

# **Microsoft Entra ID: Conditional Access, MFA, and SSO Configuration**

This document outlines the step-by-step configuration and verification of core identity protection features in Microsoft Entra ID, including Conditional Access policies, Multi-Factor Authentication (MFA), and Single Sign-On (SSO) integration.

## **Objective**

To secure organizational identities by configuring user-based MFA, enforcing Conditional Access policies, and enabling SSO for enterprise applications.

## **Tools Used**

- Microsoft Entra Admin Center
- Azure AD Conditional Access
- Microsoft Authenticator App

## **Outcome**

Successfully enabled and tested MFA for individual users, created a Conditional Access policy to enforce MFA, and configured SSO access to connected enterprise applications.

Microsoft Entra admin center

Search resources, services, and docs (G+)

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

All users

Deleted users

User settings

Groups

Devices

Applications

Protection

Learn & support

Home > Multifactor authentication | Getting started >

Per-user multifactor authentication ...

Bulk update | Got feedback?

Skip multifactor authentication for requests from federated users on my intranet

☐

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

Enter IP address

Verification options [Learn more](#)

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

Remember multifactor authentication on trusted device [Learn more](#)

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

☒

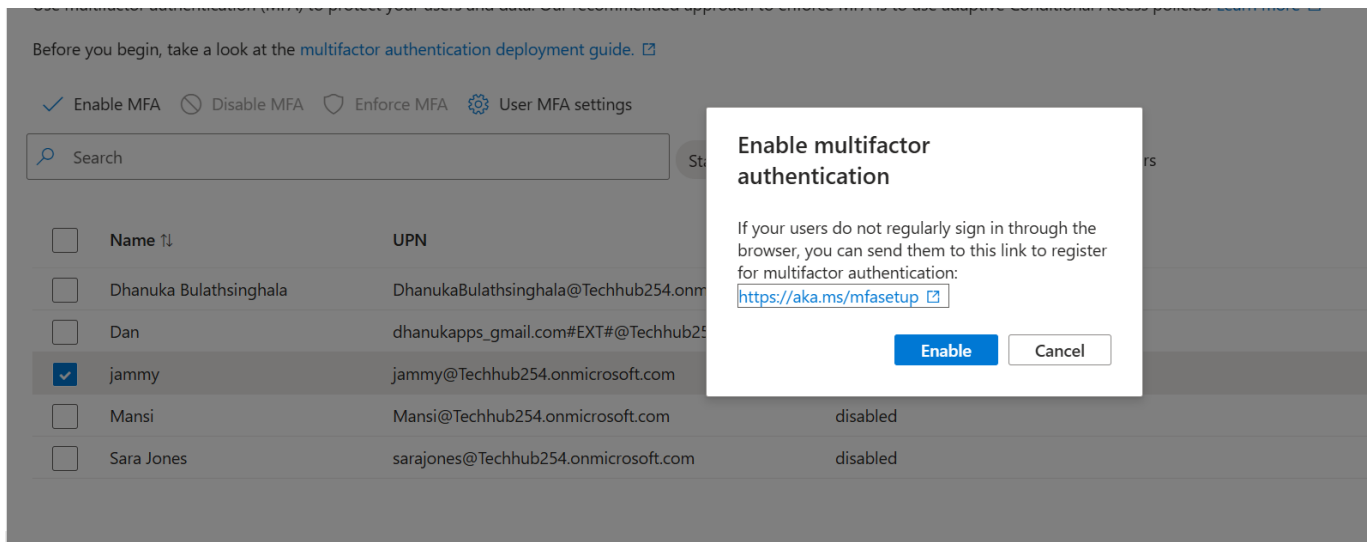
Number of days users can trust devices for

31

For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, MFA on a trusted device,' be sure to extend the duration to 90 or more days. [Learn more about reauthentication prompts](#) .

Save Discard

Description: Enabled per-user MFA in Microsoft Entra ID with options to skip trusted IPs and allow trusted device sign-in persistence for 31 days.



