Home > Perparims Cloud Solutions >

Perparims Cloud Solutions ...

How to Enable and Test MFA in Microsoft Entra ID

Real-world lab walkthrough by Perparim Abdullahu

Perparim Abdullahu
Azure Solutions Architect |
SC-300 in Progress
#PerparimLabs

Microsoft CERTIFIED
EXPERT

Why MFA Matters

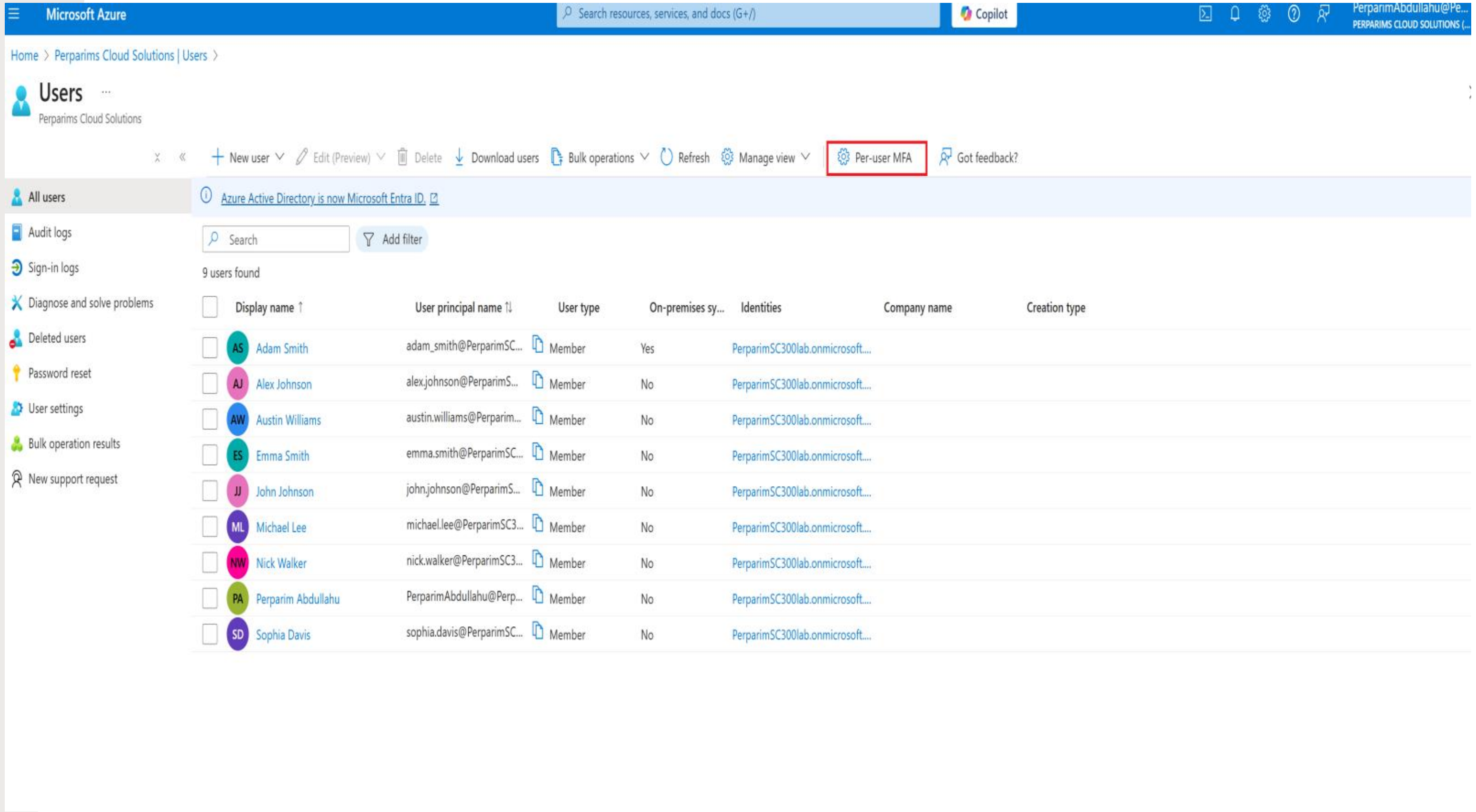
- MFA protects identities using 2+ verification factors.
- Prevents phishing, stolen passwords, and remote logins.
- Required by Zero Trust, NIST, CIS, and other standards.

