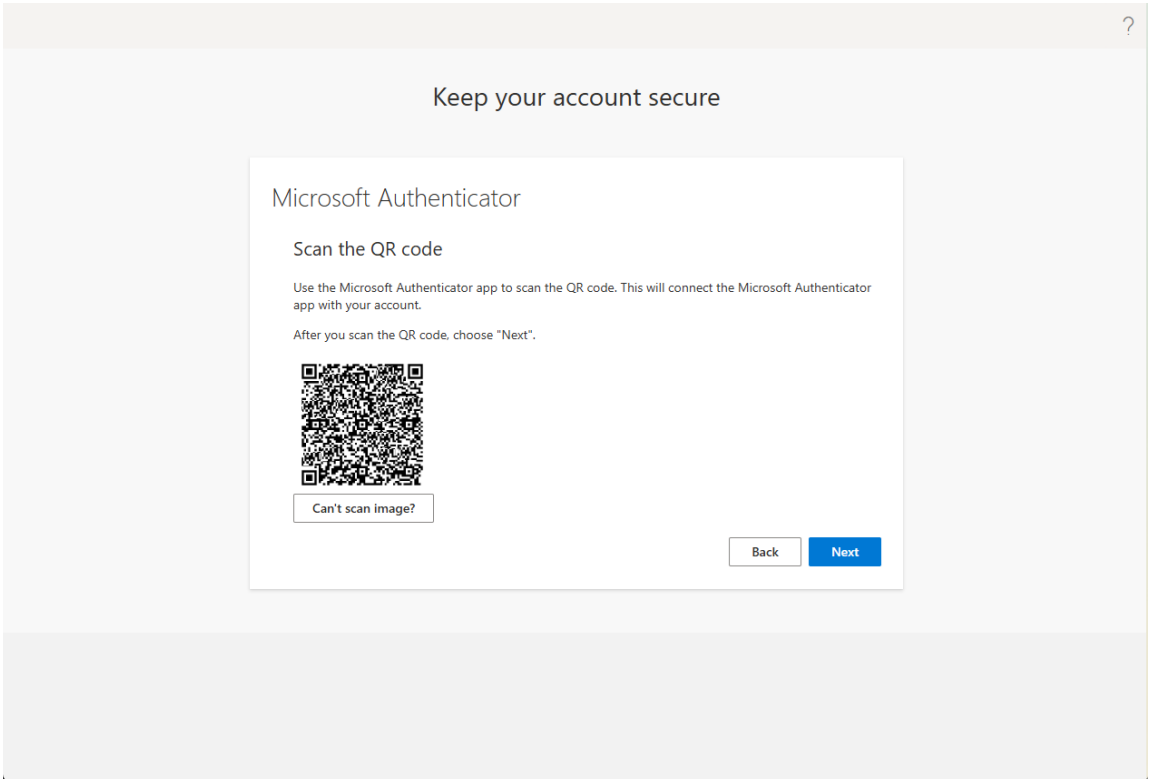
5. Preuzeti na mobilni uređaj authenticator aplikaciju i odabrati next



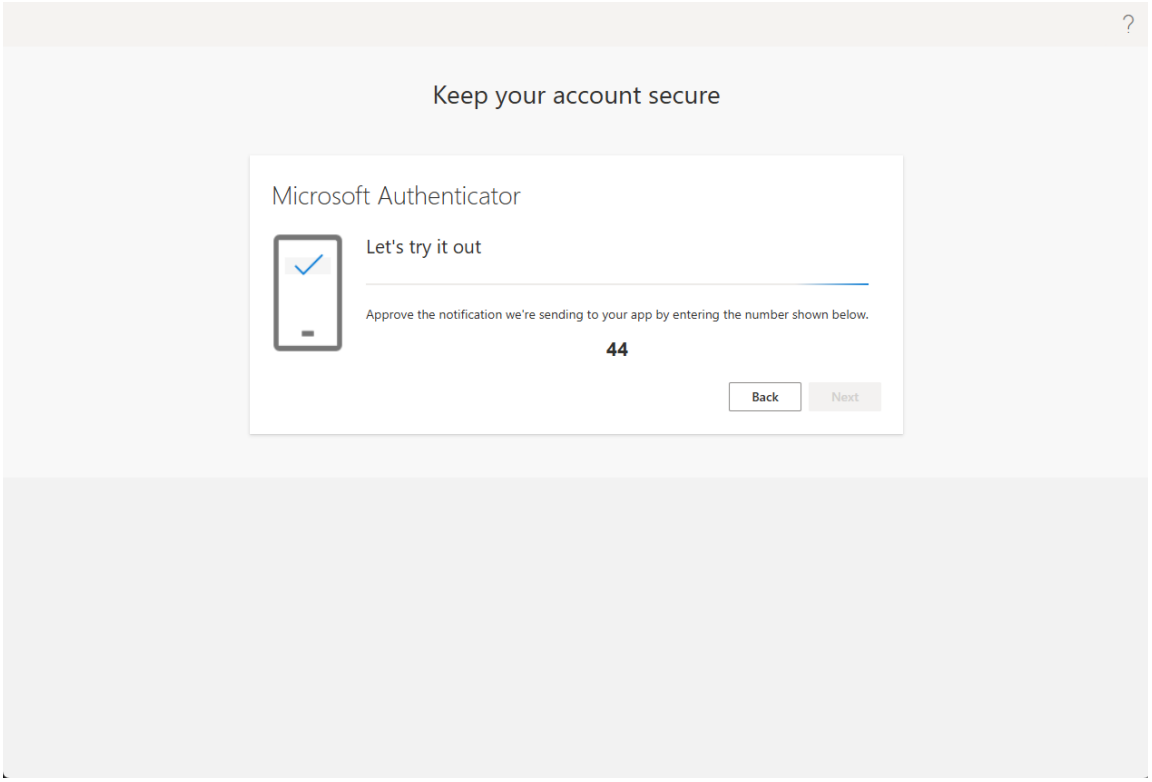
6. U sučelju odabrati next, a na mobilnom uređaju u aplikaciji odabrati znak + I odavrati Work or school account



