

Azure IAM and CyberArk Skills Showcase

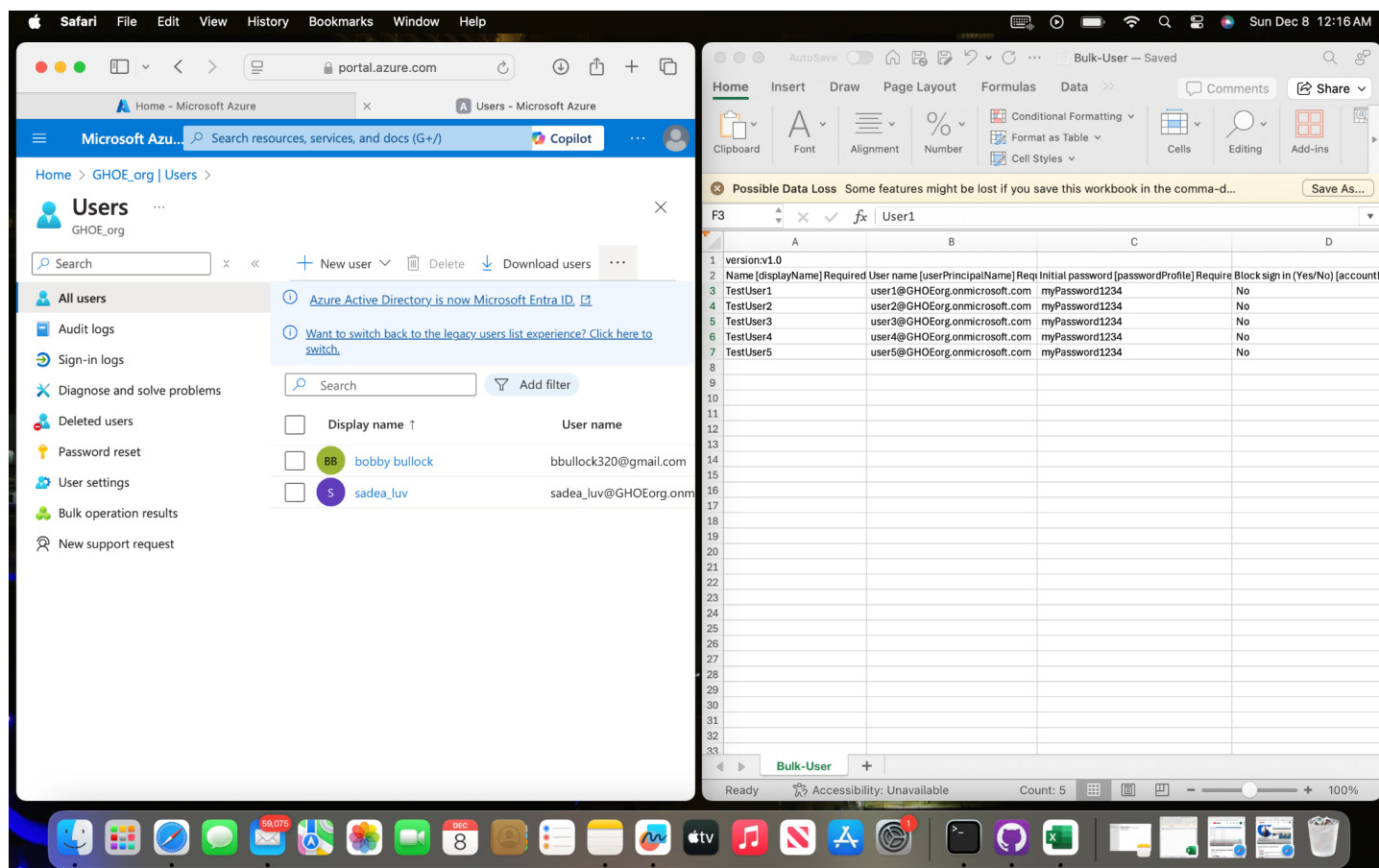
Welcome to my professional Azure Identity and Access Management (IAM) showcase. This document highlights my expertise in implementing secure access controls, managing privileged identities, configuring RBAC roles, and working with Azure Virtual Machines (VMs). I also have experience with CyberArk Privileged Access Security (PAS) and Microsoft PIM to ensure compliance and security best practices. My certifications include:

- CompTIA Security+
- ISC2 Certified in Cybersecurity (CC)
- Microsoft SC-300: Identity and Access Administrator Associate
- CompTIA Network+
- Certified Scrum Master (CSM)

This portfolio demonstrates how I've applied these skills using Azure and other IAM tools.

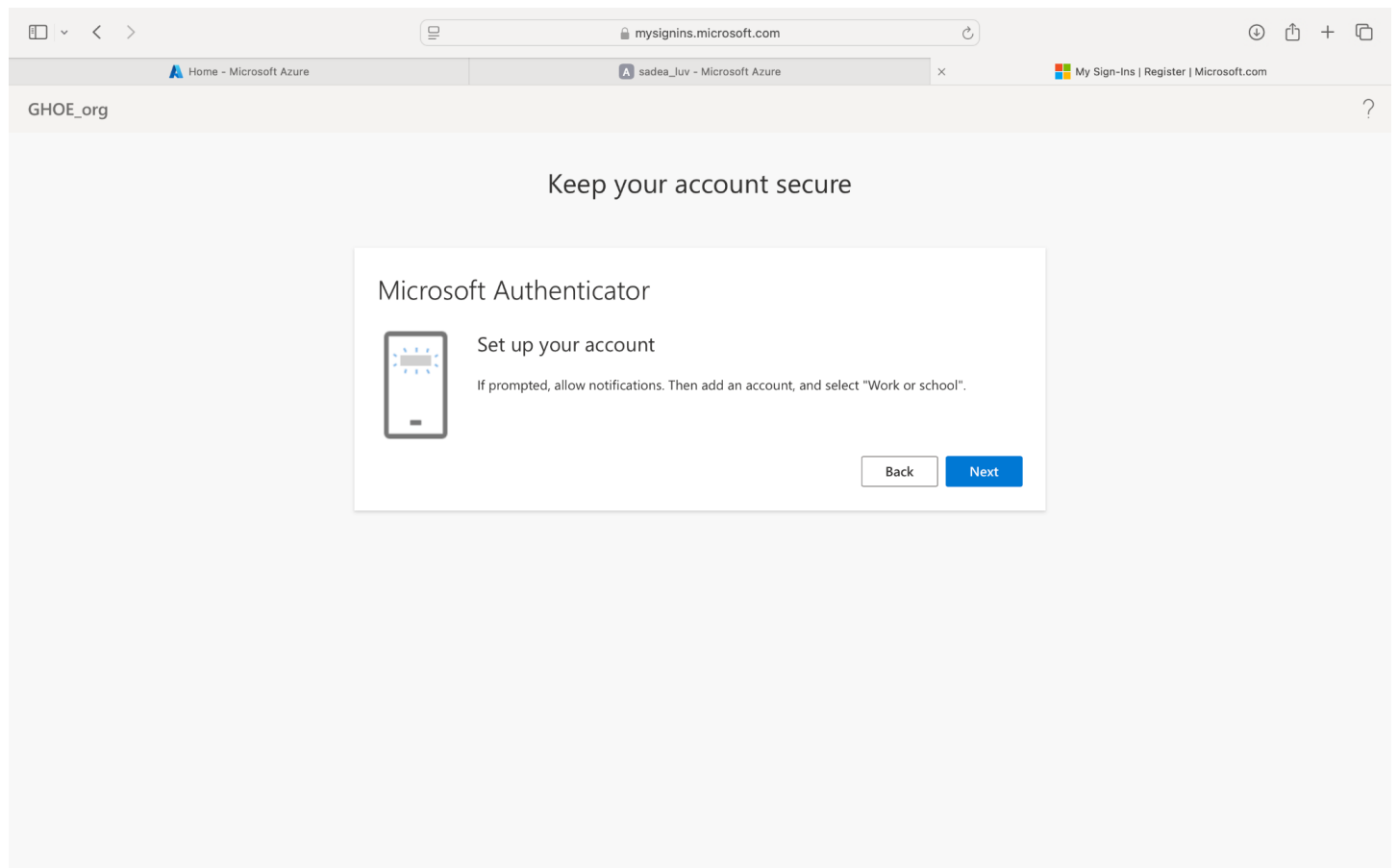
1. Bulk User Creation in Azure Active Directory

I created multiple users using Azure's bulk upload feature. This allows organizations to efficiently onboard users while ensuring secure access configurations.



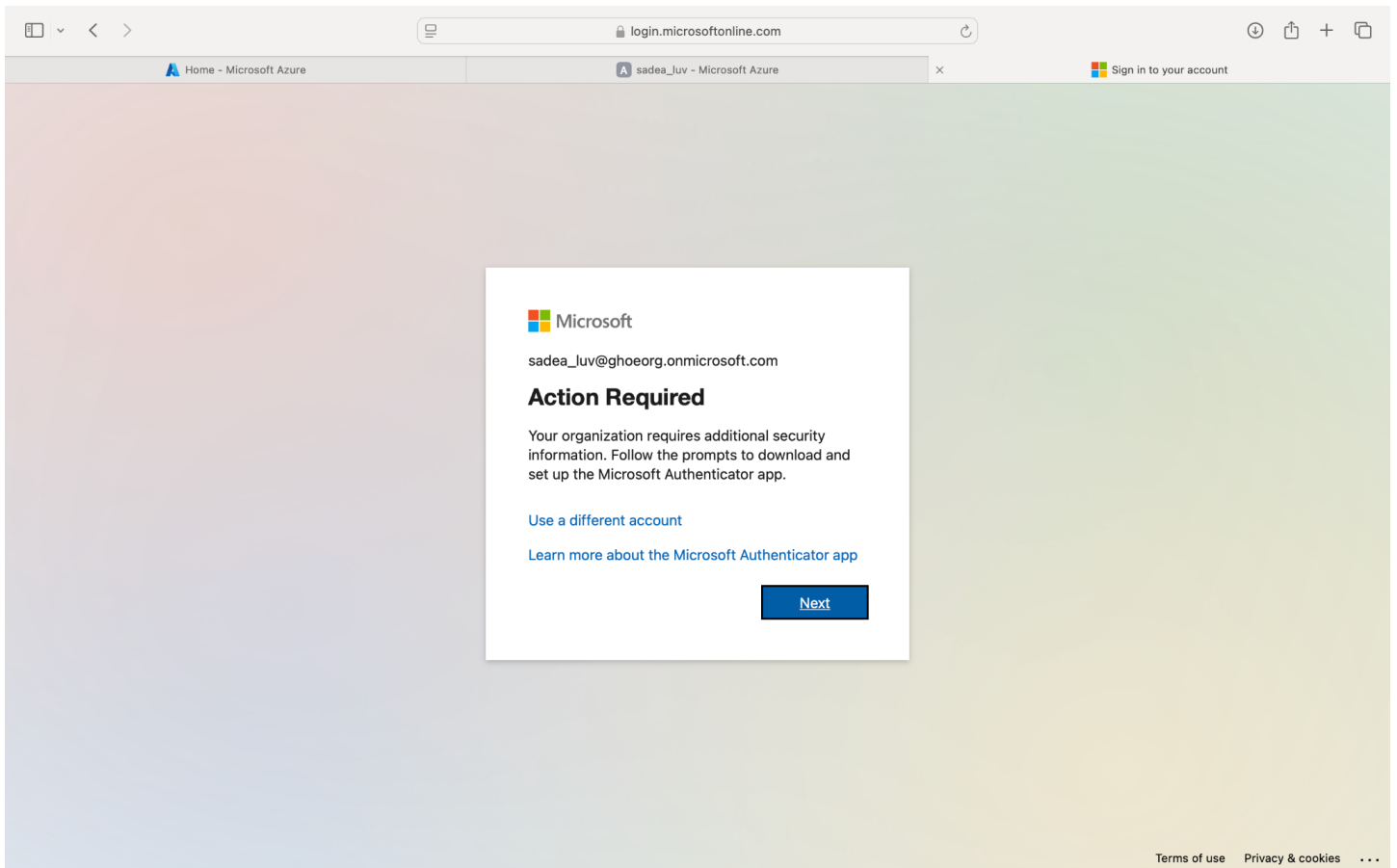
2. Implementing Multi-Factor Authentication (MFA)

Enabled MFA through Microsoft Authenticator to add an additional layer of security to user sign-ins, preventing unauthorized access.



3. Enforcing MFA Policies

Implemented MFA enforcement for all users in the organization, ensuring compliance with security policies.



4. User Lifecycle Management - Account Overview

Demonstrated managing user accounts (enabling, disabling, and lifecycle tracking) to ensure proper identity governance.

portal.azure.com

Home - Microsoft Azure

sadea_luv - Microsoft Azure

Sign in to your account

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

bbullock320@gmail.com

GHOE_ORG (GHOEORG.ONMICR...

Home >

sadea_luv

User

Search

Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview

- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Assigned roles
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods
- New support request

sadea_luv

sadea_luv@GHOEorg.onmicrosoft.com

Member

User principal name	sadea_luv@GHOEorg.onmicrosoft.com	Group memberships	View
Object ID	c7fc2ce4-624d-449c-a675-8ec9bfd3bcc	Applications	View
Created date time	Dec 7, 2024 at 6:48 PM	Assigned roles	View
User type	Member	Assigned licenses	View
Identities	GHOEorg.onmicrosoft.com		

My Feed

Account status

Disabled

[Edit](#)

B2B invitation

[Convert to external user](#)

Quick actions

[Edit properties](#)

5. Account Lockout for Security

Implemented account lockout policies to protect against brute-force attacks and malicious login attempts.

portal.azure.com

Home - Microsoft Azure

Test User3 - Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

bbullock320@gmail.com

GHOE_ORG (GHOEORG.ONMICR...

Home >

Test User3

User

Search

Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Assigned roles

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

New support request

Overview Monitoring Properties

Basic info

TU Test User3

test.user3@GHOEorg.onmicrosoft.com

Member

User principal name test.user3@GHOEorg.onmicrosoft.com

Object ID 5456b5f8-b1d8-4e34-967b-d45493985195

Created date time Dec 8, 2024 at 12:26 PM

User type Member

Identities GHOEorg.onmicrosoft.com

Group memberships View

Applications View

Assigned roles View

Assigned licenses View

My Feed

Account status Disabled

Edit

B2B invitation

Convert to external user

Quick actions

6. Role-Based Access Control (RBAC)

Assigned roles like 'Global Administrator' and 'Helpdesk Administrator' to users to ensure least privilege access and proper role segregation.

portal.azure.com

Home - Microsoft Azure | How to migrate to the Authentication methods policy - Mi... | Deployment considerations for Microsoft Entra multifactor... | bobby bullock - Microsoft Azure

Microsoft Azure | Search resources, services, and docs (G+)

Home > Users > bobby bullock

bobby bullock | Assigned roles | User

Search | Add assignments | Remove assignments | Refresh | Got feedback?

Overview | Audit logs | Sign-in logs | Diagnose and solve problems | **Assigned roles** | Groups | Applications | Licenses | Devices | Azure role assignments | Authentication methods | New support request

Administrative roles
Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. [Learn more](#)

Search by name or description | Add filters

Role	Description	Resource Name	Resource Type	Assignment Path	Type
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	Directory	Organization	Direct	Built-in

7. Privileged Identity Management (PIM)

Managed and monitored privileged identities using Azure PIM to ensure elevated permissions are granted only when required.

Microsoft Azure

Home > Users >

Per-user multifactor authentication

Bulk update | Got feedback?

Users **Service settings**

App passwords [Learn more](#)

☒ Allow users to create app passwords to sign in to non-browser apps

☐ Do not allow users to create app passwords to sign in to non-browser apps

Trusted IPs [Learn more](#)

Skip multifactor authentication for requests from federated users on my intranet ☐

Skip multifactor authentication for requests from following range of IP address subnets:

Enter IP address

Verification options [Learn more](#)

Authentication methods for MFA and SSPR can now be managed in one converged policy. [Learn more](#)

Methods available to users:

☒ Call to phone

☒ Text message to phone

☒ Notification through mobile app

☒ Verification code from mobile app or hardware token

Remember multifactor authentication on trusted device [Learn more](#)

Conclusion

This showcase highlights my ability to configure and manage Azure IAM features, including RBAC, MFA, and Privileged Identity Management (PIM). My experience extends to managing Azure VMs, implementing secure user lifecycle policies, and working with CyberArk to enhance privileged access controls. I combine these skills with strong certifications to deliver effective identity governance solutions for organizations.