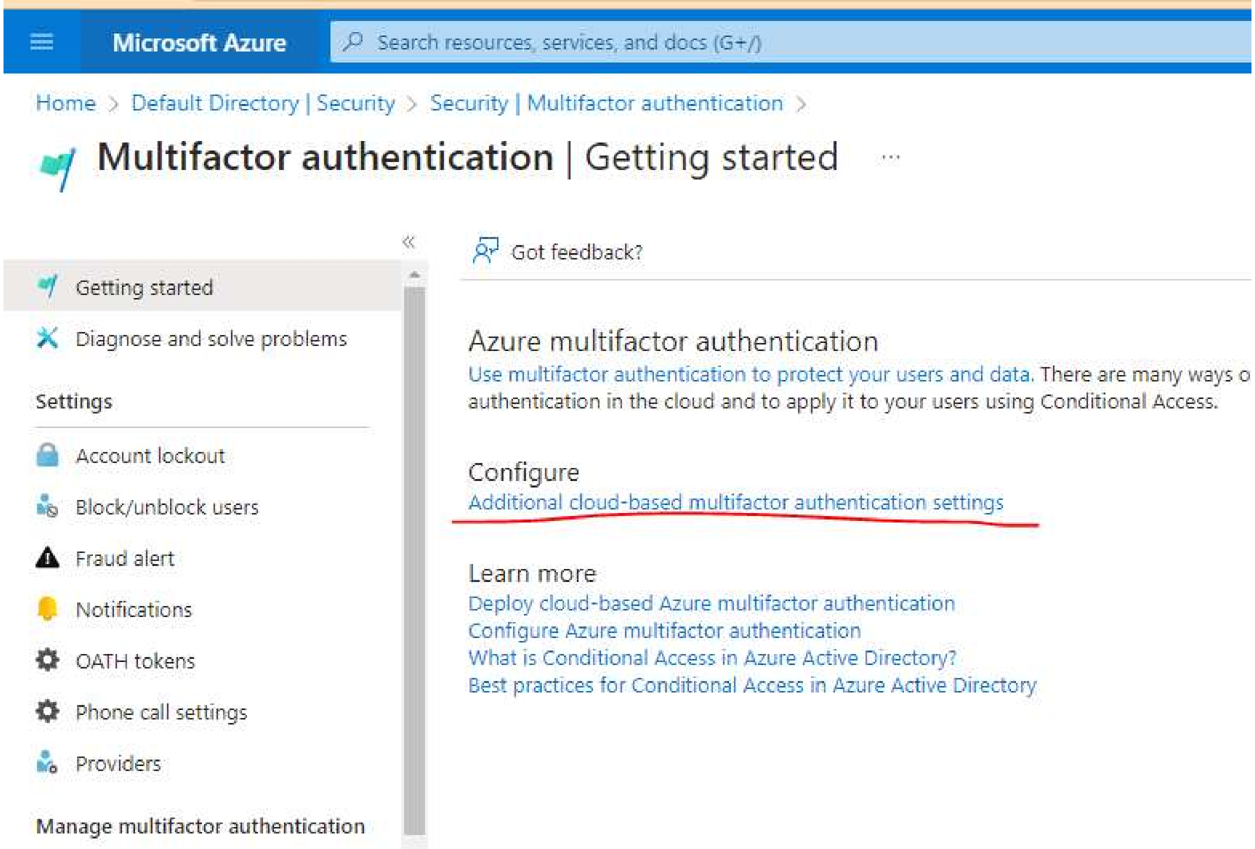
Azure AD (AAD)- MFA - Demo

Following are the steps to be followed to enable MFA for users.

Note - Even after disabling MFA for some users, if you get below screen (this is related to security default settings, not exactly MFA), and if you want to disable it (not recommended by MS), follow step starting from 8.

1. Login to Azure portal as Global Admin and go to Azure Active Directory and go to "Security"
2. Select "Multifactor authentication" from left side menu.
3. Click "Additional cloud-based multifactor authentication settings"



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | Security > Security | Multifactor authentication >
Multifactor authentication | Getting started ...
Got feedback?
Getting started
Diagnose and solve problems
Settings
Account lockout
Block/unblock users
Fraud alert
Notifications
OATH tokens
Phone call settings
Providers
Manage multifactor authentication

Azure multifactor authentication

Use multifactor authentication to protect your users and data. There are many ways o authentication in the cloud and to apply it to your users using Conditional Access.