Description: Enabled Multi-Factor Authentication (MFA) for user 'jammy' using the classic per-user MFA portal with registration link.



## Pick an account



jammy  
jammy@Techhub254.onmicrosoft.com  
Signed in



Dhanuka Bulathsinghala

Description: Signed in to Entra ID as the user 'jammy' to test MFA functionality.

jammy | Authentication methods

User

Search

«

+ Add authentication method

Reset password

Require re-register multifactor authentication

Revoke multifactor authentication sessions

...

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	iPhone 16

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	PhoneAppNotification

Description: Verified MFA authentication method using Microsoft Authenticator app linked to user's iPhone 16.

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

DhanukaBula  
TECHHUB (TECHHUB)

Home > Multifactor authentication | Getting started

### New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

MFA policy ✓

Assignments

Users ⓘ

Specific users included

✖ "Select users and groups" must be configured

Target resources ⓘ

No target resources selected

Network **NEW** ⓘ

Not configured

Enable policy

Report-only On Off

⚠ It looks like you're about to manage your organization's Conditional Access policies. Make sure you have the necessary permissions.

Create

### Select users and groups

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

Search

6 results found

All Users Groups

	Name	Type	Details
<input type="checkbox"/>	Dan	User	dhanukapps@gmail.com
<input type="checkbox"/>	Managers	Group	
<input type="checkbox"/>	Dhanuka Bulathsinghala	User	DhanukaBulathsinghala@Techhub254.onmicrosoft.com
<input checked="" type="checkbox"/>	jammy	User	jammy@Techhub254.onmicrosoft.com
<input type="checkbox"/>	Mansi	User	Mansi@Techhub254.onmicrosoft.com
<input type="checkbox"/>	Sara Jones	User	sarajones@Techhub254.onmicrosoft.com

Selected (1)

Reset

jammy  
jammy@Techhub254.onmicrosoft.com

Description: Creating a Conditional Access policy named 'MFA policy' and selecting user 'jammy' as the target.



# Grant



Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access



Require multifactor authentication



Consider testing the new "Require authentication strength". [Learn more](#)



Require authentication strength



"Require authentication strength" cannot be used



Description: Configuring Conditional Access grant controls to require MFA as an access condition.

Enterprise applications - Micros

entra.microsoft.com/#view/Microsoft\_AAD\_IAM/StartboardApplicationsMenuBlade/~/.AppAppsPre...

Microsoft Entra admin center

Search resources, services, and docs (G+)

Copilot

DhanukaBulathsinghala...  
TECHHUB (TECHHUB254.0NMIC...

Home > Enterprise applications

## Enterprise applications | All applications

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Private Network connectors
- User settings
- App launchers
- Custom authentication extensions

Security

- Conditional Access
- Consent and permissions

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs

+ New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

2 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expir...	Active Certificat...	Identifier URI (E...
MG Microsoft Gra...	ba5be63e-7675-4e7...	14d82eec-204b-4c2f...	https://docs.microso...	6/11/2025	-	-	14d82eec-204b-4c2f...
Oracle Access...	dd357167-f94b-423...	ce3b316b-c0b2-468...	https://*.YOUR_OAM...	6/12/2025	-	-	ce3b316b-c0b2-468...

Description: Navigating to Enterprise Applications in Entra ID to configure SSO for apps like Microsoft Graph and Oracle.

