Configuration Manual

MSc Research Project
MSc Cyber Security

Shalini Jaganmohan
Student ID: 22201505

School of Computing
National College of Ireland

Supervisor: Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shalini Jaganmohan		
Student ID:	x22201505		
Programme:	MSc in Cyber Security	**Year:**	2023-2024
Module:	MSc Research Project		
Lecturer:	Michael Prior		
Submission Due Date:	12-08-2024		
Project Title:	Investigate access control models, and authentication mechanisms for a regulated industry based on Role-based JIT access control using PIM and Biometrics in Azure AD		
Word Count:	832	**Page Count:**	13

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Shalini Jaganmohan

Date: 11-08-2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Shalini Jaganmohan
Student ID: 22201505

1 Introduction

The main purpose of this document contains all the information and requirements about the technology used and tools that were used during this research project with the idea of creating Just in Time (JIT) access through Microsoft Azure Admin Centre in addition to that I have enabled Cognitive Services (FACE API) for login to the users.

2 Hardware Specification

Web Brower – Google Chrome
Hardware Specification Ram – 16 GB
Disk Space – Minimum 500 GB
OS – Windows 10 Pro and above

3 Tools Specification

Microsoft 365 Admin Centre – Licence; Microsoft 365 E3
Microsoft AZURE Portal - Licence: Microsoft Entra ID P2
Microsoft Entra Admin Centre – Licence: Microsoft Entra ID P2
Microsoft Intune Admin Centre – Licence: Microsoft Entra ID P2

4 Tools Info

Microsoft 365 Admin Centre:
It is used to create User IDs and Groups

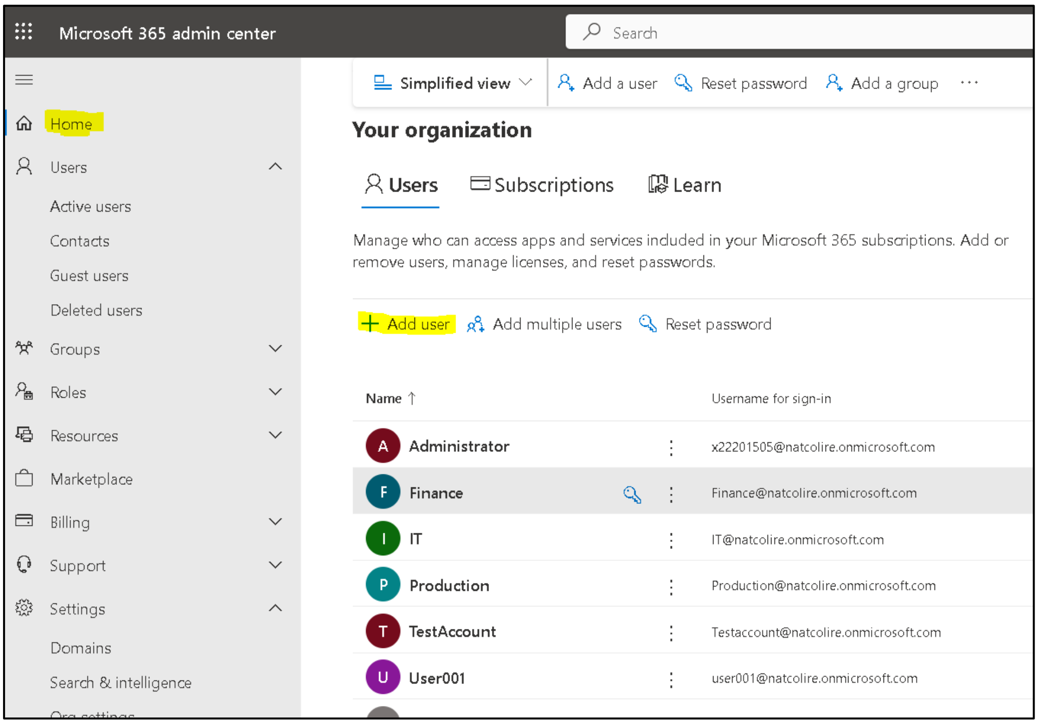
Microsoft AZURE Portal:
It is used to create Just in Time (JIT) Access for the Users

Microsoft Entra Admin Centre:
It is used to configure Policies and Conditional Access to enable the MFA to be a secondary authentication for the users.

Microsoft Intune Admin Centre:
It is used to manage and secure the device through application management and compliance monitoring.

5 Implementation

User ID creation and Setup

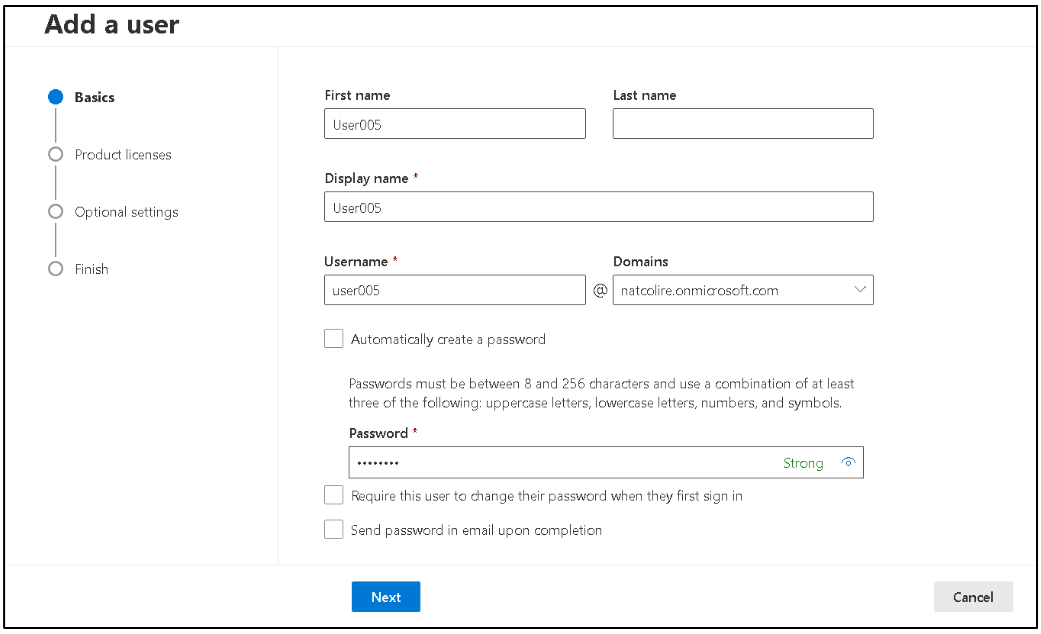


Your organization

Manage who can access apps and services included in your Microsoft 365 subscriptions. Add or remove users, manage licenses, and reset passwords.

Name ↑	Username for sign-in
Administrator	x22201505@natcolire.onmicrosoft.com
Finance	Finance@natcolire.onmicrosoft.com
IT	IT@natcolire.onmicrosoft.com
Production	Production@natcolire.onmicrosoft.com
TestAccount	Testaccount@natcolire.onmicrosoft.com
User001	user001@natcolire.onmicrosoft.com

1. Login to https://admin.microsoft.com (Microsoft 365 Admin Console)
2. Click Add user



Add a user

First name: User005

Last name:

Display name *: User005

Username *: user005 @ Domains: natcolire.onmicrosoft.com

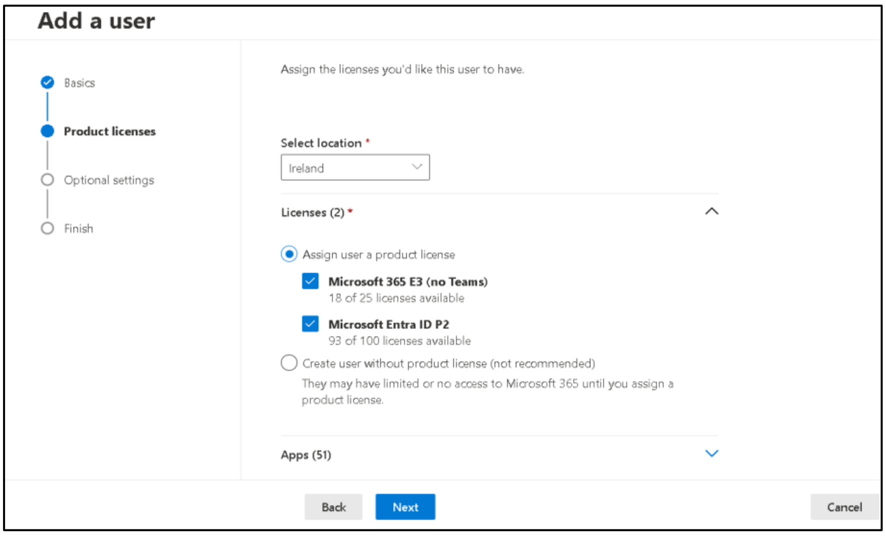
□ Automatically create a password

Passwords must be between 8 and 256 characters and use a combination of at least three of the following: uppercase letters, lowercase letters, numbers, and symbols.

Password *: •••••••• Strong

□ Require this user to change their password when they first sign in

□ Send password in email upon completion



Add a user

Assign the licenses you'd like this user to have.

Select location *
Ireland

Licenses (2) *

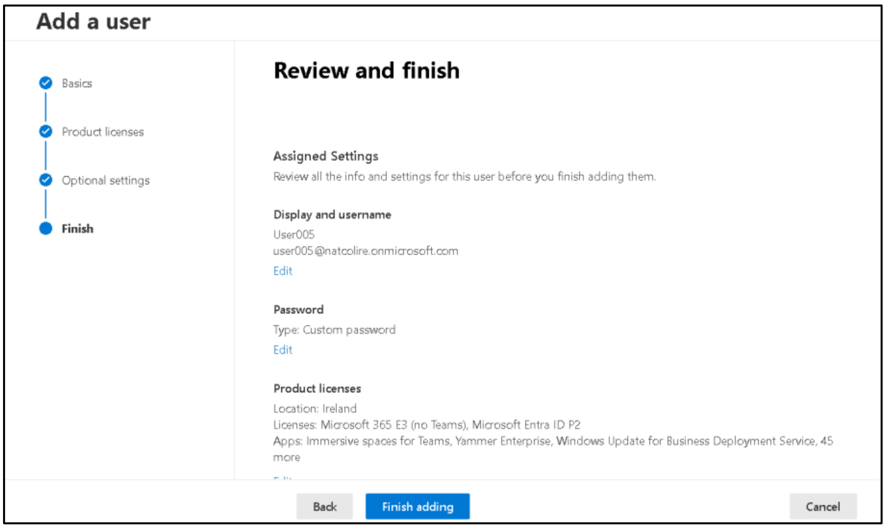
● Assign user a product license

☑ Microsoft 365 E3 (no Teams)
18 of 25 licenses available

☑ Microsoft Entra ID P2
93 of 100 licenses available

○ Create user without product license (not recommended)
They may have limited or no access to Microsoft 365 until you assign a product license.

Apps (51)



Add a user

Review and finish

Assigned Settings
Review all the info and settings for this user before you finish adding them.

Display and username
User005
user005@natcolire.onmicrosoft.com
Edit

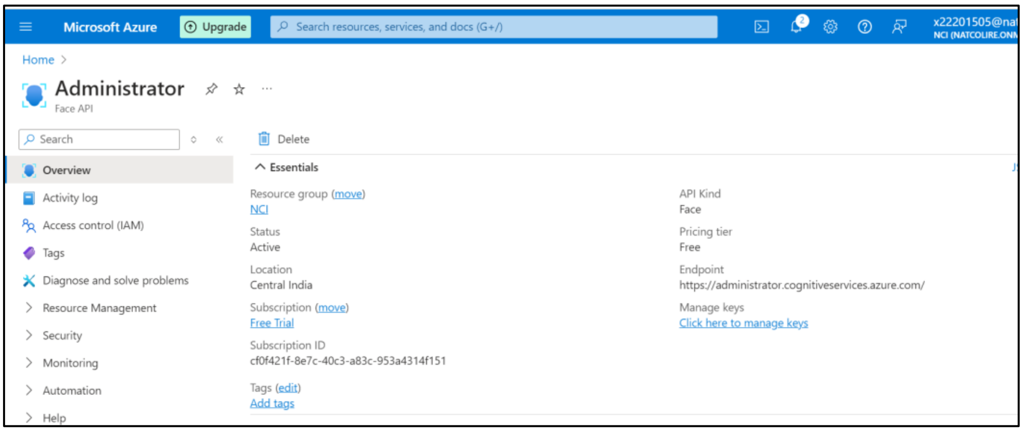
Password
Type: Custom password
Edit

Product licenses
Location: Ireland
Licenses: Microsoft 365 E3 (no Teams), Microsoft Entra ID P2
Apps: Immersive spaces for Teams, Yammer Enterprise, Windows Update for Business Deployment Service, 45 more

3. Fill the user details with the appropriate license and create the ID.

Biometrics Concept

1. Purchased the FACE API software in Azure Marketplace to enable biometrics and synced it with our users to make secondary authentication.