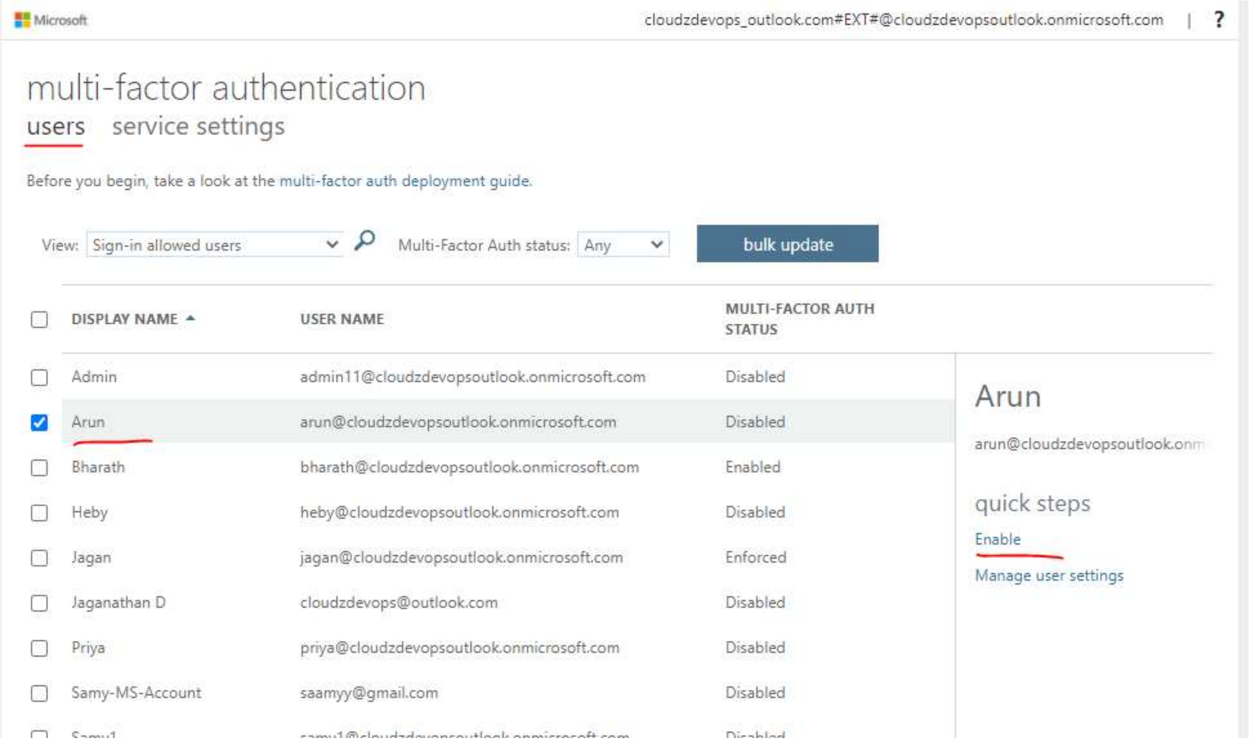
Configure

Additional cloud-based multifactor authentication settings

Learn more

Deploy cloud-based Azure multifactor authentication
Configure Azure multifactor authentication
What is Conditional Access in Azure Active Directory?
Best practices for Conditional Access in Azure Active Directory

4. Select the user you want to enable MFA and click "enable"



Microsoft   cloudzdevops_outlook.com#EXT#@cloudzdevopsoutlook.onmicrosoft.com | ?

multi-factor authentication

users   service settings

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

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	Admin	admin11@cloudzdevopsoutlook.onmicrosoft.com	Disabled
☑	Arun	arun@cloudzdevopsoutlook.onmicrosoft.com	Disabled
□	Bharath	bharath@cloudzdevopsoutlook.onmicrosoft.com	Enabled
□	Heby	heby@cloudzdevopsoutlook.onmicrosoft.com	Disabled
□	Jagan	jagan@cloudzdevopsoutlook.onmicrosoft.com	Enforced
□	Jaganathan D	cloudzdevops@outlook.com	Disabled
□	Priya	priya@cloudzdevopsoutlook.onmicrosoft.com	Disabled
□	Samy-MS-Account	saamyy@gmail.com	Disabled
□	Samy1	samy1@cloudzdevopsoutlook.onmicrosoft.com	Disabled

