



# **LAB REPORT [WEEK #2]**

**BY**

**EMMANUEL MUTURIA™**

**ADMISSION NUMBER**  
**[ADC-SE02-25011]**

## TABLE OF CONTENTS

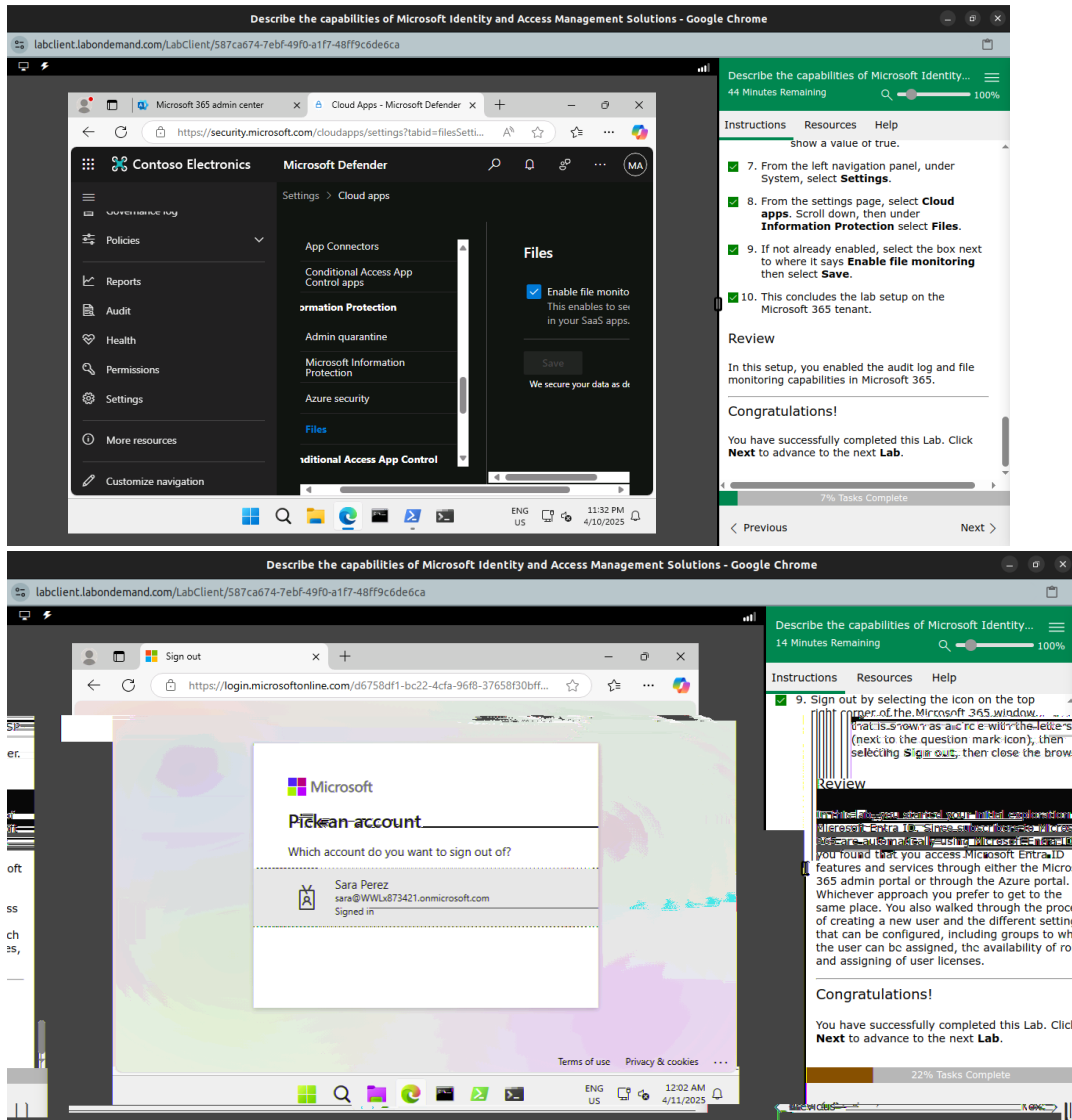
INTRODUCTION.....	
SECTION #1 [Explore Microsoft Entra ID User Settings].....	
SECTION #2 [Microsoft Entra self-service password reset].....	
SECTION #3 [Microsoft Entra Conditional Access].....	
SECTION #4 [Explore Privileged Identity Management].....	
CONCLUSION.....	
REFERENCES.....	



## **INTRODUCTION**

This report documents my continuation of the SC-900 Lab 1: Microsoft Identity and Access Management Solutions Lab as required by the Cyber Shujaa Program [Security Engineer Track]. It contains screenshots and links to the badges to prove the completion of the learning path's modules.

## SECTION #1 [Explore Microsoft Entra ID User Settings]



The image displays two screenshots from a lab environment titled "Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome".

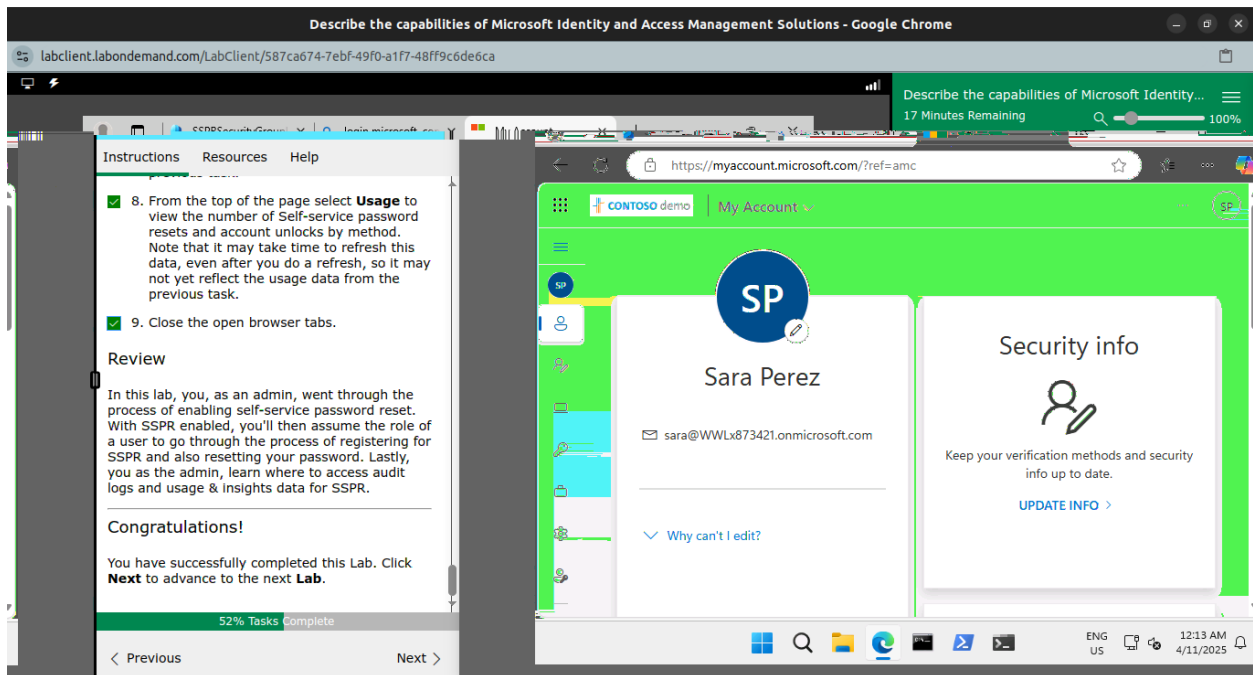
The top screenshot shows the Microsoft Defender console in the Microsoft 365 admin center. The left navigation pane includes sections like Policies, Reports, Audit, Health, Permissions, Settings, and More resources. The main content area is titled "Microsoft Defender" and shows settings for "Cloud apps". Under "Files", the "Enable file monitoring" checkbox is checked, with a note: "This enables file monitoring in your SaaS apps." A "Save" button is visible at the bottom of the Files section.

The bottom screenshot shows a Microsoft sign-out prompt. The prompt asks "Which account do you want to sign out of?" and lists the account "Sara Perez" with email "sara@WWLx873421.onmicrosoft.com" and status "Signed in". The prompt also includes links for "Terms of use" and "Privacy & cookies".

Both screenshots include a sidebar on the right with instructions, resources, and help. The top screenshot's sidebar shows steps 7 through 10, and the bottom screenshot's sidebar shows step 9. Both sidebars also include a "Review" section with a "Congratulations!" message and a "Next" button to advance to the next lab.

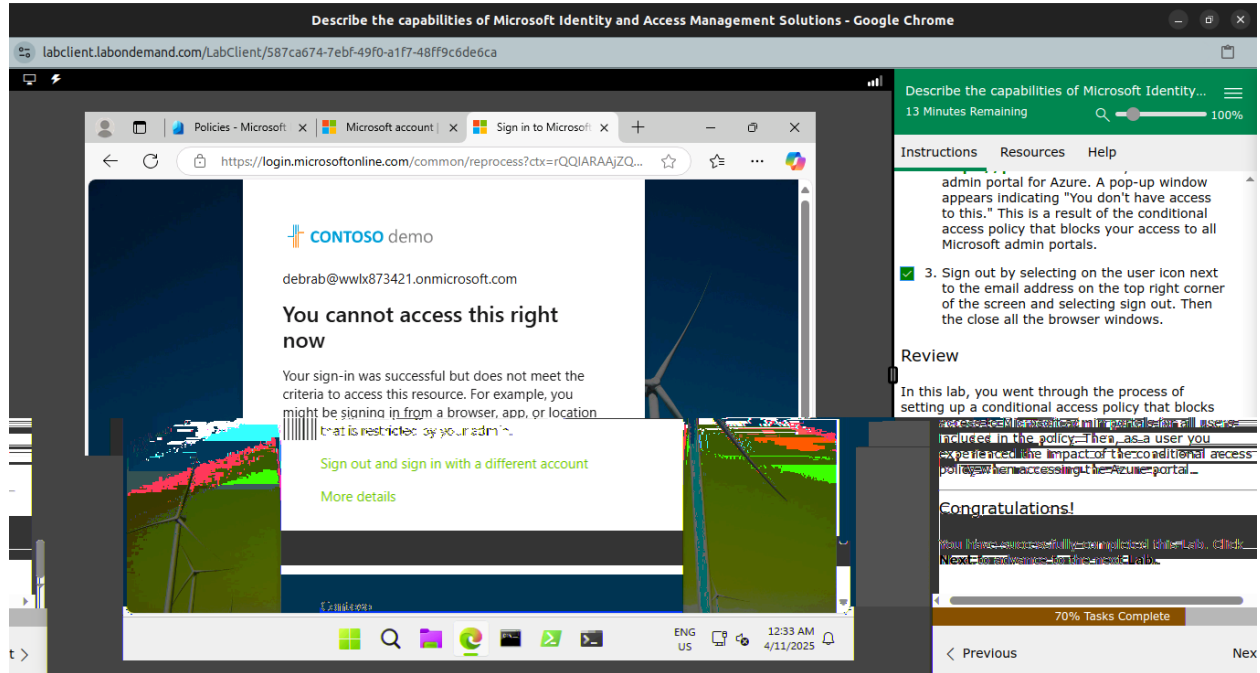
This lab helped solidify: The Capabilities of Microsoft Entra, The Function and Identity Types of Entra ID, and The Types of Identities by accessing Microsoft Entra ID and creating a user and configuring the different settings, including adding licenses.

## SECTION #2 [Microsoft Entra self-service password reset]



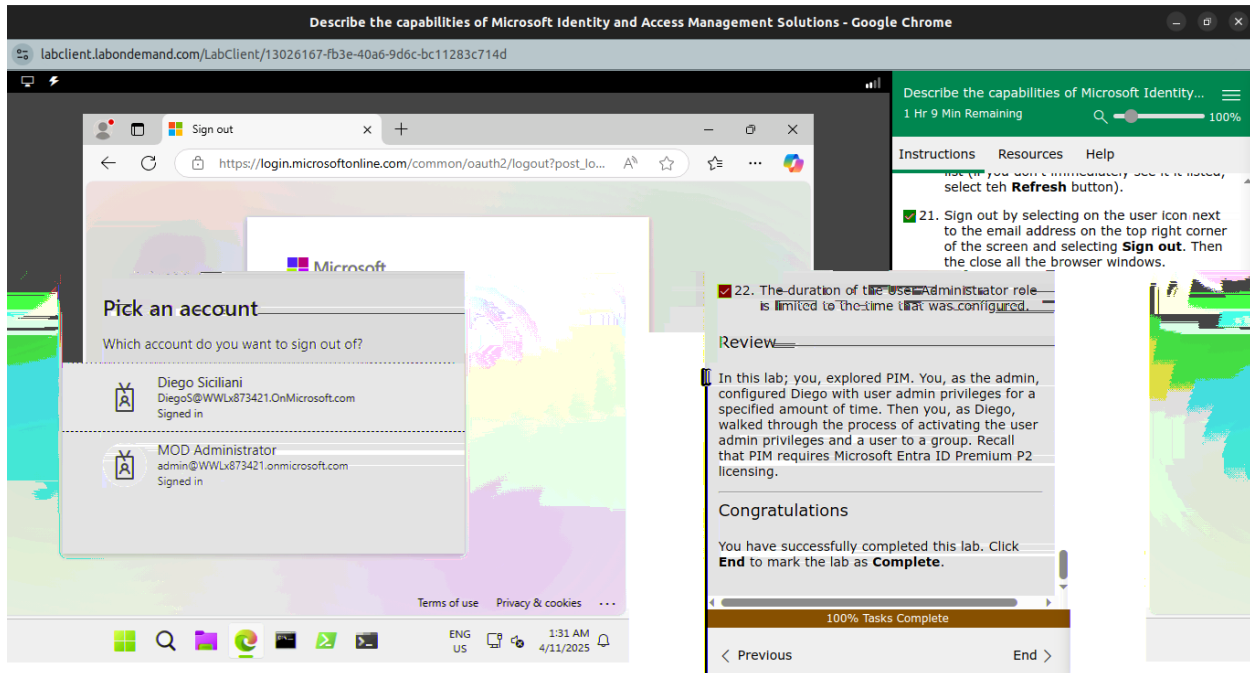
This lab helped solidify: The Capabilities of Microsoft Entra, The Function and Identity Types of Entra ID, and The Types of Identities by adding a user to the SSPR security group and also assuming the role of a user and going through the process of registering for SSPR and also resetting the user's password, and finally viewing audit logs and usage data & insights for SSPR as the admin.

## SECTION #3 [Microsoft Entra Conditional Access]



This lab helped solidify: The Capabilities of Microsoft Entra, The Access Management Capabilities of Microsoft Entra, and Conditional Access by exploring conditional access MFA, from the perspective of an admin and a user. The Admin role helped demonstrate how to create a policy that will require a user to go through Multi-Factor authentication when accessing any of the Microsoft Admin portals. The User role helped visualise the impact of the conditional access policy, including the process of registering for MFA.

## SECTION #4 [Explore Privileged Identity Management]



This lab helped solidify: The Capabilities of Microsoft Entra, The Identity Protection and Governance Capabilities of Microsoft Entra, and The Capabilities of Privileged Identity Management by using the Admin role to configure one of the users, Diego Siciliani, with a Microsoft Entra user administrator role, through Privileged ID management (PIM). With User Admin privileges, Diego created users and groups manage licenses, and more. Both the Admin and the User, Diego, were configured for Microsoft Entra ID P2 licensing.

## CONCLUSION

This report has provided my chronological summary and documentation of the SC-900 Lab 1: Microsoft Identity and Access Management Solutions Lab. It has also included relevant resources that prove the same and serve as a testament to the satisfaction of Week #2's learning requirements as a prerequisite to the following lessons.



## REFERENCES

*Login - Skillable TMS.* (2024). Learnondemand.net.

[https://msle.learnondemand.net/Lab/62465?  
instructionSetLang=en&classId=676662](https://msle.learnondemand.net/Lab/62465?instructionSetLang=en&classId=676662)

wwlpublish. (n.d.). *Describe core infrastructure security services in Azure - Training.* Learn.microsoft.com.

[https://learn.microsoft.com/en-us/training/modules/describe-basic-security-  
capabilities-azure/](https://learn.microsoft.com/en-us/training/modules/describe-basic-security-capabilities-azure/)

wwlpublish. (2025). *Describe the security management capabilities in Azure - Training.* Microsoft.com.

[https://learn.microsoft.com/en-us/training/modules/describe-security-  
management-capabilities-of-azure/](https://learn.microsoft.com/en-us/training/modules/describe-security-management-capabilities-of-azure/)

wwlpublish. (2025). *Describe the capabilities in Microsoft Sentinel - Training.*

Microsoft.com. [https://learn.microsoft.com/en-us/training/modules/describe-  
security-capabilities-of-azure-sentinel/](https://learn.microsoft.com/en-us/training/modules/describe-security-capabilities-of-azure-sentinel/)

wwlpublish. (2025). *Describe threat protection with Microsoft Defender XDR - Training.* Microsoft.com.

[https://learn.microsoft.com/en-us/training/modules/describe-threat-  
protection-with-microsoft-365-defender/](https://learn.microsoft.com/en-us/training/modules/describe-threat-protection-with-microsoft-365-defender/)