Administrator
Face API

Resource group (move)
NCI

Status
Active

Location
Central India

Subscription (move)
Free Trial

Subscription ID
cf0f421f-8e7c-40c3-a83c-953a4314f151

Tags (edit)
Add tags

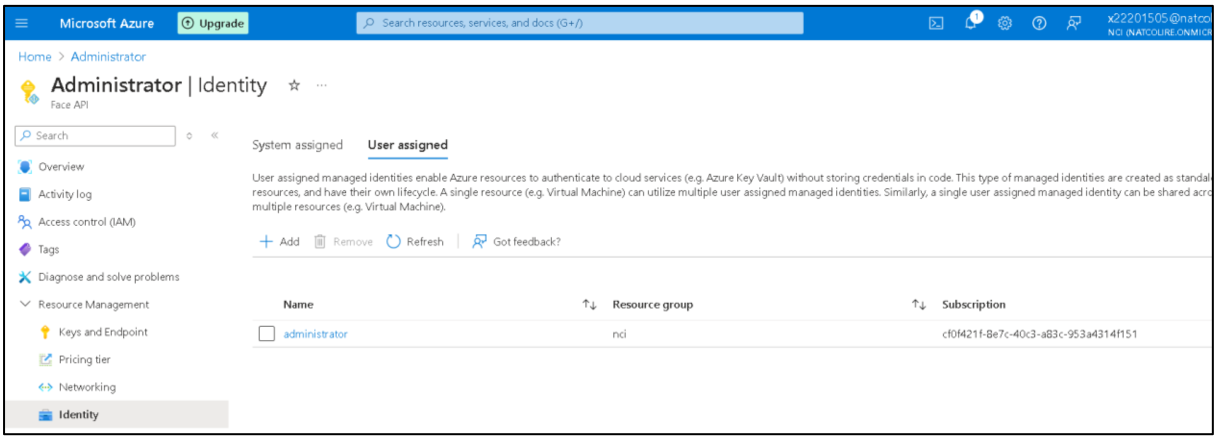
API Kind
Face

Pricing tier
Free

Endpoint
https://administrator.cognitiveservices.azure.com/

Manage keys
Click here to manage keys

2. The user has been added to the Microsoft Azure Face API for the authentication to log in to the sector.



Administrator | Identity

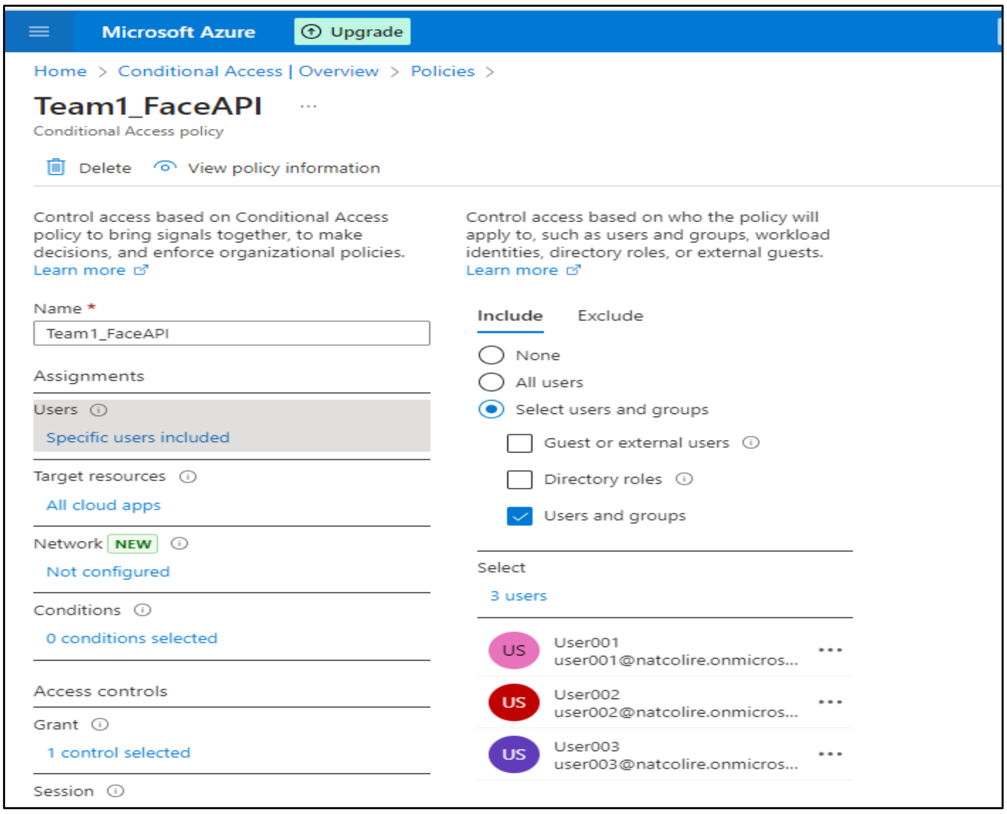
Face API

User assigned managed identities enable Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. This type of managed identities are created as standal resources, and have their own lifecycle. A single resource (e.g. Virtual Machine) can utilize multiple user assigned managed identities. Similarly, a single user assigned managed identity can be shared acro multiple resources (e.g. Virtual Machine).

