

AZURE MULTIFACTOR AUTHENTICATION (MFA)

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

- 1. Configure & manage Azure Multifactor Authentication (MFA)**
- 2. Two Factor authentication**
- 3. Different methods of the two factor authentication**
- 4. Setup self-service password reset:**
- 5. Configure MFA**
- 6. Configure and deploy self-service password reset**
- 7. Implement and manage Azure MFA settings**
- 8. Account Lockout**
- 9. Manage MFA settings for users**
- 10. Extend Azure AD MFA to third party and on-premises devices**
- 11. Monitor Azure AD MFA activity**
- 12. OAuth Tokens.**

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

- o Configure MFA and SSPR
- o Monitor security settings

Microsoft Azure Upgrade Search resources, services, and docs (G+) Copilot

Home > **i Default Directory | Overview**

Add Manage tenants What's new Preview features Got feedback?

Overview Preview features Diagnose and solve problems

Manage Monitoring Properties Recommendations Setup guides

Search your tenant

Basic information

Name	Default Directory	Users	1
Tenant ID	0437b39c-0850-472f-aa19-f1915bbef0d	Groups	0
Primary domain	tanishkadeepakkadam@gmail.onmicrosoft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

⚠️ **Migrate to the converged Authentication methods policy**

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact

[Learn more](#)

My feed

Try Microsoft Entra admin center
Secure your identity environment with Microsoft Entra ID, permissions management and more.

TANISHKA KADAM
09040e0d-052b-4986-a36d-cc1dd0c07be View role information

Secure Score for Identity
42.11%
Secure score updates can take up to 48 hours.

Add or remove favorites by pressing Ctrl+Shift+F

Home >

i Default Directory | Overview

The screenshot shows the Azure AD Default Directory Overview page. At the top, there's a navigation bar with 'Add', 'Manage tenants', 'What's new', 'Preview features', and 'Got feedback?'. On the left, a sidebar lists 'Overview' (selected), 'Preview features', 'Diagnose and solve problems', 'Manage', 'Monitoring', and 'Troubleshooting + Support'. The main content area has three sections: 'Try Microsoft Entra admin center' (with a link to 'Go to Microsoft Entra'), 'Microsoft Entra Connect' (status: 'Not enabled', last sync: 'Sync has never run', with a link to 'Go to Microsoft Entra Connect'), and 'Secure Score for Identity' (score: '42.11%', note: 'Secure score updates can take up to 48 hours', with a link to 'View secure score'). Below these are 'Feature highlights' for 'Identity Protection', 'Access reviews', 'Authentication methods', 'Microsoft Entra Domain Services', 'Tenant restrictions', and 'Entra Permissions Management'. At the bottom, there's a 'Quick actions' section with icons for 'Add user', 'Add group', 'Add enterprise application', and 'Add application registration'. A note at the bottom left says 'Add or remove favorites by pressing Ctrl+Shift+F'.

◆ 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:

- o **User name:** testuser1 (this becomes the email like `testuser1@yourdomain.onmicrosoft.com`)
- o **Name:** Test User 1

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

4. Click Create.

5. Repeat for testuser2, testuser3.

Default Directory | Overview

Overview

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Basic information

Name	Default Directory	Users	1
Tenant ID	0437b39c-0850-472f-aa19-f1915fbbe0d4	Groups	0
Primary domain	tanishkadeepakkadam@gmail.onmicrosoft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

Migrate to the converged Authentication methods policy

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact.

[Learn more](#)

My feed

Try Microsoft Entra admin center

Secure your identity environment with Microsoft Entra ID, permissions management and more.

TANISHKA KADAM
09040e0d-052b-4986-a36d-cc0000000000
Global Administrator
[View role information](#)

Secure Score for Identity
42.11%
Secure score updates can take up to 24 hours.

 **Users** ...
Default Directory

X « + New user Edit Delete Download users Bulk operations Refresh Manage view | Per-user MFA Got it

All users (1 user found) Search Add filter

	Display name ↑	User principal name ↑	User type	On-premises sync	Identities	Company
	TK TANISHKA KADAM	tanishkadeepakkad... 	Member	No	MicrosoftAccount	

 Audit logs
 Sign-in logs
 Diagnose and solve problems
 Deleted users
 Password reset
 User settings
 Bulk operation results
 New support request

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 

Create new user

...

Create a new internal user in your organization

Basics

Properties

Assignments

Review + create

Basics

User principal name	testuser1@tanishkadeepakkadam@gmail.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

Users ...
Default Directory

X << + New user Edit Delete Download users Bulk operations Refresh Manage view Per-user M...

All users (1) Azure Active Directory is now Microsoft Entra ID.

Audit logs Sign-in logs Diagnose and solve problems Deleted users Password reset User settings Bulk operation results

Search Add filter 2 users found

	Display name ↑	User principal name ↓	User type	On-premises sy...	Identities
<input type="checkbox"/>	TK TANISHKA KADAM	tanishkadeepakka...	Member	No	MicrosoftAccount
<input type="checkbox"/>	TU Test User 1	testuser1@tanish...	Member	No	tanishkadeepakkadamg...