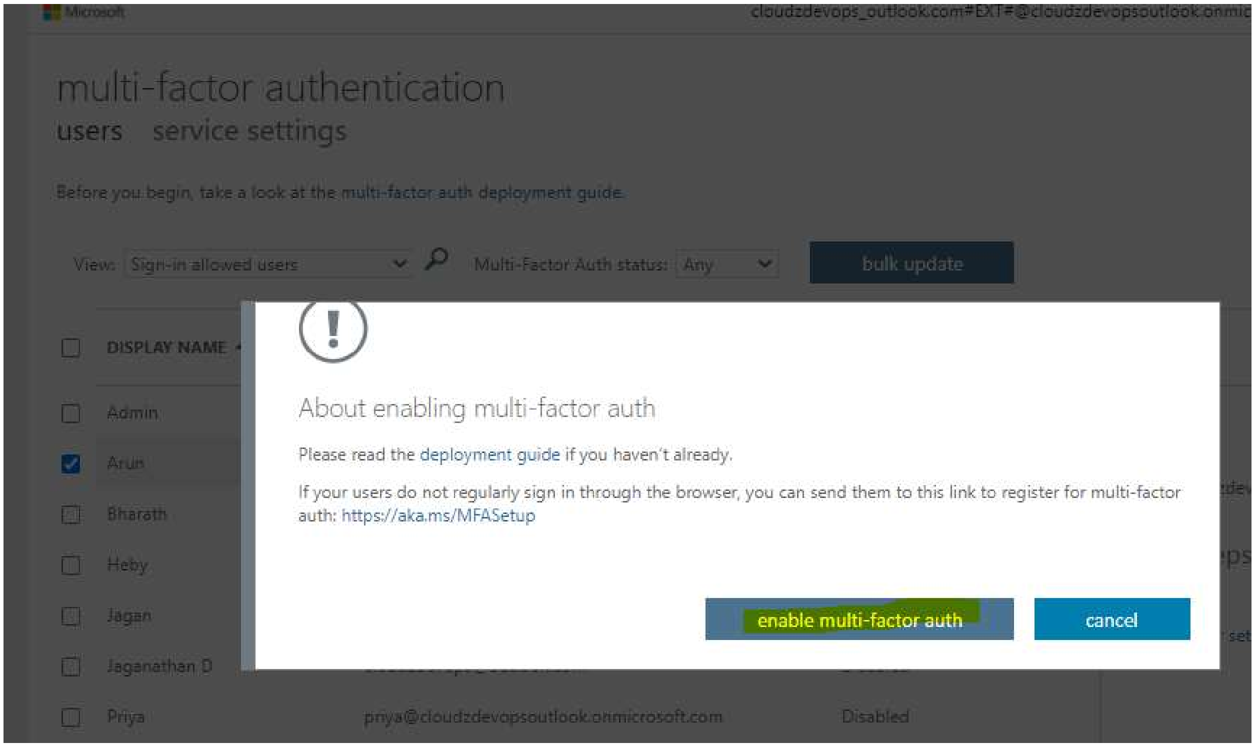
Arun

arun@cloudzdevopsoutlook.onm

quick steps

Enable

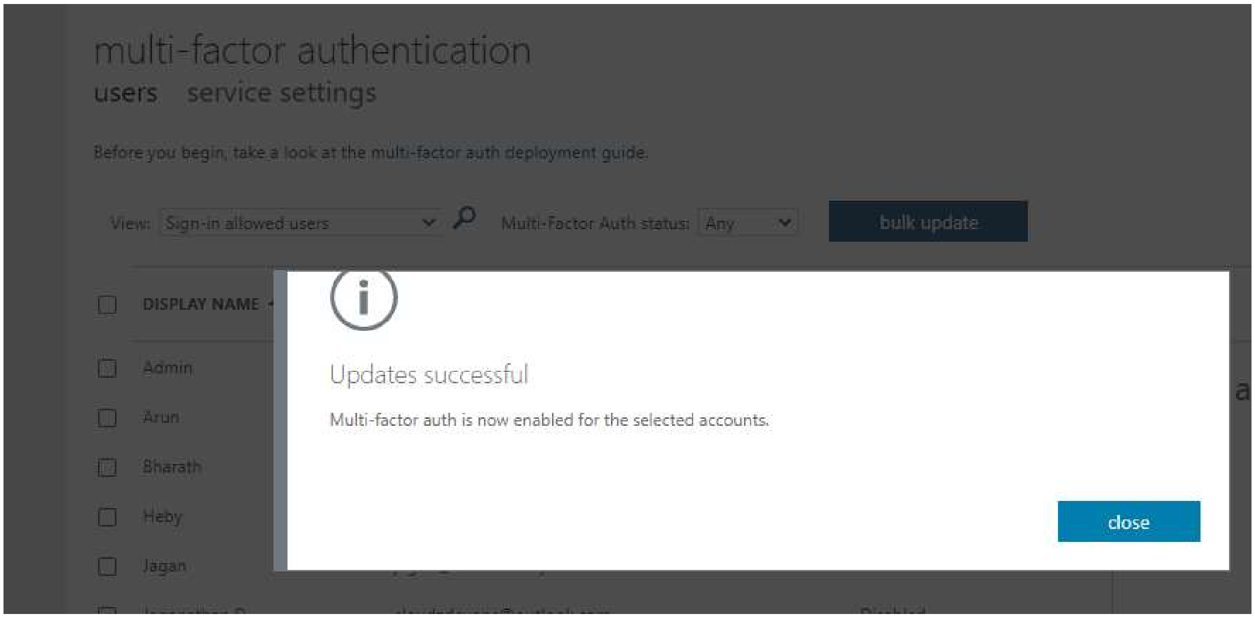
Manage user settings



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



multi-factor authentication

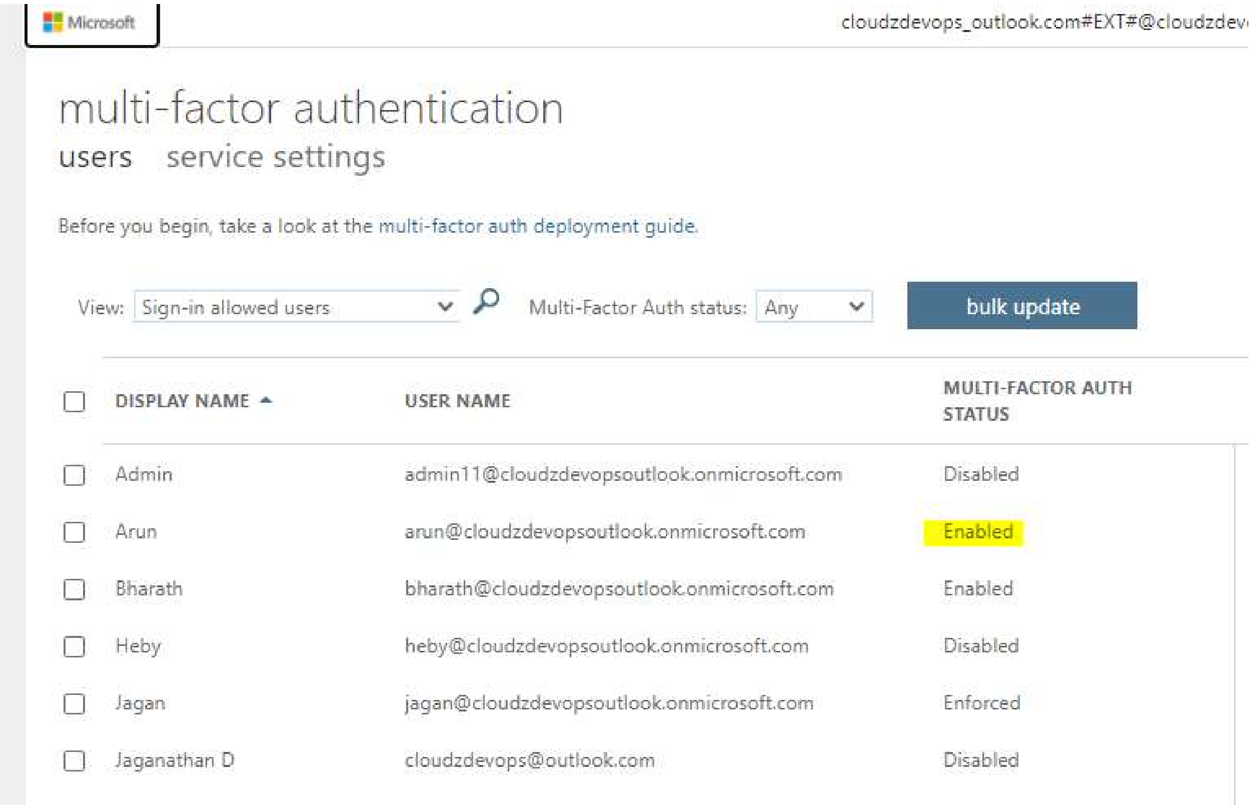
users service settings

Before you begin, take a look at the multi-factor auth deployment guide.

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

Updates successful

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



cloudzdevops_outlook.com#EXT#@cloudzdev

multi-factor authentication

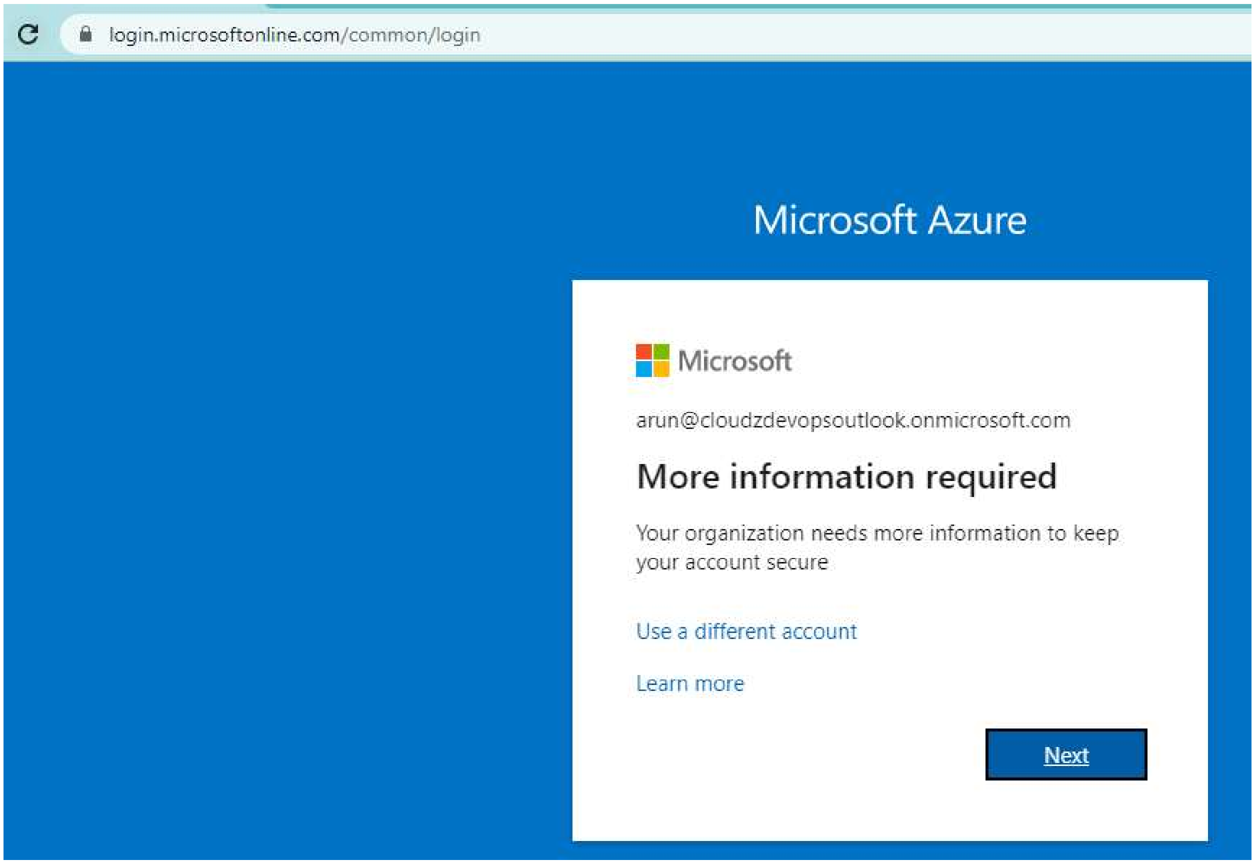
users service settings

Before you begin, take a look at the multi-factor auth deployment guide.

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

☐	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Admin	admin11@cloudzdevopsoutlook.onmicrosoft.com	Disabled
☐	Arun	arun@cloudzdevopsoutlook.onmicrosoft.com	Enabled
☐	Bharath	bharath@cloudzdevopsoutlook.onmicrosoft.com	Enabled
☐	Heby	heby@cloudzdevopsoutlook.onmicrosoft.com	Disabled
☐	Jagan	jagan@cloudzdevopsoutlook.onmicrosoft.com	Enforced
☐	Jaganathan D	cloudzdevops@outlook.com	Disabled

5. Login to portal.azure.com as user “arun” and you’ll be getting below screem



login.microsoftonline.com/common/login

Microsoft Azure

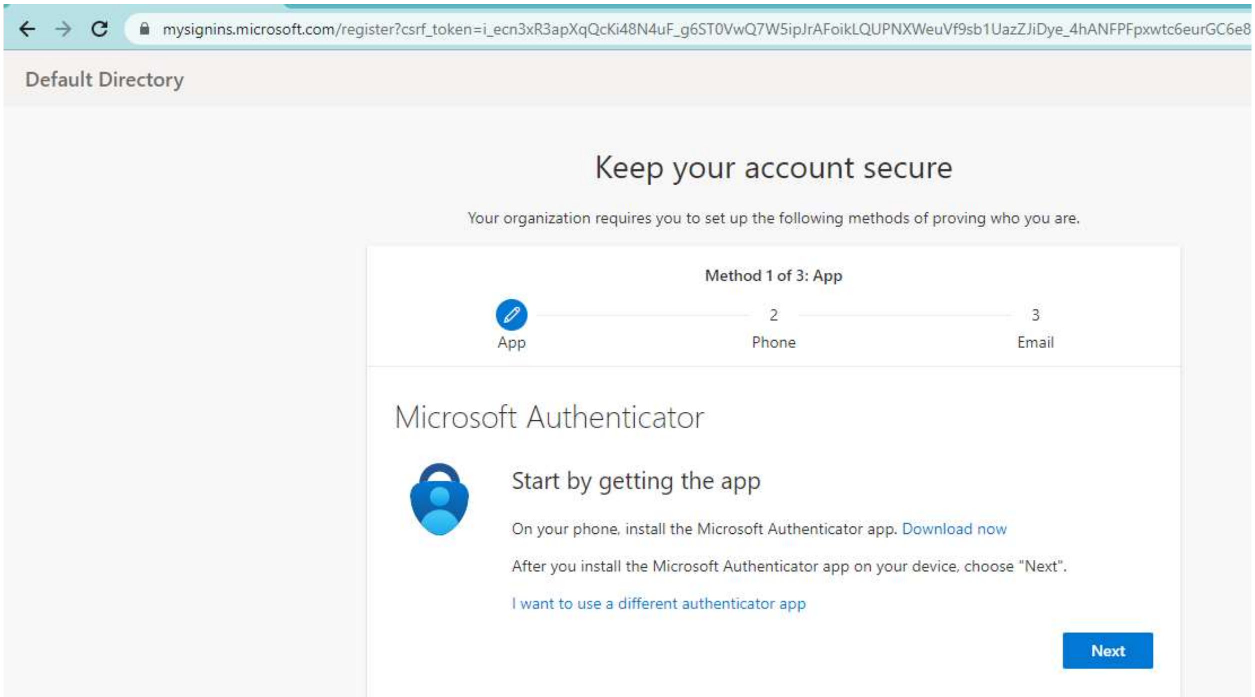
Microsoft

arun@cloudzdevopsoutlook.onmicrosoft.com

More information required

Your organization needs more information to keep your account secure

6. You'll be asked to setup authentication if you had not done already. If not, you will be



mysignins.microsoft.com/register?csrf_token=i_ecn3xR3apXqQcKi48N4uF_g6ST0VwQ7W5ipJrAFoikLQUPNXWeuVf9sb1UazZJiDye_4hANFPFpxwtc6eurGC6e8