	Name	Resource group	Subscription
□	administrator	nci	cf0f421f-8e7c-40c3-a83c-953a4314f151

Create Conditional Access

3. By Creating a new policy for Conditional Access which needs Azure AD to enable biometrics to the selected users.



Team1_FaceAPI

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

Name *

Team1_FaceAPI

Assignments

Users: Specific users included

Target resources: All cloud apps

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Grant: 1 control selected

Session

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

○ None

○ All users

● Select users and groups

□ Guest or external users

□ Directory roles

☑ Users and groups

Select

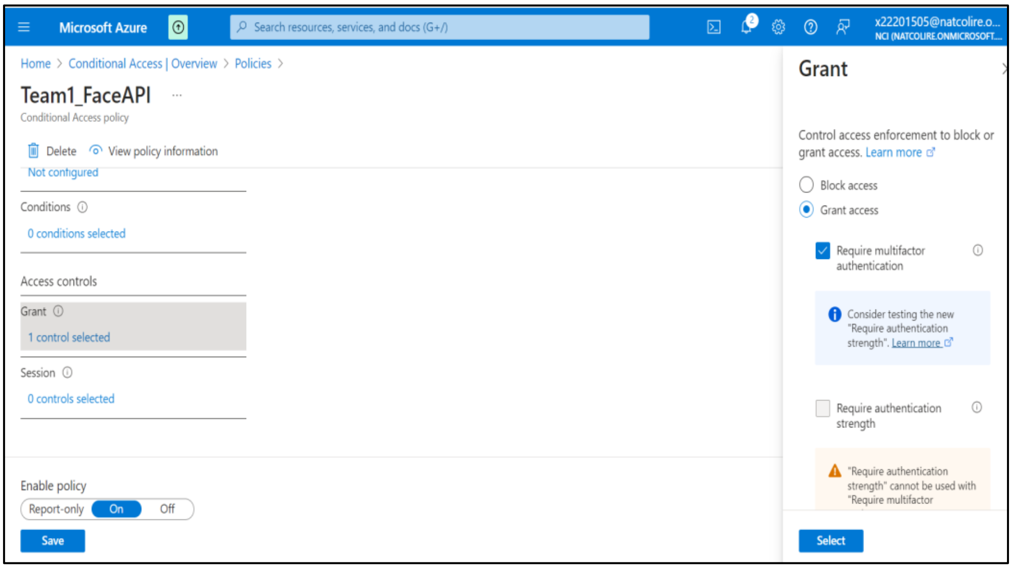
3 users

US User001 user001@natcolire.onmicros...

US User002 user002@natcolire.onmicros...

US User003 user003@natcolire.onmicros...

4. The selected users will be enabled under the FACE API authentication by granting control access.



Microsoft Azure
Search resources, services, and docs (G+/)
x22201505@natcolire.o...
NCI (NATCOLIRE.ONMICROSOFT....
Home > Conditional Access | Overview > Policies >
Delete
View policy information
Save
Select

Team1_FaceAPI ...