Microsoft Entra admin center

Home > Enterprise applications | All applications

### Add Assignment

Users and groups

None Selected

Select a role

Default Organization

### Users and groups

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

Search

7 results found

All Users Groups

	Name	Type	Details
<input type="checkbox"/>	Dan	User	dhanukapps@gmail.com
<input type="checkbox"/>	m65 group	Group	m65group@Techhub254.onmicrosoft.com
<input type="checkbox"/>	Dhanuka Bulathsinghala	User	DhanukaBulathsinghala@Techhub254.onmicrosoft.com
<input type="checkbox"/>	Managers	Group	
<input checked="" type="checkbox"/>	jammy	User	jammy@Techhub254.onmicrosoft.com
<input checked="" type="checkbox"/>	Mansi	User	Mansi@Techhub254.onmicrosoft.com

Selected (2)

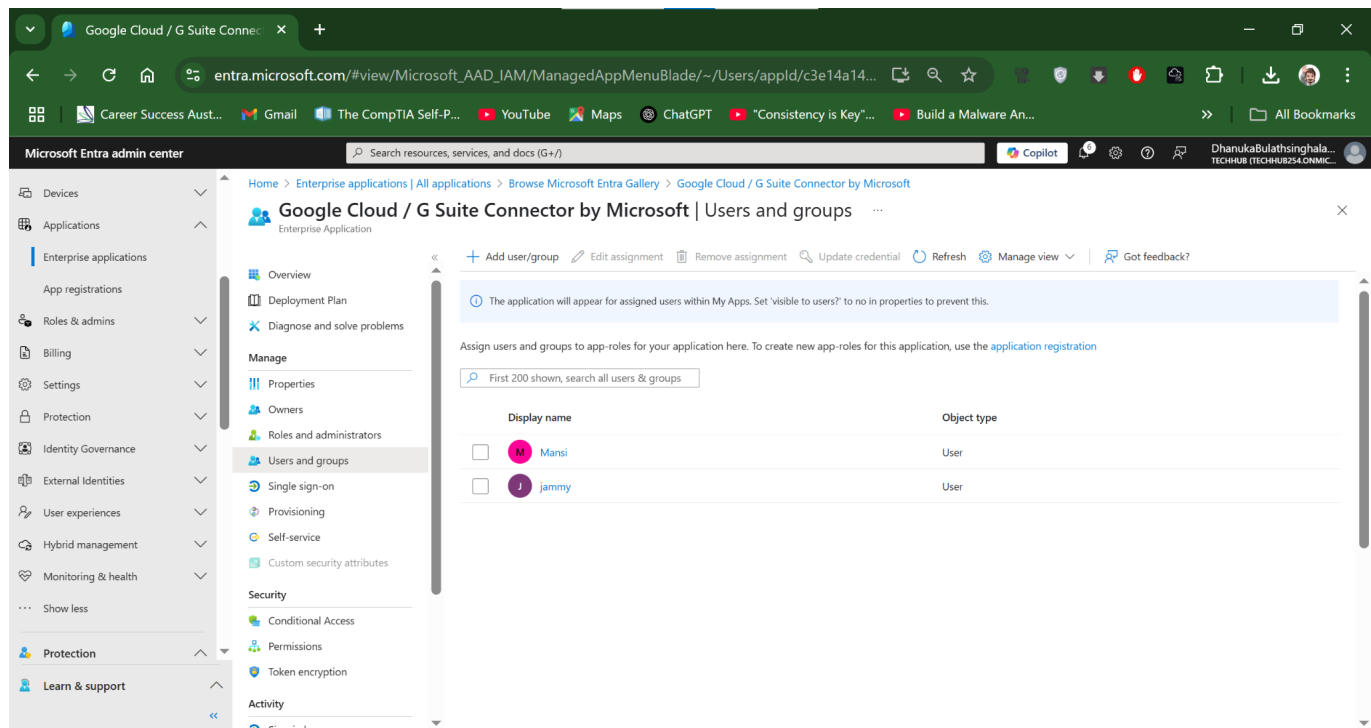
Reset

- jammy  
jammy@Techhub254.onmicrosoft.com
- Mansi  
Mansi@Techhub254.onmicrosoft.com

Assign

Select

Description: Assigning users 'jammy' and 'Mansi' to an enterprise app to enforce SSO-based access control.



Description: Viewing user assignments under the 'G Suite Connector by Microsoft' enterprise application for SSO implementation.