## **Entra ID User & Group Lifecycle Management**

**Date:** 04/08/2025  
**Tools Used:** Microsoft Entra ID, Microsoft 365 Admin Center

1. **Project Overview:**

**Objective:**

Implement automated user lifecycle management including:

* User Provisioning/Deprovisioning
* Group-based license assignment
* RBAC implementation
* Security policy enforcement

1. **Implementation Steps:**

**2.1) User Creation in Entra ID**

**Steps:**

1. Navigate to Entra Admin Center (<https://entra.microsoft.com/).>

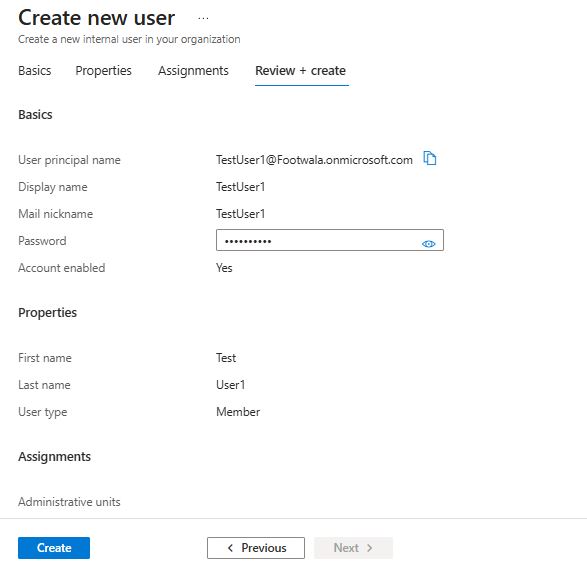
2. Go to **Identity → Users → All users → + New user**

3. Configure:

* Display Name: Test User1
* UPN: [TestUser1@footwala.onmicrosoft.com](mailto:TestUser1@footwala.onmicrosoft.com)
* Password

**Screenshot:**

1. **User Creation**



**2.2) Create Security Groups**

**Steps:**

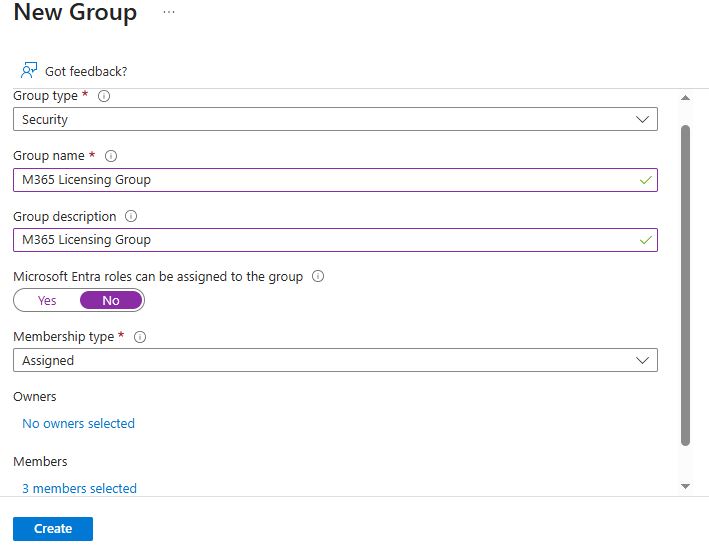
1. Navigate to **Entra Admin Center > Groups > All groups**
2. Click **+ New group**
3. Select:

* **Group type:** Security
* **Group Name:** M365 Licensing Group
* **Membership type:** Assigned

1. Add your test users to the group.
2. Click **Create.**

**Screenshot:**

1. **Security Group Creation**



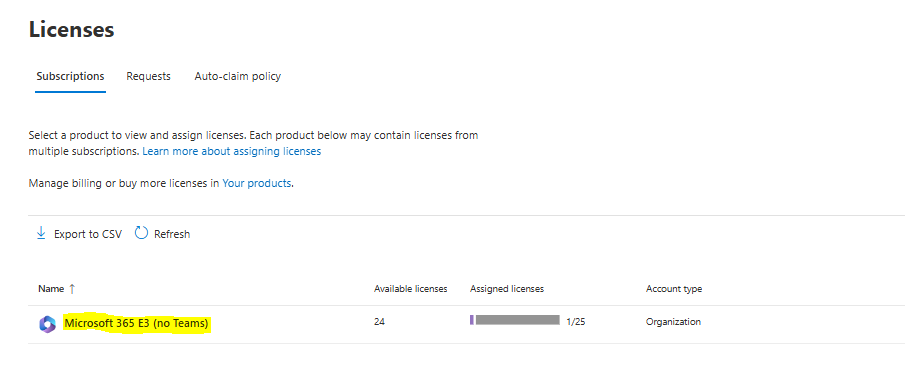
**2.3) Assign Microsoft 365 Licenses via Group-Based Licensing**

**Steps:**

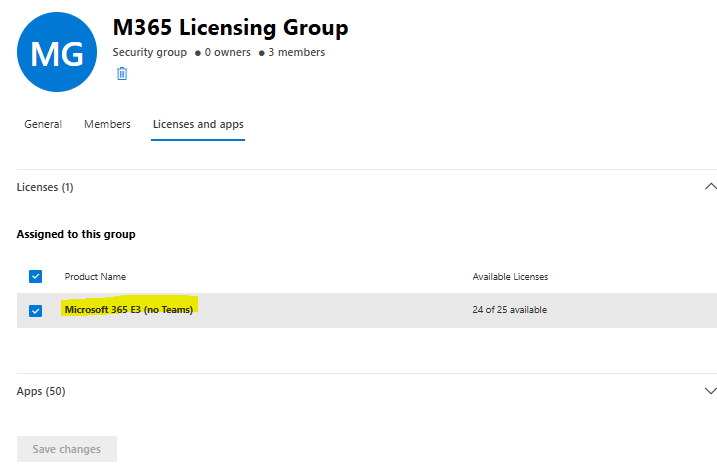
1. Go to **Microsoft 365 Admin Center > Billing > Licenses.**
2. Ensure licenses (e.g., Microsoft 365 E3) are available.
3. Then Go to **Groups** **> Active groups > M365 Licensing Group**
4. Click **Licenses and apps,** select **Microsoft 365 E3**
5. Click **Save changes.**
6. Users in the group will automatically get assigned the selected license.

**Screenshot:**

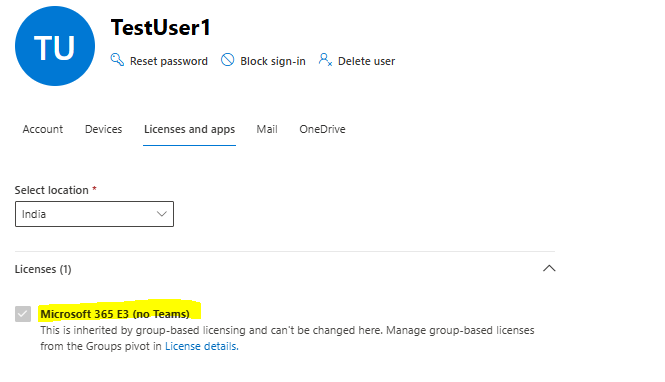
1. **Checking License Availability**



1. **Assigned License to M365 Licensing Group**



1. **Checking License assigned to User or Not.**



**2.4) Configure RBAC Roles**

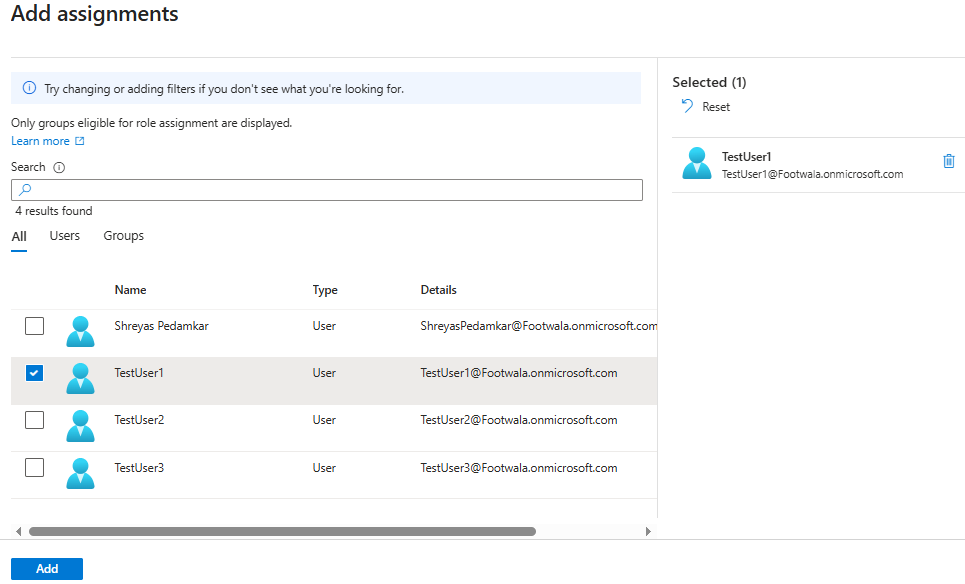
**Steps:**

1. Go to **Entra Admin Center > Roles and administrators**
2. Choose a role (e.g., User Administrator)
3. Click **+ Add assignments**
4. Select test user and assign the role.

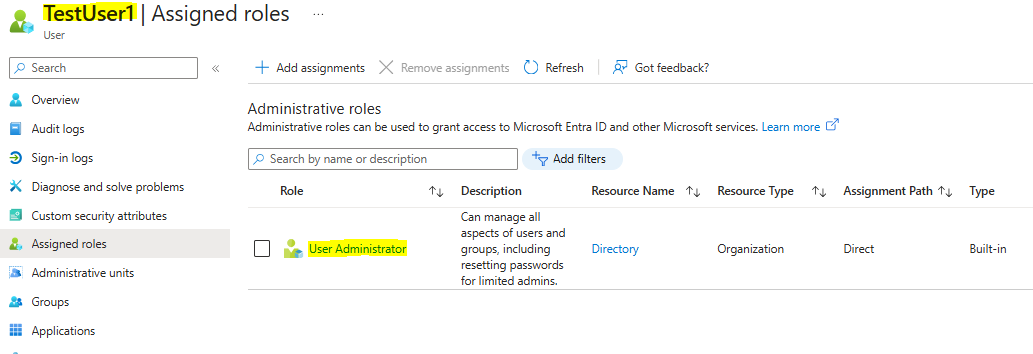
This applies Role-Based Access Control to limit admin Permissions.

**Screenshot:**

1. **RBAC configuration**



1. **Checking Role Assignment**



**2.5) User Onboarding and Offboarding**

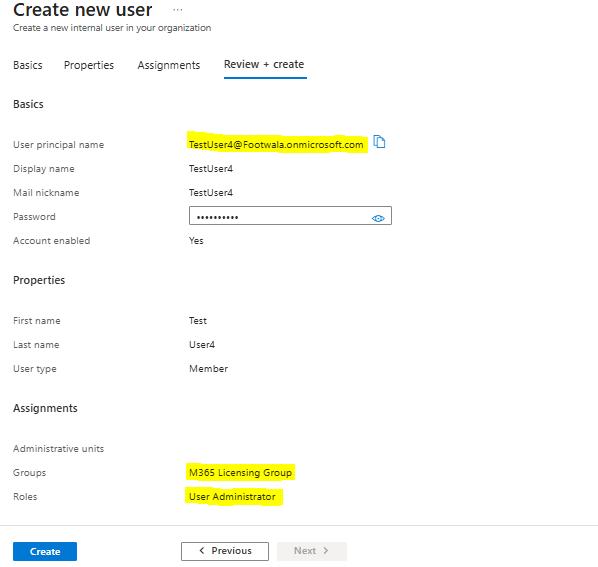
**Steps:**

**Onboarding:**

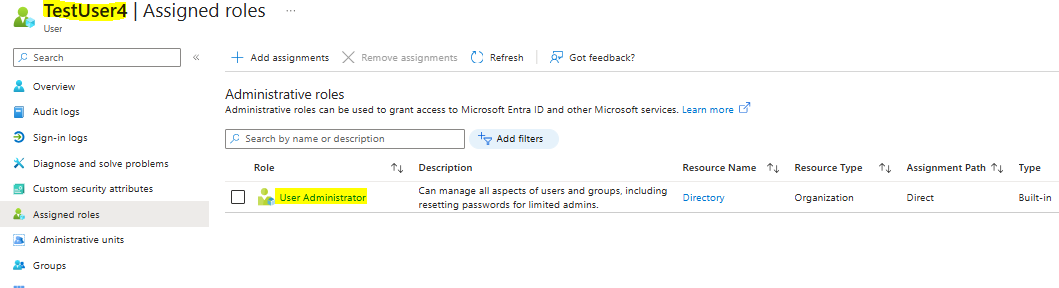
1. Created a new user.
2. Add user to licensing group (auto license assigned)
3. Assigned appropriate RBAC role
4. Test Sign-in via <https://office.com>

**Screenshot:**

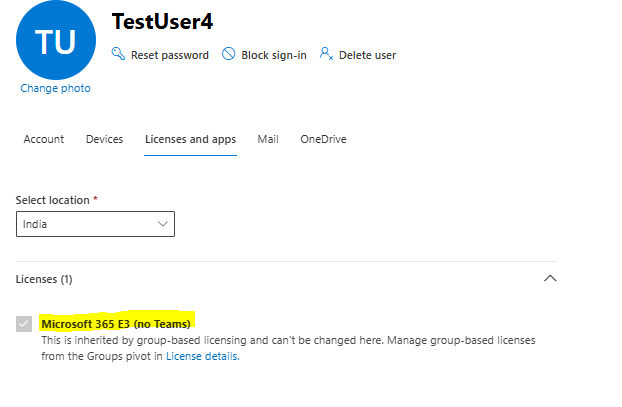
1. **Create user, add to group and assigned RBAC role**



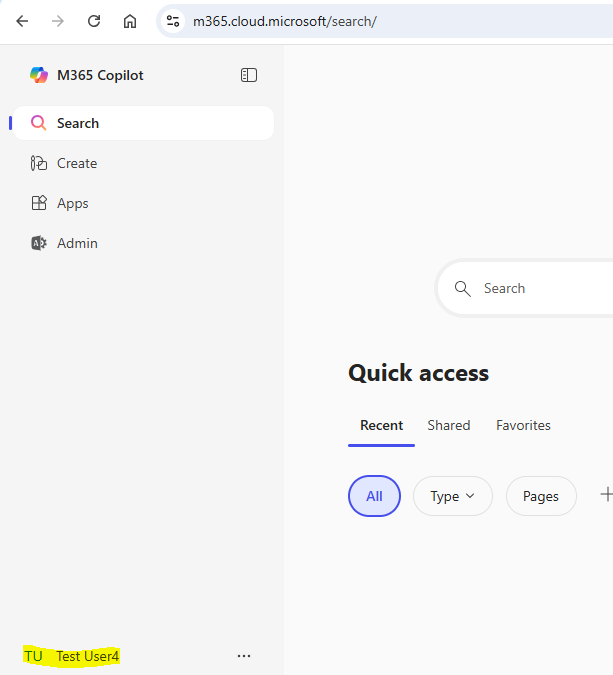
1. **RBAC role Assigned**



1. **Microsoft 365 E3 license Assigned**



1. **Tested sign-in via https://office.com**

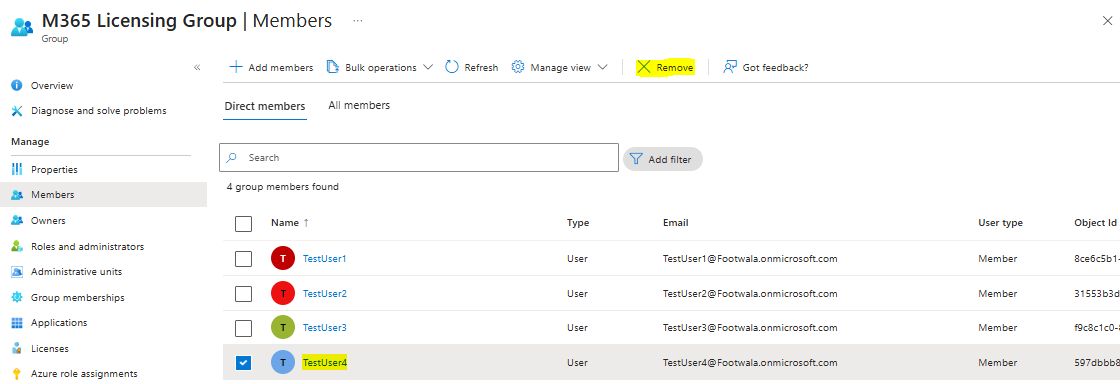


**Offboarding:**

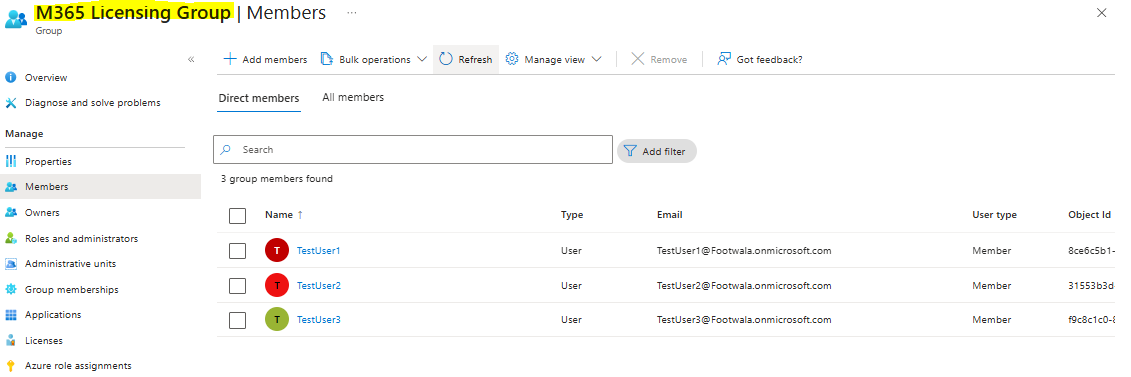
1. Removed user form group (license revoked)
2. Removed RBAC role
3. Deleted User

**Screenshot:**

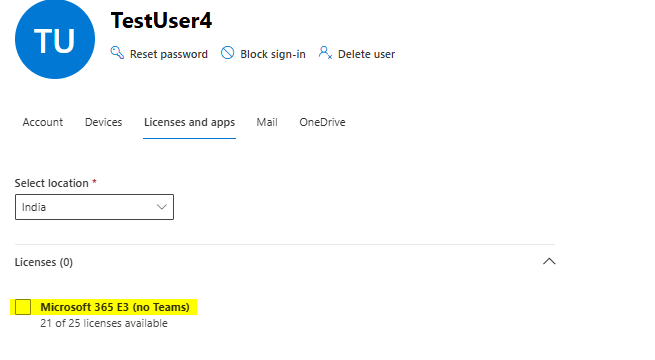
1. **Removed user from group**



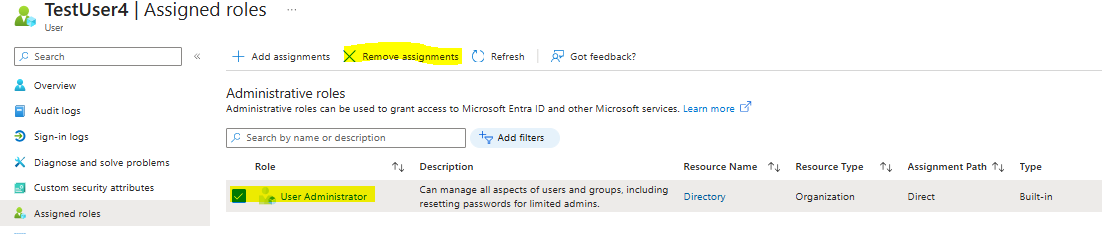
1. **TestUser4 not available in M365 licensing group**



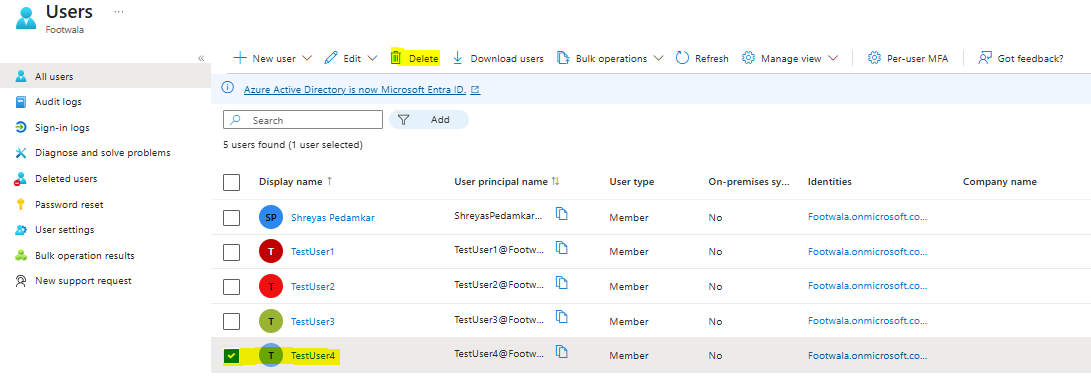
1. **License Revoked for TestUser4**



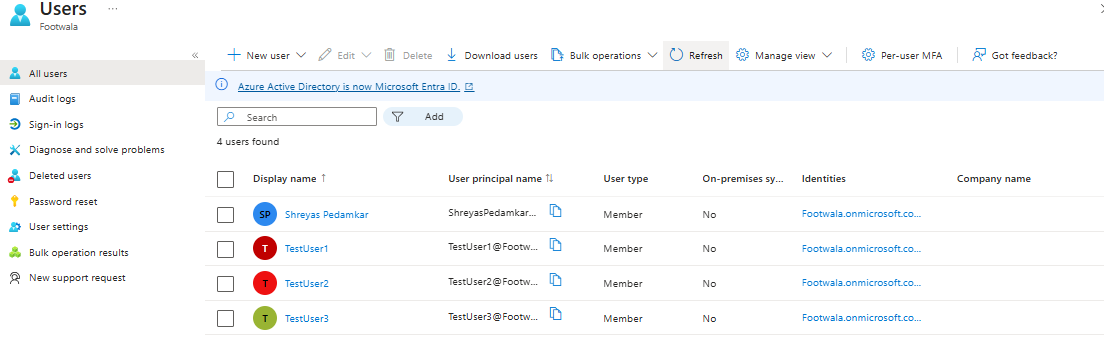
1. **Removed RBAC role for TestUser4**



1. **Deleted TestUser4**



1. **TestUser4 Successfully Deleted**



**2.5) Create Conditional Access Policy**

**Steps:**

1. Go to Entra Admin Center > Conditional Access.
2. Click + Create new policy
3. Configure:

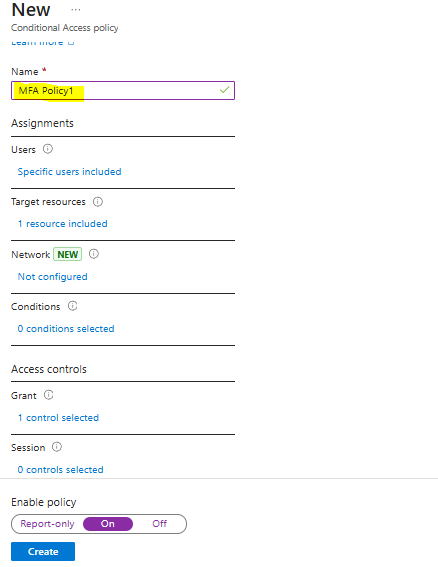
* Users: M365 Licensing Group
* Cloud Apps: Office 365
* Access Control: Required MFA

1. Click Create

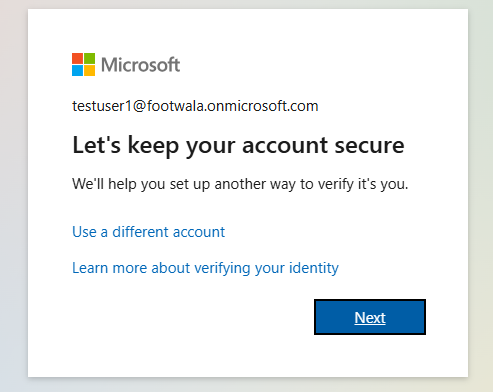
Test User will be prompted for MFA when accessing Office 365.

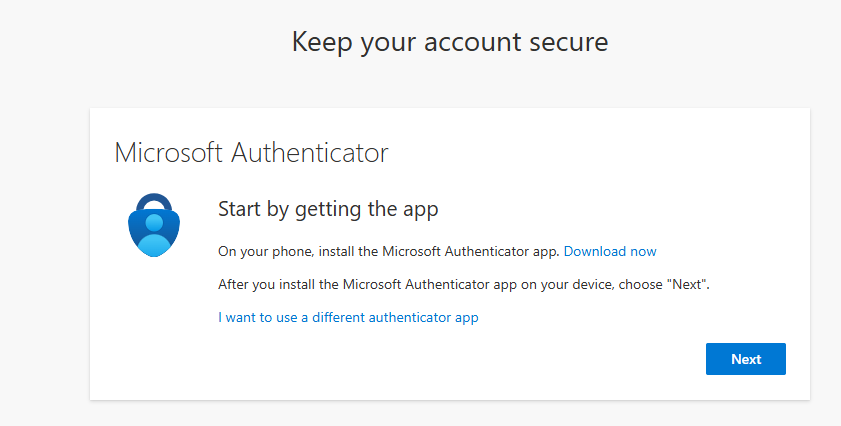
**Screenshot:**

1. **Created MFA conditional access policy**

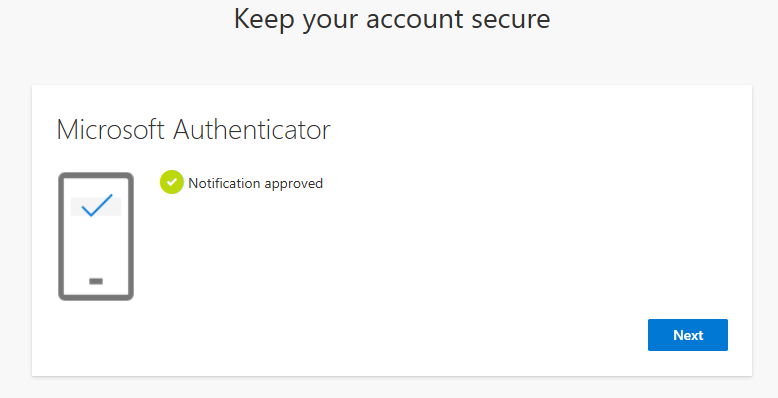


1. **TestUser1 asked for MFA**





1. **Multifactor Authentication Approved**



**2.6) Enable and Review Sign-in Logs**

**Steps:**

1. Go to Entra Admin Center > Monitoring > Sign-in logs.
2. Filter logs by user, status, or location.
3. Analyze:

* Successful/Failed logins
* MFA usage
* Conditional access policy result

Screenshot:

