

Per user MFA

Per-user multi-factor authentication (MFA) is a security feature that requires users to provide two or more forms of verification before they can access an account or resource. In the context of Azure Active Directory (Azure AD), per-user MFA enables organizations to enforce MFA on a per-user basis, rather than applying it globally to all users.

Here's a summary of per-user MFA:

1. **Individual Configuration:** With per-user MFA, administrators can enable multi-factor authentication for specific users or groups within Azure AD. This allows organizations to tailor security measures based on user roles, privileges, or risk factors.
2. **Enhanced Security:** By requiring additional verification steps beyond just a password, per-user MFA adds an extra layer of security to user accounts. This helps prevent unauthorized access, even if passwords are compromised.
3. **Flexible Deployment:** Per-user MFA can be deployed selectively, allowing organizations to prioritize MFA for users with elevated access rights, sensitive data access, or those accessing resources from untrusted locations or devices.
4. **User Experience:** Users experience minimal disruption with per-user MFA, as they are prompted to provide additional verification only when accessing resources that have MFA enforcement enabled for their accounts.
5. **Adaptive Access Policies:** Azure AD's Conditional Access policies can be used in conjunction with per-user MFA to dynamically enforce MFA based on various conditions such as location, device state, or user risk level.
6. **Compliance Requirements:** Per-user MFA helps organizations meet regulatory compliance requirements by implementing stronger authentication mechanisms for users accessing sensitive data or applications.


Overall, per-user multi-factor authentication provides organizations with a flexible and granular approach to enhancing security by requiring additional verification steps for specific users or groups within Azure AD. This helps mitigate the risk of unauthorized access and strengthens overall cybersecurity posture.

In this lab, we're enabling per-user multi-factor authentication (MFA) for specific users in Azure AD. The end goal is to enhance the security of user accounts by requiring additional verification steps beyond just a password. By enabling MFA on a per-user basis, organizations can strengthen access controls and mitigate the risk of unauthorized access to sensitive data or applications.

To begin with the Lab:

1. The prerequisite for this lab is that you should have Microsoft Authenticator App downloaded in your mobile phones.
2. Now to enable MFA you have to be in Users in Microsoft Entra ID.
3. Then choose this option Per-user MFA.

- Now you'll be on the new page from here you can enable the MFA for the user's of your choice. Here we are enabling it for demo user 2.
- For that select demo user 2 then click on Enable.

 pulkitkumar2711_gmail.com#EXT#@pulkitkumar2711gmail.onmicrosoft.com | ?

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](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	demouser1	demouser1@pulkitkumar2711gmail.onmicrosoft.com	Disabled
<input checked="" type="checkbox"/>	demouser2	demouser2@pulkitkumar2711gmail.onmicrosoft.com	Disabled
<input type="checkbox"/>	demouser3	demouser3@pulkitkumar2711gmail.onmicrosoft.com	Disabled
<input type="checkbox"/>	demouser4	demouser4@pulkitkumar2711gmail.onmicrosoft.com	Disabled
<input type="checkbox"/>	ExternalUser	PulkitKumar@CloudFreeks.onmicrosoft.com	Disabled

demouser2
demouser2@pulkitkumar2711gm
quick steps
[Enable](#)
[Manage user settings](#)

- After that it will ask you to verify again, click on enable.



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>

enable multi-factor authcancel

- Then you will get the update successful message.



Updates successful

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

close

8. Now you can also see that MFA is enabled for demo user 2.

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	demouser1	demouser1@pulkitkumar2711gmail.onmicrosoft.com	Disabled
<input checked="" type="checkbox"/>	demouser2	demouser2@pulkitkumar2711gmail.onmicrosoft.com	Enabled

9. After that you have to login with demo user 2 then suddenly get this message that action required. Just click on next.