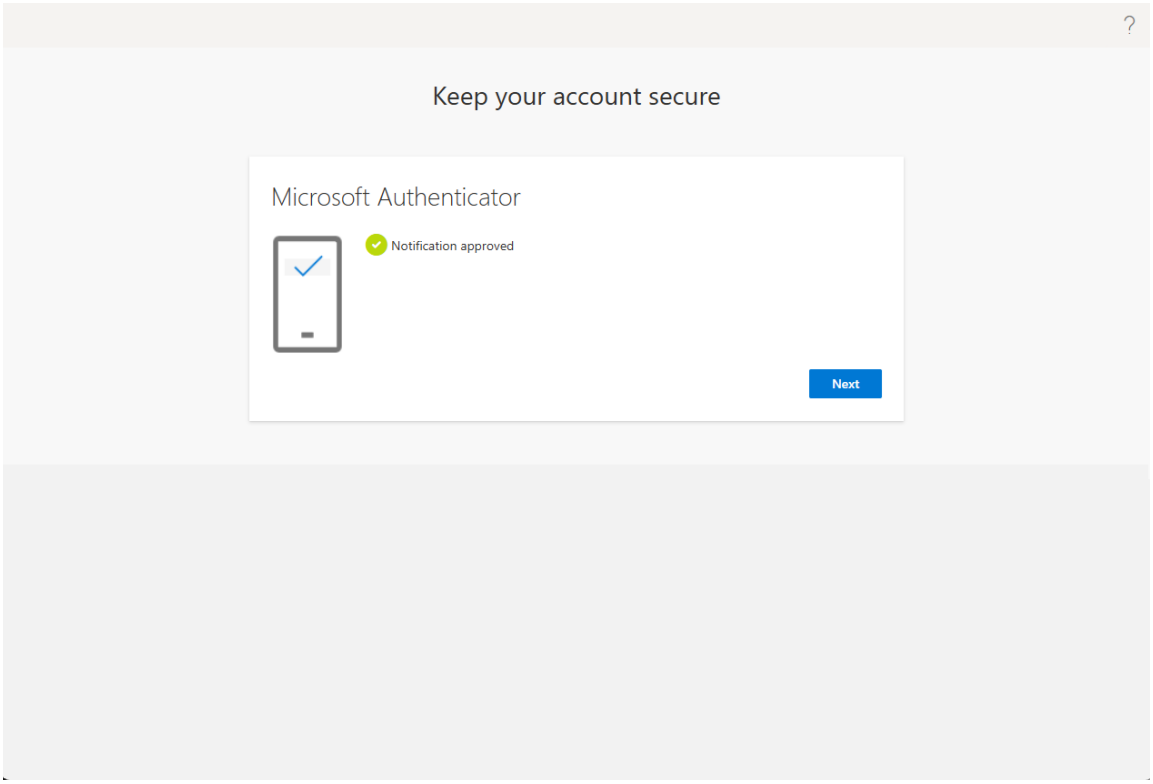
7. Sa mobilnom aplikacijom skenirati QR kod i odabrati next



8. Unjeti na mobilnom uređaju u novo otvorenom prozoru broj prikazan na ekranu



9. Odabrati next



10. Odabrati done