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

Table of Contents 2

Introduction 3

Setting up the Microsoft 365 tenant 3

Microsoft Entra ID User settings 4

Microsoft Entra Self-Service Password Reset 5

Microsoft Entra Conditional Access 6

Exploring Privileged Identity Management 7

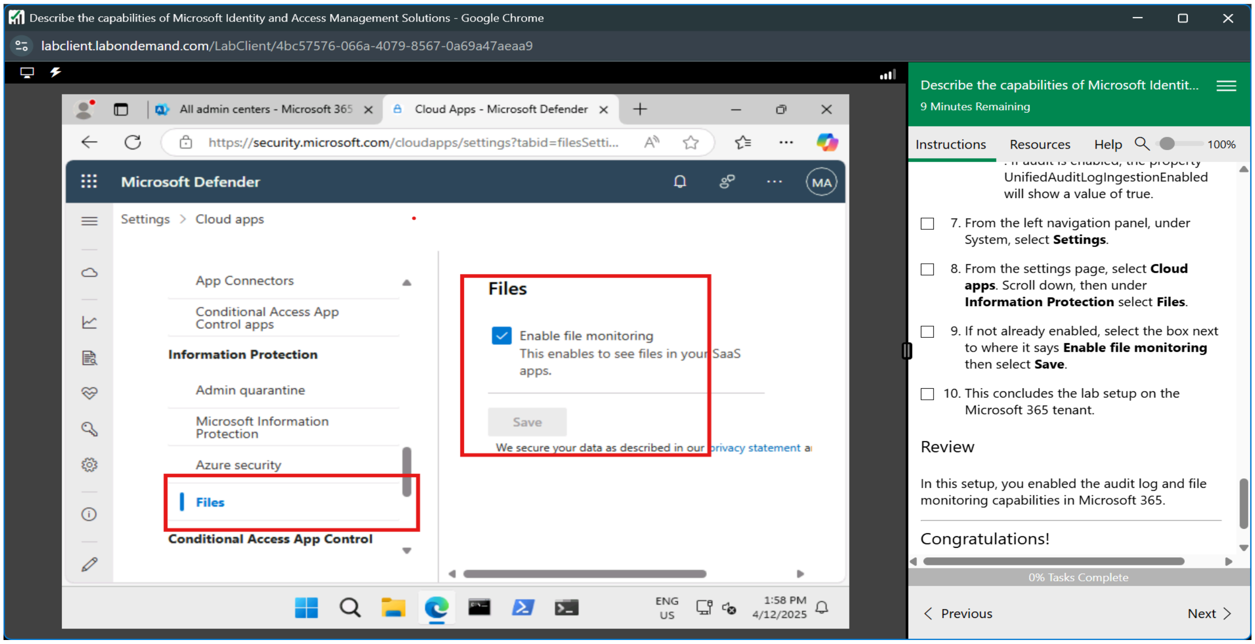
Conclusion 8

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.



Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/4bc57576-066a-4079-8567-0a69a47aeaa9
All admin centers - Microsoft 365
Cloud Apps - Microsoft Defender
https://security.microsoft.com/cloudapps/settings?tabid=filesSetti...
Microsoft Defender
MA
Settings > Cloud apps
App Connectors
Conditional Access App Control apps
Information Protection
Admin quarantine
Microsoft Information Protection
Azure security
Files
Conditional Access App Control
Save
ENG US
1:58 PM 4/12/2025
Describe the capabilities of Microsoft Identit...
9 Minutes Remaining
Instructions
Resources
Help
100%
0% Tasks Complete
Previous
Next

Files

☑ Enable file monitoring
This enables to see files in your SaaS apps.

We secure your data as described in our privacy statement a

. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.

□ 7. From the left navigation panel, under System, select **Settings**.

□ 8. From the settings page, select **Cloud apps**. Scroll down, then under **Information Protection** select **Files**.

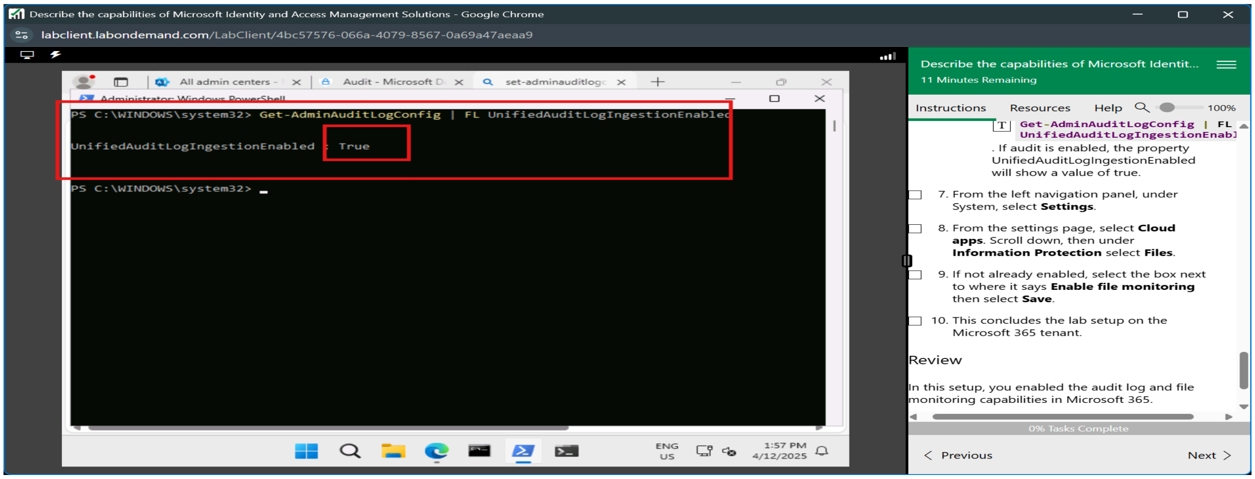
□ 9. If not already enabled, select the box next to where it says **Enable file monitoring** then select **Save**.

□ 10. This concludes the lab setup on the Microsoft 365 tenant.

Review

In this setup, you enabled the audit log and file monitoring capabilities in Microsoft 365.

Congratulations!



Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/4bc57576-066a-4079-8567-0a69a47aeaa9
All admin centers
Audit - Microsoft D
set-adminauditlog
Administrator: Windows PowerShell
ENG US
1:57 PM 4/12/2025
Describe the capabilities of Microsoft Identit...
11 Minutes Remaining
Instructions
Resources
Help
100%
0% Tasks Complete
Previous
Next

```
PS C:\WINDOWS\system32> Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled

UnifiedAuditLogIngestionEnabled : True

PS C:\WINDOWS\system32> _
```

```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabl
```

. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.

□ 7. From the left navigation panel, under System, select **Settings**.

□ 8. From the settings page, select **Cloud apps**. Scroll down, then under **Information Protection** select **Files**.

□ 9. If not already enabled, select the box next to where it says **Enable file monitoring** then select **Save**.

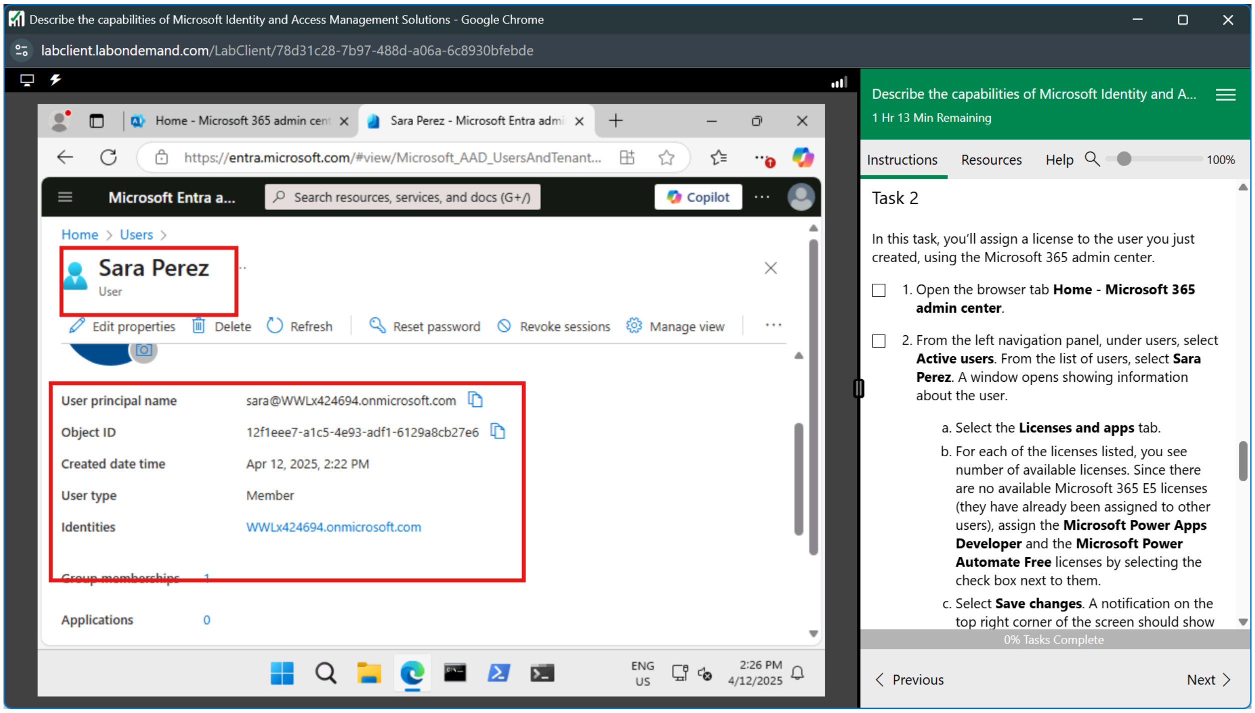
□ 10. This concludes the lab setup on the Microsoft 365 tenant.

Review

In this setup, you enabled the audit log and file monitoring capabilities in Microsoft 365.

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.


Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/78d31c28-7b97-488d-a06a-6c8930bfebde
Home - Microsoft 365 admin cent
Sara Perez - Microsoft Entra adm
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenant...
Microsoft Entra a...
Search resources, services, and docs (G+/)
Copilot
Home > Users >
Sara Perez
User
Edit properties
Delete
Refresh
Reset password
Revoke sessions
Manage view
ENG
US
2:26 PM
4/12/2025
Describe the capabilities of Microsoft Identity and A...
1 Hr 13 Min Remaining
Instructions
Resources
Help
100%
0% Tasks Complete
Previous
Next

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
Group memberships	1
Applications	0

Task 2

In this task, you'll assign a license to the user you just created, using the Microsoft 365 admin center.

☐ 1. Open the browser tab **Home - Microsoft 365 admin center**.

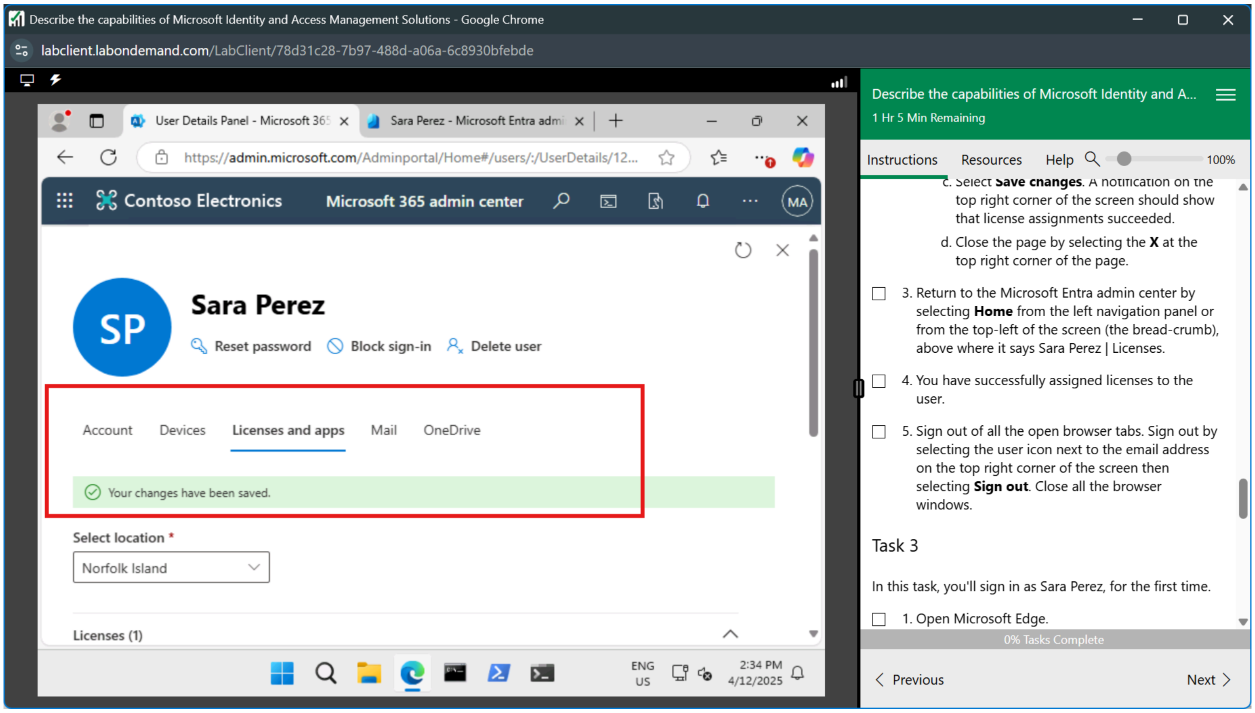
☐ 2. From the left navigation panel, under users, select **Active users**. From the list of users, select **Sara Perez**. A window opens showing information about the user.

a. Select the **Licenses and apps** tab.

b. For each of the licenses listed, you see number of available licenses. Since there are no available Microsoft 365 E5 licenses (they have already been assigned to other users), assign the **Microsoft Power Apps Developer** and the **Microsoft Power Automate Free** licenses by selecting the check box next to them.

c. Select **Save changes**. A notification on the top right corner of the screen should show

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


Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/78d31c28-7b97-488d-a06a-6c8930bfebde
User Details Panel - Microsoft 365
Sara Perez - Microsoft Entra adm
https://admin.microsoft.com/Adminportal/Home#/users/:/UserDetails/12...
Contoso Electronics
Microsoft 365 admin center
MA
SP
Sara Perez
Reset password
Block sign-in
Delete user
Account
Devices
Licenses and apps
Mail
OneDrive
ENG
US
2:34 PM
4/12/2025
Describe the capabilities of Microsoft Identity and A...
1 Hr 5 Min Remaining
Instructions
Resources
Help
100%
0% Tasks Complete
Previous
Next

Your changes have been saved.

Select location *

Norfolk Island

Licenses (1)

c. Select **Save changes**. A notification on the top right corner of the screen should show that license assignments succeeded.

d. Close the page by selecting the **X** at the top right corner of the page.

☐ 3. Return to the Microsoft Entra admin center by selecting **Home** from the left navigation panel or from the top-left of the screen (the bread-crumb), above where it says Sara Perez | Licenses.

☐ 4. You have successfully assigned licenses to the user.

☐ 5. Sign out of all the open browser tabs. Sign out by selecting the user icon next to the email address on the top right corner of the screen then selecting **Sign out**. Close all the browser windows.

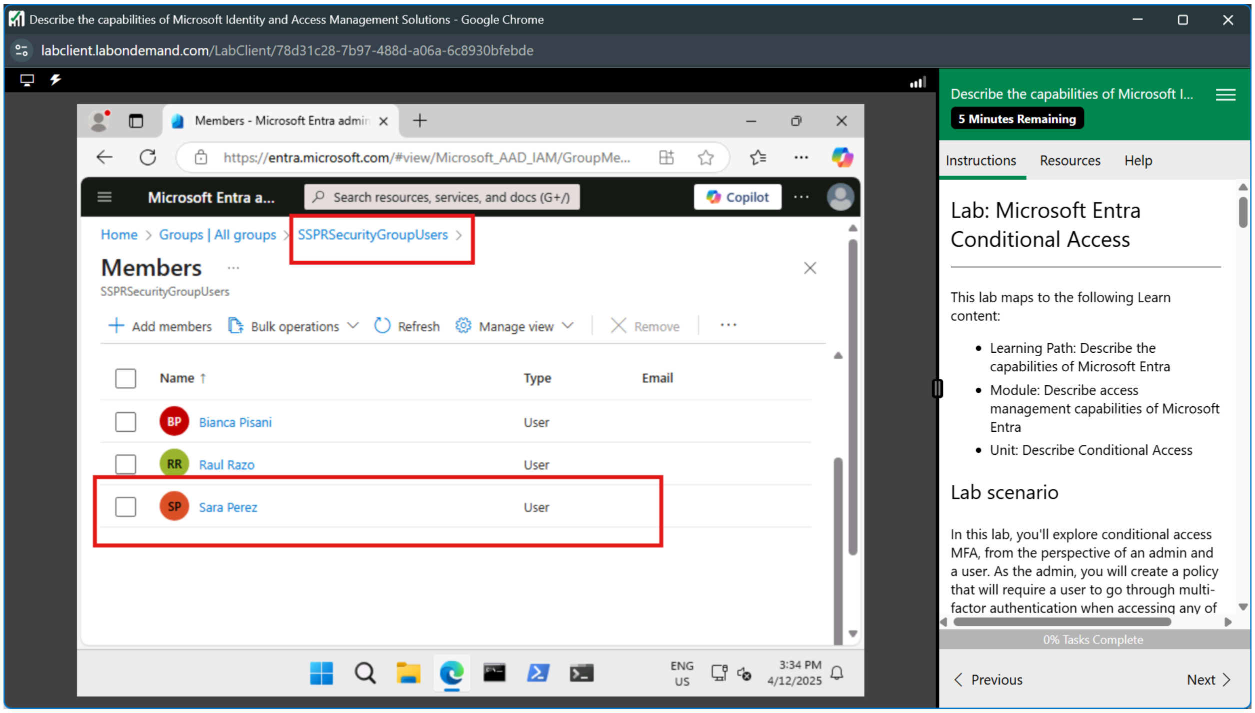
Task 3

In this task, you'll sign in as Sara Perez, for the first time.

☐ 1. Open Microsoft Edge.

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.



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

labclient.labondemand.com/LabClient/78d31c28-7b97-488d-a06a-6c8930bfebde

Members - Microsoft Entra admin

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/GroupMe...

Microsoft Entra a... | Search resources, services, and docs (G+/) | Copilot

Home > Groups | All groups > SSPRSecurityGroupUsers >

Members

SSPRSecurityGroupUsers

+ Add members | Bulk operations | Refresh | Manage view | Remove

	Name ↑	Type	Email
□	BP Bianca Pisani	User	
□	RR Raul Razo	User	
□	SP Sara Perez	User	

ENG US 3:34 PM 4/12/2025

Describe the capabilities of Microsoft I...

5 Minutes Remaining

Instructions | Resources | Help

Lab: Microsoft Entra Conditional Access

This lab maps to the following Learn content:

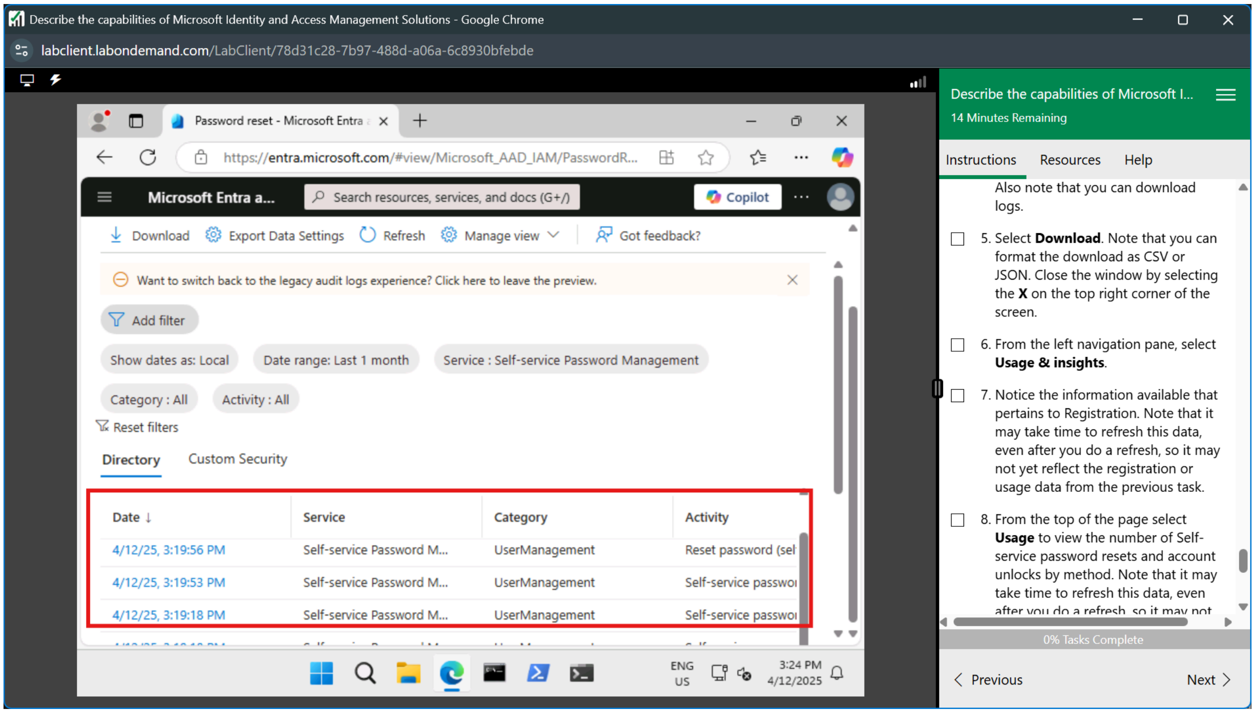
- Learning Path: Describe the capabilities of Microsoft Entra
- Module: Describe access management capabilities of Microsoft Entra
- Unit: Describe Conditional Access

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

0% Tasks Complete

< Previous | Next >



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

labclient.labondemand.com/LabClient/78d31c28-7b97-488d-a06a-6c8930bfebde

Password reset - Microsoft Entra

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/PasswordR...

Microsoft Entra a... | Search resources, services, and docs (G+/) | Copilot

Download | Export Data Settings | Refresh | Manage view | Got feedback?

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

Add filter

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 passwo
4/12/25, 3:19:18 PM	Self-service Password M...	UserManagement	Self-service passwo

ENG US 3:24 PM 4/12/2025

Describe the capabilities of Microsoft I...

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.

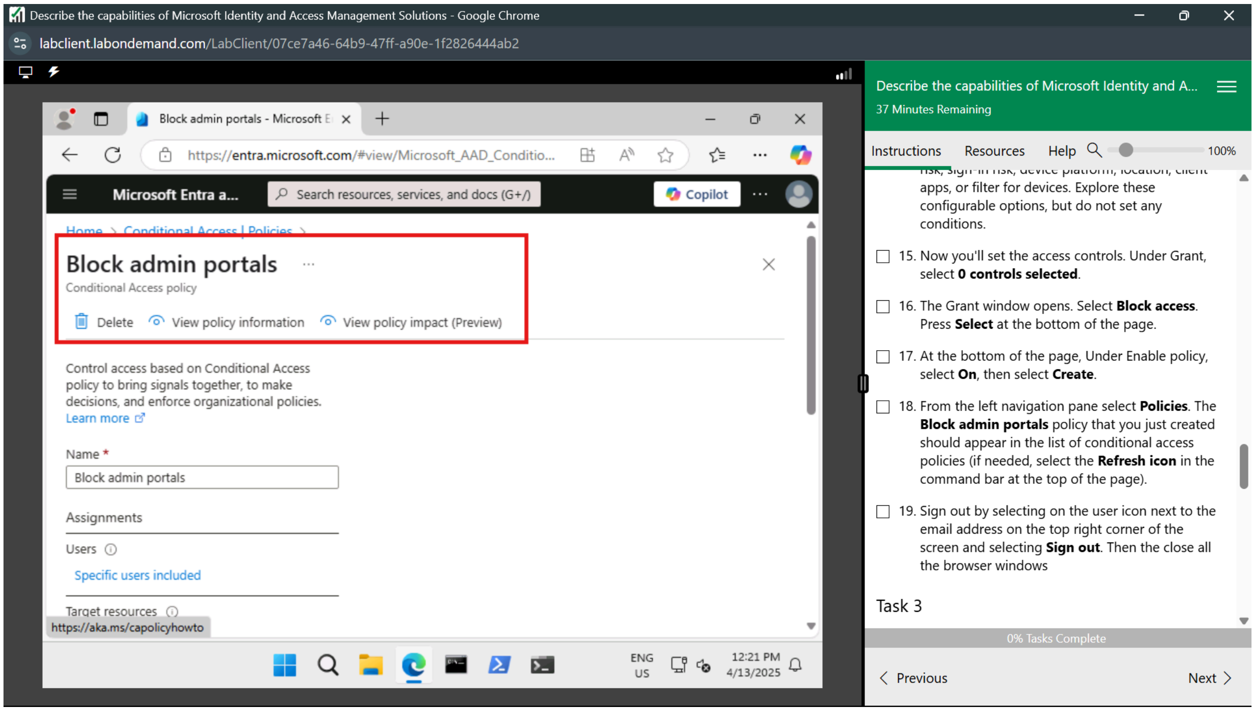
□ 8. From the top of the page select **Usage** to view the number of Self-service password resets and account unlocks by method. Note that it may take time to refresh this data, even after you do a refresh, so it may not

0% 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.



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

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

Block admin portals - Microsoft E

https://entra.microsoft.com/#view/Microsoft_AAD_Conditio...

Microsoft Entra a... Search resources, services, and docs (G+/) Copilot

Home > Conditional Access | Policies >

Block admin portals ...

Conditional Access policy

Delete View policy information View policy impact (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *

Block admin portals

Assignments

Users

Specific users included

Target resources

https://aka.ms/capolicyhowto

ENG US 12:21 PM 4/13/2025

Describe the capabilities of Microsoft Identity and A...

37 Minutes Remaining

Instructions Resources Help 100%

risk, sign-in risk, device platform, location, client apps, or filter for devices. Explore these configurable options, but do not set any 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**.

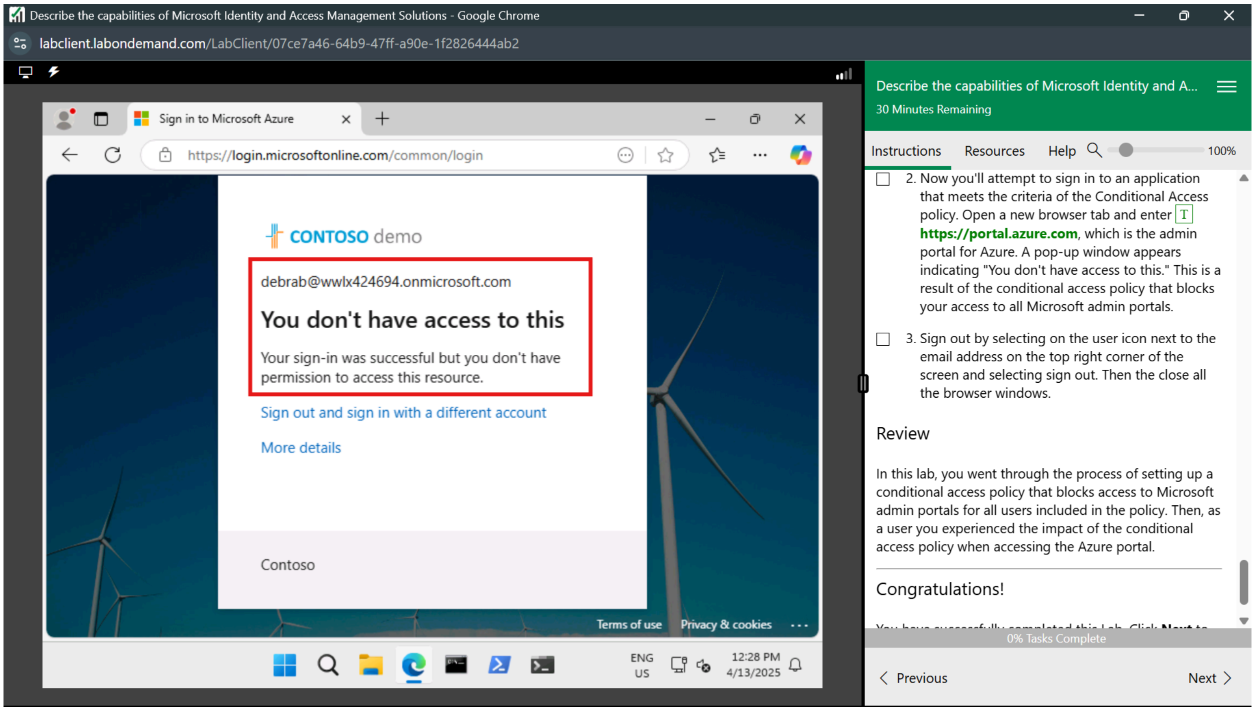
□ 18. From the left navigation pane select **Policies**. The **Block admin portals** policy that you just created should appear in the list of conditional access policies (if needed, select the **Refresh icon** in the command bar at the top of the page).

□ 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

0% Tasks Complete

Previous Next



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

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

Sign in to Microsoft Azure

https://login.microsoftonline.com/common/login

CONTOSO demo

debrab@wwlx424694.onmicrosoft.com

You don't have access to this

Your sign-in was successful but you don't have permission to access this resource.

Sign out and sign in with a different account

More details

Contoso

Terms of use Privacy & cookies ...

ENG US 12:28 PM 4/13/2025

Describe the capabilities of Microsoft Identity and A...

30 Minutes Remaining

Instructions Resources Help 100%

□ 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 T **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 the 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!

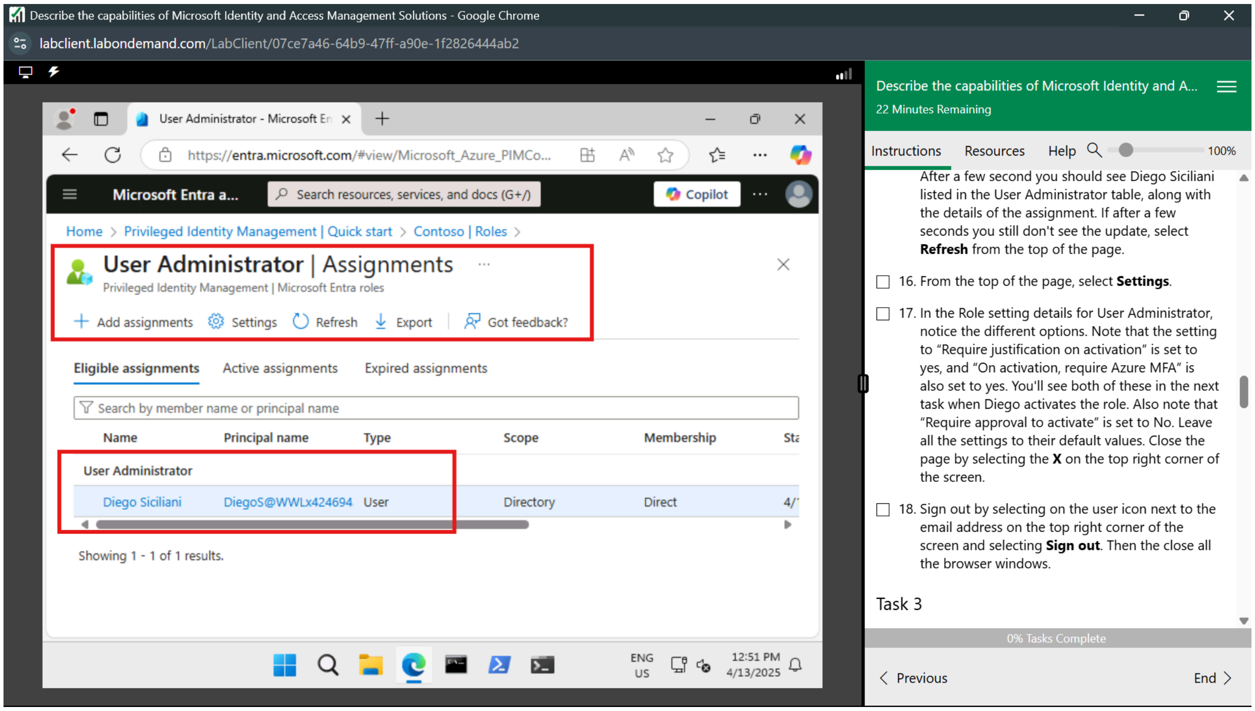
You have successfully completed this Lab. Click **Next** to

0% Tasks Complete

Previous Next

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
User Administrator - Microsoft En
https://entra.microsoft.com/#view/Microsoft_Azure_PIMCo...
Microsoft Entra a...
Search resources, services, and docs (G+/)
Copilot
Home > Privileged Identity Management | Quick start > Contoso | Roles >
Add assignments
Settings
Refresh
Export
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by member name or principal name
ENG US
12:51 PM 4/13/2025
Describe the capabilities of Microsoft Identity and A...
22 Minutes Remaining
Instructions
Resources
Help
100%
0% Tasks Complete
Previous
End

User Administrator | Assignments

Privileged Identity Management | Microsoft Entra roles

Name	Principal name	Type	Scope	Membership	Sta
User Administrator					
Diego Siciliani	DiegoS@WWLx424694	User	Directory	Direct	4/

Showing 1 - 1 of 1 results.

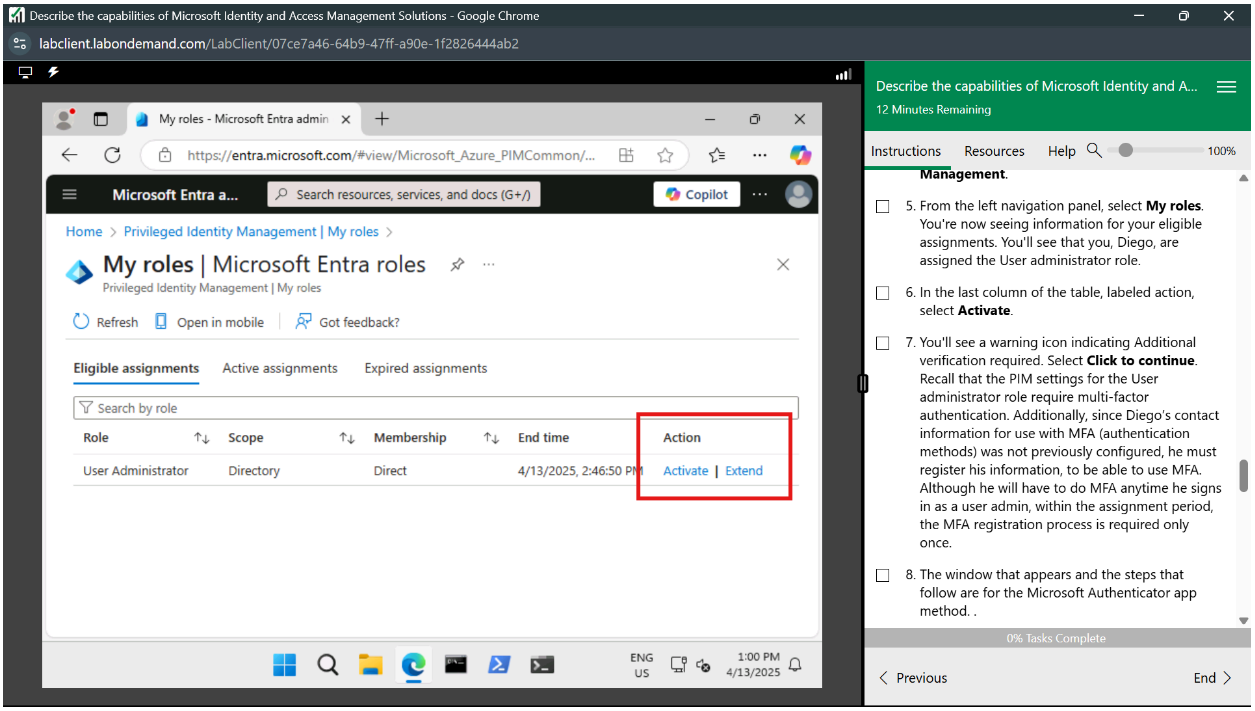
After a few second you should see Diego Siciliani listed in the User Administrator table, along with the details of the assignment. If after a few seconds you still don't see the update, select **Refresh** from the top of the page.

□ 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 windows.

Task 3


Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/07ce7a46-64b9-47ff-a90e-1f2826444ab2
My roles - Microsoft Entra admin
https://entra.microsoft.com/#view/Microsoft_Azure_PIMCommon/...
Microsoft Entra a...
Search resources, services, and docs (G+/)
Copilot
Home > Privileged Identity Management | My roles >
Refresh
Open in mobile
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by role
ENG US
1:00 PM 4/13/2025
Describe the capabilities of Microsoft Identity and A...
12 Minutes Remaining
Instructions
Resources
Help
100%
0% Tasks Complete
Previous
End

My roles | Microsoft Entra roles

Privileged Identity Management | My roles

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

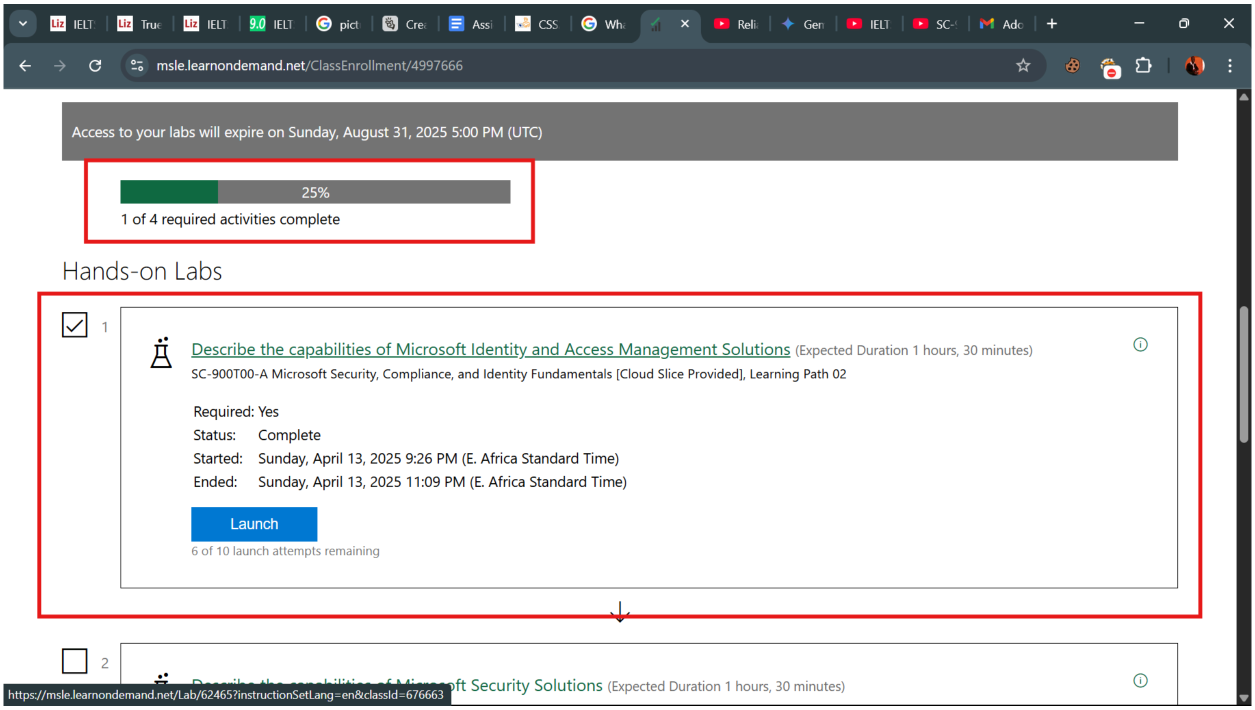
Management.

□ 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. .



Access to your labs will expire on Sunday, August 31, 2025 5:00 PM (UTC)

25%

1 of 4 required activities complete

Hands-on Labs

☑ 1

Describe the capabilities of Microsoft Identity and Access Management Solutions (Expected Duration 1 hours, 30 minutes)

SC-900T00-A Microsoft Security, Compliance, and Identity Fundamentals [Cloud Slice Provided], Learning Path 02

Required: Yes
Status: Complete
Started: Sunday, April 13, 2025 9:26 PM (E. Africa Standard Time)
Ended: Sunday, April 13, 2025 11:09 PM (E. Africa Standard Time)

Launch

6 of 10 launch attempts remaining

□ 2

Describe the capabilities of Microsoft Security Solutions (Expected Duration 1 hours, 30 minutes)

https://msle.learnondemand.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.