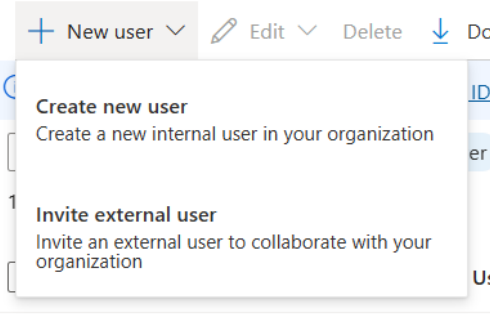
Lab 1 – Microsoft 365 / Azure AD (with Evidence)

In this lab, I set up a new Microsoft 365 tenant and created user accounts in Entra ID. I assigned licenses to the users and configured Multi-Factor Authentication (MFA) to secure sign-ins. This gave me a working Microsoft 365 environment with basic identity and access management.

Step 1 – Add User

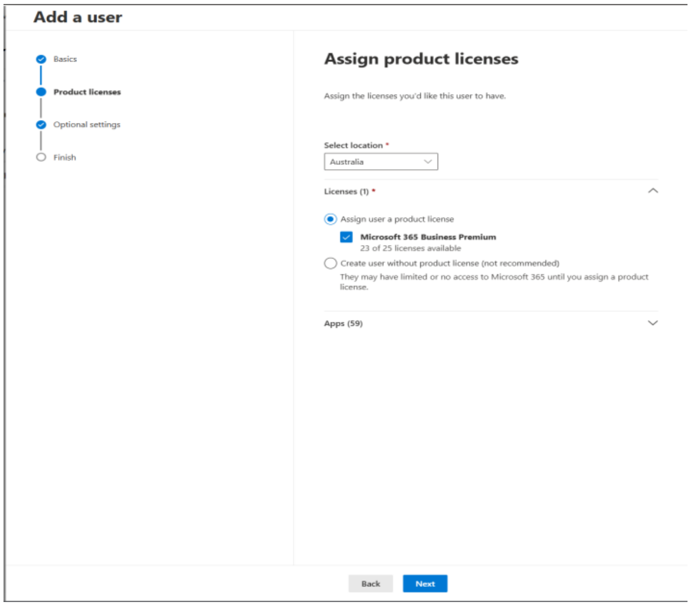


Create new user
Create a new internal user in your organization

Invite external user
Invite an external user to collaborate with your organization

Notes: Added a user named Tim.

