AZURE MULTIFACTOR AUTHENTICATION (MFA)

Configure & manage Azure Multifactor Authentication (MFA) and self-service password reset:

I. Introduction

---

1. What is Azure MFA?

Azure MFA requires a second form of authentication in addition to your password:

- Something you know (password)

- Something you have (phone, OTP app, etc.)

2. Two-Factor Authentication Methods

Azure MFA supports:

- Text message or phone call
- Microsoft Authenticator app
- OATH hardware tokens
- Biometrics (via FIDO2 keys)

3. How to Enable MFA in Azure AD

Step-by-Step:

Option 1: Per-user MFA (legacy method)

1. Go to https://portal.azure.com
2. Navigate to: Azure Active Directory > Users
3. Click Multi-Factor Authentication (top menu)
4. Select users > Click Enable > Confirm

Option 2: Conditional Access (modern method – recommended)

1. Navigate to: Azure Active Directory > Security > Conditional Access
2. Click + New policy
3. Name it: e.g., "Require MFA"
4. Under Users, select "All users" or specific group
5. Under Cloud apps, choose "All cloud apps"
6. Under Grant, select "Require multi-factor authentication"
7. Click Create

4. Configure MFA Authentication Methods

Go to:

- Azure AD > Security > Authentication methods
- You'll see Authentication method policies
    - Enable or disable Microsoft Authenticator, Text message, etc.

5. Manage MFA Settings for Users

1. Go to: Azure AD > Users > [Select user]
2. Under Authentication methods, view or change:
    - Phone numbers
    - App registrations
3. You can reset MFA for users here if needed.

6. Account Lockout Settings (MFA fraud protection)

To protect against MFA brute force:

1. Go to Azure AD > Security > Authentication methods > Password protection
2. Set:
    - Lockout threshold (e.g., 10 attempts)
    - Lockout duration (e.g., 60 seconds)

7. What is SSPR?

SSPR lets users reset their own password without contacting IT, using:

- Email
- Phone
- Authenticator app
- Security questions (optional)

8. Setup Self-Service Password Reset (SSPR)

Step-by-Step:

1. Go to: Azure AD > Password reset
2. Click Properties
3. Enable SSPR for:
    - All users
    - A specific group
4. Click Save

9. Configure Authentication Methods for SSPR

1. Under Password reset > Authentication methods:
    - Choose number of methods required (1 or 2)
    - Choose methods: email, phone, app

10. Deploy SSPR to Users

Recommend:

- Create a test group: Azure AD > Groups > New group
- Add your test users
- Enable SSPR only for this group first

11. User Registration for SSPR & MFA

Ask users to go to:

- https://aka.ms/mfasetup or https://aka.ms/ssprsetup
- They'll enter phone/email and app options

12. Extend Azure MFA to 3rd Party & On-Premises Apps

Use:

- Azure AD Application Proxy for on-prem apps
- NPS Extension for Azure MFA for VPNs, RADIUS-based systems

13. Monitor Azure AD MFA & SSPR Activity

View Reports:

1. Go to Azure AD > Monitoring > Sign-ins
    - Filter by "MFA required", "MFA passed/failed"
2. Go to Azure AD > Password reset > Usage & insights
    - Shows who used SSPR, success/failure

14. OAuth Tokens (Brief Overview)

OAuth is a standard for authorization (not authentication). In Azure:

- Used for apps to access resources without exposing user passwords
- Access tokens are issued by Azure AD after login

Explore:

- Azure AD > App registrations > [Your app] > API permissions

II. Implementation

PART 0: Set Up Your Azure Environment (Required Before Starting)

- **Step 0.1: Create a Free Azure Account**
  - Open this link in your browser: https://azure.microsoft.com/free/
  - Click the button "**Start free**".
  - Sign in using your **Microsoft account** (like Outlook.com, Hotmail.com, or even a work email).
  - Fill in:
  - **Basic info**: Name, country, etc.
  - **Phone number**: For verification
  - **Credit card**: ONLY for identity verification (you won't be charged if you stay within the free tier)
  - After verifying, you'll be redirected to the **Azure Portal**.
  - You now have ₹14,500 or $200 in free credits, valid for 30 days.

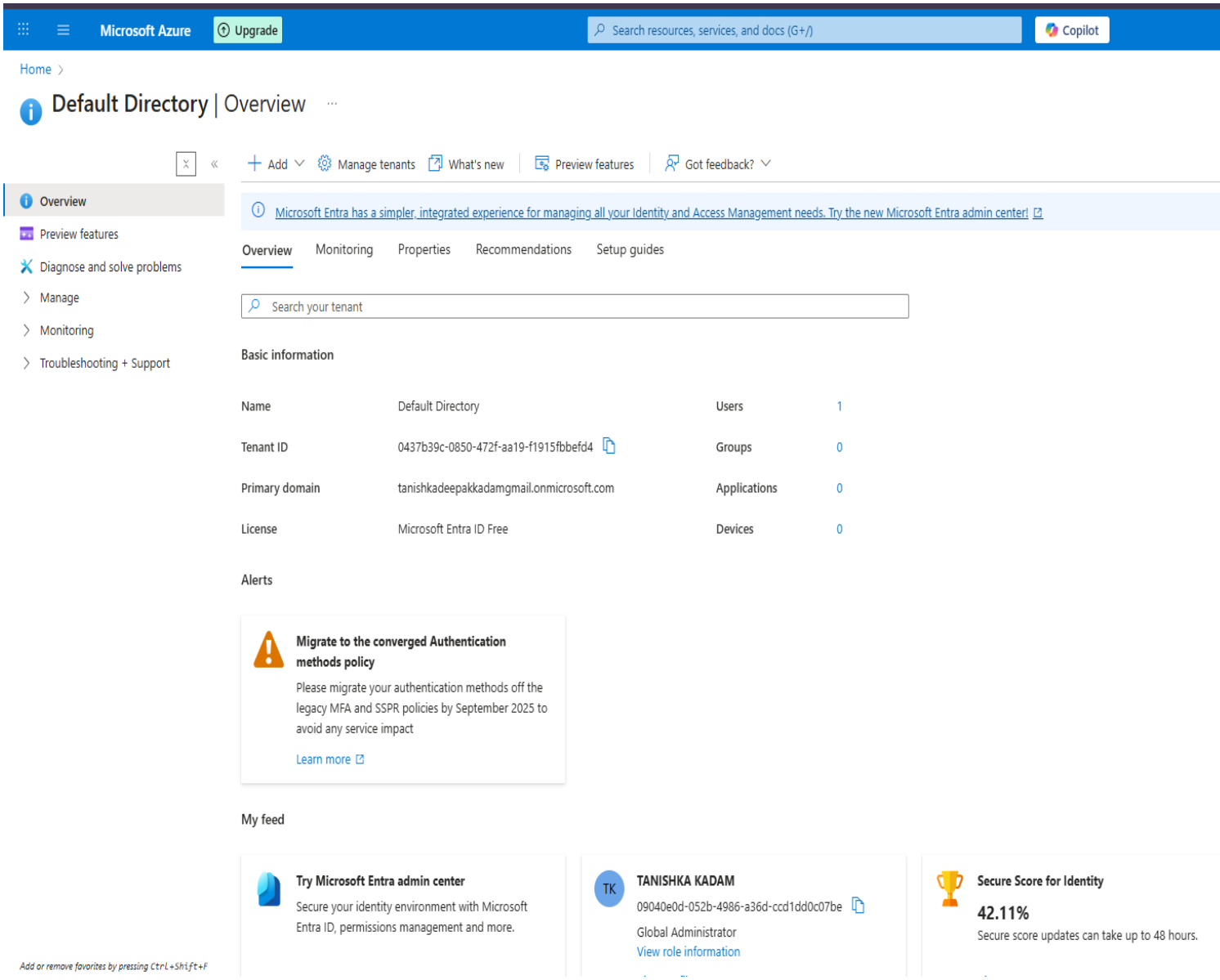
- **Step 0.2: Access Azure Active Directory (AAD)**

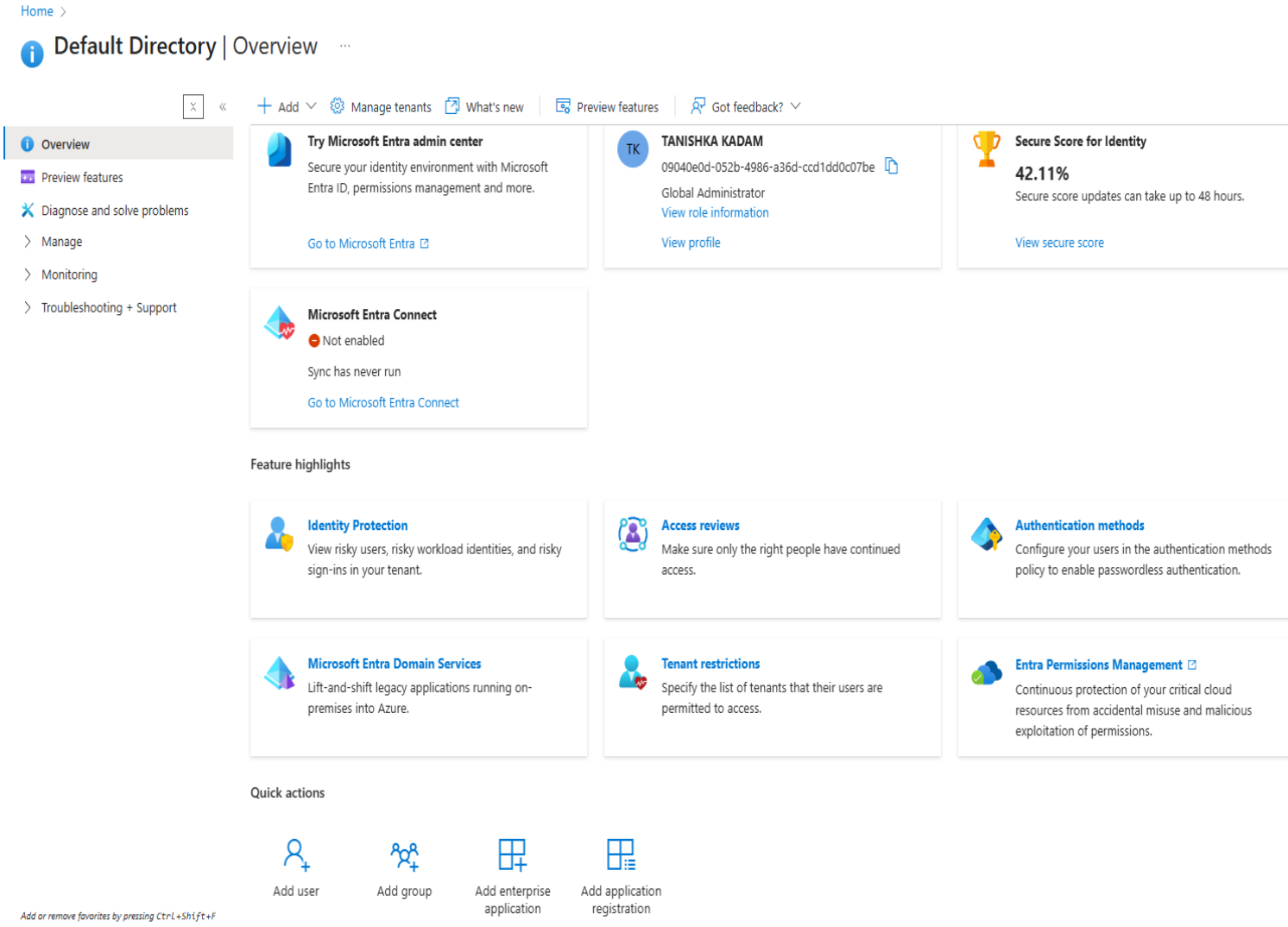
1. Open: https://portal.azure.com
2. On the home screen or top search bar, type:

Azure Active Directory

3. Click on the result that says **Azure Active Directory**.
4. You're now in your **AAD dashboard**, where you can:
    - Manage users and groups

- Configure MFA and SSPR
- Monitor security settings





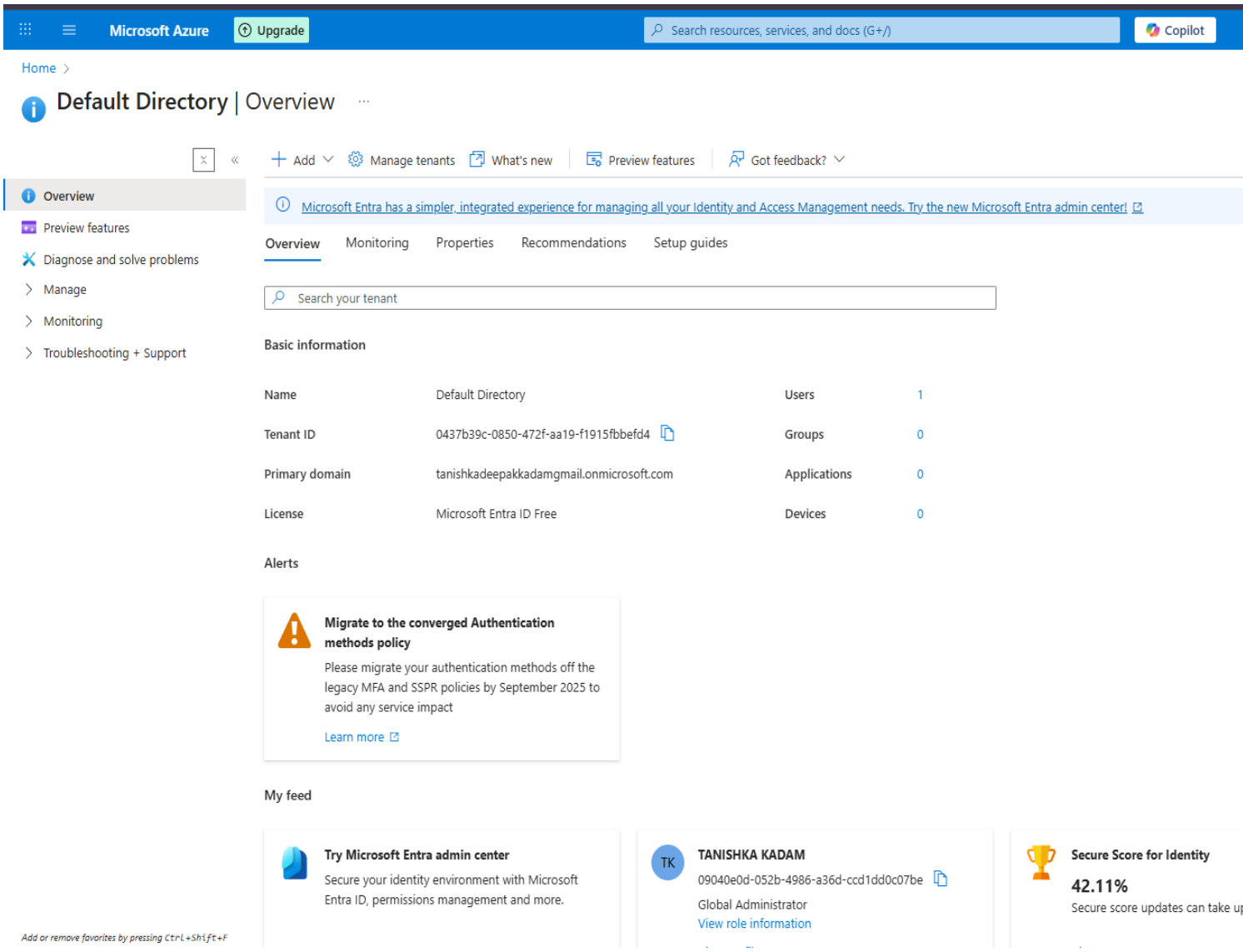
- **Step 0.3: Create Test Users & Groups**

