Microsoft ADC Cybersecurity Skilling Program

Week 2 Assignment

Student Name: Vincent Onchieku Collins

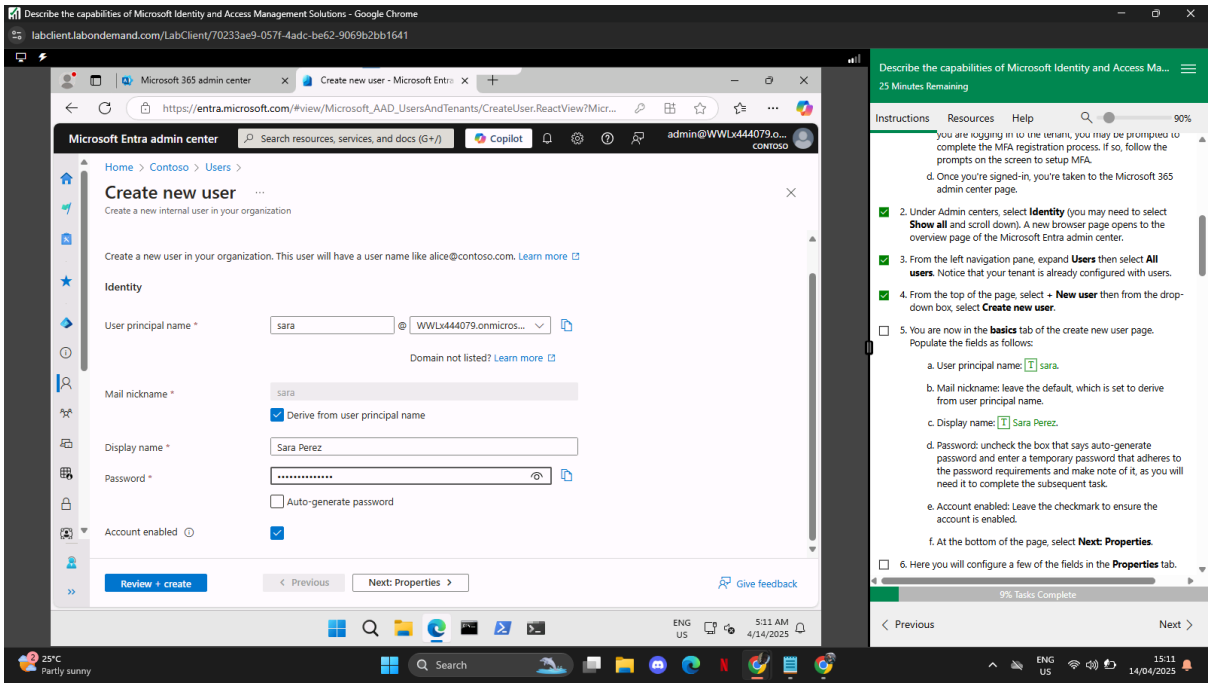
Student ID: ADC-CSS02-25052

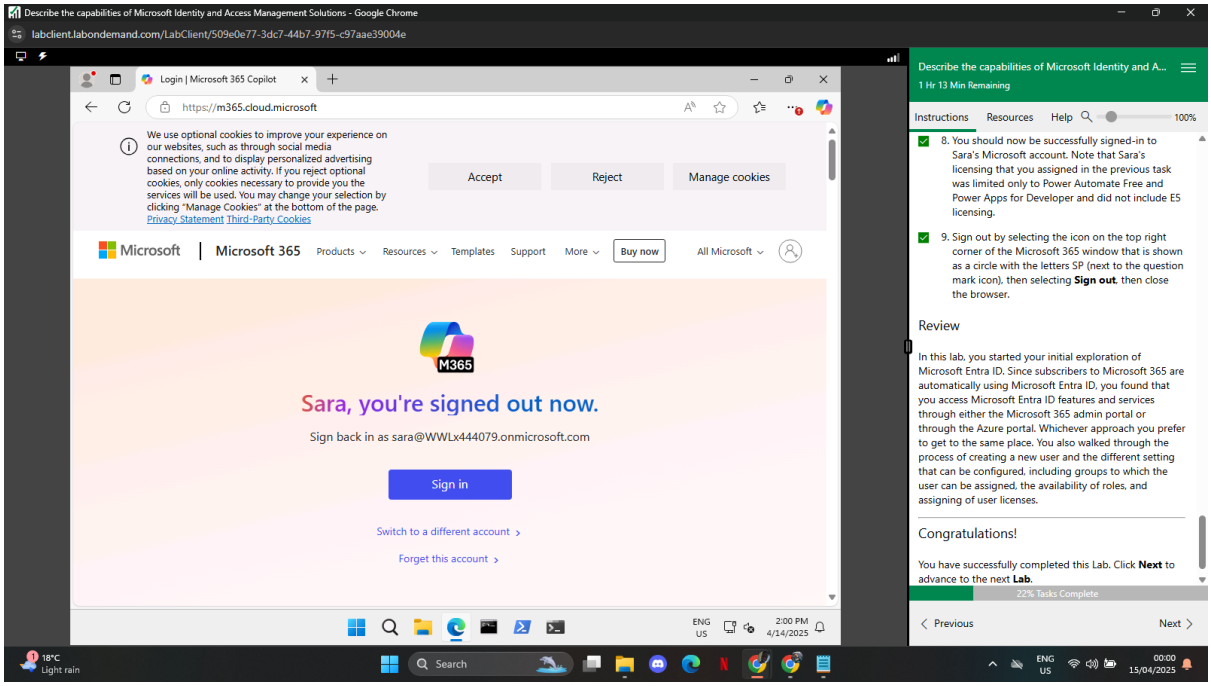
Introduction

The Microsoft Entra ID labs provided a practical and insightful journey into core identity and access management features within Microsoft's cloud environment. Through four sequential lab activities, I gained hands-on experience in configuring user accounts, managing self-service password reset settings, applying conditional access policies, and exploring Privileged Identity Management (PIM). These labs not only deepened my understanding of Microsoft Entra's capabilities but also demonstrated how administrators can efficiently manage identities, secure access, and maintain control over permissions and authentication across the organization.

Lab 1: Explore Microsoft Entra ID User Settings – Completion Summary

In this lab, I explored the Microsoft Entra ID environment through both the Microsoft 365 admin center and the Microsoft Entra admin center. I successfully created a new user account named Sara Perez by configuring her basic details, assigning a group membership (Operations), and reviewing the available directory roles. I ensured the usage location was set correctly, which enabled me to assign licenses in the Microsoft 365 admin portal. I then assigned the Microsoft Power Apps Developer and Microsoft Power Automate Free licenses to the user due to unavailability of the E5 license. After setting up the user, I tested the login process using Sara's credentials, changed the temporary password, and completed multi-factor authentication. This hands-on activity allowed me to familiarize myself with user creation, group management, license assignments, and user sign-in within the Microsoft Entra ID environment, reinforcing the identity and access management capabilities of Microsoft Entra.

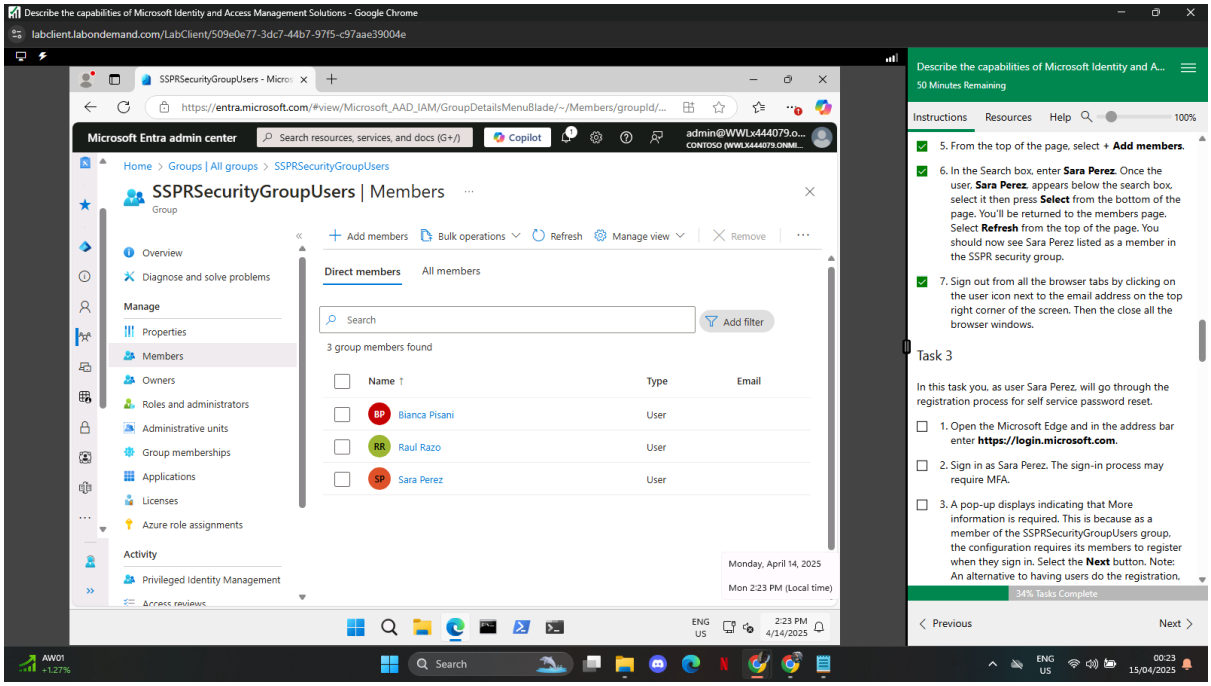


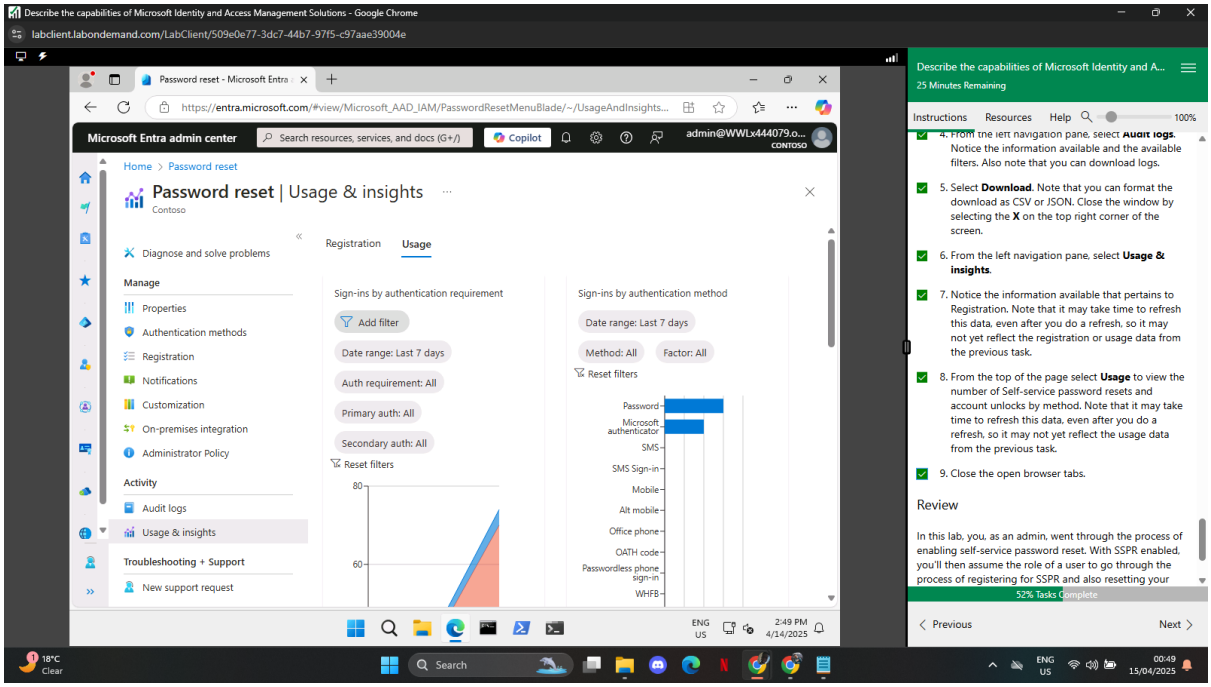


Lab 2: Microsoft Entra self-service password reset

In Lab 2, I explored the self-service password reset (SSPR) capabilities of Microsoft Entra ID. As the administrator, I reviewed the configuration settings for SSPR, including enabling SSPR

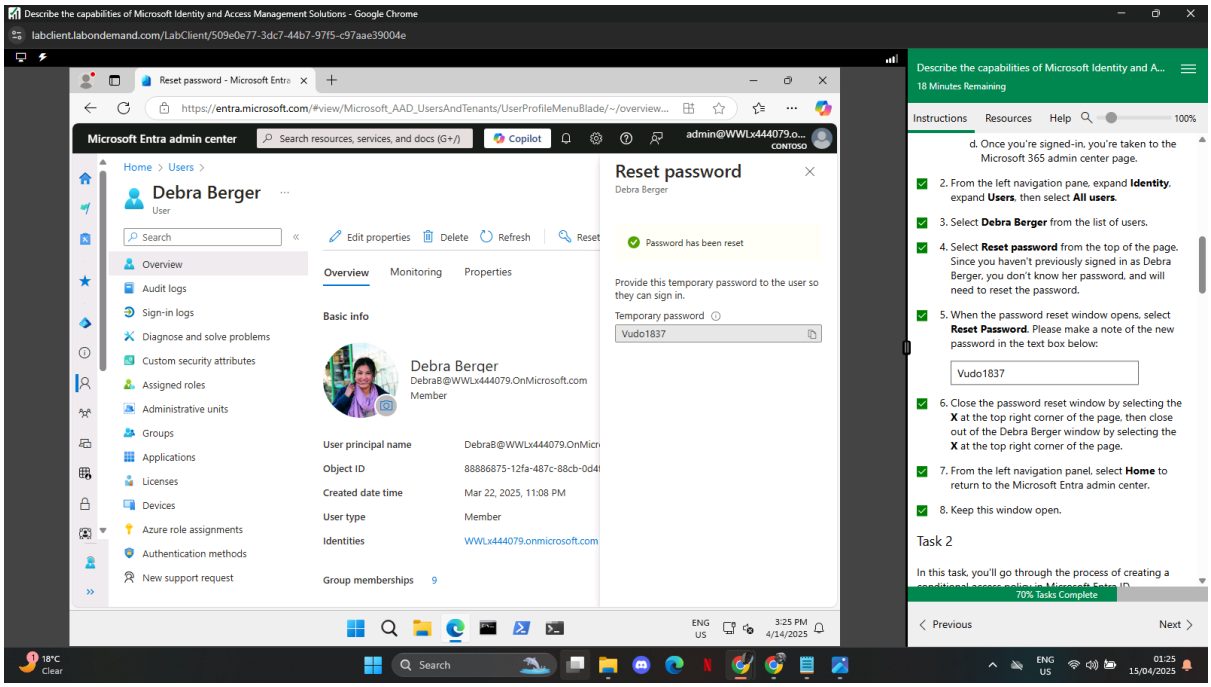
for a specific group SSPRSecurityGroupUsers and adjusting authentication methods, registration settings, and notifications. I then added a user, Sara Perez, to this group. Next, acting as Sara, I registered for SSPR using the Microsoft Authenticator app and completed the process of resetting her password. Finally, I returned to the admin role to view audit logs and usage insights, gaining visibility into SSPR activity and verifying the system's logging capabilities.

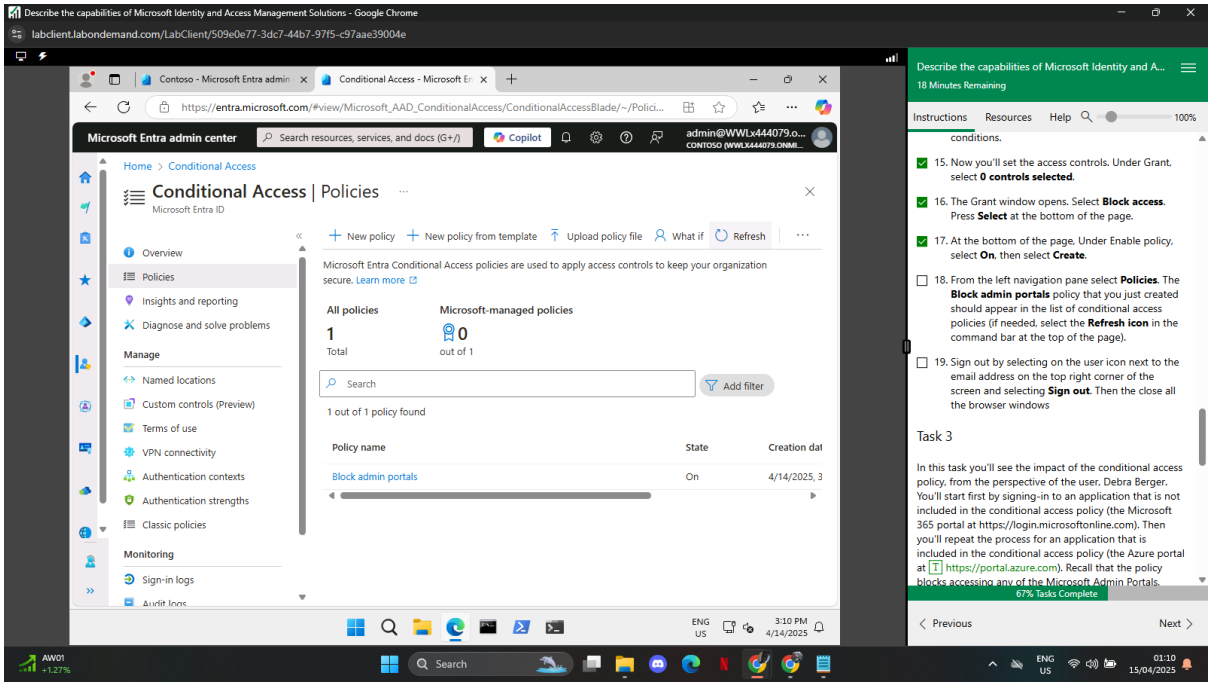


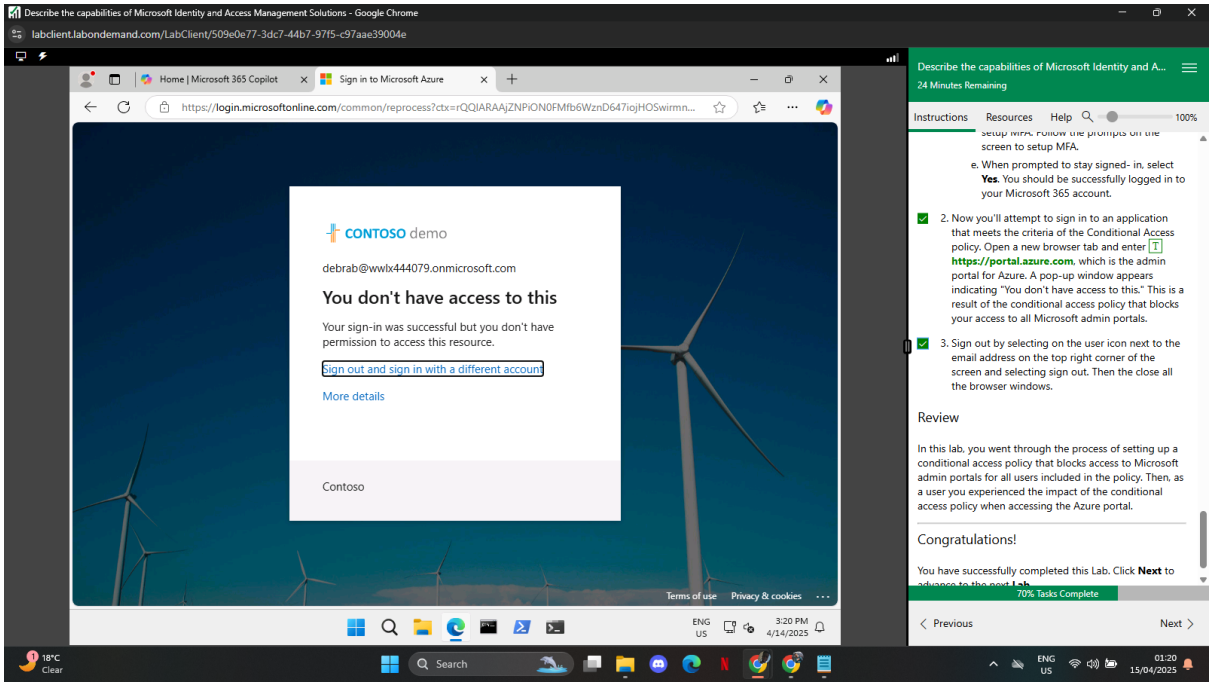


Lab 3: Microsoft Entra Conditional Access

In Lab 3: Microsoft Entra Conditional Access, I explored the functionality of Conditional Access policies within Microsoft Entra, focusing on Multi-Factor Authentication (MFA). As an administrator, I reset the password for user Debra Berger and created a Conditional Access policy that blocks access to Microsoft Admin portals, applying the policy specifically to Debra. I then signed in as Debra to experience the user impact of the policy. While I was able to access the Microsoft 365 portal, I was blocked from accessing the Azure portal due to the Conditional Access rule. This lab provided hands-on experience in managing and enforcing access controls based on user and application context.

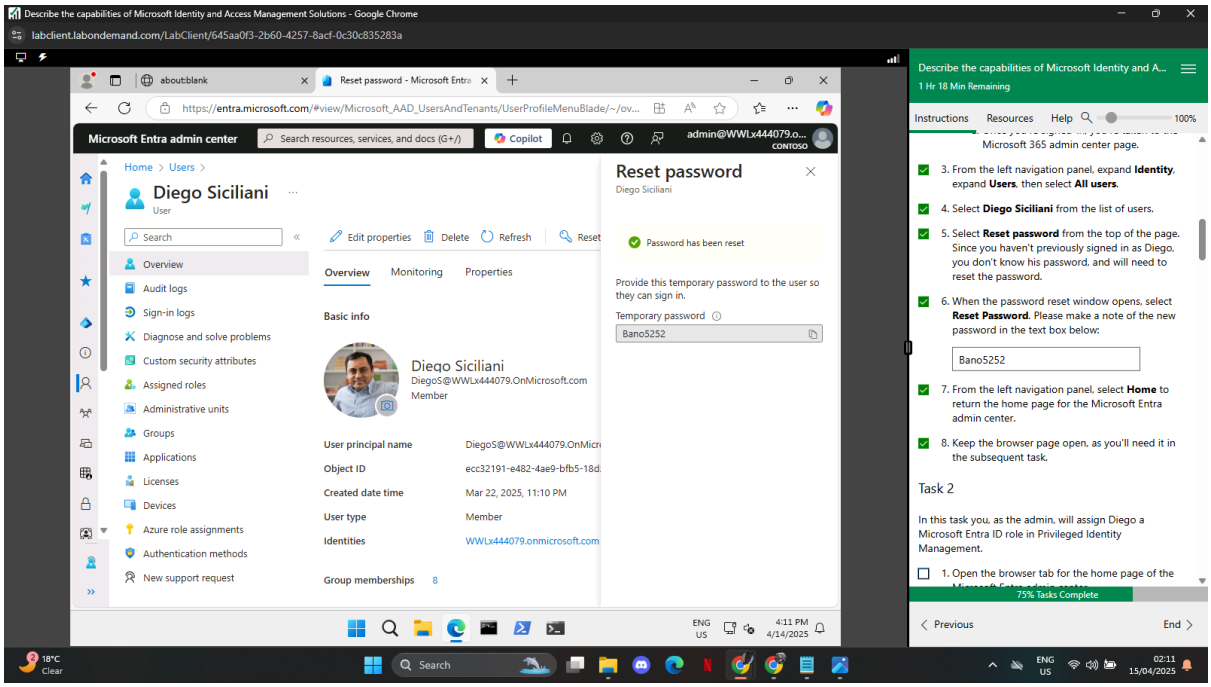

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/509e0e77-3dc7-44b7-97f5-c97aae39004e
Reset password - Microsoft Entra
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/overview...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
admin@WWLx444079.o...
CONTOSO
Home > Users >
Debra Berger
User
Edit properties
Delete
Refresh
Reset
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request
Overview
Monitoring
Properties
Basic info
Debra Berger
DebraB@WWLx444079.OnMicrosoft.com
Member
User principal name
Object ID
Created date time
Mar 22, 2025, 11:08 PM
User type
Member
Identities
WWLx444079.onmicrosoft.com
Group memberships
9
Reset password
Debra Berger
Password has been reset
Provide this temporary password to the user so they can sign in.
Temporary password
Vudo1837
Describe the capabilities of Microsoft Identity and A...
18 Minutes Remaining
Instructions
Resources
Help
100%
d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.
2. From the left navigation pane, expand Identity, expand Users, then select All users.
3. Select Debra Berger from the list of users.
4. Select Reset password from the top of the page. Since you haven't previously signed in as Debra Berger, you don't know her password, and will need to reset the password.
5. When the password reset window opens, select Reset Password. Please make a note of the new password in the text box below:
Vudo1837
6. Close the password reset window by selecting the X at the top right corner of the page, then close out of the Debra Berger window by selecting the X at the top right corner of the page.
7. From the left navigation panel, select Home to return to the Microsoft Entra admin center.
8. Keep this window open.
Task 2
In this task, you'll go through the process of creating a
70% Tasks Complete
Previous
Next
18°C
Clear
Search
ENG
US
3:25 PM
4/14/2025
01:25
15/04/2025

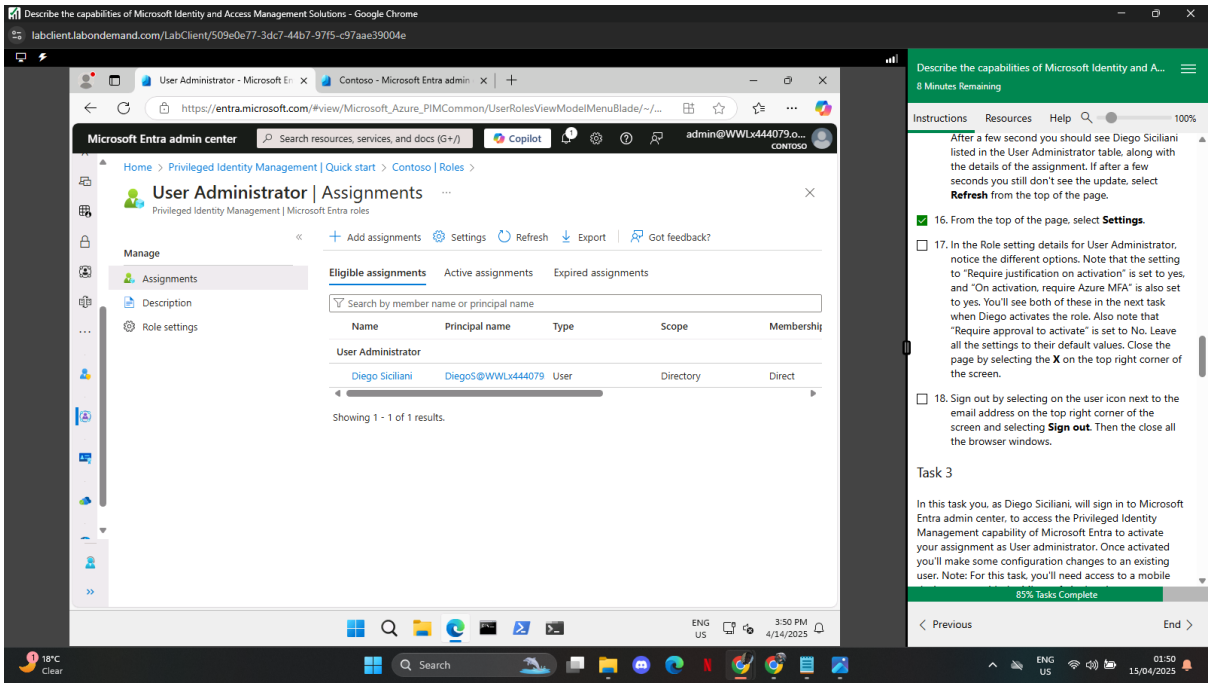

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/509e0e77-3dc7-44b7-97f5-c97aae39004e
Contoso - Microsoft Entra admin
Conditional Access - Microsoft Entra
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Polici...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
admin@WWLx444079.o...
CONTOSO (WWLX444079.ONMI...
Home > Conditional Access
Conditional Access | Policies
Microsoft Entra ID
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
New policy
New policy from template
Upload policy file
What if
Refresh
Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more
All policies
1
Total
Microsoft-managed policies
0
out of 1
Search
Add filter
1 out of 1 policy found
Policy name
State
Creation dat
Block admin portals
On
4/14/2025, 3
Describe the capabilities of Microsoft Identity and A...
18 Minutes Remaining
Instructions
Resources
Help
100%
conditions.
15. Now you'll set the access controls. Under Grant, select 0 controls selected.
16. The Grant window opens. Select Block access. Press Select at the bottom of the page.
17. At the bottom of the page. Under Enable policy, select On, then select Create.
18. From the left navigation pane select Policies. The Block admin portals policy that you just created should appear in the list of conditional access policies (if needed, select the Refresh icon in the command bar at the top of the page).
19. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting Sign out. Then the close all the browser windows
Task 3
In this task you'll see the impact of the conditional access policy, from the perspective of the user, Debra Berger. You'll start first by signing-in to an application that is not included in the conditional access policy (the Microsoft 365 portal at https://login.microsoftonline.com). Then you'll repeat the process for an application that is included in the conditional access policy (the Azure portal at https://portal.azure.com). Recall that the policy blocks accessing any of the Microsoft Admin Portals.