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + createCreate 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

Users

Default Directory

All users	i Azure Active Directory is now Microsoft Entra ID.				
	Search	Add filter			
3 users found					
	<input type="checkbox"/> Display name ↑	User principal name ↑↓	User type	On-premises syn...	Identities
TANISHKA KADAM	TK	tanishkadeepakka...		Member	No
Test User 1	TU	testuser1@tanish...		Member	No
Test User 2	TU	testuser2@tanish...		Member	No

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

@ tanishkadeepakkadam...



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

The screenshot shows the Azure Active Directory Users page. On the left, there's a sidebar with links like All users, Audit logs, Sign-in logs, Diagnose and solve problems, Deleted users, Password reset, User settings, Bulk operation results, and New support request. The main area has a search bar and a table displaying user information. The table columns are: Display name, User principal name, User type, On-premises sync status, and Identities. The users listed are:

Display name	User principal name	User type	On-premises sync	Identities
TANISHKA KADAM	tanishkadeepakka...	Member	No	MicrosoftAccount
Test User 1	testuser1@tanish...	Member	No	tanishkadeepakkadam...
Test User 2	testuser2@tanish...	Member	No	tanishkadeepakkadam...
Test User 3	testuser3@tanish...	Member	No	tanishkadeepakkadam...

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:
 - o **Group type:** Security
 - o **Group name:** TestMFAGroup
 - o **Group description:** Group for MFA/SSPR testing
 - o **Membership type:** Assigned
5. Click **No members selected** > Click **+ Add members**
6. Search and select:
 - o testuser1
 - o testuser2 (or any other test users you created)
7. Click **Select** > then **Create**

Groups | Overview

Default Directory

...



New group



Download groups



Preview features

Overview

All groups

Deleted groups

Diagnose and solve problems

> Settings

> Activity

> Troubleshooting + Support

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

X

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

Selected (3)

↶ Reset



Test User 1

testuser1@tanishkadeepakkadam@gmail.on...



Test User 2

testuser2@tanishkadeepakkadam@gmail.on...



Test User 3

testuser3@tanishkadeepakkadam@gmail.on...



Select

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

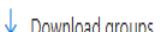
3 members selected

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

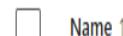


Search

Add filter

Search mode  Contains

1 group found



Name ↑

Object Id

Group type

Members



2173672c-8d0c-44b4-9061-af4ad3848fcb



TestMFAGroup

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 >

The screenshot shows the 'Users' page in the Azure portal. The top navigation bar includes links for 'New user', 'Edit', 'Delete', 'Download users', 'Bulk operations', 'Refresh', 'Manage view', and 'Per-user MFA'. On the left, a sidebar lists various logs and diagnostic tools. The main table displays four user entries:

	Display name ↑	User principal name ↑	User type	On-premises sync	Identities
	TK TANISHKA KADAM	tanishkadeepakka...	Member	No	MicrosoftAccount
	TU Test User 1	testuser1@tanish...	Member	No	tanishkadeepakkadam...
	TU Test User 2	testuser2@tanish...	Member	No	tanishkadeepakkadam...
	TU Test User 3	testuser3@tanish...	Member	No	tanishkadeepakkadam...

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 Access policies.

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 filter

<input type="checkbox"/>	Name ↑↓	UPN	Status
<input type="checkbox"/>	TANISHKA KADAM	tanishkadeepakkadam_gmail.com#EXT#@tanishkadeepak	disabled
<input type="checkbox"/>	Test User 1	testuser1@tanishkadeepakkadamgmail.onmicrosoft.com	disabled
<input type="checkbox"/>	Test User 2	testuser2@tanishkadeepakkadamgmail.onmicrosoft.com	disabled
<input type="checkbox"/>	Test User 3	testuser3@tanishkadeepakkadamgmail.onmicrosoft.com	disabled

Per-user multifactor authentication

[Bulk update](#) | [Got feedback?](#)

[Users](#) [Service settings](#)

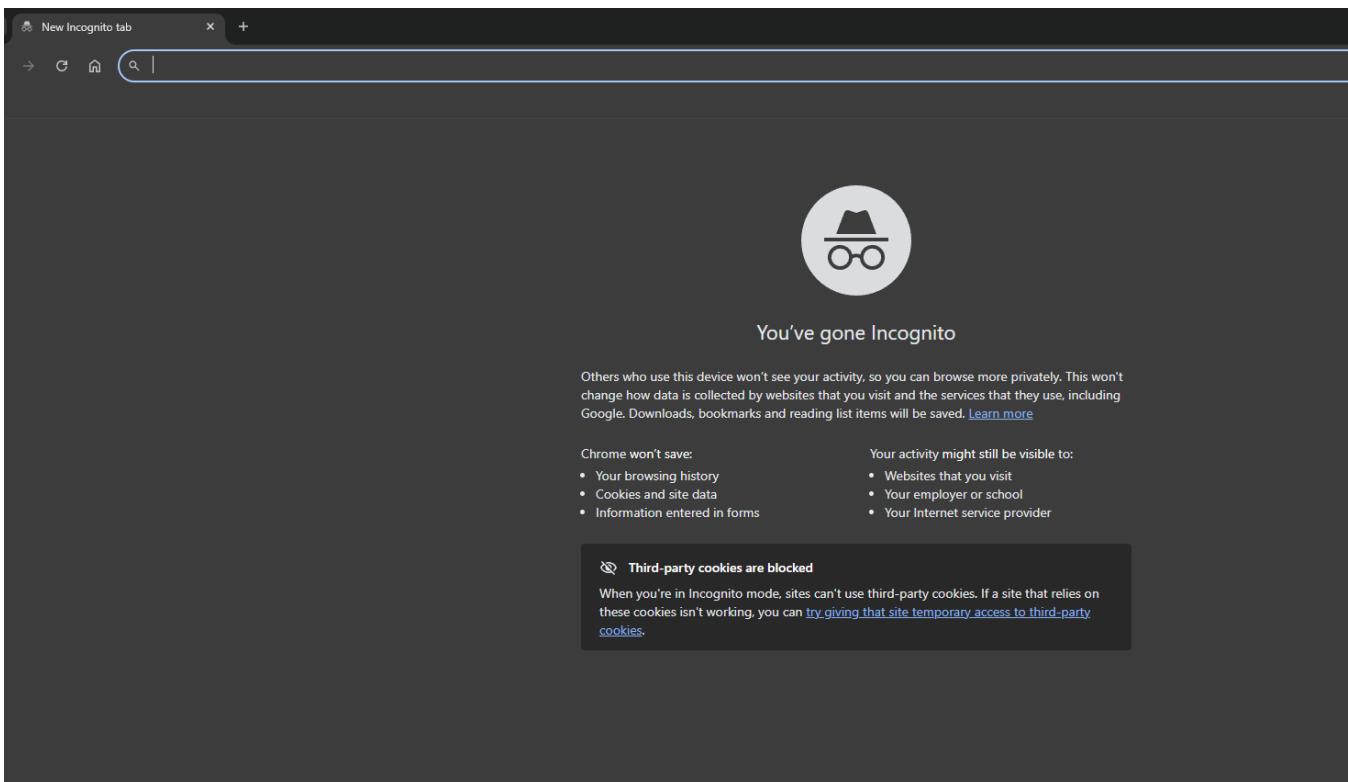
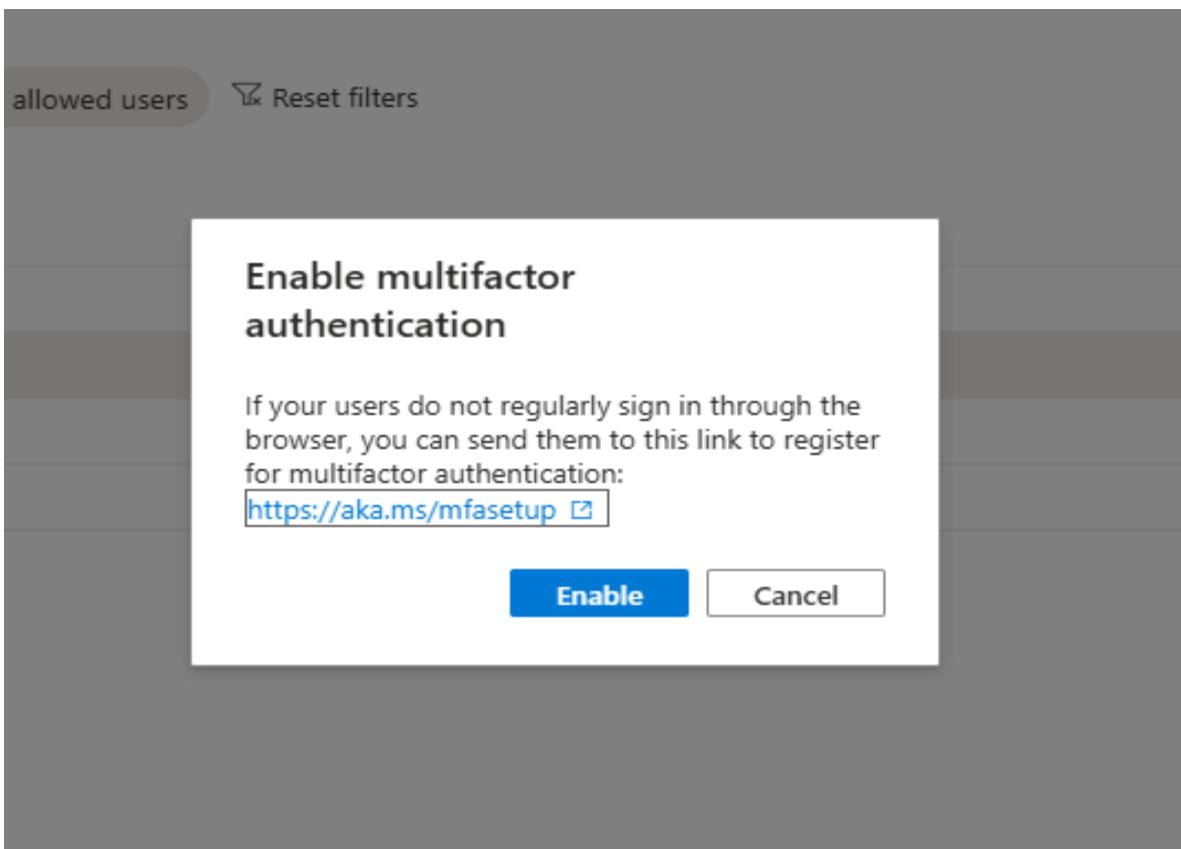
Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies.