Conditional Access policy

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only [✓ On] Off

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

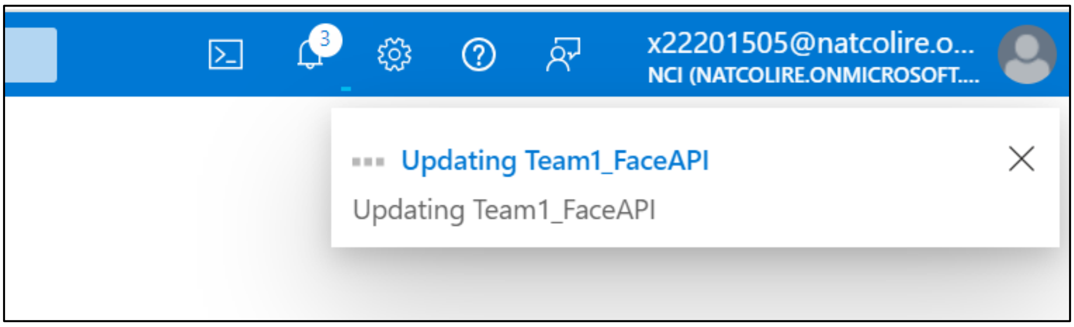
☑ Require multifactor authentication ⓘ

Consider testing the new "Require authentication strength". Learn more

□ Require authentication strength ⓘ

"Require authentication strength" cannot be used with "Require multifactor

5. Post selecting the appropriate access click save and then the policy with be updated and synced with users.



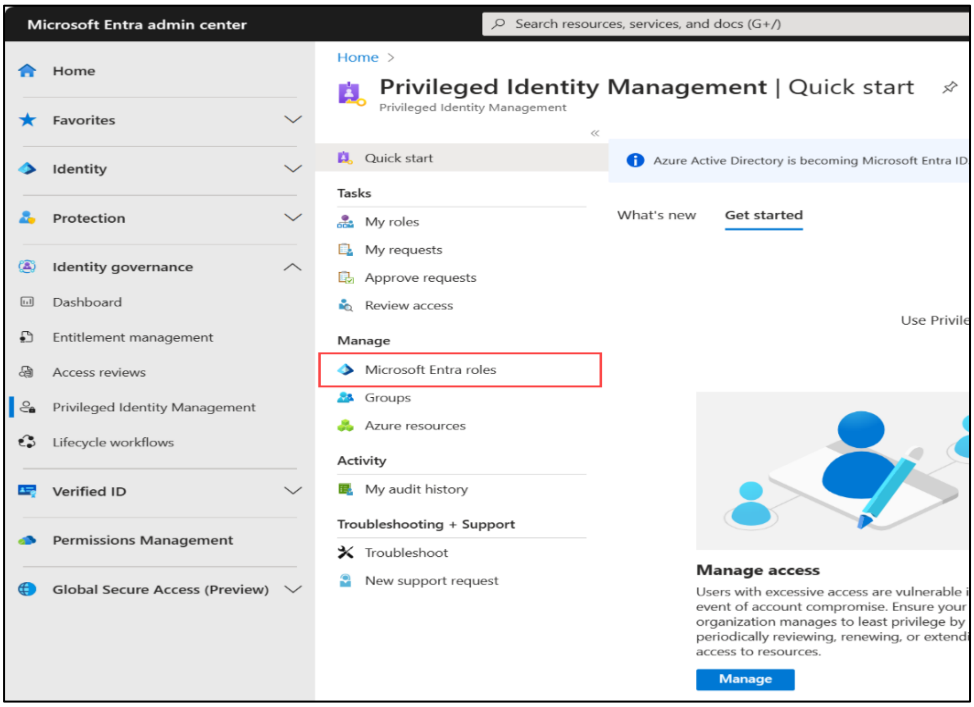
Updating Team1_FaceAPI

Updating Team1_FaceAPI

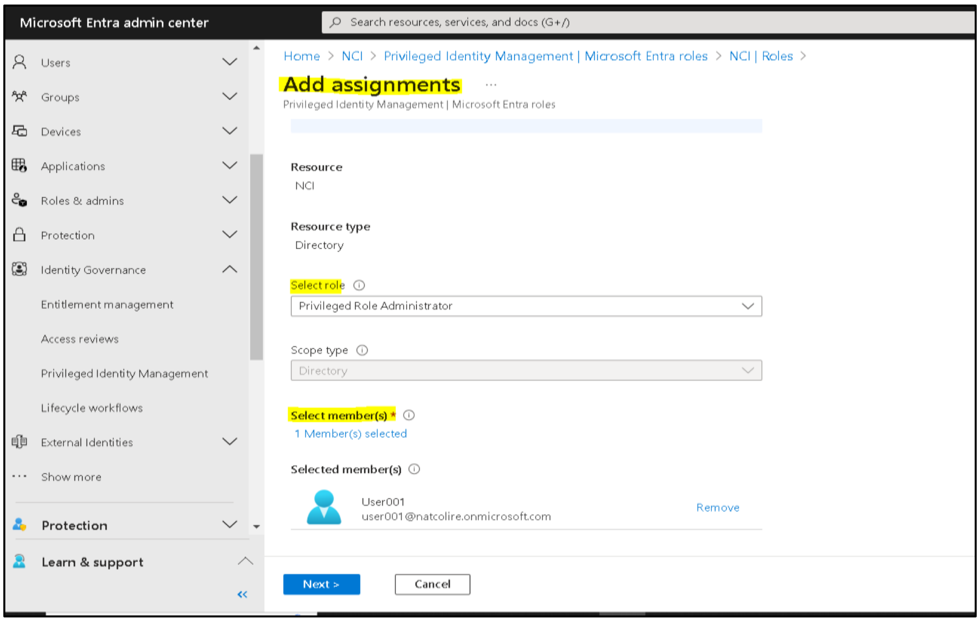
Create access reviews

Sign in to the [Microsoft Entra admin centra]() user who is assigned to one of the prerequisite roles(s).

1. Identity Governance > Privileged Identity Management
2. For (Microsoft Entra roles) - Move to Microsoft Entra. Then for Azure resources select Azure resources.
3. Under Manage select Microsoft Entra roles again. For Azure resources, select the Subscription to manage.
4. Then under Manage click Access Reviews and then New to create a new access review



Users with excessive access are vulnerable i event of account compromise. Ensure your organization manages to least privilege by periodically reviewing, renewing, or extendi access to resources.


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Users
Groups
Devices
Applications
Roles & admins
Protection
Identity Governance
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
External Identities
Show more
Protection
Learn & support
Home > NCI > Privileged Identity Management | Microsoft Entra roles > NCI | Roles >
Add assignments
Privileged Identity Management | Microsoft Entra roles
Remove
Next >
Cancel

Resource
NCI

Resource type
Directory

Select role
Privileged Role Administrator

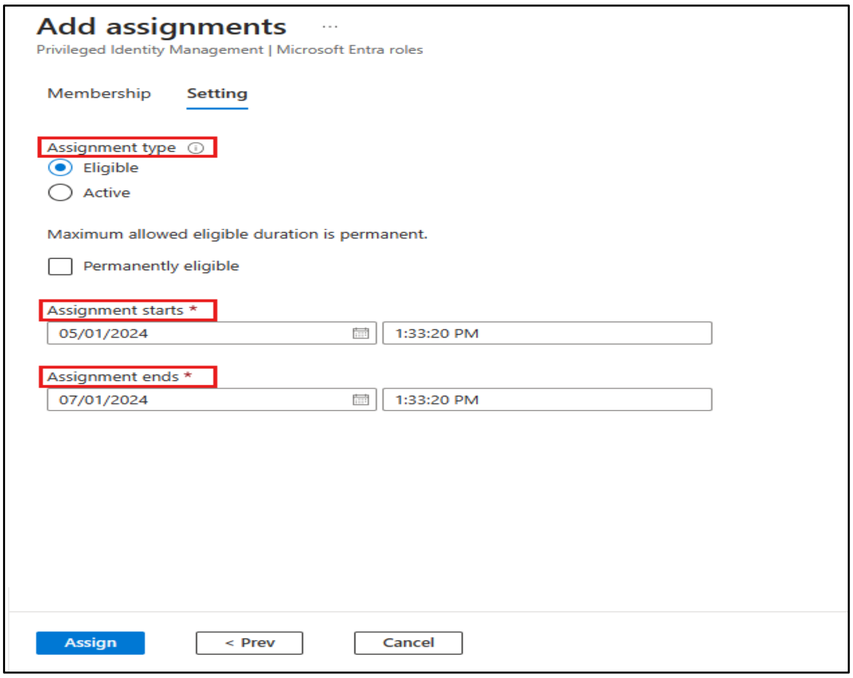
Scope type
Directory

Select member(s) *
1 Member(s) selected

Selected member(s)
User001
user001@natcolire.onmicrosoft.com

5. Click Add Assignments - Add Assignments page.
6. Click role - In a user page.
7. Select a role - assign - user who is to assign the role then click Next followed by Finish.
8. Select a role which you want to assign, then pick the user to which you want to mention the role and click on Next.
9. On the Membership settings box, select either Eligible or Active from the Assignment type list.
10. Eligible assignments are those where the role member must activate the role, such as performing an MFA check biometric authentication, providing a business clarification, or requesting approval from designated approvers.
11. In-progress assignments do not have the member having to act to use the role.

12. To assign a role for a fixed period, fill in the start and end date and time boxes. Once you have completed all the boxes, click Assign and create the new role assignment.
13. All assignments will never expire. This should be used with permanent staff who regularly require role permissions.
14. An announcement message upon assignment of role status is displayed.



Add assignments ...

Privileged Identity Management | Microsoft Entra roles

Membership **Setting**

Assignment type ⓘ

● Eligible

○ Active

Maximum allowed eligible duration is permanent.