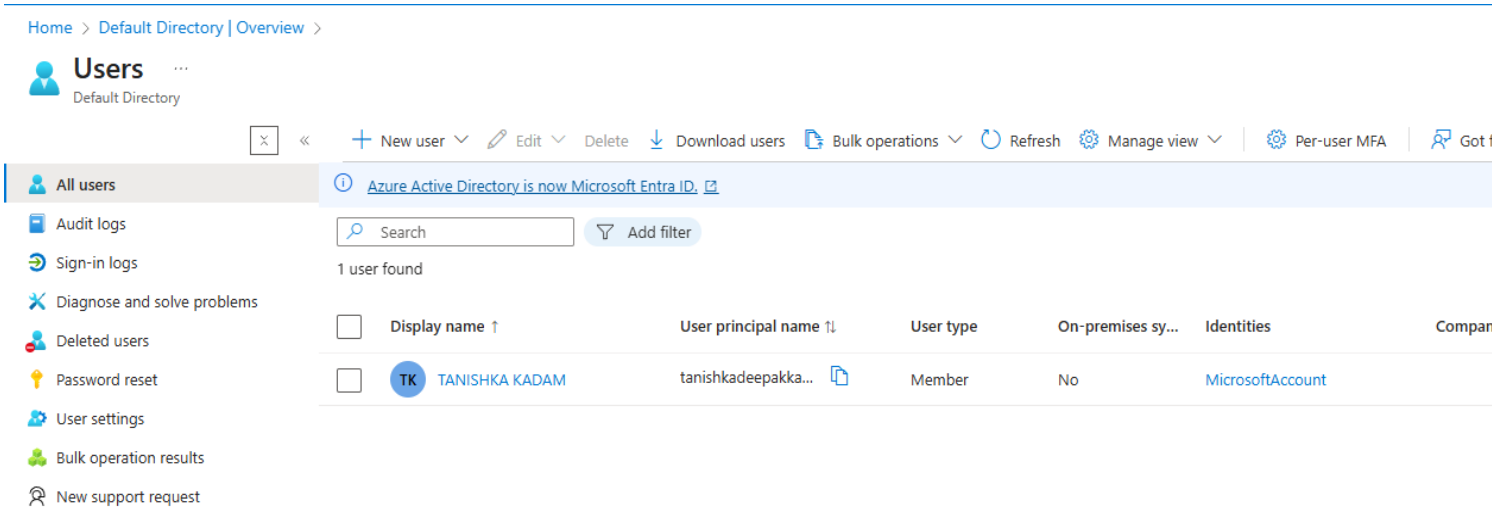
A. Create Test Users

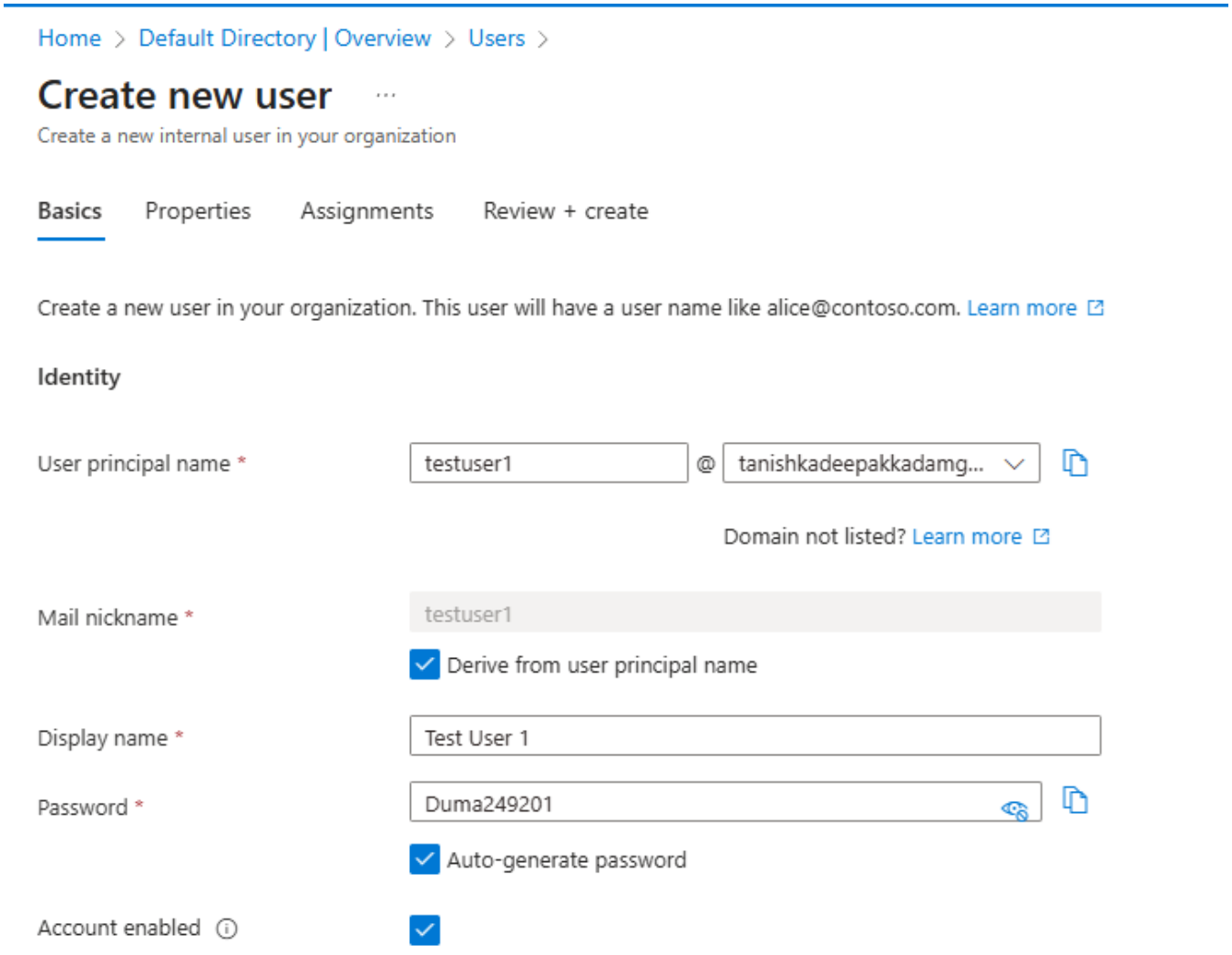
1. In the Azure AD dashboard, click on **Users** (left-side menu).
2. Click the **+ New user** button (top menu).
3. In the **Create user** panel:
    - **User name**: testuser1 (this becomes the email like testuser1@yourdomain.onmicrosoft.com)
    - **Name**: Test User 1

- **Password**: Choose **Auto-generate password** (copy the password shown!)

4. Click **Create**.
5. Repeat for testuser2, testuser3.




Home > Default Directory | Overview >
Users
Default Directory
New user
Edit
Delete
Download users
Bulk operations
Refresh
Manage view
Per-user MFA
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Deleted users
Password reset
User settings
Bulk operation results
New support request
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
1 user found
Display name
User principal name
User type
On-premises sy...
Identities
TK
TANISHKA KADAM
tanishkadeepakka...
Member
No
MicrosoftAccount


Home > Default Directory | Overview > Users >
Create new user
Create a new internal user in your organization
Basics
Properties
Assignments
Review + create
Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more
Identity
User principal name *
testuser1
@
tanishkadeepakkadamg...
Domain not listed? Learn more
Mail nickname *
testuser1
Derive from user principal name
Display name *
Test User 1
Password *
Duma249201
Auto-generate password
Account enabled

Home > Default Directory | Overview > Users >

Create new user

Create a new internal user in your organization

Basics Properties Assignments **Review + create**

Basics

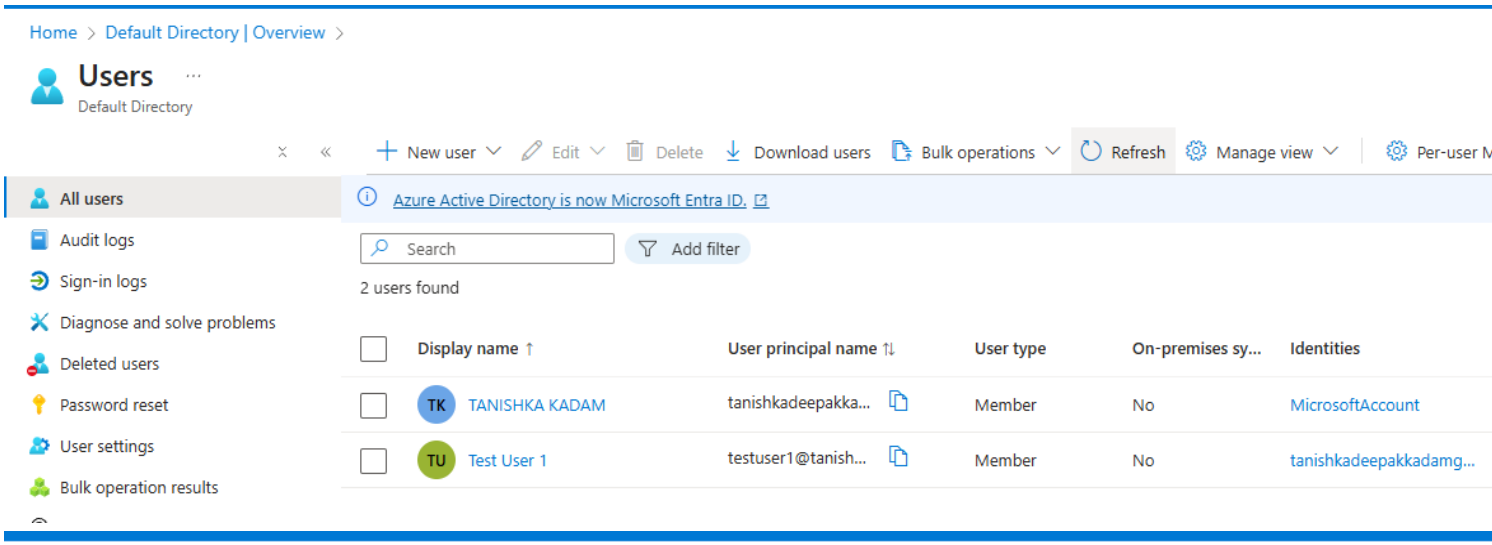
User principal name	testuser1@tanishkadeepakkadamgmail.onmicrosoft.com
Display name	Test User 1
Mail nickname	testuser1
Password	Duma249201
Account enabled	Yes

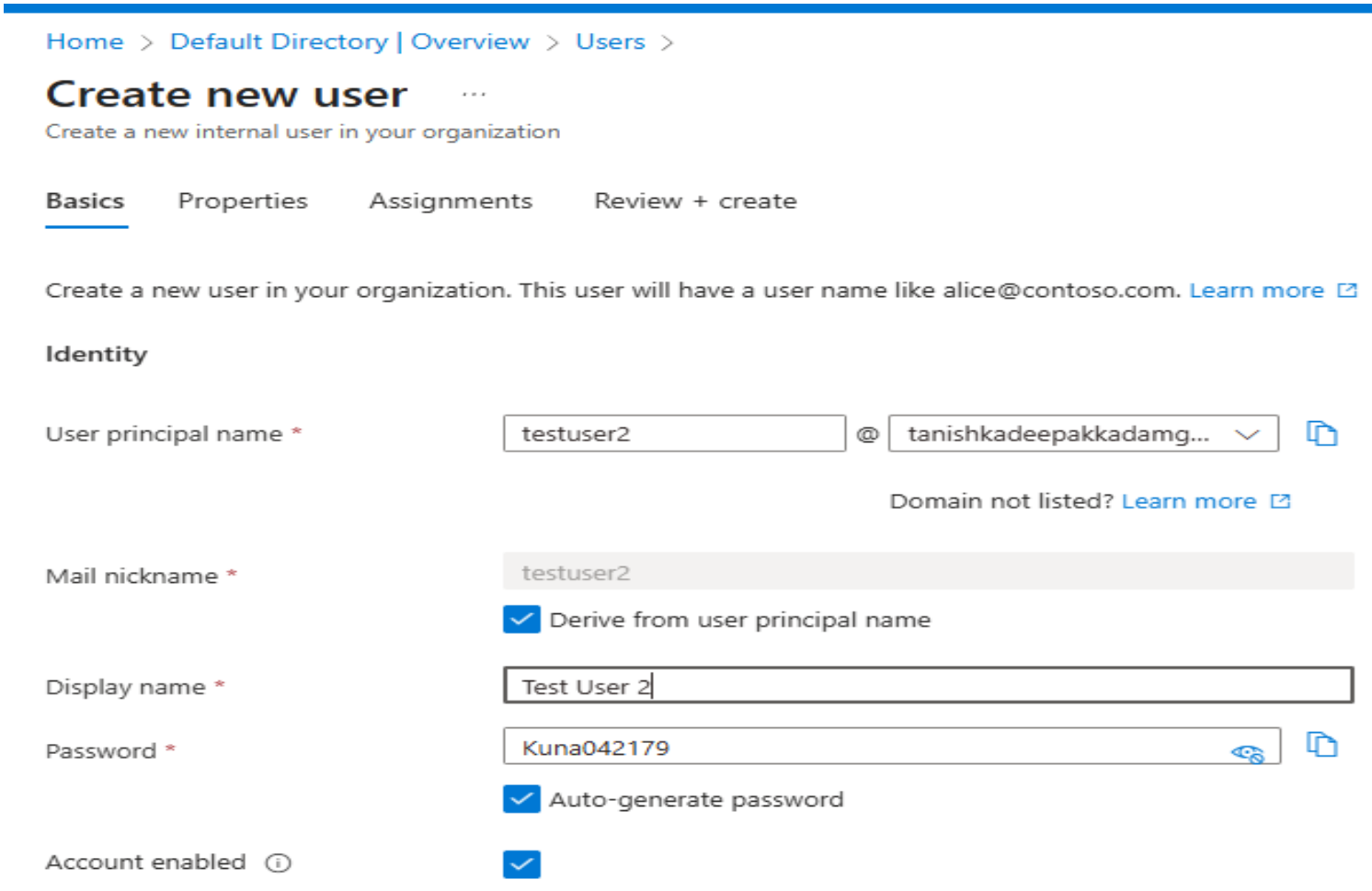
Properties

Other emails	View
User type	Member

Assignments

Administrative units	
Groups	
Roles	


Home > Default Directory | Overview >
Users
Default Directory
New user
Edit
Delete
Download users
Bulk operations
Refresh
Manage view
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Deleted users
Password reset
User settings
Bulk operation results
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
2 users found
Display name
User principal name
User type
On-premises sy...
Identities
TANISHKA KADAM
tanishkadeepakka...
Member
No
MicrosoftAccount
Test User 1
testuser1@tanish...
Member
No
tanishkadeepakkadamg...


Home > Default Directory | Overview > Users >
Create new user
Create a new internal user in your organization
Basics
Properties
Assignments
Review + create
Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more
Identity
User principal name *
testuser2
@
tanishkadeepakkadamg...
Domain not listed? Learn more
Mail nickname *
testuser2
Derive from user principal name
Display name *
Test User 2
Password *
Kuna042179
Auto-generate password
Account enabled

Create new user

Create a new internal user in your organization

Basics Properties Assignments **Review + create**

Basics

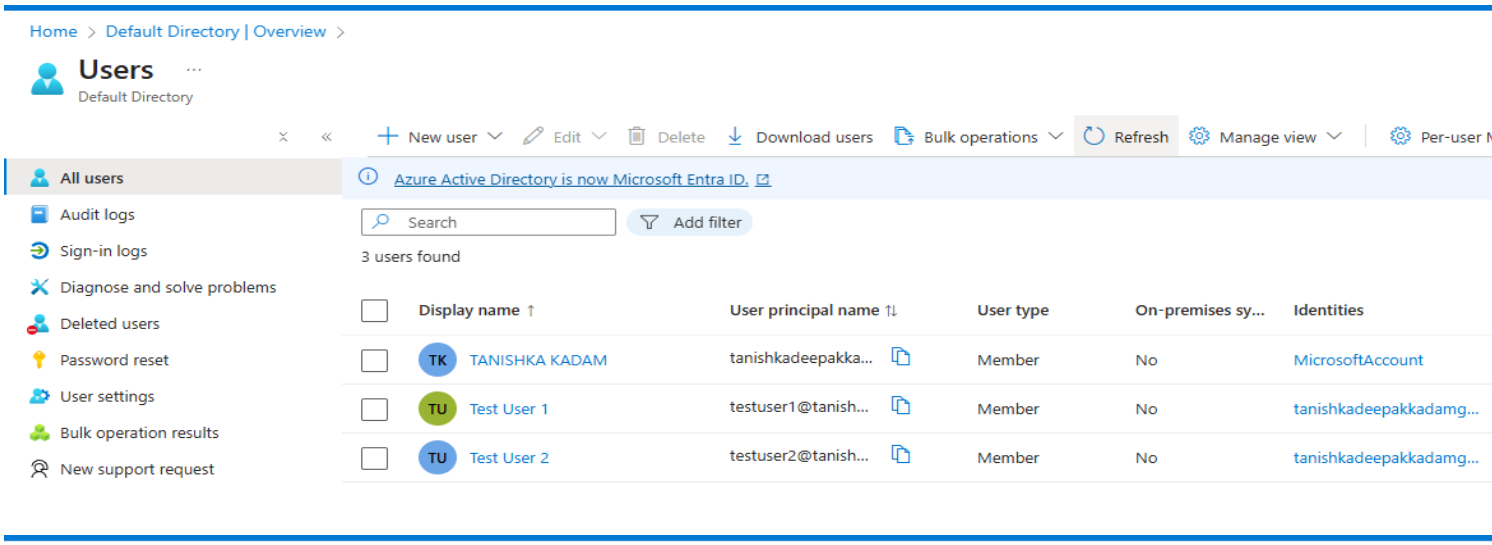
User principal name	testuser2@tanishkadeepakkadamgmail.onmicrosoft.com
Display name	Test User 2
Mail nickname	testuser2
Password	Kuna042179
Account enabled	Yes

