ROC TECH

IDENTITY ACCESS MANAGEMENT
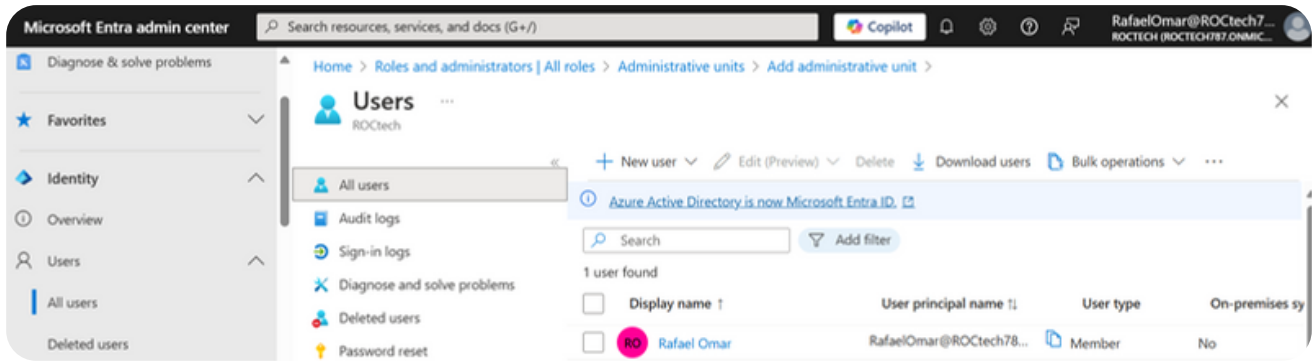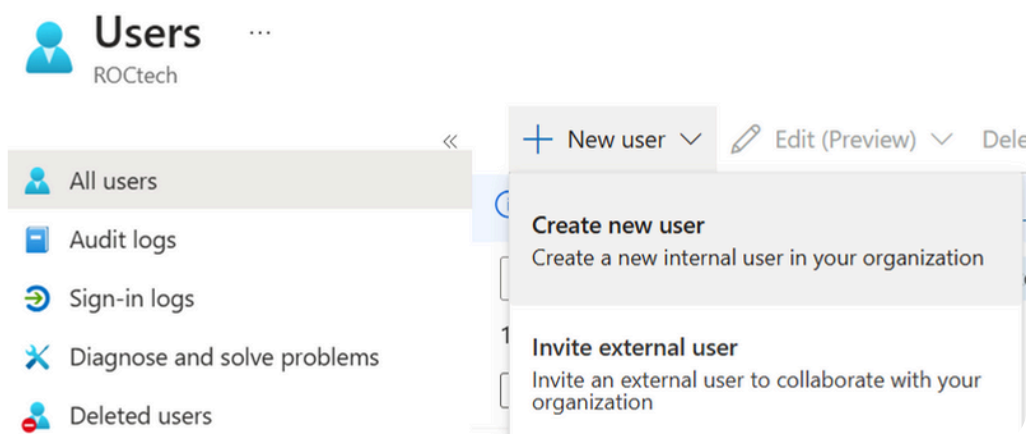
MICROSOFT ENTRA

PRESENTED BY

Rafael Omar Cruz

Configure & Manage a Microsoft Entra Tenant

1. Create a user on Microsoft Entra admin center.

2. We click on "New user" to create a new internal user for our new employee.

3. Complete all the basic information for the new employee.

Create new user ...
Create a new internal user in your organization

Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more ⧉

Identity

User principal name * `tomasjeff` @ `ROCtech787.onmicroso...` ⌄ 🗐

Domain not listed? Learn more ⧉

Mail nickname * `tomasjeff`

☑ Derive from user principal name

Display name * `Tomas Jeff`

Password * `••••••••••` 🗐

☑ Auto-generate password

Account enabled ⓘ ☑

Create new user ...
Create a new internal user in your organization

Basics **Properties** Assignments Review + create

Identity

First name `Tomas`

Last name `Jeff`

User type `Member` ⌄

Authorization info + Edit Certificate user IDs

Job Information

Job title `Help Desk Tech 1`

Company name `ROCTech`

Department `IT`

Employee ID `1234567890`

4. Provide with the new hire its appropiate roles. In this case we are assigning printer priviledges and roles to Tomas Jeff.