Step 2 – Assign Product License



Add a user

Assign product licenses

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

Select location *
Australia

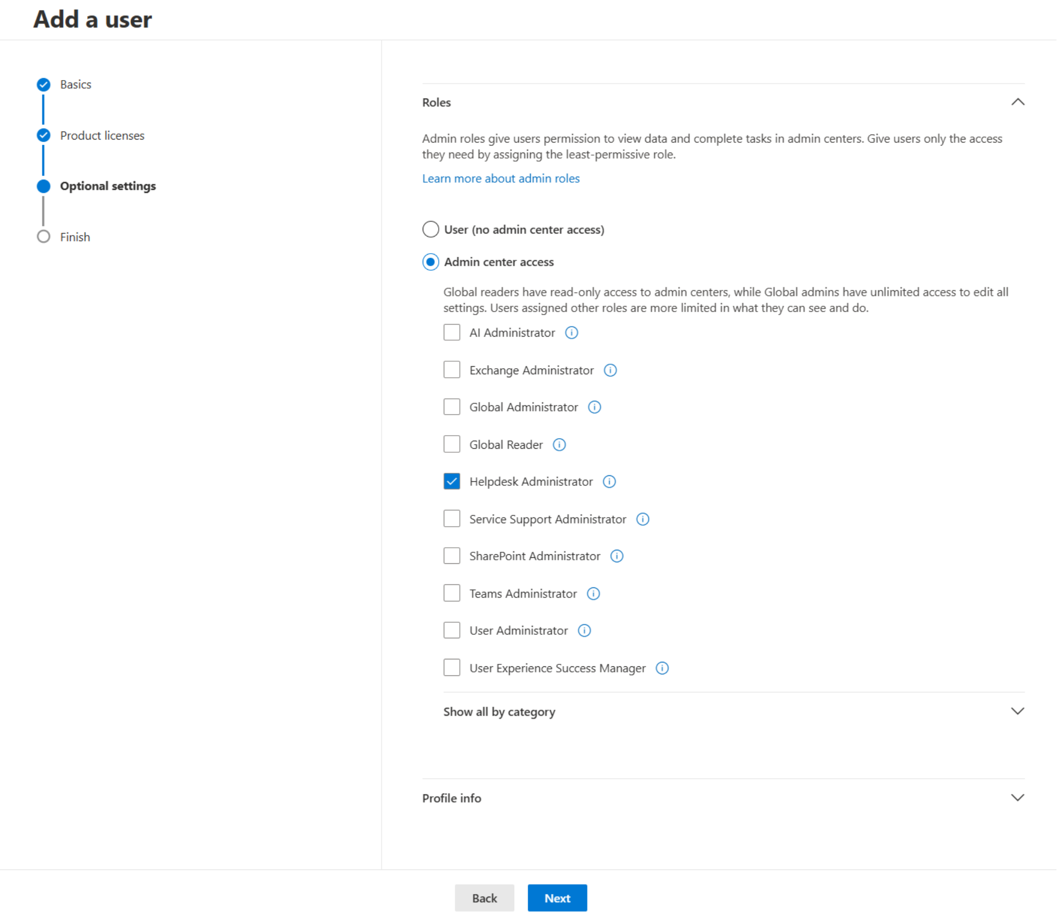
Licenses (1) *

● Assign user a product license
☑ Microsoft 365 Business Premium
23 of 25 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 (59)

Notes: I have a total of 25 licenses that I can provision within the company. Tim was assigned a Microsoft 365 Business Premium license.

Step 2b – Assign Role (Least Privilege)



Add a user

- ✓ Basics
- ✓ Product licenses
- ● **Optional settings**
- ○ Finish

Roles

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.

Learn more about admin roles

○ User (no admin center access)

● Admin center access

Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

- □ AI Administrator
- □ Exchange Administrator
- □ Global Administrator
- □ Global Reader
- ☑ Helpdesk Administrator
- □ Service Support Administrator
- □ SharePoint Administrator
- □ Teams Administrator
- □ User Administrator
- □ User Experience Success Manager

Show all by category

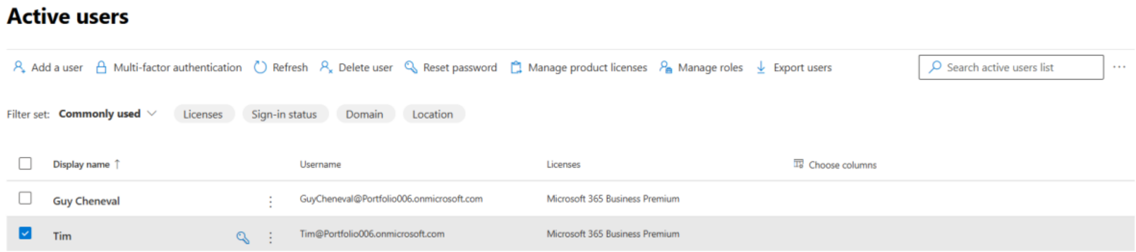
Profile info

Back | Next

Notes:

Applied the principle of least privilege by assigning Tim the Helpdesk Administrator role instead of Global Admin. This limits his permissions to only what is required.