Step 1 – **Go to Per-user MFA Settings**

- **Lab Action:**

- Go to: Microsoft Entra ID > Users

- Click the ⋯ **(three dots)** in the top-right > Select **Per-user MFA**



9 users found

Display name ↑	User principal name ↑↓	User type	On-premises sy...	Identities	Company name	Creation type
AS Adam Smith	adam_smith@PerparimSC...	Member	Yes	PerparimSC300lab.onmicrosoft....		
AJ Alex Johnson	alex.johnson@PerparimS...	Member	No	PerparimSC300lab.onmicrosoft....		
AW Austin Williams	austin.williams@Perparim...	Member	No	PerparimSC300lab.onmicrosoft....		
ES Emma Smith	emma.smith@PerparimSC...	Member	No	PerparimSC300lab.onmicrosoft....		
JJ John Johnson	john.johnson@PerparimS...	Member	No	PerparimSC300lab.onmicrosoft....		
ML Michael Lee	michael.lee@PerparimSC3...	Member	No	PerparimSC300lab.onmicrosoft....		
NW Nick Walker	nick.walker@PerparimSC3...	Member	No	PerparimSC300lab.onmicrosoft....		
PA Perparim Abdullahu	PerparimAbdullahu@Perp...	Member	No	PerparimSC300lab.onmicrosoft....		
SD Sophia Davis	sophia.davis@PerparimSC...	Member	No	PerparimSC300lab.onmicrosoft....		

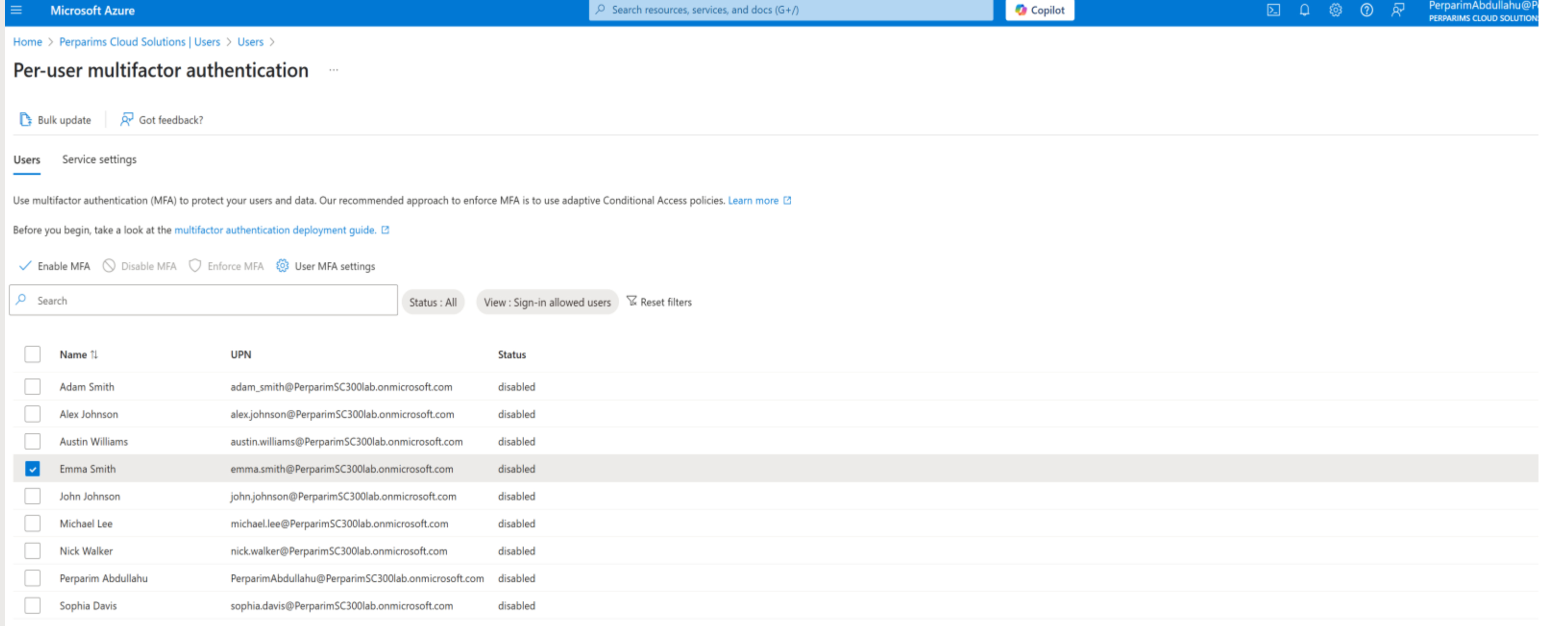
Step 2 – Enable & Enforce MFA for Test User