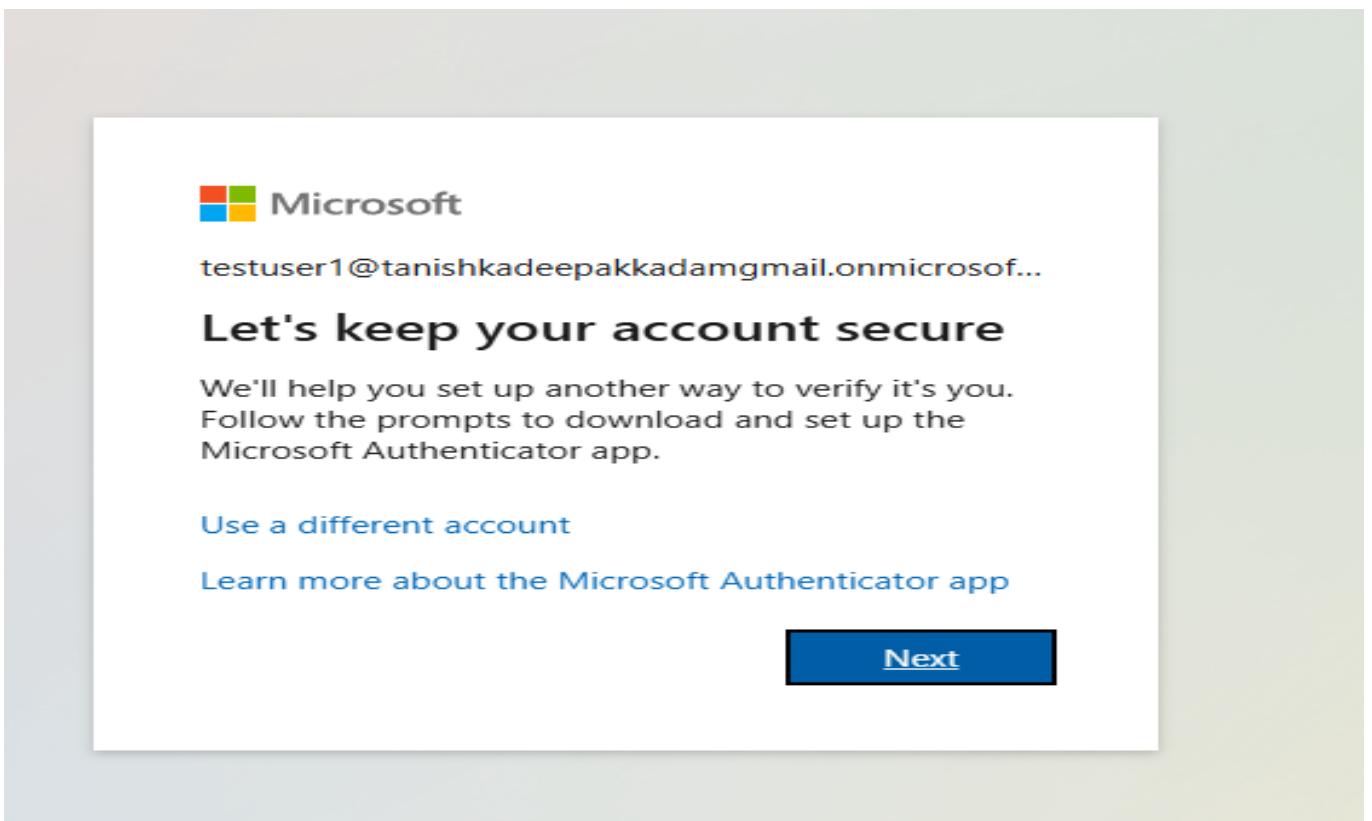
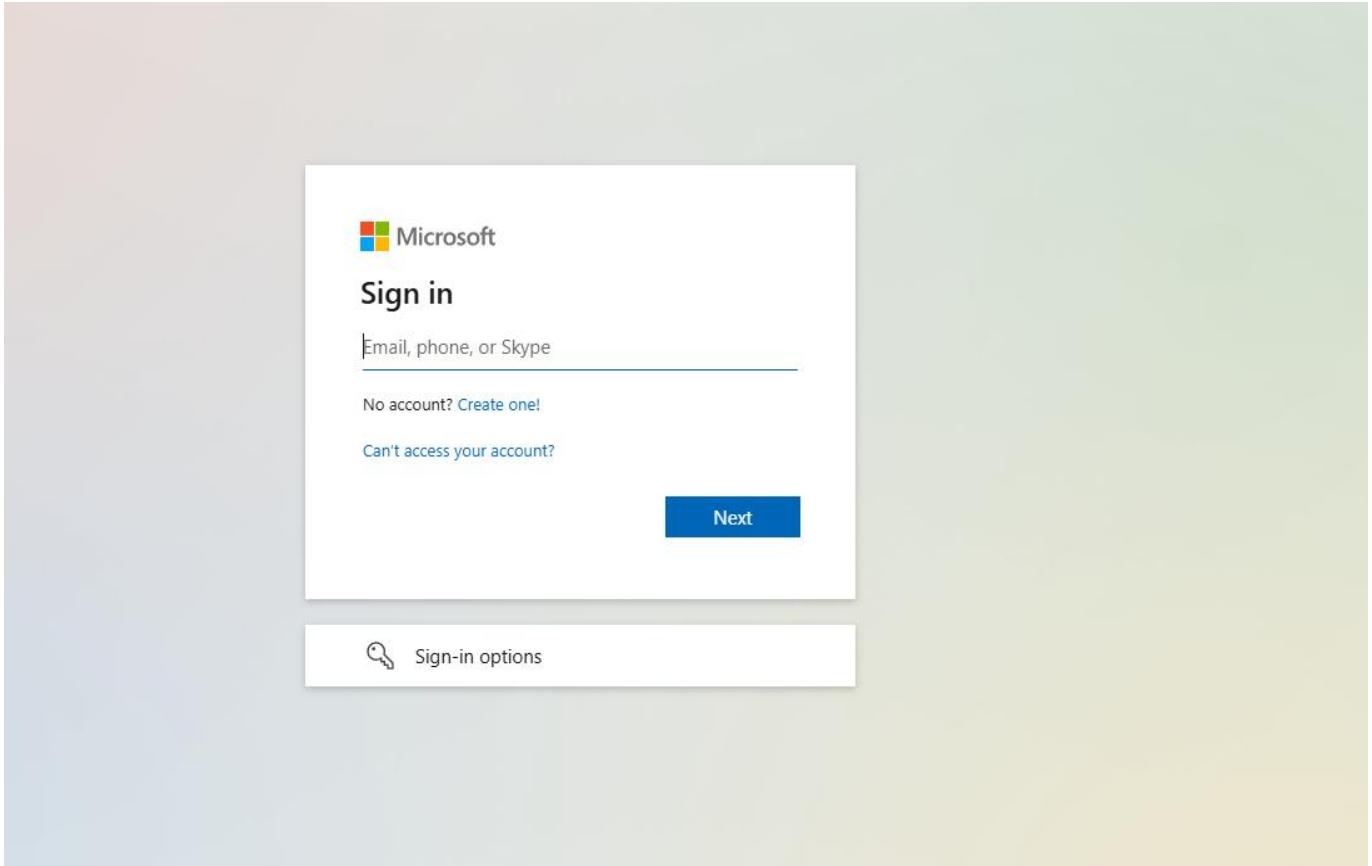
Before you begin, take a look at the [multifactor authentication deployment guide](#).

