Name: Anne Musau

Program Details: Data Protection Specialist - C1 – 2025

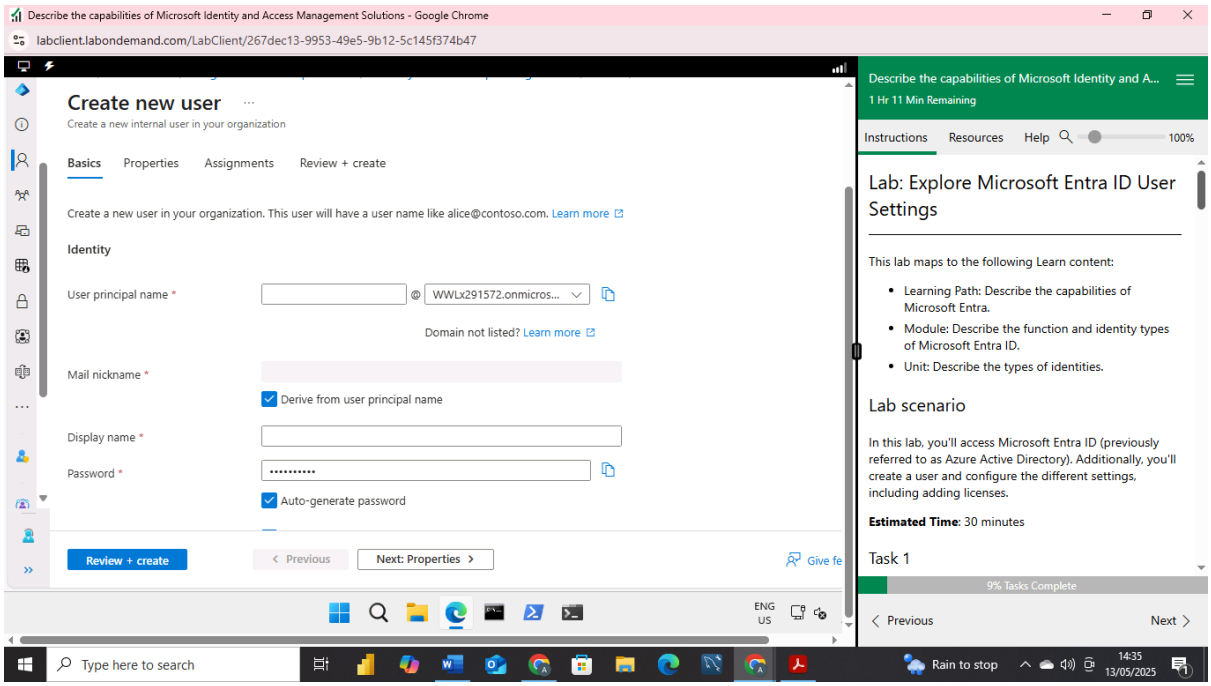
Admission: adc-dp01-25032

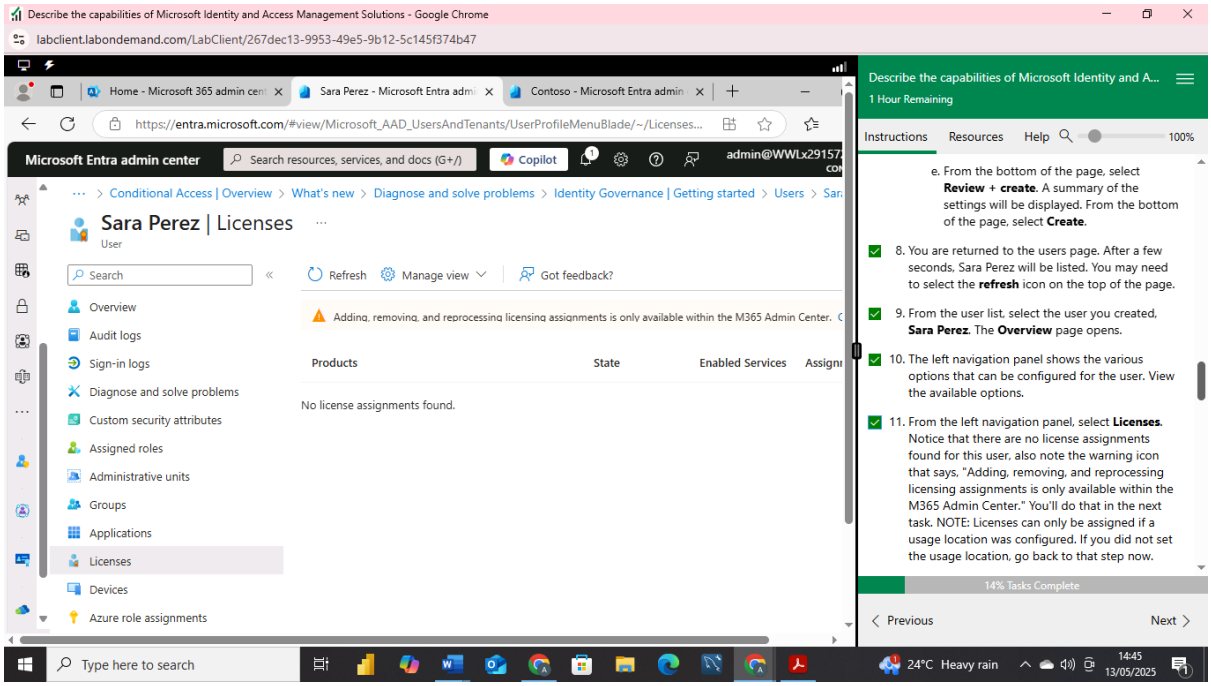
Week 2 Lab Assignment: SC-900 Lab 1

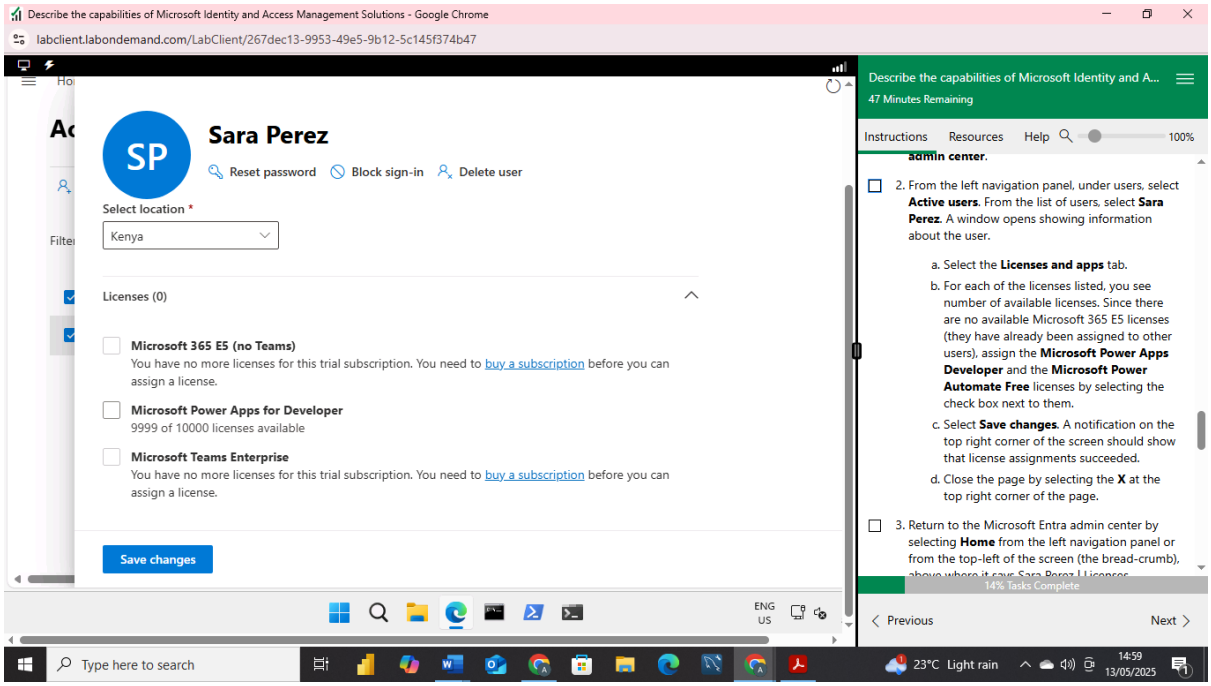
Microsoft Identity and Access Management Solutions.

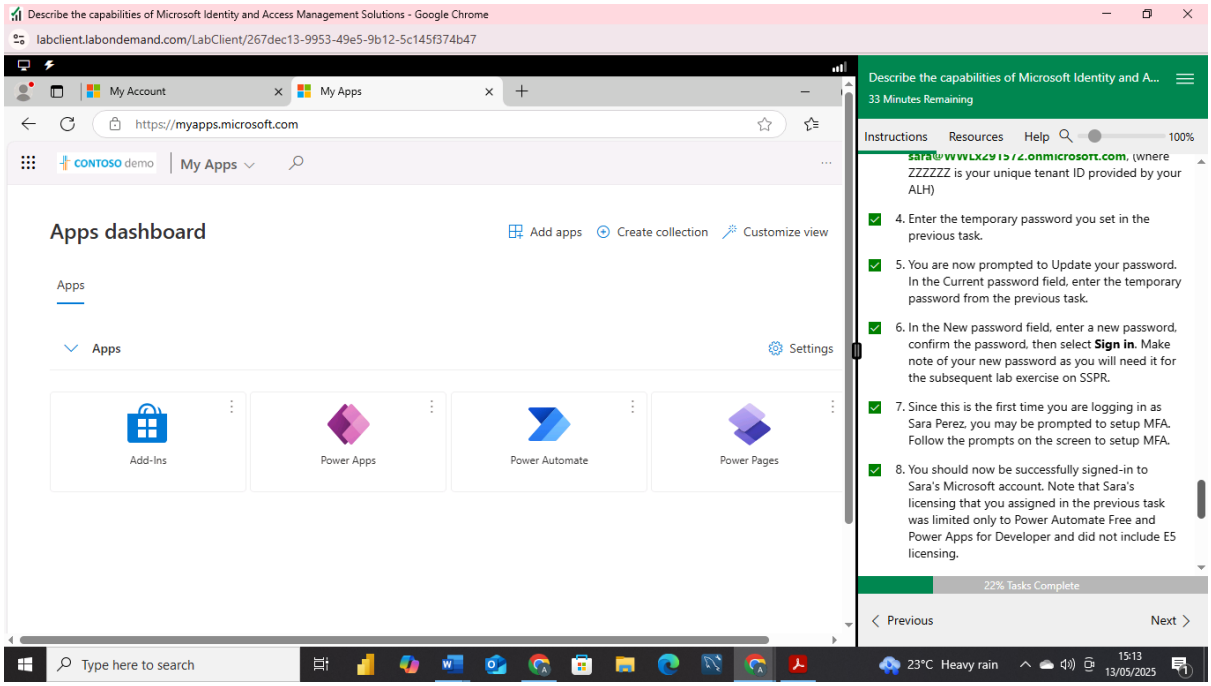
1. Lab: Explore Microsoft Entra ID User Settings
2. Lab: Microsoft Entra self-service password reset
3. Lab: Microsoft Entra Conditional Access
4. Lab: Explore Privileged Identity Management

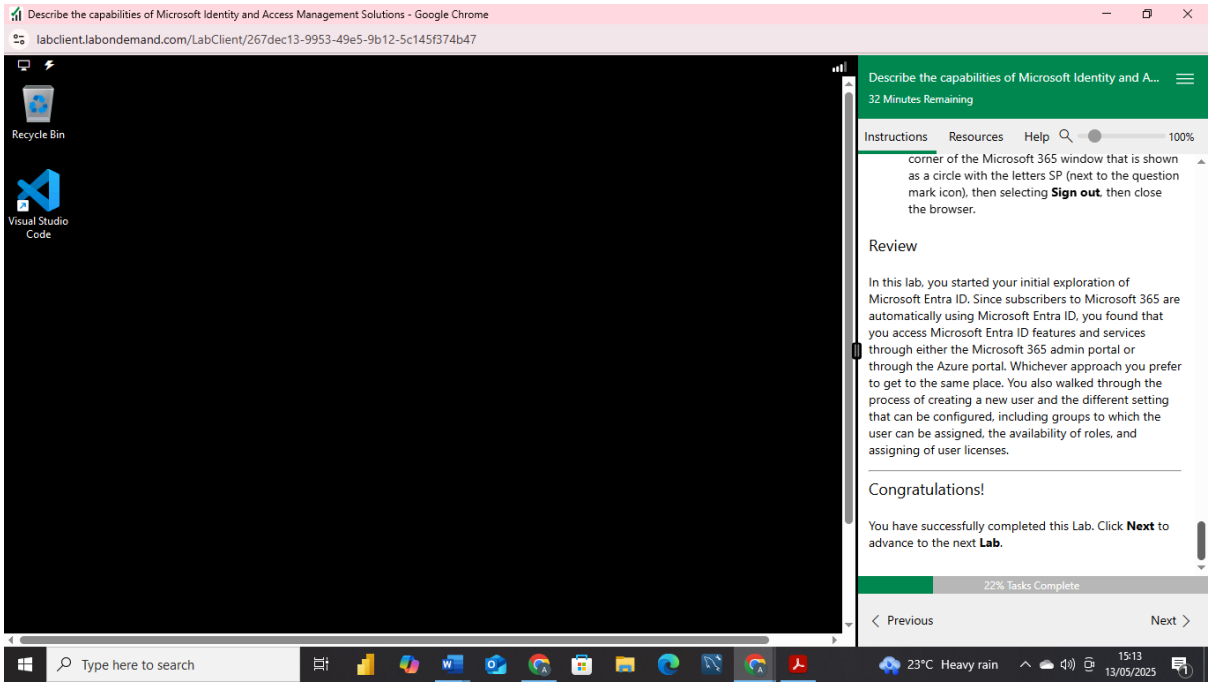
Lab 1: Explore Microsoft Entra ID User Settings




Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/267dec13-9953-49e5-9b12-5c145f374b47
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Conditional Access | Overview > What's new > Diagnose and solve problems > Identity Governance | Getting started > Users
Sara Perez | Licenses
User
Search
Refresh
Manage view
Got feedback?
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Products
State
Enabled Services
No license assignments found.
Describe the capabilities of Microsoft Identity and A...
1 Hour Remaining
Instructions
Resources
Help
100%
e. From the bottom of the page, select Review + create. A summary of the settings will be displayed. From the bottom of the page, select Create.
8. You are returned to the users page. After a few seconds, Sara Perez will be listed. You may need to select the refresh icon on the top of the page.
9. From the user list, select the user you created, Sara Perez. The Overview page opens.
10. The left navigation panel shows the various options that can be configured for the user. View the available options.
11. From the left navigation panel, select Licenses. Notice that there are no license assignments found for this user, also note the warning icon that says, "Adding, removing, and reprocessing licensing assignments is only available within the M365 Admin Center." You'll do that in the next task. NOTE: Licenses can only be assigned if a usage location was configured. If you did not set the usage location, go back to that step now.
14% Tasks Complete
Previous
Next
Type here to search
24°C Heavy rain
14:45
13/05/2025

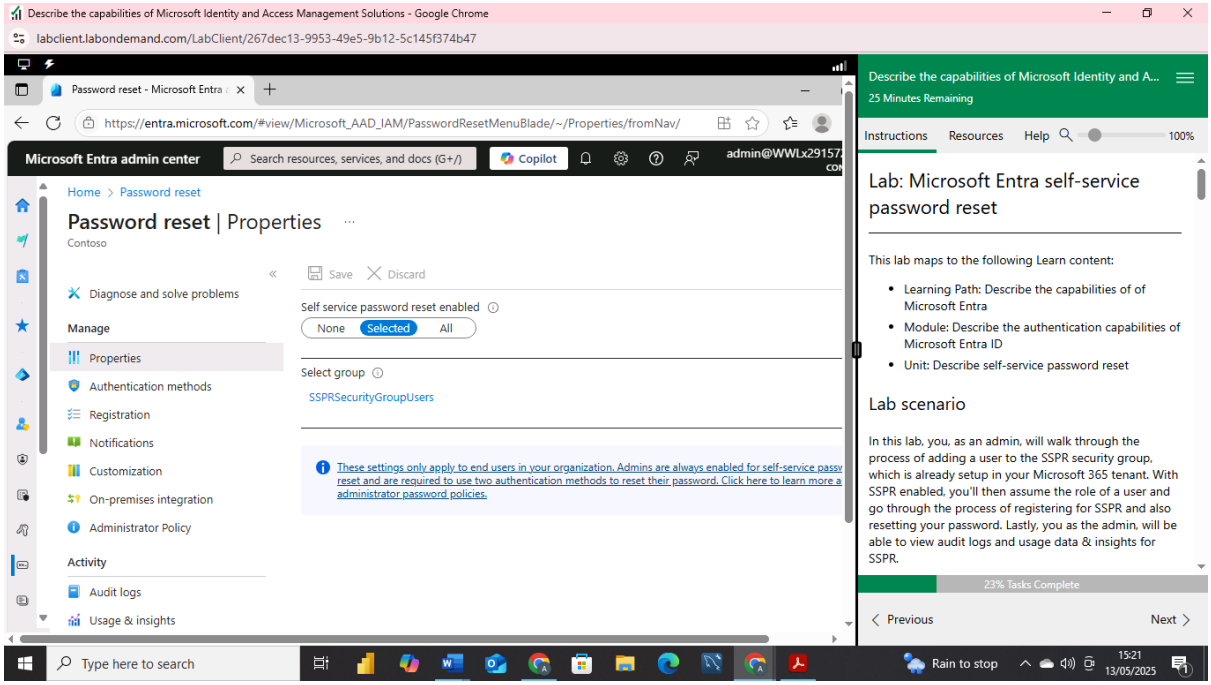

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/267dec13-9953-49e5-9b12-5c145f374b47
SP
Sara Perez
Reset password
Block sign-in
Delete user
Select location *
Kenya
Licenses (0)
Microsoft 365 E5 (no Teams)
You have no more licenses for this trial subscription. You need to buy a subscription before you can assign a license.
Microsoft Power Apps for Developer
9999 of 10000 licenses available
Microsoft Teams Enterprise
You have no more licenses for this trial subscription. You need to buy a subscription before you can assign a license.
Save changes
Describe the capabilities of Microsoft Identity and A...
47 Minutes Remaining
Instructions
Resources
Help
100%
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 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),
14% Tasks Complete
Previous
Next
Type here to search
23°C Light rain
14:59
13/05/2025

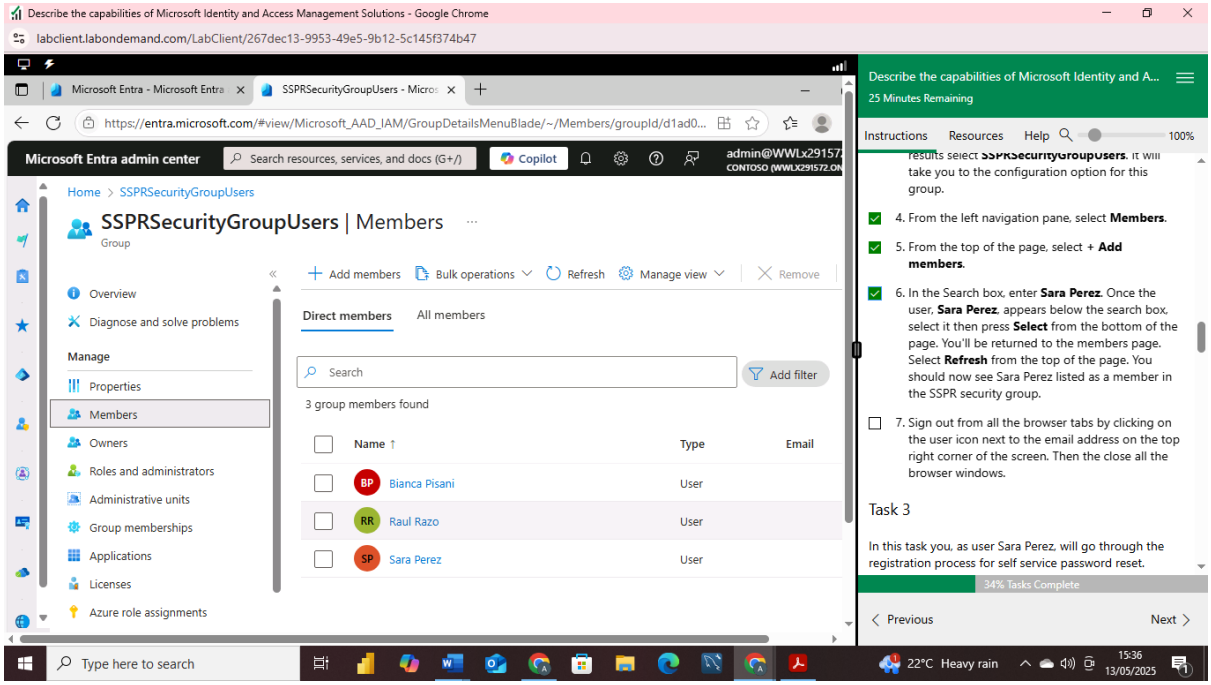


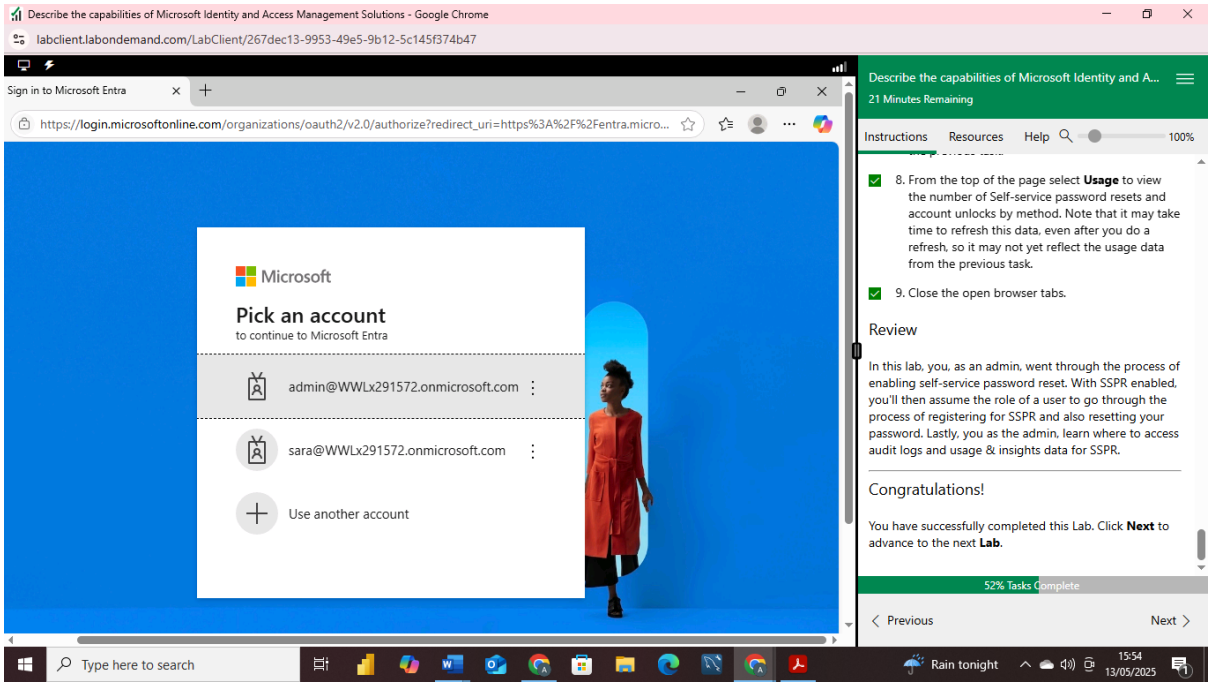


In this lab, I worked with Microsoft Entra ID to manage user identities and access. I began by creating a new user through the Microsoft 365 admin portal which provides access to Entra ID features. After creating the user, I added the user to a security group to help manage access permissions more efficiently. I then proceeded to assign Microsoft 365 licenses to the user. During this process, I observed that a usage location must be configured before licenses can be successfully assigned, highlighting an important prerequisite for license management.

Lab 2: Microsoft Entra self-service password reset

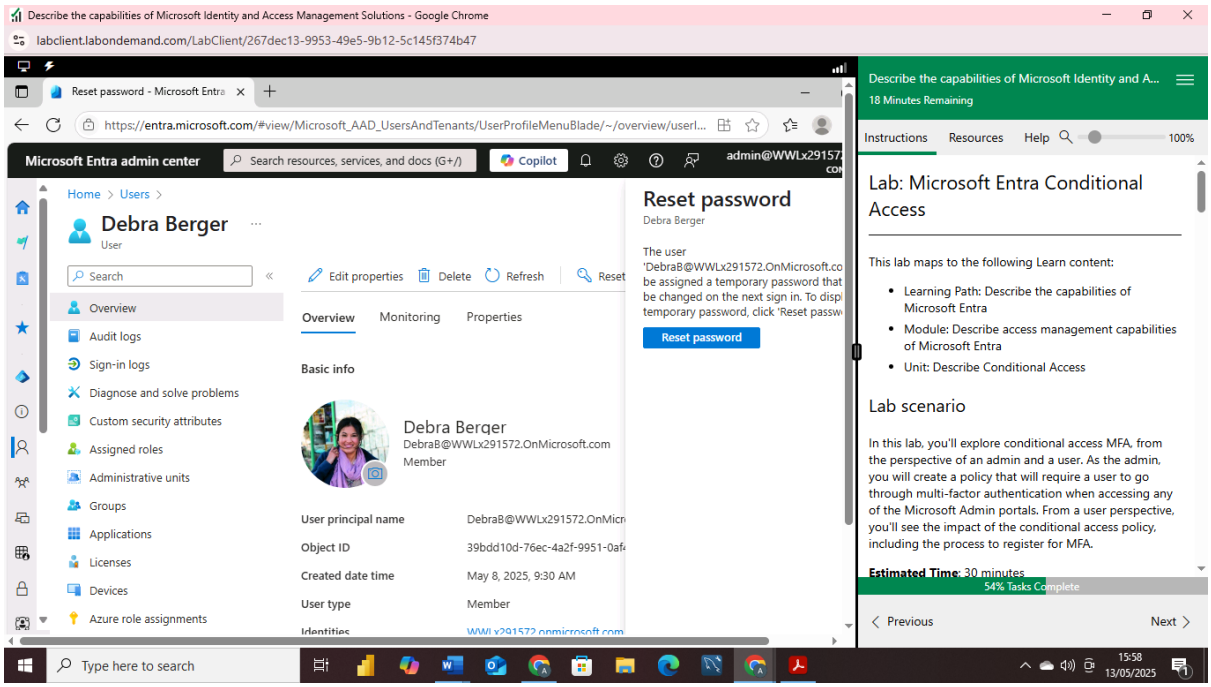


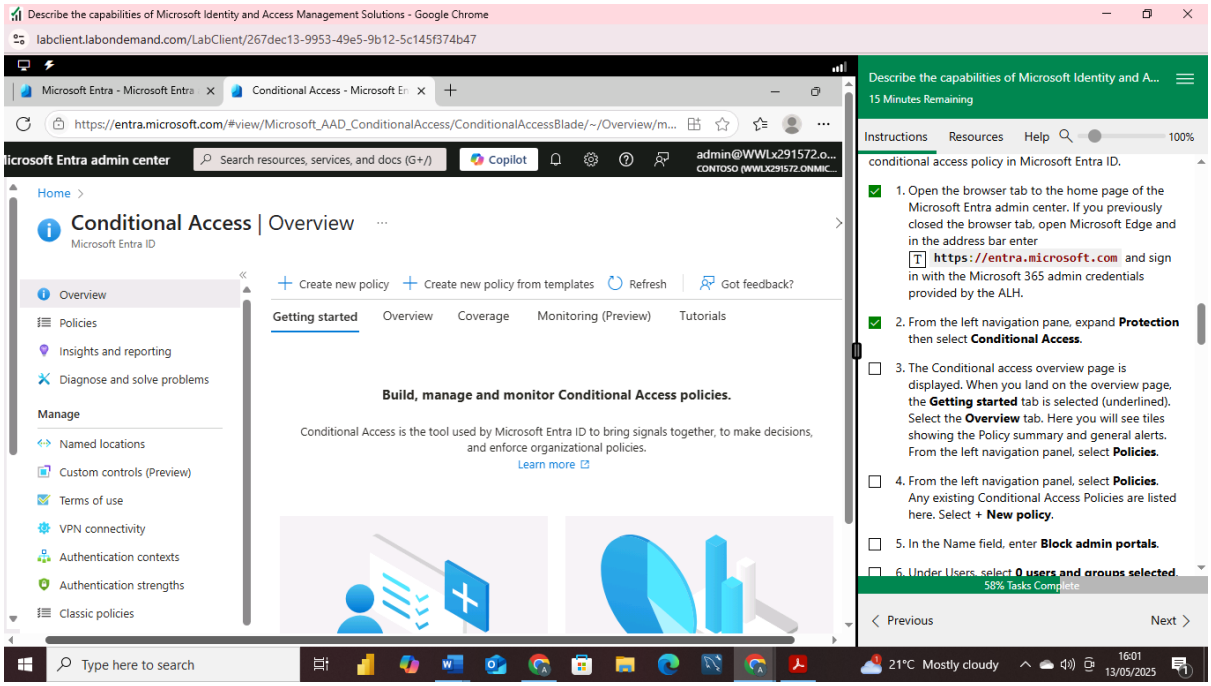


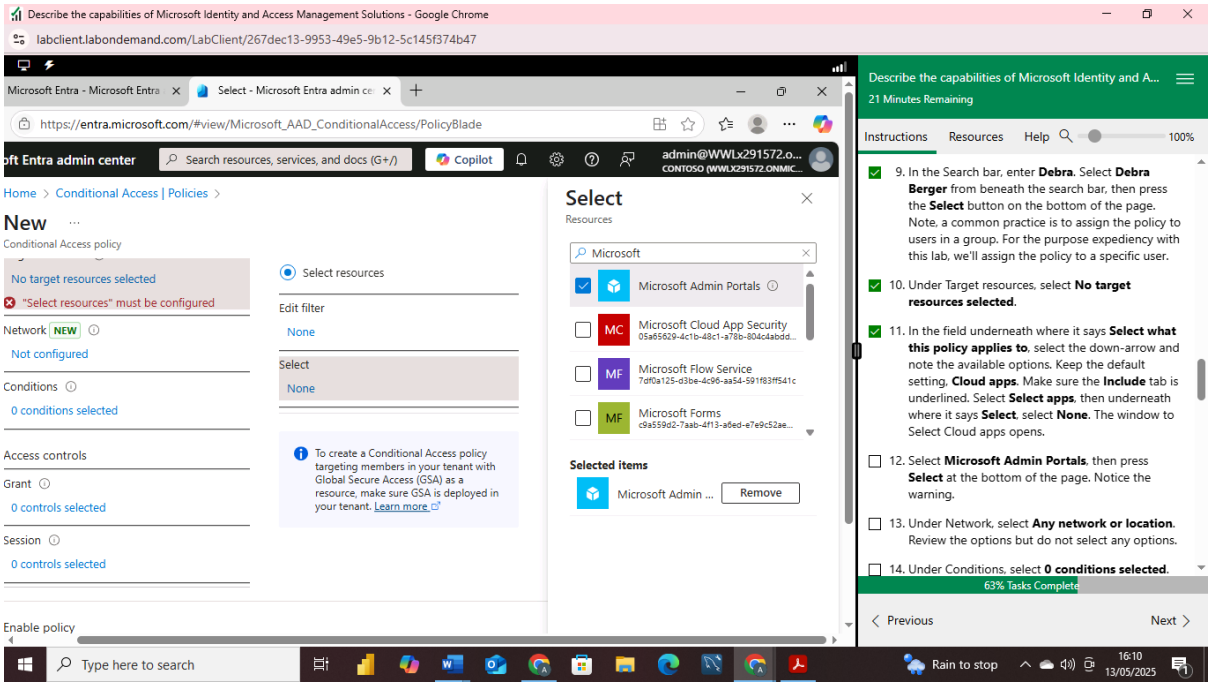


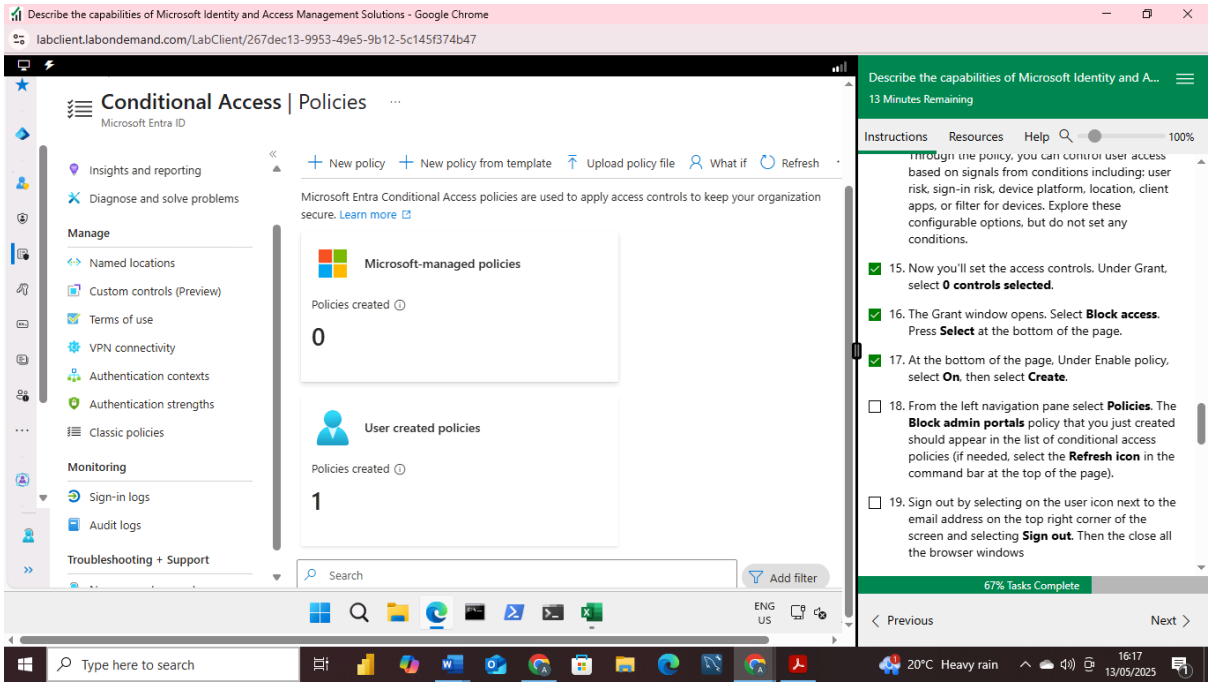
In this lab, I explored the password reset settings within the Microsoft Entra ID admin center. I reviewed the navigation pane and examined the available configuration options, including audit logs and usage & insights, which help track user activity and monitor password reset