Lab Action:

1.Find a user like TestUser1

2.Click the checkbox > Click **Enable** > Confirm

3.Then click **Enforce** to make it mandatory

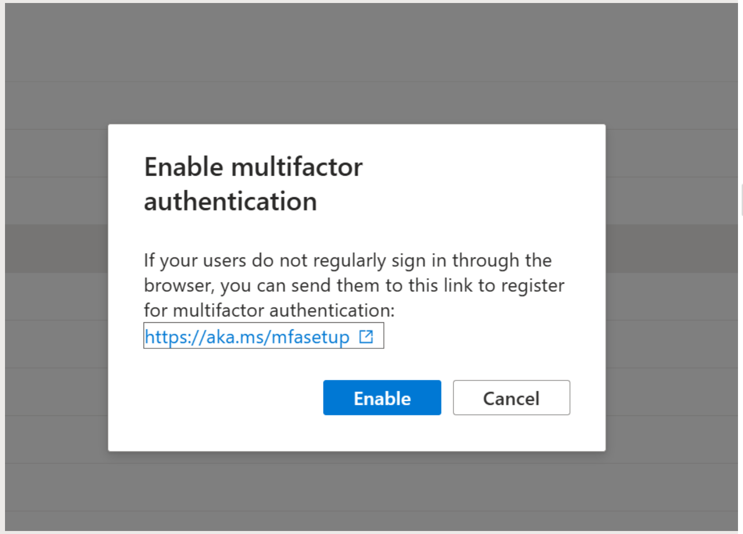


Per-user multifactor authentication

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

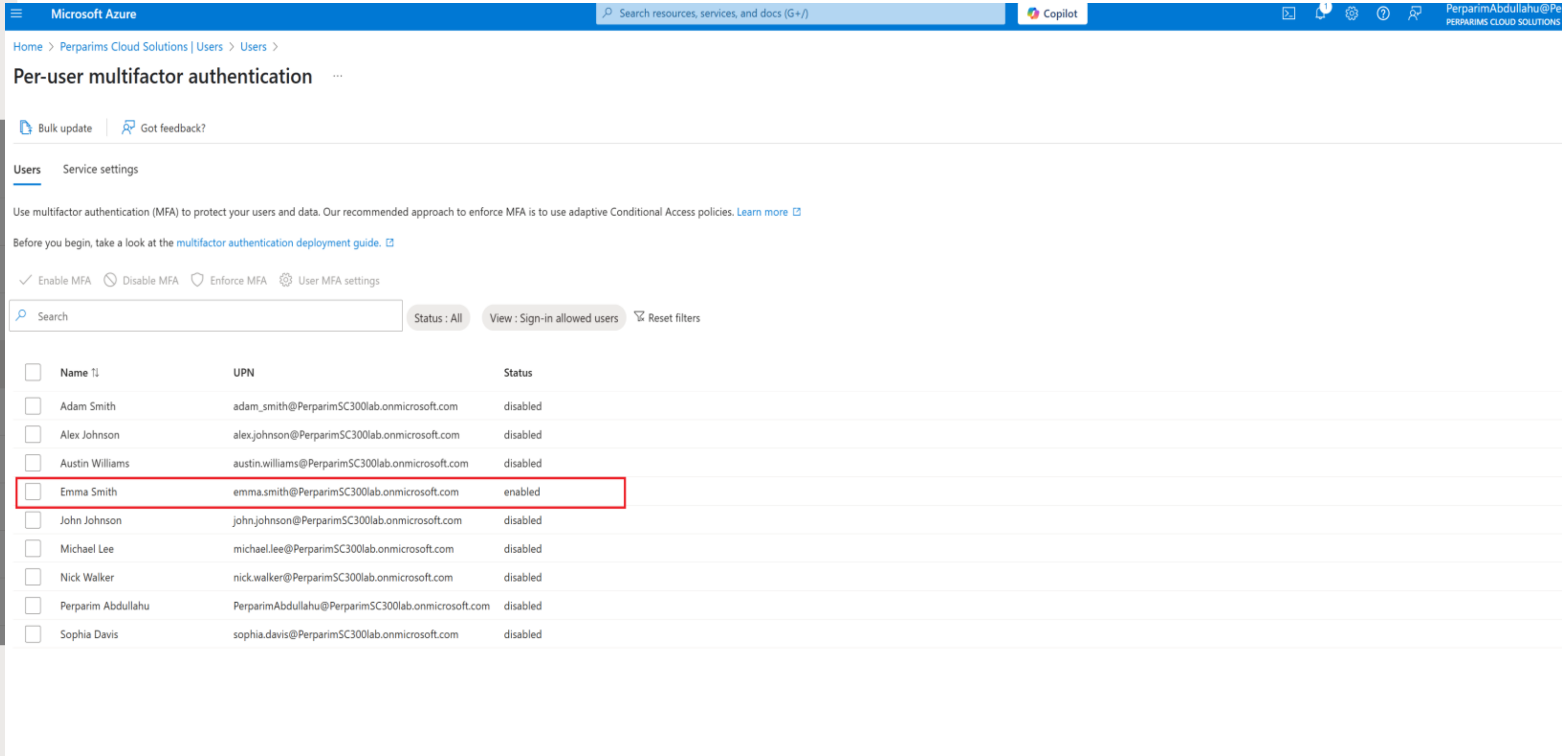
Before you begin, take a look at the multifactor authentication deployment guide.

