

# Cyber Shujaa

## Cloud Security Specialist

### Assignment 3: Lab on Microsoft Identity and Access Management Solutions

**NAME: WELDON KIPKIRUI KENEI**

**CS NO: ADC-CSS02-25027**

# Table of Contents

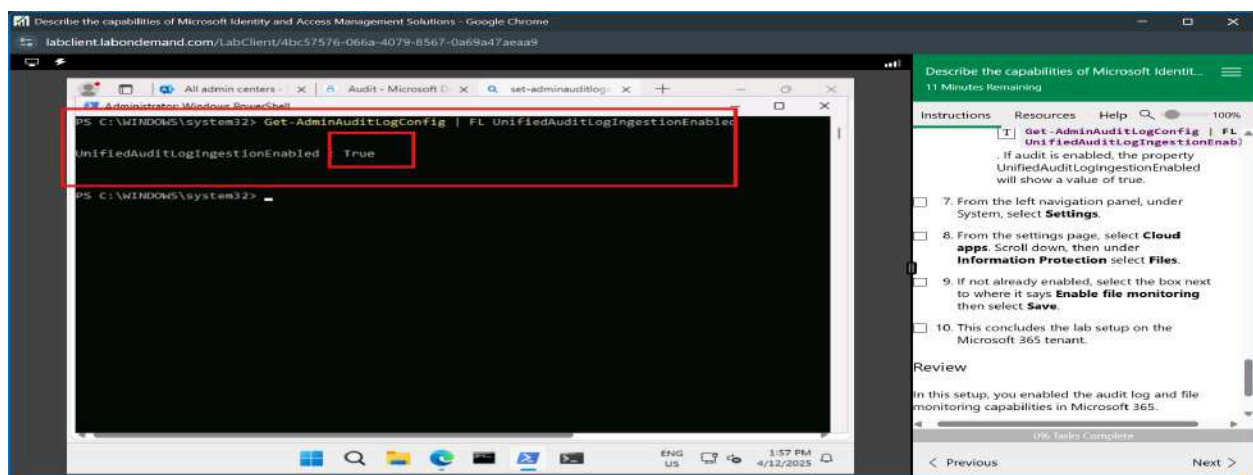
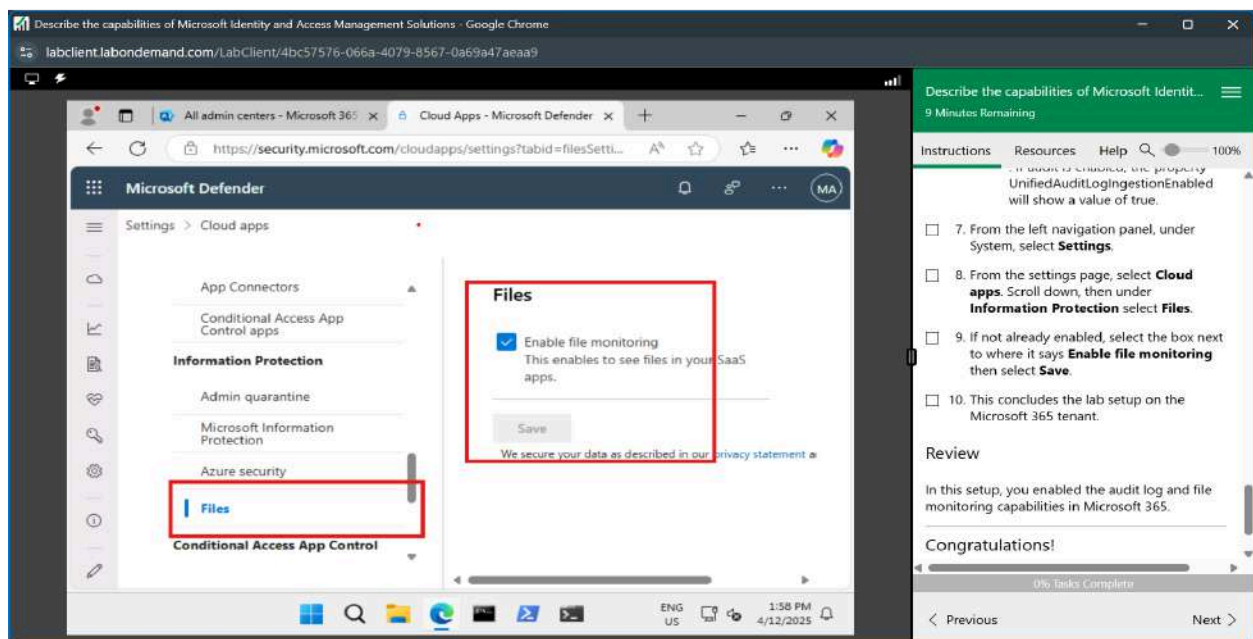
<b>Table of Contents</b>	<b>2</b>
<b>Introduction</b>	<b>3</b>
<b>Setting up the Microsoft 365 tenant</b>	<b>3</b>
<b>Microsoft Entra ID User settings</b>	<b>4</b>
<b>Microsoft Entra Self-Service Password Reset</b>	<b>5</b>
<b>Microsoft Entra Conditional Access</b>	<b>6</b>
<b>Exploring Privileged Identity Management</b>	<b>7</b>
<b>Conclusion</b>	<b>8</b>

# Introduction

In this assignment, we will work on a lab on Microsoft IAM solutions and their capabilities. We will be looking at auditing logs and file monitoring, Microsoft Entra ID user settings, Password reset self-service, conditional access, and privileged identity management.

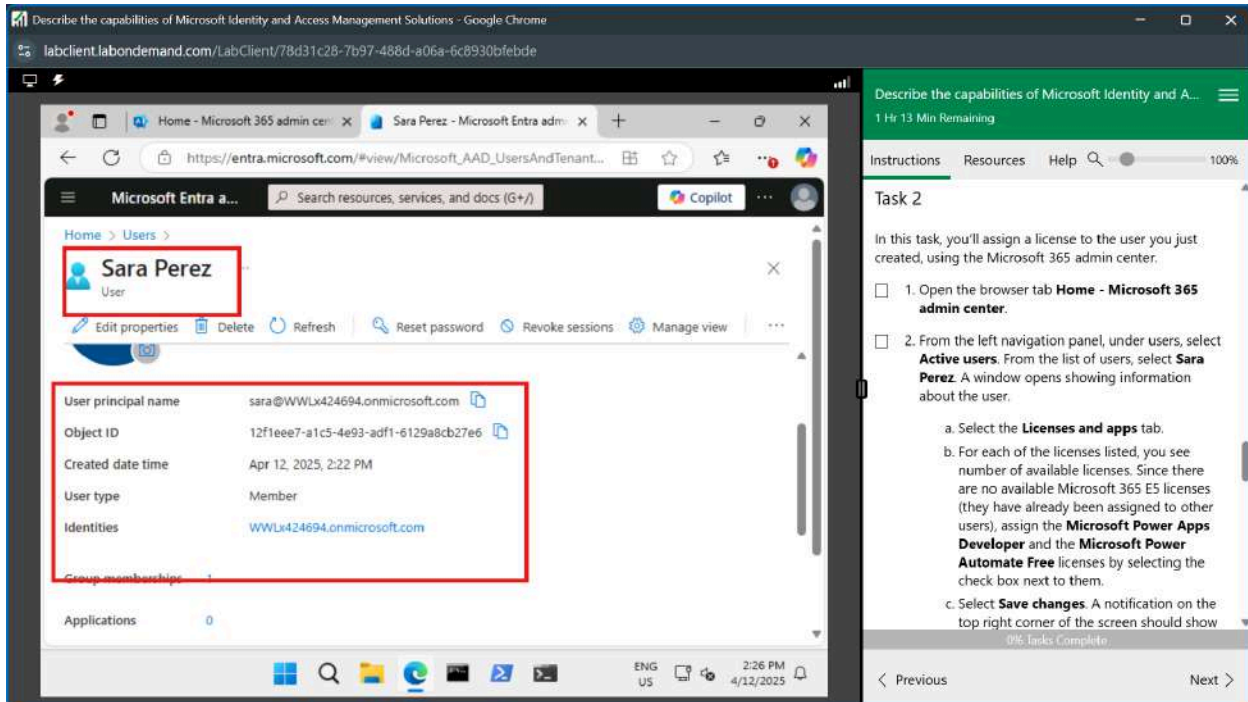
## Setting up the Microsoft 365 tenant

In this step, we configured auditing and file monitoring for the Microsoft 365 tenant, as shown below. We used the PowerShell cli to configure auditing and the GUI to configure file monitoring.



# Microsoft Entra ID User settings

In this lab, we will utilize Ms Entra ID to create a user and assign them groups, roles, and licenses. In task 1 of this lab, we created a user with attributes as shown in the screenshot below.

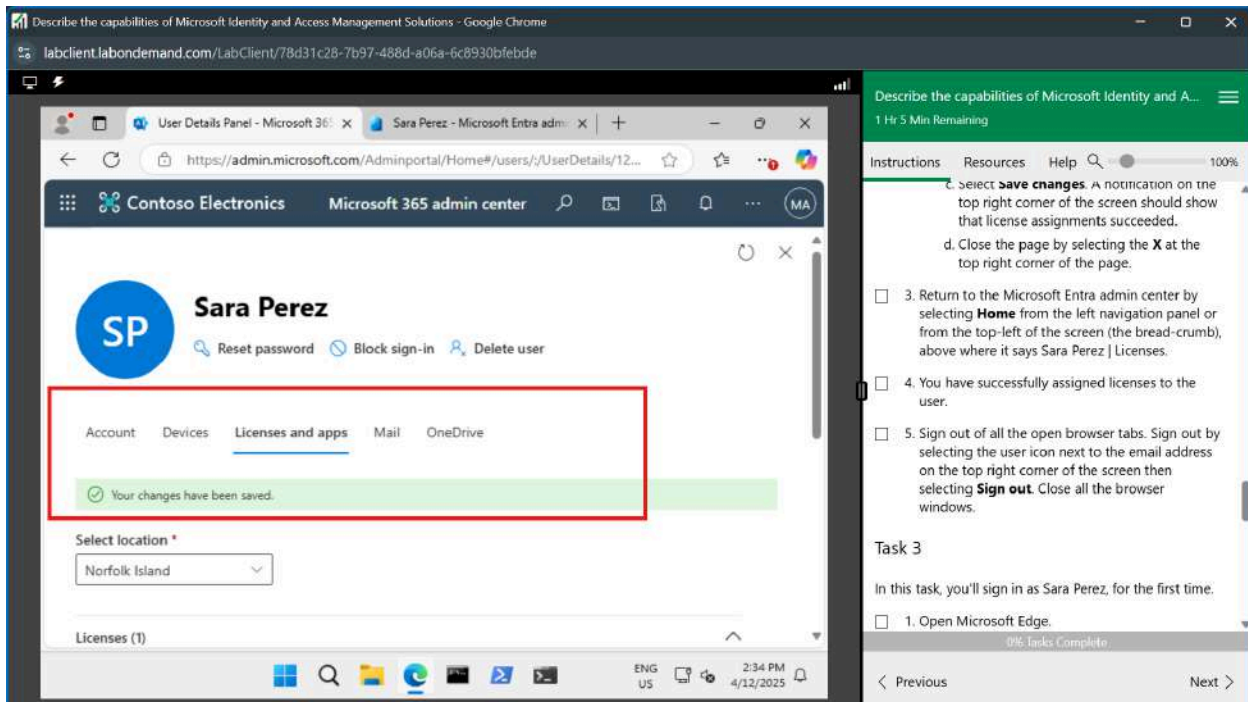


The screenshot shows the Microsoft Entra admin center interface. The user profile for Sara Perez is displayed, with the following details highlighted in a red box:

- User principal name: sara@WWLx424694.onmicrosoft.com
- Object ID: 12f1eee7-a1c5-4e93-adf1-6129a8cb27e6
- Created date time: Apr 12, 2025, 2:22 PM
- User type: Member
- Identities: WWLx424694.onmicrosoft.com

Other visible details include the user's email address (sara.perez@contoso.com), phone number, and a list of applications (currently empty). The interface also shows navigation options like 'Edit properties', 'Delete', 'Refresh', 'Reset password', 'Revoke sessions', and 'Manage view'.

In the next task, we assigned the user a license, as shown below;



The screenshot shows the Microsoft 365 admin center interface. The user profile for Sara Perez is displayed, with the 'Licenses and apps' tab selected. The following details are highlighted in a red box:

- Account: Devices
- Licenses and apps: Your changes have been saved.
- Select location: Norfolk Island

Other visible details include the user's email address (sara.perez@contoso.com), phone number, and a list of licenses (currently empty). The interface also shows navigation options like 'Reset password', 'Block sign-in', and 'Delete user'.

# Microsoft Entra Self-Service Password Reset

In this lab, we will walk through the process of assigning a user to a self-service password reset security group that is part of the Microsoft 365 tenant. We will also view the audit log for the activities relating to SSPR.

The screenshot displays the Microsoft Entra admin center interface. The top navigation bar shows the 'Members' page for the 'SSPRSecurityGroupUsers' group. The 'Members' table lists three users: Bianca Pisani, Raul Razo, and Sara Perez. Sara Perez is highlighted with a red box. The right sidebar shows the 'Lab: Microsoft Entra Conditional Access' page, which includes instructions, resources, and a lab scenario. The bottom section of the screenshot shows the 'Password reset' page, which displays a table of audit logs for the 'Self-service Password Management' service. The table is filtered by 'Date range: Last 1 month' and 'Service: Self-service Password Management'. The table has four columns: Date, Service, Category, and Activity. The data shows three entries for 'Self-service Password Management' on 4/12/25, all categorized as 'UserManagement' and 'Reset password (sel)'. The first entry is highlighted with a red box.

Members - Microsoft Entra admin center

SSPRSecurityGroupUsers

Members

Name	Type	Email
Bianca Pisani	User	
Raul Razo	User	
Sara Perez	User	

Lab: Microsoft Entra Conditional Access

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft Entra
- Module: Describe access management capabilities of Microsoft Entra
- Unit: Describe Conditional Access

Lab scenario

In this lab, you'll explore conditional access MFA, from the perspective of an admin and a user. As the admin, you will create a policy that will require a user to go through multi-factor authentication when accessing any of...

100% tasks Complete

Previous Next

Password reset - Microsoft Entra admin center

Want to switch back to the legacy audit logs experience? Click here to leave the preview.

Download Export Data Settings Refresh Manage view Got feedback?

Show dates as: Local Date range: Last 1 month Service: Self-service Password Management

Category: All Activity: All

Reset filters

Directory Custom Security

Date	Service	Category	Activity
4/12/25, 3:19:56 PM	Self-service Password M...	UserManagement	Reset password (sel)
4/12/25, 3:19:53 PM	Self-service Password M...	UserManagement	Self-service passwoi
4/12/25, 3:19:18 PM	Self-service Password M...	UserManagement	Self-service passwoi

14 Minutes Remaining

Instructions Resources Help

Also note that you can download logs.

5. Select **Download**. Note that you can format the download as CSV or JSON. Close the window by selecting the **X** on the top right corner of the screen.
6. From the left navigation pane, select **Usage & insights**.
7. Notice the information available that pertains to Registration. Note that it may take time to refresh this data, even after you do a refresh, so it may not yet reflect the registration or usage data from the previous task.
8. From the top of the page select **Usage** to view the number of Self-service password resets and account unlocks by method. Note that it may take time to refresh this data, even after you do a refresh, so it may not yet reflect the registration or usage data from the previous task.

100% tasks Complete

Previous Next



# Microsoft Entra Conditional Access

In this lab, we'll explore conditional access MFA from the perspective of an admin and a user. As the admin, we will create a policy requiring a user to use multi-factor authentication when accessing any of the Microsoft Admin portals. From a user perspective, we'll see the impact of the conditional access policy, including the process to register for MFA.

The screenshot shows the Microsoft Entra admin portal interface. The main content area displays the 'Block admin portals' conditional access policy. A red box highlights the policy name and the 'Delete' button. Below the policy name, there are links for 'View policy information' and 'View policy impact (Preview)'. The policy description states: 'Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more'. The 'Name' field contains 'Block admin portals'. The 'Assignments' section shows 'Users' with a link to 'Specific users included'. The 'Target resources' section shows 'https://aka.ms/capolicyhowto'. On the right side, there is a sidebar with instructions for the lab, including steps 15 through 19, and a 'Task 3' section with a progress bar.

The screenshot shows the Microsoft Azure login page. The main content area displays a message from 'CONTOSO demo' stating: 'debrab@wvix424694.onmicrosoft.com You don't have access to this. Your sign-in was successful but you don't have permission to access this resource.' Below the message, there are links for 'Sign out and sign in with a different account' and 'More details'. The 'Contoso' logo is visible at the bottom. On the right side, there is a sidebar with instructions for the lab, including steps 2 and 3, and a 'Review' section. The 'Review' section states: 'In this lab, you went through the process of setting up a conditional access policy that blocks access to Microsoft admin portals for all users included in the policy. Then, as a user you experienced the impact of the conditional access policy when accessing the Azure portal.' Below the review, there is a 'Congratulations!' message and a progress bar.

# Exploring Privileged Identity Management

In this lab, we'll explore some of the basic functionality of Privileged Identity Management (PIM). We will assign a user privileged access as an admin for a while and then walk through how the user activates the assignment role.

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome

labclient.labondemand.com/LabClient/07ce7a46-64b9-47ff-a90e-1f2826444ab2

Microsoft Entra admin center

Home > Privileged Identity Management | Quick start > Contoso | Roles >

**User Administrator | Assignments**

Privileged Identity Management | Microsoft Entra roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	Membership	Start time
<b>User Administrator</b>					
Diego Siciliani	DiegoS@WWLx424694	User	Directory	Direct	4/13/2025

Showing 1 - 1 of 1 results.

ENG US 12:51 PM 4/13/2025

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome

22 Minutes Remaining

Instructions Resources Help 100%

After a few seconds you should see Diego Siciliani listed in the User Administrator table, along with the details of the assignment. If after a few seconds you still don't see the update, select **Refresh** from the top of the page.

16. From the top of the page, select **Settings**.

17. In the Role setting details for User Administrator, notice the different options. Note that the setting to "Require justification on activation" is set to yes, and "On activation, require Azure MFA" is also set to yes. You'll see both of these in the next task when Diego activates the role. Also note that "Require approval to activate" is set to No. Leave all the settings to their default values. Close the page by selecting the **X** on the top right corner of the screen.

18. 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 close all the browser windows.

Task 3

0% Tasks Complete

< Previous End >

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome

labclient.labondemand.com/LabClient/07ce7a46-64b9-47ff-a90e-1f2826444ab2

Microsoft Entra admin center

Home > Privileged Identity Management | My roles >

**My roles | Microsoft Entra roles**

Privileged Identity Management | My roles

Refresh Open in mobile Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

Role	Scope	Membership	End time	Action
User Administrator	Directory	Direct	4/13/2025, 2:46:50 PM	Activate   Extend

ENG US 1:00 PM 4/13/2025

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome

12 Minutes Remaining

Instructions Resources Help 100%

**Management**

5. From the left navigation panel, select **My roles**. You're now seeing information for your eligible assignments. You'll see that you, Diego, are assigned the User administrator role.

6. In the last column of the table, labeled action, select **Activate**.

7. You'll see a warning icon indicating Additional verification required. Select **Click to continue**. Recall that the PIM settings for the User administrator role require multi-factor authentication. Additionally, since Diego's contact information for use with MFA (authentication methods) was not previously configured, he must register his information, to be able to use MFA. Although he will have to do MFA anytime he signs in as a user admin, within the assignment period, the MFA registration process is required only once.

8. The window that appears and the steps that follow are for the Microsoft Authenticator app method.

0% Tasks Complete

< Previous End >

The screenshot shows a web browser window with the URL `msle.learndemand.net/ClassEnrollment/4997666`. At the top, a grey banner states: "Access to your labs will expire on Sunday, August 31, 2025 5:00 PM (UTC)". Below this, a progress bar indicates "25%" completion, with the text "1 of 4 required activities complete" underneath. The section is titled "Hands-on Labs". The first lab, numbered 1, is titled "Describe the capabilities of Microsoft Identity and Access Management Solutions" (Expected Duration 1 hours, 30 minutes). It includes the identifier "SC-900T00-A Microsoft Security, Compliance, and Identity Fundamentals [Cloud Slice Provided], Learning Path 02". The lab status is "Required: Yes", "Status: Complete", "Started: Sunday, April 13, 2025 9:26 PM (E. Africa Standard Time)", and "Ended: Sunday, April 13, 2025 11:09 PM (E. Africa Standard Time)". A blue "Launch" button is present, with the note "6 of 10 launch attempts remaining". A red box highlights the progress bar and the first lab details. A red arrow points down from the first lab to the second lab, which is partially visible at the bottom. The second lab is numbered 2 and titled "Describe the capabilities of Microsoft Security Solutions" (Expected Duration 1 hours, 30 minutes). The URL at the bottom of the browser window is `https://msle.learndemand.net/Lab/62465?instructionSetLang=en&classId=676663`.

## Conclusion

In this lab session, we explored the capabilities of Microsoft Entra ID as part of an access management solution. We have walked through auditing logs and file monitoring, Microsoft Entra ID user settings, Password reset self-service, conditional access, and privileged identity management.