behaviour. I then added the user created in the previous task to a security group that enforces self-service password reset (SSPR) policies. To test the configuration, I assumed the role of the user and performed a new registration, as the group settings required members to register for SSPR during sign-in. I also verified that the user could reset their password as intended, confirming the group's policy enforcement.

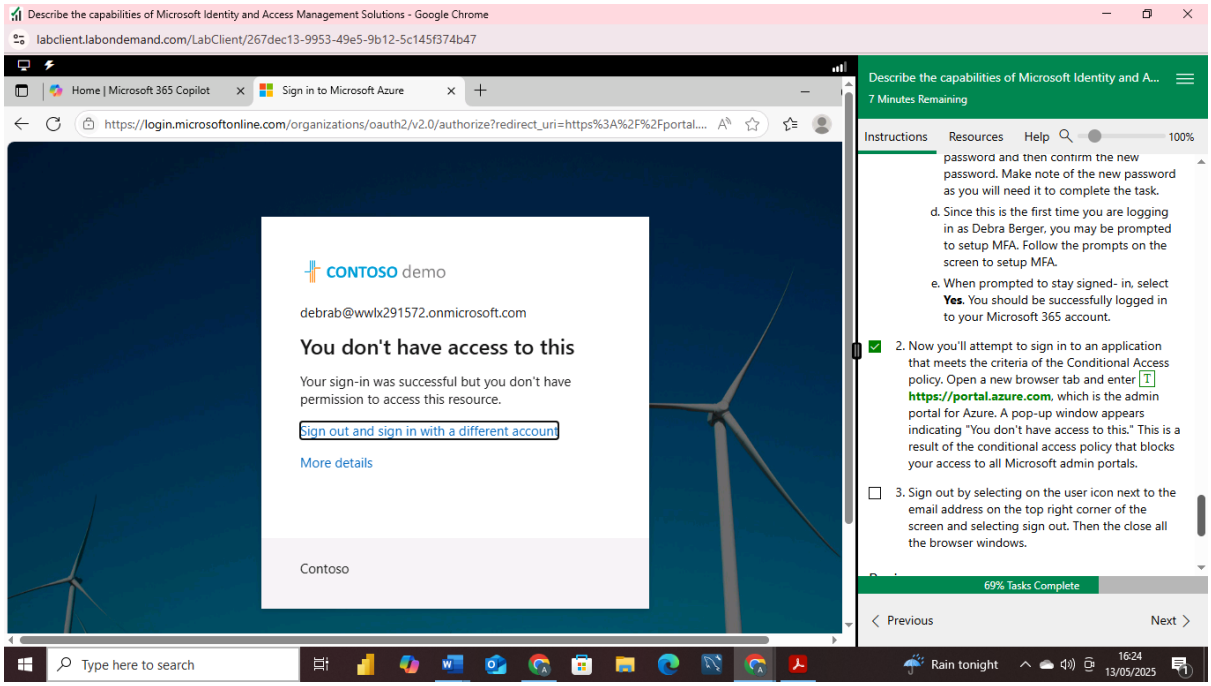
Lab 3: Microsoft Entra Conditional Access