□	Name ⇅	UPN	Status
□	Adam Smith	adam_smith@PerparimSC300lab.onmicrosoft.com	disabled
□	Alex Johnson	alex.johnson@PerparimSC300lab.onmicrosoft.com	disabled
□	Austin Williams	austin.williams@PerparimSC300lab.onmicrosoft.com	disabled
☑	Emma Smith	emma.smith@PerparimSC300lab.onmicrosoft.com	disabled
□	John Johnson	john.johnson@PerparimSC300lab.onmicrosoft.com	disabled
□	Michael Lee	michael.lee@PerparimSC300lab.onmicrosoft.com	disabled
□	Nick Walker	nick.walker@PerparimSC300lab.onmicrosoft.com	disabled
□	Perparim Abdullahu	PerparimAbdullahu@PerparimSC300lab.onmicrosoft.com	disabled
□	Sophia Davis	sophia.davis@PerparimSC300lab.onmicrosoft.com	disabled



Enable multifactor authentication

If your users do not regularly sign in through the browser, you can send them to this link to register for multifactor authentication:
https://aka.ms/mfasetup



Per-user multifactor authentication

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

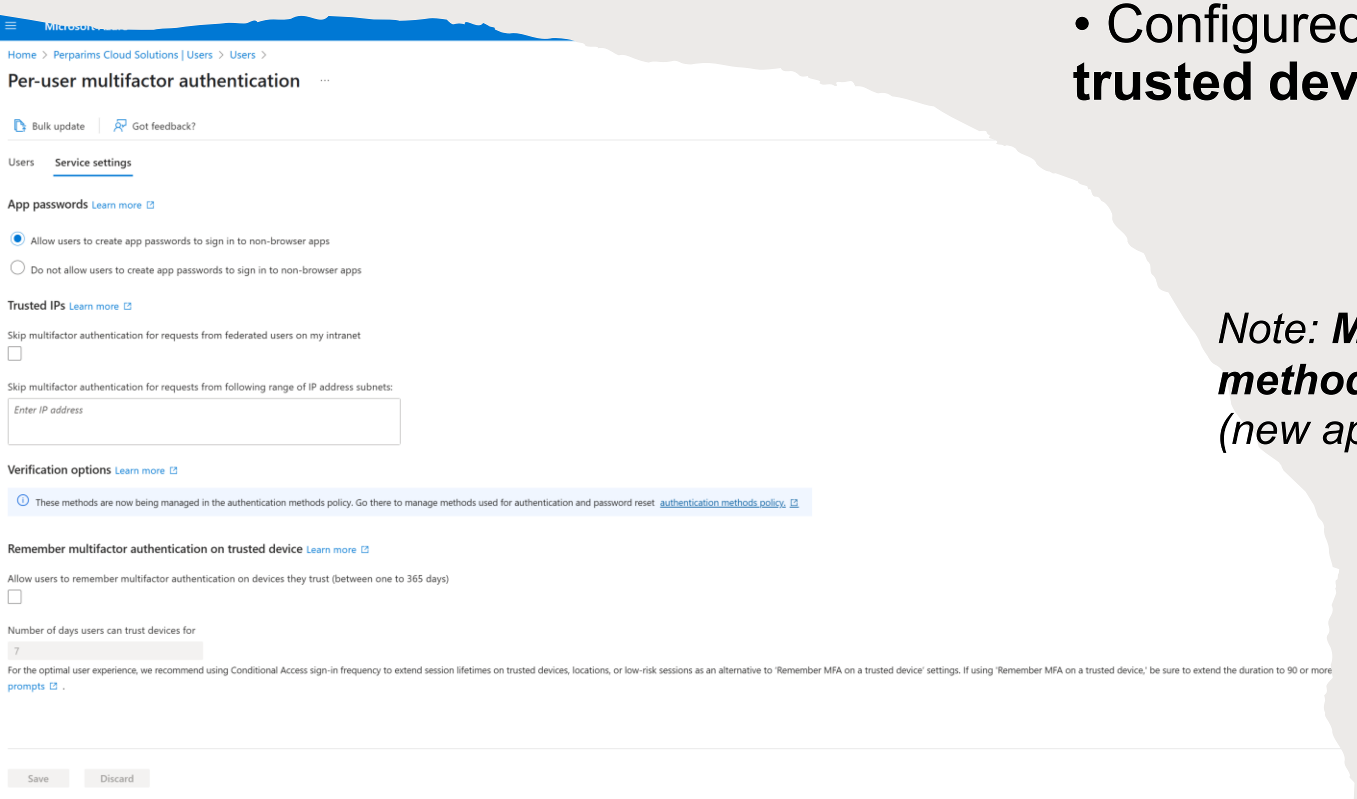
Before you begin, take a look at the multifactor authentication deployment guide.

□	Name ⇅	UPN	Status
□	Adam Smith	adam_smith@PerparimSC300lab.onmicrosoft.com	disabled
□	Alex Johnson	alex.johnson@PerparimSC300lab.onmicrosoft.com	disabled
□	Austin Williams	austin.williams@PerparimSC300lab.onmicrosoft.com	disabled
□	Emma Smith	emma.smith@PerparimSC300lab.onmicrosoft.com	enabled
□	John Johnson	john.johnson@PerparimSC300lab.onmicrosoft.com	disabled
□	Michael Lee	michael.lee@PerparimSC300lab.onmicrosoft.com	disabled
□	Nick Walker	nick.walker@PerparimSC300lab.onmicrosoft.com	disabled
□	Perparim Abdullahu	PerparimAbdullahu@PerparimSC300lab.onmicrosoft.com	disabled
□	Sophia Davis	sophia.davis@PerparimSC300lab.onmicrosoft.com	disabled

Step 3 – Manage MFA Service Settings

- Disabled legacy **App passwords** to improve security.
- Skipped MFA for trusted **IP addresses** and **federated users** if needed.
- Configured the option to **“Remember MFA on trusted devices”** (e.g., 7–90 days).

*Note: **Microsoft now manages MFA methods** under **Authentication Methods** (new approach).*



Home > Perparims Cloud Solutions | Users > Users >

Per-user multifactor authentication ···

App passwords Learn more

● Allow users to create app passwords to sign in to non-browser apps

○ Do not allow users to create app passwords to sign in to non-browser apps

Trusted IPs Learn more

Skip multifactor authentication for requests from federated users on my intranet

□

Skip multifactor authentication for requests from following range of IP address subnets:

Enter IP address

Verification options Learn more

ⓘ These methods are now being managed in the authentication methods policy. Go there to manage methods used for authentication and password reset authentication methods policy.