Step 3 – Verify User in Active Users List



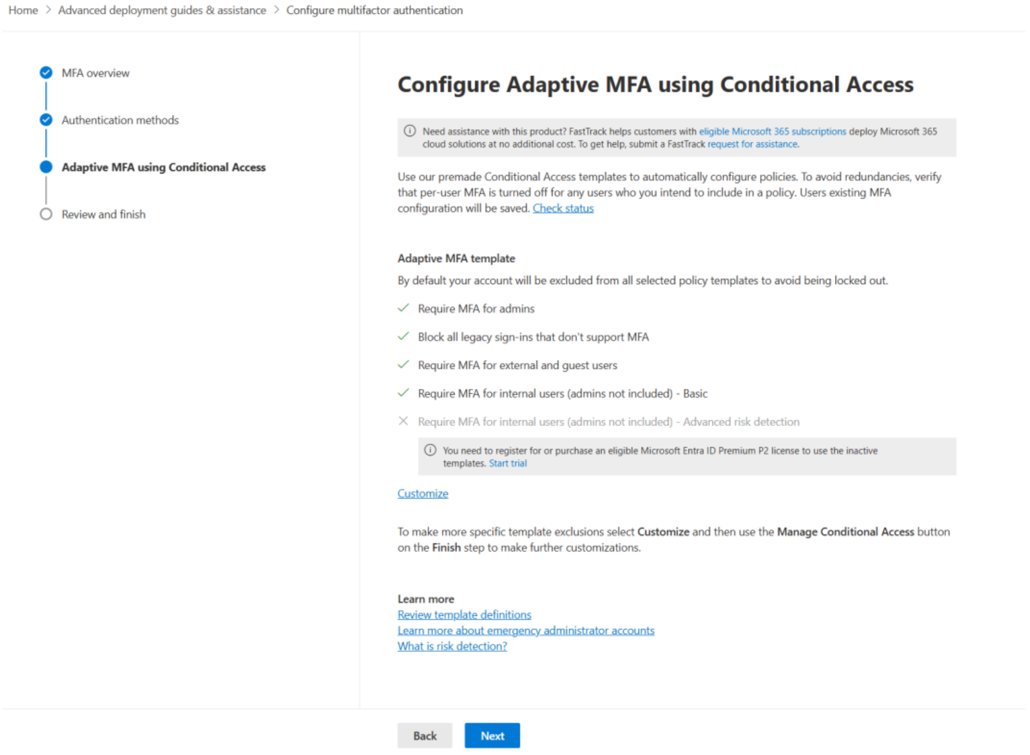
Active users

Filter set: **Commonly used** | Licenses | Sign-in status | Domain | Location

□	Display name ↑	Username	Licenses	Choose columns
□	Guy Cheneval	GuyCheneval@Portfolio006.onmicrosoft.com	Microsoft 365 Business Premium	
☑	Tim	Tim@Portfolio006.onmicrosoft.com	Microsoft 365 Business Premium	

Notes: The tenant now contains two accounts: my Admin account and Tim, who has just been added.

Step 4 – Configure MFA (Conditional Access)


Home > Advanced deployment guides & assistance > Configure multifactor authentication
MFA overview
Authentication methods
Adaptive MFA using Conditional Access
Review and finish
Back
Next

Configure Adaptive MFA using Conditional Access

ⓘ Need assistance with this product? FastTrack helps customers with eligible Microsoft 365 subscriptions deploy Microsoft 365 cloud solutions at no additional cost. To get help, submit a FastTrack request for assistance.

Use our premade Conditional Access templates to automatically configure policies. To avoid redundancies, verify that per-user MFA is turned off for any users who you intend to include in a policy. Users existing MFA configuration will be saved. Check status

Adaptive MFA template

By default your account will be excluded from all selected policy templates to avoid being locked out.