Default Directory

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

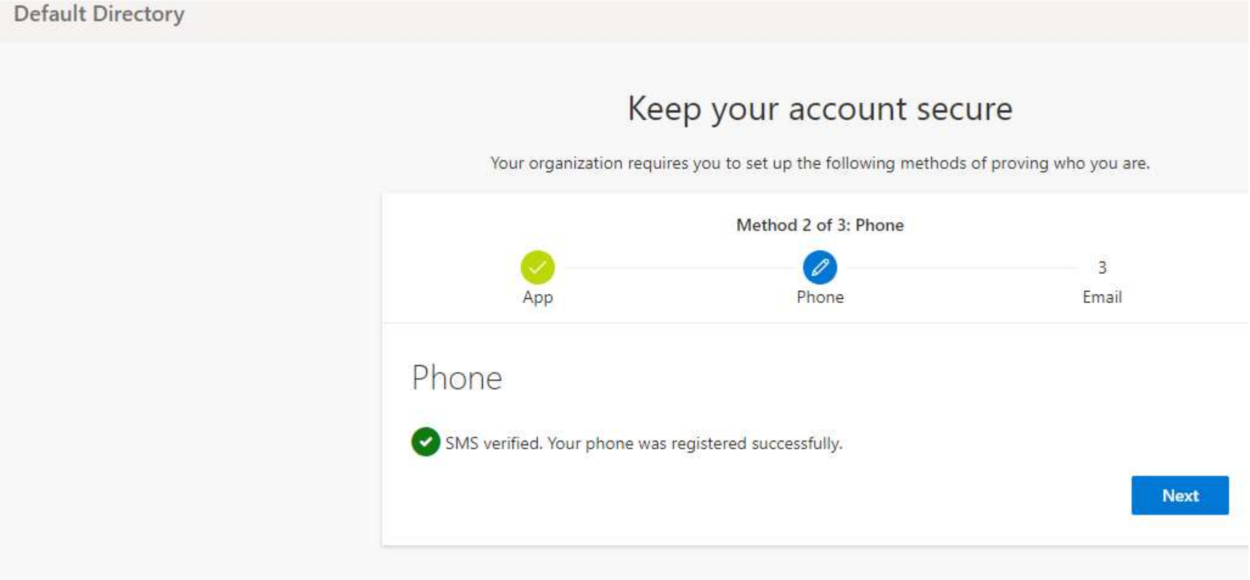
Method 1 of 3: App

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".



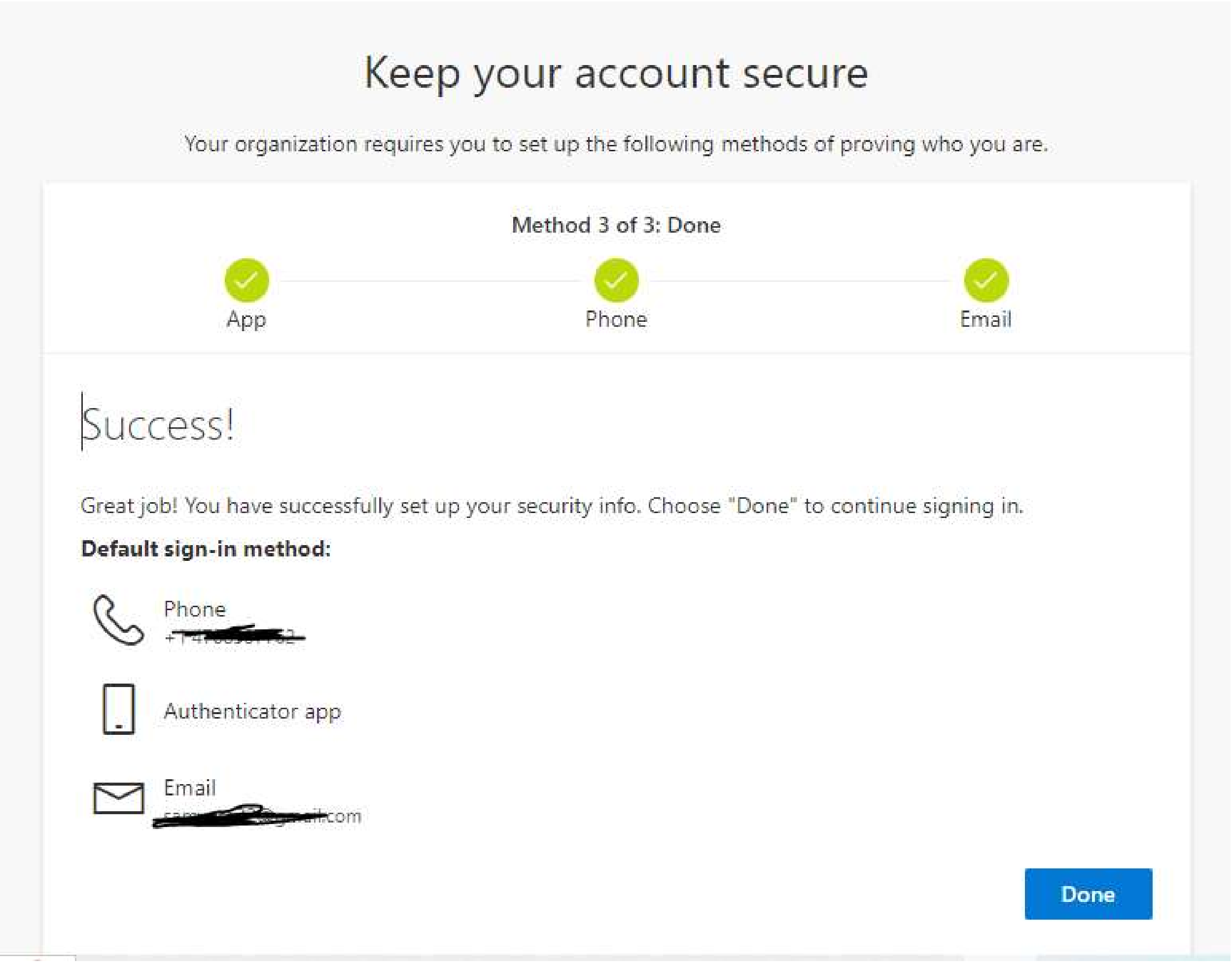
Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 3: Phone

Phone

✓ SMS verified. Your phone was registered successfully.