Remember multifactor authentication on trusted device Learn more

Allow users to remember multifactor authentication on devices they trust (between one to 365 days)

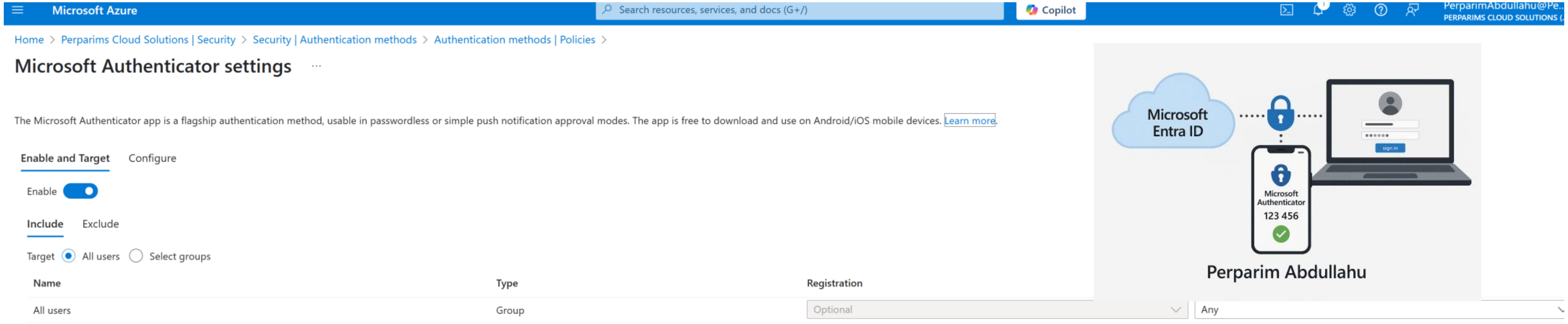
□

Number of days users can trust devices for

7

For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more

prompts .



Home > Perparims Cloud Solutions | Security > Security | Authentication methods > Authentication methods | Policies >

Microsoft Authenticator settings ...

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more

Enable and Target | Configure

Enable: on

Include | Exclude

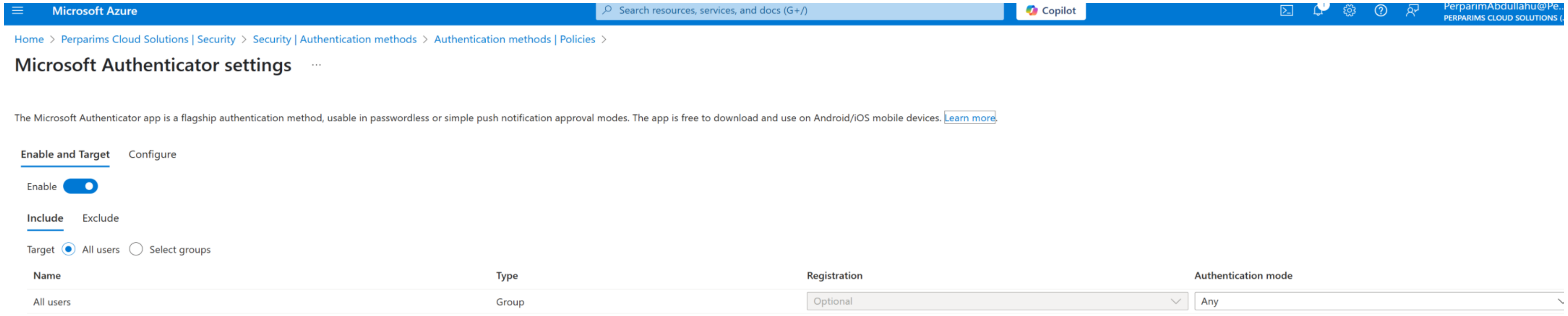
Target ● All users ○ Select groups

Name	Type	Registration	
All users	Group	Optional	Any

Step 4 – Enable Microsoft Authenticator for MFA

- Enabled Microsoft Authenticator app for MFA.
- Scoped to All Users or specific group (depending on your config).
- This is the **modern, recommended method** to enforce MFA registration.
- Authentication methods like FIDO2, SMS can be added similarly.