- ✓ Require MFA for admins
- ✓ Block all legacy sign-ins that don't support MFA
- ✓ Require MFA for external and guest users
- ✓ Require MFA for internal users (admins not included) - Basic
- ✕ Require MFA for internal users (admins not included) - Advanced risk detection

ⓘ You need to register for or purchase an eligible Microsoft Entra ID Premium P2 license to use the inactive templates. Start trial

Customize

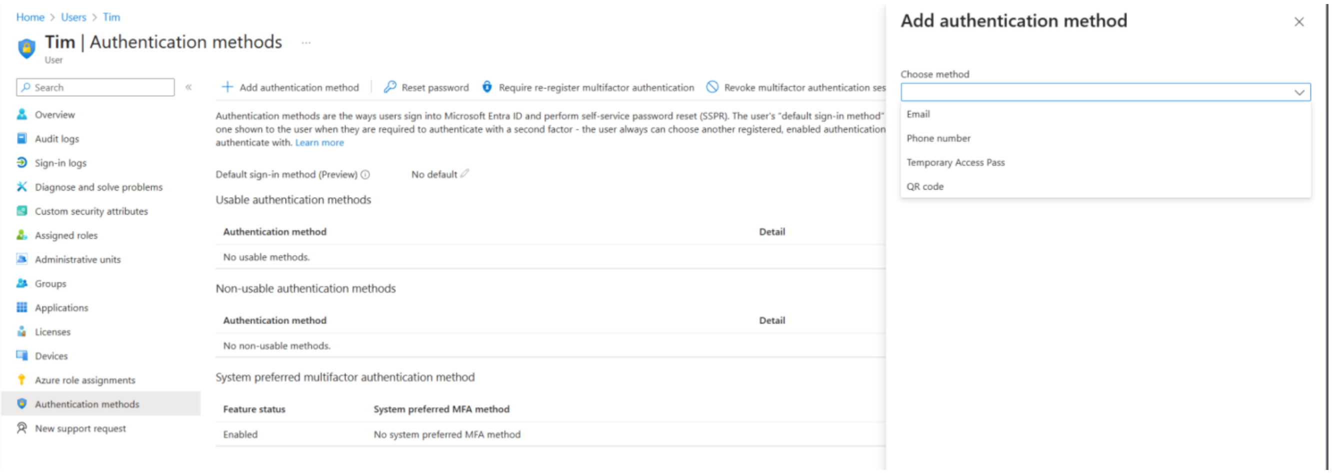
To make more specific template exclusions select **Customize** and then use the **Manage Conditional Access** button on the **Finish** step to make further customizations.

Learn more

Review template definitions
Learn more about emergency administrator accounts
What is risk detection?

Notes: Configured tenant policies so all employees are required to register and use the Microsoft Authenticator app.

Step 4b – User Authentication Methods



Tim | Authentication methods

User

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" one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication authenticate with. Learn more

Default sign-in method (Preview) ⓘ No default

Usable authentication methods

Authentication method	Detail
No usable methods.	

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	No system preferred MFA method

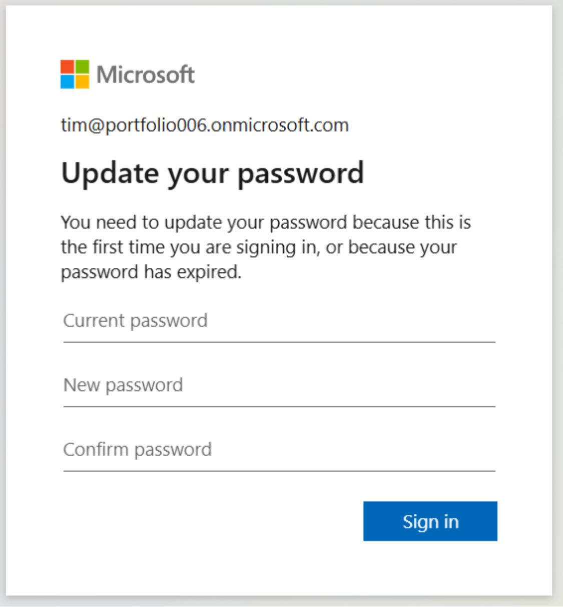
Add authentication method

Choose method

- Email
- Phone number
- Temporary Access Pass
- QR code

Notes: Verified that Tim has no authentication methods yet. As admin, I can enforce that all accounts register the Microsoft Authenticator app and optionally pair with their mobile number.

Step 5 – First Login (Password Update)



Microsoft

tim@portfolio006.onmicrosoft.com

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

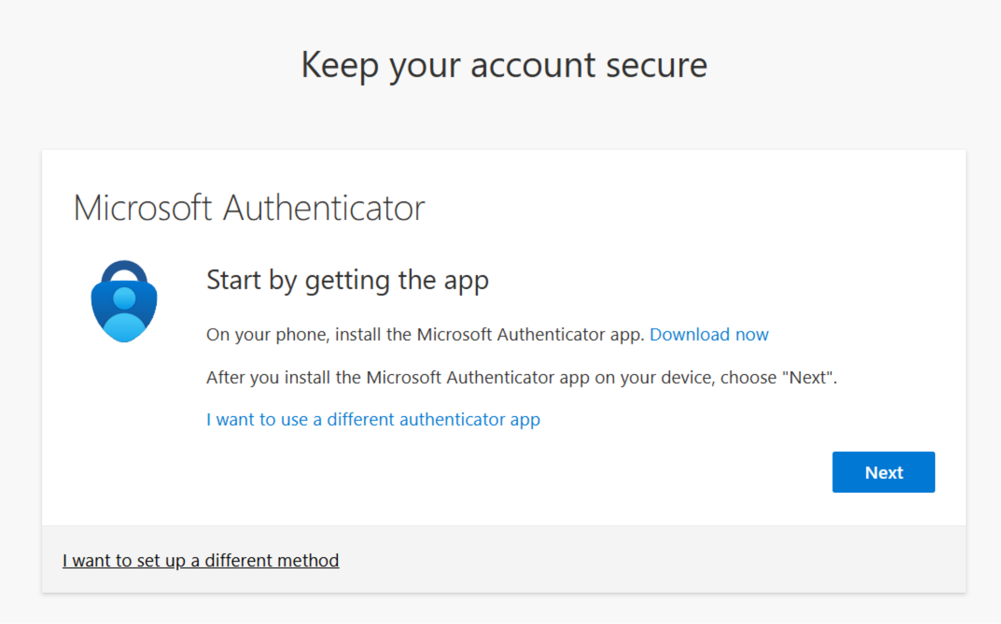
New password

Confirm password

Sign in

Notes: On first login, Tim was required to change his password. This enforces a strong password policy and demonstrates good security practice (e.g. mandatory resets every 90 days).

Step 6 – MFA Prompt (Download App)



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".

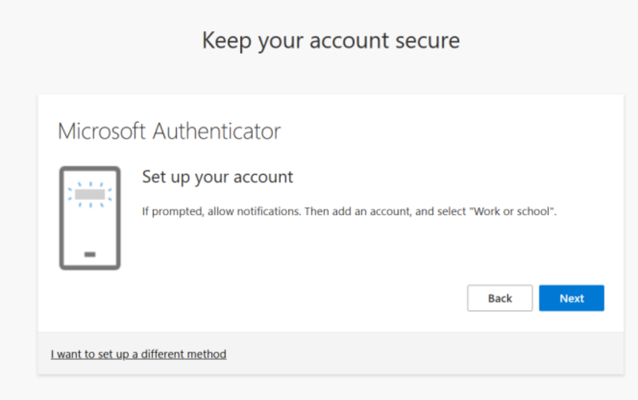
I want to use a different authenticator app

Next

I want to set up a different method

Notes: User was prompted to install the Microsoft Authenticator app before completing login.