5. We confirm the new user created for Tomas Jeff with its corresponding roles.

6. On our MS365 admin center we can confirm that Tomas Jeff has not been assigned any licenses.
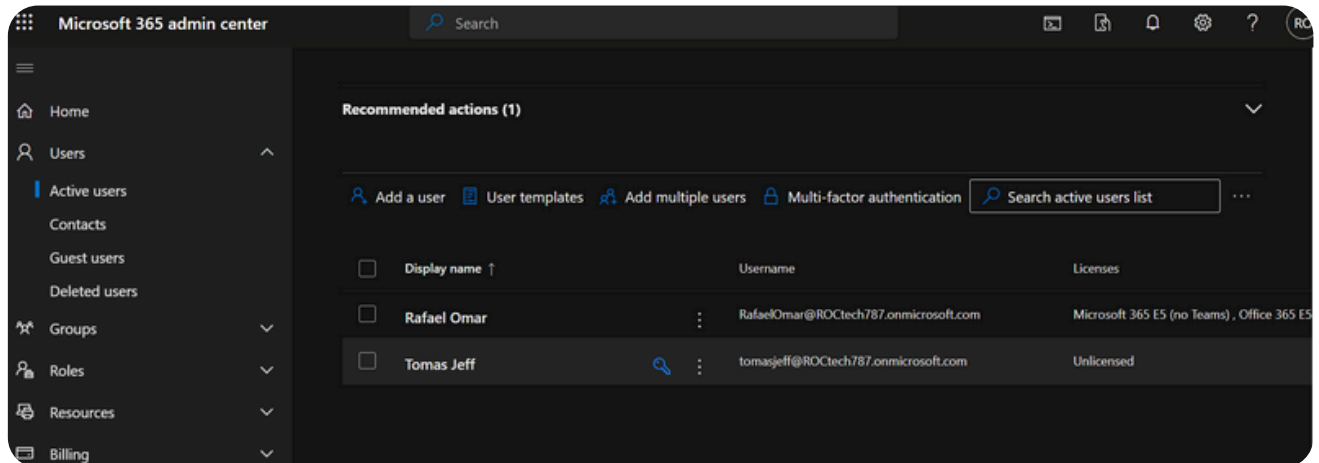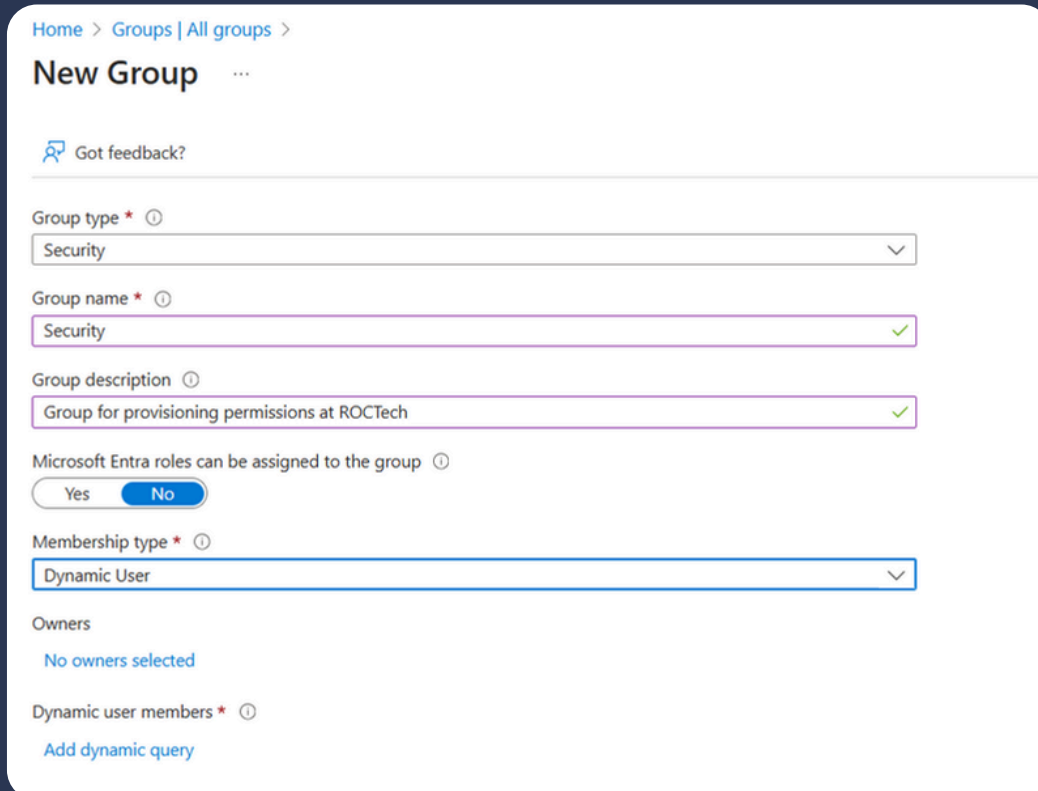
7. We then proceed to assign the new employee with his licenses, in this case Microsoft 365 and Office 365 E5.
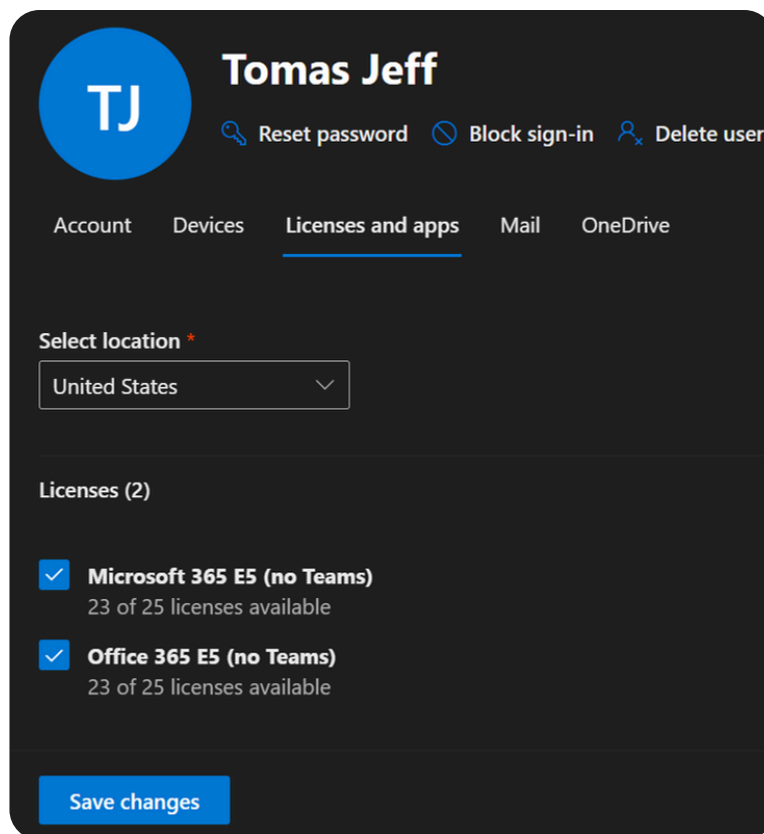
CREATING & MANAGING GROUPS IN ENTRA