Authentication method settings have moved here to provide unified control over both MFA and Self-Service Password Reset (SSPR).


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
PerparimAbdullahu@Pe..
PERPARIMS CLOUD SOLUTIONS (.

Home > Perparims Cloud Solutions | Security > Security | Authentication methods > Authentication methods | Policies >

Microsoft Authenticator settings ...

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more

Enable and Target   Configure

Enable ●

Include   Exclude

Target ● All users ○ Select groups

Name	Type	Registration	Authentication mode
All users	Group	Optional	Any

Configure MFA Authentication Methods

Lab Action:

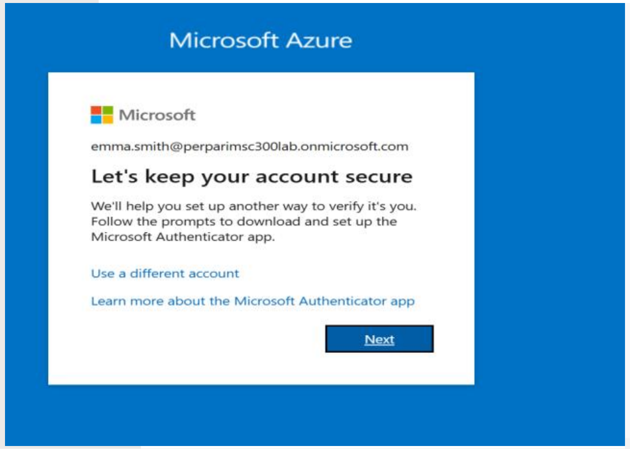
1.Go to: Microsoft Entra ID > Security > Authentication Methods

2.Click on **Microsoft Authenticator** > Enable for All Users

3.(Optional) Enable FIDO2 or SMS

Step 5 – Test User MFA Registration Experience

- Logged in as the test user after enforcing MFA.
- Prompted to register an MFA method (e.g., Microsoft Authenticator App).
- User can scan QR code or set up via phone number/SMS.
- **Required by policy** if Enforced via per-user MFA or Conditional Access.



Microsoft Azure

Microsoft

emma.smith@perparimsc300lab.onmicrosoft.com

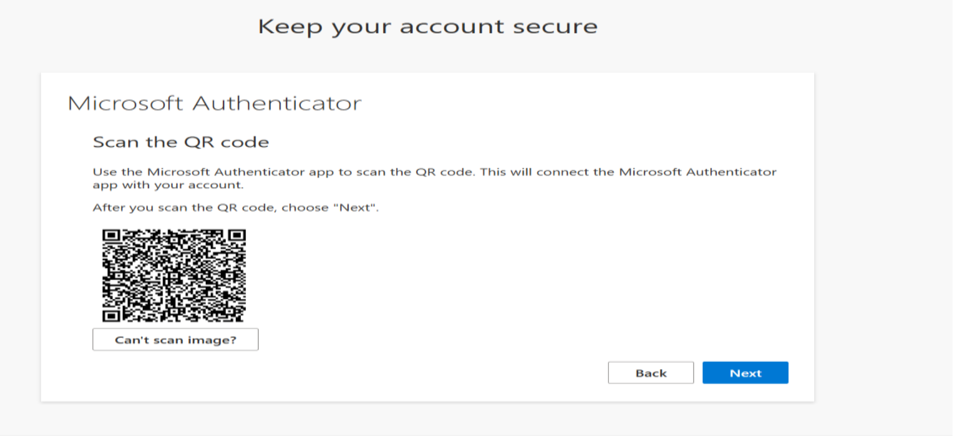
Let's keep your account secure

We'll help you set up another way to verify it's you. Follow the prompts to download and set up the Microsoft Authenticator app.

