NAME: BINYANYA DEBORAH NYATICHI

CS NO: ADC-CSS02-25051.

DESCRIPTION: Week 2 Assignment 3

ASSIGNMENT: Lab on Microsoft Identity and Access Management Solutions

DATE: 05/04/2025

INTRODUCTION

In today's digital landscape, robust identity management is paramount for security, compliance, and user productivity. This lab series is designed to provide you with hands-on experience in key components of Microsoft's cutting-edge IAM platform, Microsoft Entra ID (formerly Azure AD).mThrough a series of focused labs, you will delve into critical functionalities that empower organizations to manage user identities, secure access to resources, and streamline administrative tasks. We will move beyond theoretical concepts and provide practical scenarios where you can configure and observe these powerful features in action.

This lab will guide you through the following essential areas:

- **Explore Microsoft Entra ID User Settings:** Gain a foundational understanding of how user accounts are managed within Microsoft Entra ID, including profile settings, contact information, and organizational relationships.
- **Microsoft Entra self-service password reset (SSPR):** Discover how to empower users to securely reset their own passwords, reducing helpdesk burden and improving user convenience.
- **Microsoft Entra Conditional Access:** Learn how to implement granular access control policies based on various conditions, such as user location, device compliance, and application sensitivity, to enhance security.
- **Explore Privileged Identity Management (PIM):** Understand how to manage, control, and monitor access to important resources within your organization by implementing just-in-time and approval-based privileged access.

LAB: MICROSOFT ENTRA SELF-SERVICE PASSWORD RESET

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of of Microsoft Entra
- Module: Describe the authentication capabilities of Microsoft Entra ID
- Unit: Describe self-service password reset

Lab scenario

In this lab, you, as an admin, will walk through the process of adding a user to the SSPR security group, which is already setup in your Microsoft 365 tenant. With SSPR enabled, you'll then assume the role of a user and go through the process of registering for SSPR and also resetting your password. Lastly, you as the admin, will be able to view audit logs and usage data & insights for SSPR.

Task 1

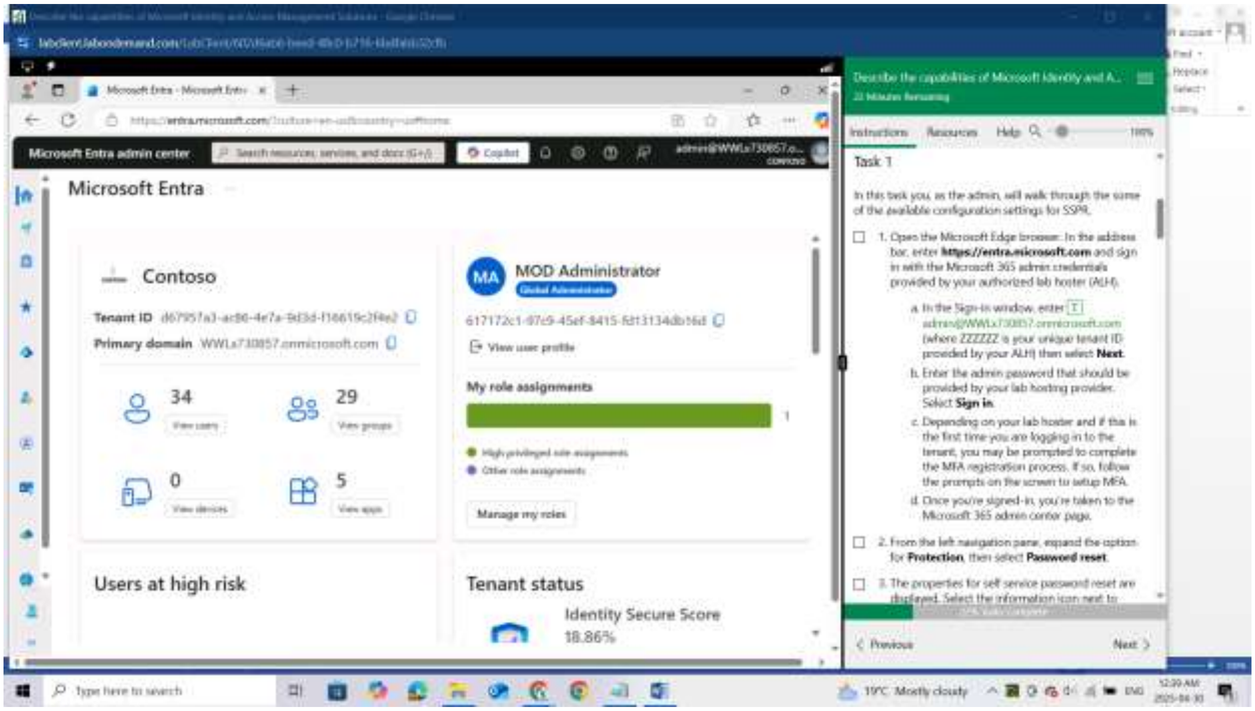
In this task you, as the admin, will walk through the some of the available configuration settings for SSPR.

a) Open the Microsoft Edge browser. In the address bar, enter https://entra.microsoft.com and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).
b) In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your ALH) then select Next.

c) Enter the admin password that should be provided by your lab hosting provider. Select Sign in.

d) Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

Once you're signed-in, you're taken to the Microsoft 365 admin center page.



Task 1

In this task you, as the admin, will walk through the some of the available configuration settings for SSPR.

☐ 1. Open the Microsoft Edge browser. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).

a. In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your ALH) then select **Next**.

b. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.

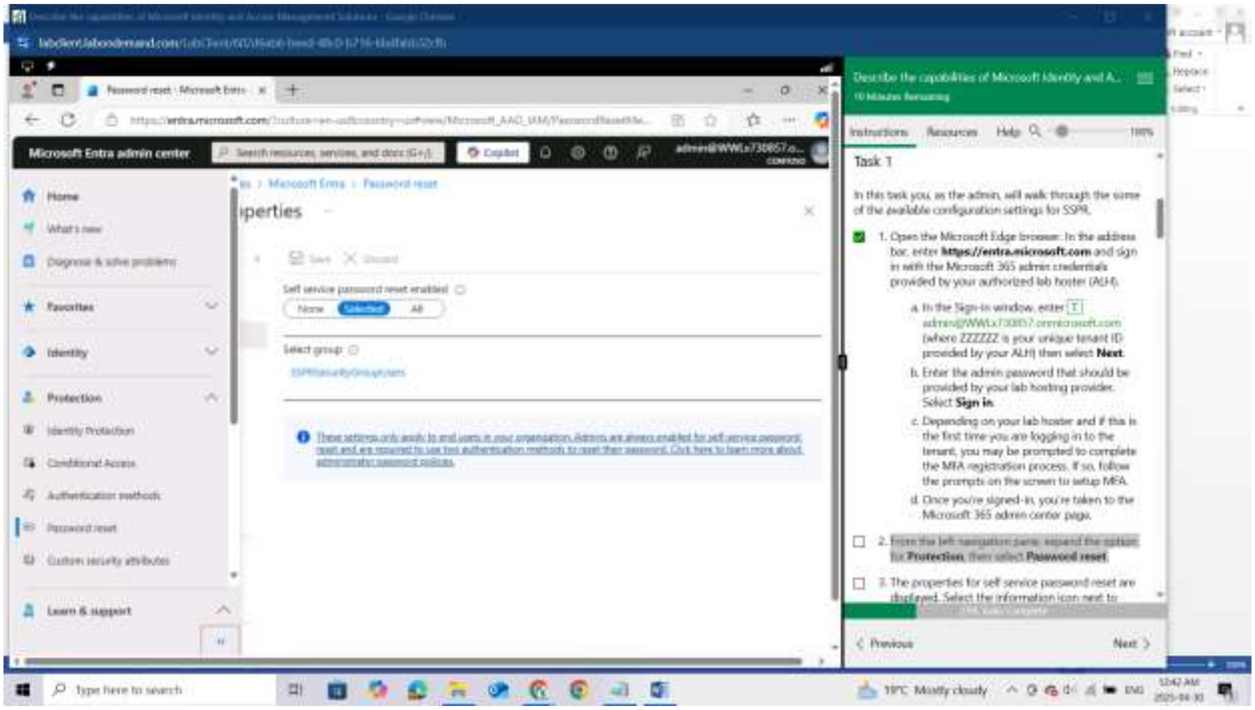
c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.

☐ 2. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.

☐ 3. The properties for self service password reset are displayed. Select the information icon next to

From the left navigation pane, expand the option for **Protection**, then select **Password reset.**



Microsoft Entra admin center

Microsoft Entra > Password reset

Properties

Self service password reset enabled ⓘ

None [✓ Selected] All

Select group ⓘ

SSPRSecurityGroupUsers

ⓘ These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Describe the capabilities of Microsoft Identity and A...

Task 1

In this task you, as the admin, will walk through the some of the available configuration settings for SSPR.

☑ 1. Open the Microsoft Edge browser. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).

   a. In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your ALH) then select **Next**.

   b. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.

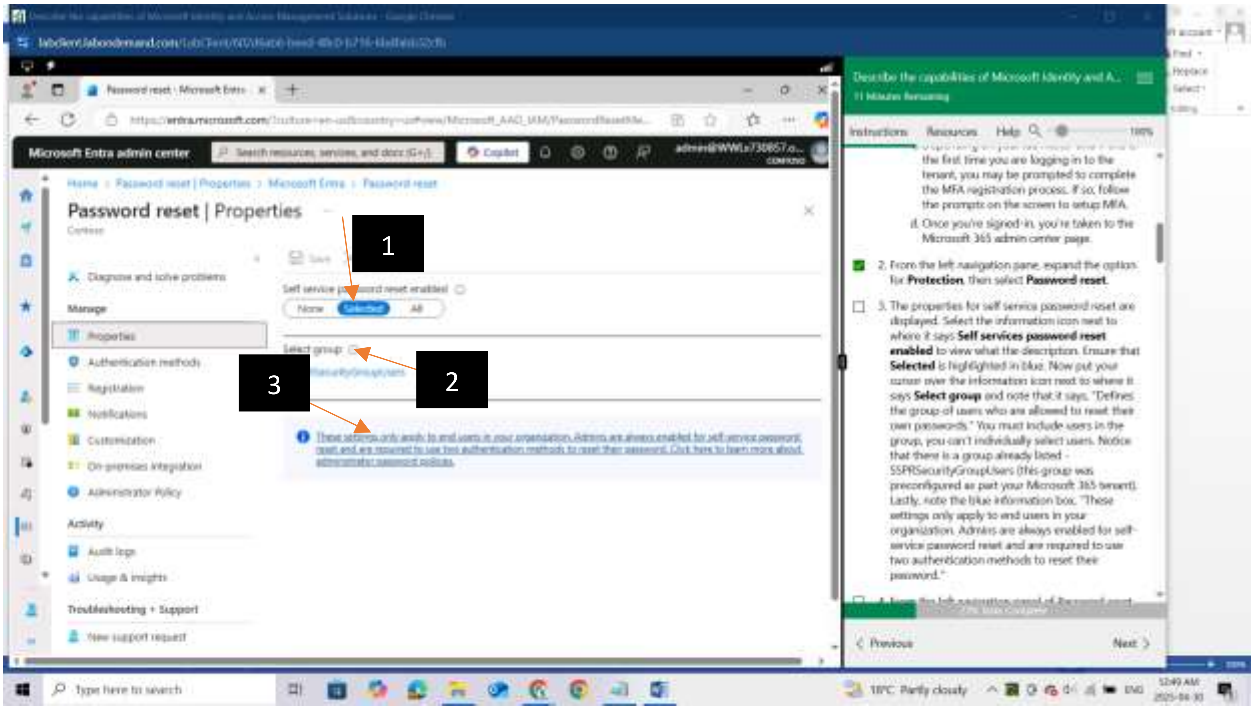
   c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

   d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.

☐ 2. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.

☐ 3. The properties for self service password reset are displayed. Select the information icon next to

The properties for self service password reset are displayed. Select the information icon next to where it says **Self services password reset enabled** to view what the description. Ensure that **Selected** is highlighted in blue. Now put your cursor over the information icon next to where it says Select group and note that it says, "**Defines the group of users who are allowed to reset their own passwords."** You must include users in the group, you can’t individually select users. Notice that there is a group already listed - SSPRSecurityGroupUsers (this group was preconfigured as part your Microsoft 365 tenant). Lastly, note the blue information box, "**These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password."**



Self service password reset enabled ⓘ
None [✓ Selected] All

Select group ⓘ
SSPRSecurityGroupUsers

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

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

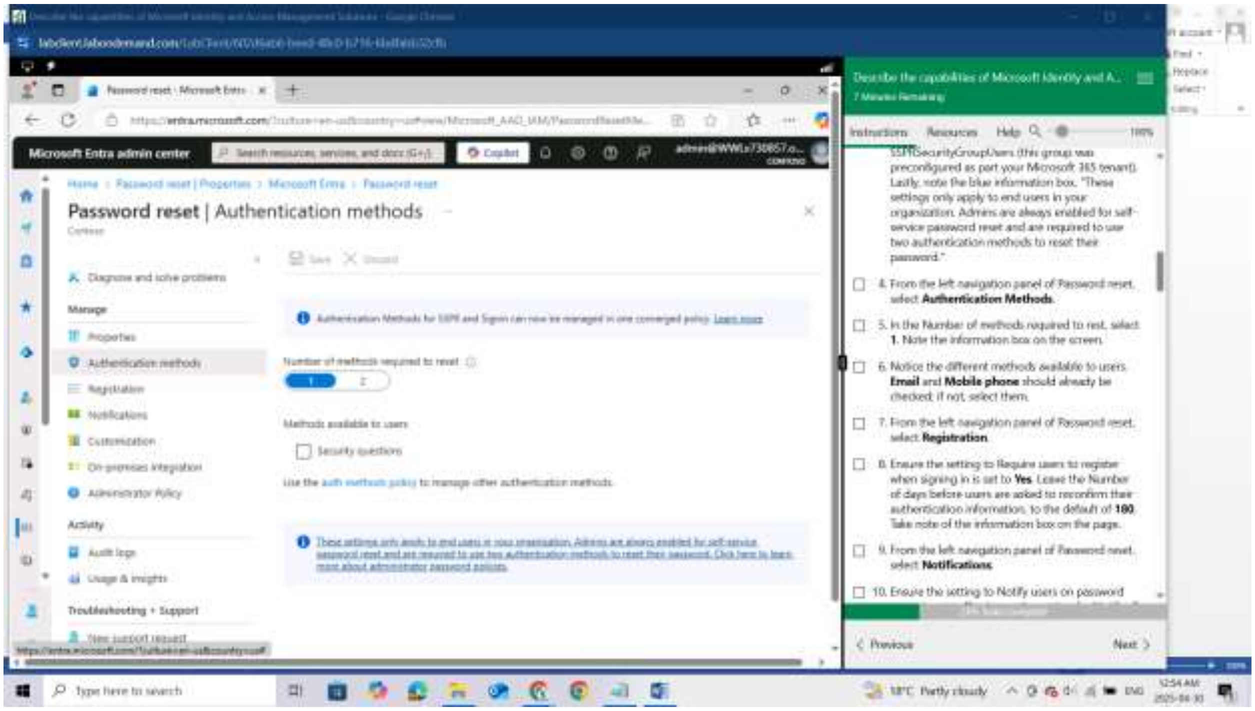
the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.

☑ 2. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.

☐ 3. The properties for self service password reset are displayed. Select the information icon next to where it says **Self services password reset enabled** to view what the description. Ensure that **Selected** is highlighted in blue. Now put your cursor over the information icon next to where it says **Select group** and note that it says, "Defines the group of users who are allowed to reset their own passwords." You must include users in the group, you can't individually select users. Notice that there is a group already listed - SSPRSecurityGroupUsers (this group was preconfigured as part your Microsoft 365 tenant). Lastly, note the blue information box. "These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password."

From the left navigation panel of Password reset, select **Authentication Methods**.



Authentication Methods for SSPR and Signin can now be managed in one converged policy. Learn more

Number of methods required to reset ⓘ
[✓ 1] 2

Methods available to users
☐ Security questions

Use the auth methods policy to manage other authentication methods.

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

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

SSPRSecurityGroupUsers (this group was preconfigured as part your Microsoft 365 tenant). Lastly, note the blue information box. "These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password."

☐ 4. From the left navigation panel of Password reset, select **Authentication Methods**.

☐ 5. In the Number of methods required to rest, select **1**. Note the information box on the screen.

☐ 6. Notice the different methods available to users. **Email** and **Mobile phone** should already be checked; if not, select them.

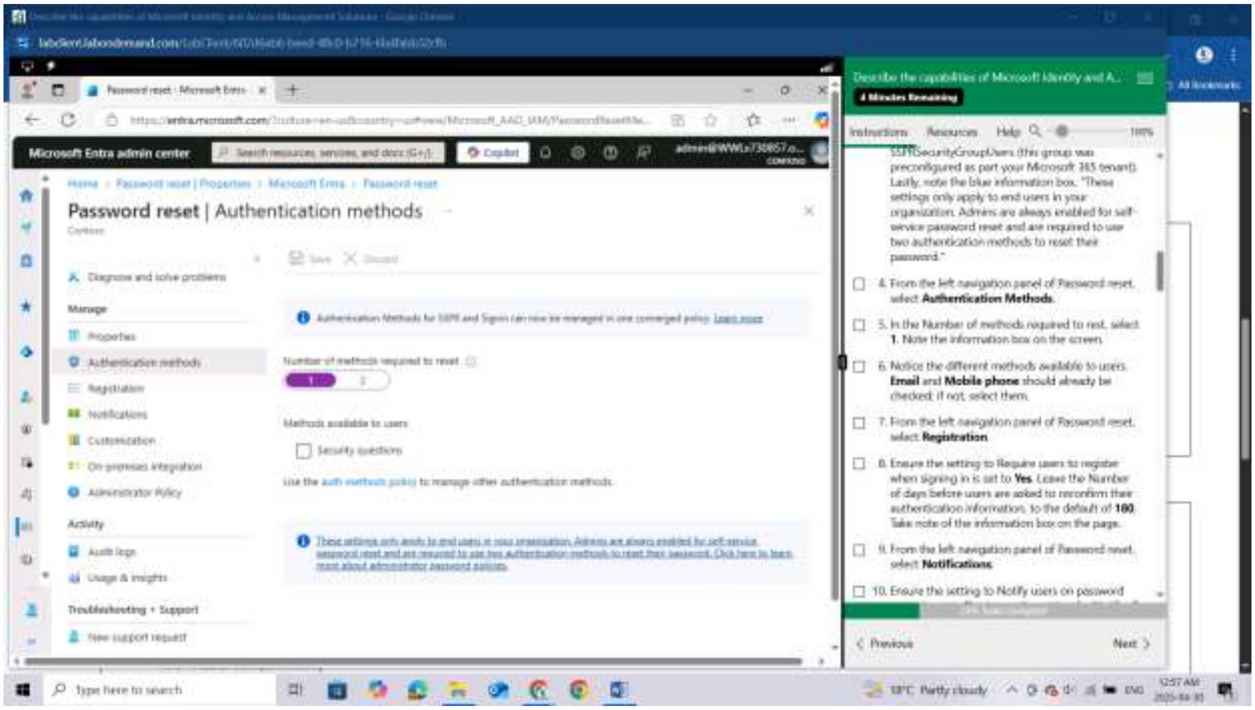
☐ 7. From the left navigation panel of Password reset, select **Registration**.

☐ 8. Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.

☐ 9. From the left navigation panel of Password reset, select **Notifications**.

☐ 10. Ensure the setting to Notify users on password

In the Number of methods required to rest, select **1**. Note the information box on the screen.



Microsoft Entra admin center

Home > Password reset | Properties > Microsoft Entra > Password reset

Password reset | Authentication methods

Contoso

- Diagnose and solve problems
- Manage
  - Properties
  - Authentication methods
  - Registration
  - Notifications
  - Customization
  - On-premises integration
  - Administrator Policy
- Activity
  - Audit logs
  - Usage & insights
- Troubleshooting + Support
  - New support request

Authentication Methods for SSPR and Signin can now be managed in one converged policy. Learn more

Number of methods required to reset: 1 | 2

Methods available to users

□ Security questions

Use the auth methods policy to manage other authentication methods.

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Describe the capabilities of Microsoft Identity and A...

4 Minutes Remaining

SSPRSecurityGroupUsers (this group was preconfigured as part your Microsoft 365 tenant). Lastly, note the blue information box. "These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password."

□ 4. From the left navigation panel of Password reset, select **Authentication Methods**.

□ 5. In the Number of methods required to rest, select **1**. Note the information box on the screen.

□ 6. Notice the different methods available to users. **Email** and **Mobile phone** should already be checked; if not, select them.

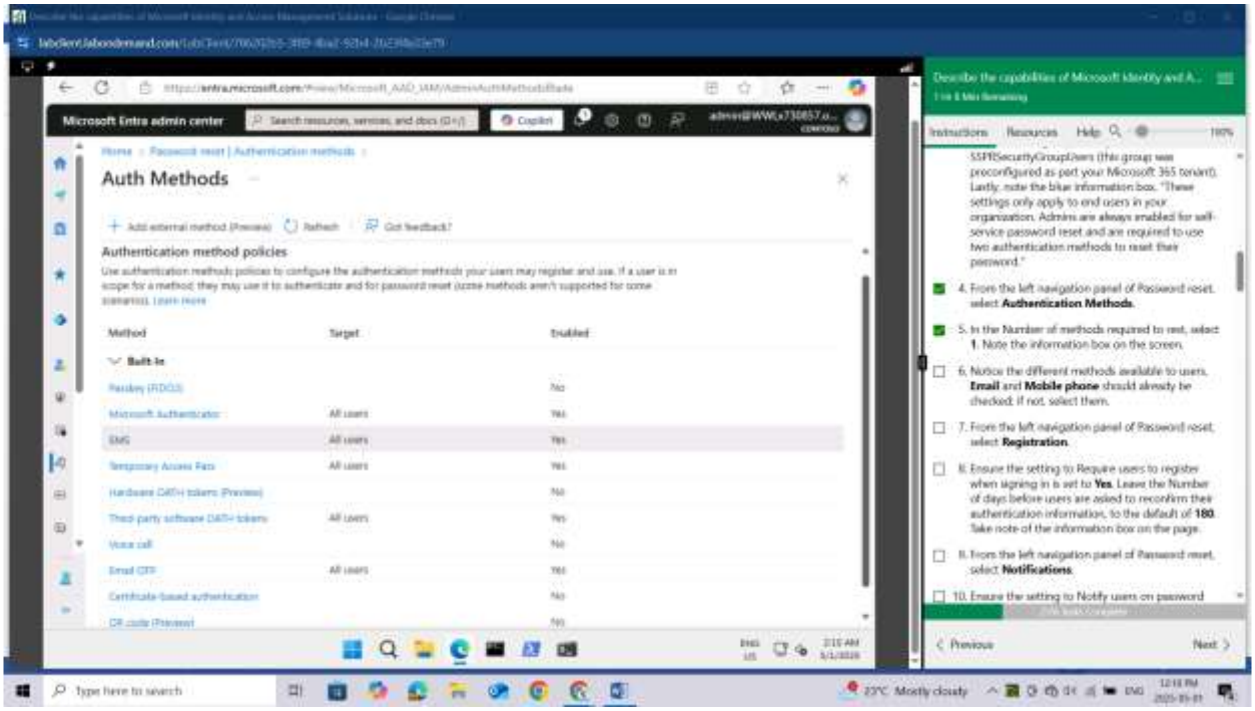
□ 7. From the left navigation panel of Password reset, select **Registration**.

□ 8. Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.

□ 9. From the left navigation panel of Password reset, select **Notifications**.

□ 10. Ensure the setting to Notify users on password

Notice the different methods available to users. **Email** and **Mobile phone** should already be checked; if not, select them.



Microsoft Entra admin center

Home > Password reset | Authentication methods >

Auth Methods

+ Add external method (Preview) | Refresh | Got feedback?

Authentication method policies

Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more

Method	Target	Enabled
Built-In		
Passkey (FIDO2)		No
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Third-party software OATH tokens	All users	Yes
Voice call		No
Email OTP	All users	Yes
Certificate-based authentication		No
QR code (Preview)		No

SSPRSecurityGroupUsers (this group was preconfigured as part your Microsoft 365 tenant). Lastly, note the blue information box. "These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password."

☑ 4. From the left navigation panel of Password reset, select **Authentication Methods**.

☑ 5. In the Number of methods required to rest, select **1**. Note the information box on the screen.

□ 6. Notice the different methods available to users. **Email** and **Mobile phone** should already be checked; if not, select them.

□ 7. From the left navigation panel of Password reset, select **Registration**.

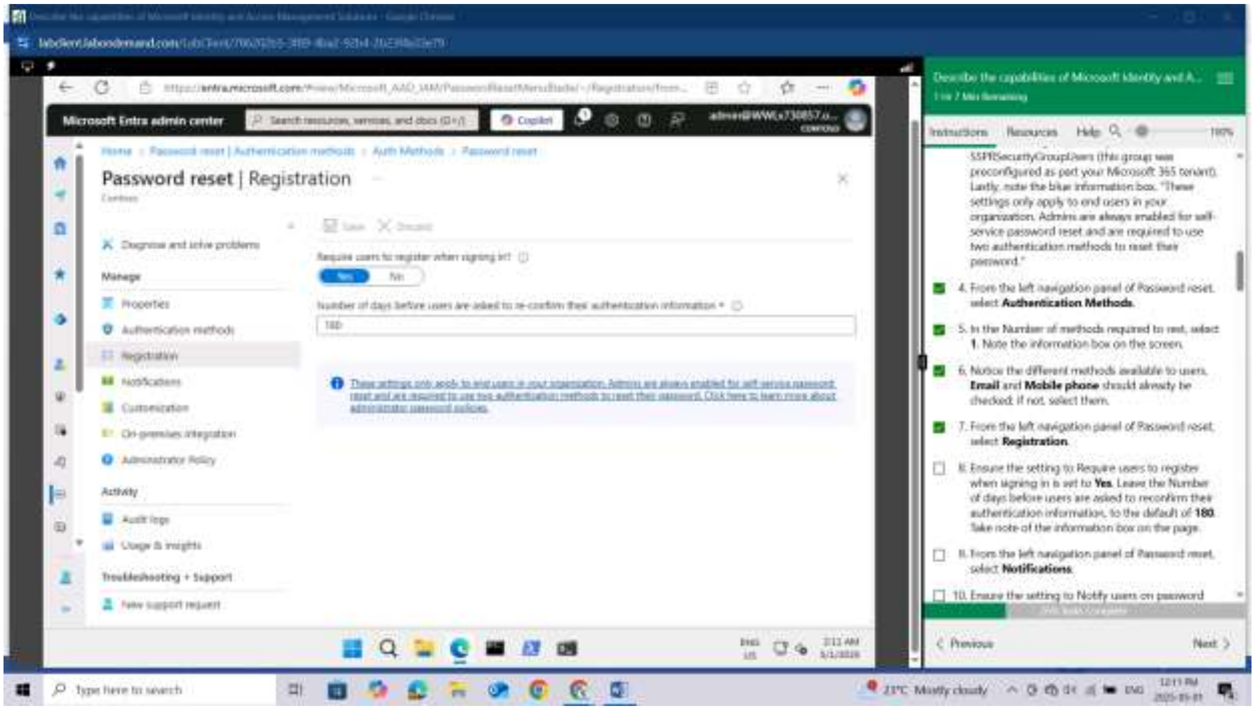
□ 8. Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.

□ 9. From the left navigation panel of Password reset, select **Notifications**.

□ 10. Ensure the setting to Notify users on password

From the left navigation panel of Password reset, select **Registration**.

Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.



Password reset | Registration

Require users to register when signing in? ● Yes ○ No

Number of days before users are asked to re-confirm their authentication information * 180

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

SSPRSecurityGroupUsers (this group was preconfigured as part your Microsoft 365 tenant). Lastly, note the blue information box. "These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password."

☑ 4. From the left navigation panel of Password reset, select **Authentication Methods**.

☑ 5. In the Number of methods required to rest, select **1**. Note the information box on the screen.

☑ 6. Notice the different methods available to users. **Email** and **Mobile phone** should already be checked; if not, select them.

☑ 7. From the left navigation panel of Password reset, select **Registration**.

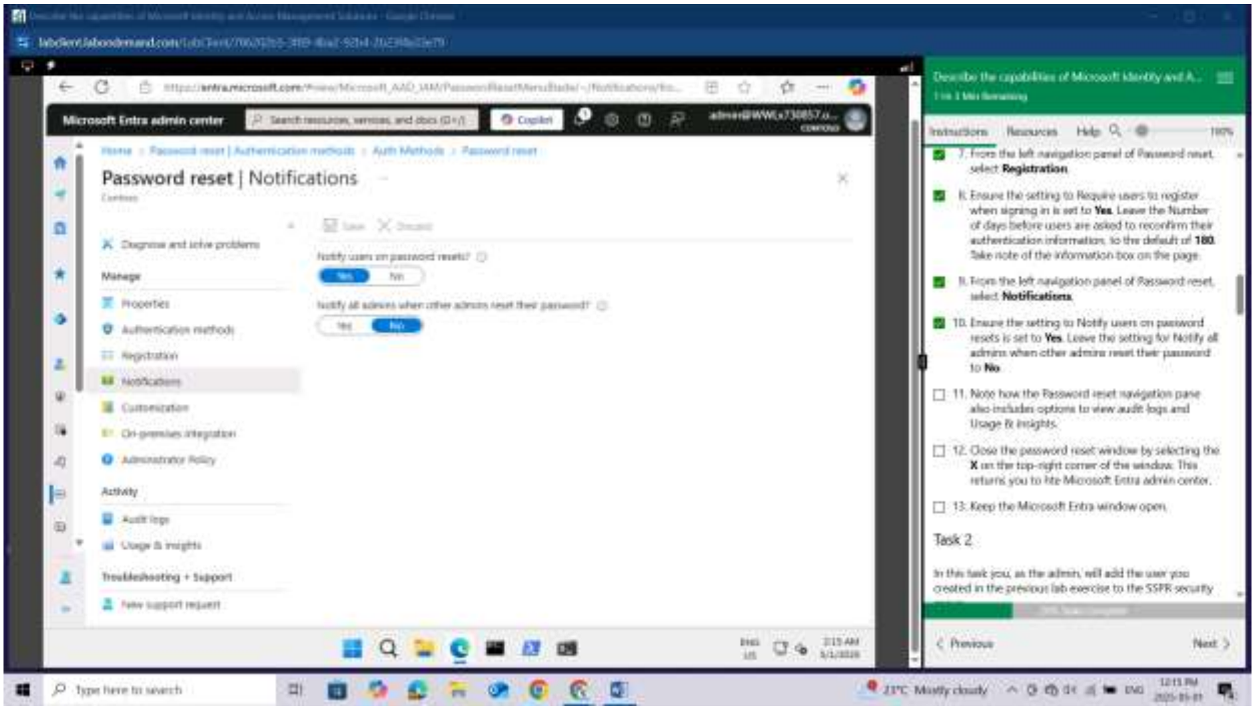
□ 8. Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.

□ 9. From the left navigation panel of Password reset, select **Notifications**.

□ 10. Ensure the setting to Notify users on password

From the left navigation panel of Password reset, select **Notifications**.

Ensure the setting to Notify users on password resets is set to **Yes**. Leave the setting for Notify all admins when other admins reset their password to **No**.



Password reset | Notifications

Notify users on password resets? ● Yes ○ No

Notify all admins when other admins reset their password? ○ Yes ● No

☑ 7. From the left navigation panel of Password reset, select **Registration**.

☑ 8. Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.

☑ 9. From the left navigation panel of Password reset, select **Notifications**.

☑ 10. Ensure the setting to Notify users on password resets is set to **Yes**. Leave the setting for Notify all admins when other admins reset their password to **No**.

□ 11. Note how the Password reset navigation pane also includes options to view audit logs and Usage & insights.

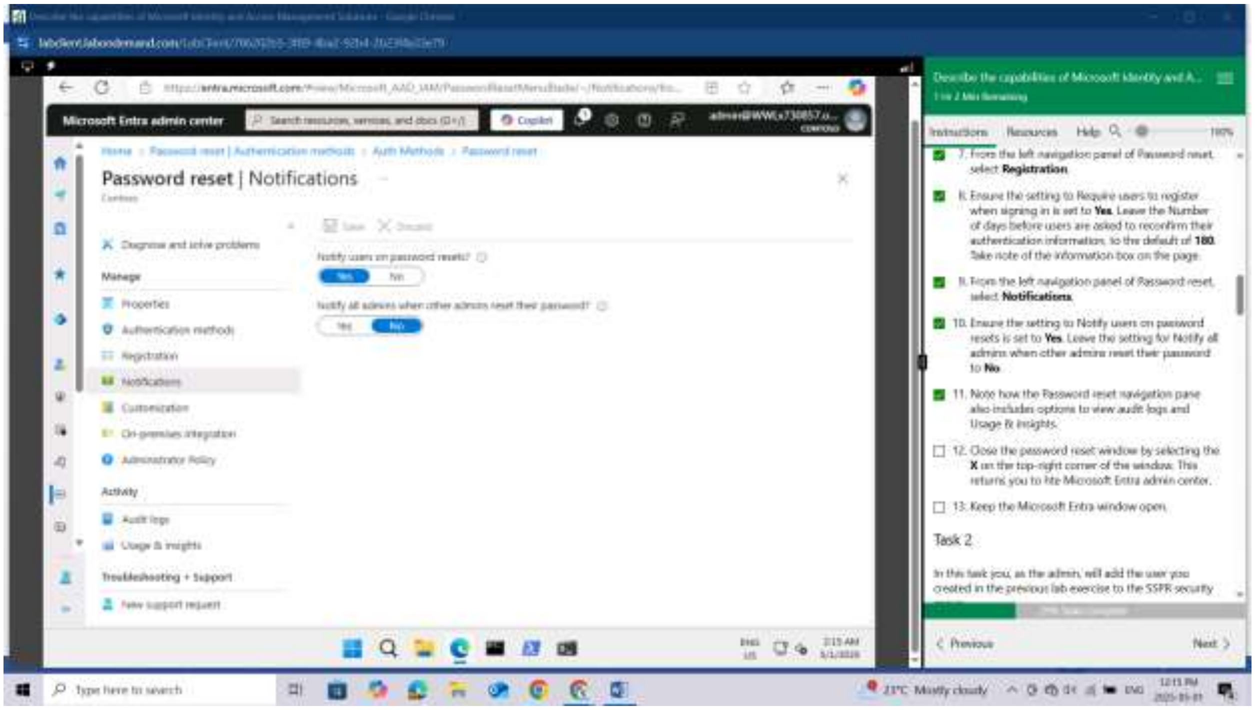
□ 12. Close the password reset window by selecting the **X** on the top-right corner of the window. This returns you to hte Microsoft Entra admin center.

□ 13. Keep the Microsoft Entra window open.

Task 2

In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security

Note how the Password reset navigation pane also includes options to view audit logs and Usage & insights.



Microsoft Entra admin center

Home > Password reset | Authentication methods > Auth Methods > Password reset

Password reset | Notifications

Contoso

- Diagnose and solve problems
- Manage
  - Properties
  - Authentication methods
  - Registration
  - Notifications
  - Customization
  - On-premises integration
  - Administrator Policy
- Activity
  - Audit logs
  - Usage & insights
- Troubleshooting + Support
  - New support request

Save | Discard

Notify users on password resets? [✓ Yes] No

Notify all admins when other admins reset their password? Yes [✓ No]

Describe the capabilities of Microsoft Identity and A...

Instructions | Resources | Help

☑ 7. From the left navigation panel of Password reset, select **Registration**.

☑ 8. Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.

☑ 9. From the left navigation panel of Password reset, select **Notifications**.

☑ 10. Ensure the setting to Notify users on password resets is set to **Yes**. Leave the setting for Notify all admins when other admins reset their password to **No**.

☑ 11. Note how the Password reset navigation pane also includes options to view audit logs and Usage & insights.

□ 12. Close the password reset window by selecting the **X** on the top-right corner of the window. This returns you to hte Microsoft Entra admin center.

□ 13. Keep the Microsoft Entra window open.

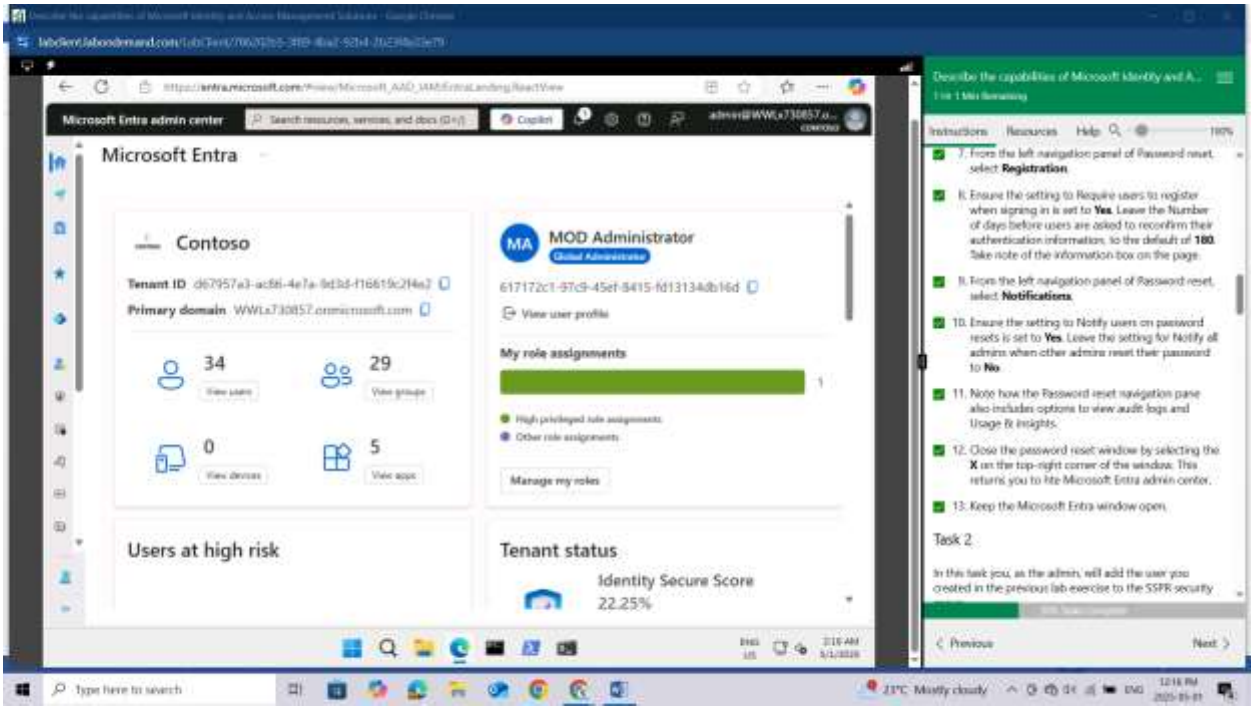
Task 2

In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security

‹ Previous | Next ›

Close the password reset window by selecting the X on the top-right corner of the window. This returns you to the Microsoft Entra admin center.

Keep the Microsoft Entra window open.



Microsoft Entra admin center

Microsoft Entra

Contoso

Tenant ID d67957a3-ac8-4e7a-9d3d-f16619c2f4e2

Primary domain WWLx730857.onmicrosoft.com

34 View users	29 View groups
0 View devices	5 View apps

MOD Administrator

Global Administrator

617172c1-97c9-45ef-8415-fd13134db16d

View user profile

My role assignments

- High privileged role assignments
- Other role assignments

Manage my roles

Users at high risk

Tenant status

Identity Secure Score 22.25%

Describe the capabilities of Microsoft Identity and A...

Instructions | Resources | Help

☑ 7. From the left navigation panel of Password reset, select **Registration**.

☑ 8. Ensure the setting to Require users to register when signing in is set to **Yes**. Leave the Number of days before users are asked to reconfirm their authentication information, to the default of **180**. Take note of the information box on the page.

☑ 9. From the left navigation panel of Password reset, select **Notifications**.

☑ 10. Ensure the setting to Notify users on password resets is set to **Yes**. Leave the setting for Notify all admins when other admins reset their password to **No**.

☑ 11. Note how the Password reset navigation pane also includes options to view audit logs and Usage & insights.

☑ 12. Close the password reset window by selecting the **X** on the top-right corner of the window. This returns you to hte Microsoft Entra admin center.

☑ 13. Keep the Microsoft Entra window open.

Task 2

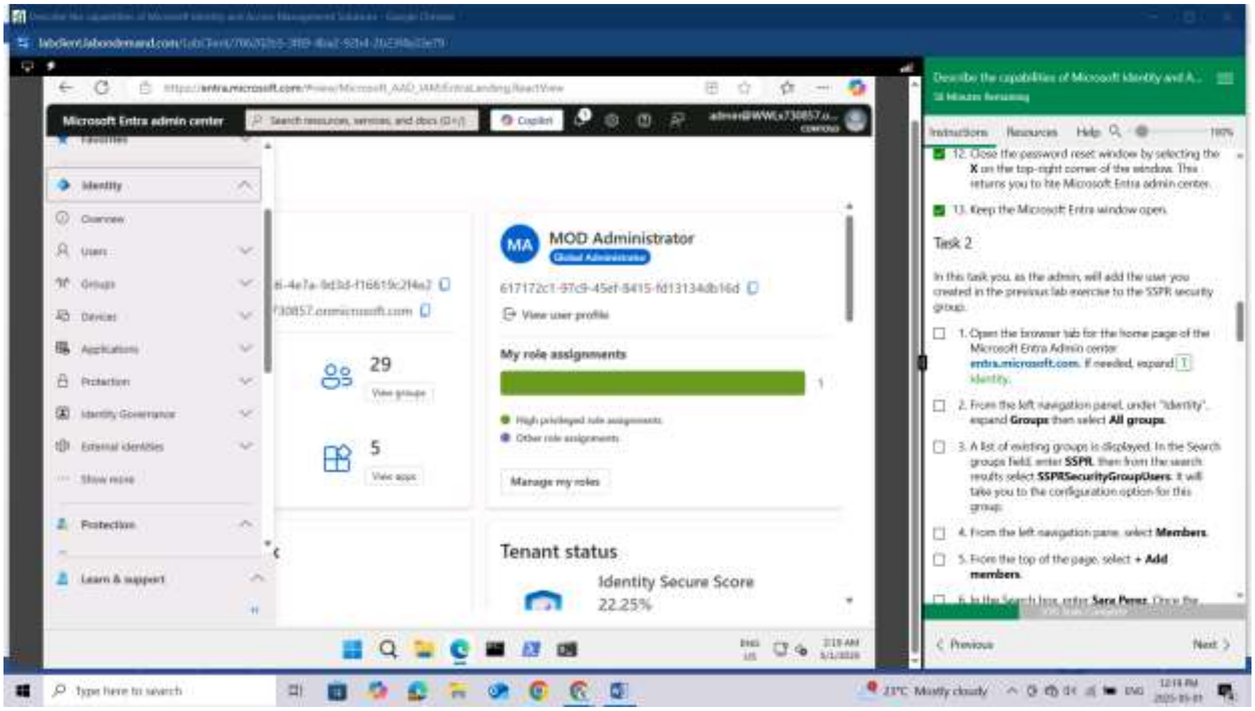
In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security

‹ Previous | Next ›

Task 2

In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security group.

Open the browser tab for the home page of the Microsoft Entra Admin center entra.microsoft.com. If needed, expand Identity.



Microsoft Entra admin center

Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Governance
External identities
Show more
Protection
Learn & support

MOD Administrator
Global Administrator
617172c1-97c9-45ef-8415-fd13134db16d
View user profile

29 View groups
5 View apps

My role assignments
● High privileged role assignments
● Other role assignments
Manage my roles

Tenant status
Identity Secure Score 22.25%

Describe the capabilities of Microsoft Identity and A...

Instructions Resources Help

☑ 12. Close the password reset window by selecting the **X** on the top-right corner of the window. This returns you to hte Microsoft Entra admin center.

☑ 13. Keep the Microsoft Entra window open.

Task 2

In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security group.

□ 1. Open the browser tab for the home page of the Microsoft Entra Admin center entra.microsoft.com. If needed, expand Identity.

□ 2. From the left navigation panel, under "Identity", expand **Groups** then select **All groups**.

□ 3. A list of existing groups is displayed. In the Search groups field, enter **SSPR**, then from the search results select **SSPRSecurityGroupUsers**. It will take you to the configuration option for this group.

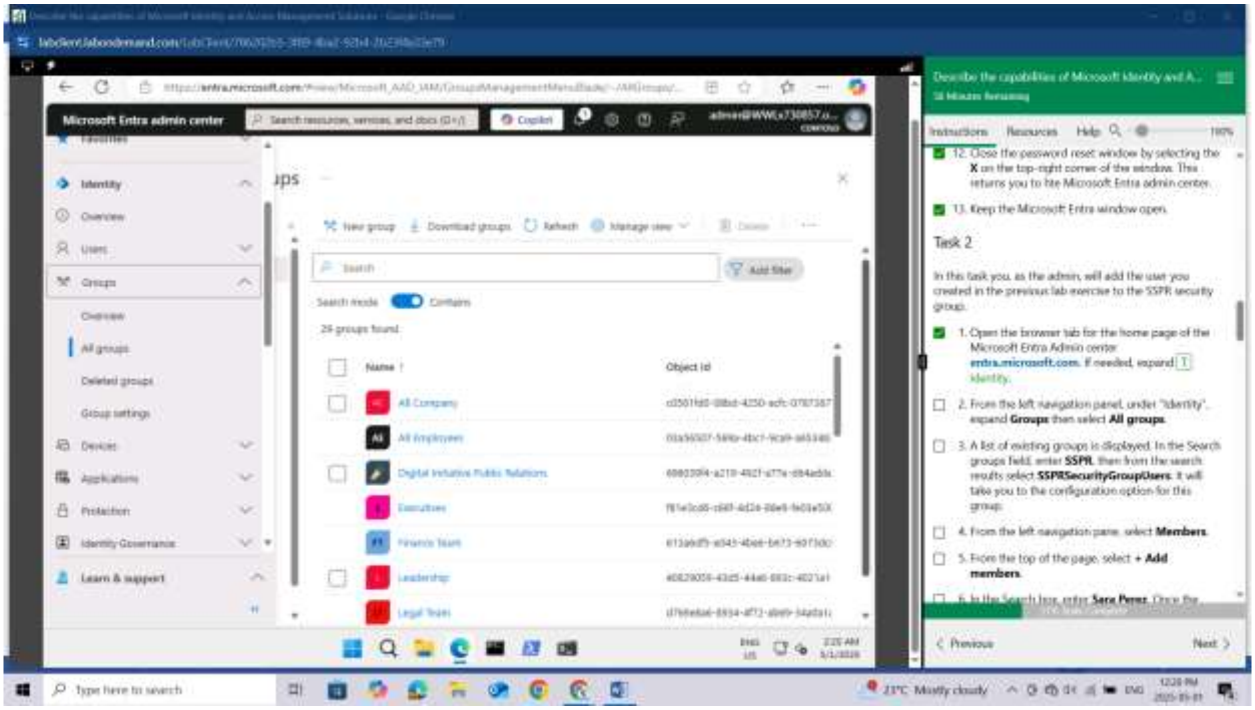
□ 4. From the left navigation pane, select **Members**.

□ 5. From the top of the page, select **+ Add members**.

□ 6. In the Search box, enter **Sara Perez**. Once the...

< Previous Next >

From the left navigation panel, under "Identity", expand **Groups** then select **All groups.**



Microsoft Entra admin center

Identity
Overview
Users
Groups
Overview
All groups
Deleted groups
Group settings
Devices
Applications
Protection
Identity Governance
Learn & support

New group | Download groups | Refresh | Manage view | Delete

Search mode Contains

29 groups found

Name	Object Id
All Company	c0501fd0-08bd-4250-acfc-0787387
All Employees	[illegible]
Digital Initiative Public Relations	[illegible]
Executives	[illegible]
Finance Team	[illegible]
Leadership	[illegible]
Legal Team	[illegible]

Describe the capabilities of Microsoft Identity and A...

Instructions Resources Help

☑ 12. Close the password reset window by selecting the **X** on the top-right corner of the window. This returns you to hte Microsoft Entra admin center.

☑ 13. Keep the Microsoft Entra window open.

Task 2

In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security group.

☑ 1. Open the browser tab for the home page of the Microsoft Entra Admin center entra.microsoft.com. If needed, expand Identity.

□ 2. From the left navigation panel, under "Identity", expand **Groups** then select **All groups**.

□ 3. A list of existing groups is displayed. In the Search groups field, enter **SSPR**, then from the search results select **SSPRSecurityGroupUsers**. It will take you to the configuration option for this group.

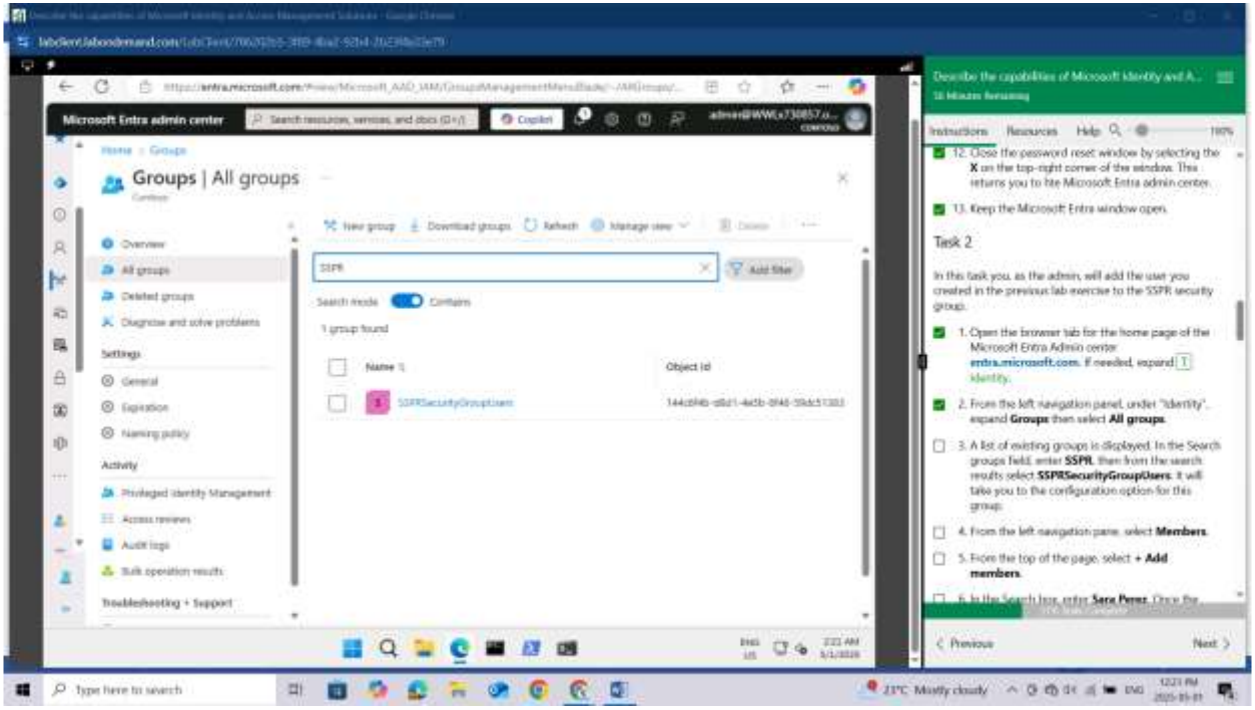
□ 4. From the left navigation pane, select **Members**.

□ 5. From the top of the page, select **+ Add members**.

□ 6. In the Search box, enter **Sara Perez**. Once the...

< Previous Next >

A list of existing groups is displayed. In the Search groups field, enter SSPR, then from the search results select SSPRSecurityGroupUsers.



SSPR

Search mode: Contains

1 group found

Name	Object Id
SSPRSecurityGroupUsers	144c6f4b-d8d1-4e5b-8f46-59dc51383

Describe the capabilities of Microsoft Identity and A...

12. Close the password reset window by selecting the **X** on the top-right corner of the window. This returns you to hte Microsoft Entra admin center.

13. Keep the Microsoft Entra window open.

Task 2

In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security group.

1. Open the browser tab for the home page of the Microsoft Entra Admin center entra.microsoft.com. If needed, expand Identity.

2. From the left navigation panel, under "Identity", expand **Groups** then select **All groups**.

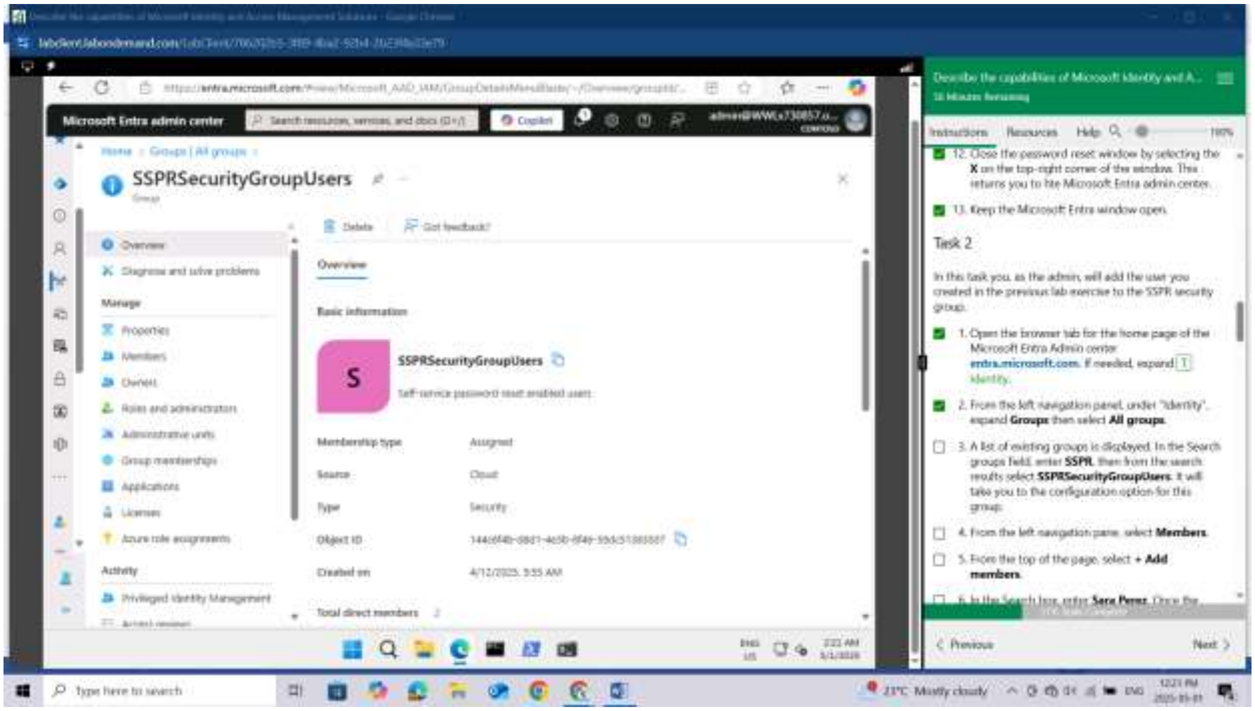
3. A list of existing groups is displayed. In the Search groups field, enter **SSPR**, then from the search results select **SSPRSecurityGroupUsers**. It will take you to the configuration option for this group.

4. From the left navigation pane, select **Members**.

5. From the top of the page, select **+ Add members**.

6. In the Search box, enter **Sara Perez**. Once the ...

It will take you to the configuration option for this group.



SSPRSecurityGroupUsers

Group

Overview

Basic information

SSPRSecurityGroupUsers

Self-service password reset enabled users

Membership type	Assigned
Source	Cloud
Type	Security
Object ID	144c6f4b-d8d1-4e5b-8f46-59dc51383587
Created on	4/12/2025, 3:55 AM
Total direct members	2

Describe the capabilities of Microsoft Identity and A...

12. Close the password reset window by selecting the **X** on the top-right corner of the window. This returns you to hte Microsoft Entra admin center.

13. Keep the Microsoft Entra window open.

Task 2

In this task you, as the admin, will add the user you created in the previous lab exercise to the SSPR security group.

1. Open the browser tab for the home page of the Microsoft Entra Admin center entra.microsoft.com. If needed, expand Identity.

2. From the left navigation panel, under "Identity", expand **Groups** then select **All groups**.

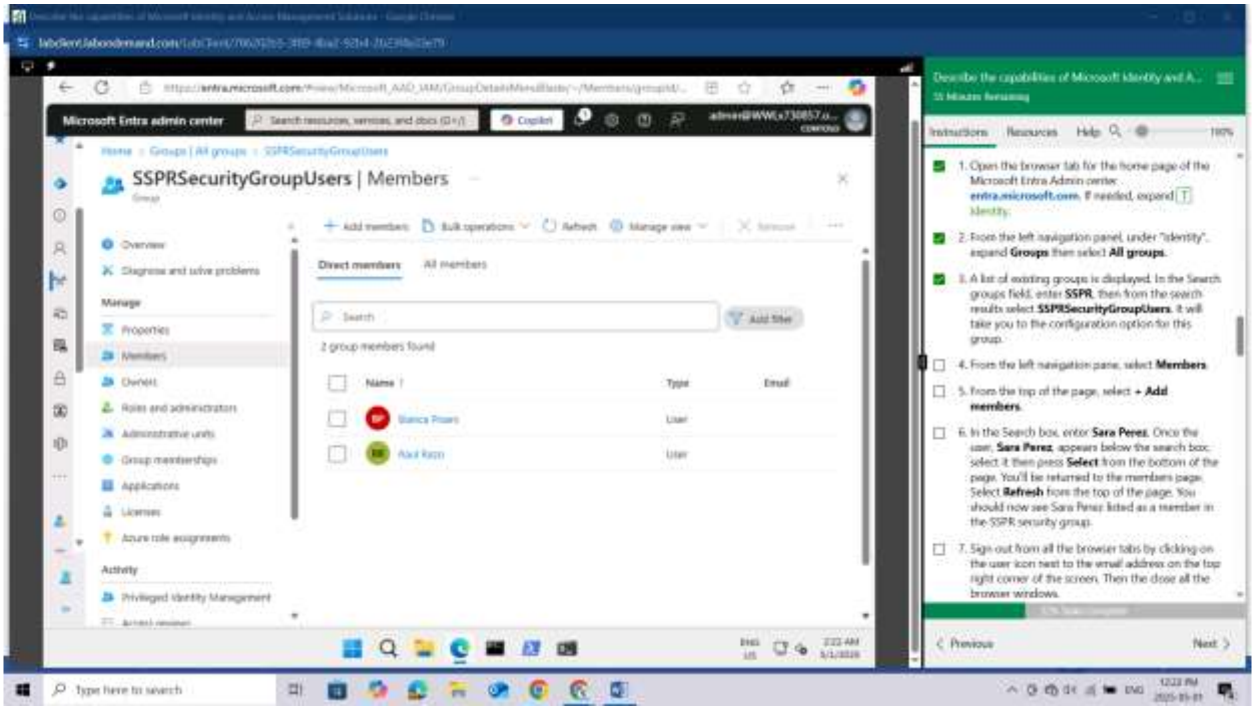
3. A list of existing groups is displayed. In the Search groups field, enter **SSPR**, then from the search results select **SSPRSecurityGroupUsers**. It will take you to the configuration option for this group.

4. From the left navigation pane, select **Members**.

5. From the top of the page, select **+ Add members**.

6. In the Search box, enter **Sara Perez**. Once the ...

From the left navigation pane, select Members.



SSPRSecurityGroupUsers | Members

Group

2 group members found

☐	Name ↑	Type	Email
☐	Bianca Pisani	User	
☐	Raul Razo	User	

Describe the capabilities of Microsoft Identity and A...

55 Minutes Remaining

☑ 1. Open the browser tab for the home page of the Microsoft Entra Admin center: **entra.microsoft.com**. If needed, expand Identity.

☑ 2. From the left navigation panel, under "Identity", expand **Groups** then select **All groups**.

☑ 3. A list of existing groups is displayed. In the Search groups field, enter **SSPR**, then from the search results select **SSPRSecurityGroupUsers**. It will take you to the configuration option for this group.

☐ 4. From the left navigation pane, select **Members**.

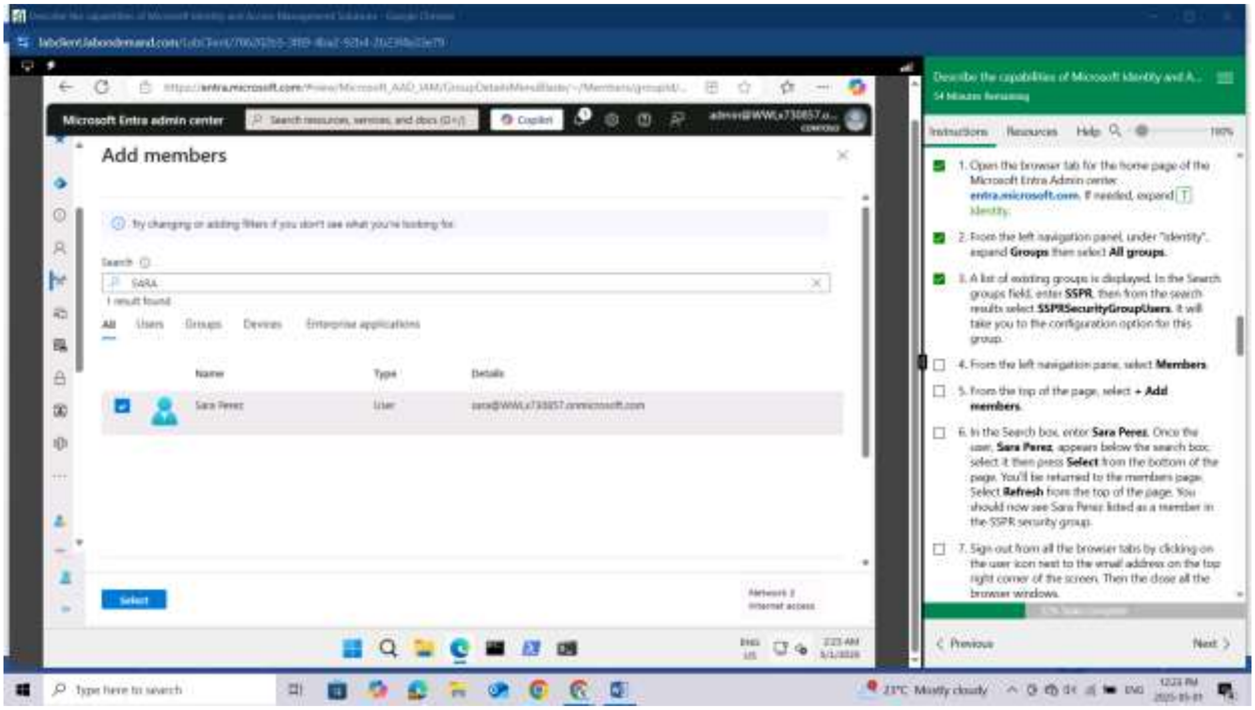
☐ 5. From the top of the page, select **+ Add members**.

☐ 6. In the Search box, enter **Sara Perez**. Once the user, **Sara Perez**, appears below the search box, select it then press **Select** from the bottom of the page. You'll be returned to the members page. Select **Refresh** from the top of the page. You should now see Sara Perez listed as a member in the SSPR security group.

☐ 7. Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.

From the top of the page, select + Add members.

In the Search box, enter Sara Perez. Once the user, Sara Perez, appears below the search box, select it then press Select from the bottom of the page.



Add members

Try changing or adding filters if you don't see what you're looking for.

Search: SARA

1 result found

		Name	Type	Details
☑		Sara Perez	User	sara@WWLx730857.onmicrosoft.com

Describe the capabilities of Microsoft Identity and A...

54 Minutes Remaining

☑ 1. Open the browser tab for the home page of the Microsoft Entra Admin center: **entra.microsoft.com**. If needed, expand Identity.

☑ 2. From the left navigation panel, under "Identity", expand **Groups** then select **All groups**.

☑ 3. A list of existing groups is displayed. In the Search groups field, enter **SSPR**, then from the search results select **SSPRSecurityGroupUsers**. It will take you to the configuration option for this group.

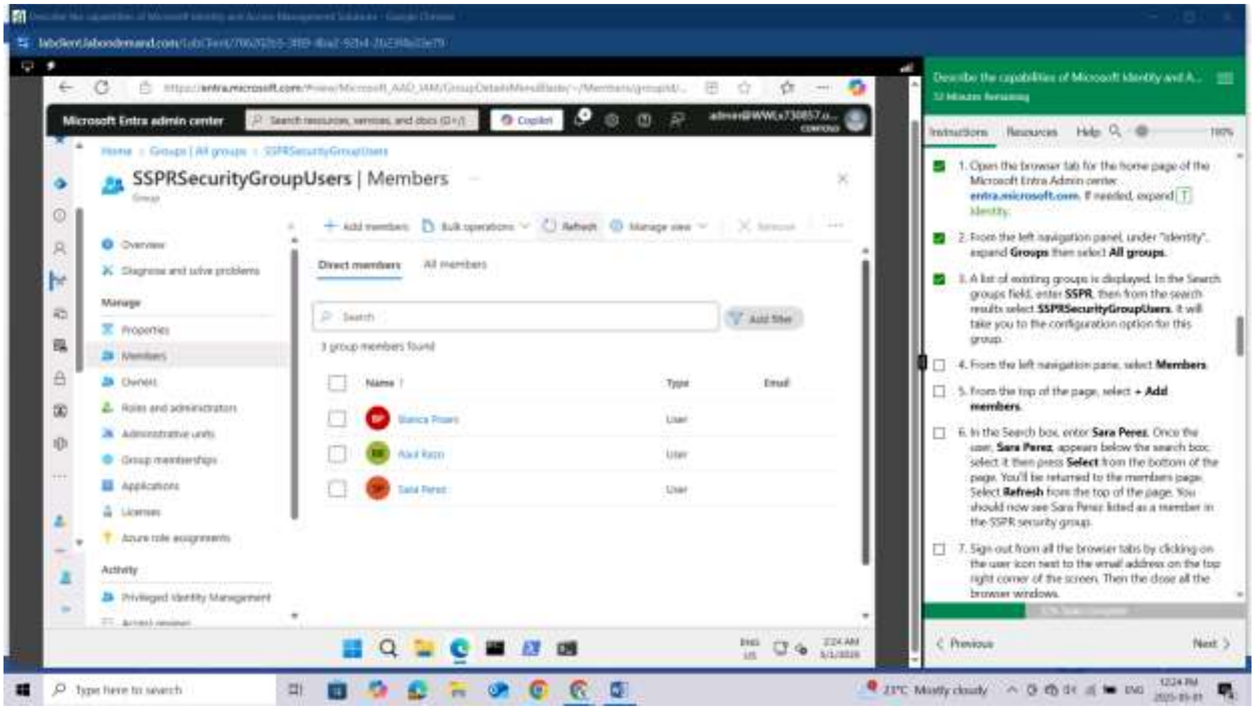
☐ 4. From the left navigation pane, select **Members**.

☐ 5. From the top of the page, select **+ Add members**.

☐ 6. In the Search box, enter **Sara Perez**. Once the user, **Sara Perez**, appears below the search box, select it then press **Select** from the bottom of the page. You'll be returned to the members page. Select **Refresh** from the top of the page. You should now see Sara Perez listed as a member in the SSPR security group.

☐ 7. Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.

You'll be returned to the members page. Select Refresh from the top of the page. You should now see Sara Perez listed as a member in the SSPR security group.


Describe the capabilities of Microsoft Identity and A...

SSPRSecurityGroupUsers | Members

3 group members found

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

☑ 1. Open the browser tab for the home page of the Microsoft Entra Admin center **entra.microsoft.com**. If needed, expand Identity.

☑ 2. From the left navigation panel, under "Identity", expand **Groups** then select **All groups**.

☑ 3. A list of existing groups is displayed. In the Search groups field, enter **SSPR**, then from the search results select **SSPRSecurityGroupUsers**. It will take you to the configuration option for this group.

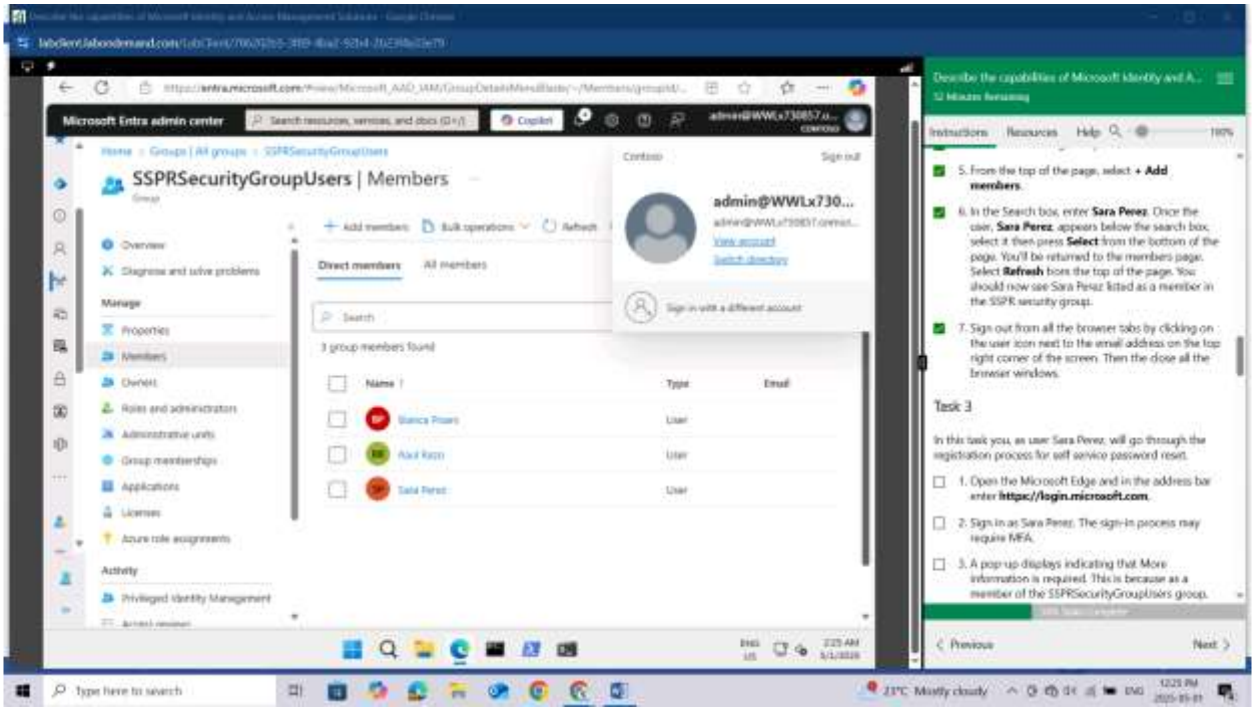
□ 4. From the left navigation pane, select **Members**.

□ 5. From the top of the page, select **+ Add members**.

□ 6. In the Search box, enter **Sara Perez**. Once the user, **Sara Perez**, appears below the search box, select it then press **Select** from the bottom of the page. You'll be returned to the members page. Select **Refresh** from the top of the page. You should now see Sara Perez listed as a member in the SSPR security group.

□ 7. Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.

Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.


SSPRSecurityGroupUsers | Members

admin@WWLx730...

Sign out

View account

Switch directory

Sign in with a different account

☑ 5. From the top of the page, select **+ Add members**.

☑ 6. In the Search box, enter **Sara Perez**. Once the user, **Sara Perez**, appears below the search box, select it then press **Select** from the bottom of the page. You'll be returned to the members page. Select **Refresh** from the top of the page. You should now see Sara Perez listed as a member in the SSPR security group.

☑ 7. Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.

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**.

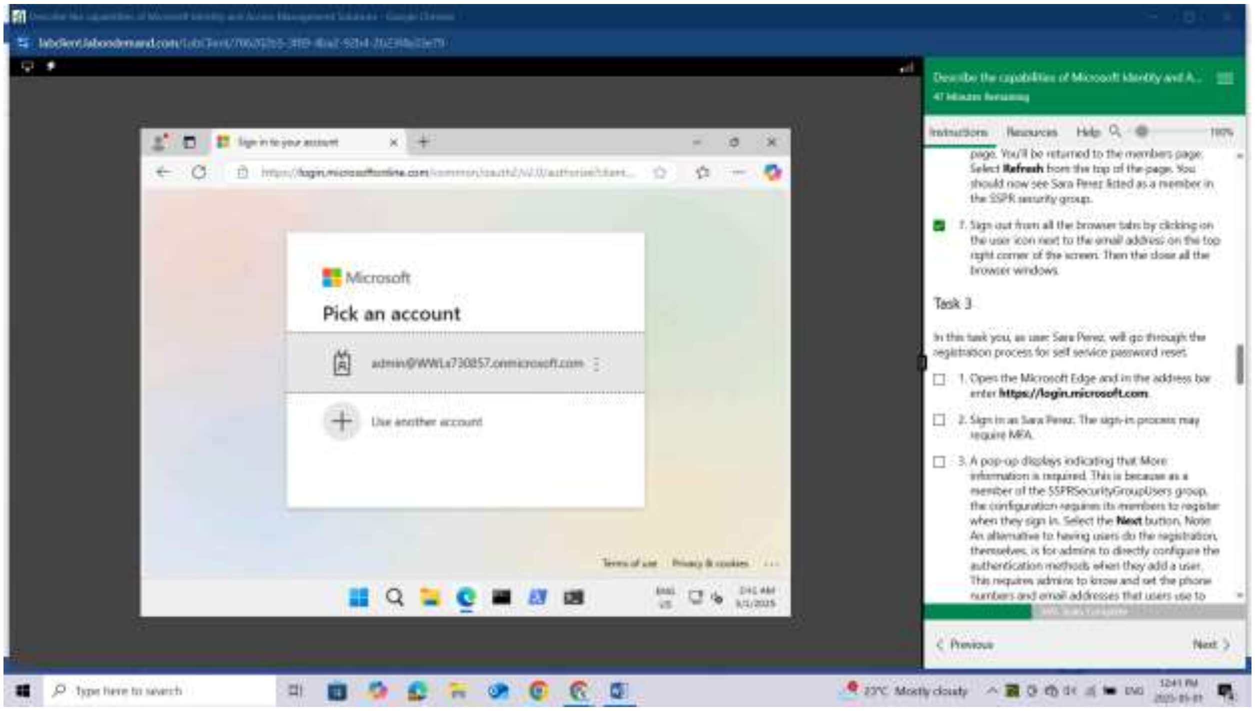
□ 2. Sign in as Sara Perez. The sign-in process may require MFA.

□ 3. A pop-up displays indicating that More information is required. This is because as a member of the SSPRSecurityGroupUsers group.

Task 3

In this task you, as user Sara Perez, will go through the registration process for self service password reset.

Open the Microsoft Edge and in the address bar enter https://login.microsoft.com.


Describe the capabilities of Microsoft Identity and A...

47 Minutes Remaining

page. You'll be returned to the members page. Select **Refresh** from the top of the page. You should now see Sara Perez listed as a member in the SSPR security group.

☑ 7. Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.

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.

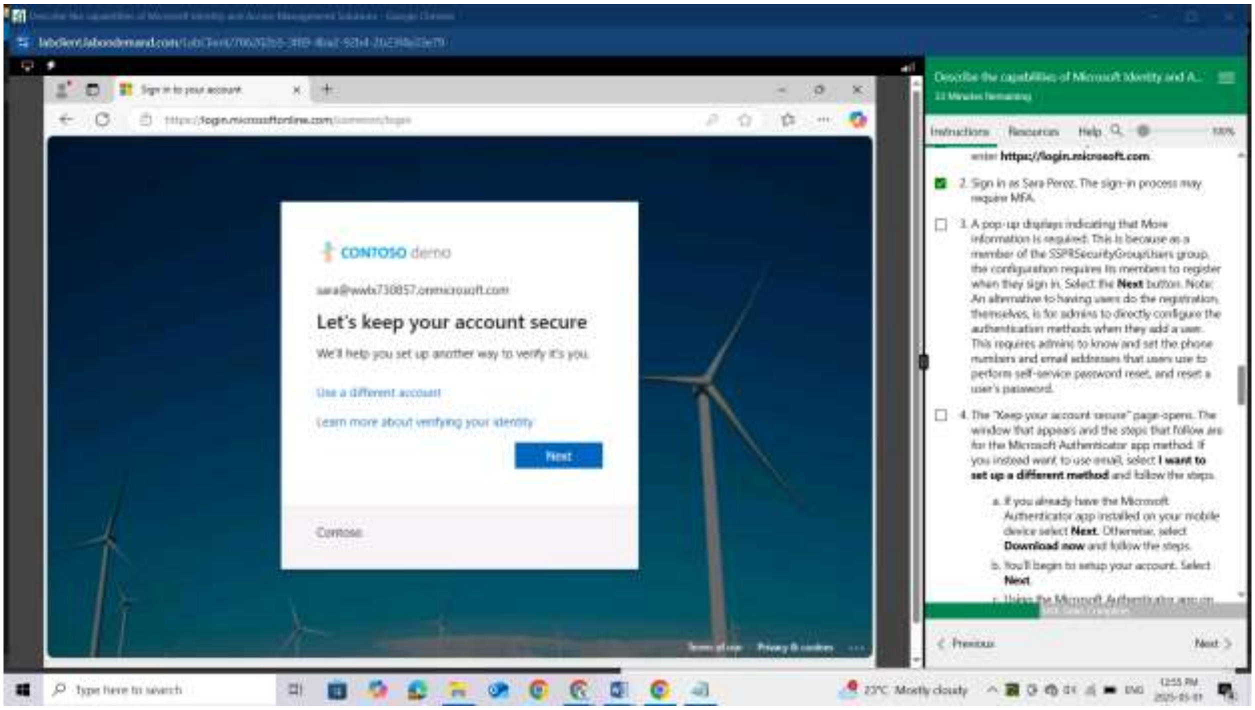
☐ 3. A pop-up displays indicating that More information is required. This is because as a member of the SSPRSecurityGroupUsers group, the configuration requires its members to register when they sign in. Select the **Next** button. Note: An alternative to having users do the registration, themselves, is for admins to directly configure the authentication methods when they add a user. This requires admins to know and set the phone numbers and email addresses that users use to

Microsoft

Pick an account

admin@WWLx730857.onmicrosoft.com

Sign in as Sara Perez.


Describe the capabilities of Microsoft Identity and A...

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. This requires admins to know and set the phone numbers and email addresses that users use to perform self-service password reset, and reset a user's password.

☐ 4. The "Keep your account secure" page opens. The window that appears and the steps that follow are for the Microsoft Authenticator app method. If you instead want to use email, select **I want to set up a different method** and follow the steps.

a. If you already have the Microsoft Authenticator app installed on your mobile device select **Next**. Otherwise, select **Download now** and follow the steps.

b. You'll begin to setup your account. Select **Next**.

c. Using the Microsoft Authenticator app on

CONTOSO demo

sara@wwlx730857.onmicrosoft.com

Let's keep your account secure

We'll help you set up another way to verify it's you.

Use a different account

Learn more about verifying your identity

Contoso

The sign-in process may require MFA.

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. This requires admins to know and set the phone numbers and email addresses that users use to perform self-service password reset, and reset a user’s password.

The “Keep your account secure” page opens. The window that appears and the steps that follow are for the Microsoft Authenticator app method. If you instead want to use email, select I want to set up a different method and follow the steps.

If you already have the Microsoft Authenticator app installed on your mobile device select Next. Otherwise, select Download now and follow the steps.

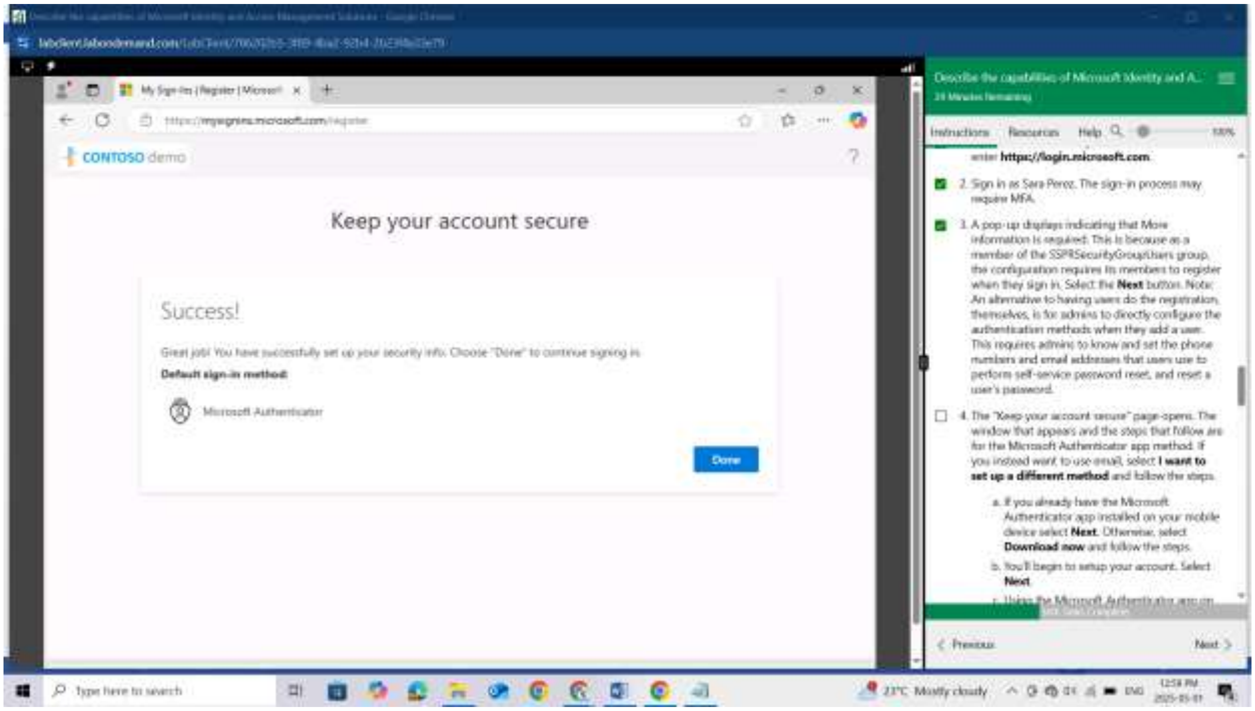
You'll begin to setup your account. Select Next.

Using the Microsoft Authenticator app on your mobile device, select the + to add an account and select Work or school account.

Select the option to Scan the QR code, then using your mobile device, scan the QR code on your PC screen .

Follow the steps on your PC and mobile device, then select Next.

Once you've setup your security info, you'll see a Success window. Select Done.



Keep your account secure

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

Microsoft Authenticator

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. This requires admins to know and set the phone numbers and email addresses that users use to perform self-service password reset, and reset a user's password.

□ 4. The "Keep your account secure" page opens. The window that appears and the steps that follow are for the Microsoft Authenticator app method. If you instead want to use email, select **I want to set up a different method** and follow the steps.

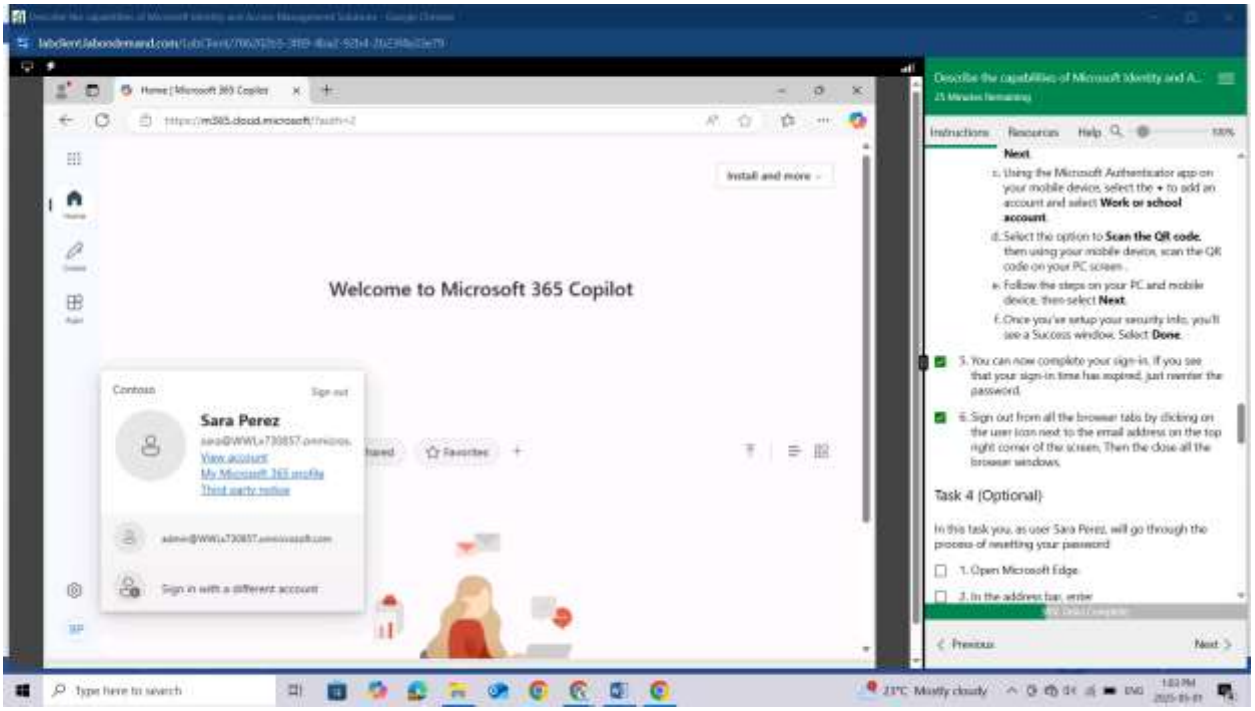
a. If you already have the Microsoft Authenticator app installed on your mobile device select **Next**. Otherwise, select **Download now** and follow the steps.

b. You'll begin to setup your account. Select **Next**.

My Sign-Ins | Register | Microsoft
https://mysignins.microsoft.com/register
CONTOSO demo
Done
Describe the capabilities of Microsoft Identity and A...
Instructions
Resources
Help
Previous
Next
Type here to search
Mostly cloudy
ENG
12:58 PM

You can now complete your sign-in. If you see that your sign-in time has expired, just reenter the password.

Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.



Next

c. Using the Microsoft Authenticator app on your mobile device, select the + to add an account and select **Work or school account**.

d. Select the option to **Scan the QR code**, then using your mobile device, scan the QR code on your PC screen.

e. Follow the steps on your PC and mobile device, then select **Next**.

f. Once you've setup your security info, you'll see a Success window. Select **Done**.

☑ 5. You can now complete your sign-in. If you see that your sign-in time has expired, just reenter the password.

☑ 6. Sign out from all the browser tabs by clicking on the user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.

Task 4 (Optional)

In this task you, as user Sara Perez, will go through the process of resetting your password

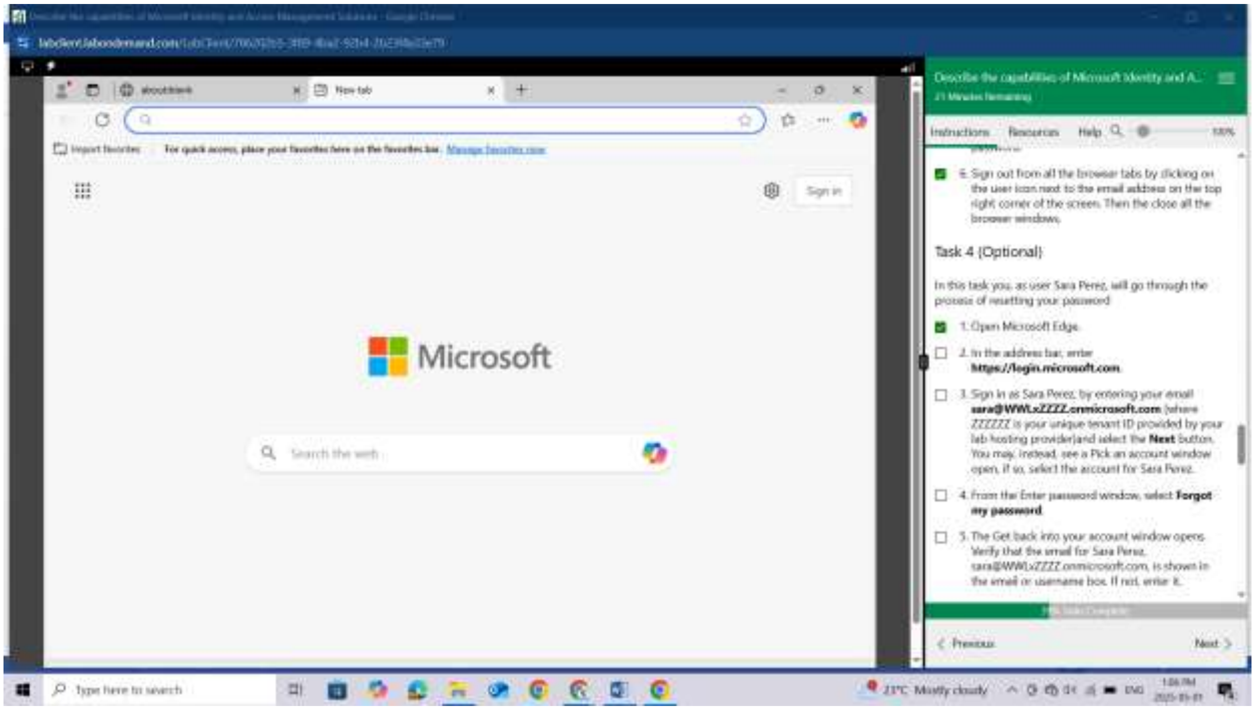
□ 1. Open Microsoft Edge

□ 2. In the address bar, enter

Task 4 (Optional)

In this task you, as user Sara Perez, will go through the process of resetting your password

Open Microsoft Edge.



Task 4 (Optional)

In this task you, as user Sara Perez, will go through the process of resetting your password

☑ 1. Open Microsoft Edge.

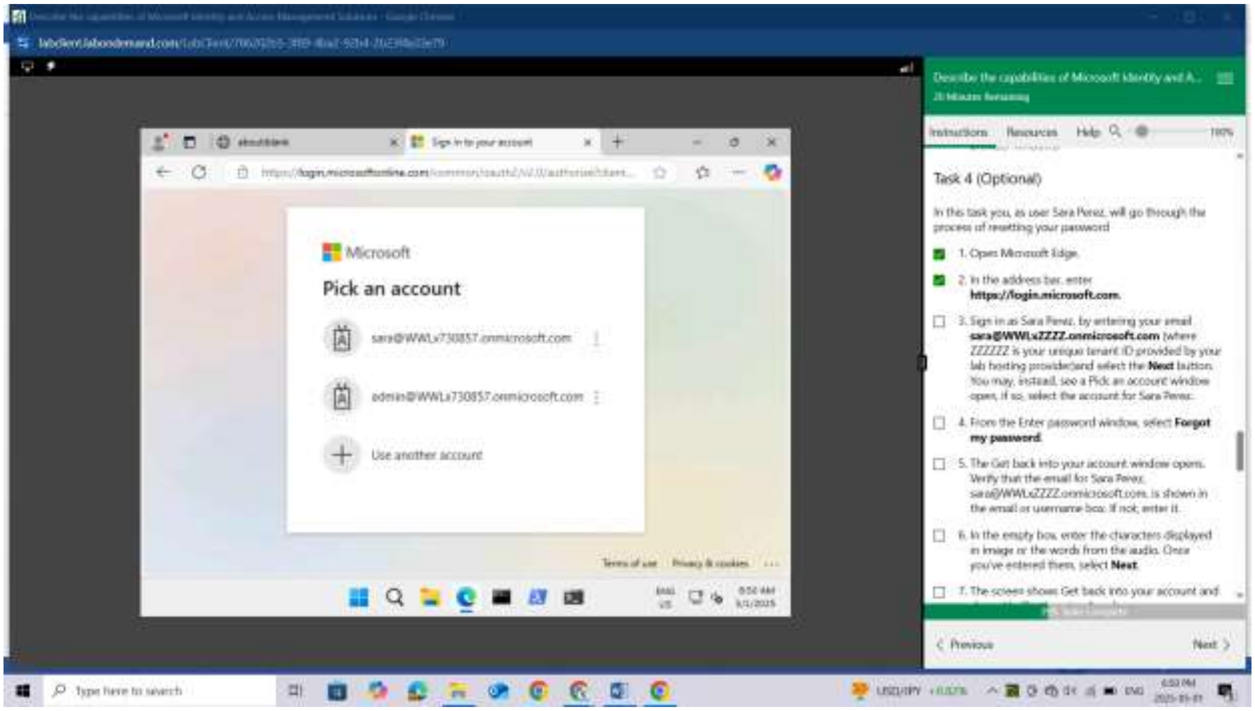
□ 2. In the address bar, enter **https://login.microsoft.com**.

□ 3. Sign in as Sara Perez, by entering your email **sara@WWLxZZZZ.onmicrosoft.com** (where ZZZZZZ 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, sara@WWLxZZZZ.onmicrosoft.com, is shown in the email or username box. If not, enter it.

In the address bar, enter https://login.microsoft.com.



Pick an account

sara@WWLx730857.onmicrosoft.com

admin@WWLx730857.onmicrosoft.com

Use another account

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** (where ZZZZZZ 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**.

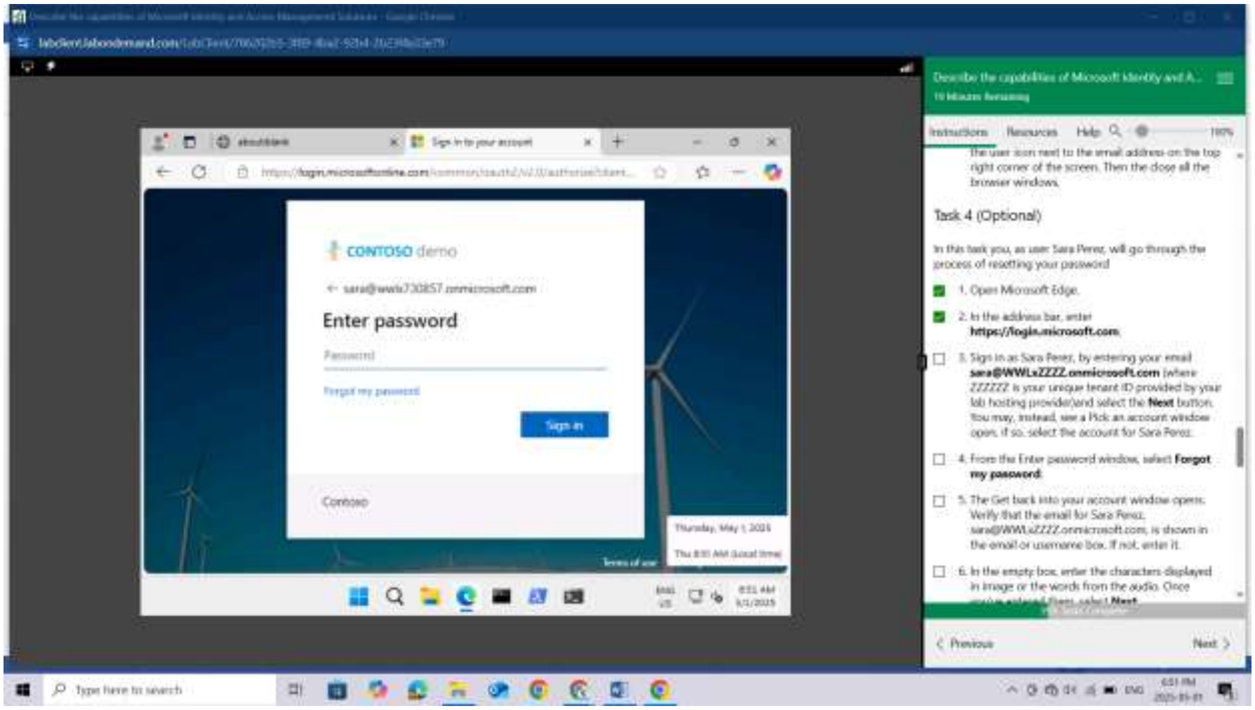
□ 5. The Get back into your account window opens. Verify that the email for Sara Perez, sara@WWLxZZZZ.onmicrosoft.com, is shown in the email or username box. If not, enter it.

□ 6. In the empty box, enter the characters displayed in image or the words from the audio. Once you've entered them, select **Next**.

□ 7. The screen shows Get back into your account and

Sign in as Sara Perez, by entering your email **sara@WWLxZZZZ.onmicrosoft.com** (where ZZZZZZ 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.

From the Enter password window, select Forgot my password.



CONTOSO demo

← sara@wwlx730857.onmicrosoft.com

Enter password

Password

Forgot my password

Sign in

Contoso

Thursday, May 1, 2025

Describe the capabilities of Microsoft Identity and A...

The user icon next to the email address on the top right corner of the screen. Then the close all the browser windows.

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** (where ZZZZZZ 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.

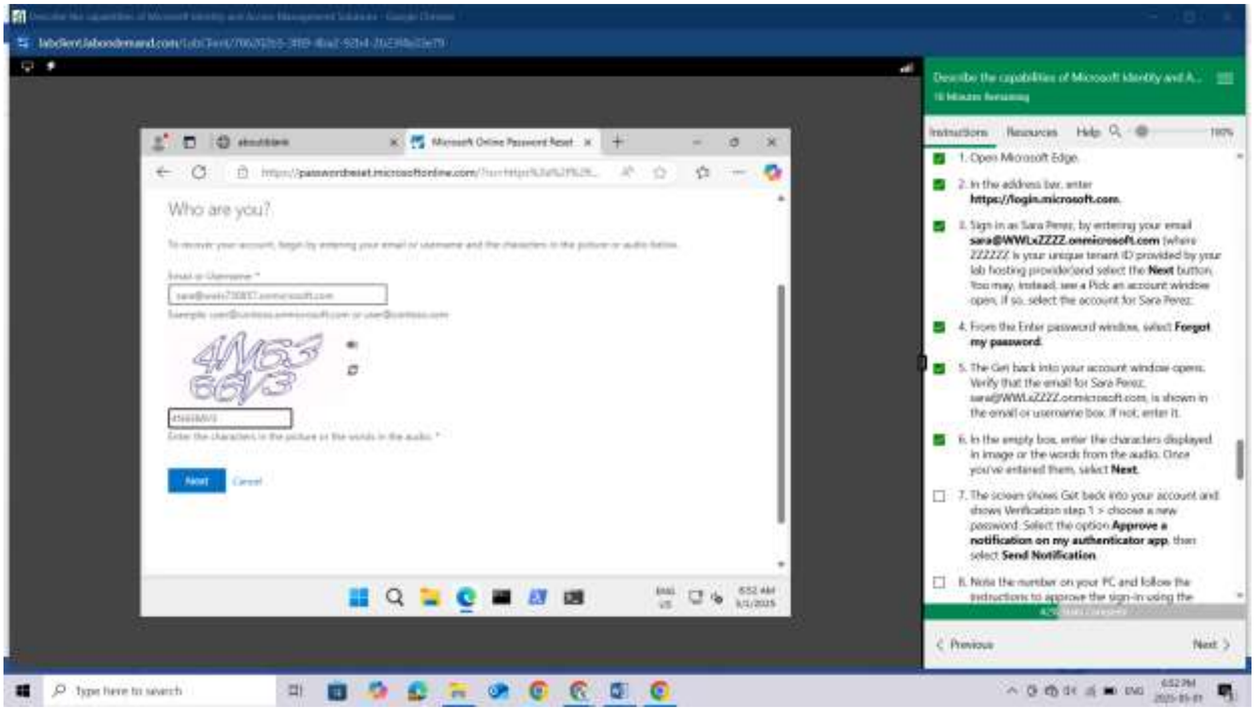
□ 4. From the Enter password window, select **Forgot my password**.

□ 5. The Get back into your account window opens. Verify that the email for Sara Perez, sara@WWLxZZZZ.onmicrosoft.com, is shown in the email or username box. If not, enter it.

□ 6. In the empty box, enter the characters displayed in image or the words from the audio. Once you've entered them, select **Next**.

The Get back into your account window opens. Verify that the email for Sara Perez, sara@WWLxZZZZ.onmicrosoft.com, is shown in the email or username box. If not, enter it.

In the empty box, enter the characters displayed in image or the words from the audio. Once you've entered them, select **Next**.



Who are you?

To recover your account, begin by entering your email or username and the characters in the picture or audio below.

Email or Username: *

Sample: user@contoso.onmicrosoft.com or user@contoso.com

Enter the characters in the picture or the words in the audio. *

Next Cancel

Describe the capabilities of Microsoft Identity and A...

☑ 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** (where ZZZZZZ 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**.

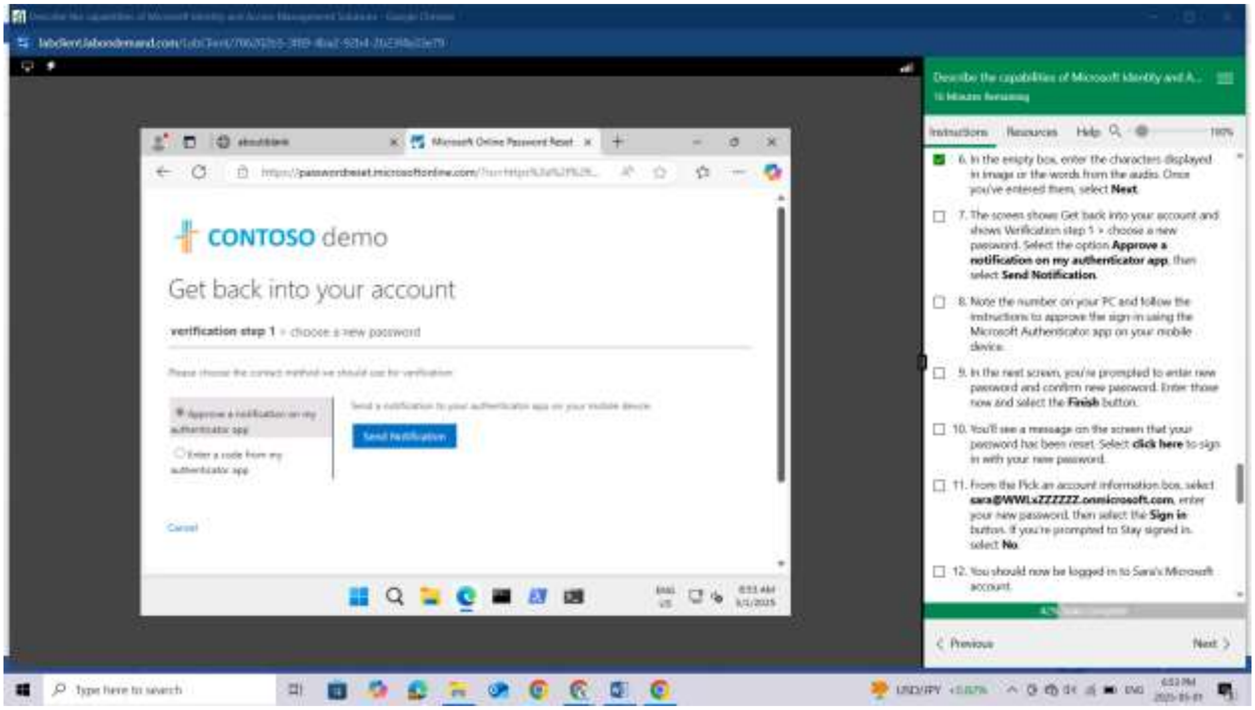
☑ 5. The Get back into your account window opens. Verify that the email for Sara Perez, sara@WWLxZZZZ.onmicrosoft.com, is shown in the email or username box. If not, enter it.

☑ 6. In the empty box, enter the characters displayed in image or the words from the audio. Once you've entered them, select **Next**.

□ 7. The screen shows Get back into your account and shows Verification step 1 > choose a new password. Select the option **Approve a notification on my authenticator app**, then select **Send Notification**.

□ 8. Note the number on your PC and follow the instructions to approve the sign-in using the

The screen shows Get back into your account and shows Verification step 1 > choose a new password. Select the option Approve a notification on my authenticator app, then select Send Notification.



CONTOSO demo

Get back into your account

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

● Approve a notification on my authenticator app

○ Enter a code from my authenticator app

Send a notification to your authenticator app on your mobile device.

Describe the capabilities of Microsoft Identity and A...

☑ 6. In the empty box, enter the characters displayed in image or the words from the audio. Once you've entered them, select **Next**.

☐ 7. The screen shows Get back into your account and shows Verification step 1 > choose a new password. Select the option **Approve a notification on my authenticator app**, then select **Send Notification**.

☐ 8. Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.

☐ 9. In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the **Finish** button.

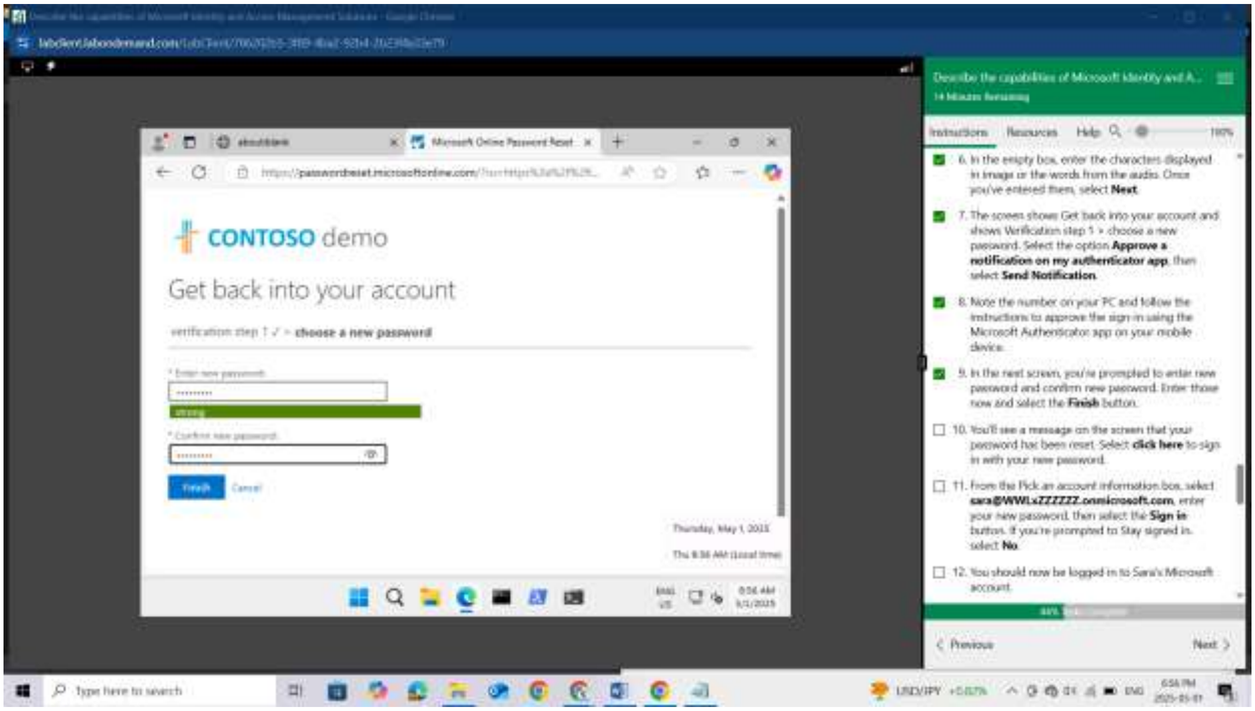
☐ 10. You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.

☐ 11. From the Pick an account information box, select **sara@WWLxZZZZZZ.onmicrosoft.com**, enter your new password, then select the **Sign in** button. If you're prompted to Stay signed in, select **No**.

☐ 12. You should now be logged in to Sara's Microsoft account.

Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.

In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the Finish button.



CONTOSO demo

Get back into your account

verification step 1 ✓ > **choose a new password**

* Enter new password:

strong

* Confirm new password:

Thursday, May 1, 2025

Describe the capabilities of Microsoft Identity and A...

☑ 6. In the empty box, enter the characters displayed in image or the words from the audio. Once you've entered them, select **Next**.

☑ 7. The screen shows Get back into your account and shows Verification step 1 > choose a new password. Select the option **Approve a notification on my authenticator app**, then select **Send Notification**.

☑ 8. Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.

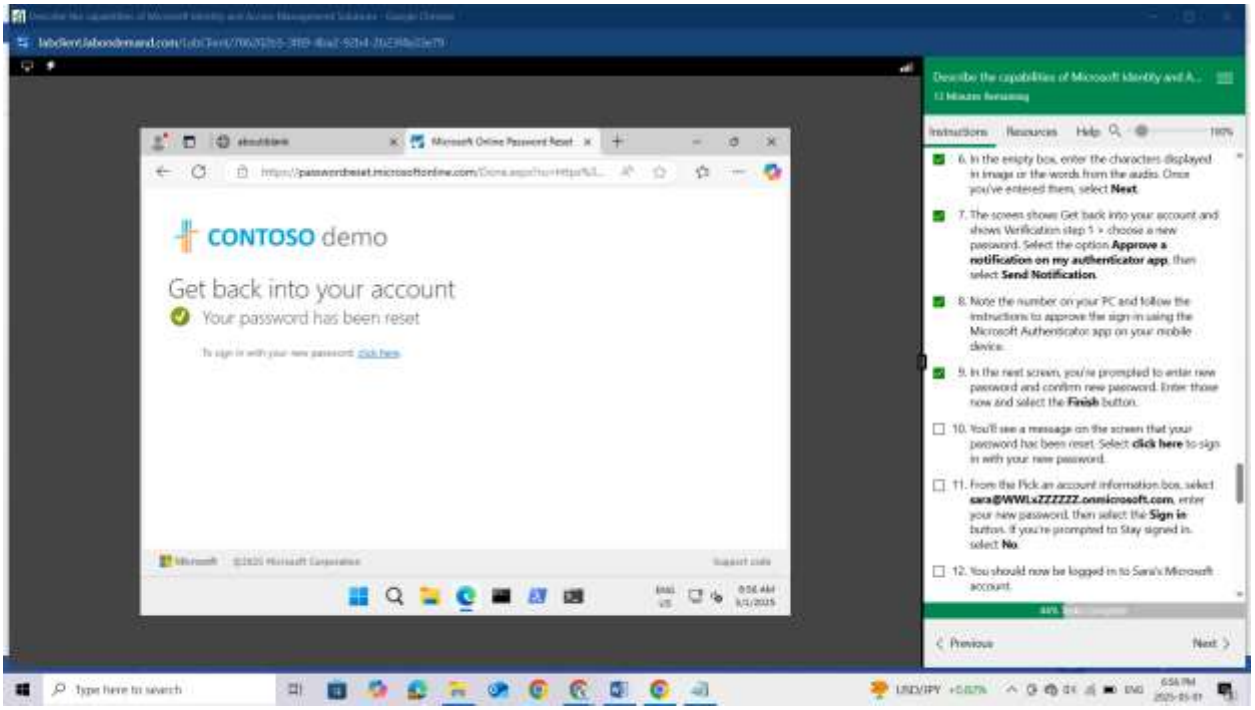
☑ 9. In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the **Finish** button.

☐ 10. You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.

☐ 11. From the Pick an account information box, select **sara@WWLxZZZZZZ.onmicrosoft.com**, enter your new password, then select the **Sign in** button. If you're prompted to Stay signed in, select **No**.

☐ 12. You should now be logged in to Sara's Microsoft account.

You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.



CONTOSO demo

Get back into your account

✓ Your password has been reset

To sign in with your new password click here.

Describe the capabilities of Microsoft Identity and A...

☑ 6. In the empty box, enter the characters displayed in image or the words from the audio. Once you've entered them, select **Next**.

☑ 7. The screen shows Get back into your account and shows Verification step 1 > choose a new password. Select the option **Approve a notification on my authenticator app**, then select **Send Notification**.

☑ 8. Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.

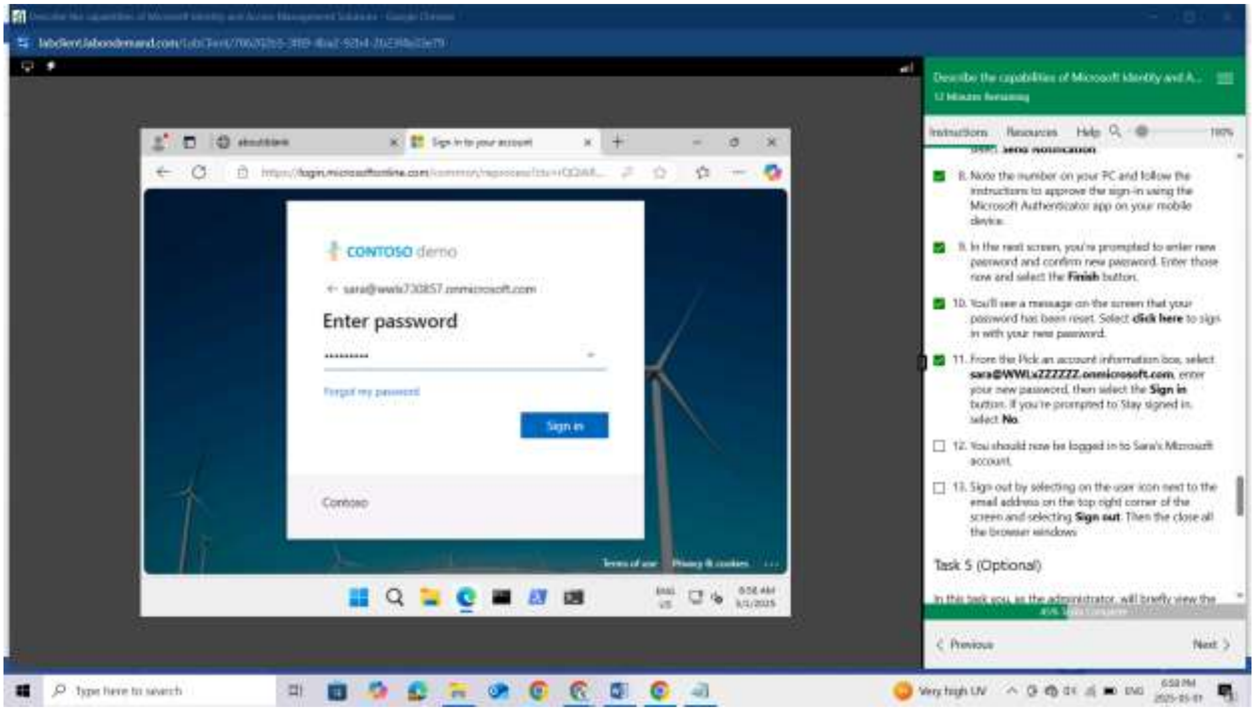
☑ 9. In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the **Finish** button.

□ 10. You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.

□ 11. From the Pick an account information box, select **sara@WWLxZZZZZZ.onmicrosoft.com**, enter your new password, then select the **Sign in** button. If you're prompted to Stay signed in, select **No**.

□ 12. You should now be logged in to Sara's Microsoft account.

From the Pick an account information box, select sara@WWLxZZZZZZ.onmicrosoft.com, enter your new password, then select the Sign in button.



CONTOSO demo

← sara@wwlx730857.onmicrosoft.com

Enter password

****

Forgot my password

Sign in

Contoso

Describe the capabilities of Microsoft Identity and A...

☑ 8. Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.

☑ 9. In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the **Finish** button.

☑ 10. You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.

☑ 11. From the Pick an account information box, select **sara@WWLxZZZZZZ.onmicrosoft.com**, enter your new password, then select the **Sign in** button. If you're prompted to Stay signed in, select **No**.

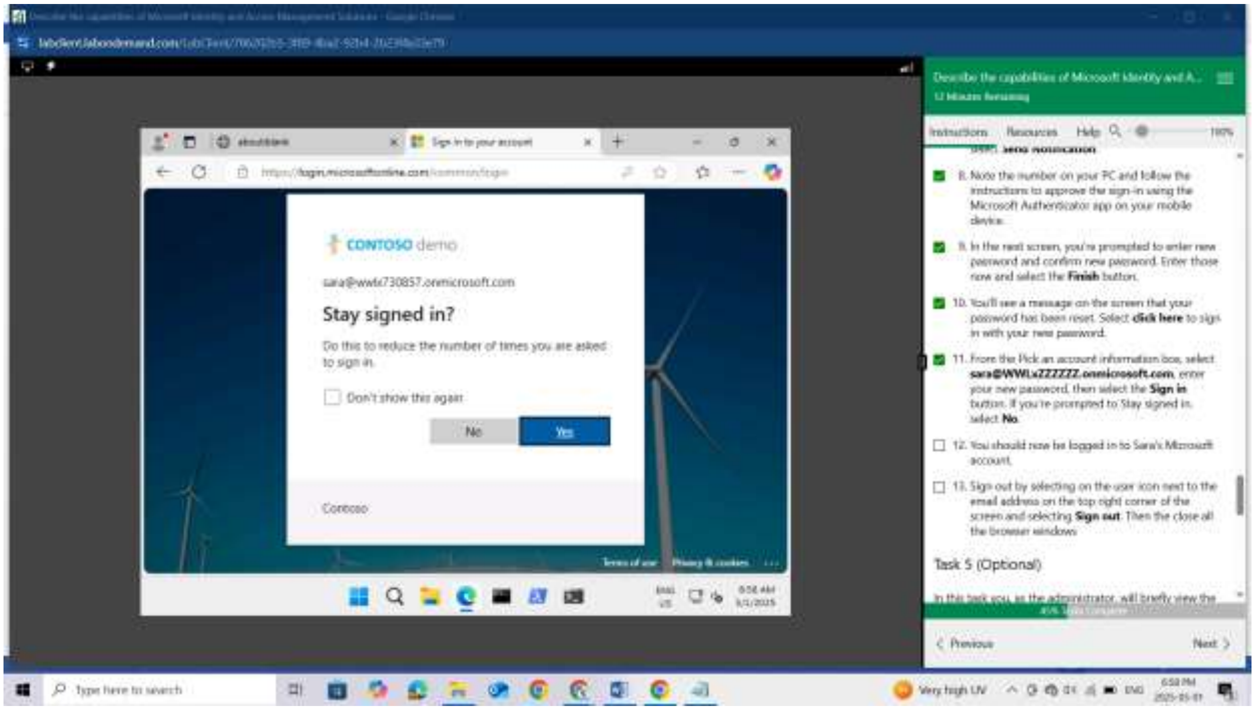
□ 12. You should now be logged in to Sara's Microsoft account.

□ 13. 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 5 (Optional)

In this task you, as the administrator, will briefly view the

If you're prompted to Stay signed in. select No.



CONTOSO demo

sara@wwlx730857.onmicrosoft.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

No | Yes

Contoso

Describe the capabilities of Microsoft Identity and A...

Instructions | Resources | Help | 100%

☑ 8. Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.

☑ 9. In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the **Finish** button.

☑ 10. You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.

☑ 11. From the Pick an account information box, select **sara@WWLxZZZZZ.onmicrosoft.com**, enter your new password, then select the **Sign in** button. If you're prompted to Stay signed in, select **No**.

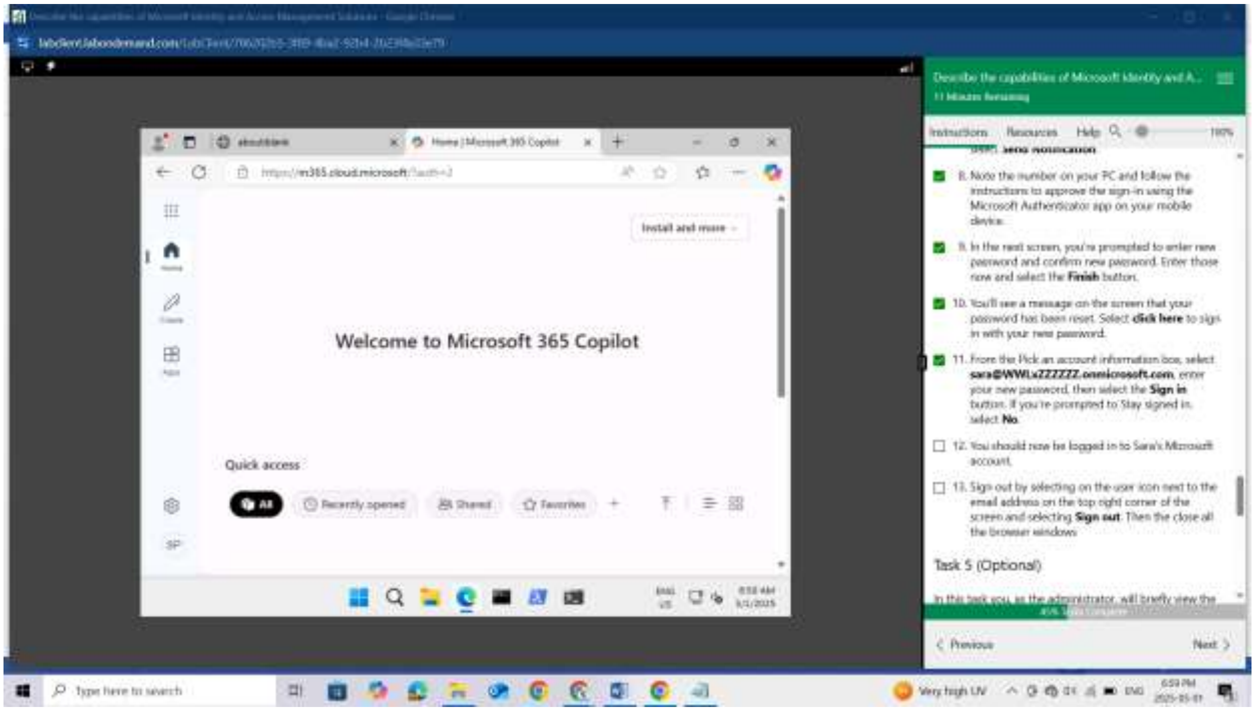
□ 12. You should now be logged in to Sara's Microsoft account.

□ 13. 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 5 (Optional)

In this task you, as the administrator, will briefly view the

You should now be logged in to Sara's Microsoft account.



Welcome to Microsoft 365 Copilot

Quick access

☑ 8. Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.

☑ 9. In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the **Finish** button.

☑ 10. You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.

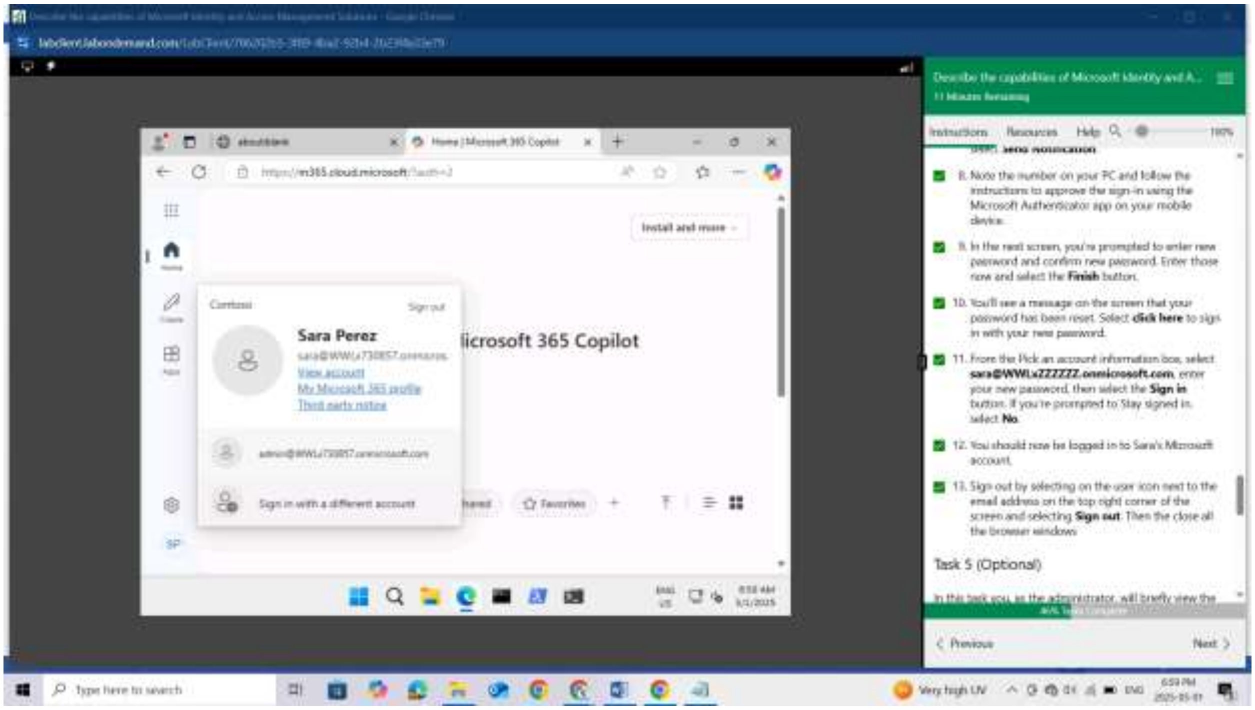
☑ 11. From the Pick an account information box, select **sara@WWLxZZZZZ.onmicrosoft.com**, enter your new password, then select the **Sign in** button. If you're prompted to Stay signed in, select **No**.

□ 12. You should now be logged in to Sara's Microsoft account.

□ 13. 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 5 (Optional)

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


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

- ☑ 8. Note the number on your PC and follow the instructions to approve the sign-in using the Microsoft Authenticator app on your mobile device.
- ☑ 9. In the next screen, you're prompted to enter new password and confirm new password. Enter those now and select the **Finish** button.
- ☑ 10. You'll see a message on the screen that your password has been reset. Select **click here** to sign in with your new password.
- ☑ 11. From the Pick an account information box, select **sara@WWLxZZZZZZ.onmicrosoft.com**, enter your new password, then select the **Sign in** button. If you're prompted to Stay signed in, select **No**.
- ☑ 12. You should now be logged in to Sara's Microsoft account.
- ☑ 13. 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

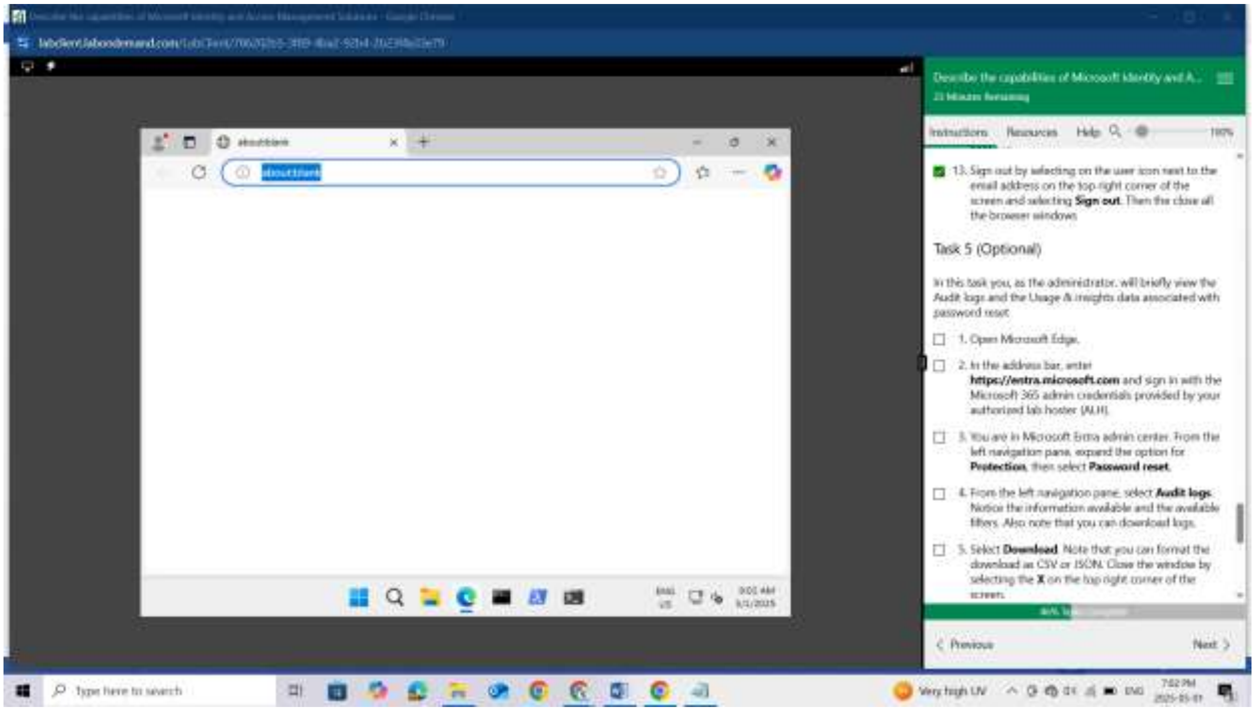
Task 5 (Optional)

In this task you, as the administrator, will briefly view the

Task 5 (Optional)

In this task you, as the administrator, will briefly view the Audit logs and the Usage & insights data associated with password reset

Open Microsoft Edge.


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

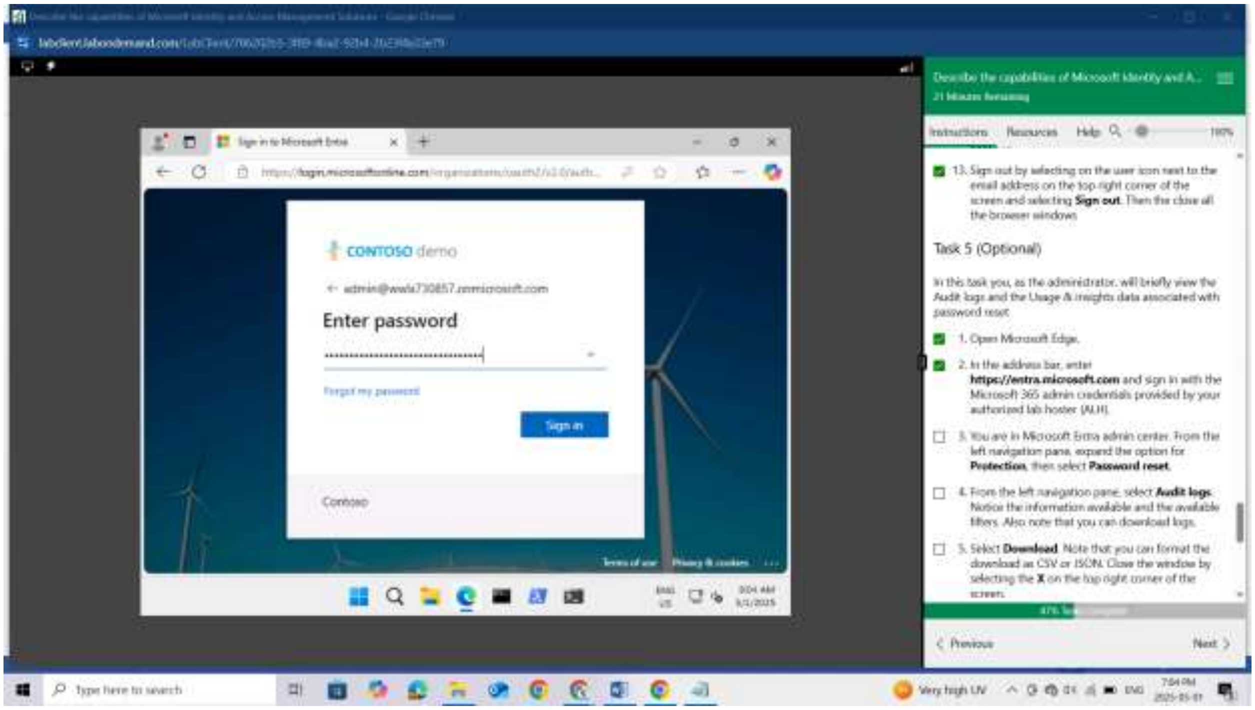
- ☑ 13. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting **Sign out**. Then the close all the browser windows

Task 5 (Optional)

In this task you, as the administrator, will briefly view the Audit logs and the Usage & insights data associated with password reset

- ☐ 1. Open Microsoft Edge.
- ☐ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).
- ☐ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.
- ☐ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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.

In the address bar, enter https://entra.microsoft.com and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).



CONTOSO demo

← admin@wwlx730857.onmicrosoft.com

Enter password

Forgot my password

Sign in

Contoso

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

Instructions Resources Help

- ☑ 13. 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

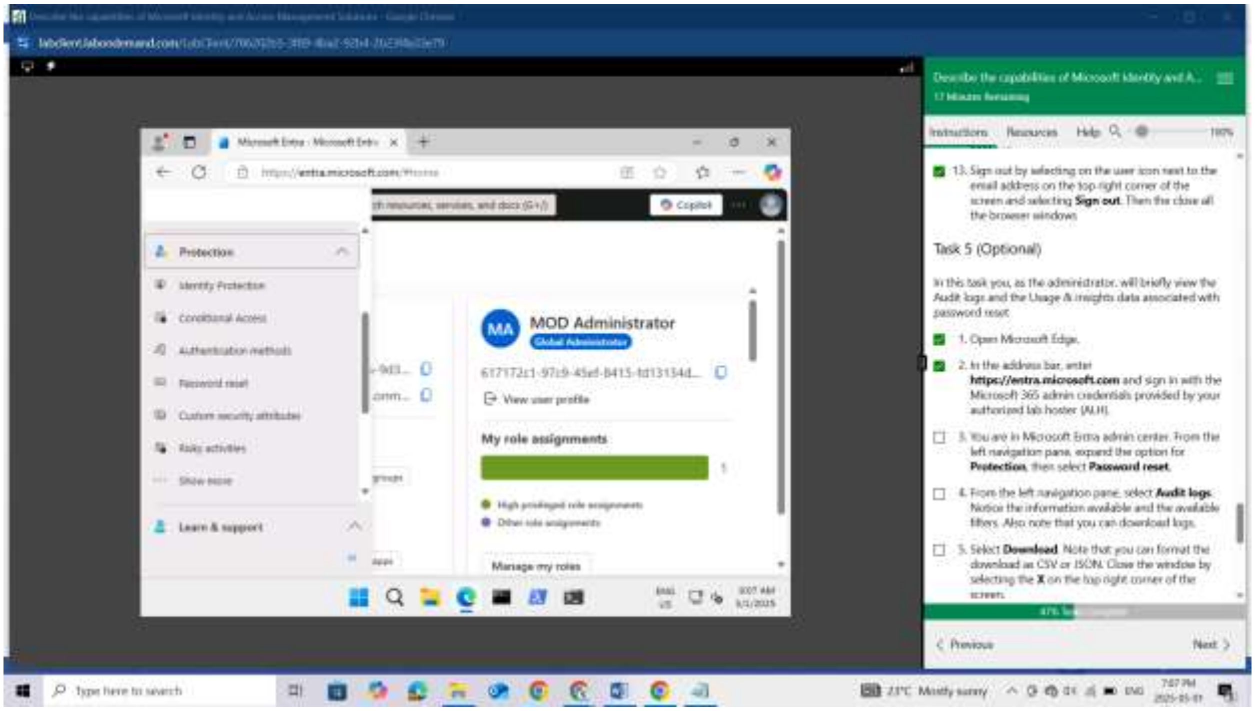
Task 5 (Optional)

In this task you, as the administrator, will briefly view the Audit logs and the Usage & insights data associated with password reset

- ☑ 1. Open Microsoft Edge.
- ☑ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).
- ☐ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.
- ☐ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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.

< Previous Next >

You are in Microsoft Entra admin center. From the left navigation pane, expand the option for Protection, then select Password reset.



MOD Administrator

Global Administrator

617172c1-97c9-45ef-8415-fd13134d...

View user profile

My role assignments

- High privileged role assignments
- Other role assignments

Manage my roles

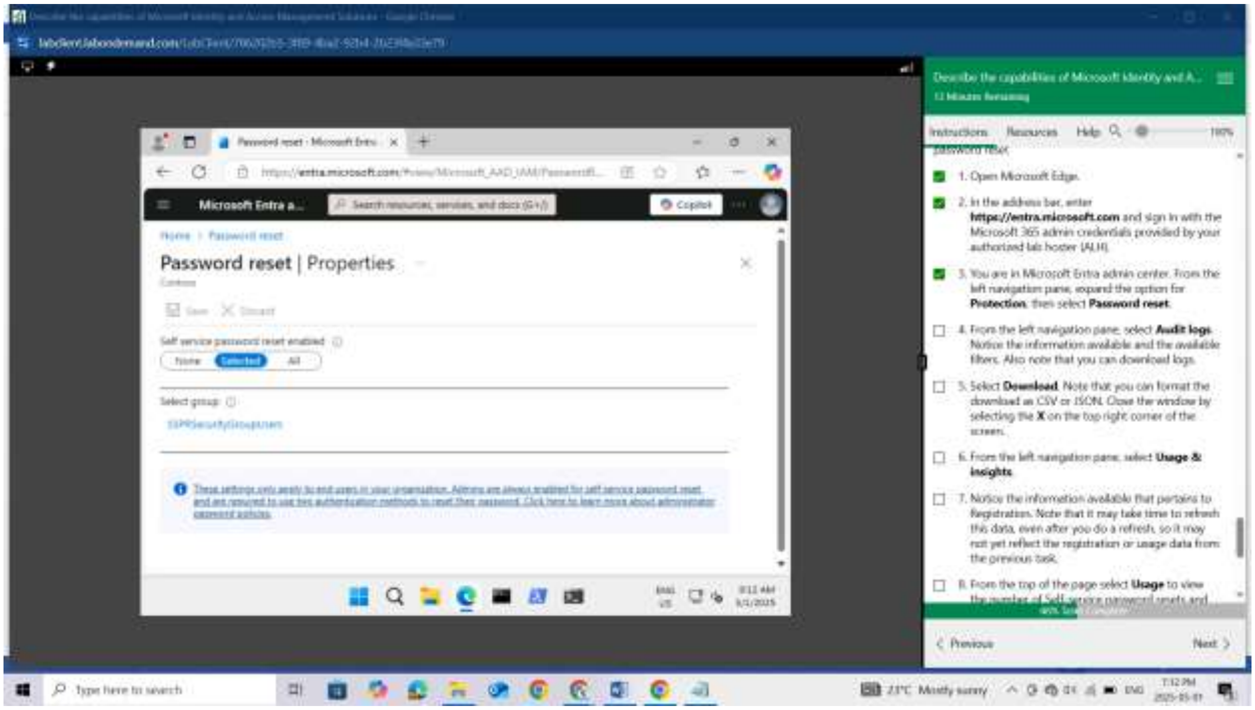
Describe the capabilities of Microsoft Identity and A...
17 Minutes Remaining

- ☑ 13. 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 5 (Optional)

In this task you, as the administrator, will briefly view the Audit logs and the Usage & insights data associated with password reset

- ☑ 1. Open Microsoft Edge.
- ☑ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).
- ☐ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.
- ☐ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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.



Password reset | Properties

Self service password reset enabled

None [✓ Selected] All

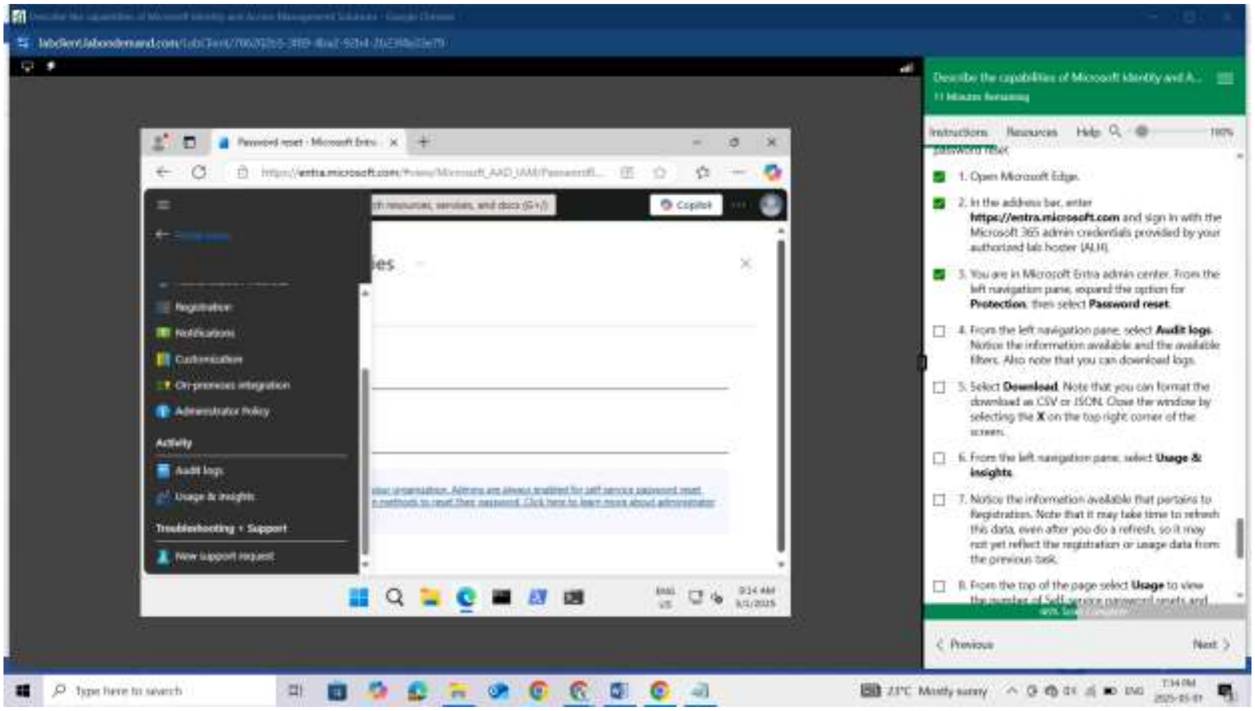
Select group: SSPRSecurityGroupUsers

These settings only apply to end users in your organization. Admins are always enabled for self service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Describe the capabilities of Microsoft Identity and A...

- ☑ 1. Open Microsoft Edge.
- ☑ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).
- ☑ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.
- □ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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

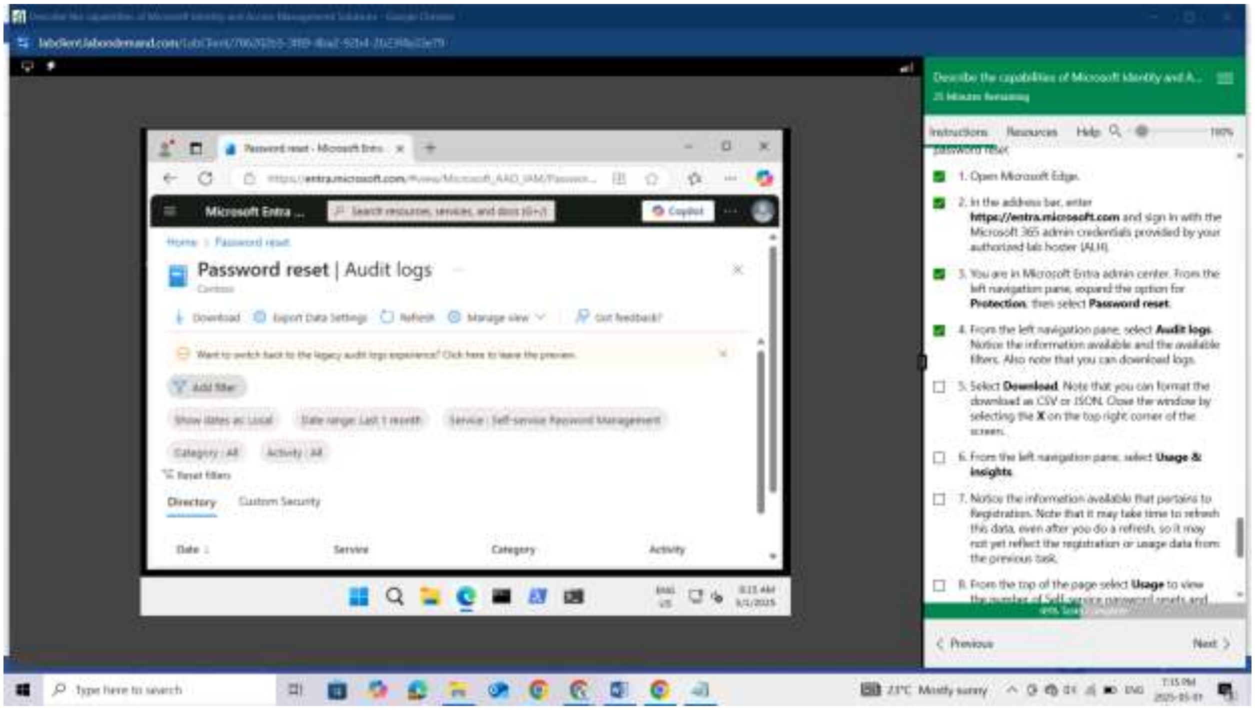
From the left navigation pane, select Audit logs.



Describe the capabilities of Microsoft Identity and A...

- ☑ 1. Open Microsoft Edge.
- ☑ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).
- ☑ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.
- □ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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

Notice the information available and the available filters. Also note that you can download logs.



Password reset | Audit logs

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

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

Date · Service · Category · Activity

Describe the capabilities of Microsoft Identity and A...

☑ 1. Open Microsoft Edge.

☑ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).

☑ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.

☑ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. Also note that you can download logs.

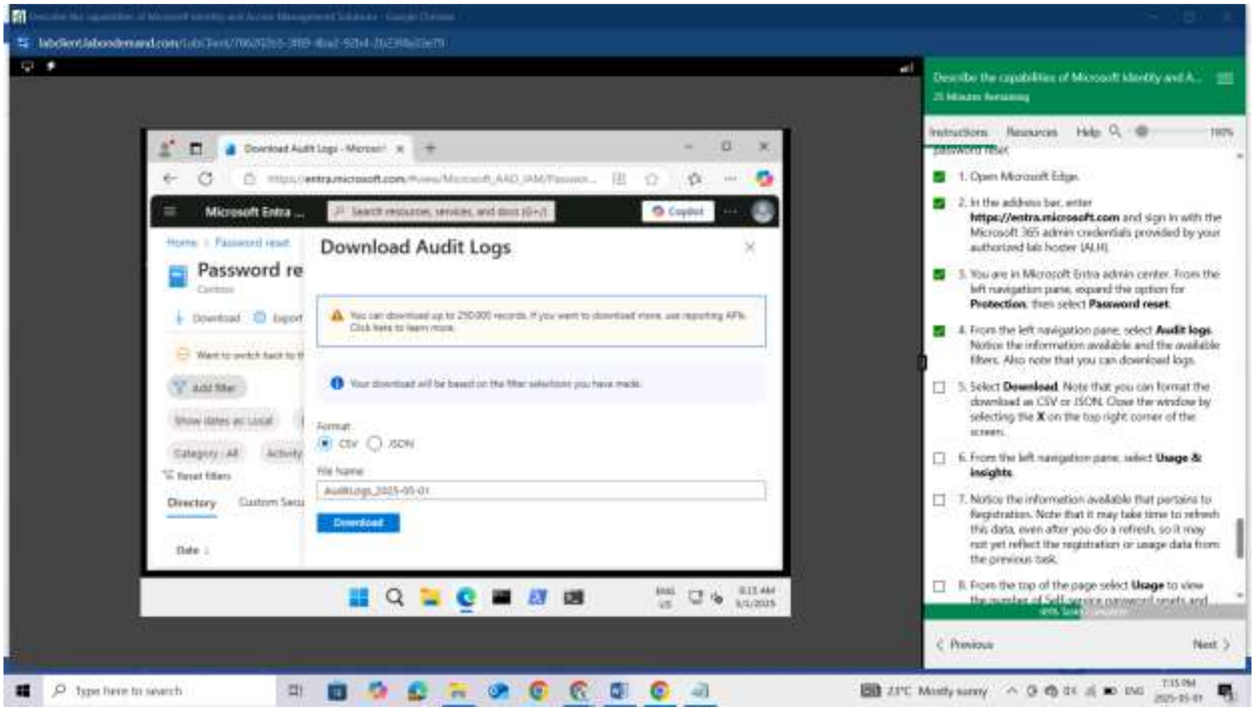
□ 5. Select **Download**. Note that you can format the download as CSV or JSON. Close the window by selecting the **X** on the top right corner of the screen.

□ 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

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.



Download Audit Logs

You can download up to 250 000 records. If you want to download more, use reporting APIs. Click here to learn more.

Your download will be based on the filter selections you have made.

Format

● CSV ○ JSON

File Name

AuditLogs_2025-05-01

☑ 1. Open Microsoft Edge.

☑ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).

☑ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.

☑ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. Also note that you can download logs.

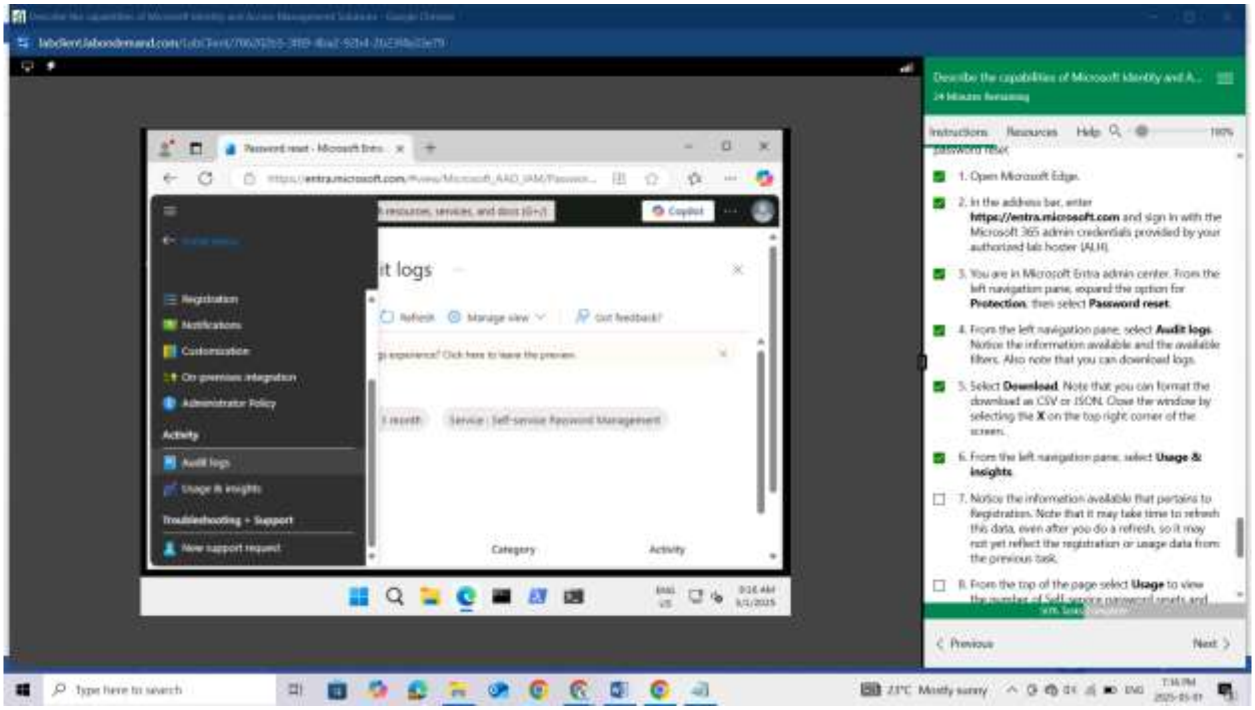
□ 5. Select **Download**. Note that you can format the download as CSV or JSON. Close the window by selecting the **X** on the top right corner of the screen.

□ 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

From the left navigation pane, select Usage & insights.



Describe the capabilities of Microsoft Identity and A...

24 Minutes Remaining

password reset

☑ 1. Open Microsoft Edge.

☑ 2. In the address bar, enter **https://entra.microsoft.com** and sign in with the Microsoft 365 admin credentials provided by your authorized lab hoster (ALH).

☑ 3. You are in Microsoft Entra admin center. From the left navigation pane, expand the option for **Protection**, then select **Password reset**.

☑ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. Also note that you can download logs.

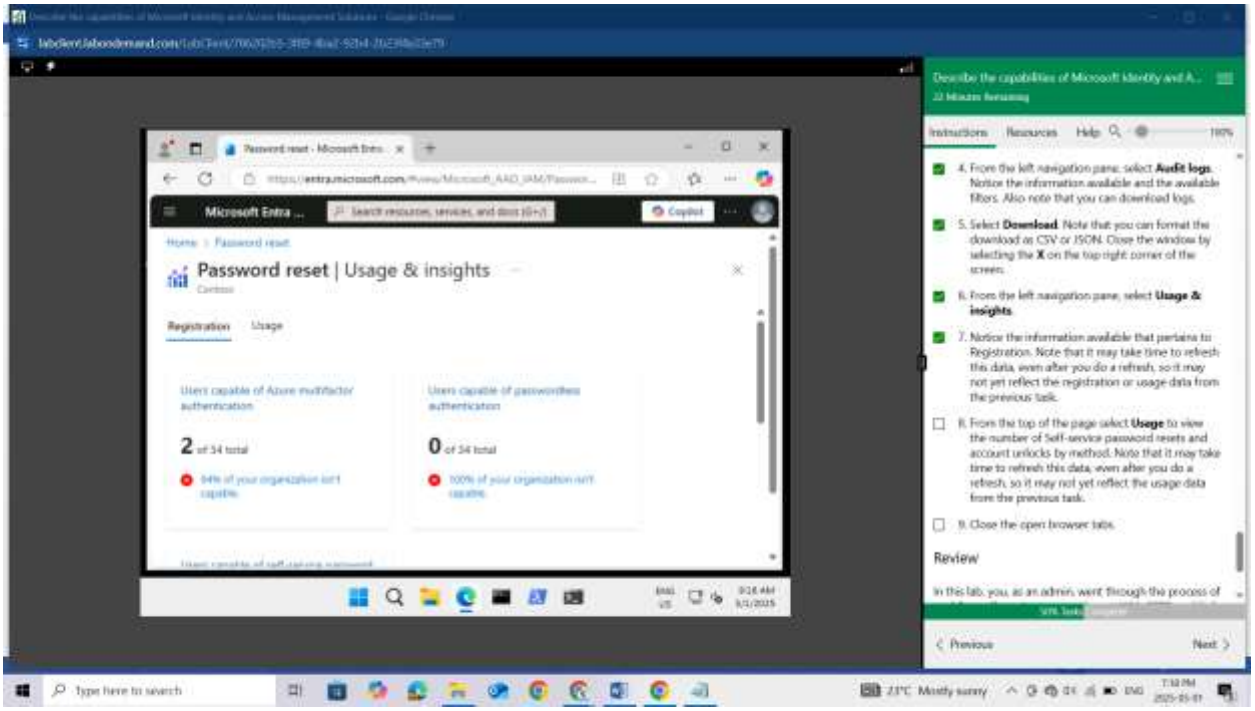
☑ 5. Select **Download**. Note that you can format the download as CSV or JSON. Close the window by selecting the **X** on the top right corner of the screen.

☑ 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

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.



Password reset | Usage & insights

Contoso

Users capable of Azure multifactor authentication

2 of 34 total

94% of your organization isn't capable.

Users capable of passwordless authentication

0 of 34 total

100% of your organization isn't capable.

Describe the capabilities of Microsoft Identity and A...

22 Minutes Remaining

☑ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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.

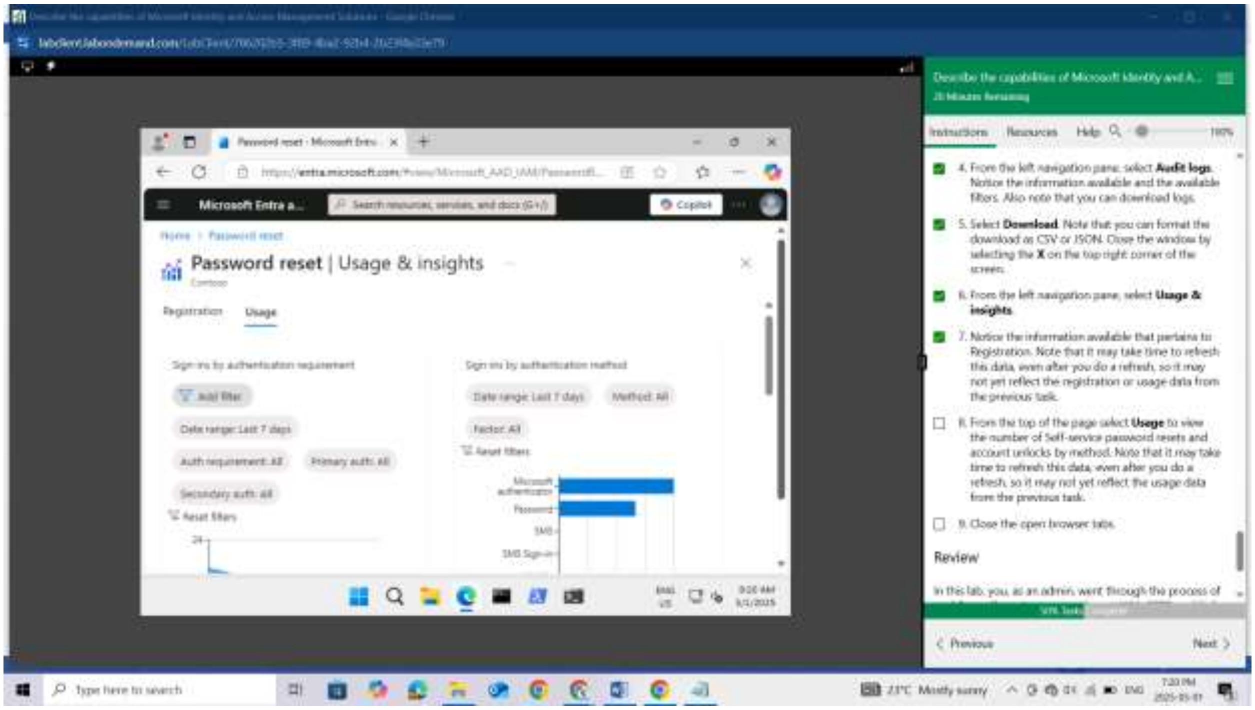
□ 8. From the top of the page select **Usage** to view the number of Self-service password resets and account unlocks by method. Note that it may take time to refresh this data, even after you do a refresh, so it may not yet reflect the usage data from the previous task.

□ 9. Close the open browser tabs.

Review

In this lab, you, as an admin, went through the process of

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 usage data from the previous task.



Describe the capabilities of Microsoft Identity and A...

☑ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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.

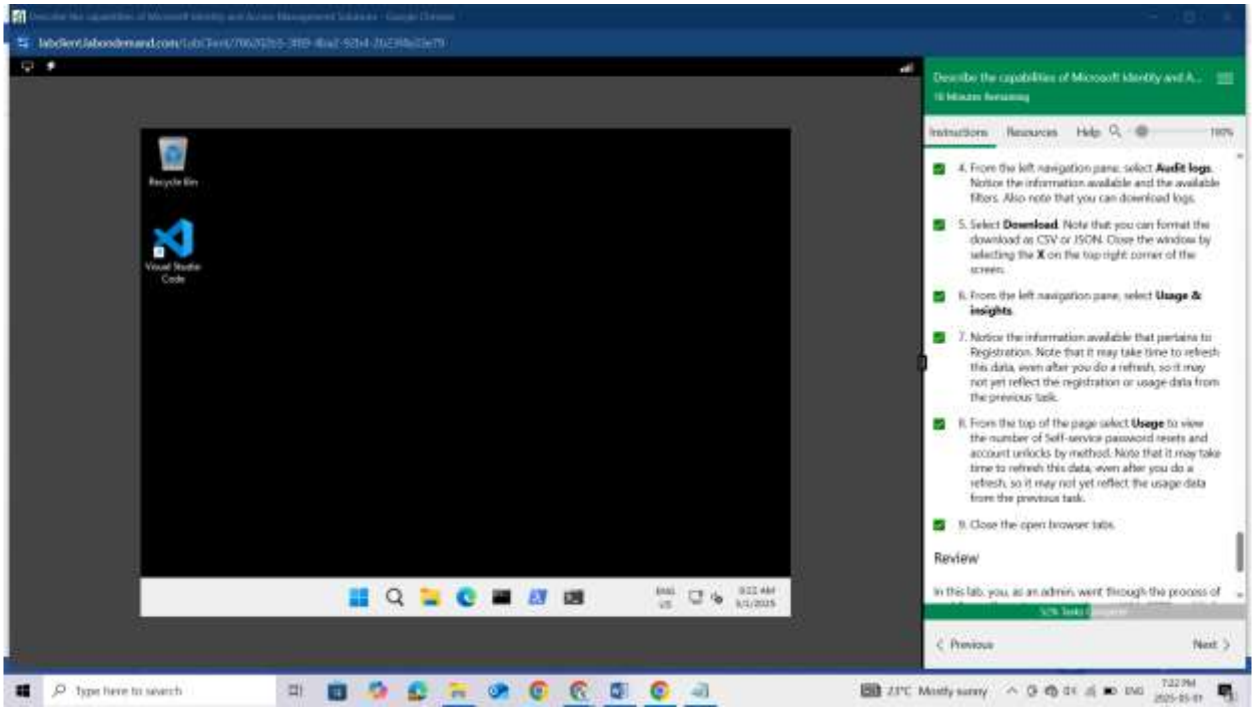
☐ 8. From the top of the page select **Usage** to view the number of Self-service password resets and account unlocks by method. Note that it may take time to refresh this data, even after you do a refresh, so it may not yet reflect the usage data from the previous task.

☐ 9. Close the open browser tabs.

Review

In this lab, you, as an admin, went through the process of

Close the open browser tabs.



Describe the capabilities of Microsoft Identity and A...

☑ 4. From the left navigation pane, select **Audit logs**. Notice the information available and the available filters. 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 usage data from the previous task.

☑ 9. Close the open browser tabs.

Review

In this lab, you, as an admin, went through the process of

Review

In this lab, you, as an admin, went through the process of enabling self-service password reset. With SSPR enabled, you'll then assume the role of a user to go through the process of registering for SSPR and also resetting your password. Lastly, you as the admin, learn where to access audit logs and usage & insights data for SSPR.

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 the Microsoft Admin portals. From a user perspective, you'll see the impact of the conditional access policy, including the process to register for MFA.

Task 1

In this task you, as the admin, will reset the password for the user Debra Berger. This step is needed so you can initially sign in as the user in subsequent tasks.

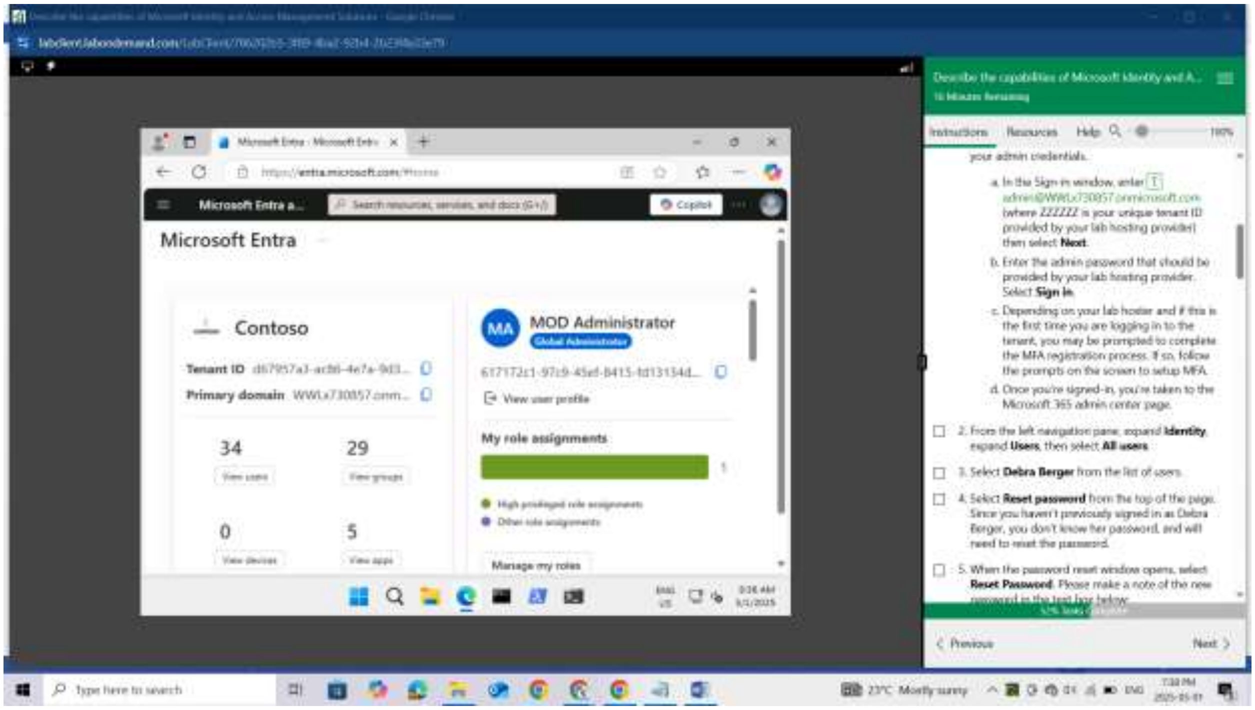
Open Microsoft Edge. In the address bar, enter https://entra.microsoft.com, and sign in with your admin credentials.

In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select Next.

Enter the admin password that should be provided by your lab hosting provider. Select Sign in.

Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

Once you're signed-in, you're taken to the Microsoft 365 admin center page.



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

your admin credentials.

a. In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.

b. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.

☐ 2. From the left navigation pane, expand **Identity**, expand **Users**, then select **All users**.

☐ 3. Select **Debra Berger** from the list of users.

☐ 4. Select **Reset password** from the top of the page. Since you haven't previously signed in as Debra Berger, you don't know her password, and will need to reset the password.

☐ 5. When the password reset window opens, select **Reset Password**. Please make a note of the new password in the text box below.

Microsoft Entra

Contoso

Tenant ID d67957a3-ac86-4e7a-9d3...

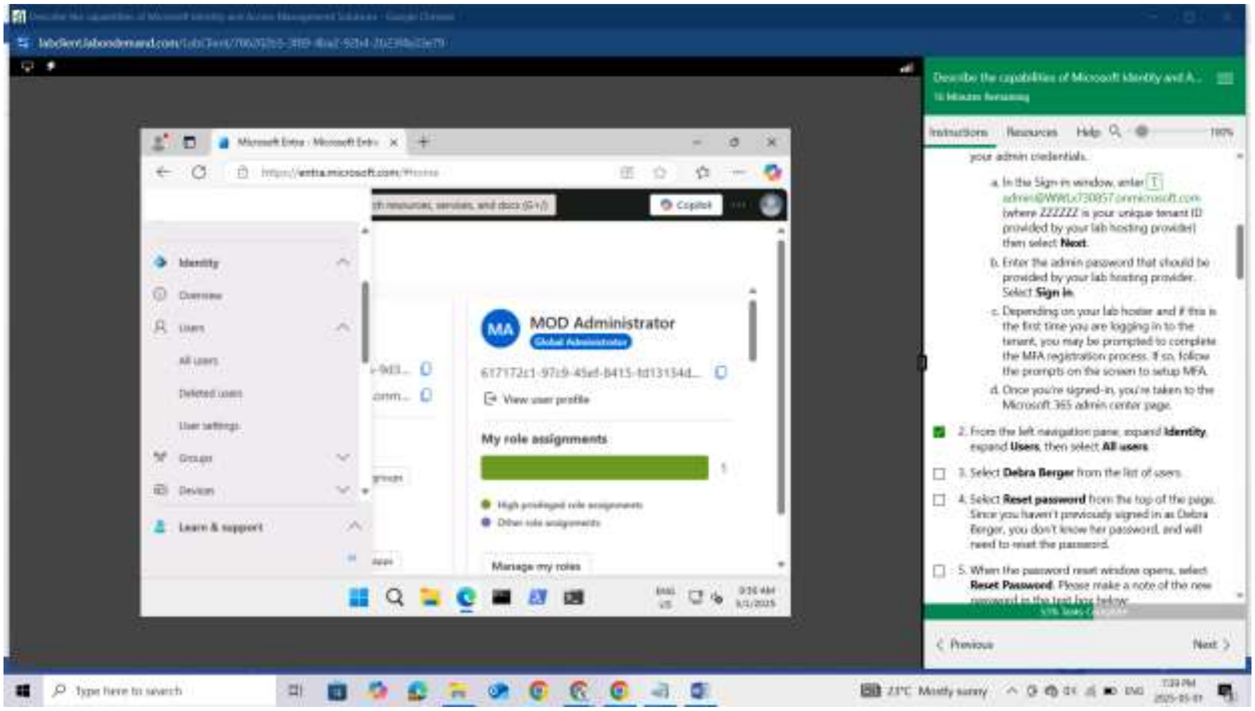
Primary domain WWLx730857.onm...

MOD Administrator

Global Administrator

617172c1-97c9-45ef-8415-fd13134d...

From the left navigation pane, expand Identity, expand Users, then select All users.



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

your admin credentials.

a. In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.

b. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.

☑ 2. From the left navigation pane, expand **Identity**, expand **Users**, then select **All users**.

☐ 3. Select **Debra Berger** from the list of users.

☐ 4. Select **Reset password** from the top of the page. Since you haven't previously signed in as Debra Berger, you don't know her password, and will need to reset the password.

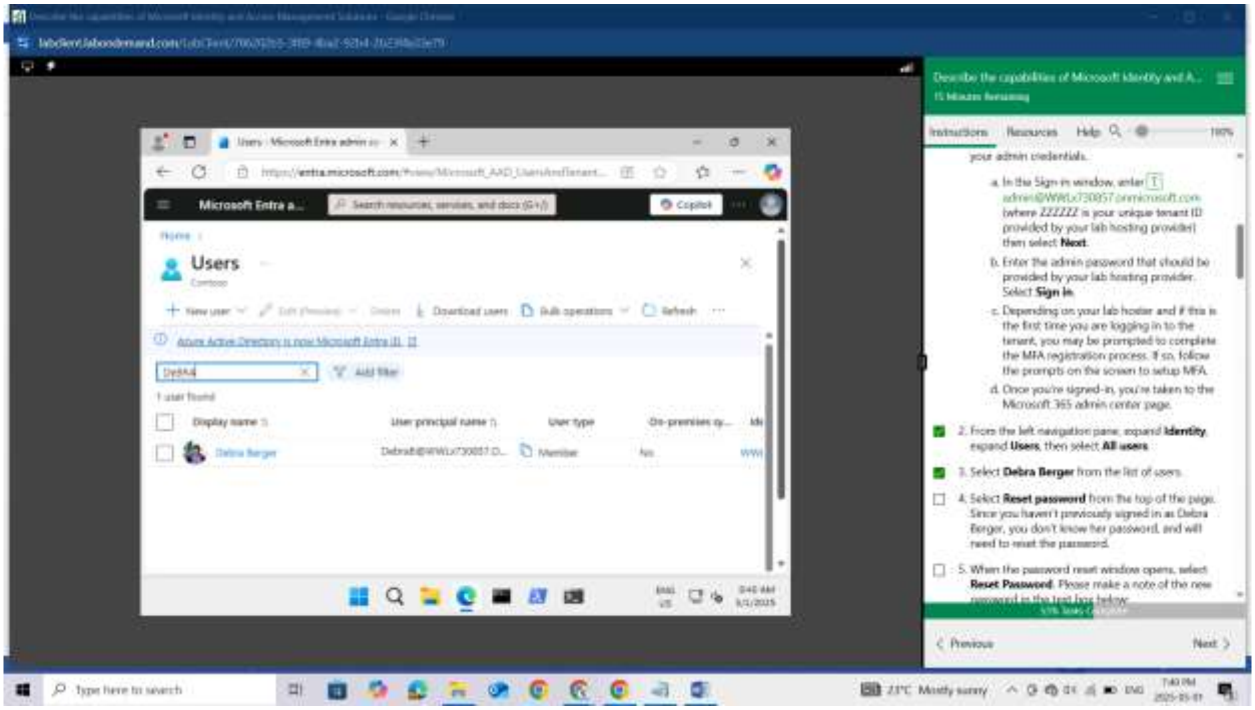
☐ 5. When the password reset window opens, select **Reset Password**. Please make a note of the new password in the text box below.

MOD Administrator

Global Administrator

617172c1-97c9-45ef-8415-fd13134d...

Select Debra Berger from the list of users.


labclient.labondemand.com
Users - Microsoft Entra admin ce
https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenant...
Microsoft Entra a...
Search resources, services, and docs (G+/)
Copilot
Home >
Users
Contoso
New user
Edit (Preview)
Delete
Download users
Bulk operations
Refresh
Azure Active Directory is now Microsoft Entra ID.
Debra
Add filter
1 user found

Display name	User principal name	User type	On-premises sy...
Debra Berger	DebraB@WWLx730857.O...	Member	No

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

Instructions
Resources
Help
100%

your admin credentials.

a. In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.

b. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.

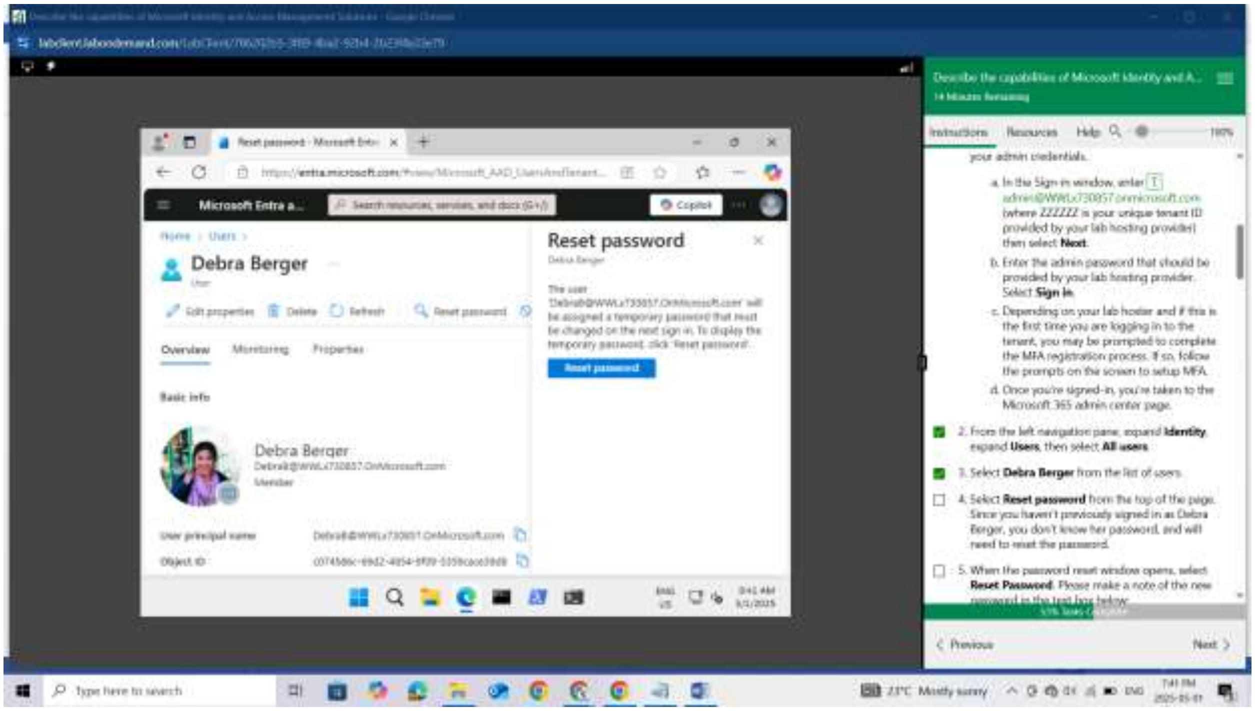
☑ 2. From the left navigation pane, expand **Identity**, expand **Users**, then select **All users**.

☑ 3. Select **Debra Berger** from the list of users.

□ 4. Select **Reset password** from the top of the page. Since you haven't previously signed in as Debra Berger, you don't know her password, and will need to reset the password.

□ 5. When the password reset window opens, select **Reset Password**. Please make a note of the new password in the text box below.

Select Reset password from the top of the page. Since you haven't previously signed in as Debra Berger, you don’t know her password, and will need to reset the password.



Debra Berger
DebraB@WWLx730857.OnMicrosoft.com
Member

User principal name: DebraB@WWLx730857.OnMicrosoft.com
Object ID: c0745b6c-69d2-4854-9f09-5358ca0d9fd8

Reset password
Debra Berger

The user 'DebraB@WWLx730857.OnMicrosoft.com' will be assigned a temporary password that must be changed on the next sign in. To display the temporary password, click 'Reset password'.

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

your admin credentials.

a. In the Sign-in window, enter admin@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.

b. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.

c. Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

d. Once you're signed-in, you're taken to the Microsoft 365 admin center page.

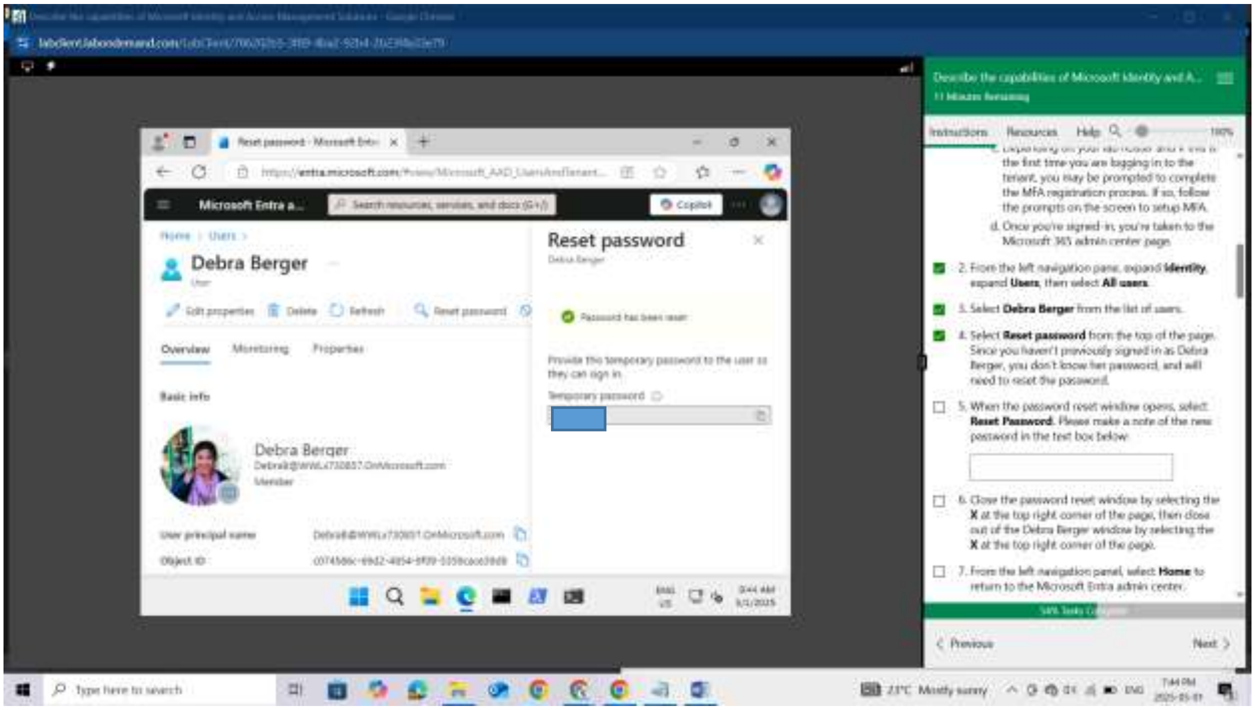
☑ 2. From the left navigation pane, expand **Identity**, expand **Users**, then select **All users**.

☑ 3. Select **Debra Berger** from the list of users.

□ 4. Select **Reset password** from the top of the page. Since you haven't previously signed in as Debra Berger, you don't know her password, and will need to reset the password.

□ 5. When the password reset window opens, select **Reset Password**. Please make a note of the new password in the text box below.

When the password reset window opens, select Reset Password. Please make a note of the new password in the text box below:



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

the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

d. Once you're signed in, you're taken to the Microsoft 365 admin center page.

☑ 2. From the left navigation pane, expand **Identity**, expand **Users**, then select **All users**.

☑ 3. Select **Debra Berger** from the list of users.

☑ 4. Select **Reset password** from the top of the page. Since you haven't previously signed in as Debra Berger, you don't know her password, and will need to reset the password.

□ 5. When the password reset window opens, select **Reset Password**. Please make a note of the new password in the text box below:

□ 6. Close the password reset window by selecting the **X** at the top right corner of the page, then close out of the Debra Berger window by selecting the **X** at the top right corner of the page.

□ 7. From the left navigation panel, select **Home** to return to the Microsoft Entra admin center.

Reset password

Debra Berger

Password has been reset

Provide this temporary password to the user so they can sign in.

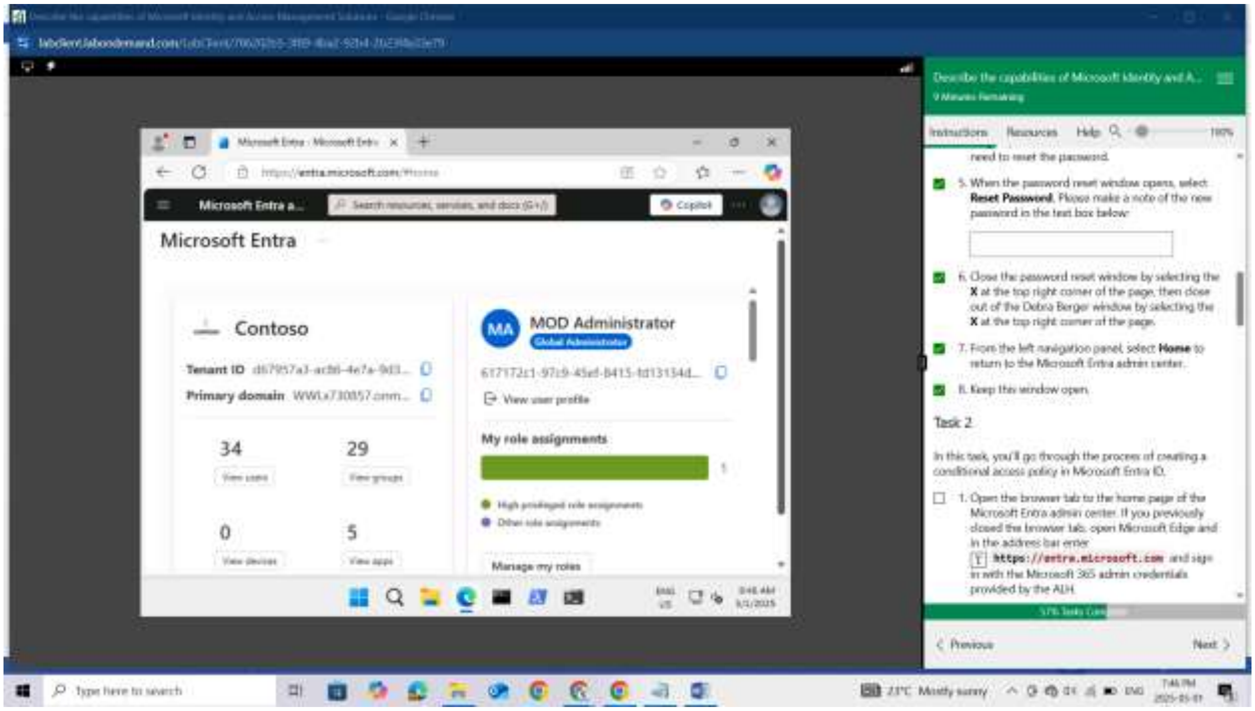
Temporary password

[redacted]

Close the password reset window by selecting the X at the top right corner of the page, then close out of the Debra Berger window by selecting the X at the top right corner of the page.

From the left navigation panel, select Home to return to the Microsoft Entra admin center.

Keep this window open.



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

need to reset the password.

☑ 5. When the password reset window opens, select **Reset Password**. Please make a note of the new password in the text box below:

☑ 6. Close the password reset window by selecting the **X** at the top right corner of the page, then close out of the Debra Berger window by selecting the **X** at the top right corner of the page.

☑ 7. From the left navigation panel, select **Home** to return to the Microsoft Entra admin center.

☑ 8. Keep this window open.

Task 2

In this task, you'll go through the process of creating a conditional access policy in Microsoft Entra ID.

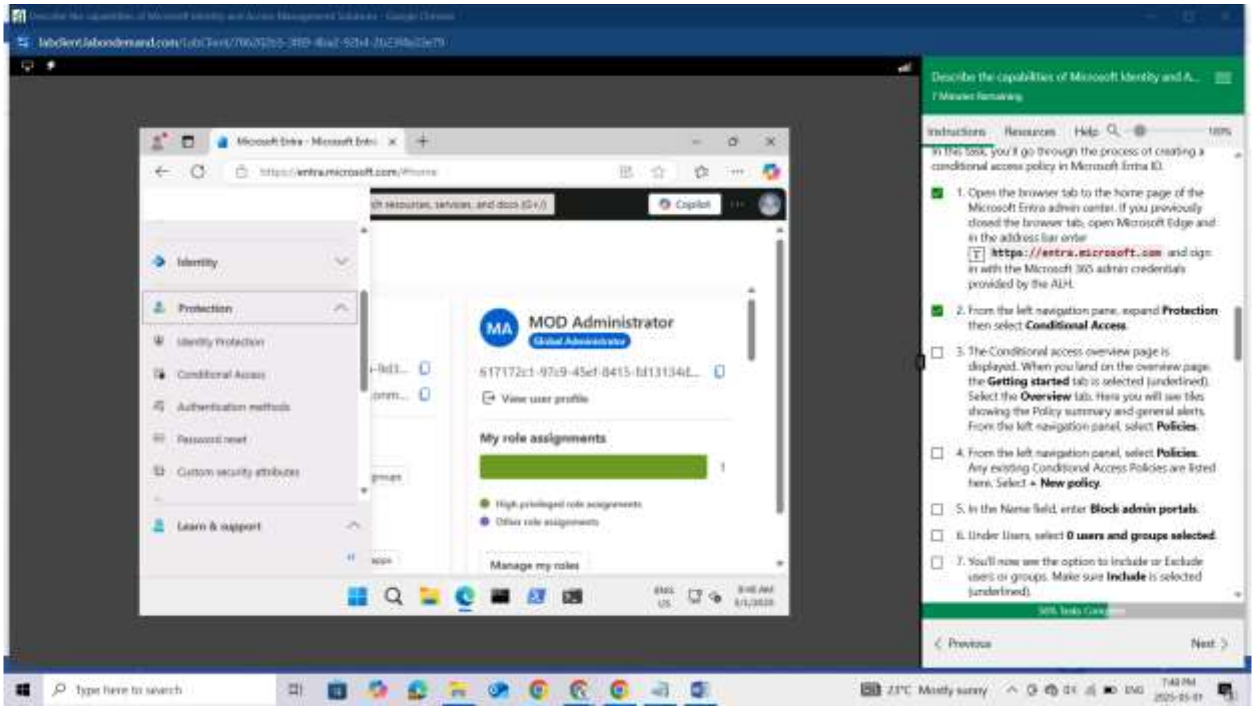
□ 1. Open the browser tab to the home page of the Microsoft Entra admin center. If you previously closed the browser tab, open Microsoft Edge and in the address bar enter `https://entra.microsoft.com` and sign in with the Microsoft 365 admin credentials provided by the ALH.

Task 2

In this task, you'll go through the process of creating a conditional access policy in Microsoft Entra ID.

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.

From the left navigation pane, expand Protection then select Conditional Access.



Describe the capabilities of Microsoft Identity and A...

7 Minutes Remaining

In this task, you'll go through the process of creating a 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**.

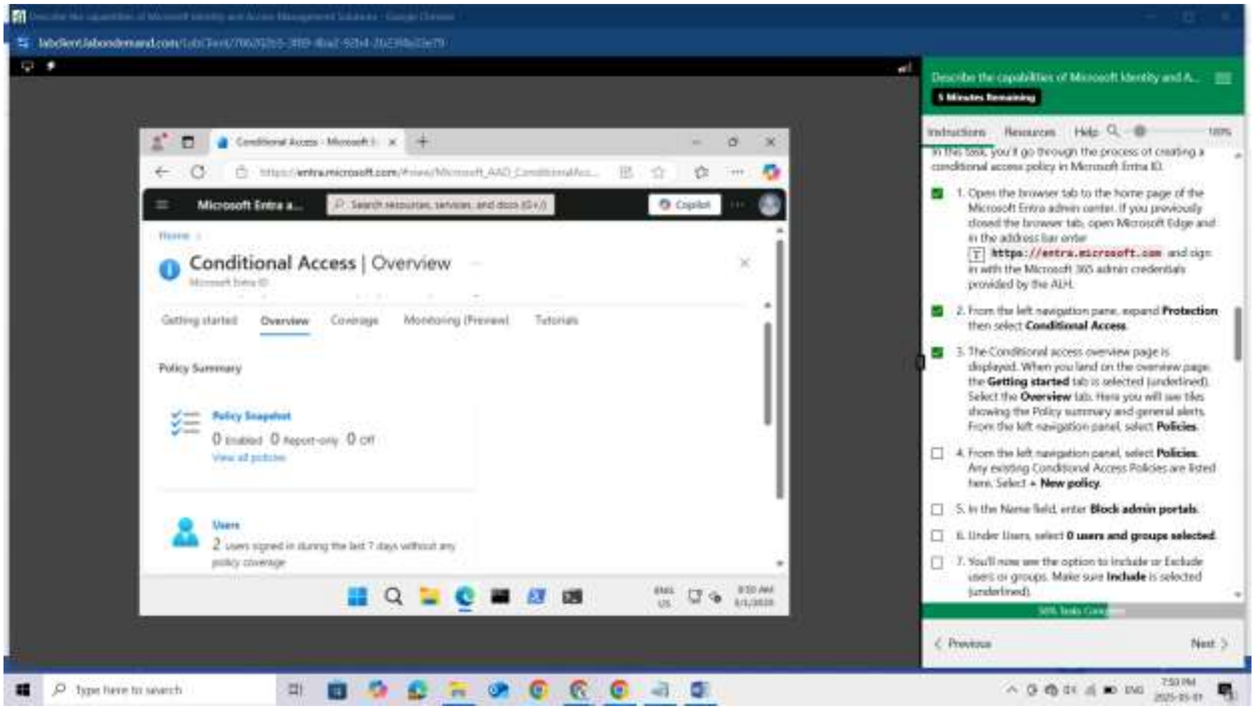
□ 4. From the left navigation panel, select **Policies**. Any existing Conditional Access Policies are listed here. Select + **New policy**.

□ 5. In the Name field, enter **Block admin portals**.

□ 6. Under Users, select **0 users and groups selected**.

□ 7. You'll now see the option to Include or Exclude users or groups. Make sure **Include** is selected (underlined).

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.



Describe the capabilities of Microsoft Identity and A...

5 Minutes Remaining

Home >

Conditional Access | Overview

Microsoft Entra ID

Policy Summary

Policy Snapshot

0 Enabled 0 Report-only 0 Off

View all policies

Users

2 users signed in during the last 7 days without any policy coverage

In this task, you'll go through the process of creating a 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**.

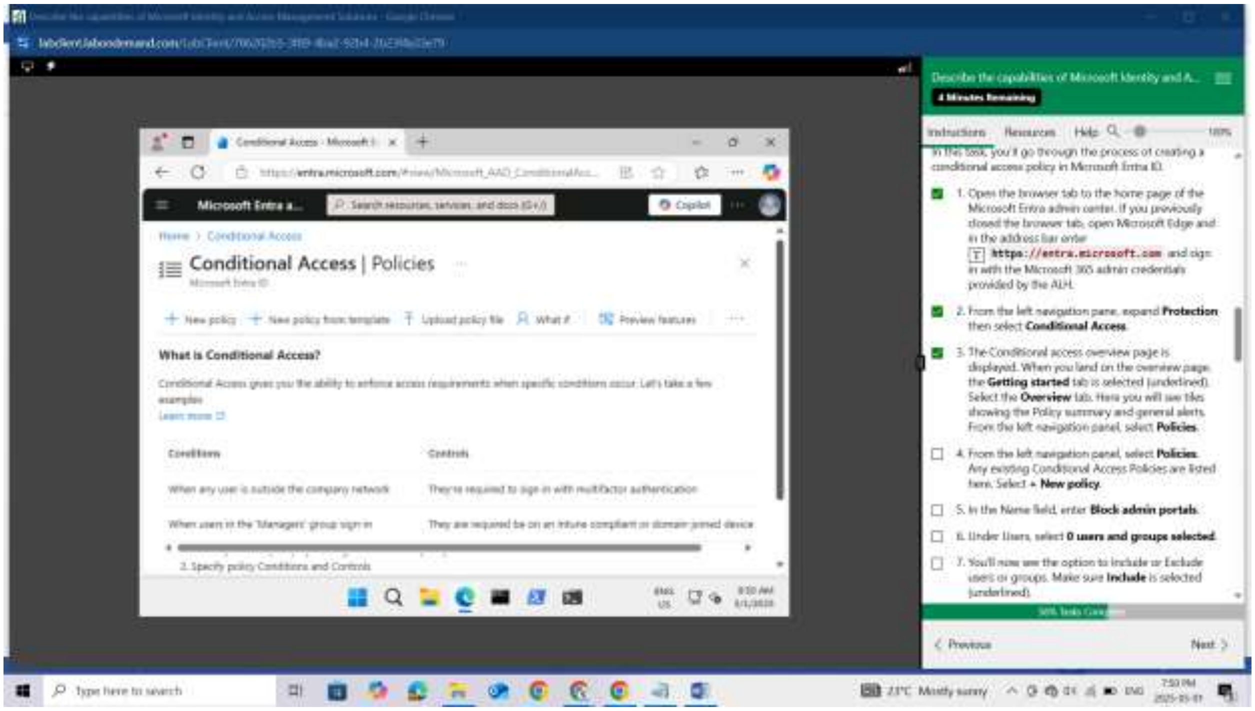
□ 4. From the left navigation panel, select **Policies**. Any existing Conditional Access Policies are listed here. Select + **New policy**.

□ 5. In the Name field, enter **Block admin portals**.

□ 6. Under Users, select **0 users and groups selected**.

□ 7. You'll now see the option to include or Exclude users or groups. Make sure **Include** is selected (underlined).

From the left navigation panel, select Policies.



Describe the capabilities of Microsoft Identity and A...

4 Minutes Remaining

Home > Conditional Access

Conditional Access | Policies

Microsoft Entra ID

What is Conditional Access?

Conditional Access gives you the ability to enforce access requirements when specific conditions occur. Let's take a few examples

Learn more

Conditions	Controls
When any user is outside the company network	They're required to sign in with multifactor authentication
When users in the 'Managers' group sign in	They are required be on an Intune compliant or domain joined device

2. Specify policy Conditions and Controls

In this task, you'll go through the process of creating a 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**.

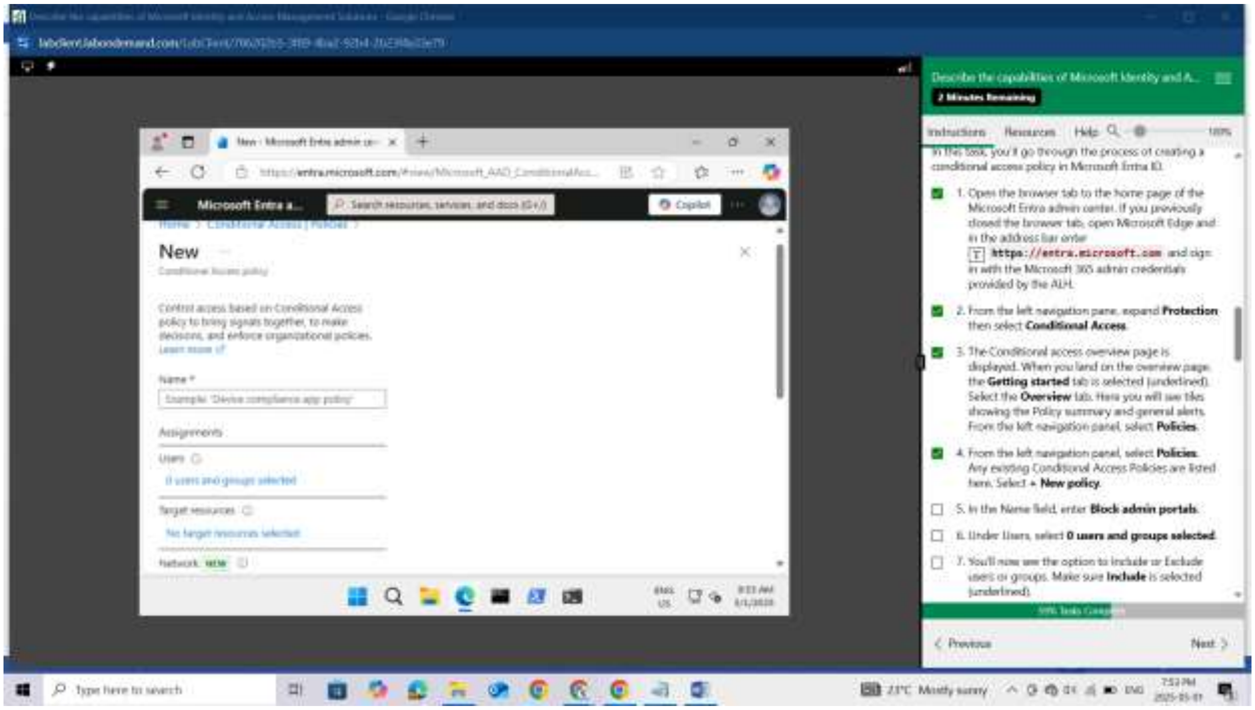
□ 4. From the left navigation panel, select **Policies**. Any existing Conditional Access Policies are listed here. Select + **New policy**.

□ 5. In the Name field, enter **Block admin portals**.

□ 6. Under Users, select **0 users and groups selected**.

□ 7. You'll now see the option to include or Exclude users or groups. Make sure **Include** is selected (underlined).

Any existing Conditional Access Policies are listed here. Select + New policy.



Describe the capabilities of Microsoft Identity and A...

2 Minutes Remaining

In this task, you'll go through the process of creating a 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**.

☐ 7. You'll now see the option to Include or Exclude users or groups. Make sure **Include** is selected (underlined).

New

Conditional Access policy

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

Name *: Example: 'Device compliance app policy'

Assignments

Users: 0 users and groups selected

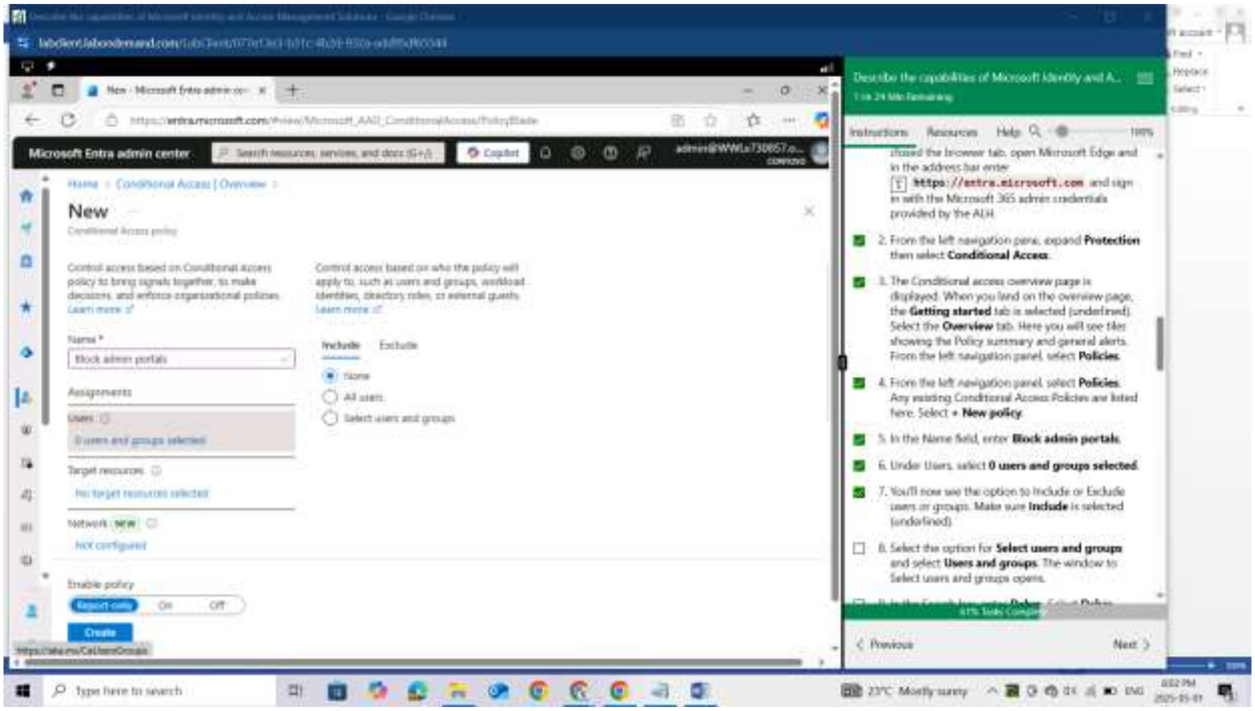
Target resources: No target resources selected

Network NEW

In the Name field, enter Block admin portals.

Under Users, select 0 users and groups selected.

You'll now see the option to Include or Exclude users or groups. Make sure Include is selected (underlined).



Describe the capabilities of Microsoft Identity and A...

1 Hr 24 Min Remaining

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**.

☑ 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.

New

Conditional Access policy

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

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

Name *: Block admin portals

Assignments

Users: 0 users and groups selected

Target resources: No target resources selected

Network NEW: Not configured

Include | Exclude

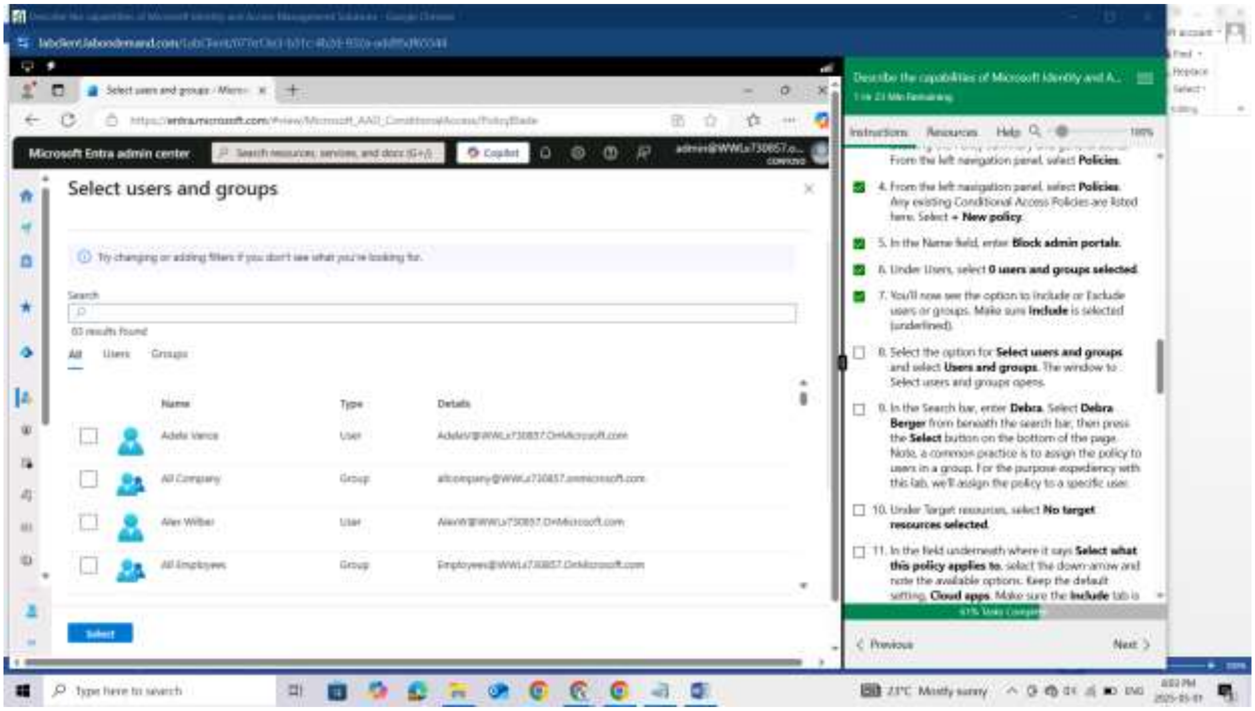
● None
○ All users
○ Select users and groups

Enable policy: Report-only | On | Off

Create

Instructions
Resources
Help
100%
Previous
Next
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home > Conditional Access | Overview >
Learn more
https://aka.ms/CaUsersGroups
23°C Mostly sunny
Type here to search

Select the option for Select users and groups and select Users and groups. The window to Select users and groups opens.



Microsoft Entra admin center

Select users and groups

ⓘ Try changing or adding filters if you don't see what you're looking for.

Search

63 results found

All | Users | Groups

	Name	Type	Details
□	Adele Vance	User	AdeleV@WWLx730857.OnMicrosoft.com
□	All Company	Group	allcompany@WWLx730857.onmicrosoft.com
□	Alex Wilber	User	AlexW@WWLx730857.OnMicrosoft.com
□	All Employees	Group	Employees@WWLx730857.OnMicrosoft.com

Select

Describe the capabilities of Microsoft Identity and A...

Instructions | Resources | Help

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).

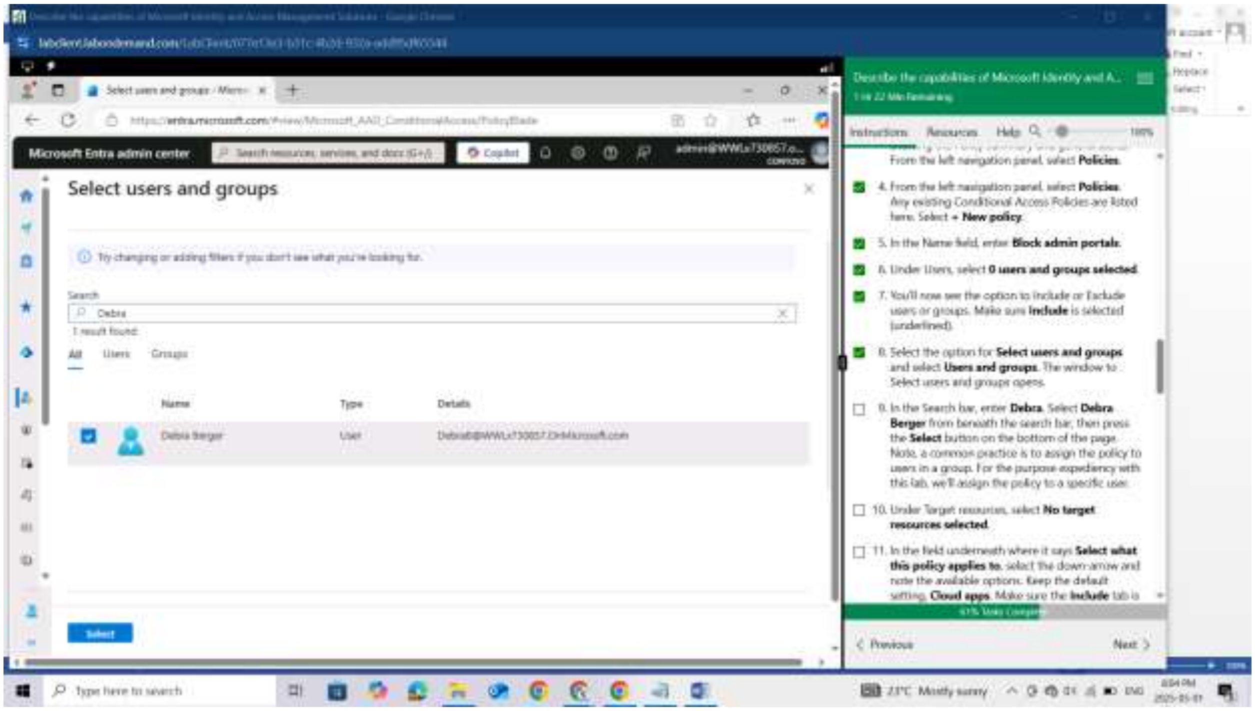
□ 8. Select the option for **Select users and groups** and select **Users and groups**. The window to Select users and groups opens.

□ 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. 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

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.



Microsoft Entra admin center

Select users and groups

ⓘ Try changing or adding filters if you don't see what you're looking for.

Search

Debra

1 result found

All | Users | Groups

	Name	Type	Details
☑	Debra Berger	User	DebraB@WWLx730857.OnMicrosoft.com

Select

Describe the capabilities of Microsoft Identity and A...

Instructions | Resources | Help

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).

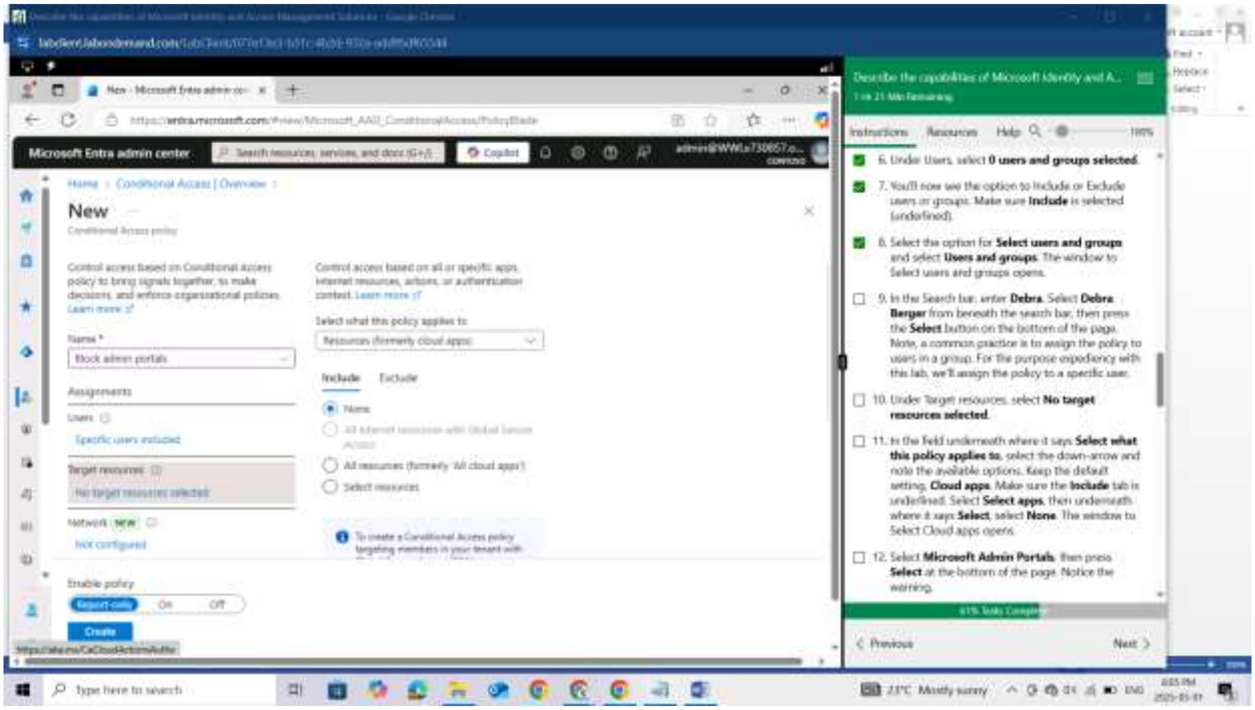
☑ 8. Select the option for **Select users and groups** and select **Users and groups**. The window to Select users and groups opens.

□ 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. 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

Under Target resources, select No target resources selected.



Microsoft Entra admin center

Home > Conditional Access | Overview >

New

Conditional Access policy

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: No target resources selected

Network NEW: Not configured

Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to: Resources (formerly cloud apps)

Include | Exclude

● None

○ All internet resources with Global Secure Access

○ All resources (formerly 'All cloud apps')

○ Select resources

To create a Conditional Access policy targeting members in your tenant with

Enable policy: Report-only | On | Off

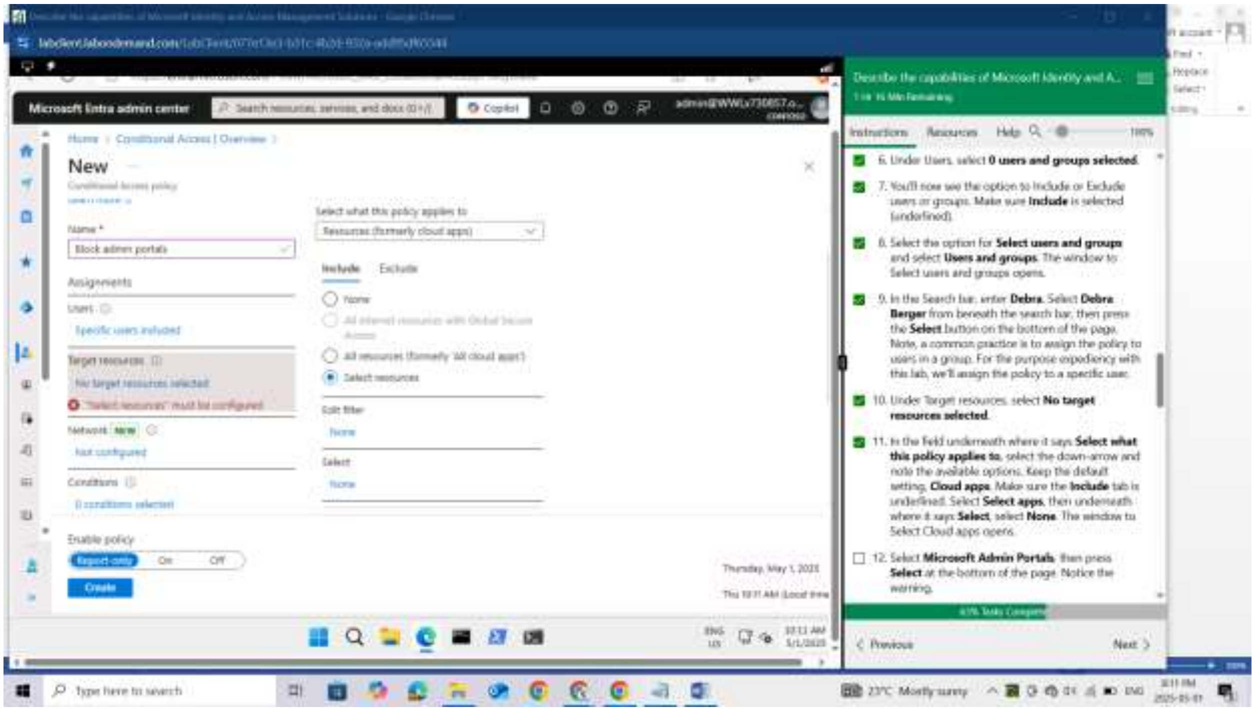
Create

Describe the capabilities of Microsoft Identity and A...

1 Hr 21 Min Remaining

- ☑ 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. 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.

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.



Microsoft Entra admin center

Home > Conditional Access | Overview >

New

Conditional Access policy

Name *: Block admin portals

Assignments

Users: Specific users included

Target resources: No target resources selected

"Select resources" must be configured

Network NEW: Not configured

Conditions: 0 conditions selected

Select what this policy applies to: Resources (formerly cloud apps)

Include | Exclude

○ None

○ All internet resources with Global Secure Access

○ All resources (formerly 'All cloud apps')

● Select resources

Edit filter: None

Select: None

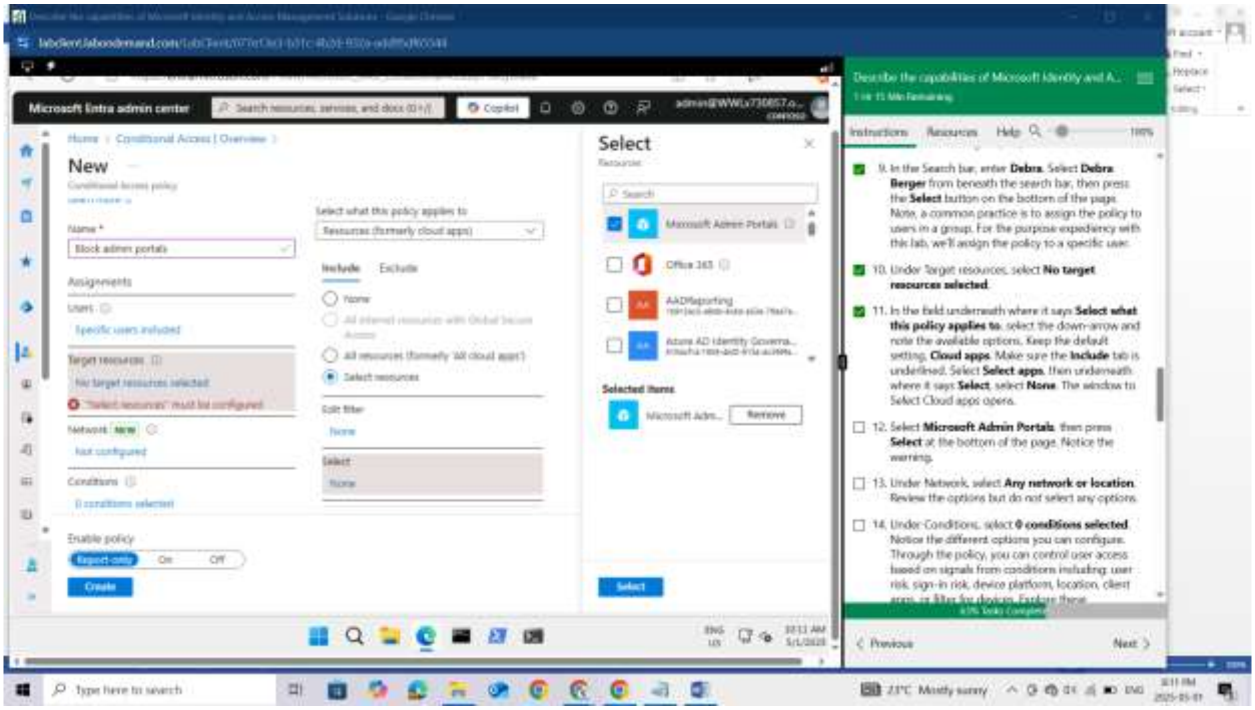
Enable policy: Report-only | On | Off

Create

Describe the capabilities of Microsoft Identity and A...

- ☑ 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. 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.

Select Microsoft Admin Portals, then press Select at the bottom of the page. Notice the warning.



Describe the capabilities of Microsoft Identity and A...

Instructions Resources Help

☑ 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**.

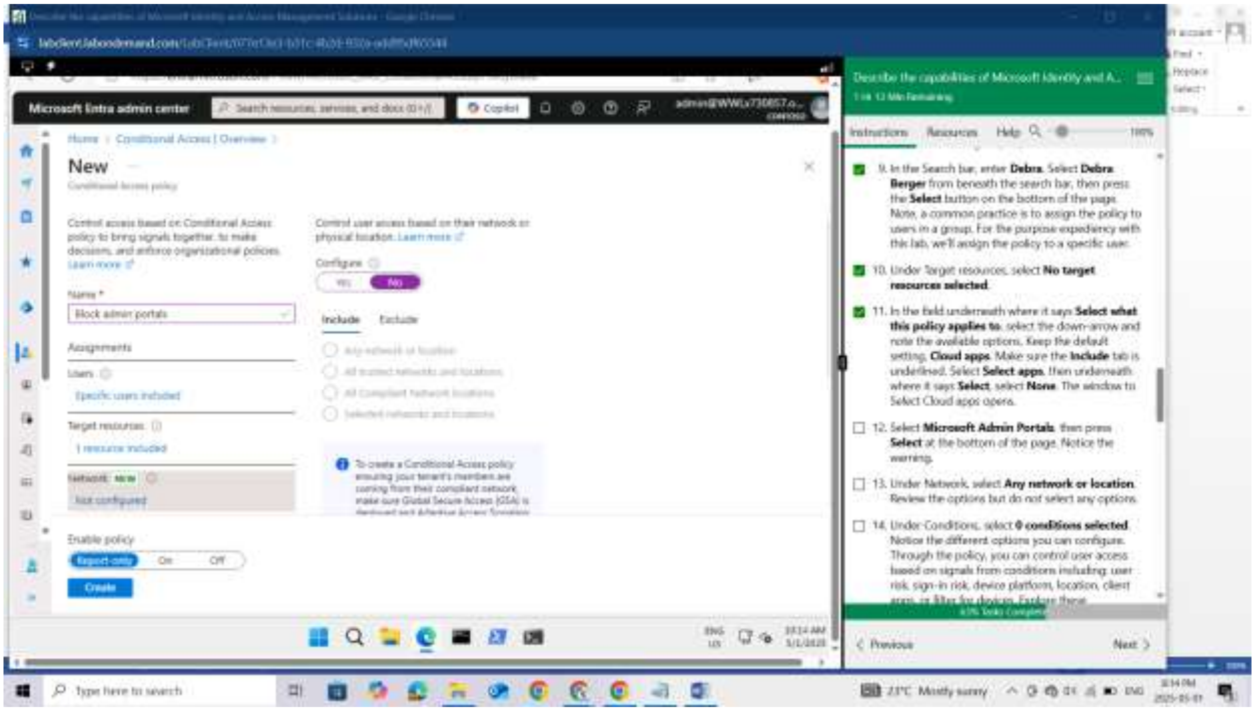
☑ 11. In the field underneath where it says **Select what this policy applies to**, select the down-arrow and note the available options. Keep the default setting, **Cloud apps**. Make sure the **Include** tab is underlined. Select **Select apps**. then underneath where it says **Select**, select **None**. 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**. Notice the different options you can configure. Through the policy, you can control user access based on signals from conditions including: user risk, sign-in risk, device platform, location, client apps, or filter for devices. Explore these

Under Network, select Any network or location. Review the options but do not select any options.



☑ 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.

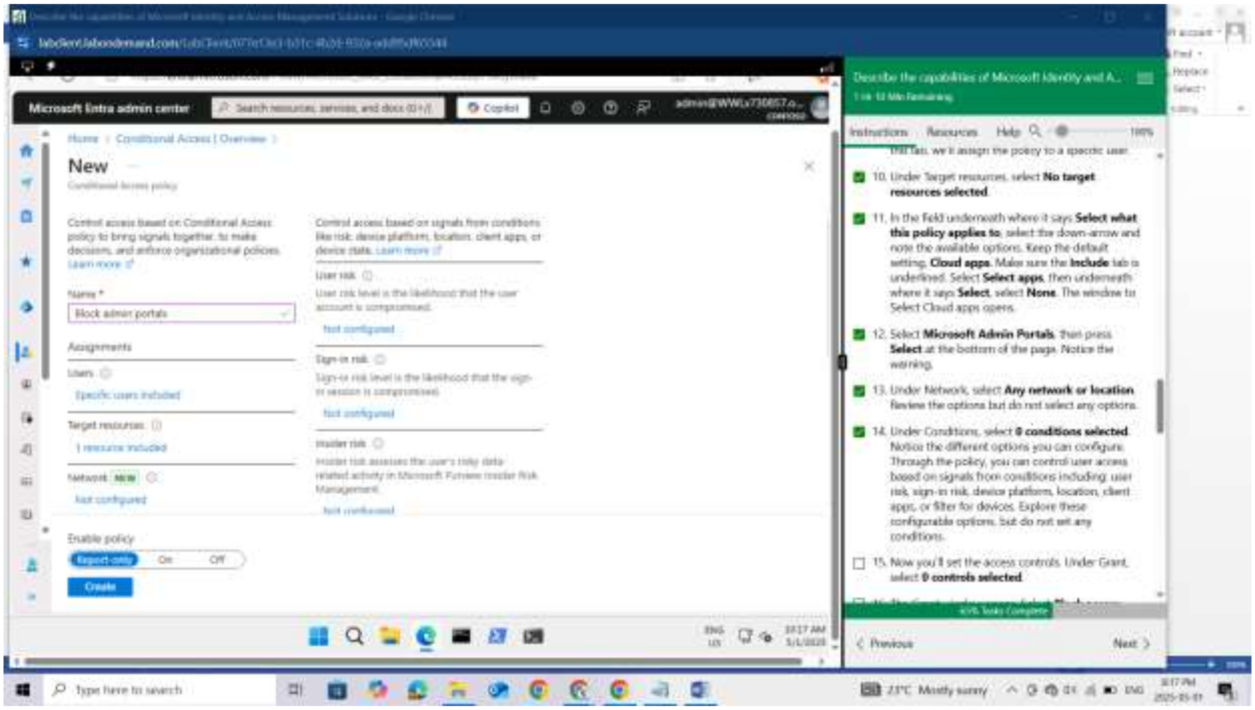
□ 13. Under Network, select **Any network or location**. Review the options but do not select any options.

□ 14. Under Conditions, select **0 conditions selected**. Notice the different options you can configure. Through the policy, you can control user access based on signals from conditions including: user risk, sign-in risk, device platform, location, client apps, or filter for devices. Explore these

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

Control user access based on their network or physical location.

Under Conditions, select 0 conditions selected. Notice the different options you can configure. Through the policy, you can control user access 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.



Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home > Conditional Access | Overview >
New
Conditional Access policy
Instructions
Resources
Help
100%
Previous
Next
Type here to search
23°C Mostly sunny

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

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

Name *: Block admin portals

Assignments

Users: Specific users included

Target resources: 1 resource included

Network NEW: Not configured

User risk: User risk level is the likelihood that the user account is compromised. Not configured

Sign-in risk: Sign-in risk level is the likelihood that the sign-in session is compromised. Not configured

Insider risk: Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management. Not configured

Enable policy: ● Report-only ○ On ○ Off

Create

Describe the capabilities of Microsoft Identity and A...

this task, 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.

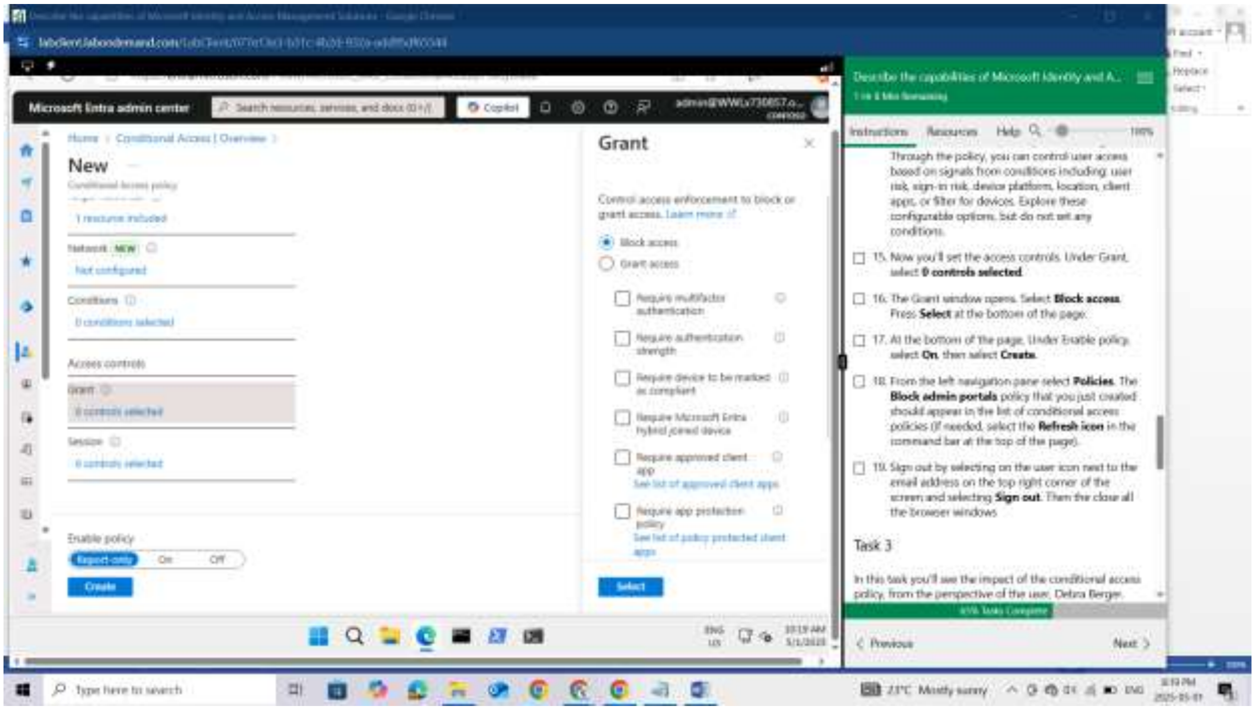
☑ 14. Under Conditions, select **0 conditions selected**. Notice the different options you can configure. Through the policy, you can control user access based on signals from conditions including: user risk, sign-in risk, device platform, location, client apps, or filter for devices. Explore these configurable options, but do not set any conditions.

☐ 15. Now you'll set the access controls. Under Grant, select **0 controls selected**.

65% Tasks Complete

Now you'll set the access controls. Under Grant, select 0 controls selected

The Grant window opens. Select Block access. Press Select at the bottom of the page.



Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home > Conditional Access | Overview >
New
Conditional Access policy
Instructions
Resources
Help
100%
Previous
Next
Type here to search
23°C Mostly sunny

1 resource included

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Session: 0 controls selected

Enable policy: ● Report-only ○ On ○ Off

Create

Grant

Control access enforcement to block or grant access. Learn more

● Block access

○ Grant access

☐ Require multifactor authentication

☐ Require authentication strength

☐ Require device to be marked as compliant

☐ Require Microsoft Entra hybrid joined device

☐ Require approved client app
See list of approved client apps

☐ Require app protection policy
See list of policy protected client apps

Select

Describe the capabilities of Microsoft Identity and A...

Through the policy, you can control user access 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).

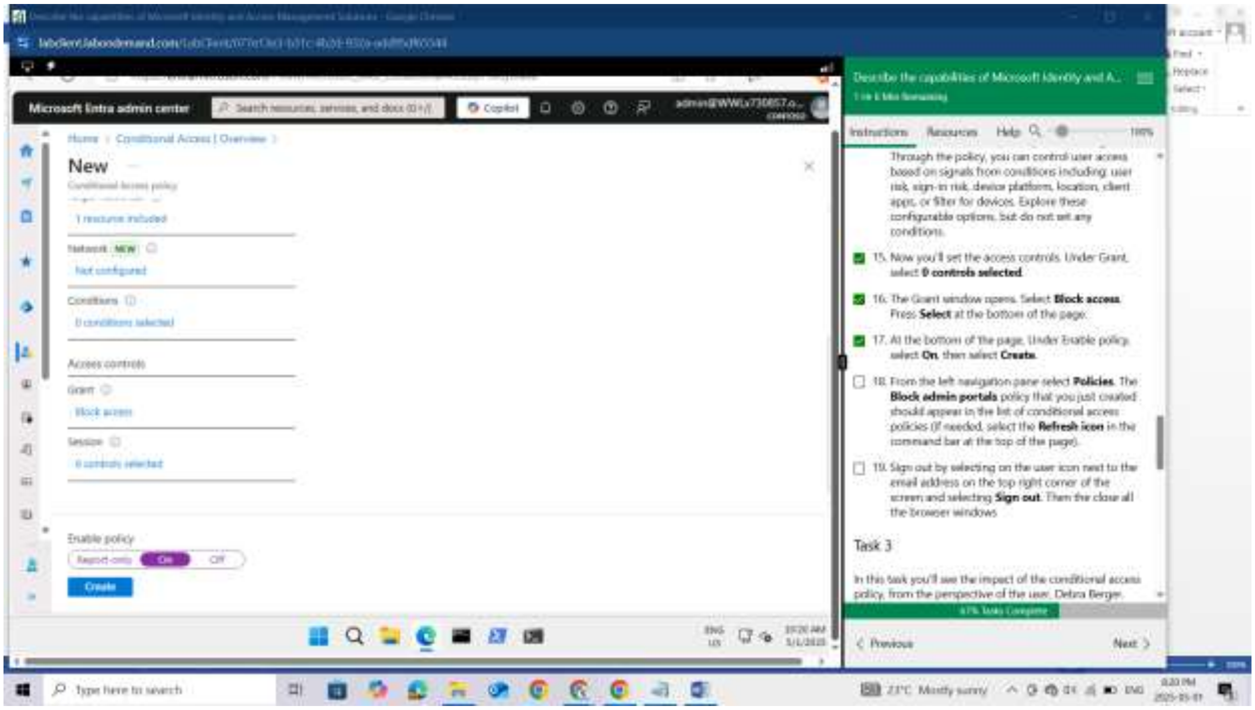
☐ 19. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting **Sign out**. Then the close all the browser windows.

Task 3

In this task you'll see the impact of the conditional access policy, from the perspective of the user, Debra Berger.

65% Tasks Complete

At the bottom of the page, Under Enable policy, select On, then select Create.



Microsoft Entra admin center

Home > Conditional Access | Overview >

New

Conditional Access policy

1 resource included

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

Report-only | On | Off

Create

Describe the capabilities of Microsoft Identity and A...

Instructions Resources Help 100%

Through the policy, you can control user access 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).

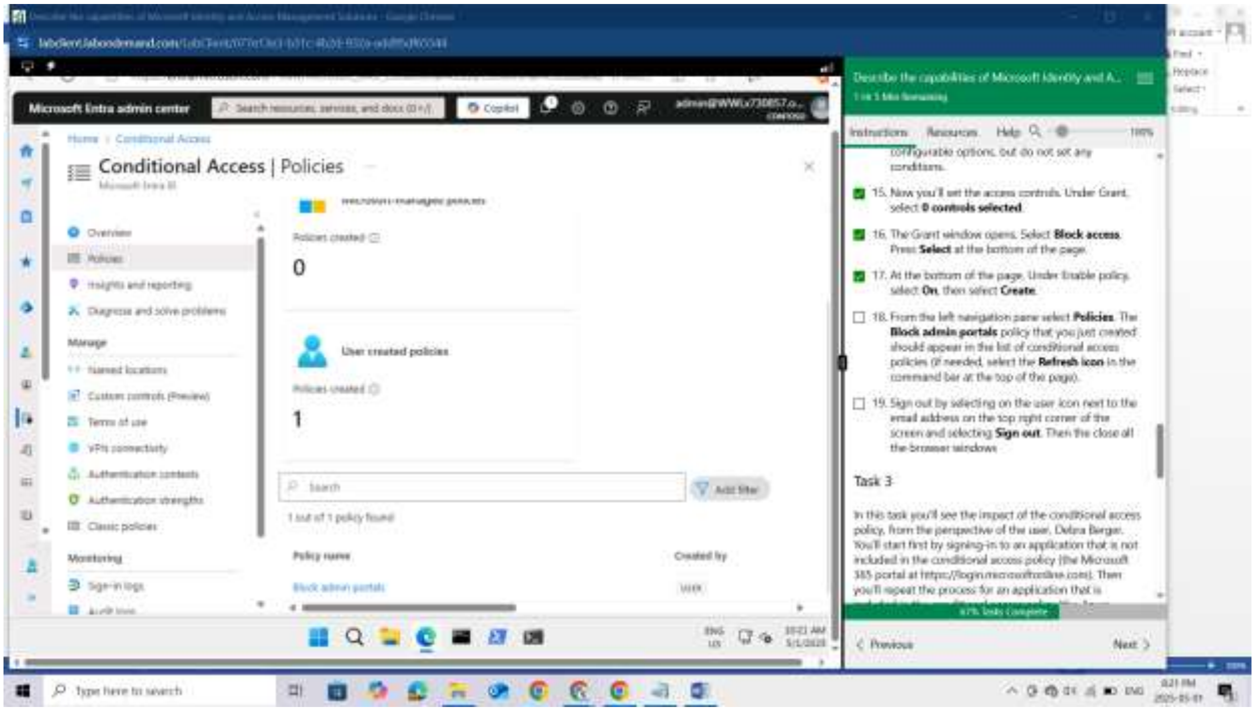
□ 19. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting **Sign out**. Then the close all the browser windows

Task 3

In this task you'll see the impact of the conditional access policy, from the perspective of the user, Debra Berger.

< Previous Next >

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).



Microsoft Entra admin center

Home > Conditional Access

Conditional Access | Policies

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

Monitoring

Sign-in logs

Microsoft-managed policies

Policies created 0

User created policies

Policies created 1

Search

Add filter

1 out of 1 policy found

Policy name	Created by
Block admin portals	User

Describe the capabilities of Microsoft Identity and A...

Instructions Resources Help 100%

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).

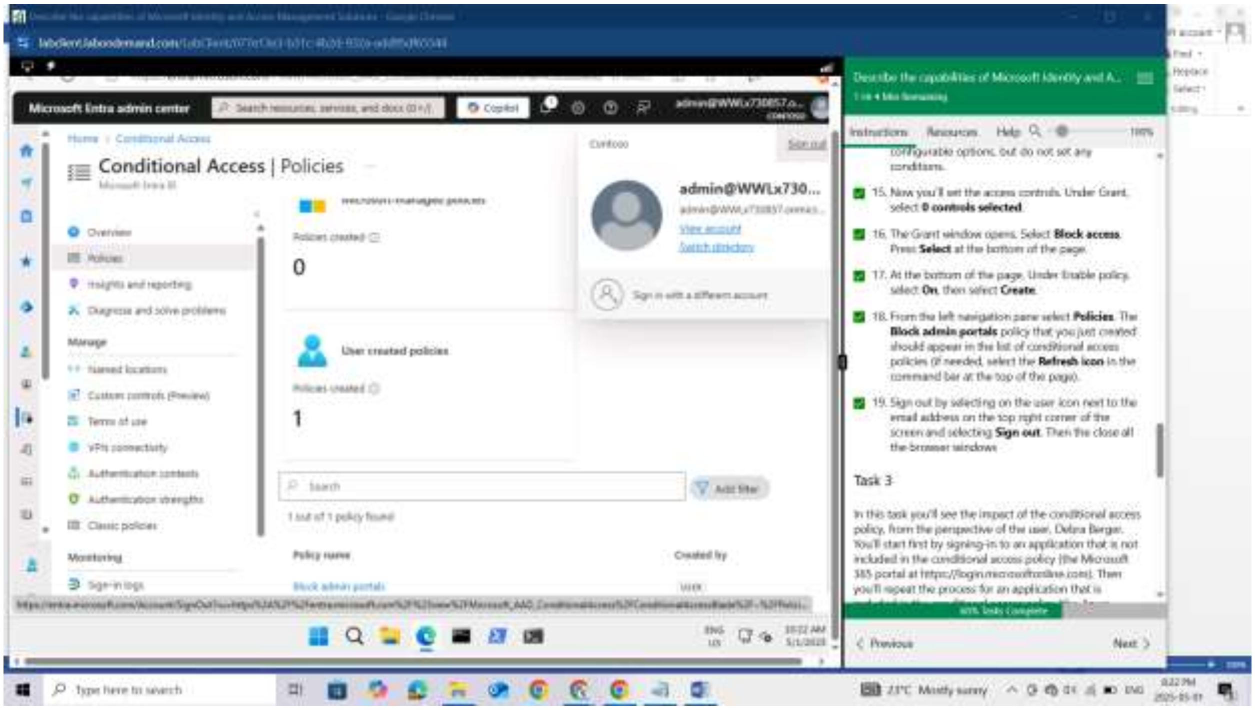
□ 19. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting **Sign out**. Then the close all the browser windows

Task 3

In this task you'll see the impact of the conditional access policy, from the perspective of the user, Debra Berger. You'll start first by signing-in to an application that is not included in the conditional access policy (the Microsoft 365 portal at https://login.microsoftonline.com). Then you'll repeat the process for an application that is

< Previous Next >

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



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

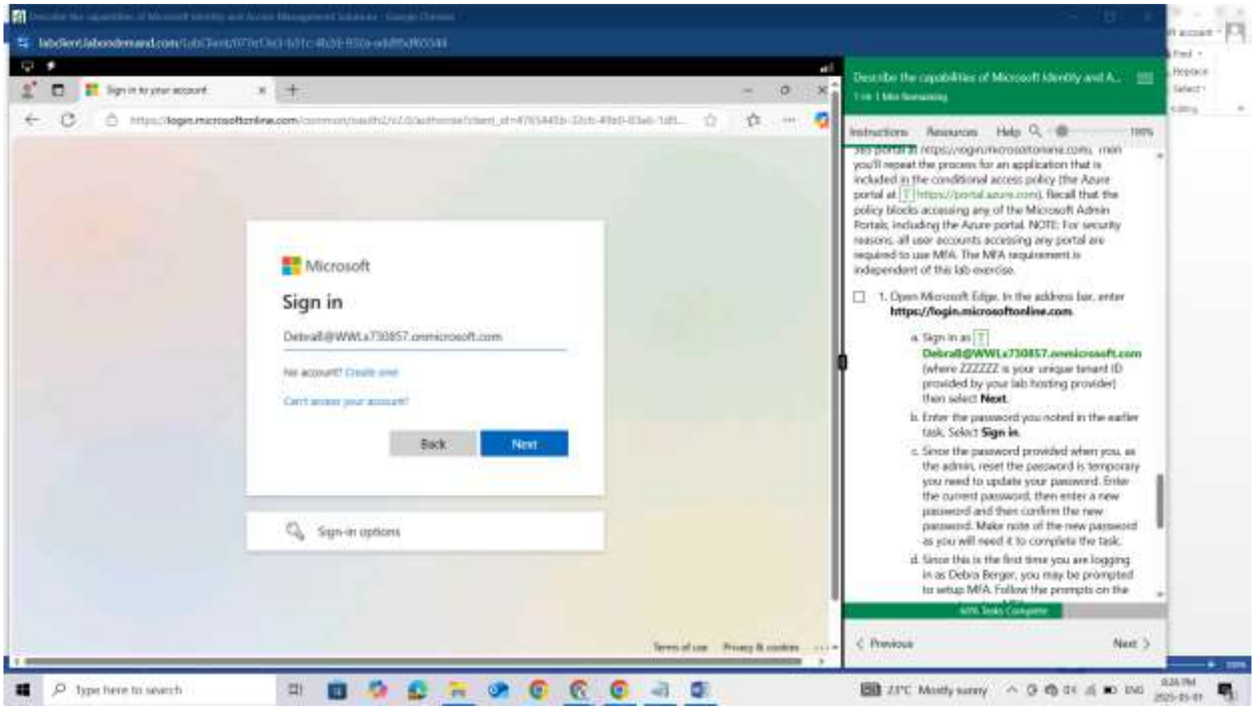
In this task you'll see the impact of the conditional access policy, from the perspective of the user, Debra Berger. You'll start first by signing-in to an application that is not included in the conditional access policy (the Microsoft 365 portal at https://login.microsoftonline.com). Then you'll repeat the process for an application that is

Task 3

In this task you'll see the impact of the conditional access policy, from the perspective of the user, Debra Berger. You'll start first by signing-in to an application that is not included in the conditional access policy (the Microsoft 365 portal at https://login.microsoftonline.com). Then you'll repeat the process for an application that is included in the conditional access policy (the Azure portal at https://portal.azure.com). Recall that the policy blocks accessing any of the Microsoft Admin Portals, including the Azure portal. NOTE: For security reasons, all user accounts accessing any portal are required to use MFA. The MFA requirement is independent of this lab exercise.

Open Microsoft Edge. In the address bar, enter https://login.microsoftonline.com.

Sign in as DebraB@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select Next.


labclient.labondemand.com
Sign in to your account
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d9...
Microsoft
Sign in
Debra8@WWLx730857.onmicrosoft.com
No account? Create one!
Can't access your account?
Back
Next
Sign-in options
Terms of use
Privacy & cookies
Describe the capabilities of Microsoft Identity and A...
1 Hr 1 Min Remaining
Instructions
Resources
Help
100%
60% Tasks Complete
Previous
Next
Type here to search
23°C Mostly sunny
ENG

365 portal at https://login.microsoftonline.com), then you'll repeat the process for an application that is included in the conditional access policy (the Azure portal at T https://portal.azure.com). Recall that the policy blocks accessing any of the Microsoft Admin Portals, including the Azure portal. NOTE: For security reasons, all user accounts accessing any portal are required to use MFA. The MFA requirement is independent of this lab exercise.

□ 1. Open Microsoft Edge. In the address bar, enter **https://login.microsoftonline.com**.

a. Sign in as T Debra8@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.

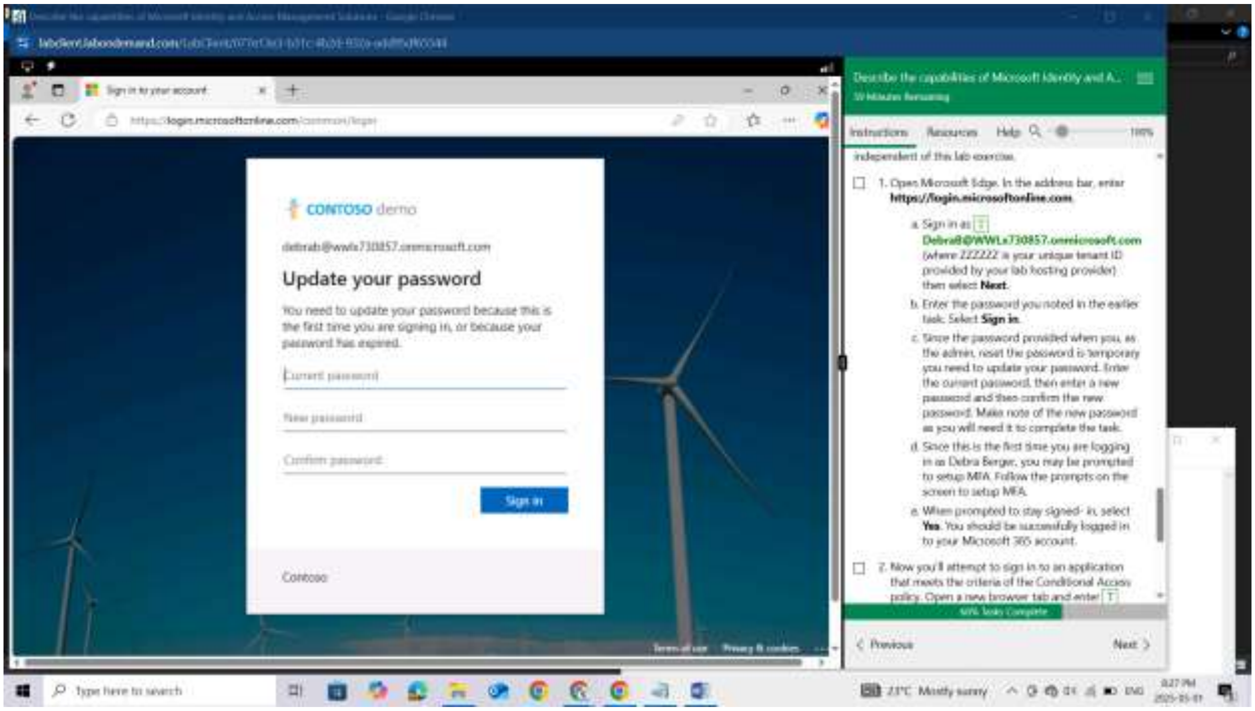
b. Enter the password you noted in the earlier task. Select **Sign in**.

c. Since the password provided when you, as the admin, reset the password is temporary you need to update your password. Enter the current password, then enter a new 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

Enter the password you noted in the earlier task. Select Sign in.

Since the password provided when you, as the admin, reset the password is temporary you need to update your password. Enter the current password, then enter a new password and then confirm the new password. Make note of the new password as you will need it to complete the task.


labclient.labondemand.com
Sign in to your account
https://login.microsoftonline.com/common/login
CONTOSO demo
debrab@wwlx730857.onmicrosoft.com
Update your password
You need to update your password because this is the first time you are signing in, or because your password has expired.
Current password
New password
Confirm password
Sign in
Contoso
Terms of use
Privacy & cookies
Describe the capabilities of Microsoft Identity and A...
59 Minutes Remaining
Instructions
Resources
Help
100%
60% Tasks Complete
Previous
Next
Type here to search
23°C Mostly sunny
ENG

independent of this lab exercise.

□ 1. Open Microsoft Edge. In the address bar, enter **https://login.microsoftonline.com**.

a. Sign in as T Debra8@WWLx730857.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.

b. Enter the password you noted in the earlier task. Select **Sign in**.

c. Since the password provided when you, as the admin, reset the password is temporary you need to update your password. Enter the current password, then enter a new password and then confirm the new password. Make note of the new password as you will need it to complete the task.

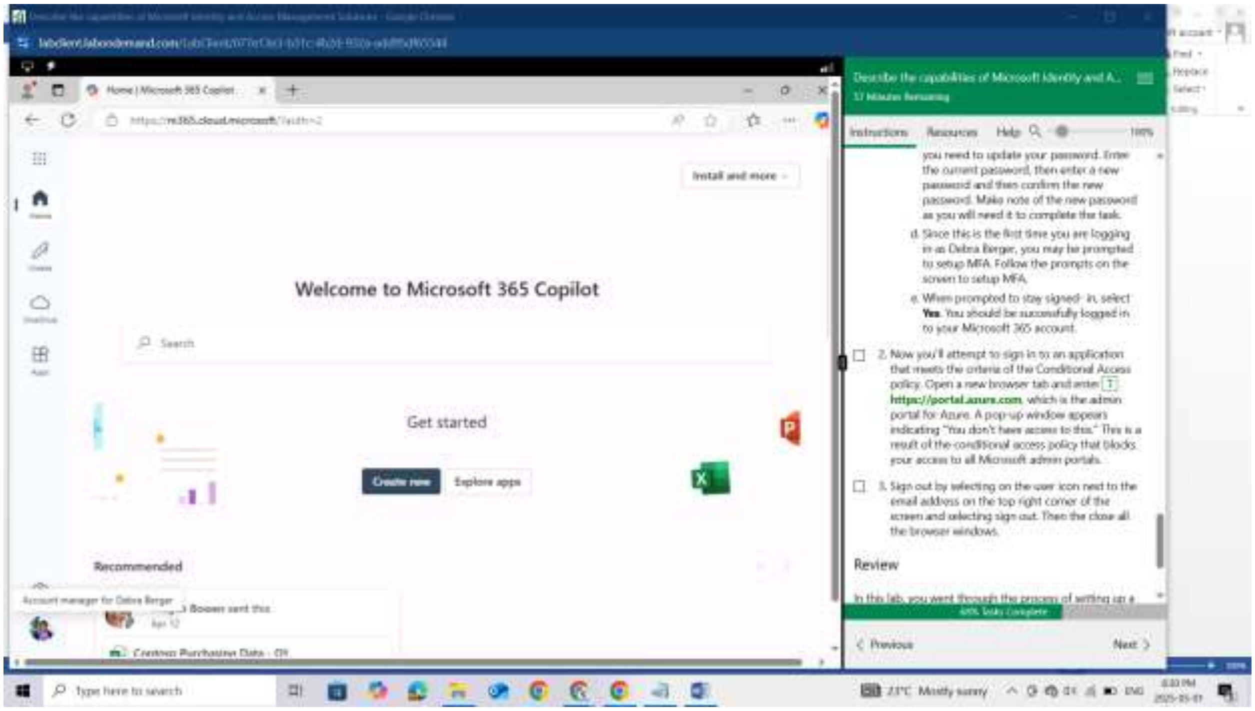
d. Since this is the first time you are logging in as Debra Berger, you may be prompted to setup MFA. Follow the prompts on the screen to setup MFA.

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

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.

When prompted to stay signed- in, select Yes. You should be successfully logged in to your Microsoft 365 account.


labclient.labondemand.com
Home | Microsoft 365 Copilot
https://m365.cloud.microsoft/?auth=2
Install and more
Welcome to Microsoft 365 Copilot
Search
Get started
Create new
Explore apps
Recommended
Account manager for Debra Berger
Describe the capabilities of Microsoft Identity and A...
57 Minutes Remaining
Instructions
Resources
Help
100%
Review
60% Tasks Complete
Previous
Next
Type here to search
23°C Mostly sunny

you need to update your password. Enter the current password, then enter a new 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.

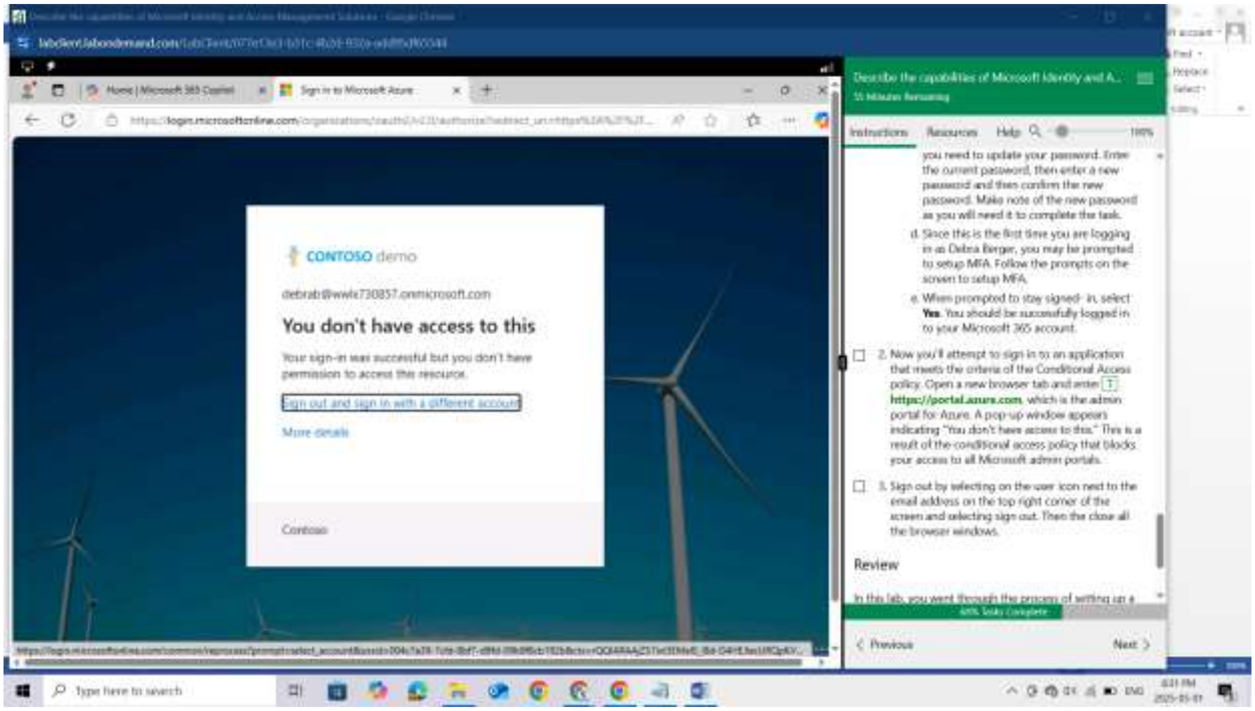
□ 2. Now you'll attempt to sign in to an application that meets the criteria of the Conditional Access policy. Open a new browser tab and enter https://portal.azure.com, which is the admin portal for Azure. A pop-up window appears indicating "You don't have access to this." This is a result of the conditional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

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.


labclient.labondemand.com
Home | Microsoft 365 Copilot
Sign in to Microsoft Azure
https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize?redirect_uri=https%3A%2F%2F...
CONTOSO demo
Contoso
Describe the capabilities of Microsoft Identity and A...
55 Minutes Remaining
Instructions
Resources
Help
100%
Review
60% Tasks Complete
Previous
Next
Type here to search

debrab@wwlx730857.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

you need to update your password. Enter the current password, then enter a new 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.

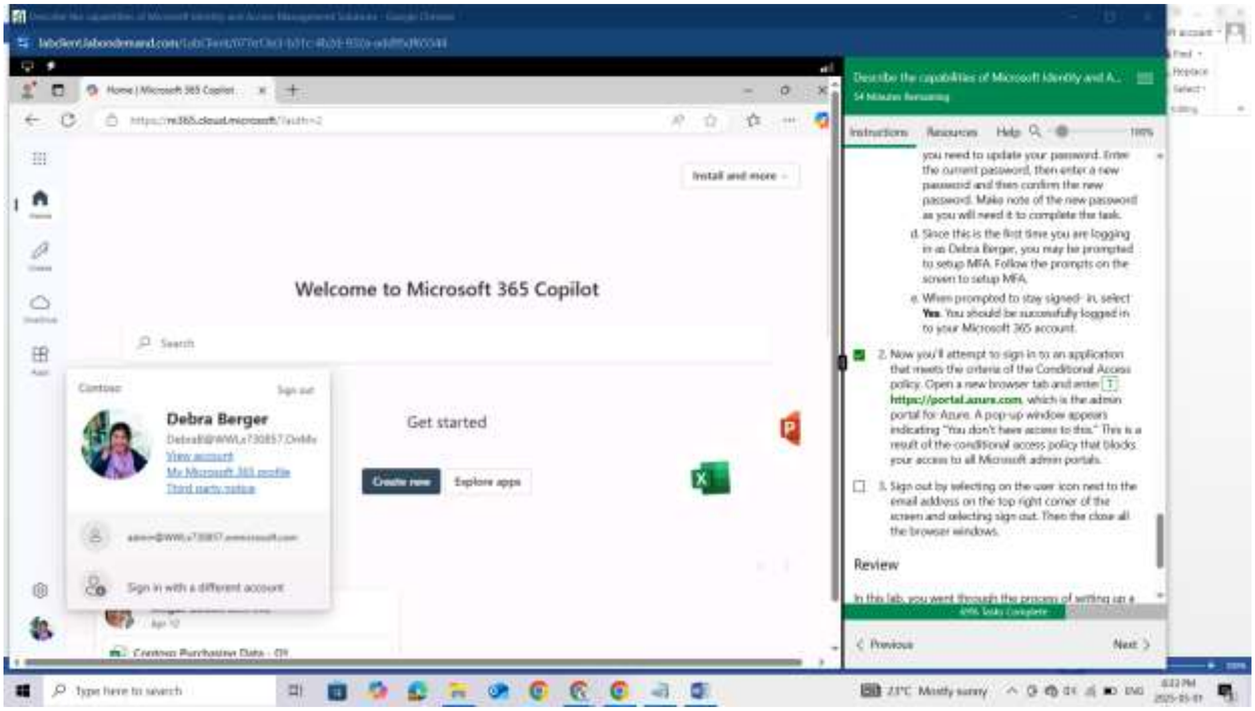
□ 2. Now you'll attempt to sign in to an application that meets the criteria of the Conditional Access policy. Open a new browser tab and enter https://portal.azure.com, which is the admin portal for Azure. A pop-up window appears indicating "You don't have access to this." This is a result of the conditional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

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.



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

you need to update your password. Enter the current password, then enter a new 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 **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

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.