Enable MFA Disable MFA Enforce MFA User MFA settings

Search Status : All View : Sign-in allowed users

<input type="checkbox"/>	Name ↑↓	UPN	Status
<input type="checkbox"/>	TANISHKA KADAM	tanishkadeepakkadam_gmail.com#EXT#@tanishkadeepak	disabled
<input checked="" type="checkbox"/>	Test User 1	testuser1@tanishkadeepakkadamgmail.onmicrosoft.com	disabled
<input type="checkbox"/>	Test User 2	testuser2@tanishkadeepakkadamgmail.onmicrosoft.com	disabled
<input type="checkbox"/>	Test User 3	testuser3@tanishkadeepakkadamgmail.onmicrosoft.com	disabled





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](#)

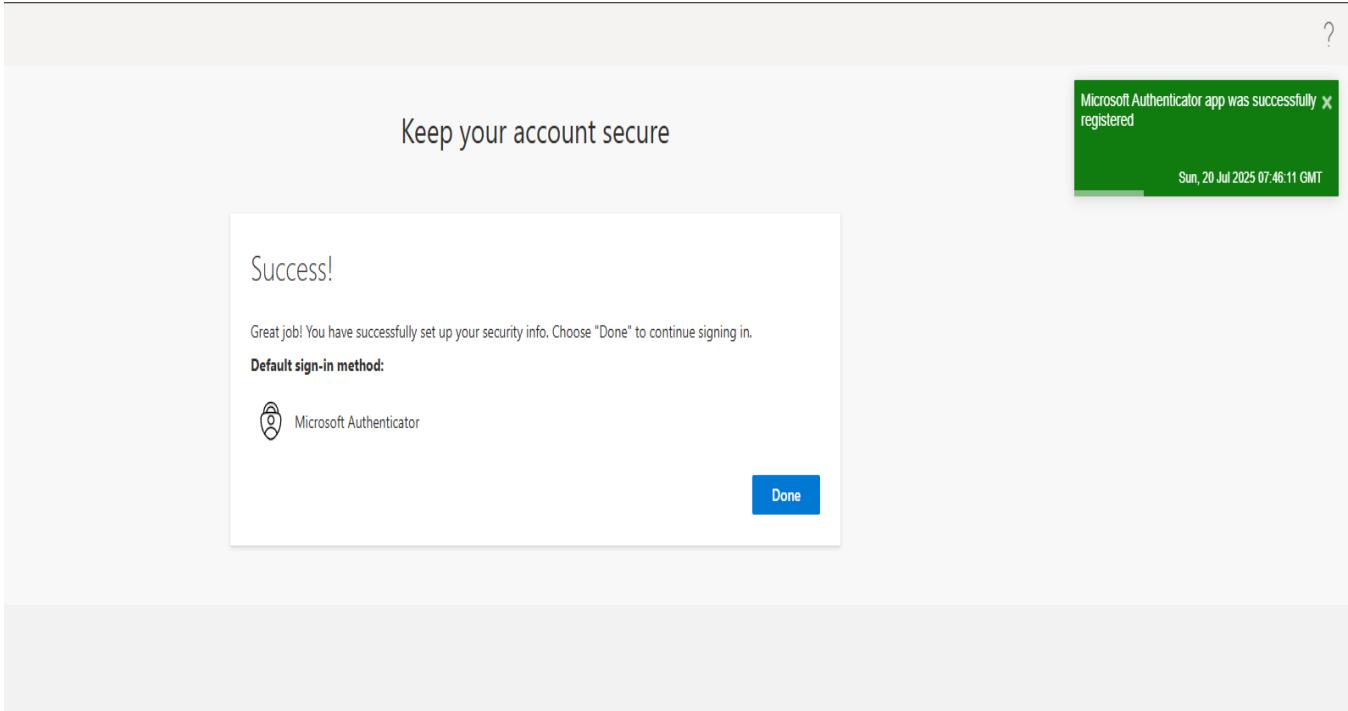
Keep your account secure

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: TestMFGGroup

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 TestMFGGroup 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 some resources:

- 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](#).

Conditional Access | Overview

Microsoft Entra ID

The screenshot shows the Microsoft Entra ID Conditional Access Overview page. At the top, there are navigation links for 'Create new policy' and 'Create new policy from templates', and a 'Got feedback?' button. A callout box at the top right encourages users to 'Create your own policies and target specific conditions like cloud apps, sign-in risk, and device platforms with Microsoft Entra ID Premium.' On the left, a sidebar lists navigation items: 'Overview' (which is selected and highlighted in grey), 'Policies', 'Insights and reporting', 'Diagnose and solve problems', 'Manage', 'Monitoring', and 'Troubleshooting + Support'. The main content area is titled 'What is Conditional Access?' and explains that it gives users the ability to enforce access requirements when specific conditions occur. It includes two examples: 'When any user is outside the company network' (requiring multifactor authentication) and 'When users in the 'Managers' group sign-in' (requiring an Intune compliant or domain-joined device). Below this, a 'Get Started' section provides three steps: 'Create your first policy by clicking "+ Create new policy"', 'Specify policy Conditions and Controls', and 'When you are done, don't forget to Enable policy and Create'. A link 'Interested in common scenarios?' is also present.

◆ 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

Home > Default Directory | Overview > Users >



Test User 1

User

Search X <> Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview Monitoring Properties

Basic info

T1 Test User 1
testuser1@tanishkadeepakkadamgmail.onmicrosoft.com
Member

User principal name	testuser1@tanishkadeepakkadamgmail.onmicrosoft.com	Group memberships	1
Object ID	ad8a742c-3ead-424e-acbe-ee0cd00894c8	Applications	0
Created date time	20 Jul 2025, 12:36	Assigned roles	0
User type	Member	Assigned licenses	0
Identities	tanishkadeepakkadamgmail.onmicrosoft.com		

My Feed

Account status
Enabled
[Edit](#)

B2B invitation
[Convert to external user](#)