Step 7 – MFA Setup (Set Up Account)



Keep your account secure

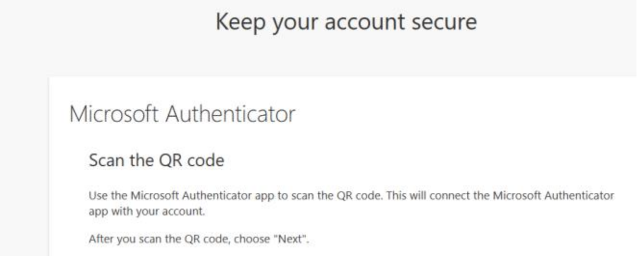
Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Notes: Apart of the MFA was Microsoft authenticator and each account needs to use it.

Step 8 – MFA Alternative (Scan QR Code)



Keep your account secure

Microsoft Authenticator

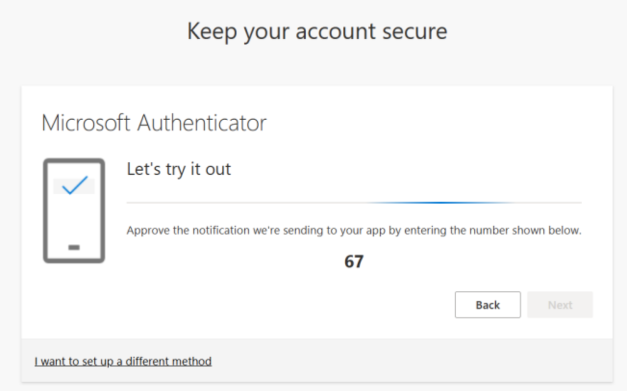
Scan the QR code

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".

Notes: The system generated a QR code, which can be scanned into Microsoft Authenticator for account pairing.

Step 9 – MFA Test (Notification Approval)



Keep your account secure

Microsoft Authenticator

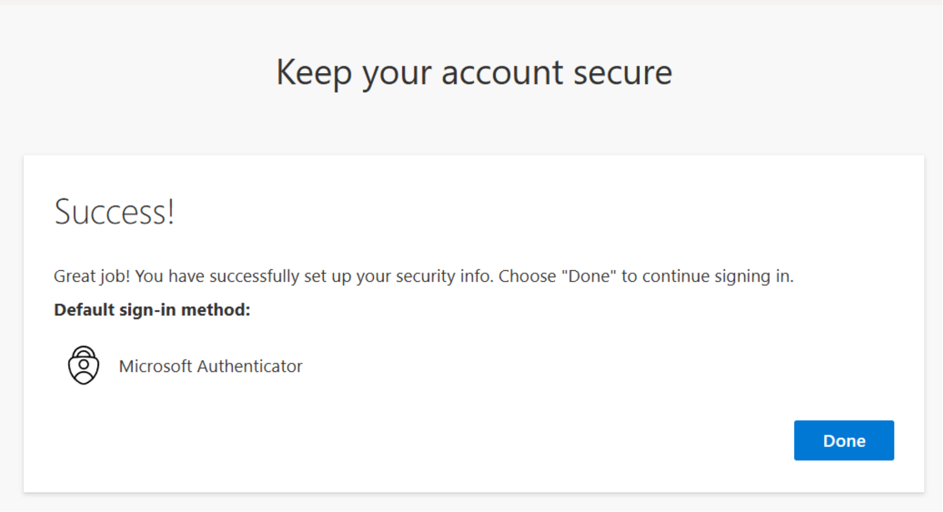
Let's try it out

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

67

Notes: A test notification was sent to the Authenticator app. User had to confirm the number to verify successful pairing, and moving forward will be prompted on there phone for any unusual activities and will be prompted for conformation if its them.

Step 10 – (MFA Success Screen)



Keep your account secure

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Microsoft Authenticator

Notes: MFA setup was completed successfully. The account is now protected with Microsoft Authenticator as the default sign-in method.

Lab – 5 Summary

This lab showed how to build a secure Microsoft 365 tenant from scratch. By creating users, assigning licenses, and applying least privilege roles, I set up the foundation for proper identity and access management. Enforcing MFA with Microsoft Authenticator added an extra layer of protection, making sure accounts are secured against unauthorized access.