1. Let's create a Security Group for provisioning permissions. We complete the basic information and select Dynamic User for Membership type. We want to automate this group's membership assignment.
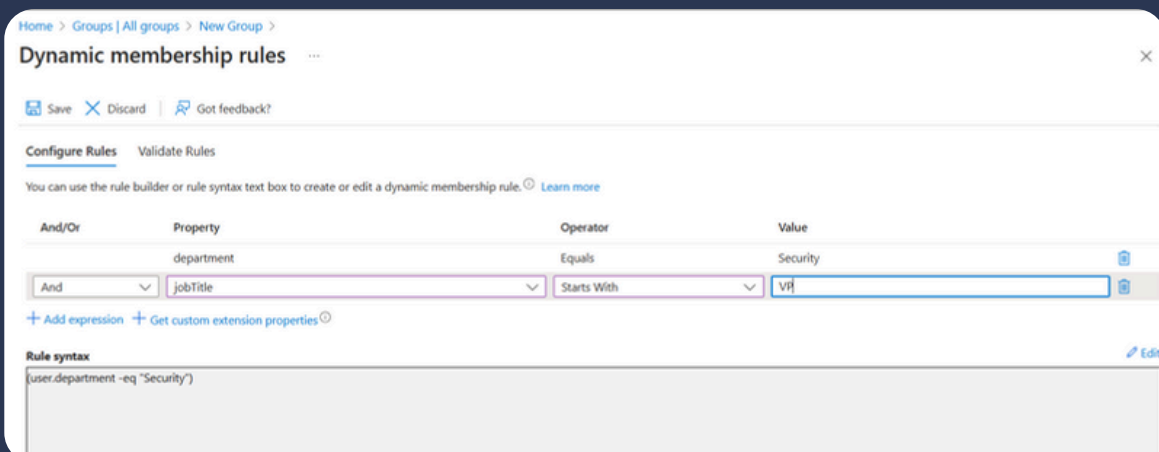
2. Let's configure the Dynamic membership rules to as follows: IF a new user is created AND is from the Security department AND the job title starts with VP then we want them to be automatically assign to this group.