Quick actions

[Edit properties](#)

Test User 1 | Authentication methods

User

Search | + Add authentication method | ⚡ Reset password | 🔑 Require re-register multifactor authentication | ⚙️ Revoke multifactor authentication sessions | 📊 View authentication methods policy

Overview | Audit logs | Sign-in logs | Diagnose and solve problems | Custom security attributes | Assigned roles | Administrative units | Groups | Applications | Licenses | Devices | Azure role assignments | **Authentication methods** | New support request

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. [Learn more](#)

Default sign-in method (Preview) ⚡ Microsoft Authenticator notification ⚡

Usable authentication methods

Authentication method	Detail
Microsoft Authenticator	SM-M215F

Non-usuable authentication methods

Authentication method	Detail
No non-usuable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	PhoneAppNotification

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 | Getting started** ...

Got feedback?

 **Getting started**

-  Diagnose and solve problems
- ▽ Protect
 -  Conditional Access
 -  Identity Protection
 -  Security Center
 -  Verified ID
- ▽ Manage
 -  Identity Secure Score
 -  Named locations
 -  Authentication methods
 -  Multifactor authentication
 -  Certificate authorities (classic)
 -  Public key infrastructure (Preview)
- ▽ Report
- ▽ Troubleshooting + Support

 **Documentation**

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

- 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](#).

Authentication methods | Policies

Default Directory - Microsoft Entra ID Security

Search



Add external method (Preview)



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

Microsoft Authenticator settings

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:
 - o Self-Service Password Reset: Select Selected or All
 - o Choose your group TestMFAGroup
 - o Save

◆ Step 3.2: Set SSPR Authentication Methods

- In Authentication methods tab:
 - o Number of methods required: 2
 - o 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

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

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 you define.

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



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.onmicrosoft.com

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



YLXW

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

[Next](#)

[Cancel](#)



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

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	<input checked="" type="checkbox"/>

security

[+ 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:
 - o Lockout threshold: e.g., 10 attempts
 - o Lockout duration: e.g., 60 seconds
 - o Custom banned passwords (optional)

Home > Default Directory | Security > Security | Authentication methods > Authentication methods

The screenshot shows the 'Authentication methods | Password protection' page in the Azure portal. The left sidebar has 'Manage' expanded, with 'Policies' and 'Password protection' selected. A message box indicates that some features require a Microsoft Entra ID Premium license. The main area contains settings for 'Custom smart lockout' (Lockout threshold: 10, Lockout duration in seconds: 60), 'Custom banned passwords' (Enforce custom list: Yes), and 'Custom banned password list' (a large empty text area). At the bottom, there are sections for 'Password protection for Windows Server Active Directory' (Enable password protection on Windows Server Active Directory: Yes) and 'Mode' (Enforced).

Some features on this page require a Microsoft Entra ID Premium license. Click here to upgrade.

Custom smart lockout

Lockout threshold ① 10

Lockout duration in seconds ① 60

Custom banned passwords

Enforce custom list ① Yes No

Custom banned password list ①

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ① Yes No

Mode ① Enforced Audit

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:

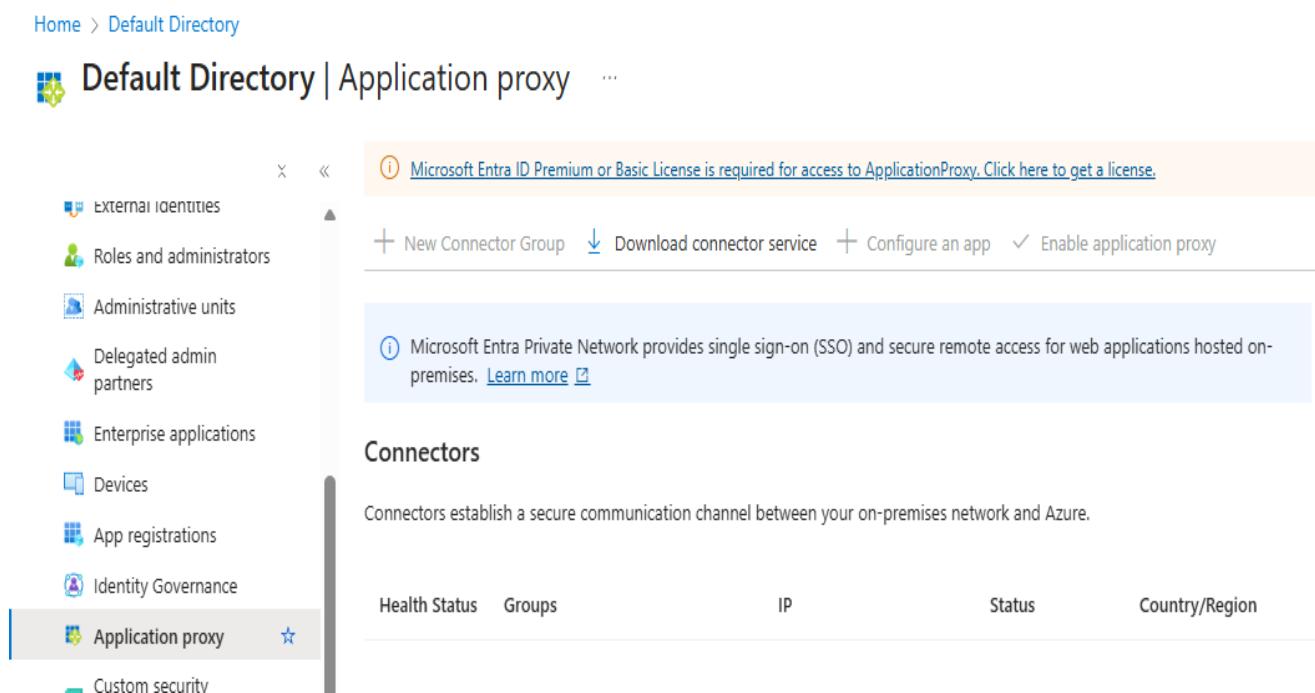
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension>