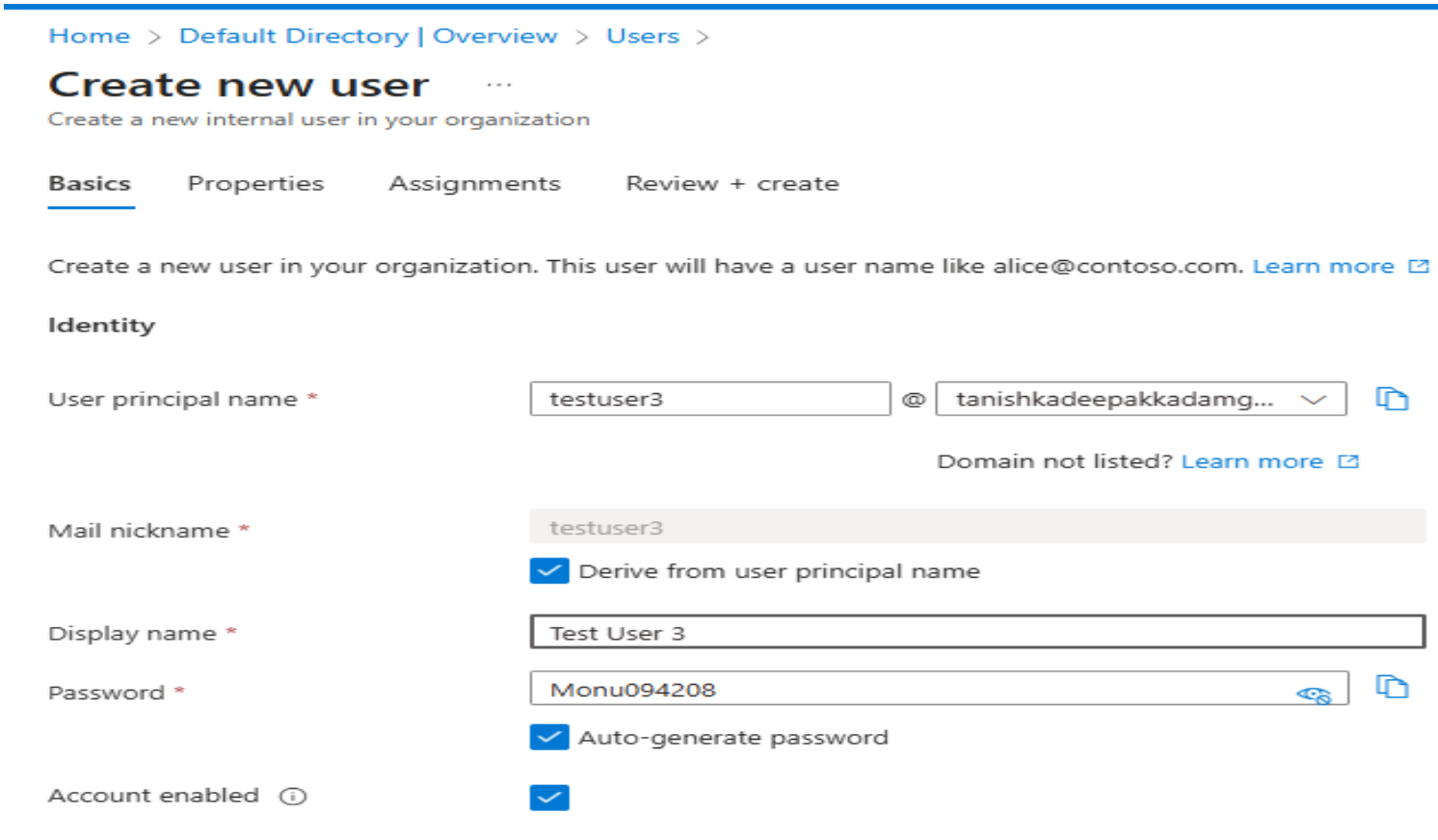
Properties

User type	Member

Assignments

Administrative units	
Groups	
Roles	


Home > Default Directory | Overview >
Users
Default Directory
New user
Edit
Delete
Download users
Bulk operations
Refresh
Manage view
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Deleted users
Password reset
User settings
Bulk operation results
New support request
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
3 users found
Display name
User principal name
User type
On-premises sy...
Identities
TANISHKA KADAM
tanishkadeepakka...
Member
No
MicrosoftAccount
Test User 1
testuser1@tanish...
Member
No
tanishkadeepakkadamg...
Test User 2
testuser2@tanish...
Member
No
tanishkadeepakkadamg...


Home > Default Directory | Overview > Users >
Create new user
Create a new internal user in your organization
Basics
Properties
Assignments
Review + create
Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more
Identity
User principal name *
testuser3
@
tanishkadeepakkadamg...
Domain not listed? Learn more
Mail nickname *
testuser3
Derive from user principal name
Display name *
Test User 3
Password *
Monu094208
Auto-generate password
Account enabled

Create new user

Create a new internal user in your organization

Basics Properties Assignments **Review + create**

Basics

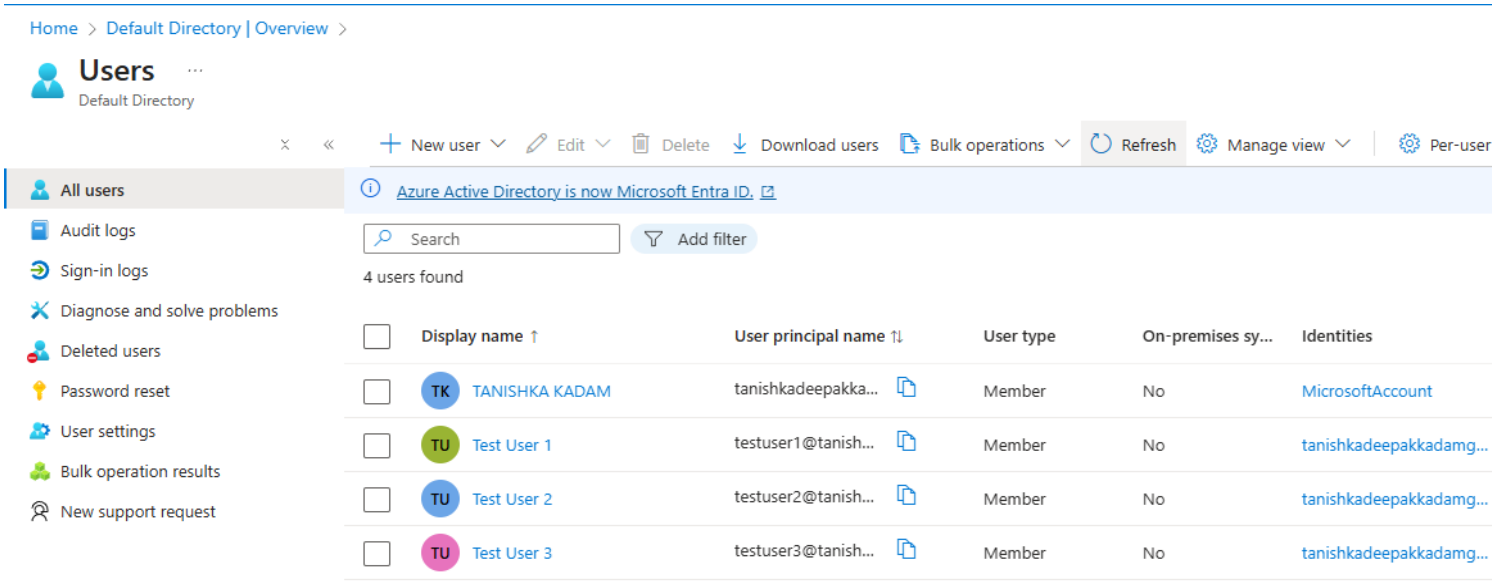
User principal name	testuser3@tanishkadeepakkadamgmail.onmicrosoft.com
Display name	Test User 3
Mail nickname	testuser3
Password	Monu094208
Account enabled	Yes

Properties

User type	Member

Assignments

Administrative units	
Groups	
Roles	



B. Create a Group for Testing (TestMFAGroup)

1. Go back to the **Azure Active Directory** panel.
2. Click on **Groups** (left menu).
3. Click **+ New Group**.
4. Fill in:
    - **Group type**: Security
    - **Group name**: TestMFAGroup
    - **Group description**: Group for MFA/SSPR testing
    - **Membership type**: Assigned
5. Click **No members selected** > Click **+ Add members**
6. Search and select:
    - testuser1
    - testuser2 (or any other test users you created)
7. Click **Select** > then **Create**

Home > Default Directory | Overview >

Groups | Overview

Default Directory

- Overview
- All groups
- Deleted groups
- Diagnose and solve problems
- Settings
- Activity
- Troubleshooting + Support

New group | Download groups | Preview features

Overview | Tutorials

Search your tenant

Basic information

Total groups	0	Dynamic groups	0
M365 groups	0	Cloud groups	0
Security groups	0	On-premises groups	0

Alerts

Feature highlights

Access reviews

Make sure only the right people have continued access.

Quick actions

Add group

Download groups

New Group

...

Got feedback?

Group type * ⓘ

Security

Group name * ⓘ

TestMFAGroup

Group description ⓘ

Group for MFA/SSPR testing

Membership type ⓘ

Assigned

Owners

No owners selected

Members

No members selected

Add members

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

Search

93 results found

All | Users | Groups | Devices | Enterprise applications

	Name	Type	Details
☐	AAD Request Verification Service...	Enterprise ap...	c728155f-7b2a-4502-a08b-b8af9b269319
☐	TANISHKA KADAM	User	tanishkadeepakkadam@gmail.com
☐	aciapi	Enterprise ap...	c5b17a4f-cc6f-4649-9480-684280a2af3a
☑	Test User 1	User	testuser1@tanishkadeepakkadamgmail.onn
☐	Azure AD Notification	Enterprise ap...	fc03f97a-9db0-4627-a216-ec98ce54e018
☑	Test User 2	User	testuser2@tanishkadeepakkadamgmail.onn
☐	Azure Advisor	Enterprise ap...	c39c9bac-9d1f-4dfb-aa29-27f6365e5cb7
☑	Test User 3	User	testuser3@tanishkadeepakkadamgmail.onn
☐	Azure Bastion	Enterprise ap...	79d7fb34-4bef-4417-8184-ff713af7a679
☐	Azure Cloud Shell	Enterprise ap...	2233b157-f44d-4812-b777-036cdaf9a96e

Selected (3)

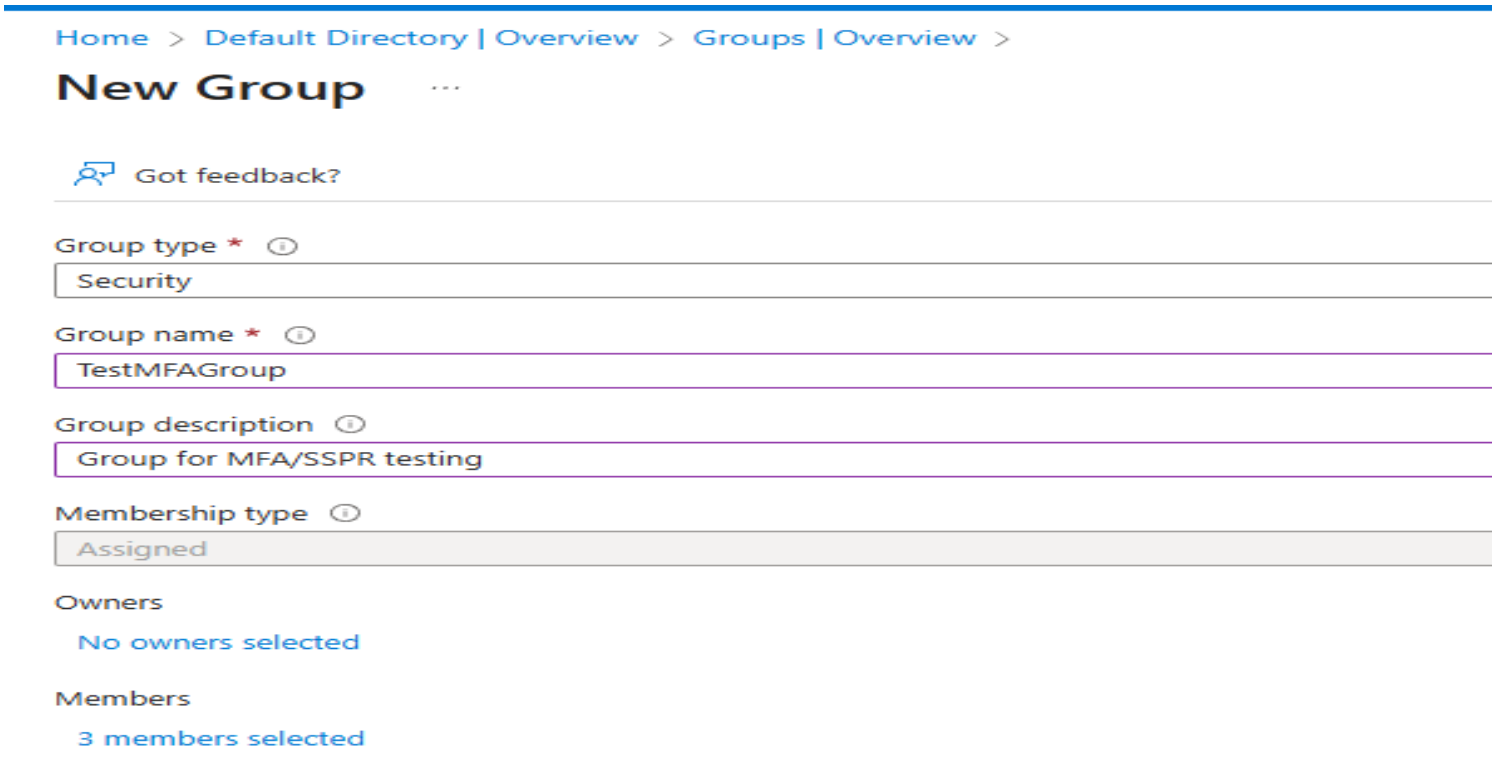
Reset

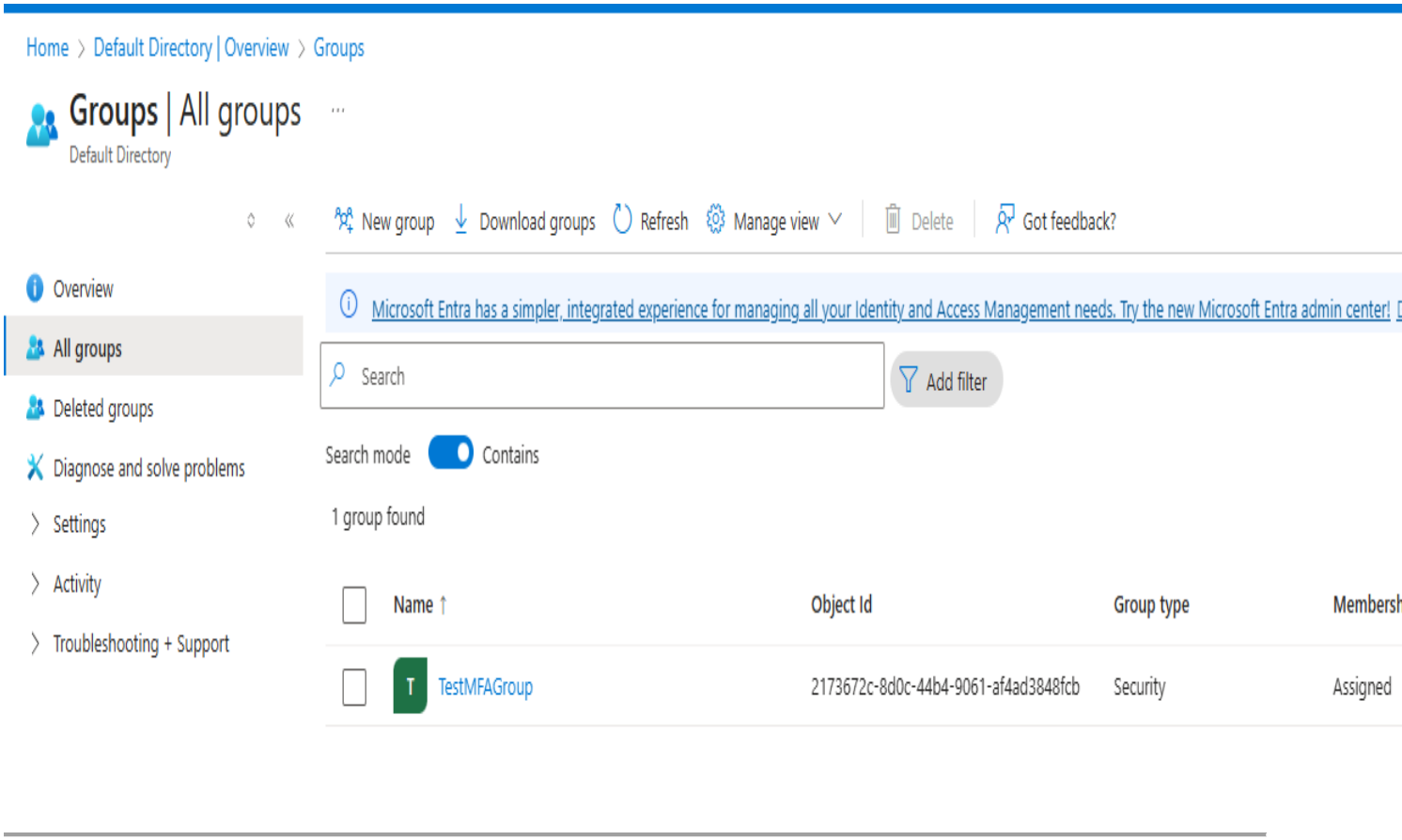
Test User 1
testuser1@tanishkadeepakkadamgmail.on...

Test User 2
testuser2@tanishkadeepakkadamgmail.on...