CREATING & MANAGING GROUPS IN ENTRA

4. Let's add an owner to the group by clicking the "No owners selected" and choosing from the current users. In this case we select "Rafael Omar".
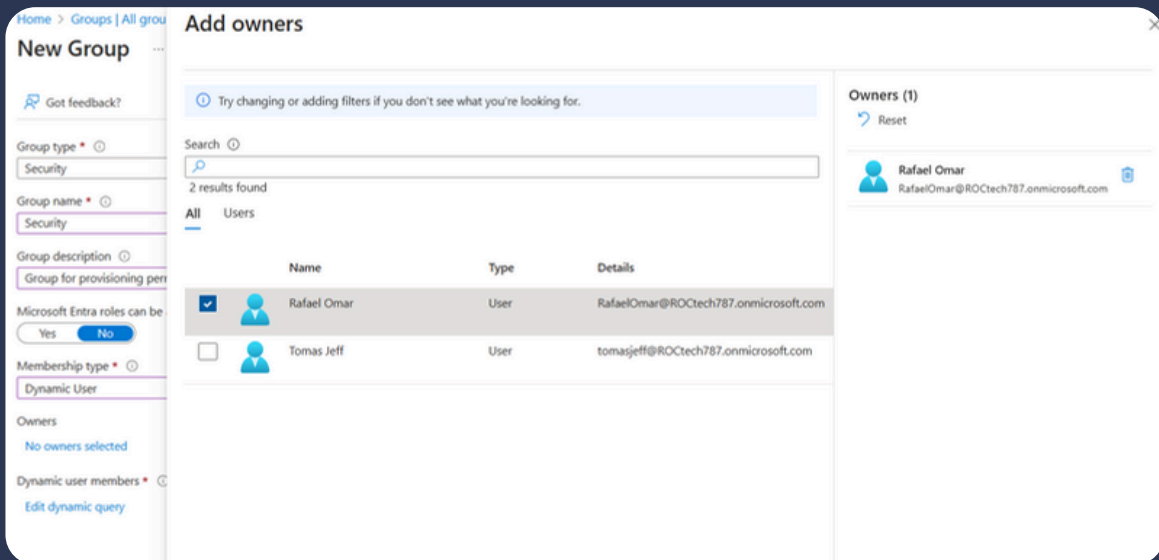
5. Here we can confirm that the Security group has been created succesfully.

6. Lastly lets make sure that the Dynamic Membership Rules are in effect. To do so we create a new user "Ben Frank". Making sure Ben's department is "Security" and his title starts with "VP".

Create new user ...
Create a new internal user in your organization

Basics   **Properties**   Assignments   Review + create

Identity

First name	Ben
Last name	Frank
User type	Member
Authorization info	+ Edit Certificate user IDs

Job Information

Job title	VP of Security Operations
Company name	ROCTech
Department	Security
Employee ID	0987654321

7. We can confirm that Ben Frank was dynamically placed at the Security Group as a member after meeting the rule criteria.

Security | Members ...
Group

+ Add members   Bulk operations ∨

Overview

Diagnose and solve problems

Direct members   All members

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

🔍 Search

1 group member found

☐ Name ↑

☐ BF Ben Frank

CONFIGURE AND ADMINISTER MULTI-FACTOR AUTHENTICATION (MFA)

1. We need to ensure that our MFA is both enabled and enforced.To do this we navigate to the users page and click on "Per-User MFA". We select our user "Ben Frank" and click on "Enable MFA" then "Enforce MFA".

CONFIGURE AND ADMINISTER MULTI-FACTOR AUTHENTICATION (MFA)

2. We can also configure which Authentication Methods to enabled for our users.

Auth Methods ...