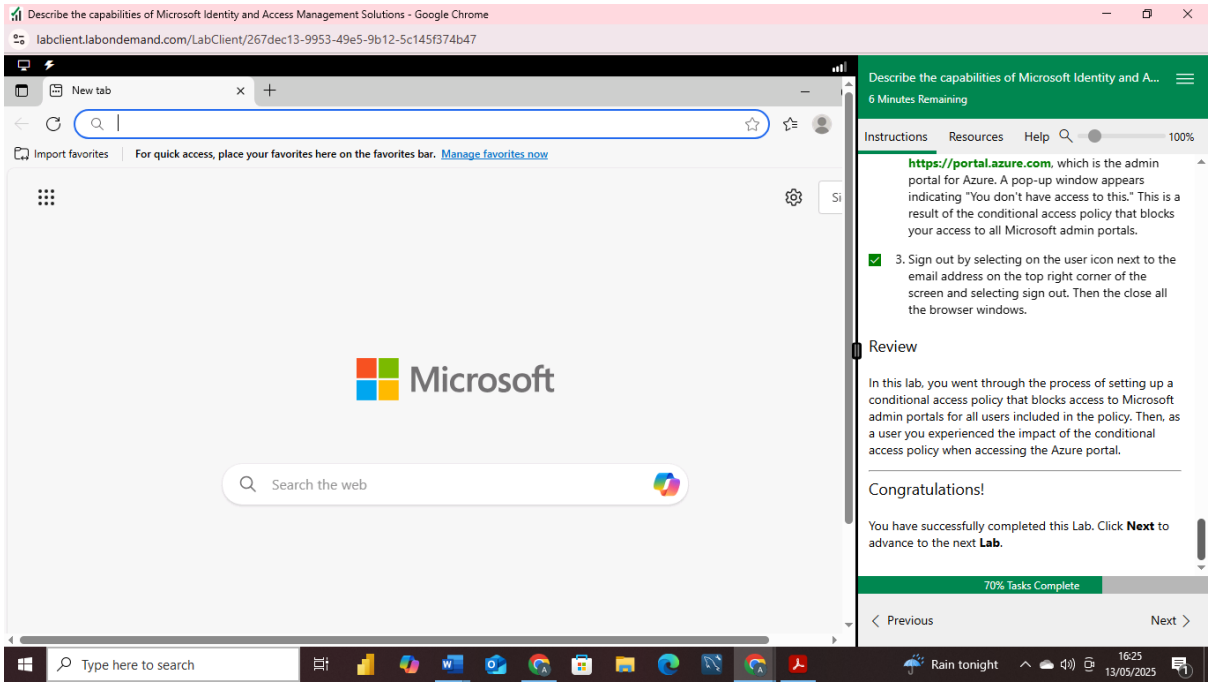



Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/267dec13-9953-49e5-9b12-5c145f374b47
Microsoft Entra - Microsoft Entra
Conditional Access - Microsoft Entra
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Overview/m...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
admin@WWLx291572.o...
CONTOSO (WWLX291572.ONMIC...
Home
Conditional Access | Overview
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
Create new policy
Create new policy from templates
Refresh
Got feedback?
Getting started
Overview
Coverage
Monitoring (Preview)
Tutorials
Build, manage and monitor Conditional Access policies.
Conditional Access is the tool used by Microsoft Entra ID to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Describe the capabilities of Microsoft Identity and A...
15 Minutes Remaining
Instructions
Resources
Help
100%
conditional access policy in Microsoft Entra ID.
1. Open the browser tab to the home page of the Microsoft Entra admin center. If you previously closed the browser tab, open Microsoft Edge and in the address bar enter https://entra.microsoft.com and sign in with the Microsoft 365 admin credentials provided by the ALH.
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.
58% Tasks Complete
Previous
Next
Type here to search
21°C Mostly cloudy
16:01
13/05/2025


Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/267dec13-9953-49e5-9b12-5c145f374b47
Microsoft Entra - Microsoft Entra
Select - Microsoft Entra admin ce
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade
Search resources, services, and docs (G+/)
Copilot
admin@WWLx291572.o...
CONTOSO (WWLX291572.ONMIC...
Home
Conditional Access | Policies
New
Conditional Access policy
No target resources selected
"Select resources" must be configured
Network NEW
Not configured
Conditions
0 conditions selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Enable policy
Select resources
Edit filter
None
Select
None
To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. Learn more
Select
Resources
Microsoft
Microsoft Admin Portals
Microsoft Cloud App Security
Microsoft Flow Service
Microsoft Forms
Selected items
Microsoft Admin ...
Remove
Describe the capabilities of Microsoft Identity and A...
21 Minutes Remaining
Instructions
Resources
Help
100%
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. Note, a common practice is to assign the policy to users in a group. For the purpose expediency with this lab, we'll assign the policy to a specific user.
10. Under Target resources, select No target resources selected.
11. In the field underneath where it says Select what this policy applies to, select the down-arrow and note the available options. Keep the default setting, Cloud apps. Make sure the Include tab is underlined. Select Select apps, then underneath where it says Select, select None. The window to Select Cloud apps opens.
12. Select Microsoft Admin Portals, then press Select at the bottom of the page. Notice the warning.
13. Under Network, select Any network or location. Review the options but do not select any options.
14. Under Conditions, select 0 conditions selected.
63% Tasks Complete
Previous
Next
Type here to search
Rain to stop
16:10
13/05/2025

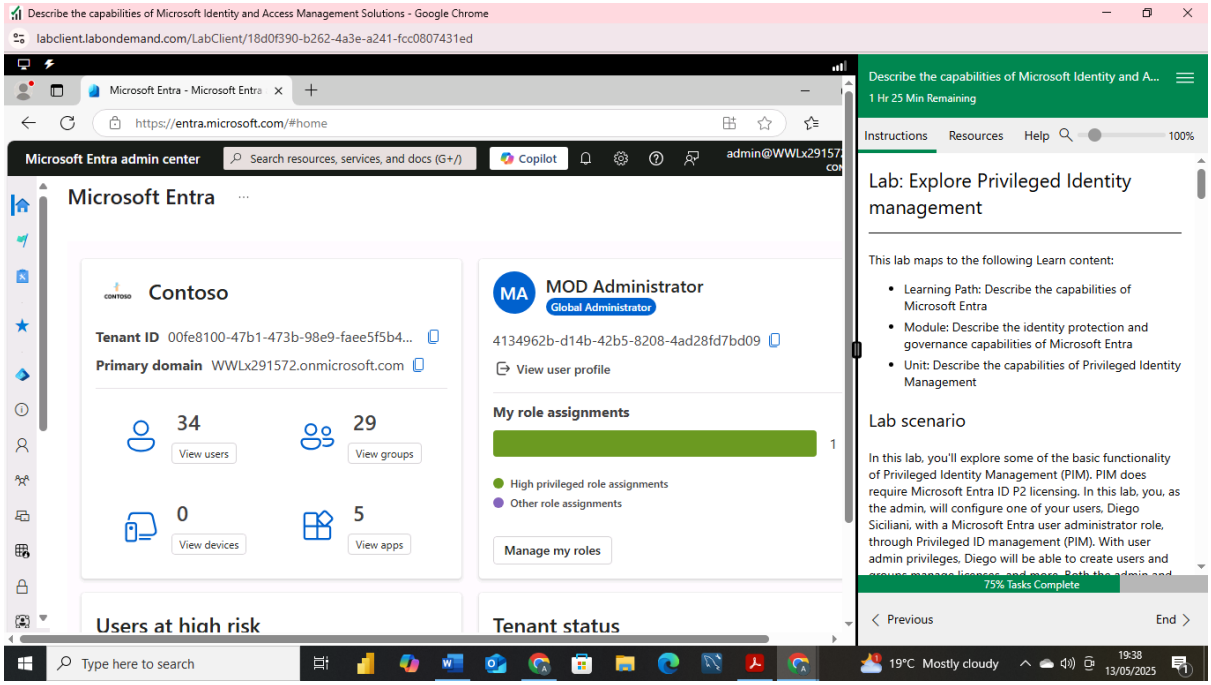

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/267dec13-9953-49e5-9b12-5c145f374b47
Conditional Access | Policies
Microsoft Entra ID
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
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
Microsoft-managed policies
Policies created
0
User created policies
Policies created
1
Search
Add filter
Describe the capabilities of Microsoft Identity and A...
13 Minutes Remaining
Instructions
Resources
Help
100%
based on signals from conditions including: user 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
67% Tasks Complete
Previous
Next
Type here to search
20°C Heavy rain
16:17
13/05/2025