□ Permanently eligible

Assignment starts *

05/01/2024 | 1:33:20 PM

Assignment ends *

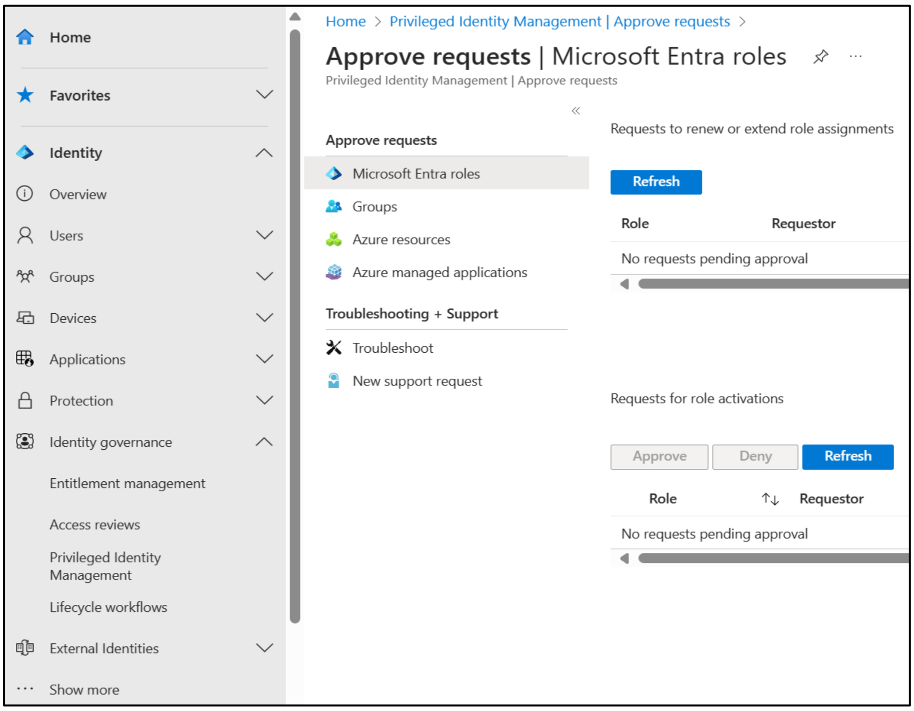
07/01/2024 | 1:33:20 PM

Assign | < Prev | Cancel

Pending Request Approval

1. Sign in to the Microsoft Entra admin center with Global Administrator.

2. Search Identity Governance > Privileged Identity Management > Approve requests.



Home > Privileged Identity Management | Approve requests >

Approve requests | Microsoft Entra roles ...

Privileged Identity Management | Approve requests

Home

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity governance

Entitlement management

Access reviews

Privileged Identity Management

Lifecycle workflows

External Identities

Show more

Approve requests

Microsoft Entra roles

Groups

Azure resources

Azure managed applications

Troubleshooting + Support

Troubleshoot

New support request

Requests to renew or extend role assignments

Refresh

Role	Requestor
No requests pending approval	

Requests for role activations

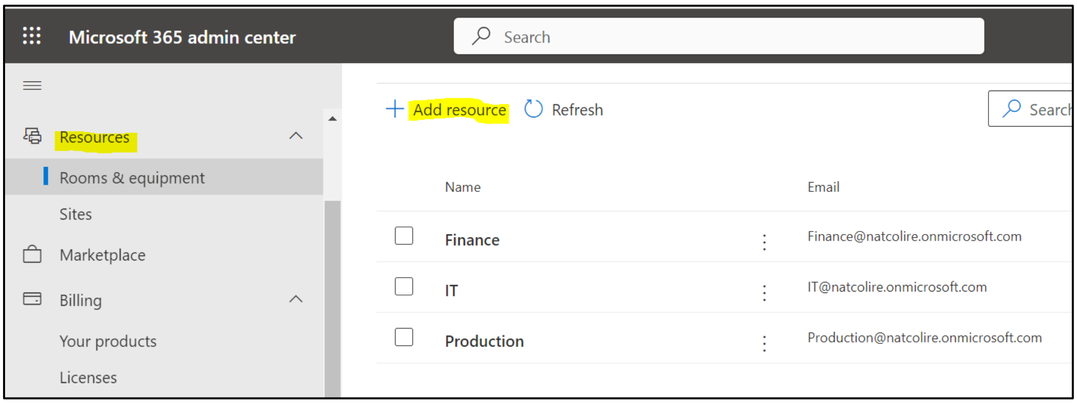
Approve | Deny | Refresh

Role ↑↓	Requestor
No requests pending approval	

We can find the list of requests that require your approval in the Requests for Role Activation section.

Creating Resources

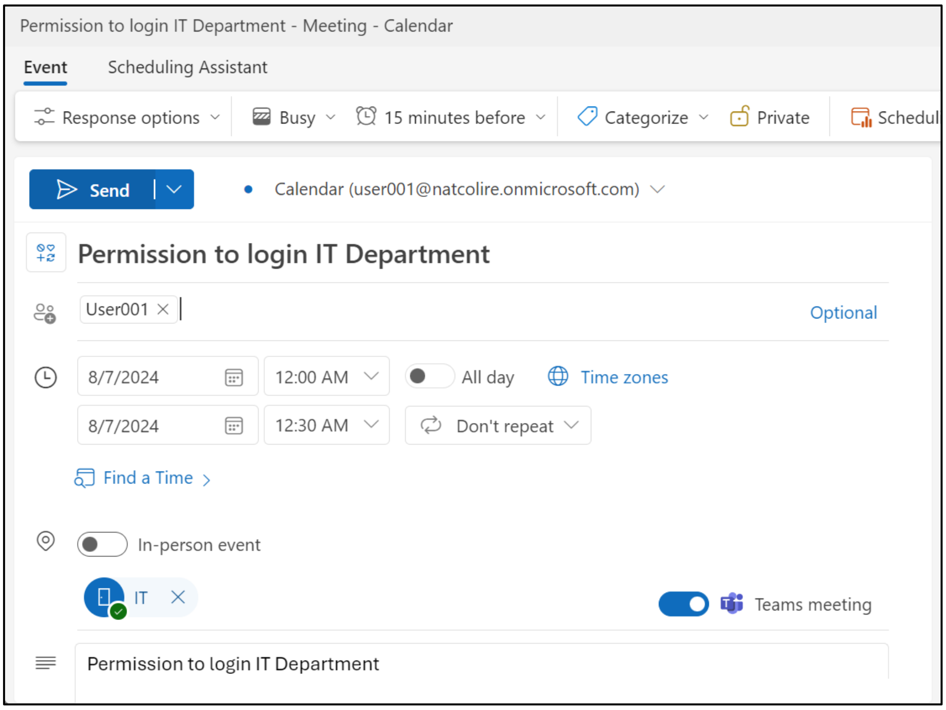
In the Add Resource tab, we have created multiple departments where the domain users can get the appropriate approval to get into the respective departments.



