

# Access Control & Identity Governance Audit Package

Environment: Microsoft Entra ID P2 (VDM Solutions LLC)

Author	Zonte Bryant
Date	September 2025
Version	v1.0
Classification	Internal Use

## Purpose

Enforce secure access controls in Microsoft Entra ID by requiring multi-factor authentication (MFA), implementing just-in-time (JIT) administrative access, and performing periodic access reviews. These measures reduce the risk of unauthorized access and support Zero Trust principles. This lab simulates controls commonly expected under NIST SP 800-53 and FedRAMP for identity and access management.

## Scope

All users and administrators within the Entra ID tenant (VDM Solutions LLC). Evidence collected from the lab includes test users, Conditional Access policies, Access Reviews, Privileged Identity Management (PIM) settings, and sign-in logs.

## Control Objectives

- CO-1: Enforce MFA for privileged accounts and sensitive access.
- CO-2: Review user/group access on a periodic basis to maintain least privilege.
- CO-3: Apply JIT admin elevation for privileged roles (no standing Global Admins).

## Implementation Summary

- Conditional Access: Policy created to require MFA for administrative roles; tested via user sign-ins.
- Access Reviews: One-time review configured for the Security Test Group to validate continued access.
- Privileged Identity Management (PIM): Test user set as Eligible Global Administrator with MFA and justification required on activation.

## Controls Alignment (NIST SP 800-53 & FedRAMP)

This lab is educational and not a full authorization package. The implemented controls map to selected NIST SP 800-53 control families commonly referenced by FedRAMP:

- AC-2 Account Management – Test identities created and reviewed via access review process.
- AC-3 Access Enforcement – Conditional Access enforces MFA and access conditions.
- AC-6 Least Privilege – PIM reduces standing privilege; elevation is time-bound and controlled.
- IA-2 Identification and Authentication – MFA enforced for privileged access and tested in sign-in flows.

# Procedures Performed

- Created test users and assigned roles in Entra ID.
- Configured Conditional Access policy requiring MFA for administrator roles.
- Validated enforcement via Azure sign-in logs (interrupted/success states).
- Created Security Test Group and launched an Access Review (one-time).
- Configured PIM: Global Administrator eligibility with MFA + justification; tested activation prompt.
- Performed password reset scenario via Microsoft 365 Admin Center.

# Audit Evidence (Screenshots)

The following figures are attached as evidence and correspond to the steps above.

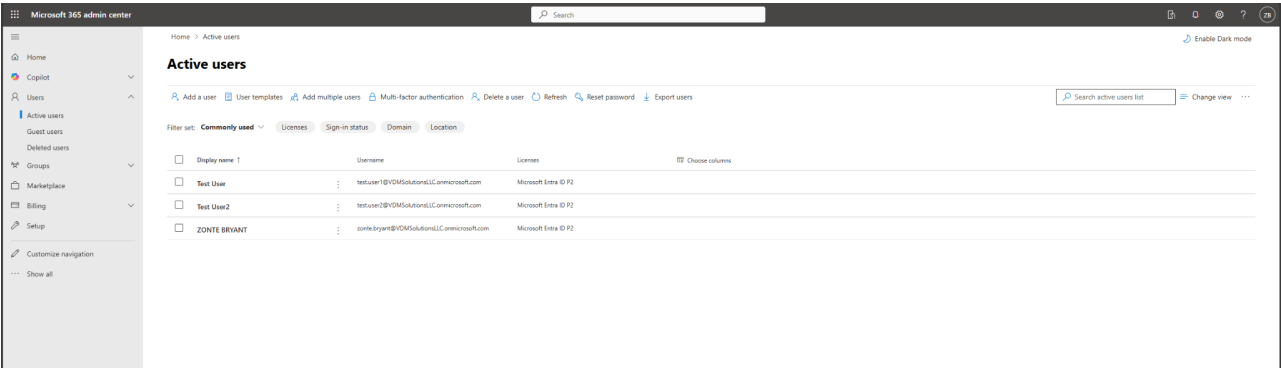


Figure: Test users created in Microsoft 365 Admin Center.

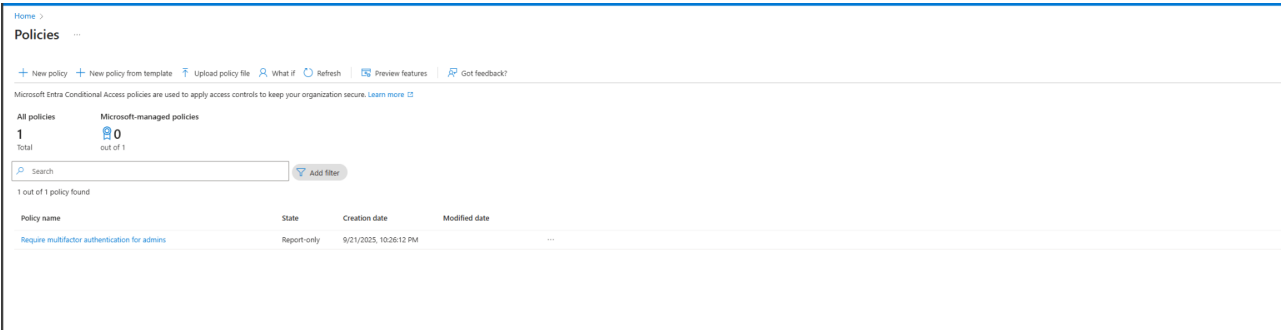


Figure: Conditional Access policy created to require MFA for admin roles.

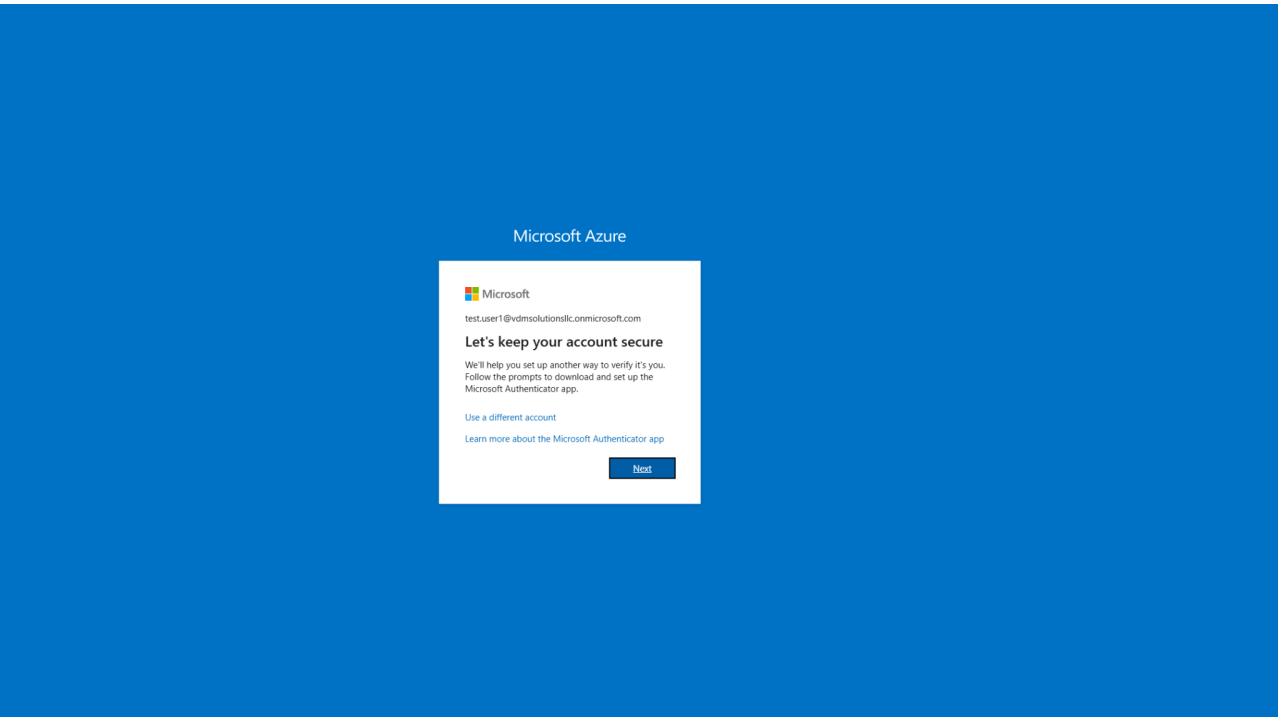


Figure: Conditional Access policies visible in Entra ID portal.

Microsoft Azure

Solutions LLC

Solutions LLC | Sign-in logs

DownloadExport data SettingsTroubleshootRefreshManage viewGot feedback?

Want to switch back to the legacy sign-in logs experience? Click here to leave the preview.

Add filterShow dates as UTCDate range: Last 24 hoursUser contains Test UserReset filters

User sign-ins (interactive)User sign-ins (non-interactive)Service principal sign-insManaged identity sign-ins

Date	Request ID	User principal name	Application	Status	IP address	Resource	Resource ID	Conditional ac...	User	Location
2025-09-22T02:38:00Z	b18e72e67-2293-4d9a-ac0c-2a9f8...	test.user1@vdm solutions...	Azure Portal	Interrupted	[REDACTED]	Azure Resource Manager	797f4846-ba00-4f57-ba...	Not applied	Test User	Charlotte, North Carolin...
2025-09-22T02:32:19Z	c312d978-4772-463b-9143-77a3...	test.user1@vdm solutions...	Azure Portal	Failure	[REDACTED]	Azure Resource Manager	797f4846-ba00-4f57-ba...	Not applied	Test User	Charlotte, North Carolin...
2025-09-22T02:34:03Z	e8d49bcc-5216-46eb-a2b9-a095...	test.user1@vdm solutions...	Azure Portal	Success	[REDACTED]	Azure Resource Manager	797f4846-ba00-4f57-ba...	Not applied	Test User	Charlotte, North Carolin...
2025-09-22T02:38:04Z	f213db3f-16f5-4666-a944-2a141...	test.user1@vdm solutions...	Azure Portal	Success	[REDACTED]	Azure Resource Manager	797f4846-ba00-4f57-ba...	Not applied	Test User	Charlotte, North Carolin...

Figure: Sign-in logs indicating Conditional Access policy effects (Interrupted/Success).

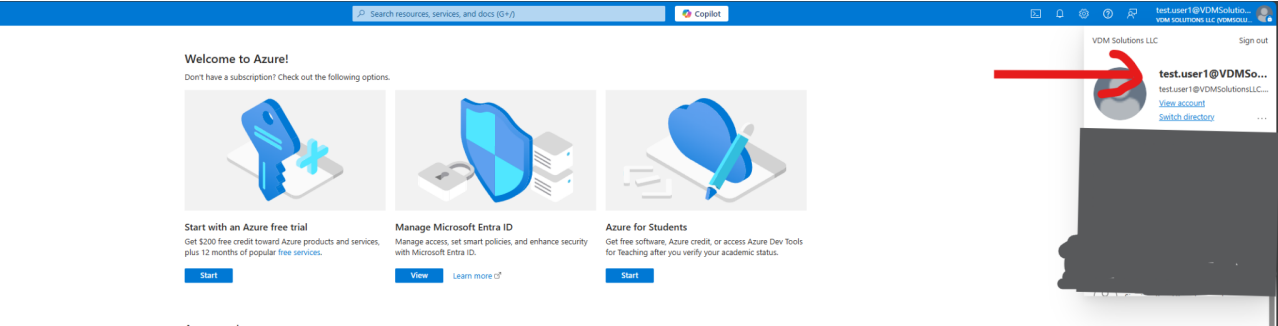


Figure: Successful sign-in after MFA registration.

Microsoft Azure

Home > VDM Solutions LLC > Groups > All groups >

## New Group

Get feedback?

Group type \*

Group name \*

Group description

Microsoft Entra roles can be assigned to the group ☐

☐ Yes ☒ No

Membership type \*

Owners  
1 owner selected

Members  
1 member selected

Create

Figure: Security Test Group created for governance review.

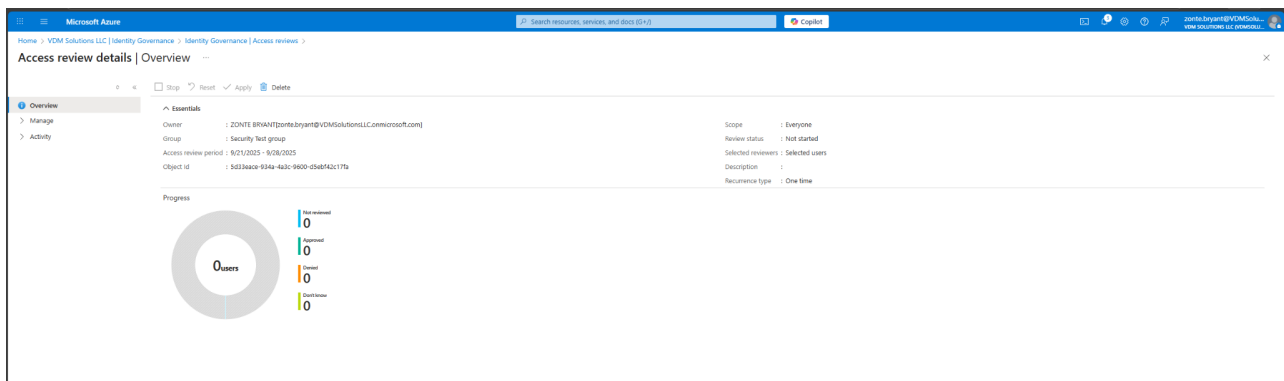


Figure: Access Review configured for the Security Test Group.

Microsoft Azure

Home > Identity Governance > Groups > Privileged Identity Management > Microsoft Entra roles > VDM Solutions LLC > Roles >

## Global Administrator | Assignments

Privileged Identity Management | Microsoft Entra roles

Manage | Add assignments | Settings | Refresh | Export | Get feedback?

Eligible assignments | Active assignments | Expired assignments

Search by member name or principal name

Name	Description	Principal name	Type	Scope	Membership	Start time	End time	Action
Global Administrator								
Test User		test.user1@VDM.com	User	Directory	Direct	9/21/2023, 11:15:48 PM	10/21/2023, 11:13:37 P...	Remove   Update   Extend

Showing 1 - 1 of 1 results.

Figure: PIM: Test user assigned as Eligible Global Administrator.

## Edit role setting - Global Administrator ...

Privileged Identity Management | Microsoft Entra roles

Activation Assignment Notification

Activation maximum duration (hours)

-----○----- 8

On activation, require


- ☐ None
- ☒ Azure MFA
- ☐ Microsoft Entra Conditional Access authentication context


[Learn more](#)

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

 Select approver(s)

No approver selected 

Update

Next: Assignment

Figure: PIM role settings requiring MFA and justification for activation.

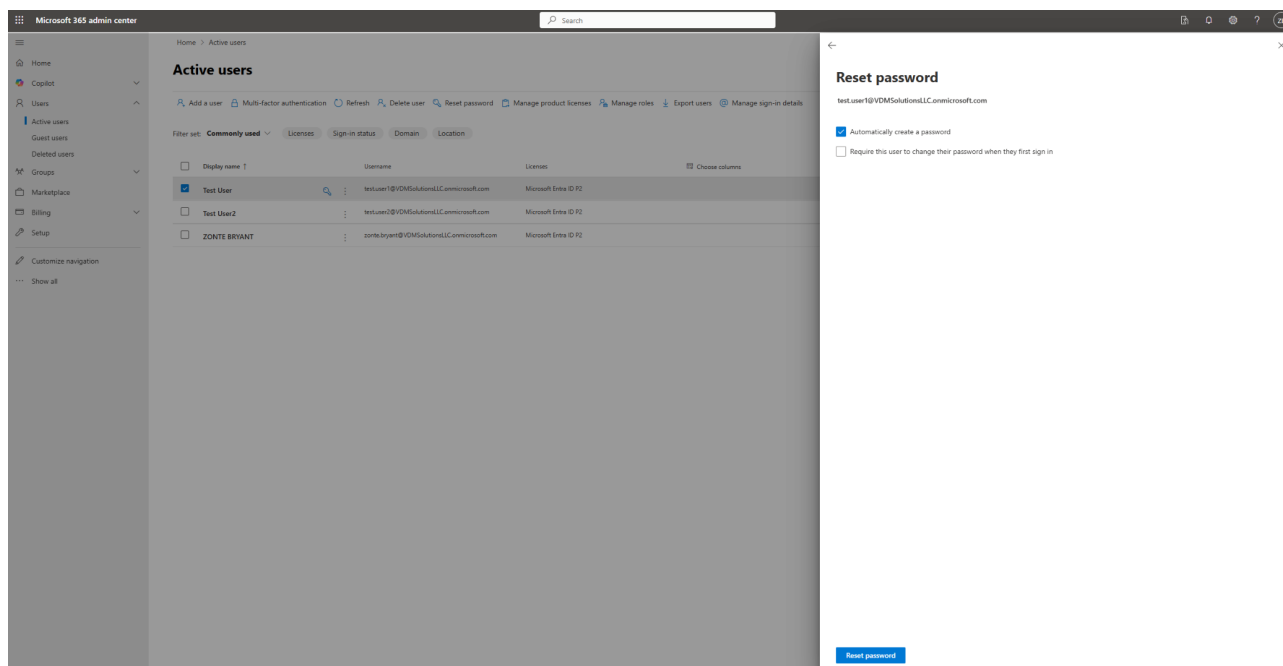


Figure: Password reset performed via Microsoft 365 Admin Center.

## Results & Conclusion

Controls operated as designed in the lab environment: MFA was enforced for targeted roles, the access review was initiated for the Security Test Group, and privileged access elevation required MFA and a justification via PIM. This demonstrates practical implementation of identity-focused Zero Trust controls aligned to NIST SP 800-53. Note: This lab is for learning; it mirrors compliance practices but is not a FedRAMP authorization.

## POA&M; / Next Steps

- Extend Conditional Access to all user populations and block legacy authentication protocols.
- Schedule quarterly access reviews; capture reviewer decisions and remediation evidence.
- Enable approval workflow for PIM activations and integrate ticket references.
- Export sign-in and audit logs to a SIEM (e.g., Microsoft Sentinel) for continuous monitoring.