Microsoft Azure



demouser2@pulkitkumar2711gmail.onmicrosoft.com

Action Required

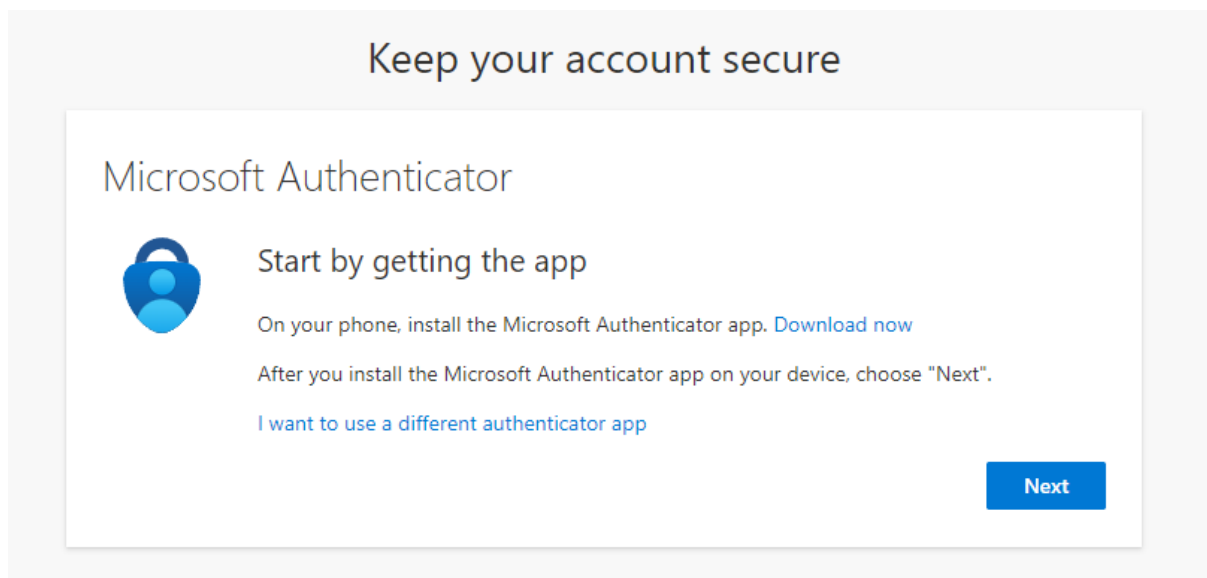
Your organization requires additional security information. Follow the prompts to download and set up the Microsoft Authenticator app.

[Use a different account](#)

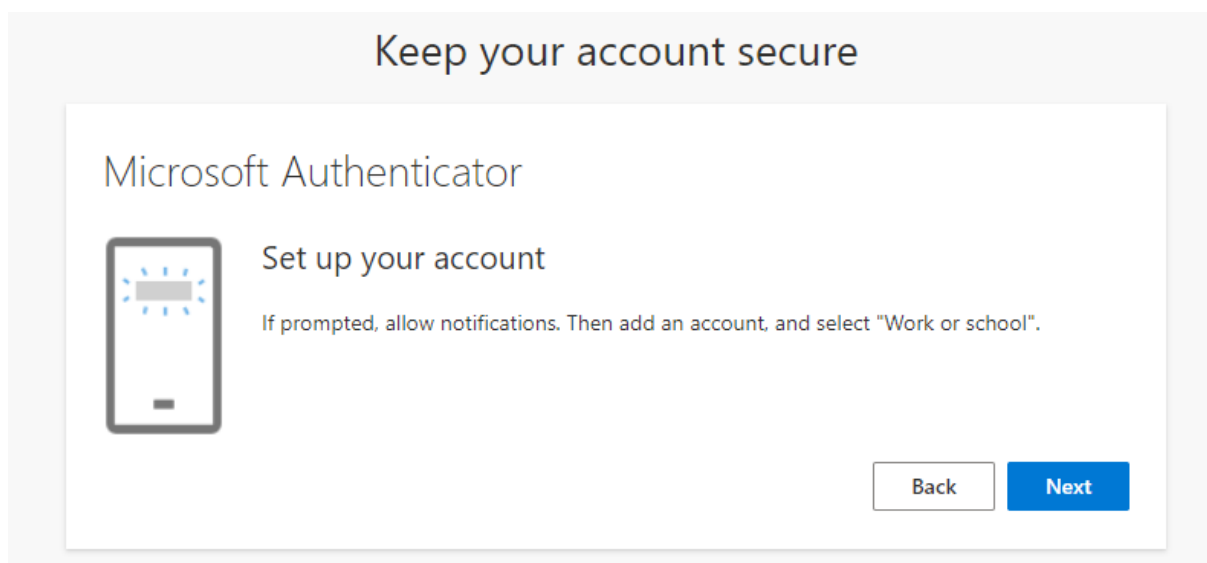
[Learn more about the Microsoft Authenticator app](#)

[Next](#)

10. Then enter your password and login. In case if you are login for the first time then you have to recreate your password do that and then login again.
11. After logging in you will directly be on this screen. Click on next.



12. Now it will ask you to set up your authenticator app.



13. Then you have to scan this QR code in your mobile phone and set the MFA. Then click on 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

14. After scanning it on your mobile device it will ask you to try it out. You have to enter the number shown below in the snapshot in your authenticator app.

Keep your account secure

Microsoft Authenticator



Let's try it out

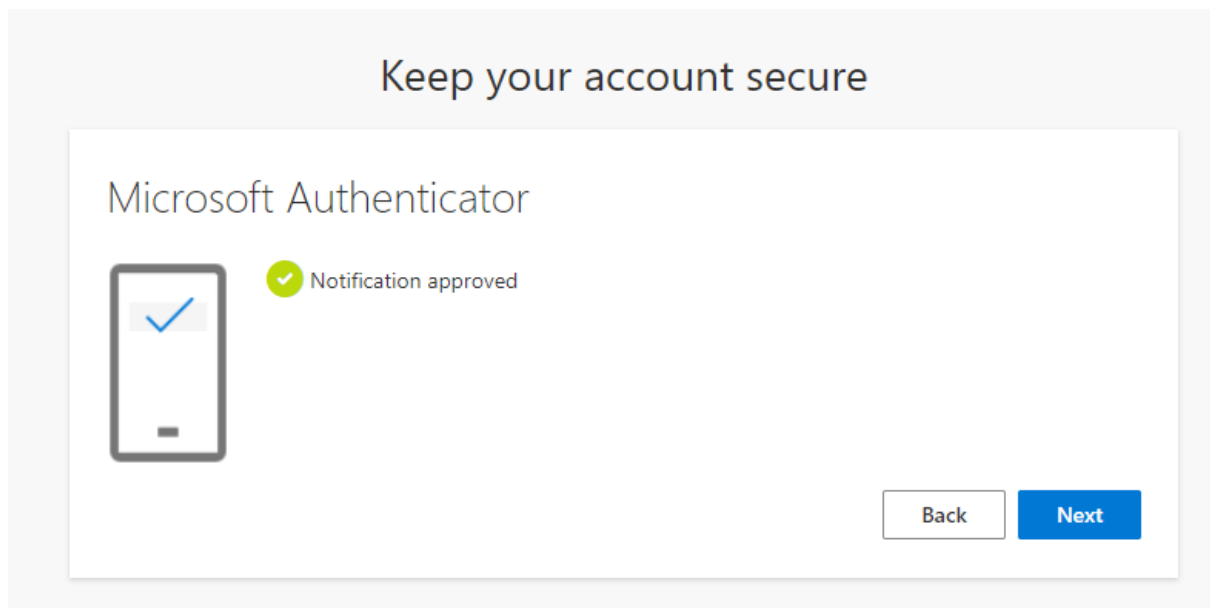
Approve the notification we're sending to your app by entering the number shown below.

92

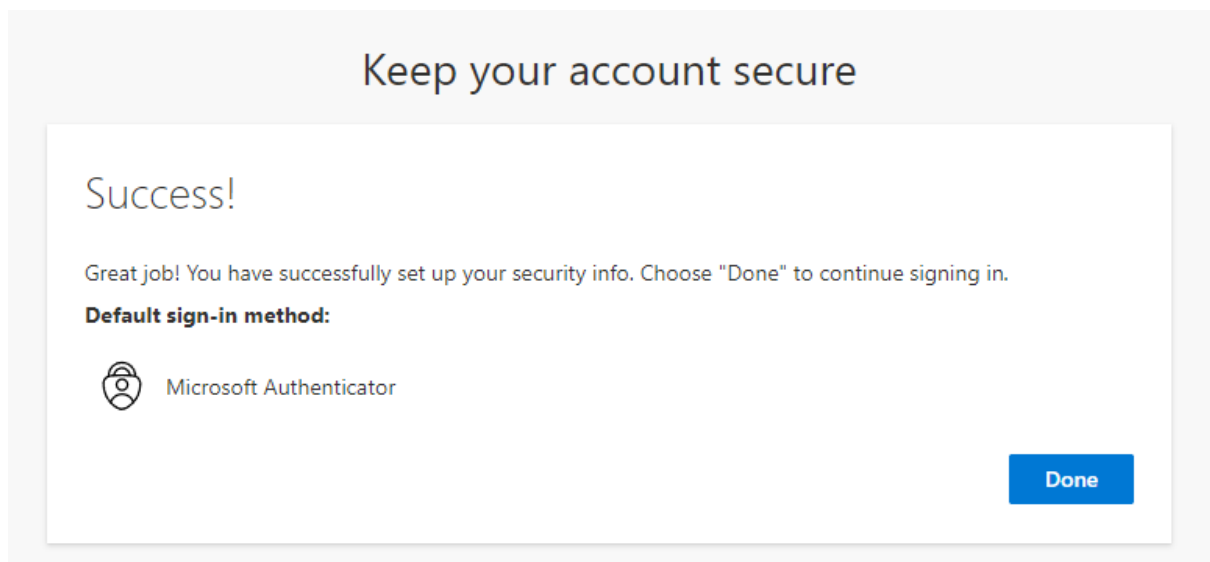
Back

Next

15. Then you will get the approved message.



16. After that the success message.



17. Then you have to re-login to check whether it is working or not. First it will ask you your password then it will ask you to type the number in the authenticator app.

Microsoft Azure



demouser2@pulkitkumar2711gmail.onmicrosoft.com

Approve sign in request



Open your Authenticator app, and enter the number shown to sign in.

23

No numbers in your app? Make sure to upgrade to the latest version.

[I can't use my Microsoft Authenticator app right now](#)

[More information](#)