+ Add external method (Preview)   ↻ Refresh | 💬 Got feedback?
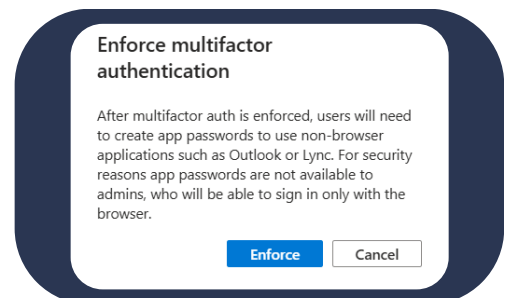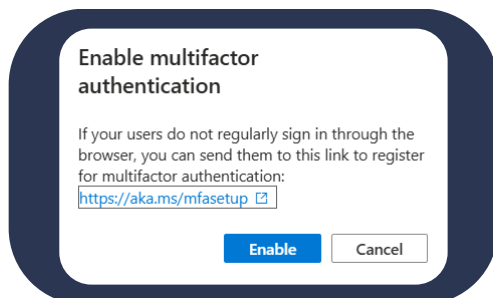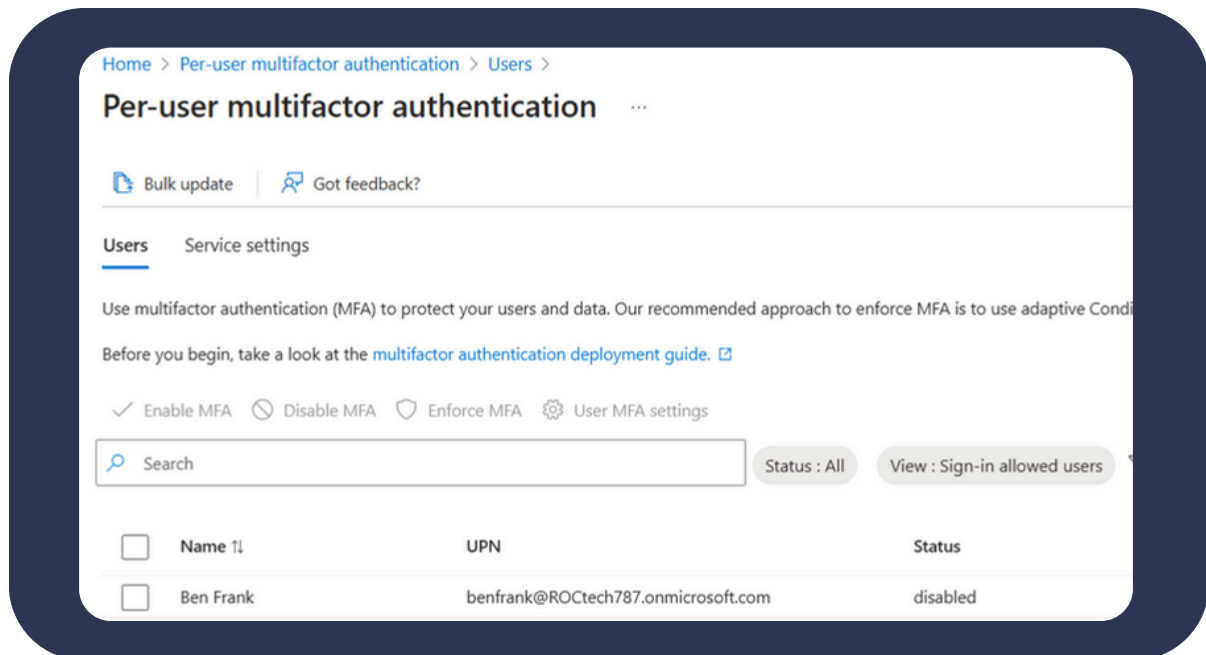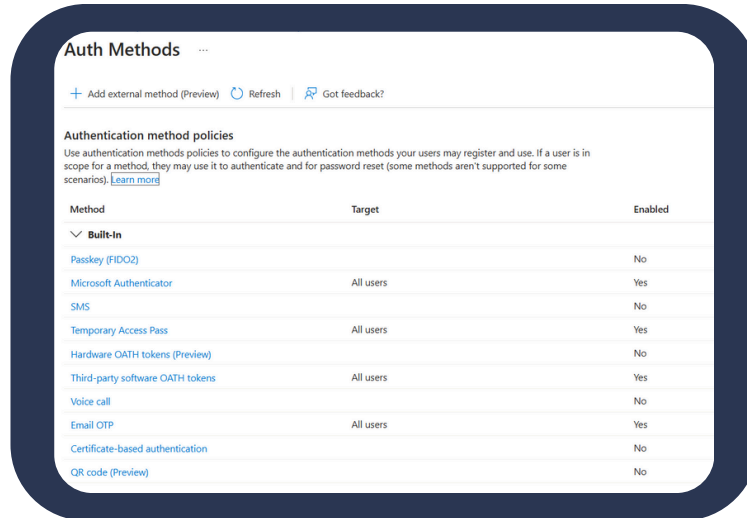
Authentication method policies

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		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 (Preview)		No

CONDITIONAL ACCESS POLICY FOR MFA

1. Lastly we can create a new "MFA" policy for conditional access requiring multifactor authentication.

Home > Users > Per-user multifactor authentication

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 ✓]

Assignments

Users ⓘ

All users

Target resources ⓘ

No target resources selected

Network **NEW** ⓘ

Not configured

Conditions ⓘ

0 conditions selected

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 authentication". Learn more ⧉

[ ] Require device to be marked as compliant ⓘ