67% Tasks Complete
Previous
Next
AW01
+1.27%
Search
ENG
US
3:10 PM
4/14/2025
01:10
15/04/2025



Lab 4: Explore Privileged Identity Management

In this lab, you explored the capabilities of Microsoft Entra Privileged Identity Management (PIM), which requires Entra ID P2 licensing. Acting as the admin, you reset Diego Siciliani's password and assigned him the User Administrator role through PIM with an eligible assignment lasting two hours. You then signed in as Diego, completed MFA setup using Microsoft Authenticator, and activated the role by providing a justification. Once activated, you navigated the Entra admin center and added Bianca Pisani to the "Mark 8 Project Team" group, demonstrating the administrative privileges granted by the role. This lab emphasized temporary privilege elevation and role-based access control with PIM.


Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/645aa0f3-2b60-4257-8acf-0c30c835283a
Microsoft Entra admin center
Diego Siciliani
Reset password
Password has been reset
Bano5252
Describe the capabilities of Microsoft Identity and A...
1 Hr 18 Min Remaining
Instructions
Resources
Help
Task 2
Previous
End
75% Tasks Complete


Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/509e0e77-3dc7-44b7-97f5-c97aae39004e
Microsoft Entra admin center
User Administrator | Assignments
Describe the capabilities of Microsoft Identity and A...
8 Minutes Remaining
Instructions
Resources
Help
Task 3
Previous
End
85% Tasks Complete

Conclusion

Overall, the lab exercises strengthened my proficiency in using Microsoft Entra ID to manage users, enforce security protocols, and apply role-based access controls. Each task reinforced the importance of secure identity management in a modern cloud infrastructure. By completing these labs, I have developed practical skills essential for real-world administration of Microsoft Entra ID, contributing to better security posture and operational efficiency in any cloud-enabled enterprise environment.