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 3 of 3: Done

Success!

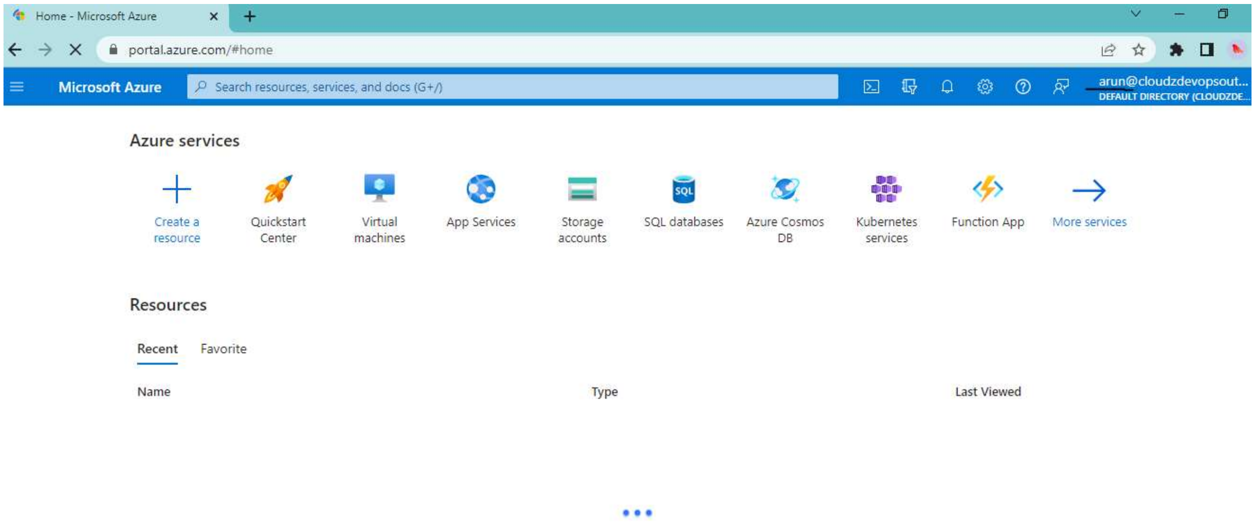
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

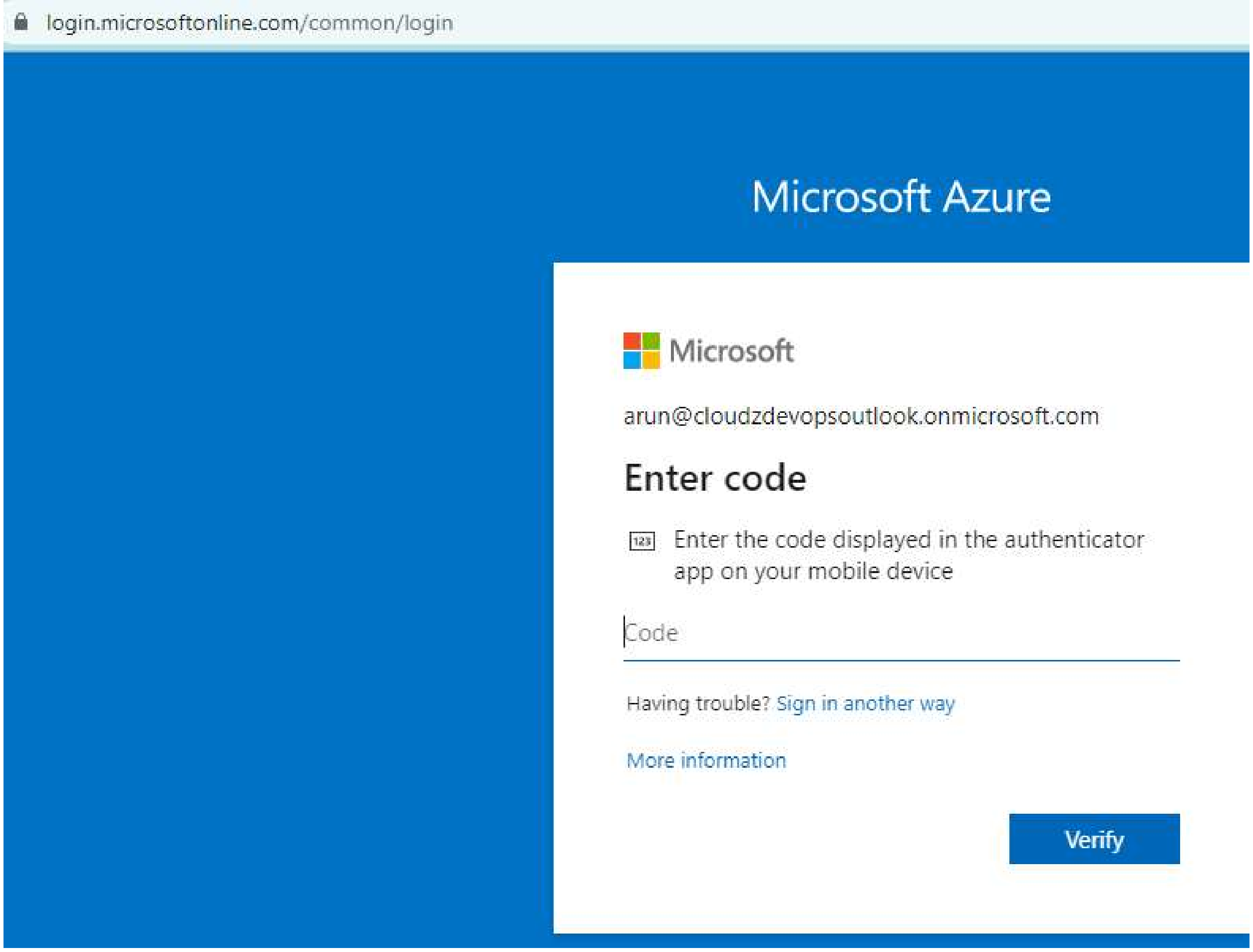
☎ Phone
[redacted]

Authenticator app

Email
[redacted]



7. MFA verification step


login.microsoftonline.com/common/login
Microsoft Azure
Microsoft

arun@cloudzdevopsoutlook.onmicrosoft.com

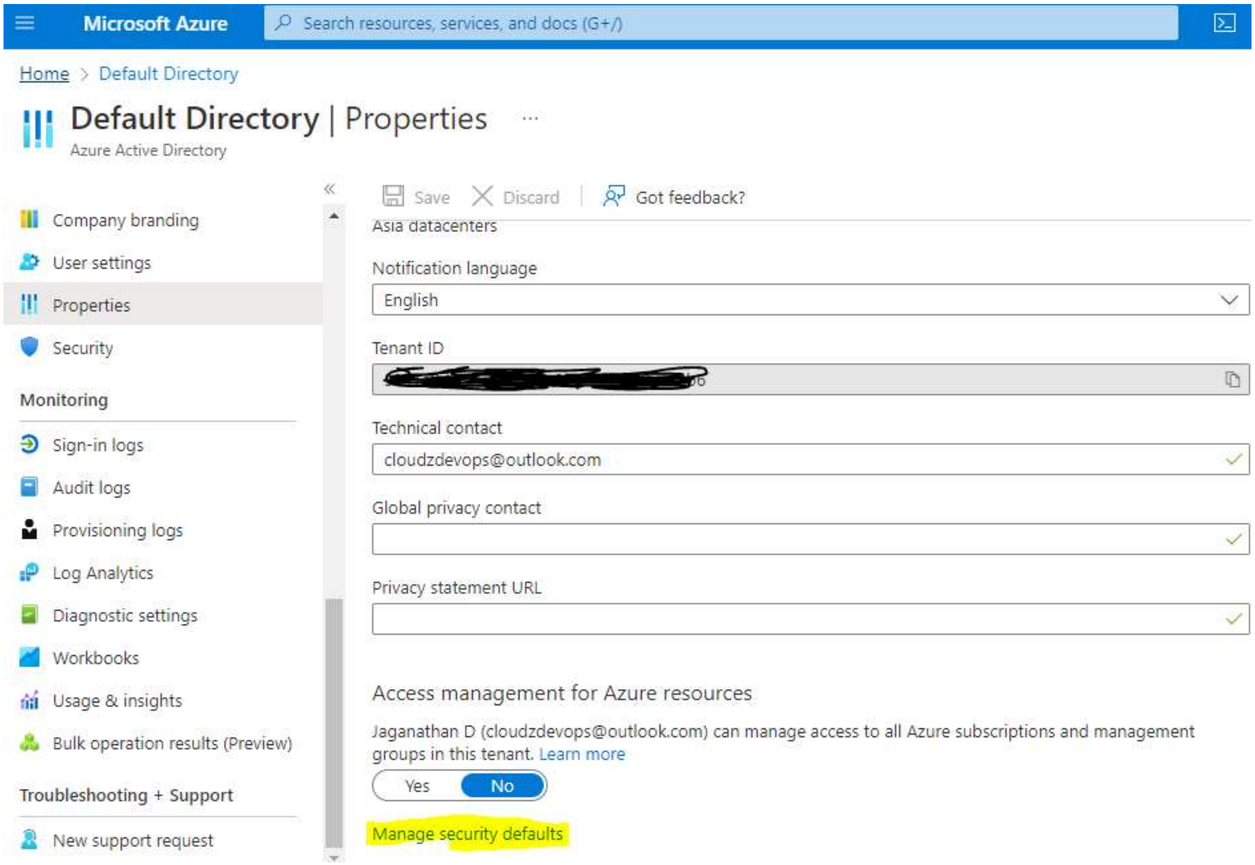
Enter code

Enter the code displayed in the authenticator app on your mobile device

Code
Having trouble? Sign in another way
More information
Verify

Below steps to be followed if you get “Security Default” screen for MFA disabled users.

8. Go to Azure AD → below manage, select “Properties”, click “Manage security default”.



Asia datacenters

Notification language: English

Tenant ID: [redacted]

Technical contact: cloudzdevops@outlook.com

Global privacy contact:

Privacy statement URL:

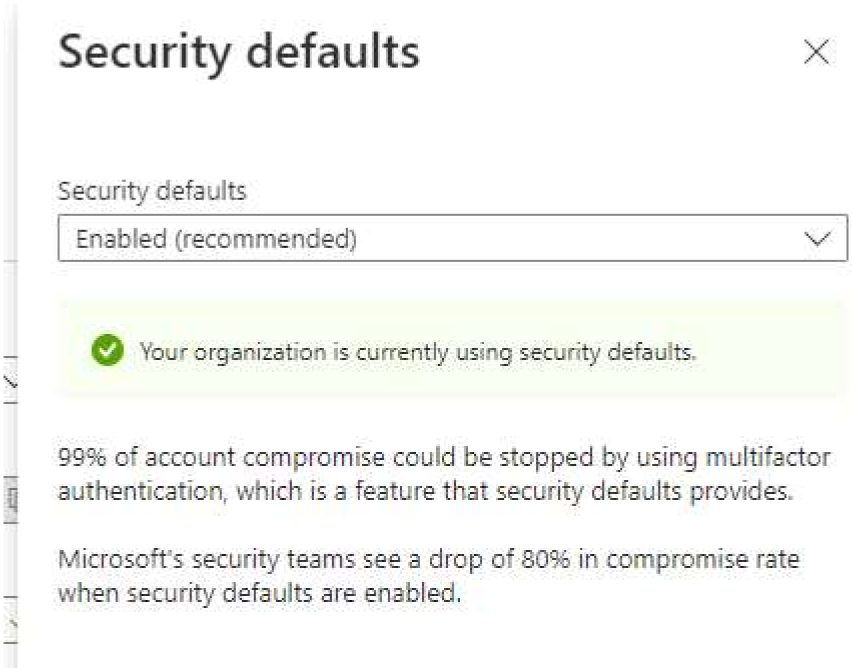
Access management for Azure resources

Jaganathan D (cloudzdevops@outlook.com) can manage access to all Azure subscriptions and management groups in this tenant. Learn more

Yes [✓ No]

Manage security defaults

9. By default, it’s “Enabled”. Select “Disabled” from below screen and hit Save.



Security defaults

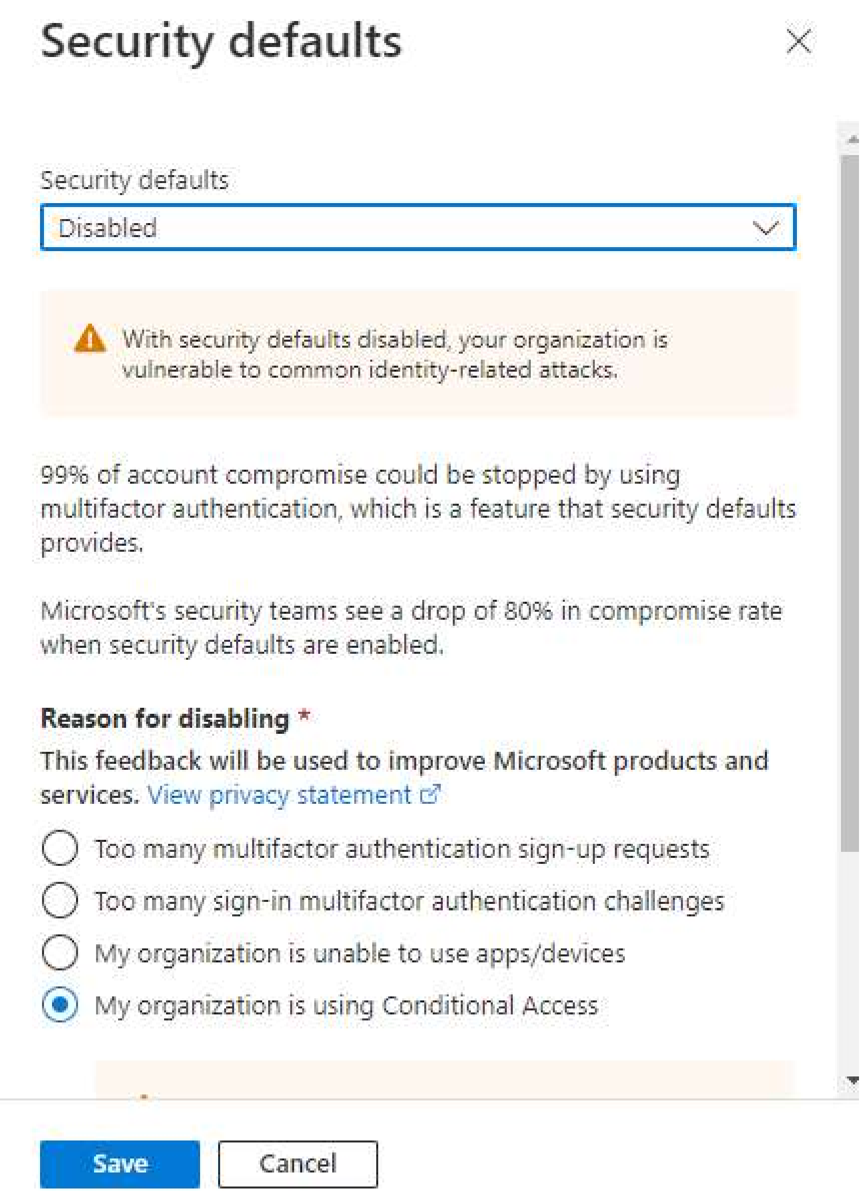
Security defaults

Enabled (recommended)

✓ Your organization is currently using security defaults.

99% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.



Security defaults

Security defaults

Disabled

With security defaults disabled, your organization is vulnerable to common identity-related attacks.

99% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

Reason for disabling *

This feedback will be used to improve Microsoft products and services. View privacy statement

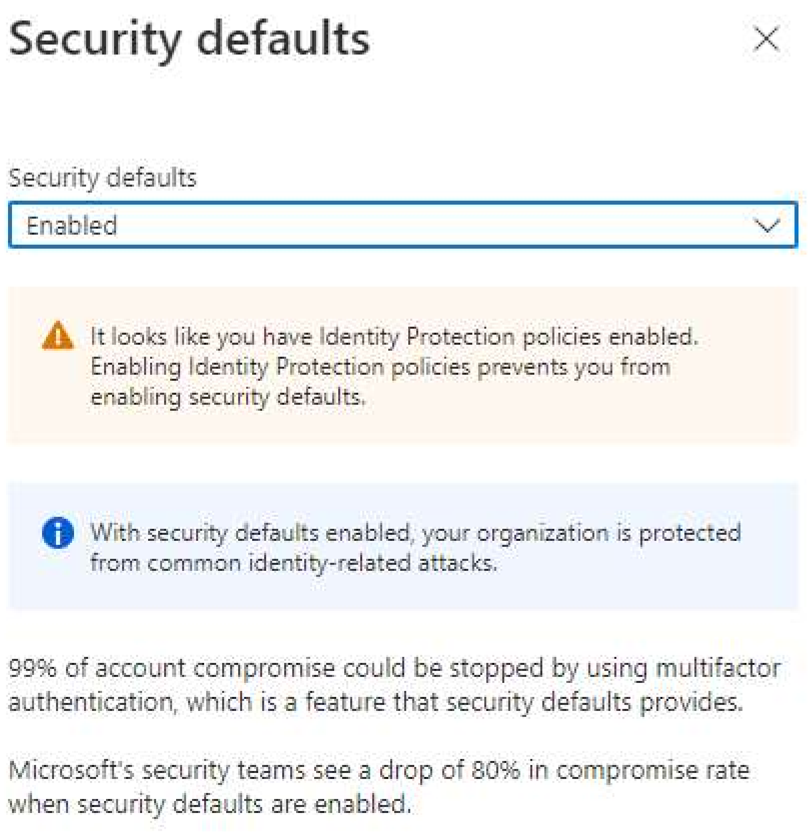
○ Too many multifactor authentication sign-up requests

○ Too many sign-in multifactor authentication challenges

○ My organization is unable to use apps/devices

● My organization is using Conditional Access

10. Note – You cannot enable it back unless you turn off MFA enforce policy.



Security defaults

Security defaults

Enabled

It looks like you have Identity Protection policies enabled. Enabling Identity Protection policies prevents you from enabling security defaults.

With security defaults enabled, your organization is protected from common identity-related attacks.

99% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

11. So, this (Security Default) is something like default MFA option provided by MS.