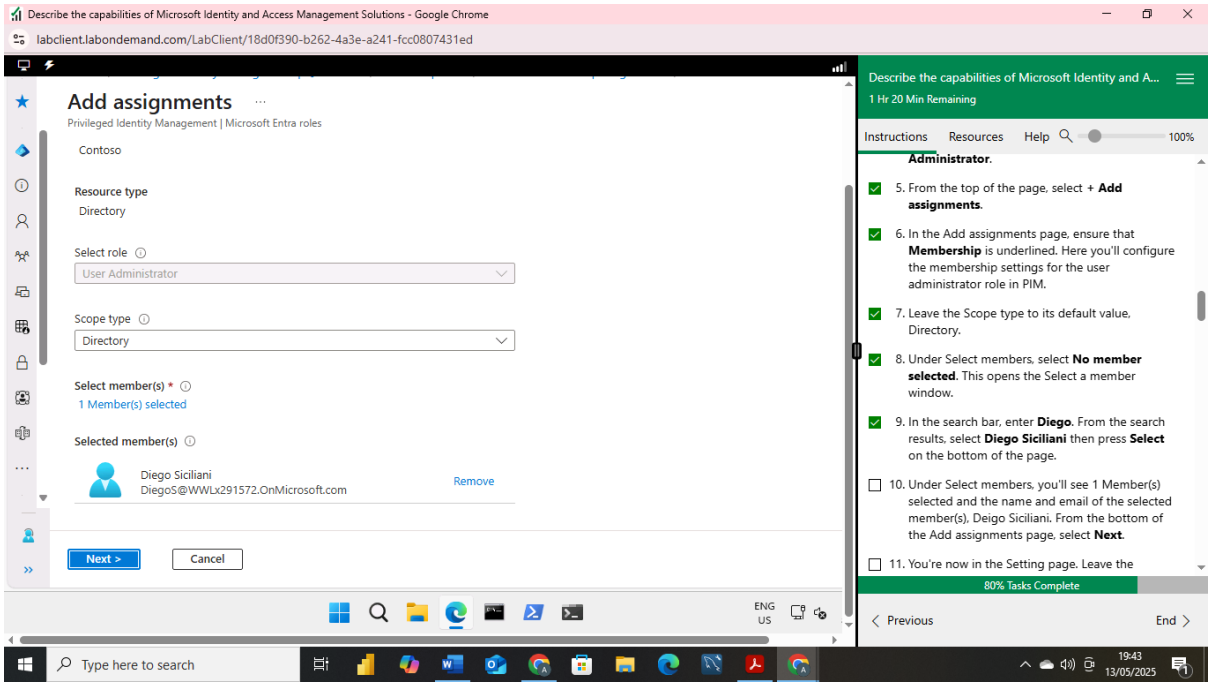

Describe the capabilities of Microsoft Identity and Access Management Solutions - Google Chrome
labclient.labondemand.com/LabClient/267dec13-9953-49e5-9b12-5c145f374b47
Home | Microsoft 365 Copilot
Sign in to Microsoft Azure
https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize?redirect_uri=https%3A%2F%2Fportal....
CONTOSO demo
debrab@wwlx291572.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
Describe the capabilities of Microsoft Identity and A...
7 Minutes Remaining
Instructions
Resources
Help
100%
password and then confirm the new password. Make note of the new password as you will need it to complete the task.
d. Since this is the first time you are logging in as Debra Berger, you may be prompted to setup MFA. Follow the prompts on the screen to setup MFA.
e. When prompted to stay signed- in, select Yes. You should be successfully logged in to your Microsoft 365 account.
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.
69% Tasks Complete
Previous
Next
Type here to search
Rain tonight
16:24
13/05/2025

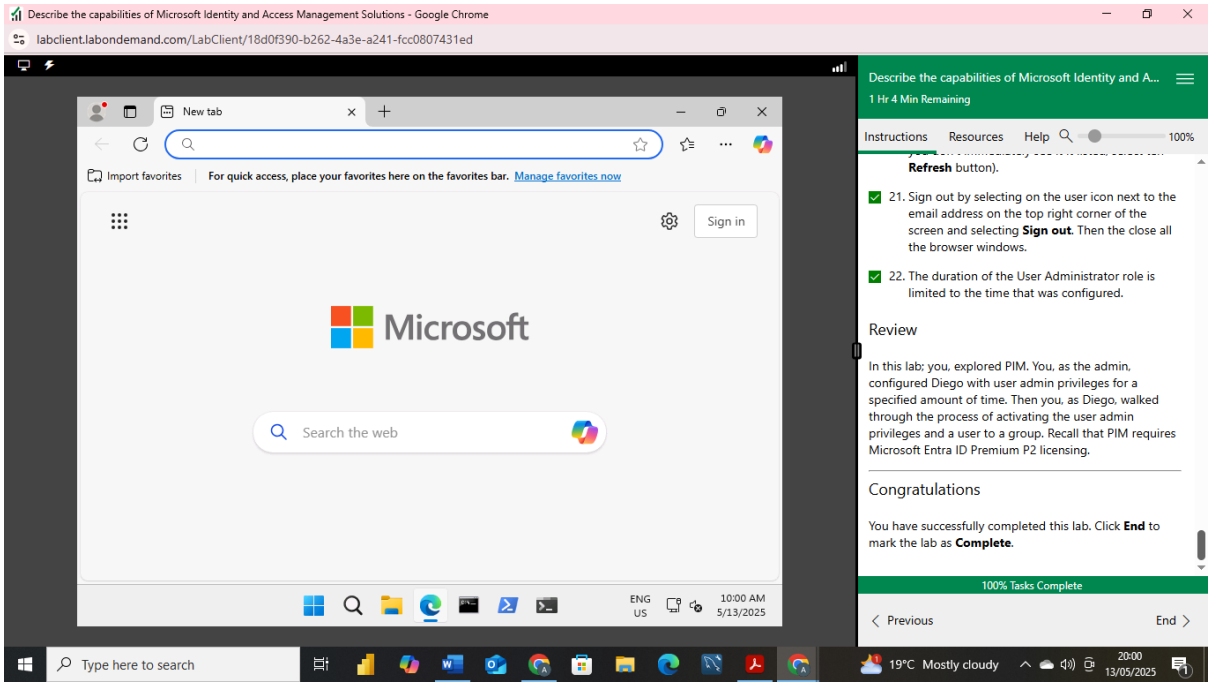


In this lab, I configured a Conditional Access policy in Microsoft Entra ID to enhance security controls. I logged in as an admin and I created a policy that specifically blocked access to Microsoft admin portals for a selected user in my case, Debra. I explored the Conditional Access Multi-Factor Authentication (MFA) settings from both the administrator and user perspectives to understand how policies affect user access. After setting up the policy, I signed in as Debra to simulate the user experience and confirmed that access to the admin portals was successfully blocked. This exercise demonstrated how Conditional Access can be used to enforce granular access restrictions and improve organizational security.

Lab 4: Explore Privileged Identity Management







In this lab, I explored the basic functionality of Microsoft Entra Privileged Identity Management (PIM). Acting as an administrator, I assigned the user Diego Siciliani the User Administrator role through PIM for a limited duration. I then assumed Diego's role to walk through the activation process of the assigned privileges and added a user to a group. This hands-on experience demonstrated how PIM enables just-in-time role activation, helping to reduce the risk of excessive, unused, or misused access permissions. Additionally, I learned that PIM requires Microsoft Entra ID P2 licensing to manage and monitor privileged roles effectively.