Test User 3
testuser3@tanishkadeepakkadamgmail.on...

Select


Home > Default Directory | Overview > Groups | Overview >
New Group
Got feedback?
Group type *
Security
Group name *
TestMFAGroup
Group description
Group for MFA/SSPR testing
Membership type
Assigned
Owners
No owners selected
Members
3 members selected


Home > Default Directory | Overview > Groups
Groups | All groups
Default Directory
New group
Download groups
Refresh
Manage view
Delete
Got feedback?
Overview
All groups
Deleted groups
Diagnose and solve problems
Settings
Activity
Troubleshooting + Support
Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!
Search
Add filter
Search mode
Contains
1 group found
Name
Object Id
Group type
Membersh
TestMFAGroup
2173672c-8d0c-44b4-9061-af4ad3848fcb
Security
Assigned

PART 1: Configure & Manage Azure MFA

🔹 Step 1.1: Understand MFA

- MFA = Password + another factor (Phone/App/etc.)
- **Multi-Factor Authentication (MFA)** requires two forms of identity:

Factor	Example
1. Something you know	Password
2. Something you have	Phone (SMS, call), Authenticator app, FIDO2 security key

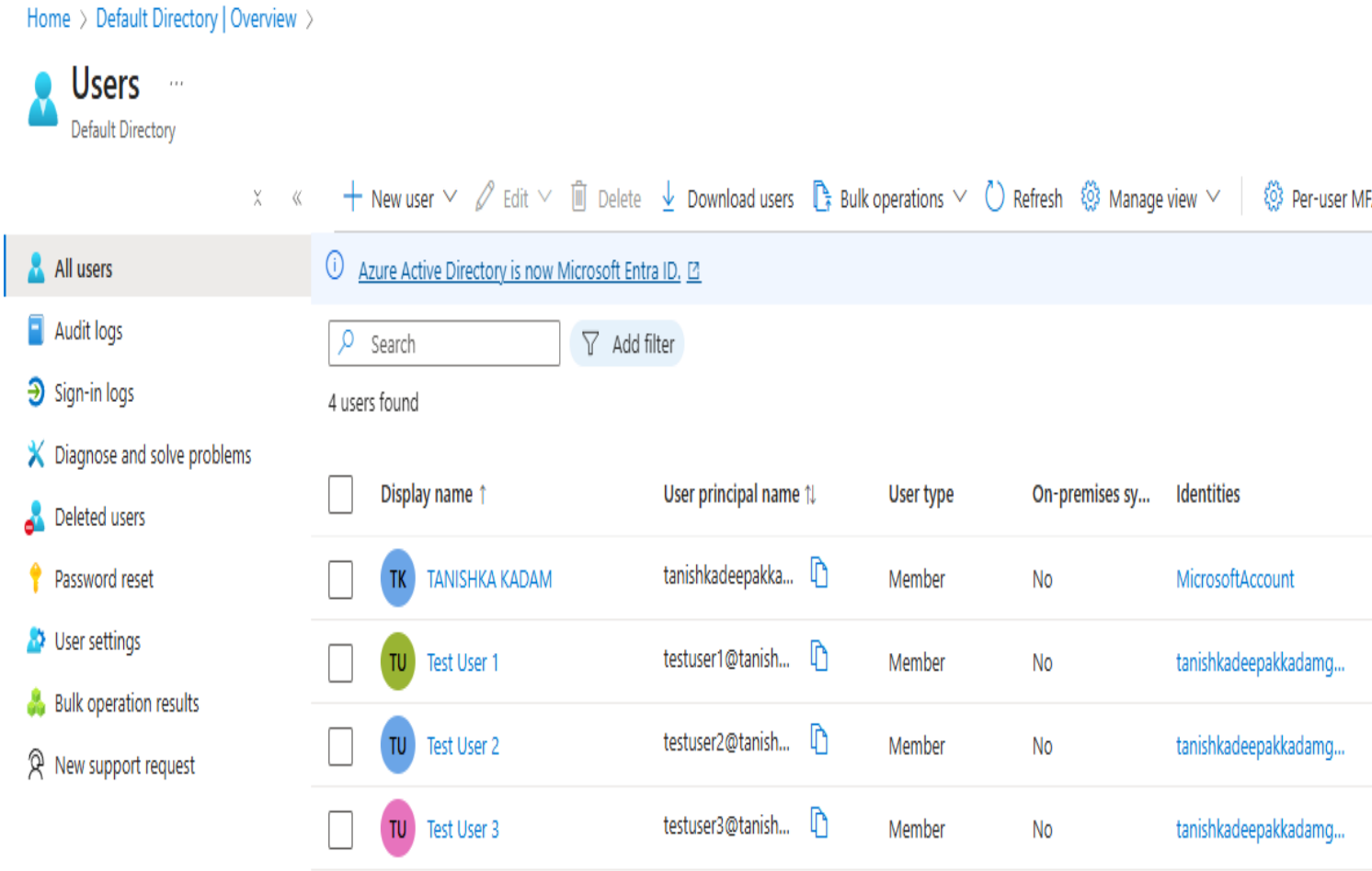
Azure uses both to secure your accounts.

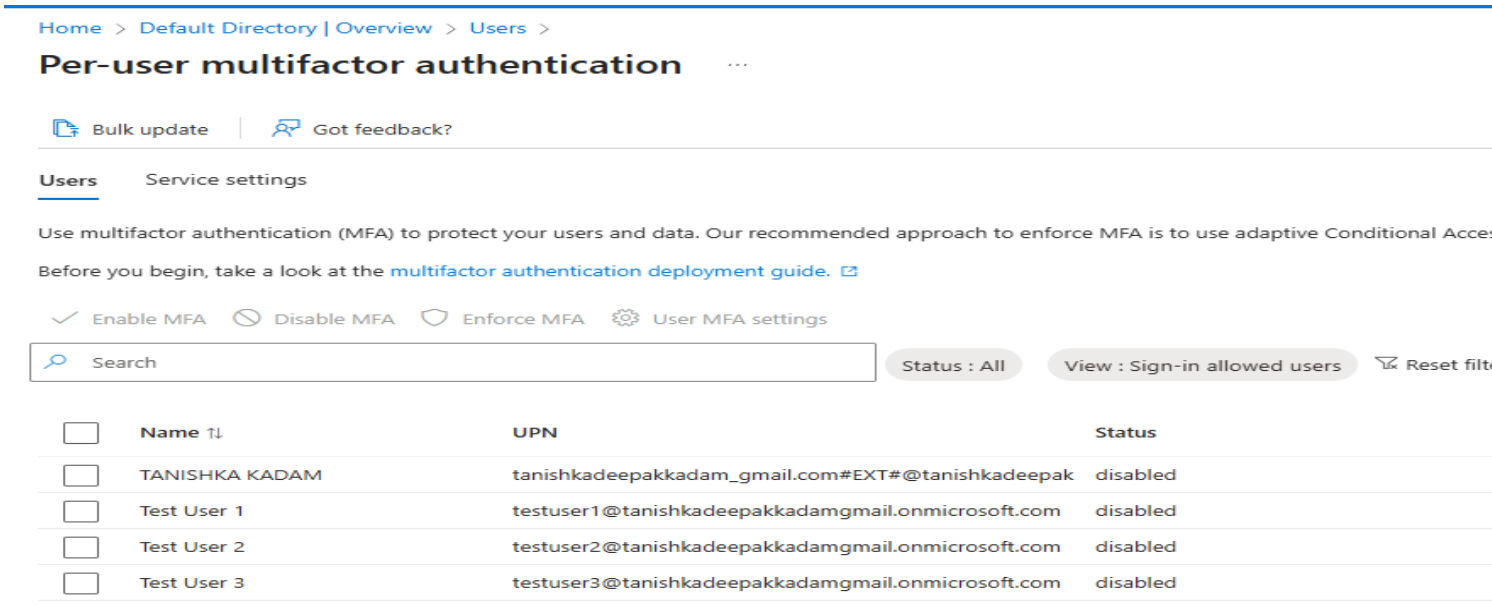
🔹 Step 1.2: Configure Per-User MFA (Basic Setup)

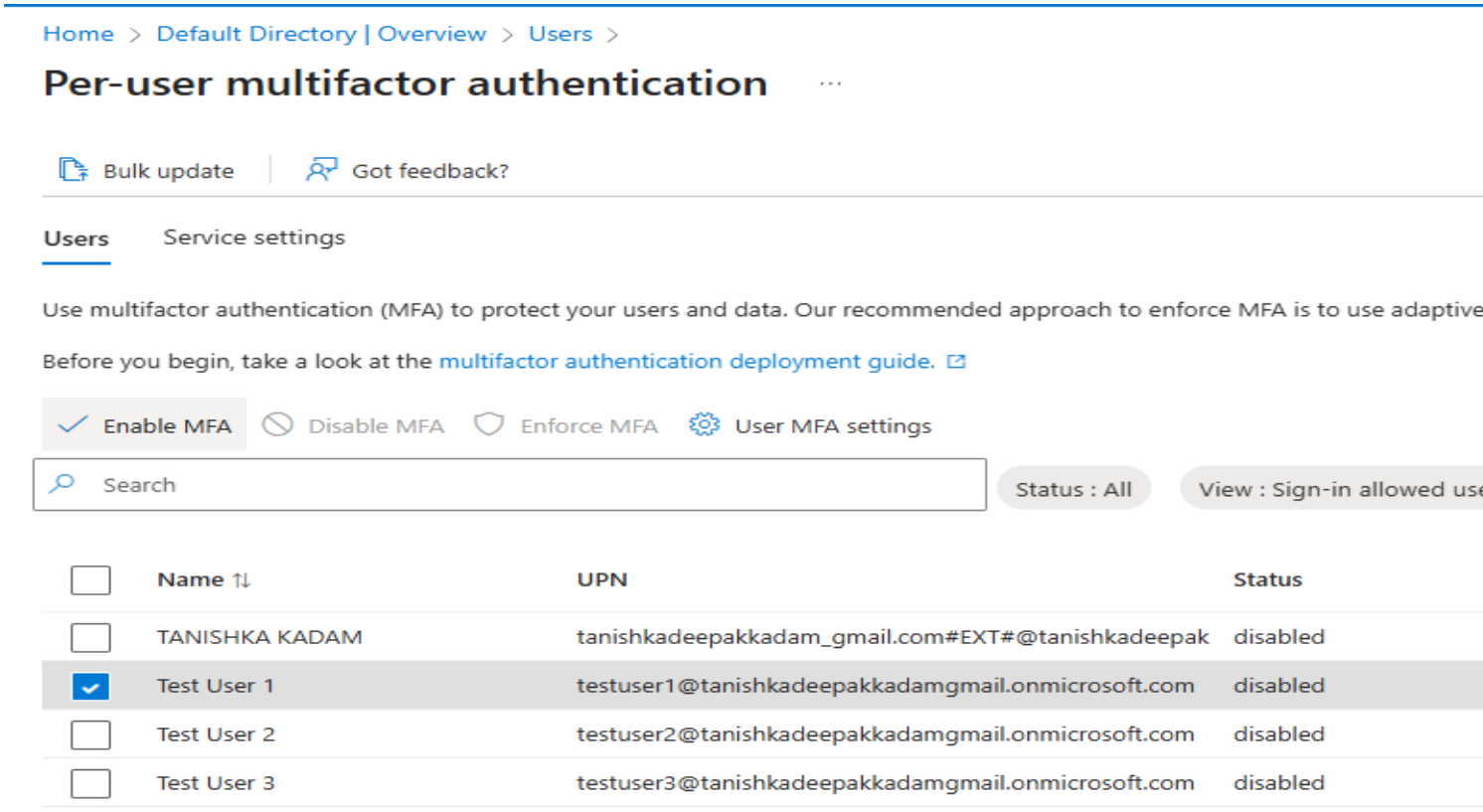
This method enables MFA for individual users manually.

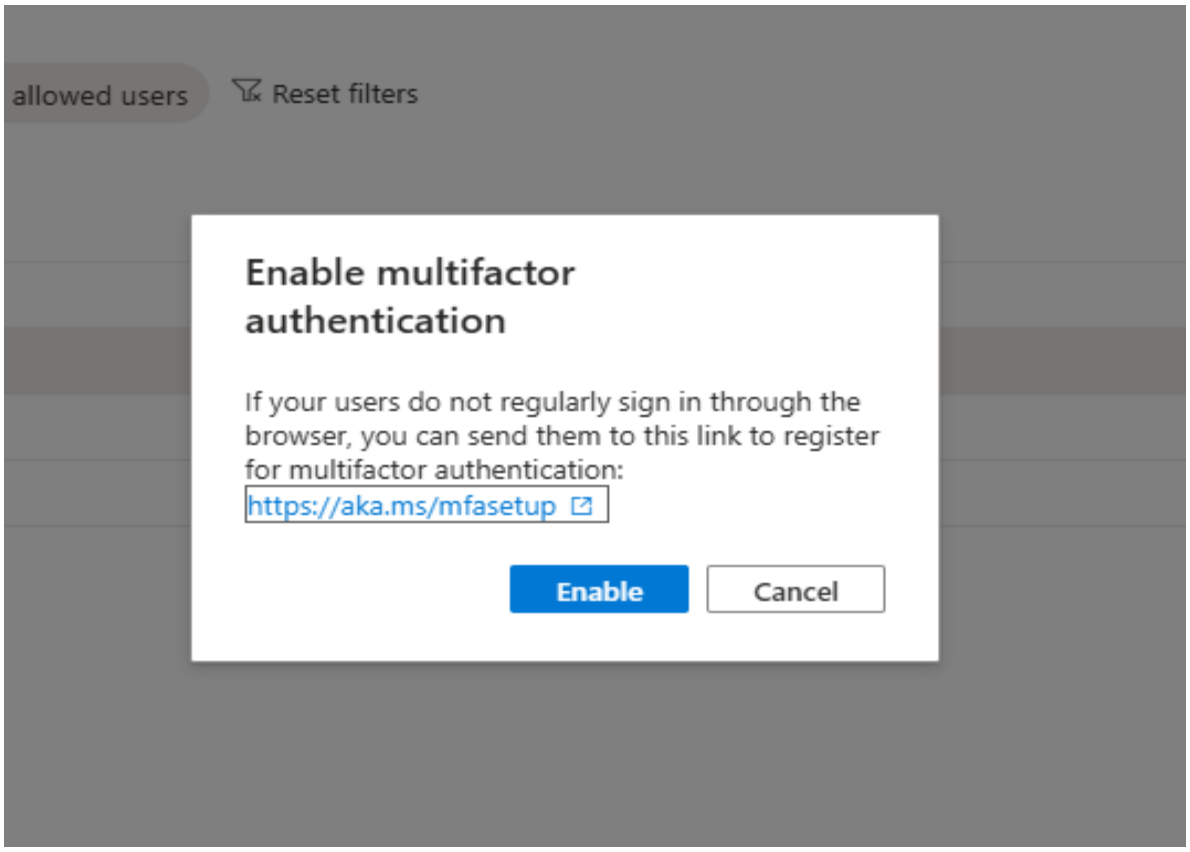
1. Go to Azure AD:
    - Open: https://portal.azure.com
    - In search bar, type: Azure Active Directory > Click it
2. Open Users Section:
    - Left menu > Click Users
3. Open the Multi-Factor Authentication Portal:
    - At the top menu, click Multi-Factor Authentication *(It opens a new browser window for MFA management.)*
4. Enable MFA for User:
    - Find your user (e.g., testuser1)
    - Check the box > Click Enable > Confirm
5. Test MFA Setup:

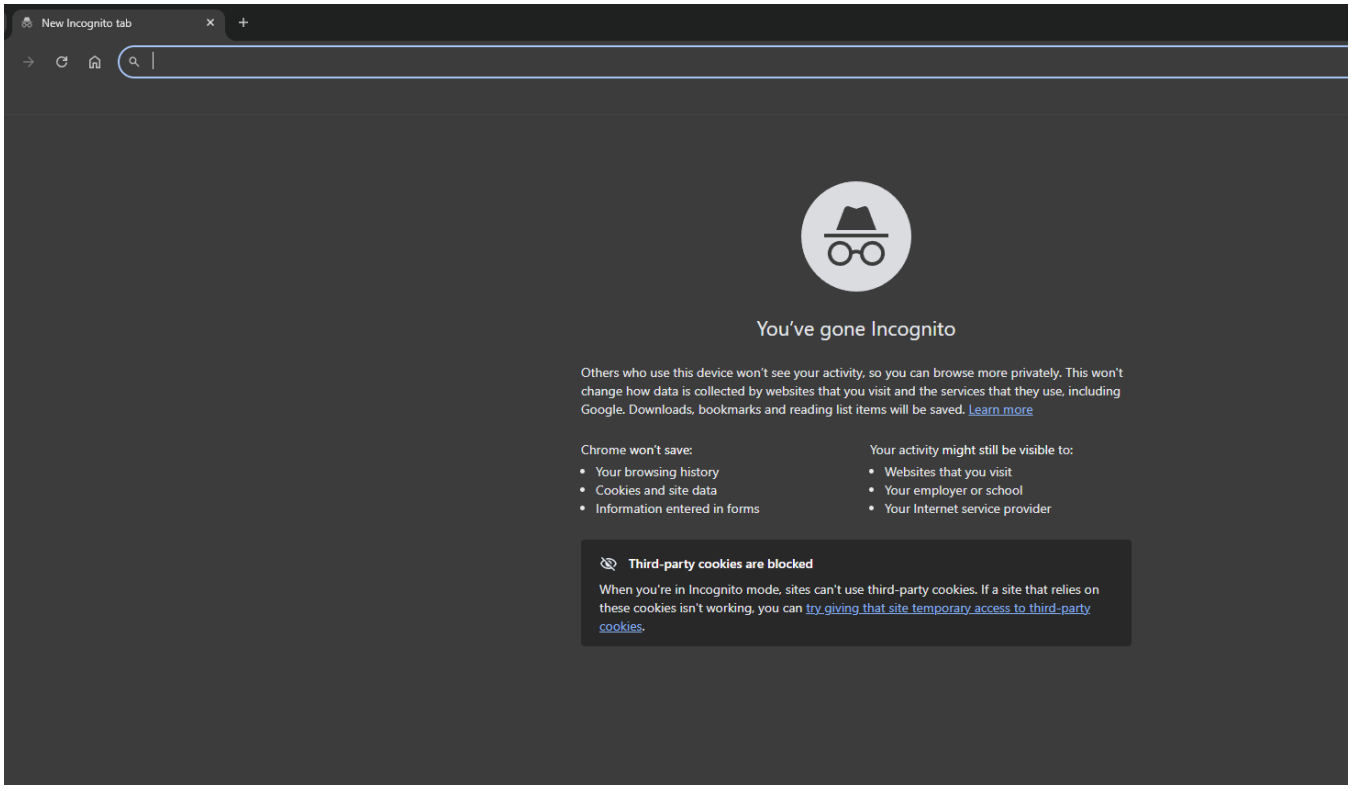
- Open an incognito browser or different browser
- Go to: https://portal.office.com
- Sign in as testuser1
- It will ask for MFA setup:
    - You can use:
        - Phone number (SMS or call)
        - Microsoft Authenticator app

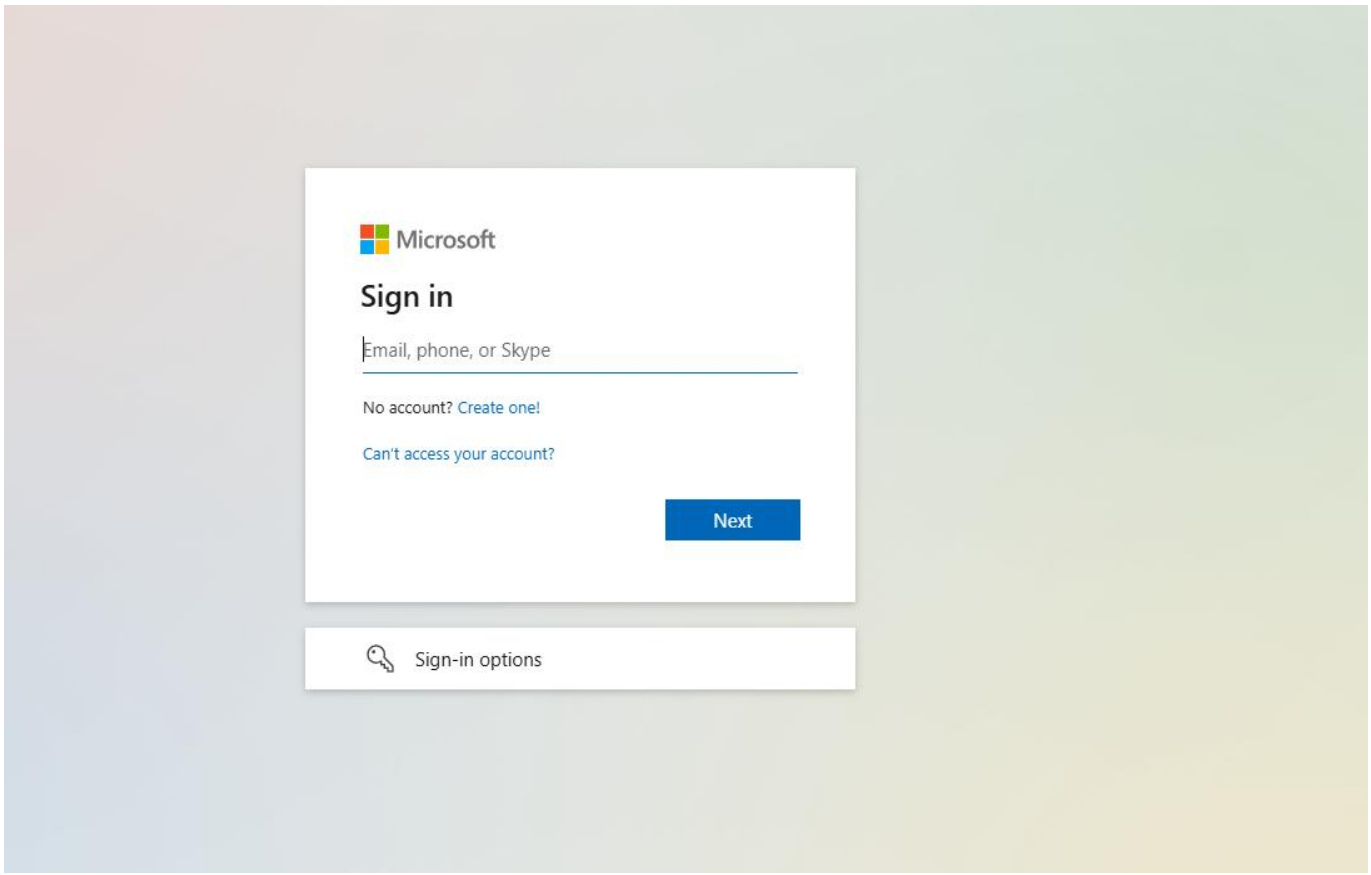


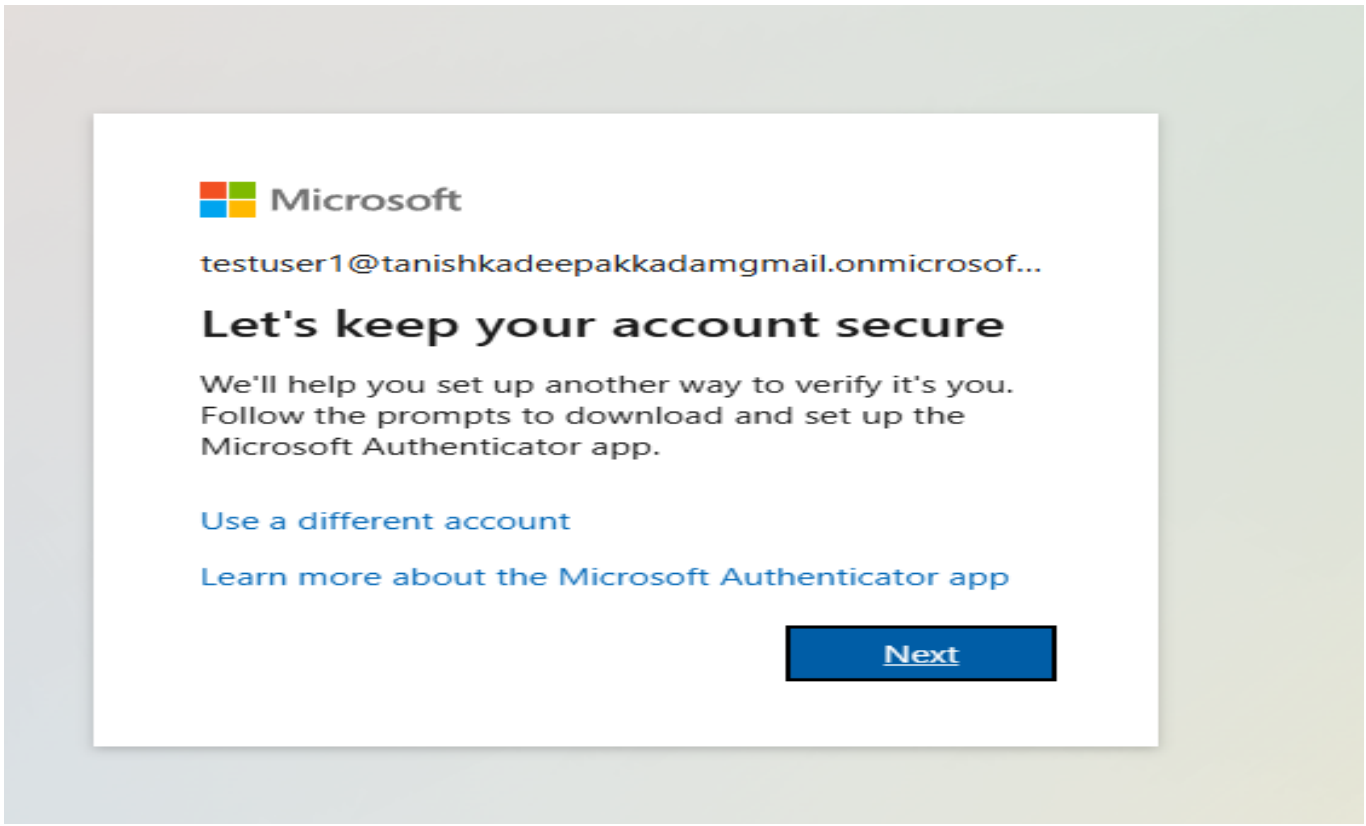

Home > Default Directory | Overview > Users >
Per-user multifactor authentication
Bulk update
Got feedback?
Users
Service settings
Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Acces
Before you begin, take a look at the multifactor authentication deployment guide.
Enable MFA
Disable MFA
Enforce MFA
User MFA settings
Search
Status : All
View : Sign-in allowed users
Reset filt
Name
UPN
Status
TANISHKA KADAM
tanishkadeepakkadam_gmail.com#EXT#@tanishkadeepak
disabled
Test User 1
testuser1@tanishkadeepakkadamgmail.onmicrosoft.com
disabled
Test User 2
testuser2@tanishkadeepakkadamgmail.onmicrosoft.com
disabled
Test User 3
testuser3@tanishkadeepakkadamgmail.onmicrosoft.com
disabled


Home > Default Directory | Overview > Users >
Per-user multifactor authentication
Bulk update
Got feedback?
Users
Service settings
Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive
Before you begin, take a look at the multifactor authentication deployment guide.
Enable MFA
Disable MFA
Enforce MFA
User MFA settings
Search
Status : All
View : Sign-in allowed use
Name
UPN
Status
TANISHKA KADAM
tanishkadeepakkadam_gmail.com#EXT#@tanishkadeepak
disabled
Test User 1
testuser1@tanishkadeepakkadamgmail.onmicrosoft.com
disabled
Test User 2
testuser2@tanishkadeepakkadamgmail.onmicrosoft.com
disabled
Test User 3
testuser3@tanishkadeepakkadamgmail.onmicrosoft.com
disabled


allowed users
Reset filters
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
Enable
Cancel


New Incognito tab
You've gone Incognito
Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites that you visit and the services that they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more
Chrome won't save:
Your browsing history
Cookies and site data
Information entered in forms
Your activity might still be visible to:
Websites that you visit
Your employer or school
Your Internet service provider
Third-party cookies are blocked
When you're in Incognito mode, sites can't use third-party cookies. If a site that relies on these cookies isn't working, you can try giving that site temporary access to third-party cookies.


Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign-in options


Microsoft
testuser1@tanishkadeepakkadamgmail.onmicrosof...
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

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

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

Let's try it out

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

16

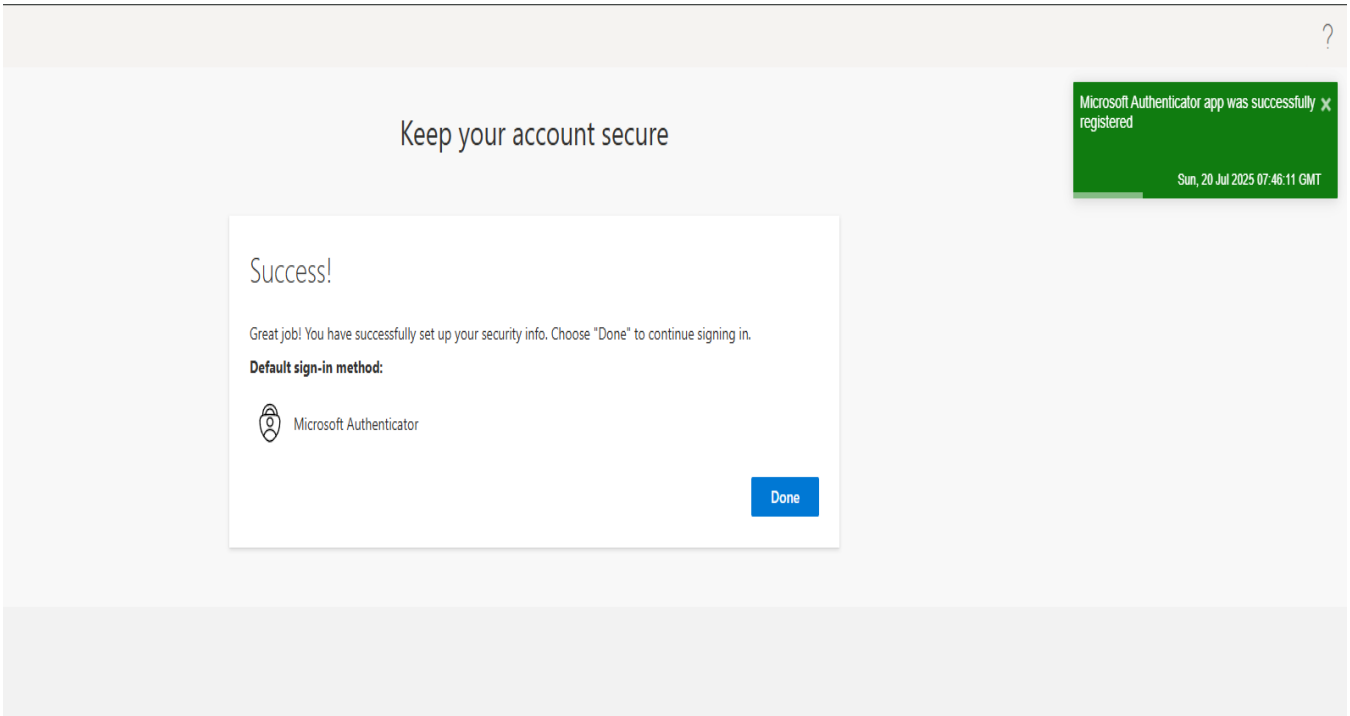
Back Next

Keep your account secure

Microsoft Authenticator

Notification approved

Next



- **Step 1.3: Configure MFA Using Conditional Access (Modern Way)**

Conditional Access is a Premium feature used to enforce MFA based on conditions like location, device compliance, or user groups. In this project, I used per-user MFA due to licensing limitations. Conditional Access allows you to **automate MFA** for **groups** instead of per-user configuration.

1. **Go to Azure AD > Security:**
    - In Azure portal, go to Azure Active Directory > Security > Conditional Access
2. **Create a New Policy:**
    - Click **+ New policy**
    - Name: Enforce MFA
3. **Assign to a Group:**
    - Under **Users or workload identities**:
        - Click **Select users and groups**

        - Choose your group: TestMFAGroup

4. **Select Cloud Apps:**
    - Click **Cloud apps or actions**
    - Choose **All cloud apps**
5. **Set Access Controls (Grant):**
    - Under **Grant**, choose:
        - **Require multi-factor authentication**
    - Click **Select**
6. **Enable the Policy:**
    - Set **Enable policy**: **On**
    - Click **Create**

MFA is now automatically required **for all users in the group** anytime they log in.

✅ **What Happens Now?**

Any user in the TestMFAGroup will **automatically be asked to set up and use MFA** during login to Office 365 or Azure.

Security | Getting started

Search

Got feedback?