◆ 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

Home > Default Directory

The screenshot shows the Azure AD Application Proxy interface. The left sidebar lists several categories: External identities, Roles and administrators, Administrative units, Delegated admin partners, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy (which is selected and highlighted in blue), and Custom security. The main content area has a heading 'Default Directory | Application proxy'. It includes a note about requiring a Microsoft Entra ID Premium or Basic license. Below this, there's a section titled 'Connectors' with a sub-note about Microsoft Entra Private Network providing SSO and secure remote access. A table at the bottom lists connectors by Health Status, Groups, IP, Status, and Country/Region.

Health Status	Groups	IP	Status	Country/Region
Green	1 group	127.0.0.1	Active	United States

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

Home > Default Directory

Default Directory | Sign-in logs

Want to switch back to the legacy signin logs experience? Click here to leave the preview.

Add filter Show dates as: UTC Date range: Last 24 hours Reset filters

Date	Request ID	User principal name	Application	Status	IP address	Resource
20/07/2025, 13:16:23	1ee38ddf-9276-478c-ae70-df86e...	testuser1@tanishkadee...	OfficeHome	Interrupted	103.160.167.152	OfficeHome

Home > Default Directory

Default Directory | Sign-in logs

Want to switch back to the legacy signin logs experience? Click here to leave the preview.

Add filter Show dates as: UTC Date range: Last 24 hours Reset filters

Date	Request ID	User principal name	Application	Status	IP address	Resource	Resource ID	Conditional ac...	User
20/07/2025, 13:16:23	1ee38ddf-9276-478c-ae70-df86e...	testuser1@tanishkadee...	OfficeHome	Interrupted	103.160.167.152	OfficeHome	4765445b-32c6-49b0-8...	Not applied	Test User
20/07/2025, 12:09:45	e3f54598-fb9d-401b-b214-574c...	tanishkadeepakkadam@...	Azure Portal	Success	103.160.167.152	Azure Resource Manager	797f4846-ba00-4fd7-ba...	Not applied	TANISHKA

Home > Default Directory

Default Directory | Sign-in logs

The screenshot shows the 'Sign-in logs' section of the Azure AD portal. It displays two sign-in events:

Date	Request ID	User principal name	Application	Status	IP address	Resource	Resource ID	Conditional ac...	User
20/07/2025, 13:16:23	1ee38ddf-9276-478c-ae70-df86e...	testuser1@tanishkadee...	OfficeHome	Interrupted	103.160.167.152	OfficeHome	4765445b-32c6-49b0-8...	Not applied	Test User 1
20/07/2025, 12:09:45	e3f54598-fb9d-401b-b214-574c...	tanishkadeepakkadam@...	Azure Portal	Success	103.160.167.152	Azure Resource Manager	797f4846-ba00-4fd7-ba...	Not applied	TANISHKA

Home > Default Directory

Default Directory | Sign-in logs

The screenshot shows the 'Sign-in logs' section of the Azure AD portal. It displays three sign-in events, including one from 'User settings':

Date	Request ID	User principal name	Application	Status	IP address	Resource	Resource ID	Conditional ac...	User	Location
~478c-ae70-df86e...	testuser1@tanishkadee...	OfficeHome	Interrupted	103.160.167.152	OfficeHome	4765445b-32c6-49b0-8...	Not applied	Test User 1	Kasarwadi, Maharashtra, India	
~401b-b214-574c...	tanishkadeepakkadam@...	Azure Portal	Success	103.160.167.152	Azure Resource Manager	797f4846-ba00-4fd7-ba...	Not applied	TANISHKA KADAM	Kasarwadi, Maharashtra, India	

◆ Step 6.2: SSPR Reporting

1. Azure AD > Password reset > Usage & Insights

2. View:

- o Who reset passwords
- o Success/Failure
- o 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
-