	Name	Email
□	Finance	Finance@natcolire.onmicrosoft.com
□	IT	IT@natcolire.onmicrosoft.com
□	Production	Production@natcolire.onmicrosoft.com

Requesting for Department access

1. We can request permission to access the mentioned department in the My Event tab from Outlook.



Calendar (user001@natcolire.onmicrosoft.com)

Permission to login IT Department

User001

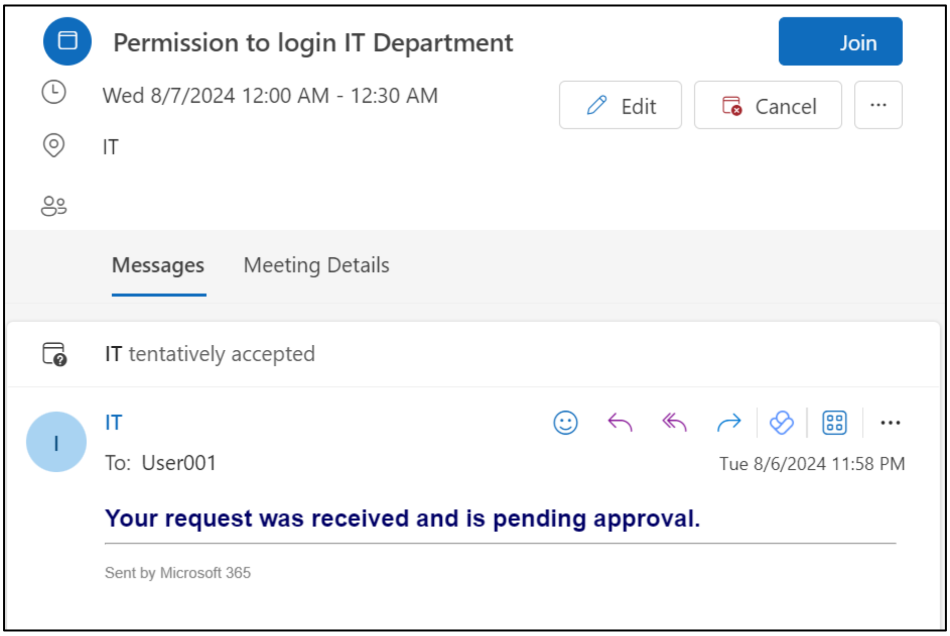
8/7/2024 12:00 AM

8/7/2024 12:30 AM

IT

Permission to login IT Department

2. Mail will be initiated to the IT Department Head to provide approval to grant permission or deny.


Permission to login IT Department

Wed 8/7/2024 12:00 AM - 12:30 AM

IT

IT tentatively accepted

IT

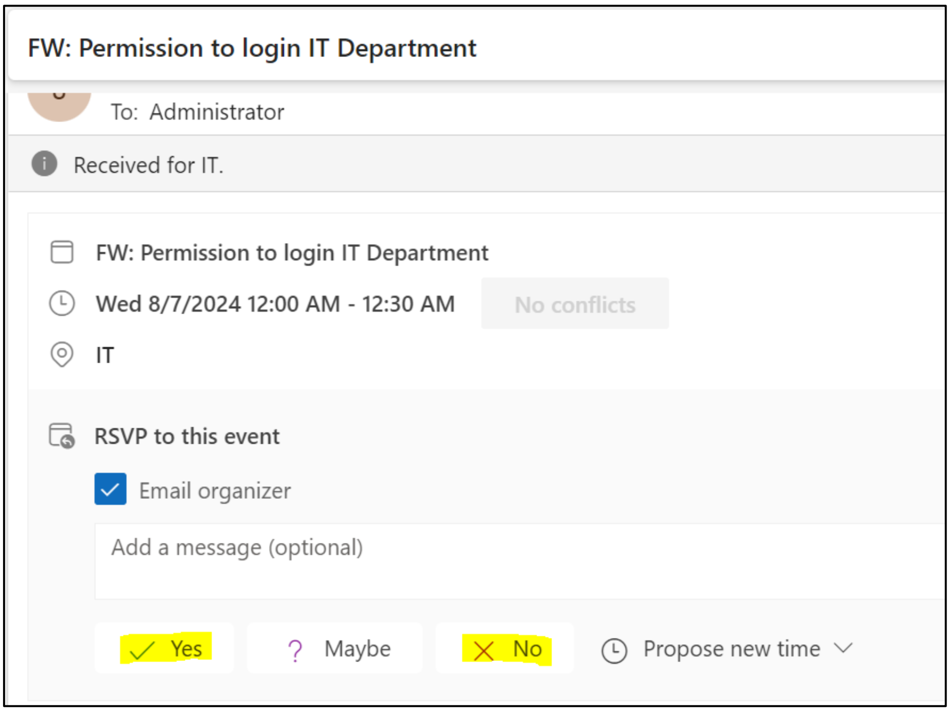
To: User001

Tue 8/6/2024 11:58 PM

Your request was received and is pending approval.

Sent by Microsoft 365

3. The IT Department Head can provide approval or denial from Outlook.


FW: Permission to login IT Department

To: Administrator

Received for IT.