- Getting started
- Diagnose and solve problems
- Protect
  - Conditional Access
  - Identity Protection
  - Security Center
  - Verified ID
- Manage
- Report
- Troubleshooting + Support

Documentation

Microsoft Entra ID offers a range of security features to protect your organization. To learn more, here are sc

- Microsoft Entra Conditional Access
- Microsoft Entra ID Protection
- Azure Security Center
- Identity Secure Score
- Named locations
- Authentication methods
- Multifactor authentication

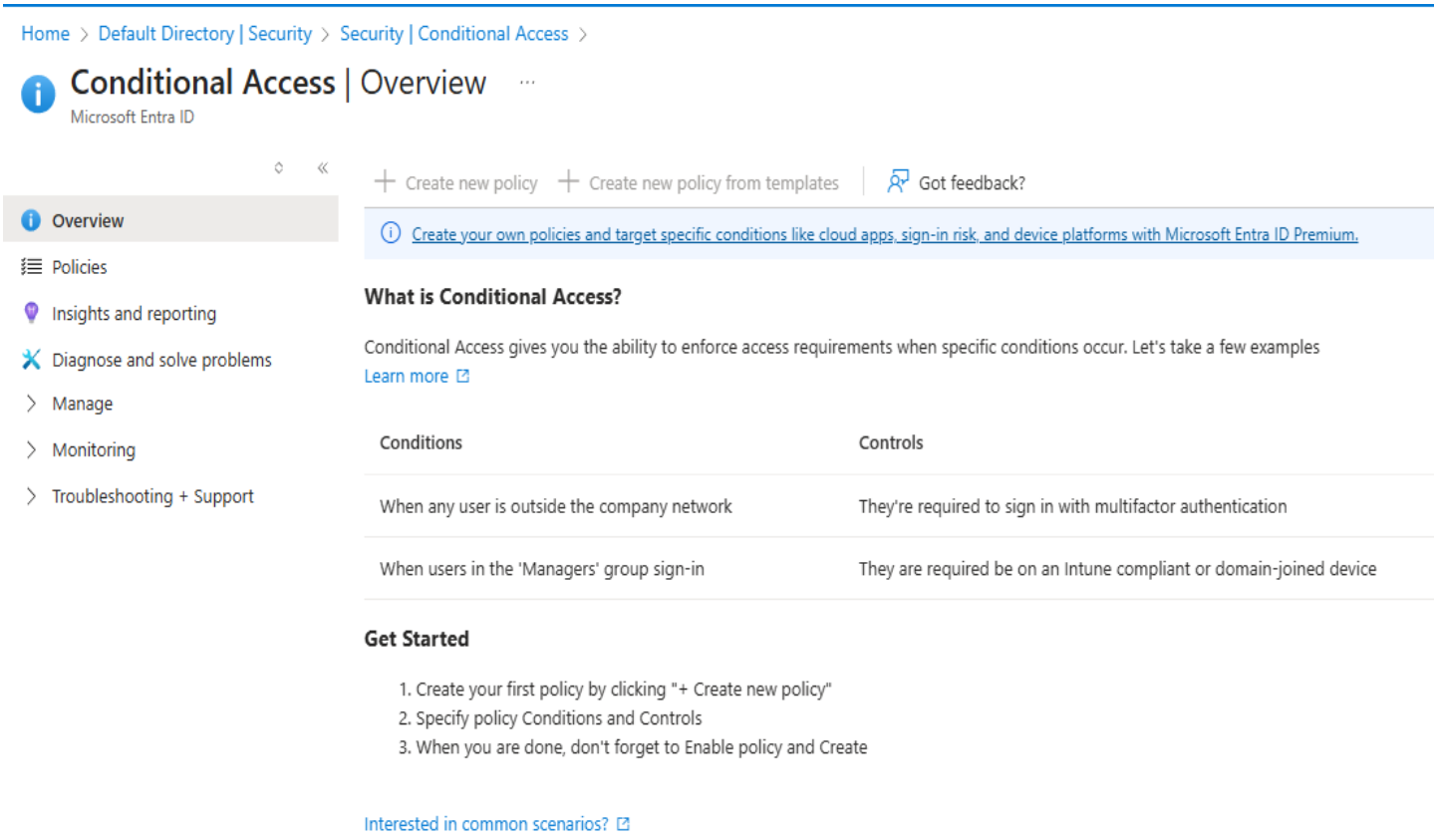
Security guidance

For a strong security posture, we recommend the following:

- 5 steps to secure your identity infrastructure
- Microsoft Entra Password Guidance
- Microsoft Entra ID Data Security Whitepaper
- How Password Hash Sync (PHS) works

Deployment guides

To deploy the above features in your organization, check out Microsoft Entra ID deployment plans.



🔹 Step 1.4: Manage MFA for Users

Let's say a user:

- Changes phone number
- Gets a new device
- Wants to reset MFA

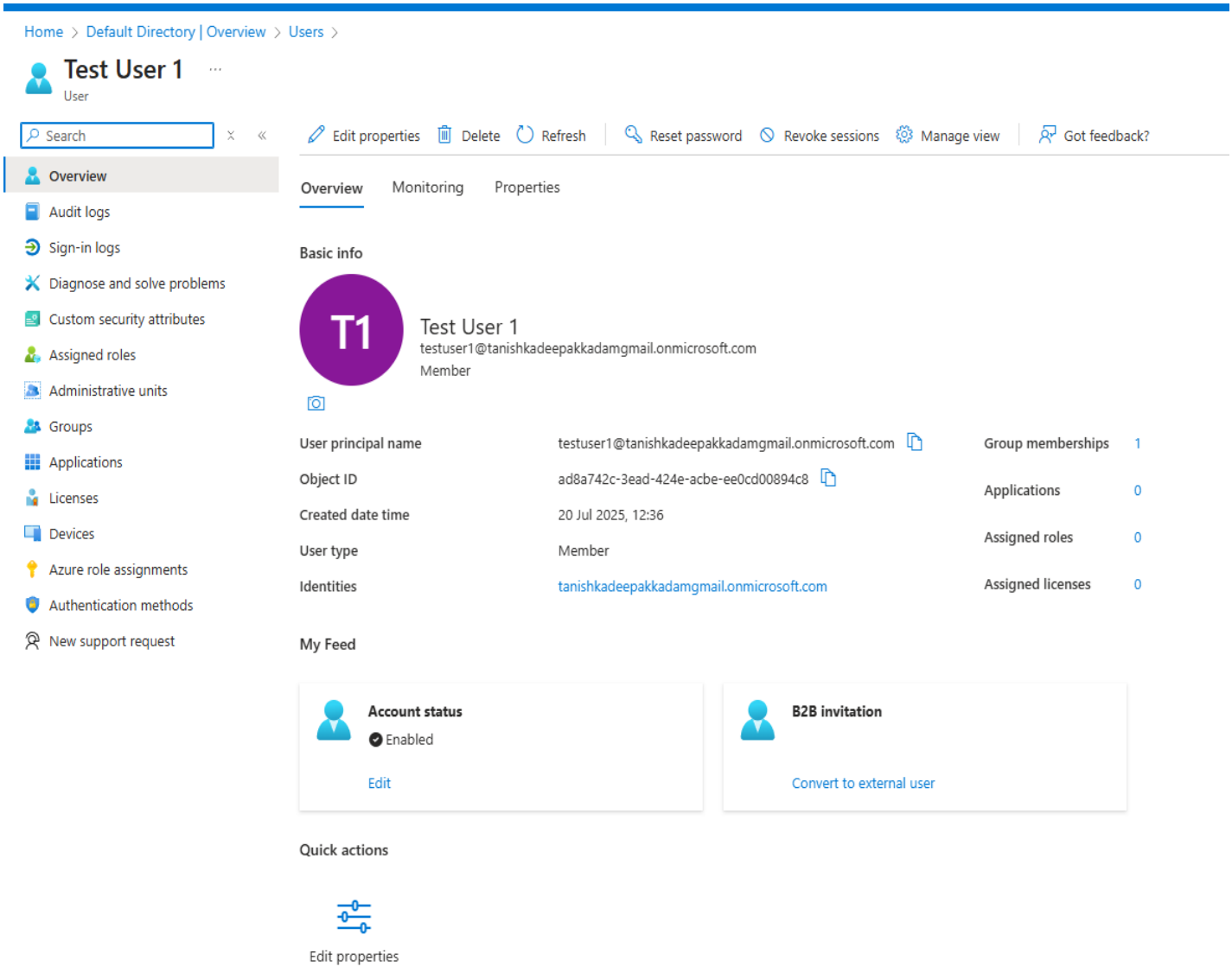
Here's how to **manage MFA settings per user**.

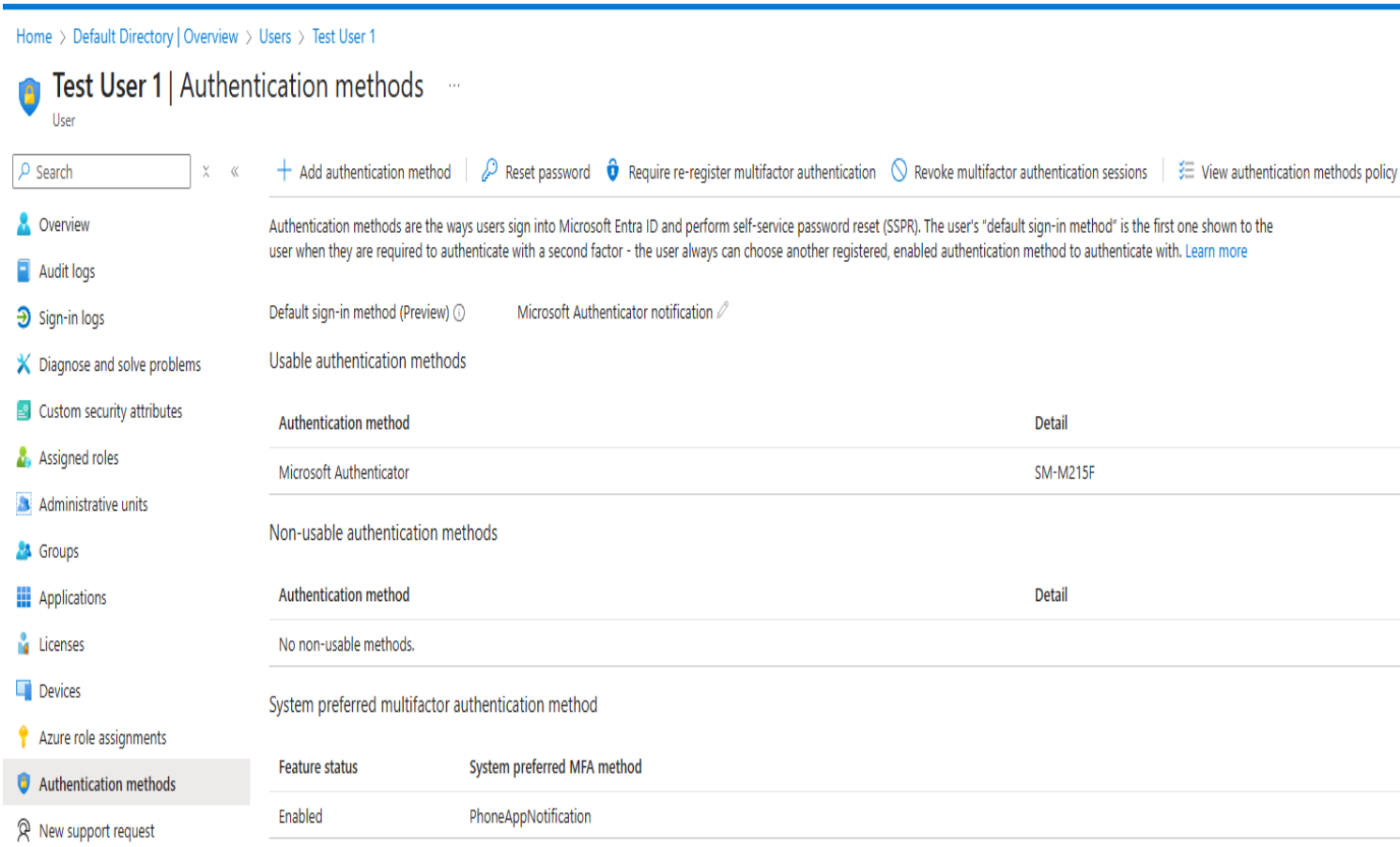
1. **Go to Azure AD > Users**
    - Find the user (e.g., testuser1)
2. **Open User Profile**
    - Click the user's name
3. **Select Authentication Methods**

- In the left pane, click **Authentication methods**

4. **You Can Now:**

Action	Description
Reset MFA	Forces user to set up MFA again
Add method	Add phone number, email, app
Remove method	Remove old phone or app





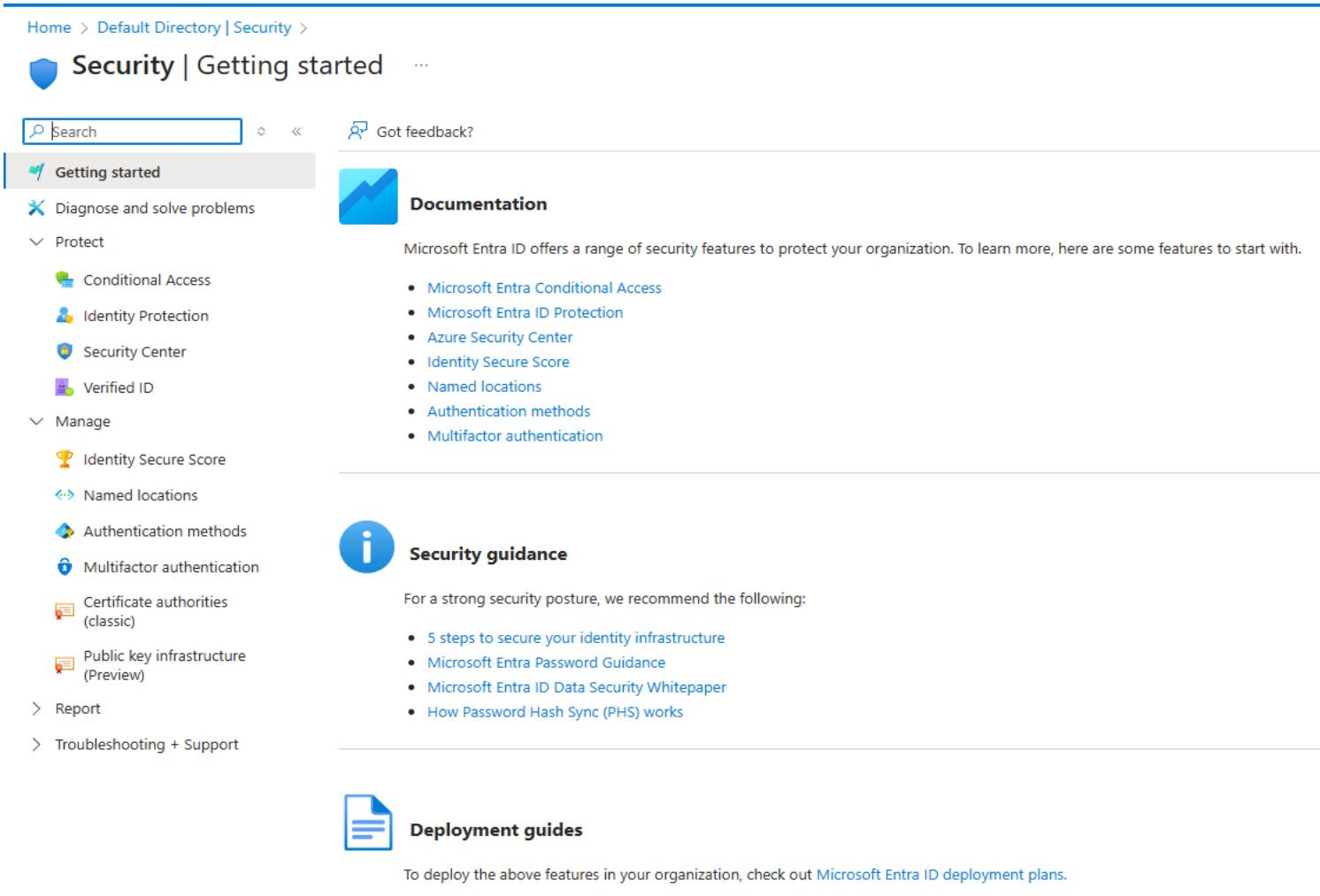
PART 2: Two-Factor Authentication & Methods

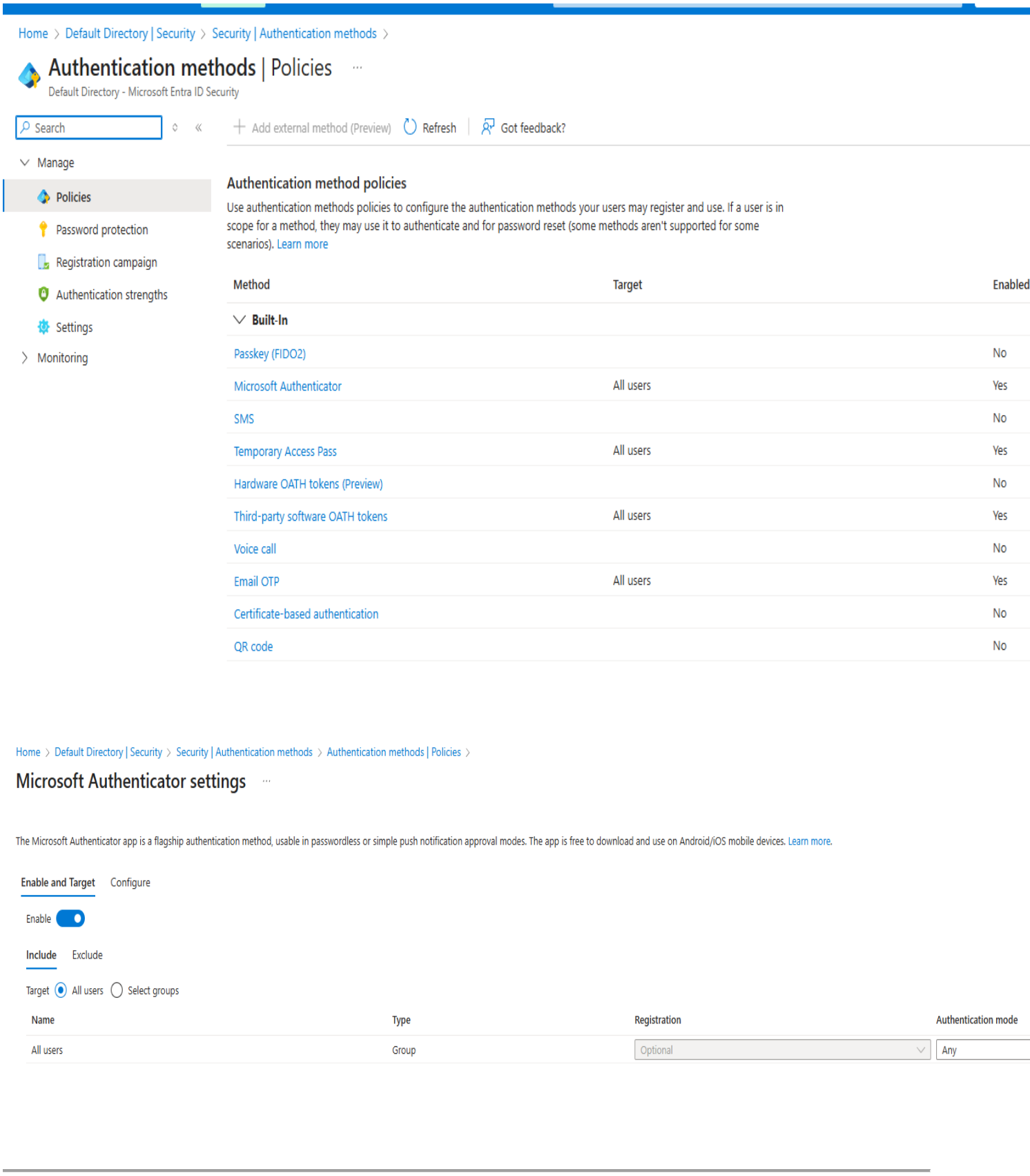
Azure supports:

Method	Description
Microsoft Authenticator	App on phone (push approval or OTP)
SMS/Text	Code sent via text message
Voice call	You get a call to approve login
OATH Token	Hardware token for OTP codes

Method	Description
FIDO2 key	Physical security key (like Yubikey)

- **Step 2.1: Enable/Disable Specific Methods**
  1. Azure AD > Security > Authentication methods
  2. Choose method (like Authenticator app) > Enable
  3. Assign to: All users or a group




Home > Default Directory | Security > Security | Authentication methods >
Authentication methods | Policies
Default Directory - Microsoft Entra ID Security
Search
Add external method (Preview)
Refresh
Got feedback?
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Authentication method policies
Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more
Method
Target
Enabled
Built-In
Passkey (FIDO2)
No
Microsoft Authenticator
All users
Yes
SMS
No
Temporary Access Pass
All users
Yes
Hardware OATH tokens (Preview)
No
Third-party software OATH tokens
All users
Yes
Voice call
No
Email OTP
All users
Yes
Certificate-based authentication
No
QR code
No

Home > Default Directory | 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

PART 3: Setup Self-Service Password Reset (SSPR)

🔹 Step 3.1: Enable SSPR

1. Azure AD > Password reset
2. Properties tab:
    - Self-Service Password Reset: Select Selected or All
    - Choose your group TestMFAGroup
    - Save

🔹 Step 3.2: Set SSPR Authentication Methods

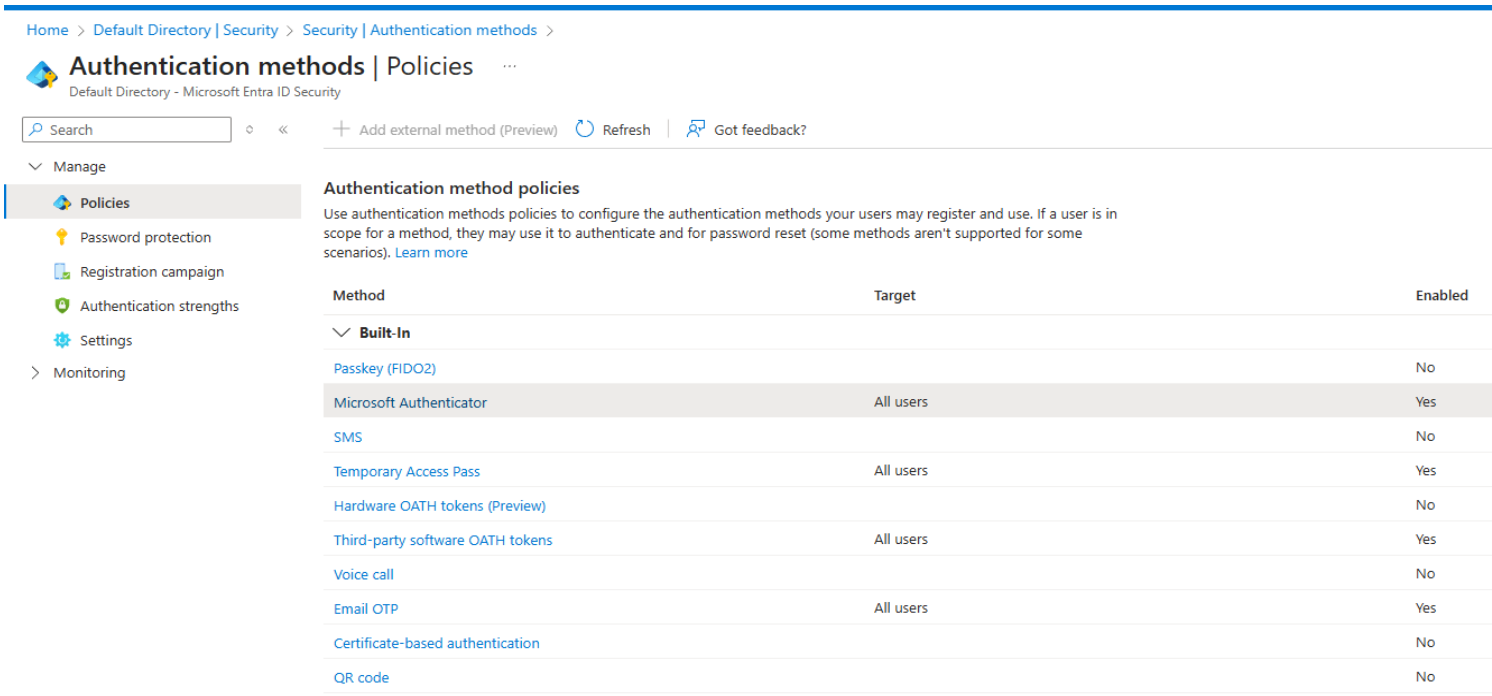
- In Authentication methods tab:
    - Number of methods required: 2
    - Select: Email, Mobile phone, Security questions

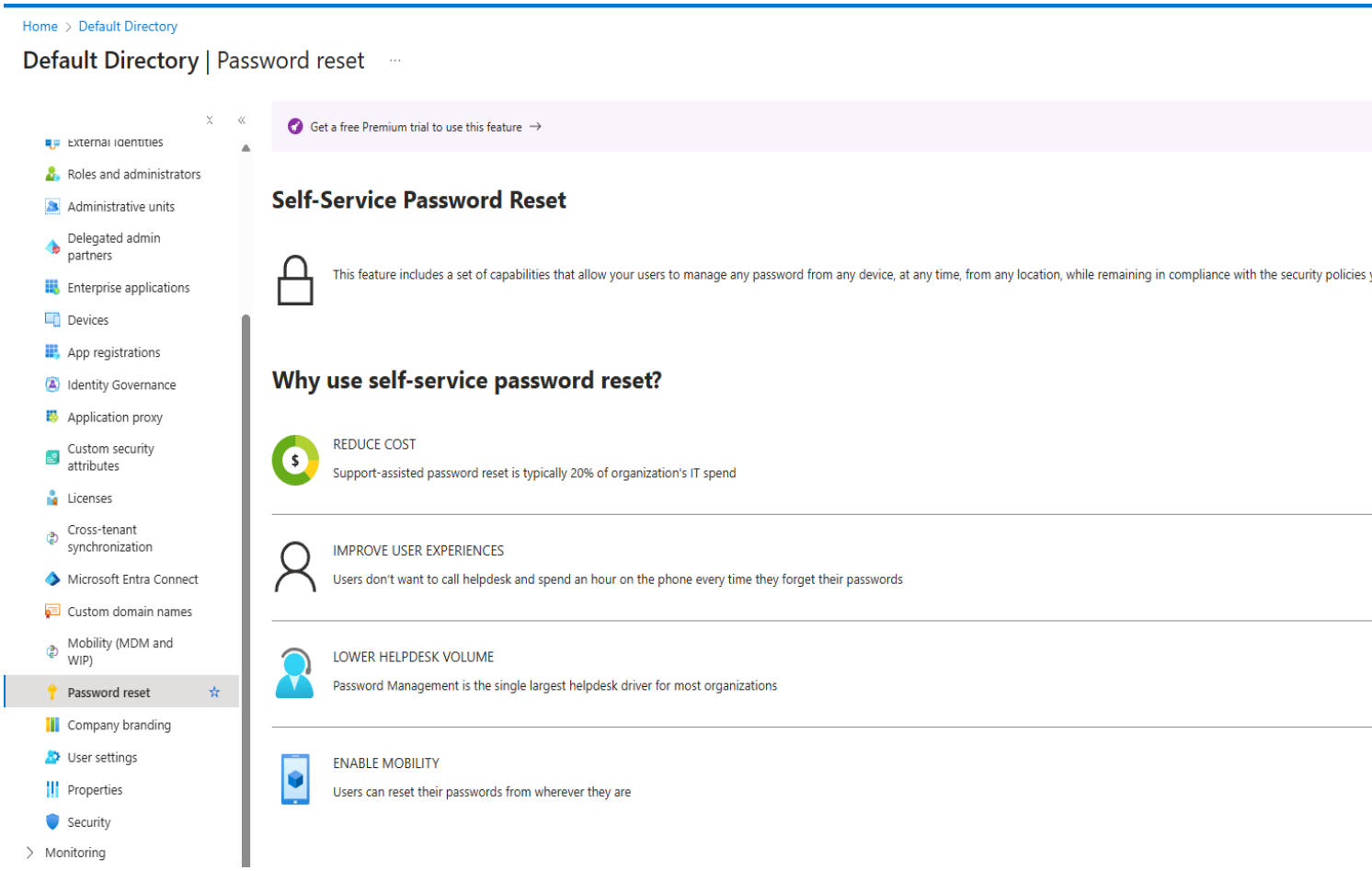
🔹 Step 3.3: Register for SSPR

Ask users to go to: https://aka.ms/ssprsetup
Have them configure their recovery email and phone.

🔹 Step 3.4: Test SSPR

- Go to: https://passwordreset.microsoftonline.com
- Enter username, follow steps to reset password using recovery method


Home > Default Directory | Security > Security | Authentication methods >
Authentication methods | Policies
Default Directory - Microsoft Entra ID Security
Search
Add external method (Preview)
Refresh
Got feedback?
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Authentication method policies
Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more
Method
Target
Enabled
Built-In
Passkey (FIDO2) No
Microsoft Authenticator All users Yes
SMS No
Temporary Access Pass All users Yes
Hardware OATH tokens (Preview) No
Third-party software OATH tokens All users Yes
Voice call No
Email OTP All users Yes
Certificate-based authentication No
QR code No


Home > Default Directory
Default Directory | Password reset
External Identities
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security attributes
Licenses
Cross-tenant synchronization
Microsoft Entra Connect
Custom domain names
Mobility (MDM and WIP)
Password reset
Company branding
User settings
Properties
Security
Monitoring
Get a free Premium trial to use this feature
Self-Service Password Reset
This feature includes a set of capabilities that allow your users to manage any password from any device, at any time, from any location, while remaining in compliance with the security policies
Why use self-service password reset?
REDUCE COST
Support-assisted password reset is typically 20% of organization's IT spend
IMPROVE USER EXPERIENCES
Users don't want to call helpdesk and spend an hour on the phone every time they forget their passwords
LOWER HELPDESK VOLUME
Password Management is the single largest helpdesk driver for most organizations
ENABLE MOBILITY
Users can reset their passwords from wherever they are

Microsoft

Get back into your account

Who are you?

To recover your account, begin by entering your email address or username and the characters in the picture or audio below.

Email or Username: *

testuser1@tanishkadeepakkadamgmail.onmicr

Example: user@contoso.onmicrosoft.com or user@contoso.com

YLXW

Enter the characters in the picture or the words in the audio. *

Next Cancel

Microsoft

Get back into your account

We're sorry

You can't reset your own password because password reset isn't set up properly for your organisation.

You must contact your administrator to both reset your password and check your organisation's setup.

Show additional details

Home › Default Directory | Security › Security | Authentication methods › Authentication methods | Policies ›

Email OTP settings ...

Email OTP sends a code to a user's email account which is then used to authenticate. >Learn more for SSPR, >learn more for external users.
For members of a tenant, email OTP is usable only for Self-Service Password Recovery. It may also be configured to be used for sign-in by guest users.

Enable and Target | Configure

Enable

Include | Exclude

Target ○ All users ◉ Select groups

Add groups

Name	Type
All users	Group

Home › Default Directory | Security › Security | Authentication methods › Authentication methods | Policies ›

SMS settings ...

This authentication method delivers a one-time code via SMS to a user's phone, and the user then inputs that code to sign-in. Learn more.
SMS is usable for multi-factor authentication and Self-Service Password Reset; it can also be configured to be used as a first factor.

Enable and Target

Enable

Include Exclude

Target All users Select groups

Name	Type	Use for sign-in
All users	Group	☑

ecurity

Add external method (Preview) Refresh Got feedback?

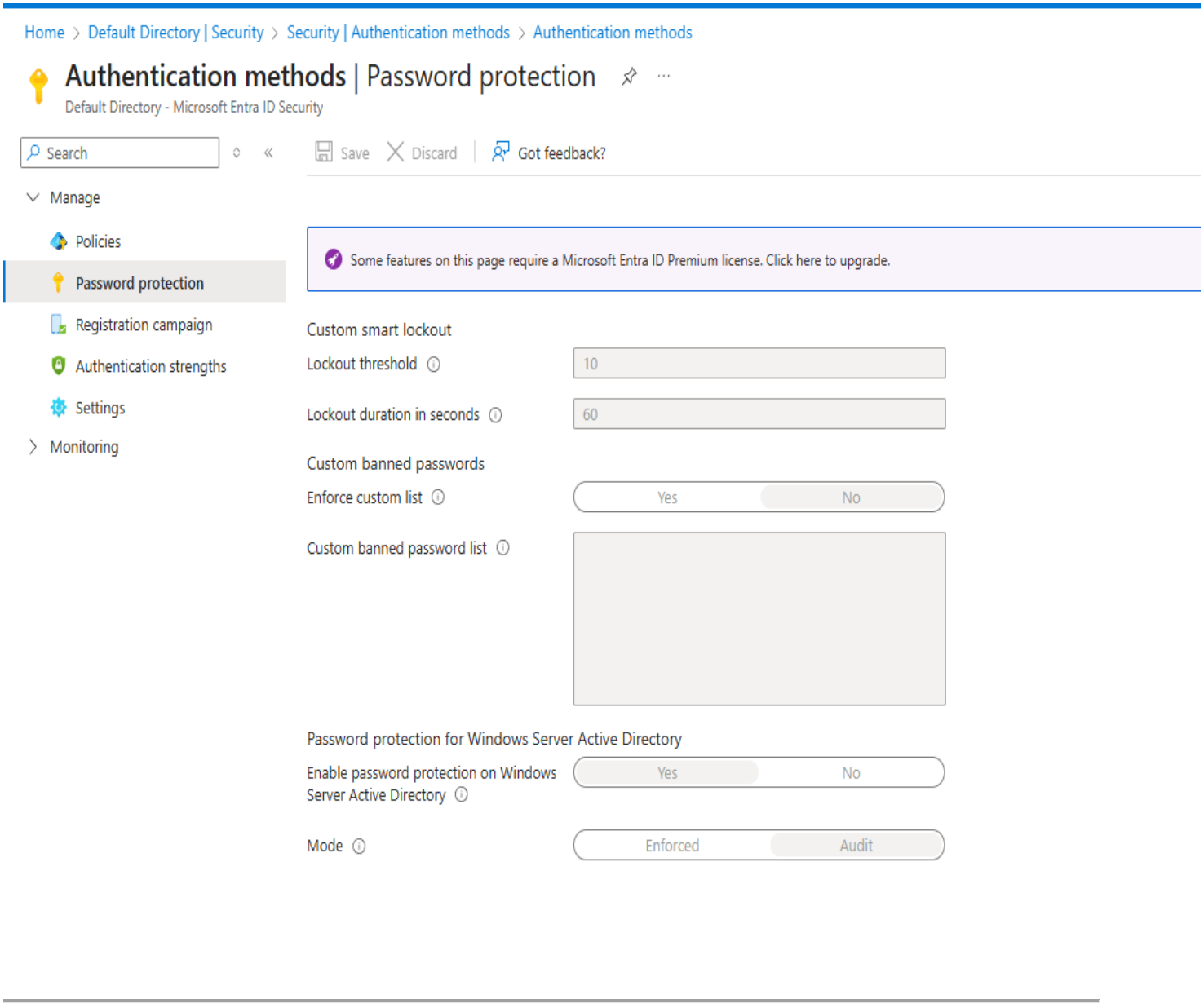
Authentication method policies

Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more

Method	Target	Enabled
Built-In		
Passkey (FIDO2)		No
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Third-party software OATH tokens	All users	Yes
Voice call		No
Email OTP	All users	Yes
Certificate-based authentication		No
QR code		No

PART 4: Account Lockout

1. Go to: Azure AD > Security > Authentication methods > Password protection
2. Configure:
    - Lockout threshold: e.g., 10 attempts
    - Lockout duration: e.g., 60 seconds
    - Custom banned passwords (optional)



PART 5: Extend MFA to On-Prem or 3rd Party

🔹 Step 5.1: Extend MFA to On-Prem Apps

Use NPS Extension to enforce MFA for:

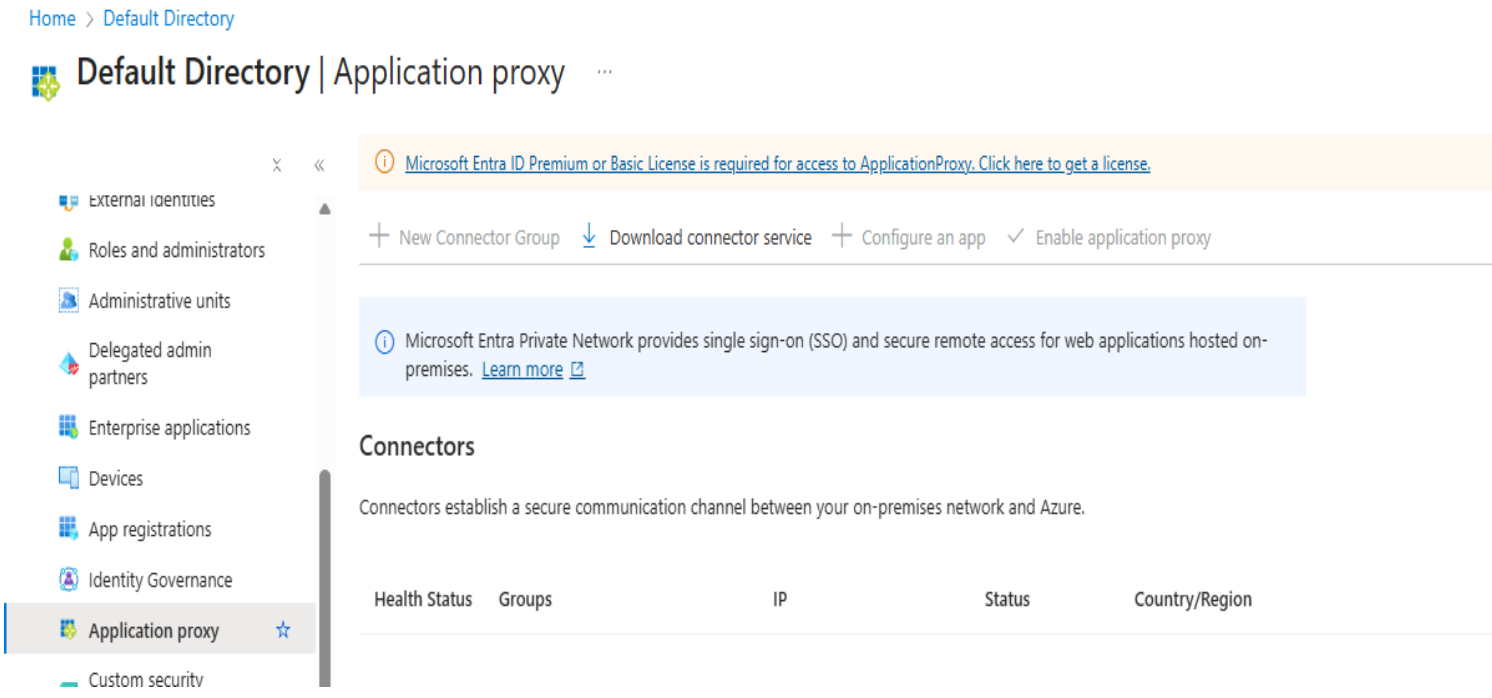
- VPN
- RADIUS-based systems

Guide:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension

🔹 Step 5.2: Extend to Web Apps

Use Azure AD Application Proxy:

1. Go to: Azure AD > Application Proxy
2. Install connector on on-prem server
3. Register app to use Azure MFA



Private Network Connector Download

Microsoft Entra ID

Download and install the Private Network connector to enable a secure connection between applications inside your network and the Private Network connector. Only one installation is necessary to service all your published applications; a second connector can be installed for high availability purposes.

System Requirements

- Operating Systems
  - Windows Server 2012 R2 or later
- Make sure the network is configured correctly for the connector.
  Learn more
- The connector must have access to all on premises applications that you intend to publish.

Installation Instructions

To install the Private Network connector, download the connector installation package and install it on a local, designated machine. For more information on the Private Network connector, see
our online content.

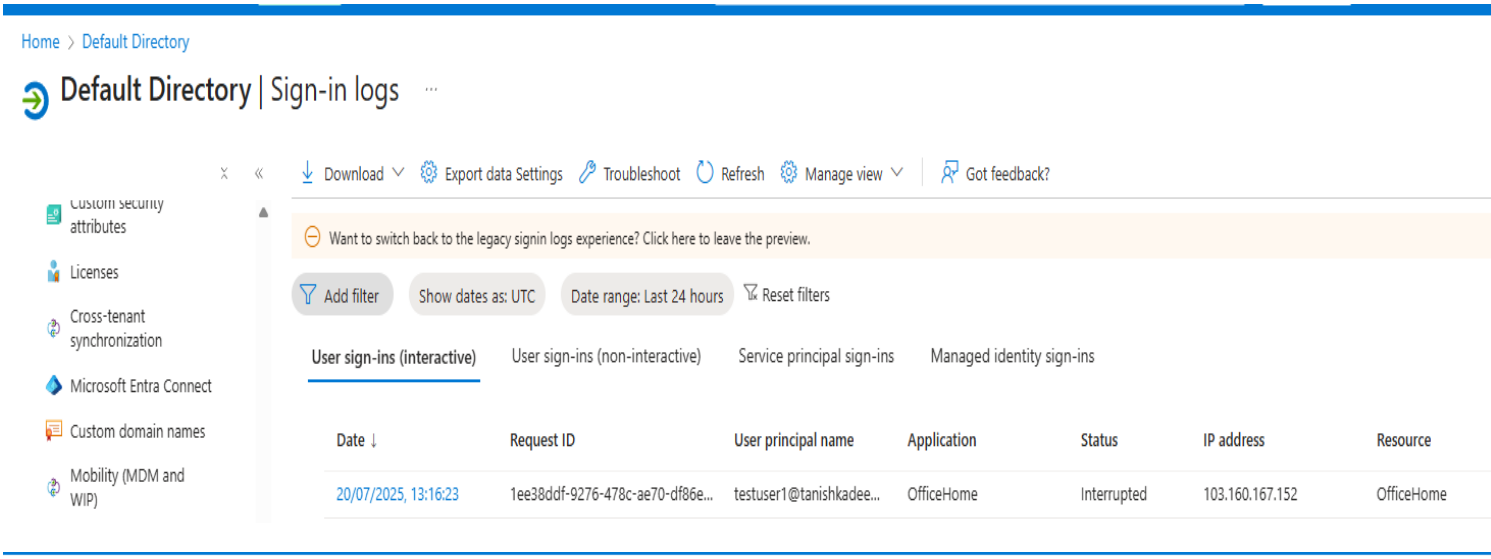
By downloading the connector, you accept our
Terms of Service.

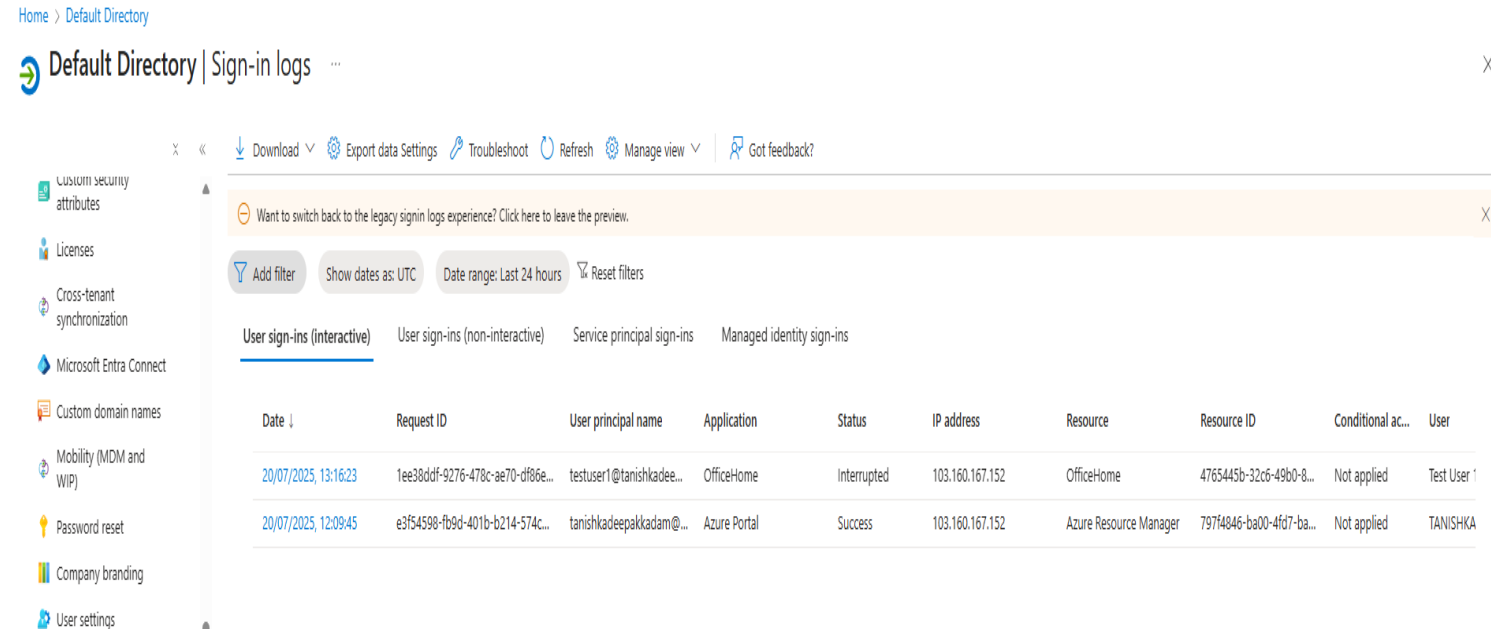
Accept terms & Download

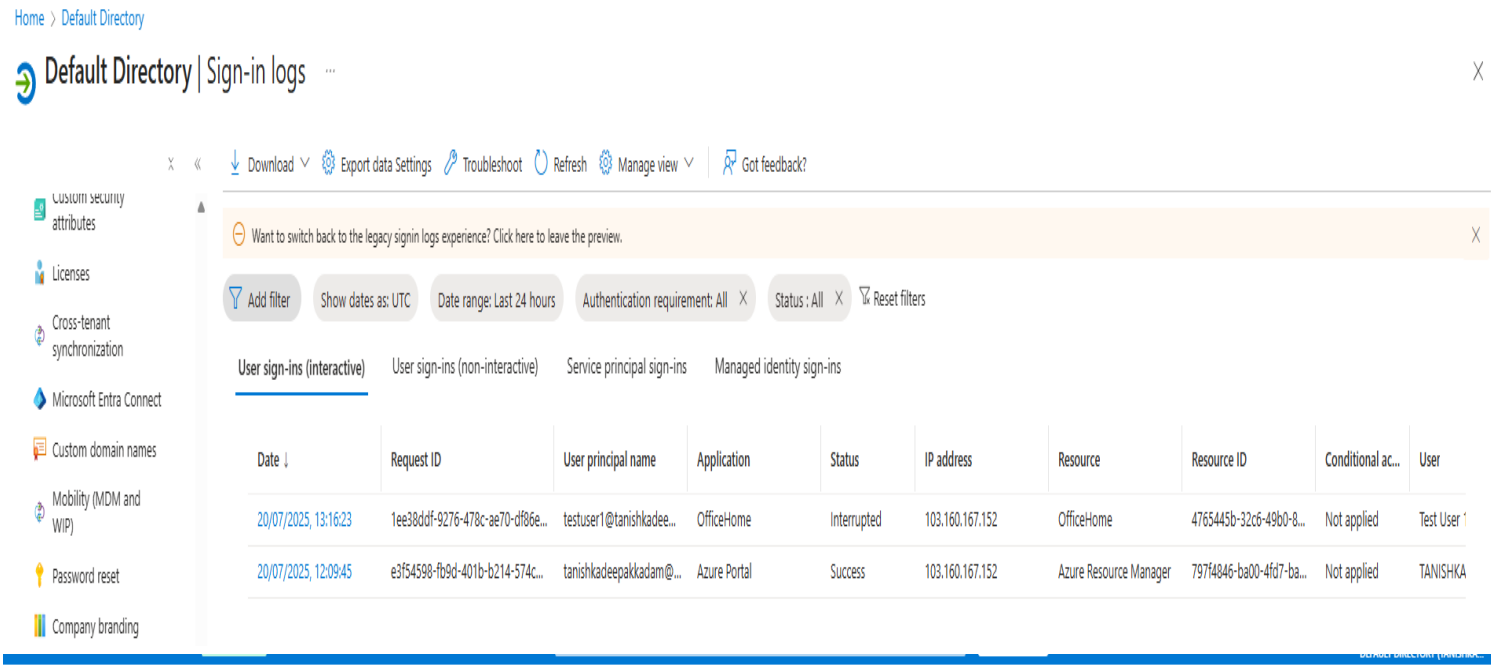
PART 6: Monitor MFA Activity

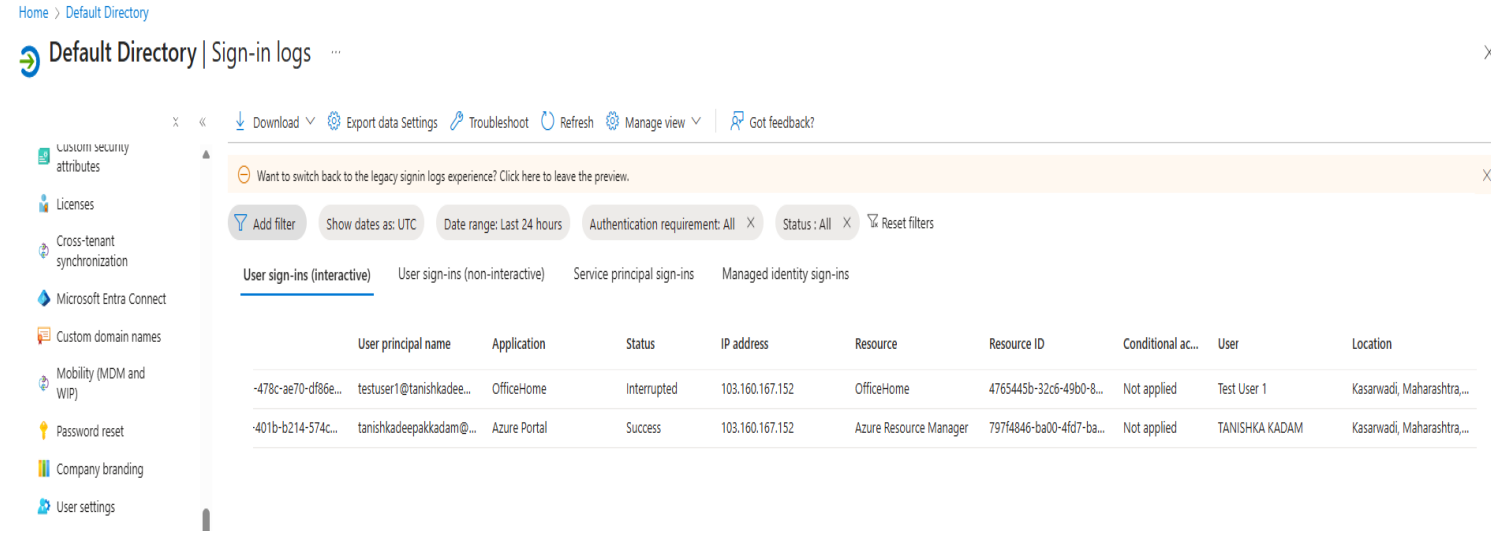
Step 6.1: Monitor Sign-ins and MFA Status

1. Azure AD > Sign-ins
2. Filter by:
    - Status (Success/Failure)
    - MFA required
    - Conditional access policy









◆ Step 6.2: SSPR Reporting

1. Azure AD > Password reset > Usage & Insights
2. View:
    - Who reset passwords
    - Success/Failure
    - Which methods used

PART 7: OAuth Tokens

🔹 Step 7.1: What is OAuth in Azure?

OAuth allows apps to get access tokens from Azure AD. OAuth is an open standard protocol that allows third-party applications to access user resources without exposing the password. In Azure AD, OAuth tokens are issued when users sign into apps like Microsoft Teams, Outlook, or third-party services registered under Azure AD.

Example:

- A web app asks you to sign in with Microsoft
- You approve it
- Azure AD gives that app a token to access your email/profile/etc.

🔹 Step 7.2: View OAuth Tokens

1. Azure AD > Enterprise Applications
2. Click an app > Go to Permissions
3. Shows OAuth tokens and permissions granted
