



**NAME:** STEPHEN KYALO -ADC-DP01-25005

**PROGRAM:** DATA PROTECTION SPECIALIST

**CLOUD SLICE TOPIC:** CAPABILITIES OF MICROSOFT IDENTITY AND ACCESS  
MANAGEMENT SOLUTION

## **EXECUTIVE SUMMARY**

The Microsoft Identity and Access Management solution is built around Microsoft Entra, enabling organisations to manage identities, access resources, and enforce policies.

The Microsoft IAM solution cloud slice gives learners hands-on experience in identity management, access management, and tracking of user activities through auditing and file monitoring.

The subsequent topics delve into the various capabilities of Microsoft Entra ID.

## **GLOSSARY**

*IAM* - Identity and Access Management

*ID*- Identity

*IDS* - Identities

*SSPR* - Self-Service Password Reset

*MFA* - Multi-Factor Authentication

**EXECUTIVE SUMMARY..... 2**

**GLOSSARY..... 2**

**1. LAB SETUP..... 3**

**2. AUDIT LOG AND FILE MONITORING..... 5**

**3. MICROSOFT ENTRA ID USER SETTING..... 6**

    3.1. USER ID CREATION..... 6

    3.2. ADDING A USER TO A GROUP..... 6

    3.3. ROLES ASSIGNMENT..... 7

    3.4. LICENSES ASSIGNMENT..... 7

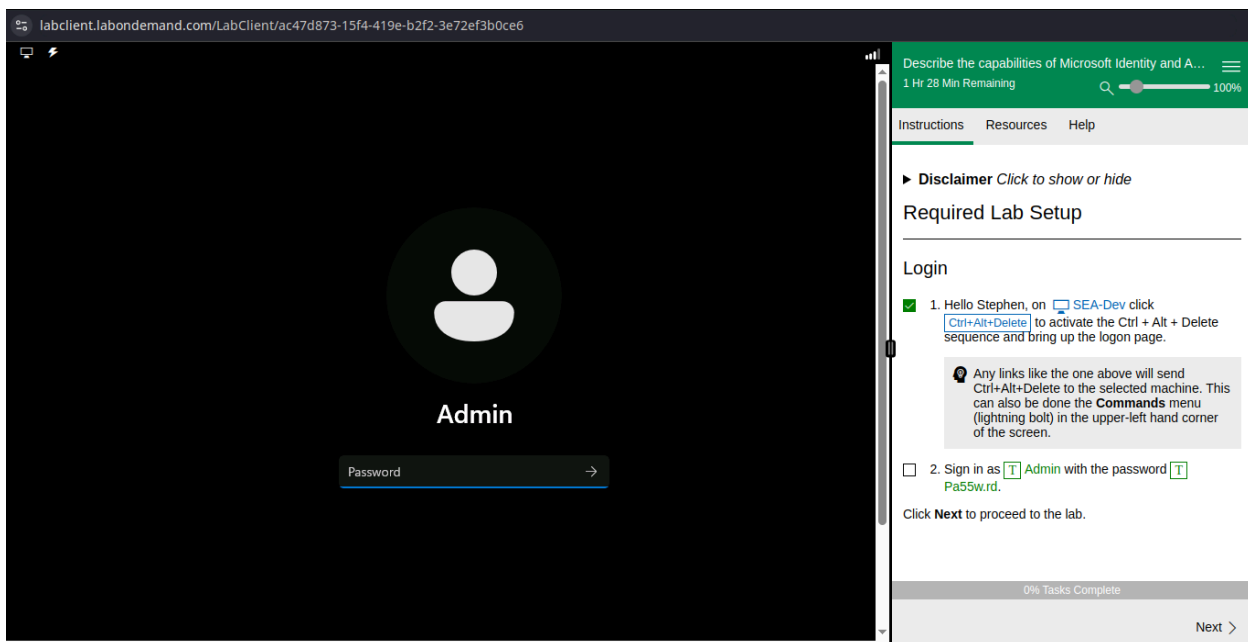
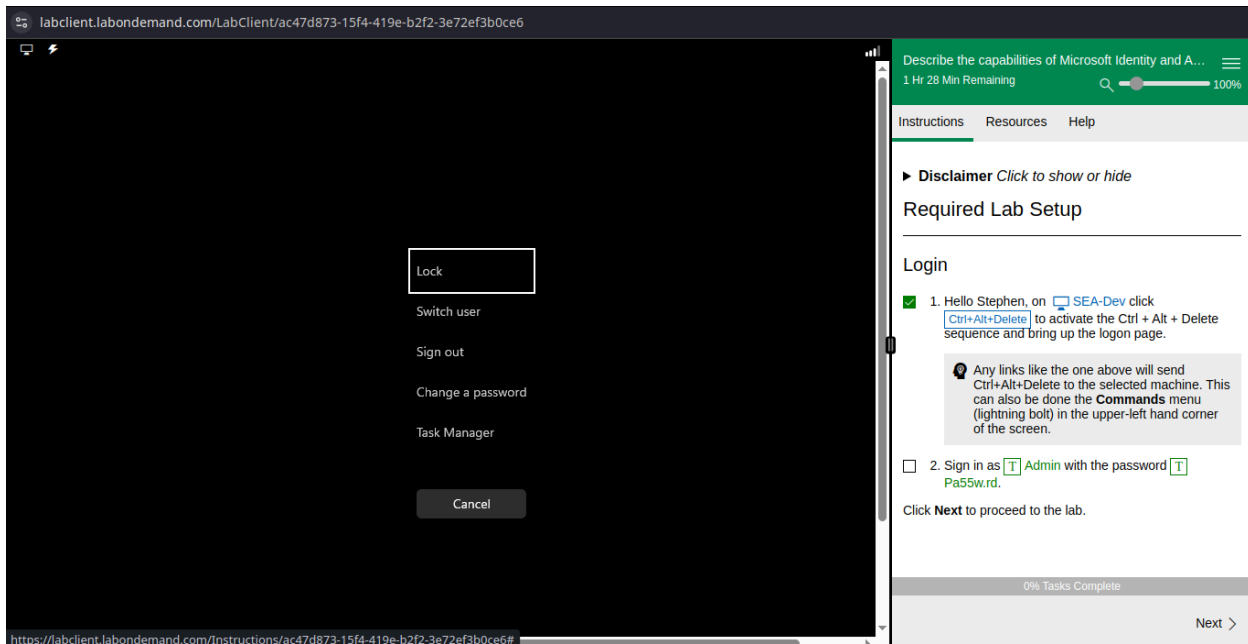
    3.5. SELF-SERVICE PASSWORD RESET..... 8

    3.6. CONDITIONAL ACCESS POLICY..... 9

    3.7. PRIVILEGED IDENTITY MANAGEMENT..... 10

## 1. LAB SETUP

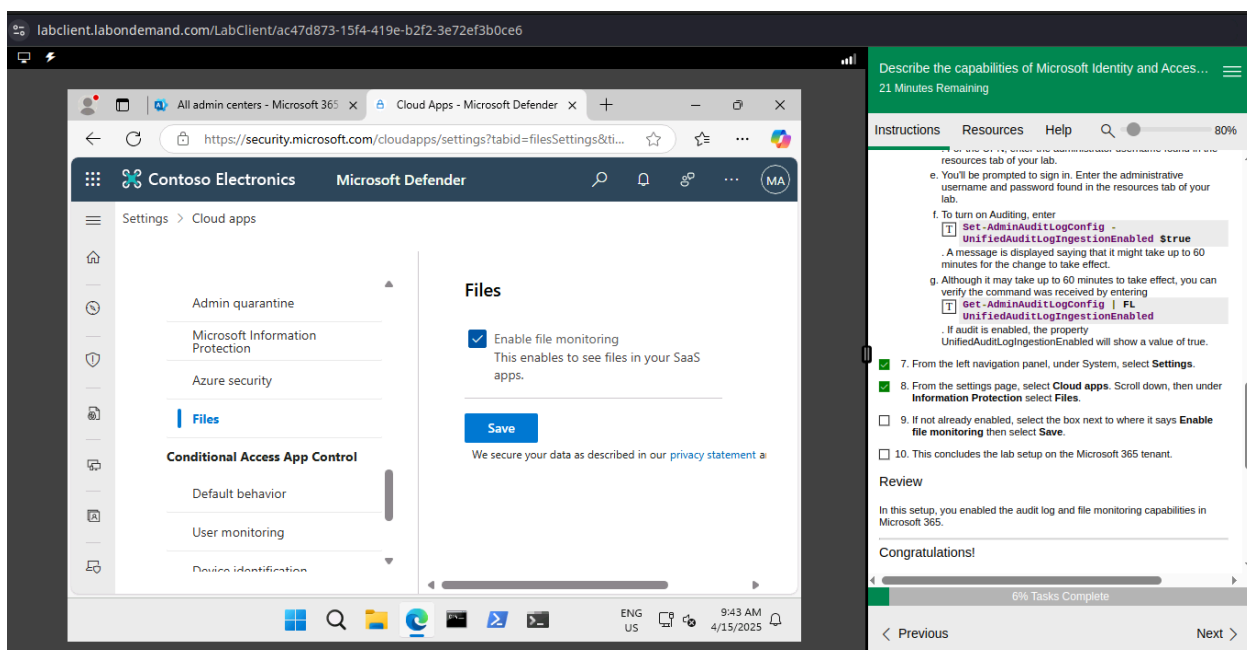
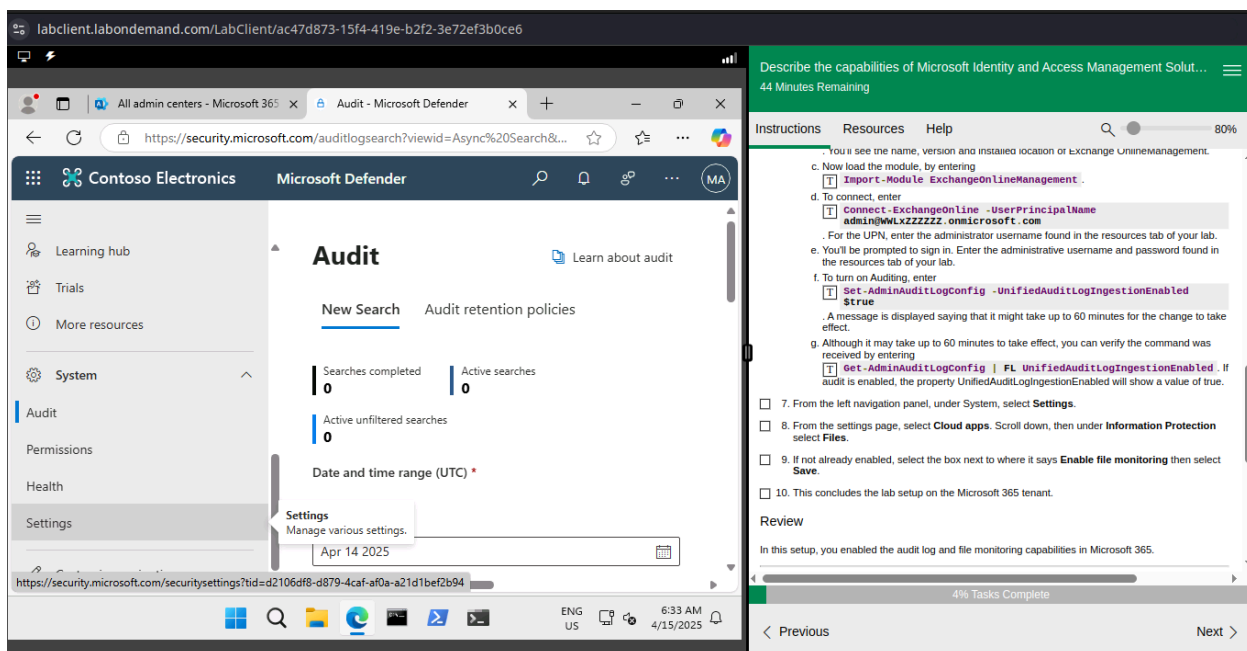
Upon launching the cloud slice, the user is required to log out of the default account and log in with the provided **ADMIN** account and **PASSWORD** as shown on the attached screenshots.



## 2. AUDIT LOG AND FILE MONITORING

Microsoft Entra Audit, when enabled, provides insight into system-related activities and identity changes in your organisation. It helps with monitoring, troubleshooting and compliance auditing.

File monitoring is not natively supported in Microsoft Entra. Through integration with other services such as Microsoft Purview and Defender, Microsoft Entra can indirectly monitor sessions in real-time, detect and alert on sensitive file downloads.



### 3. MICROSOFT ENTRA ID USER SETTING

With Microsoft Entra ID, an Administrator or any user with the proper privileges can create, modify, deactivate or delete user IDs, reset passwords, assign user privileges and roles, add users to groups, and assign licenses.

The administrators can also enforce policies and controls, such as Conditional Access Policy, MFA and Self-Service Password Reset.

#### 3.1. USER ID CREATION

The name of the user is defined as well as the user ID, together with a temporary password that the user will use to log in for the first time before changing it.

The screenshot shows the 'Create new user' page in the Microsoft Entra ID portal. The user principal name is 'sara' with a domain dropdown set to 'WWLX229499.onmicros...'. The mail nickname is 'sara' with the option 'Derive from user principal name' checked. The display name is 'Sara Perez'. The password is masked with dots, and the 'Auto-generate password' option is unchecked. The 'Account enabled' checkbox is checked. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Properties'. To the right, a task list titled 'Describe the capabilities of Microsoft Identity and Acces...' shows progress at 10% with tasks 4 through 6.

#### 3.2. ADDING A USER TO A GROUP

A user can be added to different groups, whether for collaboration with other users or to have access to certain privileges or controls, e.g an SSPR Group. The user Sara Perez is added to the Operations Group.

The screenshot shows the 'Select group' page in the Microsoft Entra ID portal. A search for 'opera' has been performed, resulting in two groups: 'Operations' and 'sg-Operations'. The 'Operations' group is selected. The page includes a 'Select' button at the bottom. To the right, a task list titled 'Describe the capabilities of Microsoft Identity and Acces...' shows progress at 11% with tasks 7 through 9.

### 3.3. ROLES ASSIGNMENT

This allows users to be granted special roles to be able to perform certain duties, in this case, duties related to the directory, such as create, delete or modify user ID. The user Sara Perez is not assigned any roles

The screenshot shows the Microsoft Entra admin center interface. The main pane displays the 'Directory roles' assignment page for user Sara Perez. A search bar is at the top, and a list of roles is shown below. The task pane on the right contains instructions for role assignment, including selecting a group and adding a role.

Role	Description
<input type="checkbox"/> AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.
<input type="checkbox"/> Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.
<input type="checkbox"/> Application Developer	Can create application registrations independent of the 'Users can register applications' setting.
<input type="checkbox"/> Attack Payload Author	Can create attack payloads that an administrator can initiate later.
<input type="checkbox"/> Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.
<input type="checkbox"/> Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.
<input type="checkbox"/> Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.

### 3.4. LICENSES ASSIGNMENT

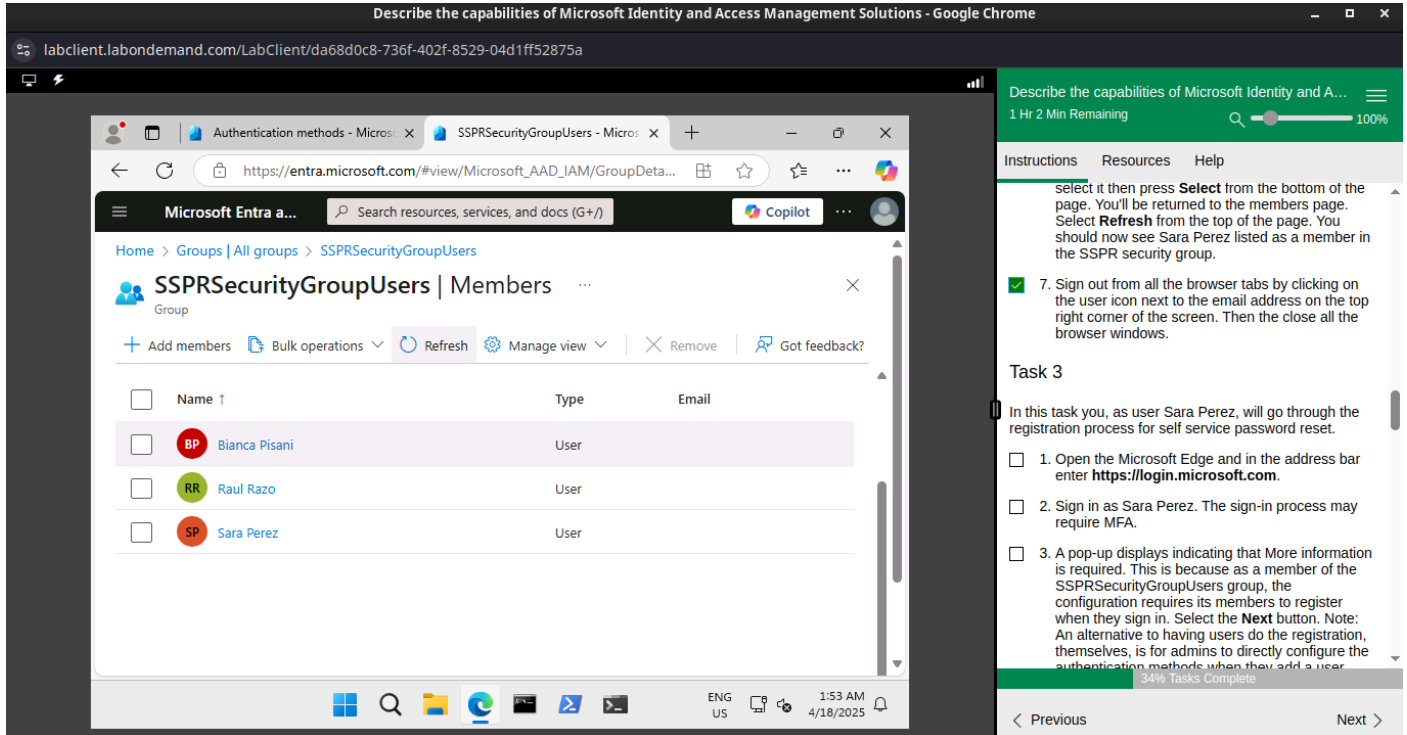
Licenses allow users to access cloud apps associated with the license assigned to them, such as Microsoft Power Apps for developers and Microsoft 365.

The screenshot shows the Microsoft 365 admin center interface. The main pane displays the 'Licenses' assignment page for user Sara Perez. A list of licenses is shown, with 'Microsoft Power Apps for Developer' selected. The task pane on the right contains instructions for license assignment, including selecting a user and assigning a license.

License	Available Licenses
<input type="checkbox"/> Microsoft 365 E5 (no Teams)	You have no more licenses for this trial subscription. You need to <a href="#">buy a subscription</a> before you can assign a license.
<input checked="" type="checkbox"/> Microsoft Power Apps for Developer	9998 of 10000 licenses available
<input type="checkbox"/> Microsoft Teams Enterprise	You have no more licenses for this trial subscription. You need to <a href="#">buy a subscription</a> before you can assign a license.

### 3.5. SELF-SERVICE PASSWORD RESET

This feature enables a user to reset their password without the intervention of the IT Helpdesk. In the cloud slice lab, the user, Sara Perez, is granted this privilege by adding them to the SSPR Security group, enabling them to reset their password.

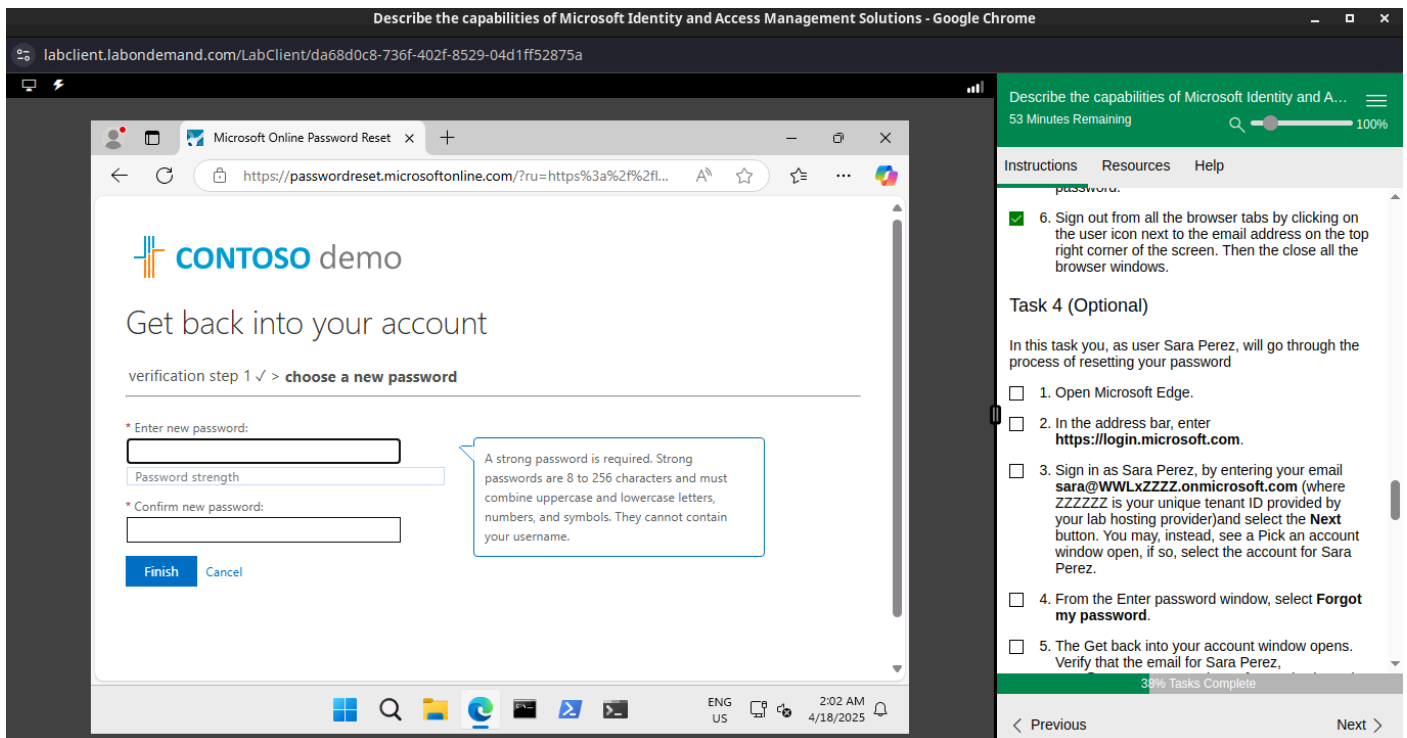


The screenshot shows the Microsoft Entra admin center interface. The main content area displays the 'SSPRSecurityGroupUsers' group with a list of members. The members list includes:

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

On the right side, there is a sidebar with instructions and a task list. The task list includes:

- Task 3: In this task you, as user Sara Perez, will go through the registration process for self service password reset.
- 1. Open the Microsoft Edge and in the address bar enter <https://login.microsoft.com>.
- 2. Sign in as Sara Perez. The sign-in process may require MFA.
- 3. A pop-up displays indicating that More information is required. This is because as a member of the SSPRSecurityGroupUsers group, the configuration requires its members to register when they sign in. Select the **Next** button. Note: An alternative to having users do the registration, themselves, is for admins to directly configure the authentication methods when they add a user.



The screenshot shows the Microsoft Online Password Reset page. The page title is 'CONTOSO demo' and the subtitle is 'Get back into your account'. The verification step is 'verification step 1 > choose a new password'. The page includes a form to enter a new password and a confirmation field. A tooltip indicates that a strong password is required, with details: 'A strong password is required. Strong passwords are 8 to 256 characters and must combine uppercase and lowercase letters, numbers, and symbols. They cannot contain your username.'

On the right side, there is a sidebar with instructions and a task list. The task list includes:

- Task 4 (Optional): In this task you, as user Sara Perez, will go through the process of resetting your password.
- 1. Open Microsoft Edge.
- 2. In the address bar, enter <https://login.microsoft.com>.
- 3. Sign in as Sara Perez, by entering your email [sara@WWLxZZZZ.onmicrosoft.com](mailto:sara@WWLxZZZZ.onmicrosoft.com) (where ZZZZZ is your unique tenant ID provided by your lab hosting provider) and select the **Next** button. You may, instead, see a Pick an account window open, if so, select the account for Sara Perez.
- 4. From the Enter password window, select **Forgot my password**.
- 5. The Get back into your account window opens. Verify that the email for Sara Perez,



### 3.6. CONDITIONAL ACCESS POLICY

This is a rule that automatically applies access controls based on certain conditions- who the user is, where the user is, the network the user is on, the type of device being used and many more.

The screenshot shows the Microsoft Entra admin center interface. The main content area displays the 'New' Conditional Access policy page. The 'Name' field is populated with 'Example: Device compliance app policy'. The 'Assignments' section shows '0 users and groups selected' and 'No target resources selected'. The right sidebar contains a list of instructions for the lab, including steps 2 through 9. The instructions are as follows:

- 2. From the left navigation pane, expand **Protection** then select **Conditional Access**.
- 3. The Conditional access overview page is displayed. When you land on the overview page, the **Getting started** tab is selected (underlined). Select the **Overview** tab. Here you will see tiles showing the Policy summary and general alerts. From the left navigation panel, select **Policies**.
- 4. From the left navigation panel, select **Policies**. Any existing Conditional Access Policies are listed here. Select **+ New policy**.
- 5. In the Name field, enter **Block admin portals**.
- 6. Under Users, select **0 users and groups selected**.
- 7. You'll now see the option to Include or Exclude users or groups. Make sure **Include** is selected (underlined).
- 8. Select the option for **Select users and groups** and select **Users and groups**. The window to Select users and groups opens.
- 9. In the Search bar, enter **Debra**. Select **Debra Berger** from beneath the search bar, then press the **Select** button on the bottom of the page.

The screenshot shows the Azure portal interface with a 'Sign-in failed' error message. The error code is AADSTS53003 and the message states that access has been blocked by Conditional Access policies. The right sidebar contains a list of instructions for the lab, including steps 2 and 3, and a 'Review' section. The instructions are as follows:

- 2. Now you'll attempt to sign in to an application that meets the criteria of the Conditional Access policy. Open a new browser tab and enter **https://portal.azure.com**, which is the admin portal for Azure. A pop-up window appears indicating "You don't have access to this." This is a result of the conditional access policy that blocks your access to all Microsoft admin portals.
- 3. 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.

**Review**

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.

**Congratulations!**

You have successfully completed this Lab. Click **Next** to advance to the next Lab.

In this scenario Conditional Access policy that denies access to the Azure Cloud Portal for certain users is enforced on the user account, Debra Berger, denying them access upon

sign-in.

### 3.7. PRIVILEGED IDENTITY MANAGEMENT

This feature allows a user to be assigned a certain privilege(s) or role for a limited time.

labclient.labondemand.com/LabClient/da68d0c8-736f-402f-8529-04d1ff52875a

Privileged Identity Management | Quick start

Azure Active Directory is becoming Microsoft Entra ID. [Learn more](#)

What's new **Get started**

Manage your privileged access

Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. [Learn more](#)

[https://entra.microsoft.com/#blade/Microsoft\\_Azure\\_PIMCommon/CommonMenuBlade/fromNav/Identity](https://entra.microsoft.com/#blade/Microsoft_Azure_PIMCommon/CommonMenuBlade/fromNav/Identity)

Describe the capabilities of Microsoft Identity and A... 19 Minutes Remaining

Instructions Resources Help

**TASK 2**

In this task you, as the admin, will assign Diego a Microsoft Entra ID role in Privileged Identity Management.

- ☐ 1. Open the browser tab for the home page of the Microsoft Entra admin center.
- ☐ 2. From the left navigation panel, under "Identity", expand **Identity Governance**, then select **Privileged Identity Management**.
- ☐ 3. You are now in the Privileged Identity Management quick start page. Review the information on the Get started page. In the main window, under where it says Manage access, select **Manage**.
- ☐ 4. You're now in the Contoso Roles page. In the search bar, on the top of the page, enter **user**. From the search results, select **User Administrator**.
- ☐ 5. From the top of the page, select **+ Add assignments**.
- ☐ 6. In the Add assignments page, ensure that **Membership** is underlined. Here you'll configure the membership settings for the user administrator role in PIM.

75% Tasks Complete

< Previous End >

*Example:* The user below has been assigned the role of User Administrator for 2 hours, allowing them to create users, modify user details, reset passwords for users, add users to groups and many more.

labclient.labondemand.com/LabClient/da68d0c8-736f-402f-8529-04d1ff52875a

User Administrator | Assignments

+ 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	Status
User Administrator					
Diego Siciliani	DiegoS@WWLx229499	User	Directory	Direct	4/18/2025

Showing 1 - 1 of 1 results.

Describe the capabilities of Microsoft Identity and A... 14 Minutes Remaining

Instructions Resources Help

From the today, so you need to change the year). For the time, set the time to two hours from the current time. After you have set the time field for the time when the Assignment ends, press the tab key on your keyboard and select **Assign** on the bottom of the page.

- ☐ 15. This takes you back the Assignments window. After a few second 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 the close all the browser tabs.

75% Tasks Complete

< Previous End >