Use a different account

Learn more about the Microsoft Authenticator app

Next



Keep your account secure

Microsoft Authenticator

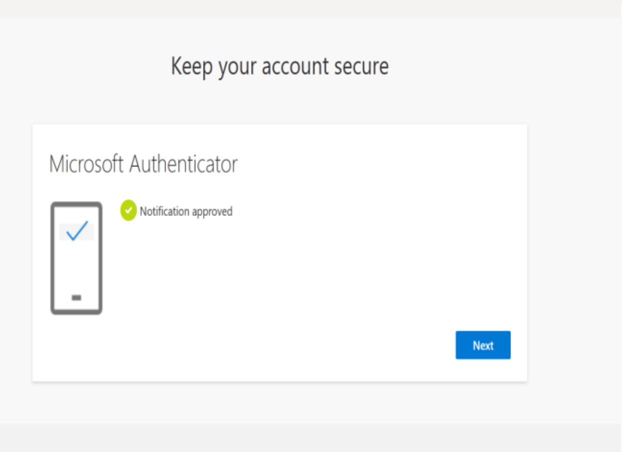
Scan the QR code

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

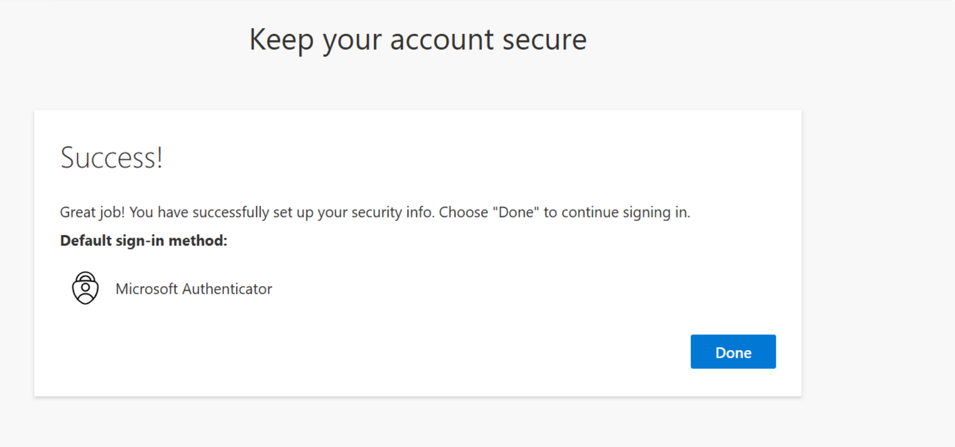


Keep your account secure

Microsoft Authenticator

✓ Notification approved

Next



Keep your account secure

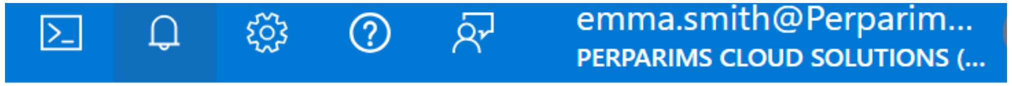
Success!

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

Default sign-in method:

Microsoft Authenticator

Done



emma.smith@Perparim...

PERPARIMS CLOUD SOLUTIONS (...

🔗 *Follow me for more Microsoft Entra labs and SC-300 insights →* **#PerparimLabs**

Using InPrivate/Incognito helps simulate the experience of a fresh sign-in and shows the MFA enforcement in action.

Key Takeaways & Summary

Perparim Abdullahu
Azure Solutions Architect | SC-300 in Progress
#PerparimLabs

- Implemented MFA using **Per-user MFA enforcement** in Microsoft Entra ID.
- Blocked legacy features like **app passwords** for stronger security posture.
- Enabled modern authentication methods like **Microsoft Authenticator App**.
- Simulated end-user experience to show real-world MFA registration.
- Future-proof MFA deployment by using **Authentication Methods** blade.

- ✅ **In enterprise environments**, it's best to enforce MFA using **Conditional Access policies**, allowing for scalable, policy-based control over user groups, locations, risk levels, and device states.
- 🔐 This lab aligns with **Zero Trust principles** by requiring strong, verified user identities before granting access.
- 🎓 Directly maps to **Microsoft SC-300 exam topics**, specifically:
- *"Implement and manage authentication methods“*
- *"Plan, implement, and manage MFA in Microsoft Entra ID*

🔐 **Built in my SC-300 lab using Microsoft Entra ID**
🧠 Follow for more labs, real-world walkthroughs, and identity security demos
📌 **#PerparimLabs | #MicrosoftEntra | #SC300 | #AzureSecurity**
📩 Let’s connect: **linkedin.com/in/perparim-abdullahu-2b0530324**