FW: Permission to login IT Department

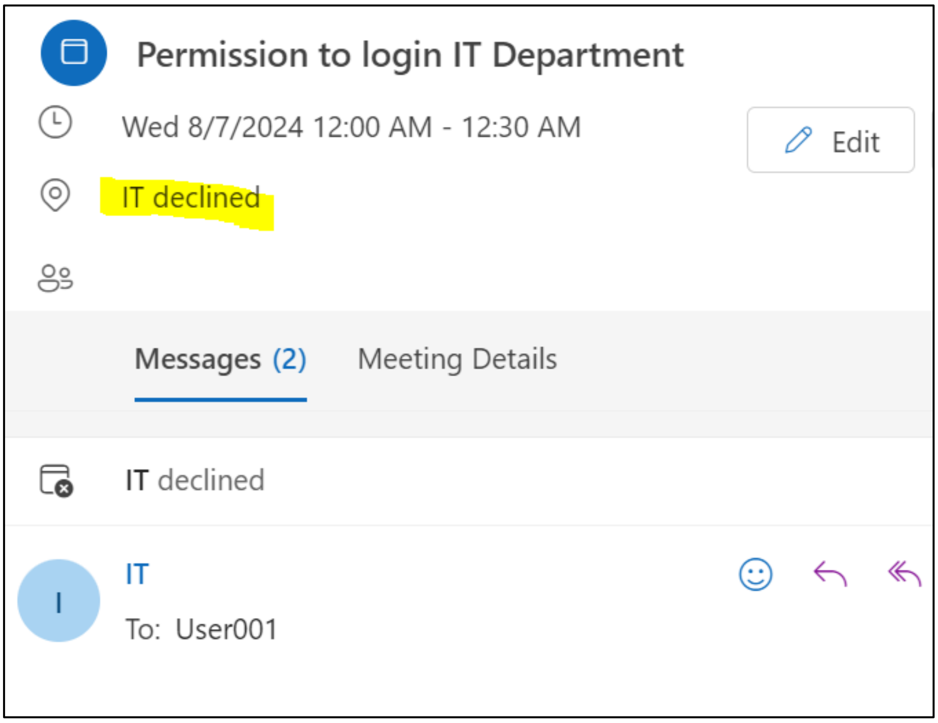
Wed 8/7/2024 12:00 AM - 12:30 AM

IT

☑ Email organizer

Add a message (optional)

4. If the IT Department Head decides to reject click No, the user will receive mail as the request is declined.



Permission to login IT Department

Wed 8/7/2024 12:00 AM - 12:30 AM

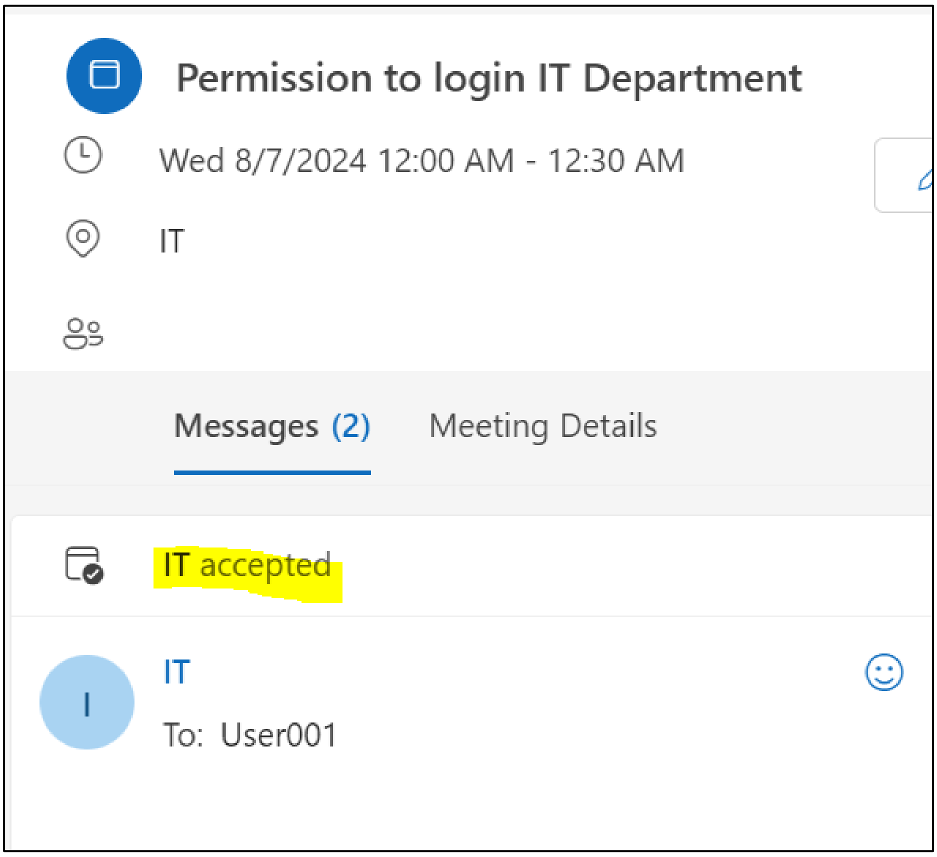
IT declined

IT declined

IT

To: User001

5. If the IT department Head decides to approve click Yes, and the user will receive mail as the request is accepted.



Permission to login IT Department

Wed 8/7/2024 12:00 AM - 12:30 AM

IT

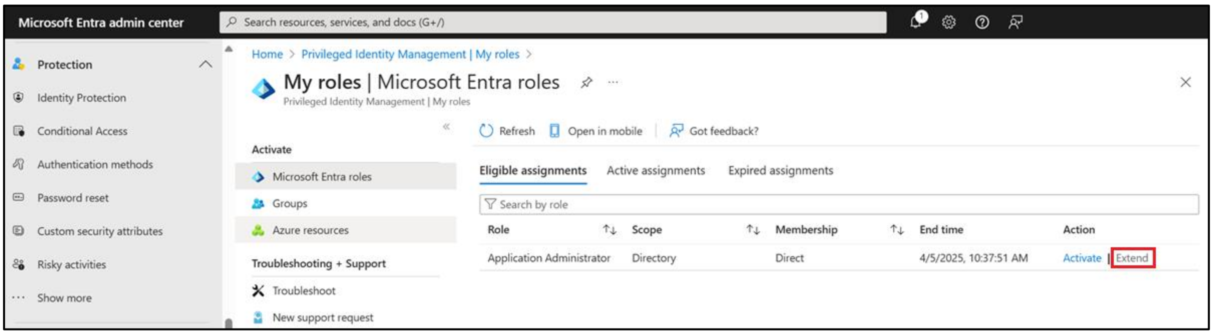
IT accepted

IT

To: User001

Extend Role Assignment

1. From the high-level My Roles page of the PIM portal, or under Microsoft Entra roles, users assigned to a particular role can **extend** their expiring role assignments and tasks straight from the 'Eligible' or 'Active' tab on the My Roles page itself.
2. An extension can be requested for an active (assigned) or eligible role which will expire in the next 14 days.



Role	Scope	Membership	End time	Action
Application Administrator	Directory	Direct	4/5/2025, 10:37:51 AM	Activate | Extend

References

1. https://learn.microsoft.com/en-gb/azure/ai-services/computer-vision/overview-identity#face-detection-and-analysis
2. https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices
3. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan