



LAB GUIDE

SC-900



Microsoft Ready4AI&Security 2024
INFRA DIGITAL FOUNDATION

Create an Azure account

To use Azure, you need an Azure account. Your Azure account is the credential you use to sign into Azure services like the [Azure Portal](#) or [Cloud Shell](#).

Option 1: Use monthly Azure credits for Visual Studio subscribers

If you have a Visual Studio subscription, your subscription includes credits for using Azure. Activate your credits by visiting the [Monthly Azure credits for Visual Studio subscribers](#) page.

Option 2: Sign up for a free Azure account

You can create an [Azure account for free](#) and receive 12 months of popular services for free and a \$200 credit to explore Azure for 30 days.

Option 3: Sign up for a pay-as-you-go account

You can also create a [pay-as-you-go Azure account](#). This option includes monthly amounts of select services for free, and charges you for what you use beyond the free limits. There is no upfront commitment and you can cancel anytime.

Option 4: Use a corporate account

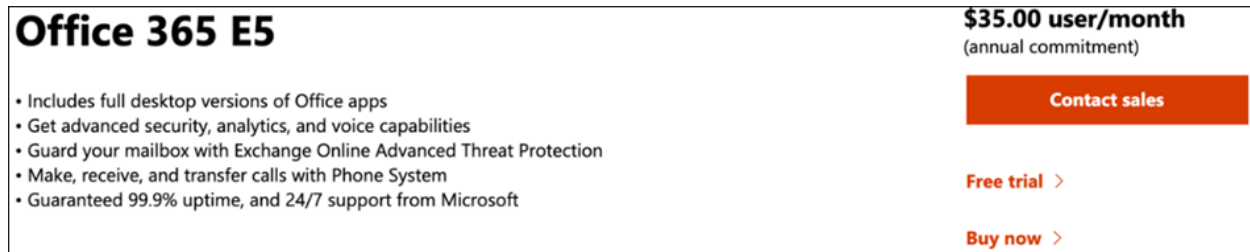
If you are using Azure at work, talk to your company's cloud administrator to get your Azure credentials and then sign in to your account with the [Azure Portal](#).

Create an Office 365 E5 trial tenant

Note

If you already have an existing Office 365 or Microsoft Entra subscription, you can skip the Office 365 E5 trial tenant creation steps.

1. Go to the [Office 365 E5 product portal](#) and select **Free trial**.



Office 365 E5

\$35.00 user/month
(annual commitment)

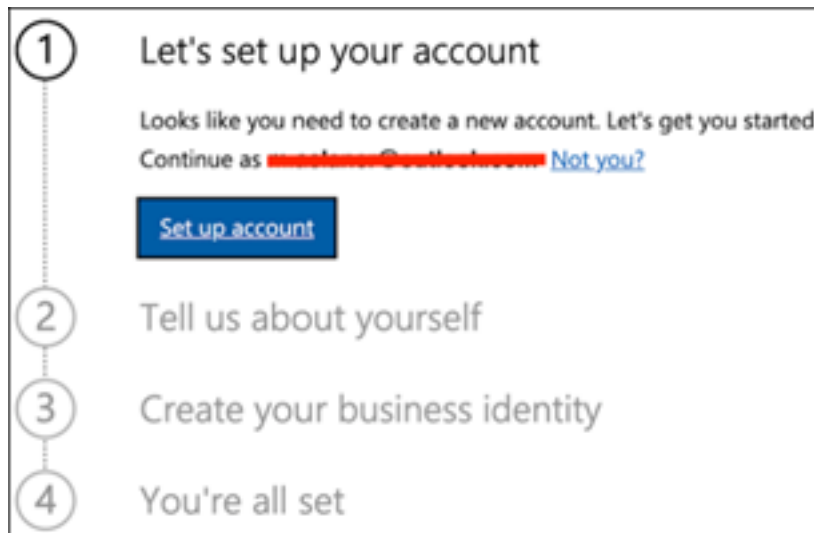
[Contact sales](#)

- Includes full desktop versions of Office apps
- Get advanced security, analytics, and voice capabilities
- Guard your mailbox with Exchange Online Advanced Threat Protection
- Make, receive, and transfer calls with Phone System
- Guaranteed 99.9% uptime, and 24/7 support from Microsoft

[Free trial >](#)

[Buy now >](#)

2. Complete the trial registration by entering your email address (personal or corporate). Click **Set up account**.



1 Let's set up your account

Looks like you need to create a new account. Let's get you started!
Continue as [\[Redacted\]](#) [Not you?](#)

[Set up account](#)

2 Tell us about yourself

3 Create your business identity

4 You're all set

3. Fill in your first name, last name, business phone number, company name, company size, and country or region.

1 Signup started

2 Tell us about yourself

3 Create your business identity

4 You're all set

First name
John

Last name
Doe

Business phone number
0000000000000000

Company name
Contoso

Company size
1000+ people

Country or region
Netherlands

Next

Note

The country or region you set here determines the data center region your Office 365 will be hosted.

4. Choose your verification preference: through a text message or call. Click **Send Verification Code**.

1 Signup started

2 Tell us about yourself

3 Create your business identity

4 You're all set

✓ ●

Prove. You're. Not. A. Robot.

Enter a number that isn't VoIP or toll free.

Text me Call me

Code (+31) Phone number

We don't save this phone number or use it for any other purpose.

[Send Verification Code](#)

[< Go back](#)

5. Set the custom domain name for your tenant, then click **Next**.

The screenshot displays a four-step wizard for creating a business identity. Step 1 is 'Signup started', step 2 is 'Nice to meet you, Milad', and step 4 is 'You're all set'. Step 3, 'Create your business identity', is the active step, indicated by a blue dot and a circled '3'. The content of step 3 includes a text prompt: 'To set up your account, you'll need a domain name. [What is a domain?](#)'. Below this is a sub-prompt: 'You'll probably want a custom domain name for your business at some point. For now, choose a name for your domain using **onmicrosoft.com**'. A text input field contains 'yourbusiness' on the top line and 'mtpdemo' on the bottom line, with '.onmicrosoft.com' to its right. A green message states 'mtpdemo.onmicrosoft.com is available.' At the bottom of the form are two buttons: 'Check availability' (disabled) and 'Next' (active).

1 Signup started

2 Nice to meet you, Milad

3 Create your business identity

To set up your account, you'll need a domain name. [What is a domain?](#)

You'll probably want a custom domain name for your business at some point. For now, choose a name for your domain using **onmicrosoft.com**

yourbusiness
mtpdemo .onmicrosoft.com

mtpdemo.onmicrosoft.com is available.

Check availability Next

4 You're all set

6. Set up the first identity, which will be a Global Administrator for the tenant. Fill in **Name** and **Password**. Click **Sign up**.

1 Signup started

2 Nice to meet you, Milad

3 Create your business identity

✓ ●

Now create your user ID and password to sign in to your account.

Name @mtpdemo.onmicrosoft.com

Password

Confirm password

By clicking **Sign up**, I agree to the [privacy statement](#) and the [trial agreement](#).

Microsoft will be contacting you with surveys, promotions, tips and advice for using our products and services. You can unsubscribe at any time.
Microsoft Online Services may contact me with information about their products, services and events:

Email

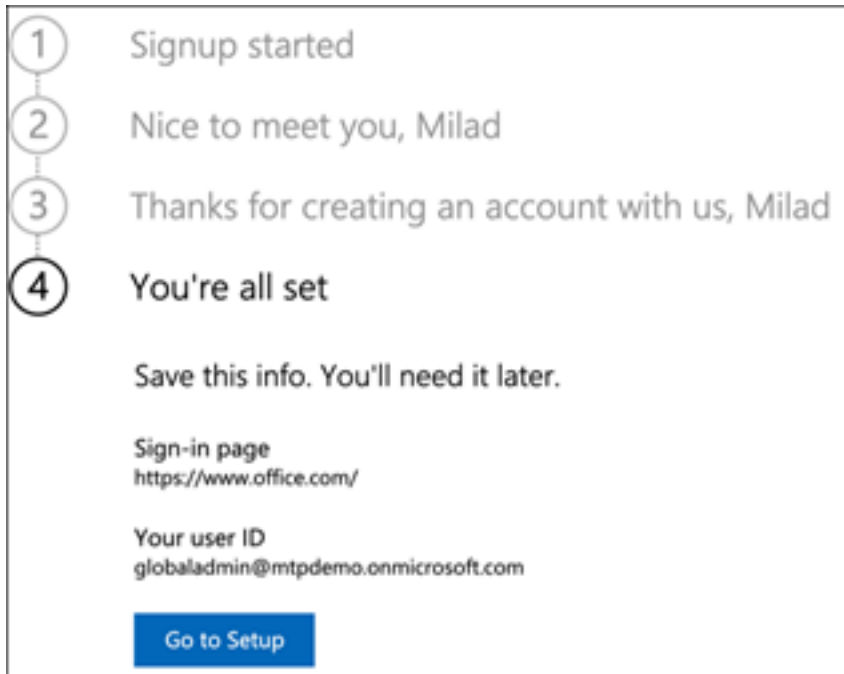
Phone

Microsoft Partners may contact me with information about their products, services, and events

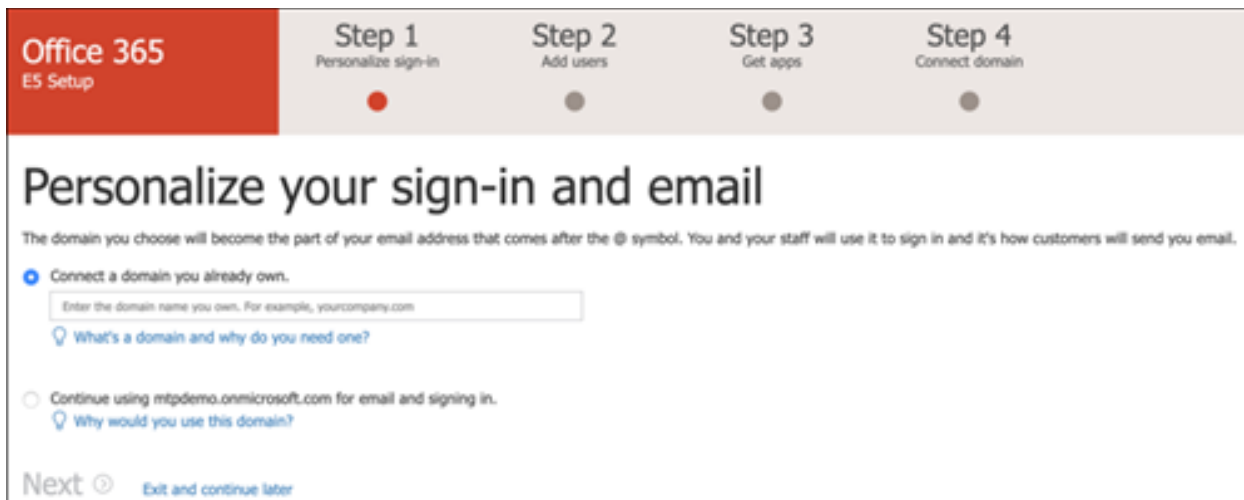
[< Go back](#)

4 You're all set

7. Click **Go to Setup** to complete the Office 365 E5 trial tenant provisioning.



8. Connect your corporate domain to the Office 365 tenant. [Optional]
Choose **Connect a domain you already own** and type in your domain name.
Click **Next**.



9. Add a TXT or MX record to validate the domain ownership. Once you've added the TXT or MX record to your domain, select **Verify**.

Verify domain

To verify that you own this domain, add this DNS record to your domain (only the domain owner can do this). Don't worry, adding this record won't affect your existing email or other services and it can safely be removed at the end of setup.

Follow these [step-by-step instructions](#) -> to create a new DNS record using the values below at Azure ->. (Not your DNS host? [↗](#))

TXT name:  @ or skip if not supported by provider.

TXT value:  

TTL:  3600 or your provider default.

[Get someone to help you.](#) Let us help you set up your TXT records.

Or, add an MX record to verify ownership instead.

[Back](#) **Verify**  [Exit and continue later](#)

10. [Optional] Create more user accounts for your tenant. You can skip this step by clicking **Next**.

Add new users

We'll assign a Office 365 E5 license to each user you add here. When you're done, we'll give you the sign-in information to share with the users.

 What happens if you don't do this now?

You have **24 of 25 license(s) available**. [View all users](#).

First name	Last name	User name
<input type="text"/>	<input type="text"/>	<input type="text"/> @ mtpdemo.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @ mtpdemo.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @ mtpdemo.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @ mtpdemo.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @ mtpdemo.com

24 license(s) available

[+ Add another user](#)

Send password for new users to my email

You can add more users anytime in the Office 365 admin center.

[Back](#) **Next**  [Exit and continue later](#)

11. [Optional] Download Office apps. Click **Next** to skip this step.

Install your Office apps

Install Office apps for yourself so you can take full advantage of your subscription. Selecting Install now will assign a subscription to you, if you don't have one already.

 **Microsoft Office Professional Plus**

Install the following apps on your computer: Word, Excel, PowerPoint and Outlook.



[Install now](#) 

 **Skype for Business**

Get instant messaging, audio and video calls, online meetings and presentations, availability information, and sharing.

[Install now](#) 

Want to install the apps later? Assign a license to yourself and go to the Office software card on the Admin center home page to find your download links.

[Back](#) **Next**  [Exit and continue later](#)


12. [Optional] Migrate email messages. Again, you can skip this step.

Migrate email messages

If you want to keep your email messages from your current email service, we'll help you move them.

Don't migrate email messages
Select this option if you have no email, you don't want to migrate email, or you'd rather migrate email later.
[What will happen if you don't migrate now?](#)

Migrate email messages
Select this option if you want to copy existing email messages to your new mailboxes. This option will take you out of setup. To resume setup, go to the Admin center home page.
[What's involved in migrating email?](#)

[Back](#) **Next**  [Exit and continue later](#)

13. Choose online services. Select **Exchange** and click **Next**.

Choose your online services

Select the services you want to start using now. For an online service to work correctly, you have to add some DNS records for each service you select. You usually manage DNS records through the same provider of your domain name, and we'll help out with step-by-step instructions. If you skip setup for a service now, just return here later when you're ready to set it up.

 [Why would I skip setting up a service?](#)

Exchange

Email, contacts, and scheduling are all provided by Exchange. Set up this service to enable all the functionality of Outlook and other email clients.

 [How many DNS records do I have to setup?](#)

Skype for Business

Online communication services like chat, conference calls, and video calls are provided by Skype for Business.

 [How many DNS records do I have to setup?](#)

Mobile Device Management for Office 365

This service helps you secure and remotely manage mobile devices that connect to your domain.

 [How many DNS records do I have to setup?](#)

[Back](#)

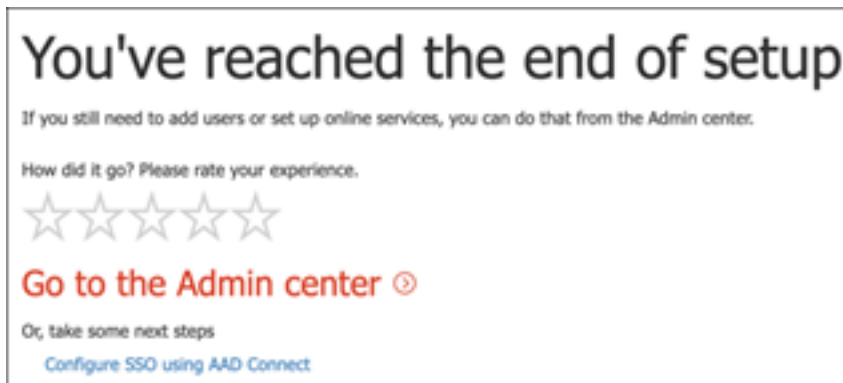
Next 

[Exit and continue later](#)

14. Add MX, CNAME, and TXT records to your domain. When completed, select **Verify**.



15. Congratulations, you have completed the provisioning of your Office 365 tenant.

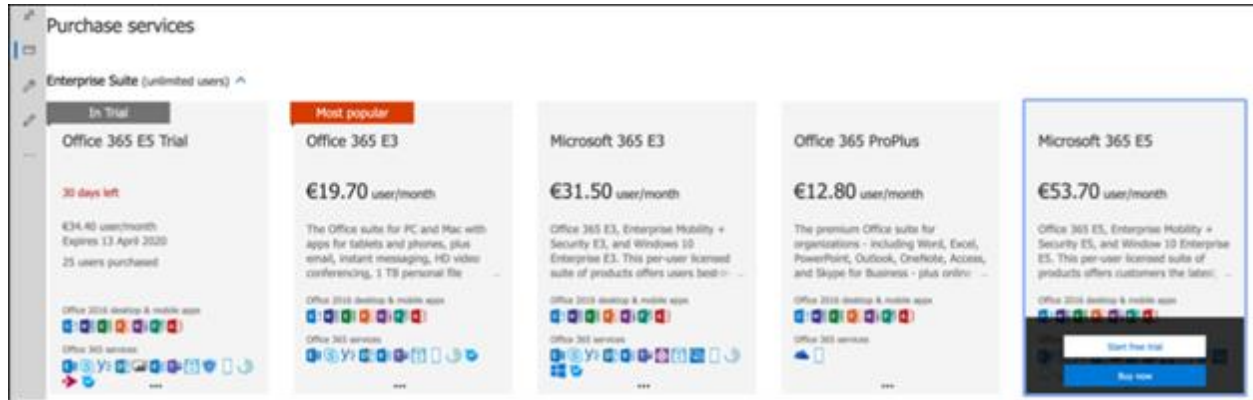


Enable Microsoft 365 trial subscription

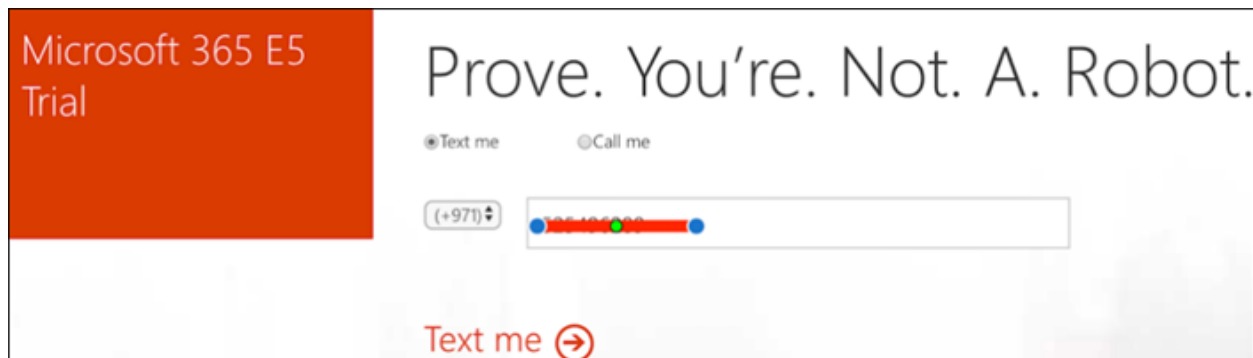
Note

Signing up for a trial gives you 25 user licenses to use for a month. See [Try or buy a Microsoft 365 subscription](#) for details.

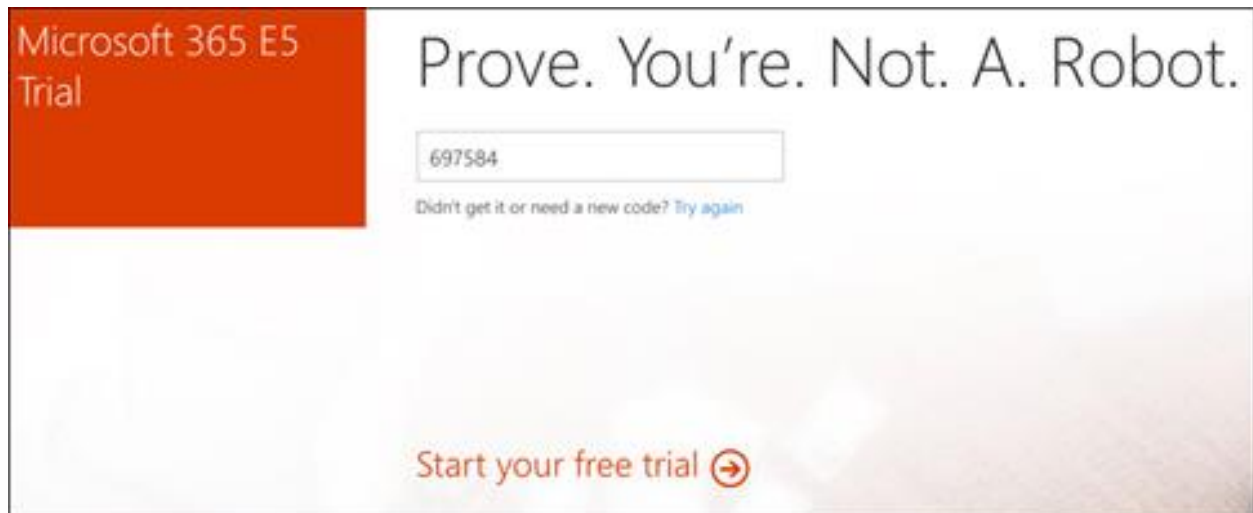
1. From [Microsoft 365 Admin Center](#), click **Billing** and then navigate to **Purchase services**.
2. Select **Microsoft 365 E5** and click **Start free trial**.



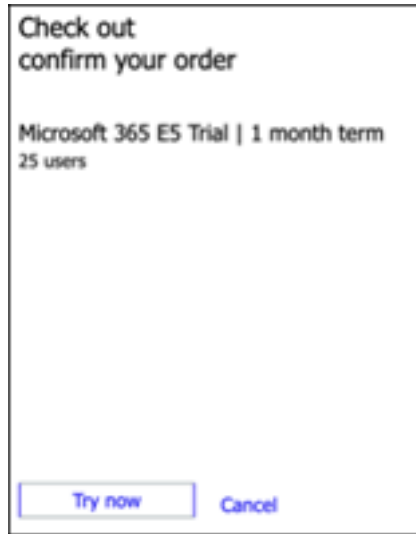
3. Choose your verification preference: through a text message or call. Once you have decided, enter the phone number, select **Text me** or **Call me** depending on your selection.



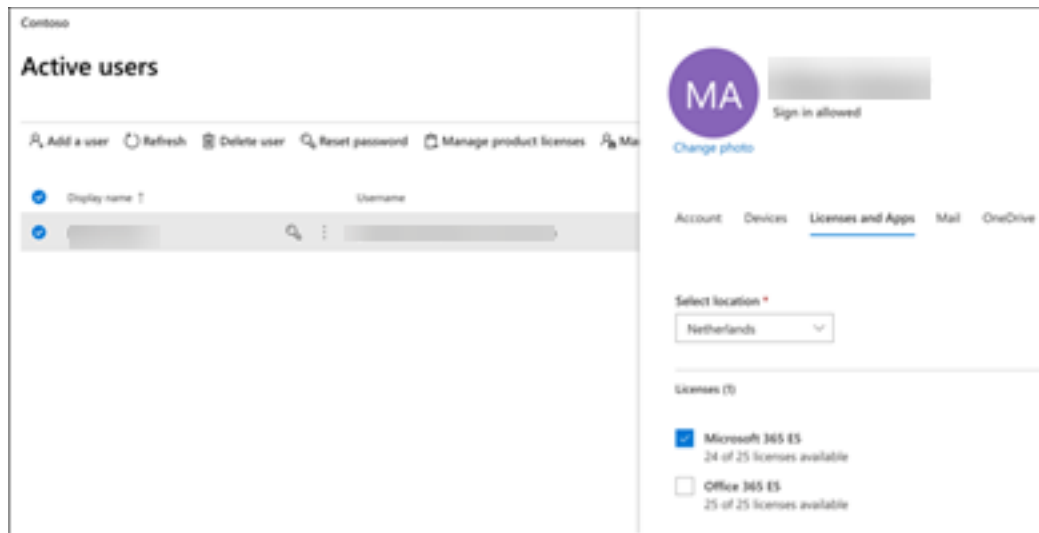
4. Enter the verification code and click **Start your free trial**.



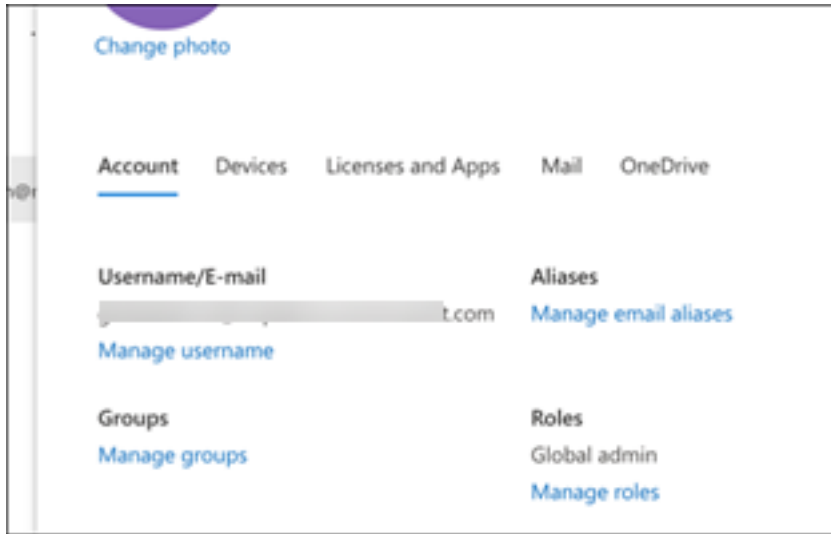
5. Click **Try now** to confirm your Microsoft 365 E5 trial.



6. Go to the **Microsoft 365 Admin Center** > **Users** > **Active users**. Select your user account, select **Manage product licenses**, then swap the license from Office 365 E5 to **Microsoft 365 E5**. Click **Save**.



7. Select the global administrator account again then click **Manage username**.



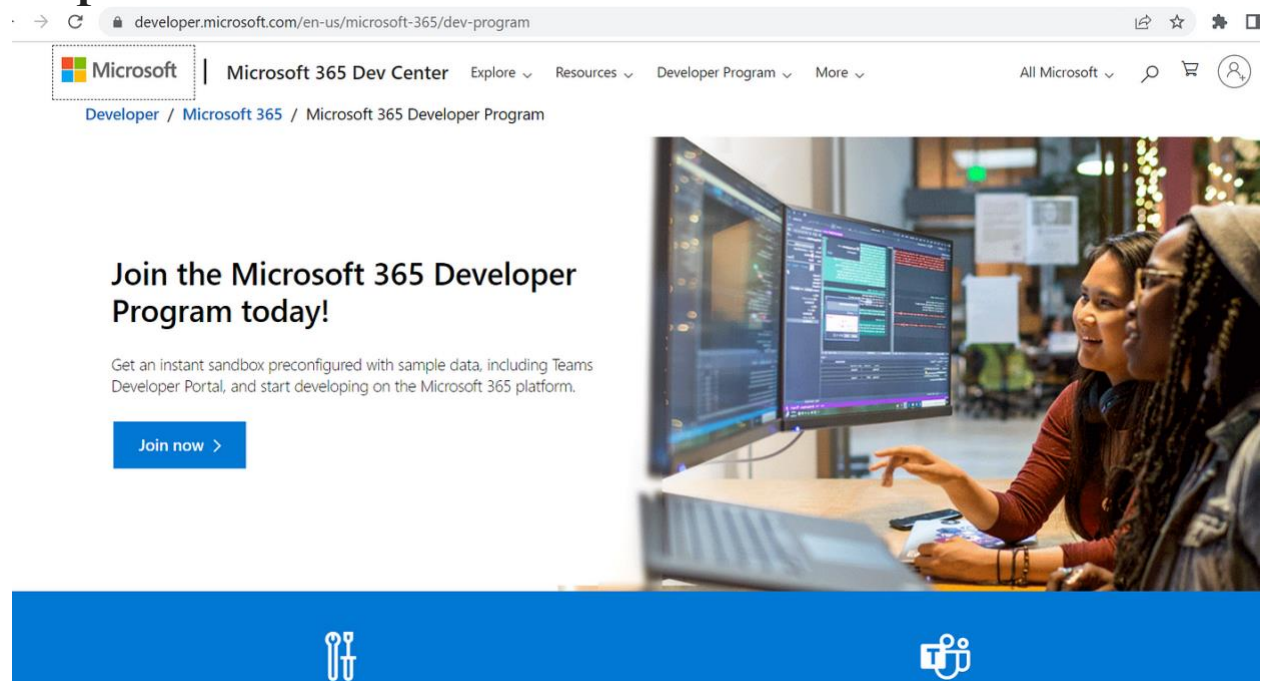
8. [Optional] Change the domain from *onmicrosoft.com* to your own domain—depending on what you chose on the previous steps. Click **Save changes**.

A screenshot of the "Manage username" form. At the top, there is a warning message: "You are about to change this user's sign-in information. Let them know about this change." Below the message is a text input field containing "globaladmin" and a dropdown menu for the domain. The dropdown menu is open, showing three options: "mtpdemo.onmicrosoft.com" (selected), "mtpdemo.com", and "mtpdemo.onmicrosoft.com".

How to Create Microsoft 365 Developer Account

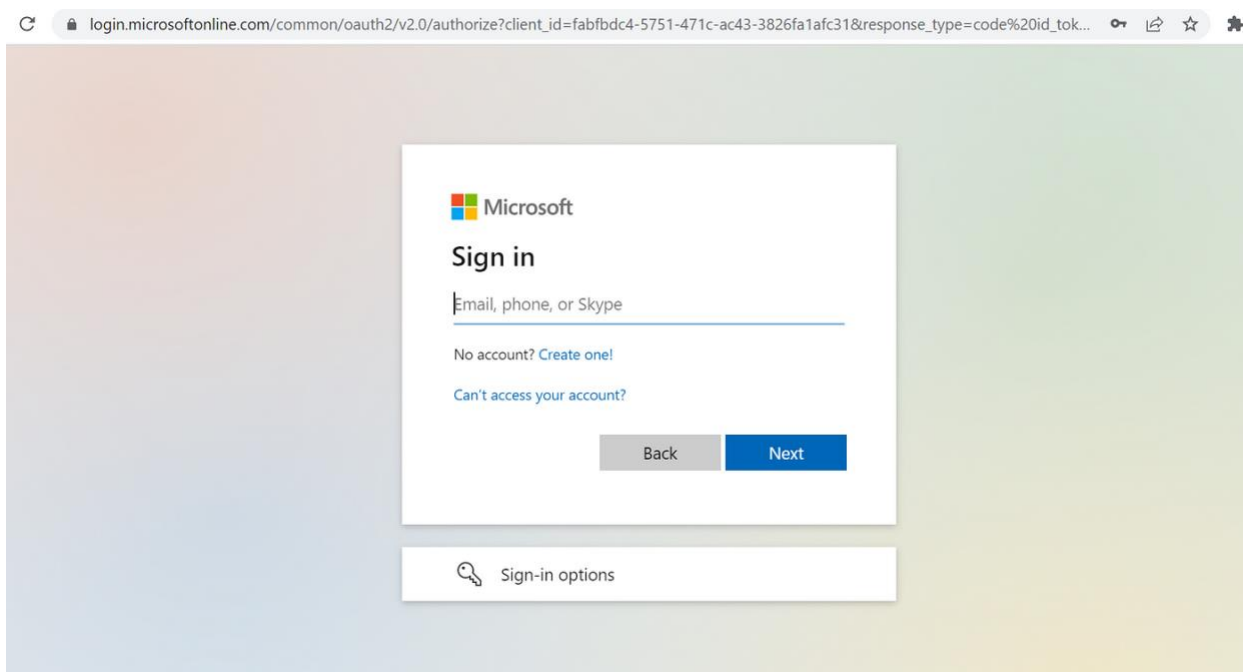
This guide shows you the step by step process of how to create a Microsoft 365 developer account and also how to resolve any issue during the process.

Step 1:



Go to <https://aka.ms/m365DevAccount>

Click on join now



If you have an outlook account sign in the account and skip to **Step 2**.
If you don't have an Outlook account. Click on Create one!

How to Create an Account

If you have an outlook account sign in and skip this process to Step 2



Create account

|someone@example.com

[Use a phone number instead](#)

[Get a new email address](#)

Next



Create account

Rachellove678 | @outlook.com

[Use a phone number instead](#)

[Use your email instead](#)

Next

Click on Next



← Rachellove678@outlook.com

Create a password

Enter the password you would like to use with your account.

|.....

Show password

I would like information, tips, and offers about Microsoft products and services.

Choosing **Next** means that you agree to the [Microsoft Services Agreement](#) and [privacy and cookies statement](#).

Next

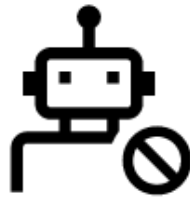
Add a password



← Rachellove678@outlook.com

Create account

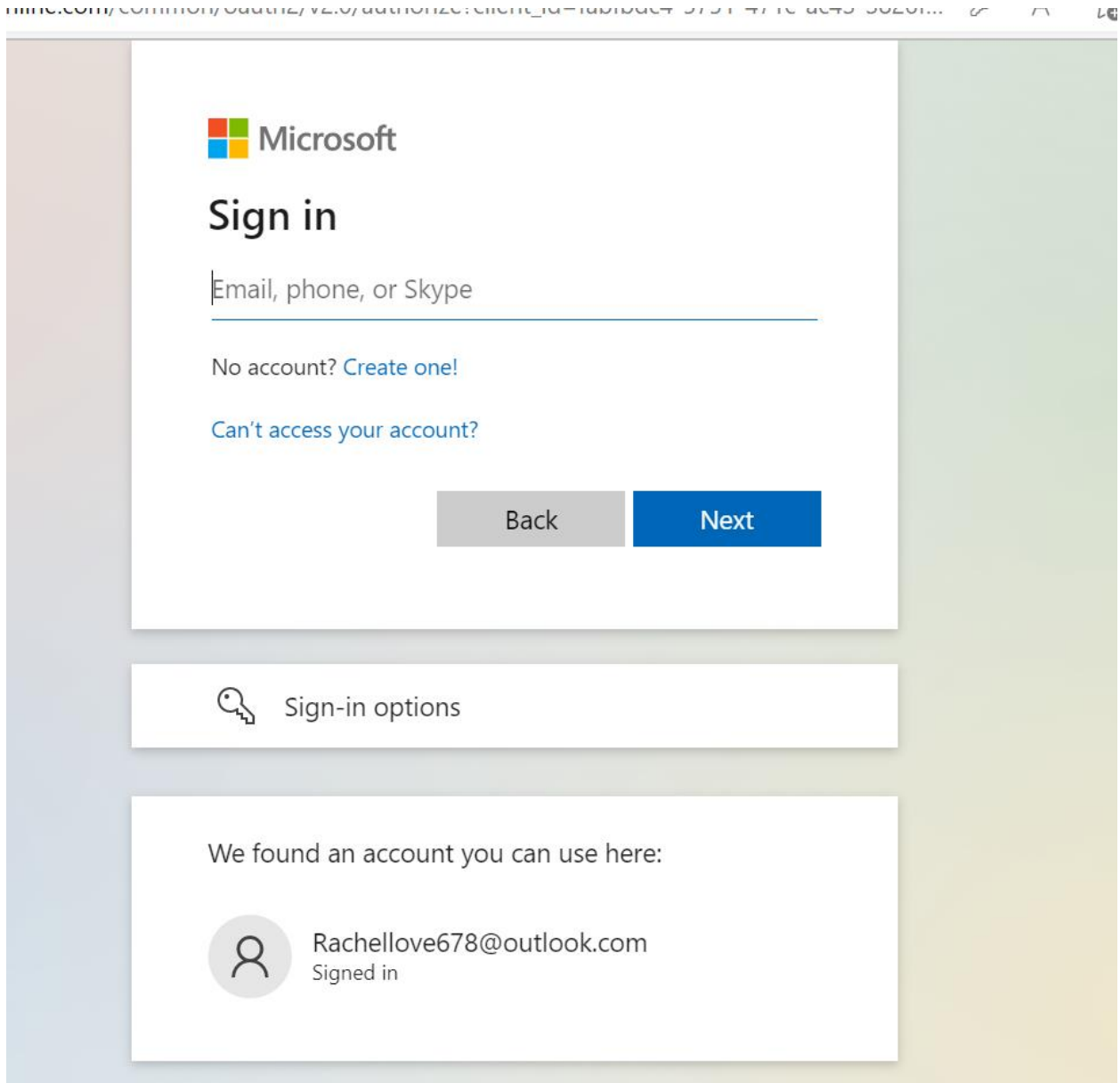
Please solve the puzzle so we know you're not a robot.



Next



Solve the puzzle

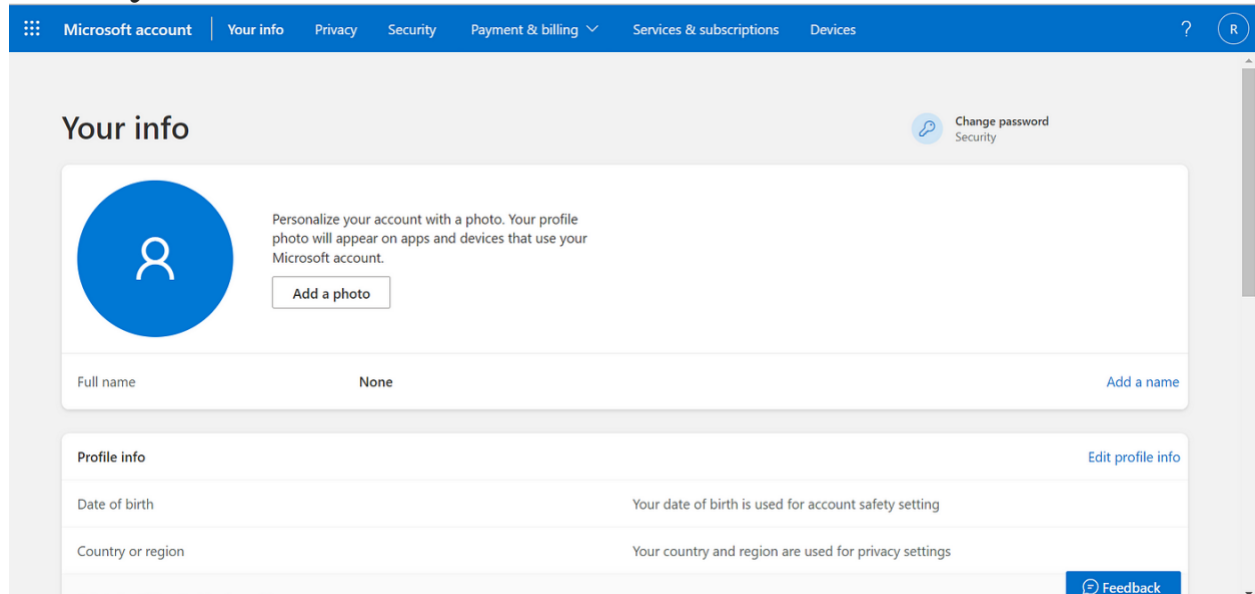


Sign in your account

Congrats 🎉

Step 2:

Build your Profile

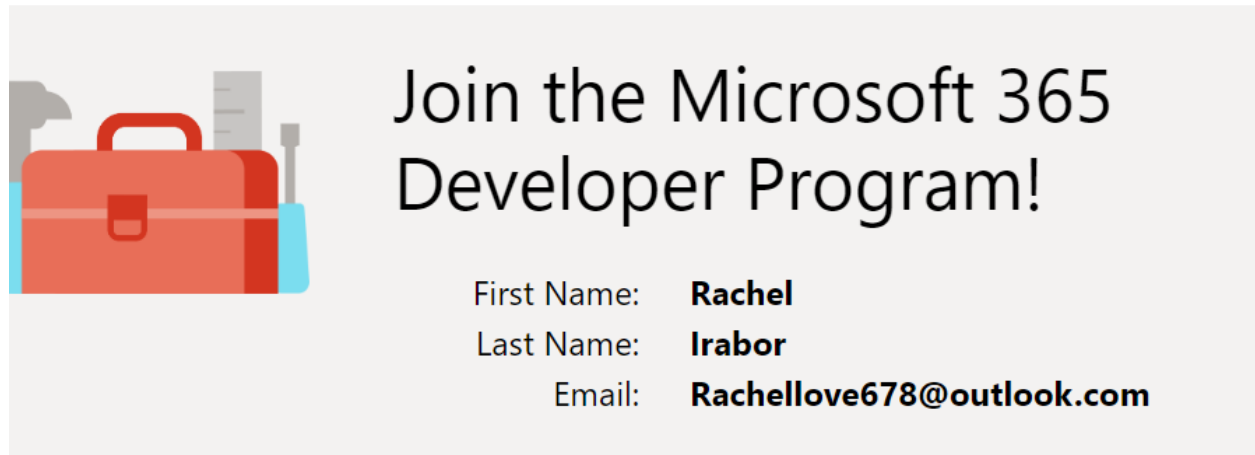


The screenshot shows the Microsoft account profile page. At the top, there is a blue navigation bar with the following links: Microsoft account, Your info, Privacy, Security, Payment & billing, Services & subscriptions, and Devices. On the right side of the navigation bar, there is a question mark icon and a circular profile icon with the letter 'R'. Below the navigation bar, the page title is "Your info". To the right of the title, there is a "Change password" link with a key icon and the word "Security" below it. The main content area is divided into several sections. The first section is a large white box with a blue circular profile picture placeholder containing a white person icon. To the right of the placeholder, there is text: "Personalize your account with a photo. Your profile photo will appear on apps and devices that use your Microsoft account." Below this text is a button labeled "Add a photo". Below the photo section, there is a "Full name" field with the value "None" and a link "Add a name". The next section is "Profile info" with a link "Edit profile info". It contains two rows: "Date of birth" with the note "Your date of birth is used for account safety setting" and "Country or region" with the note "Your country and region are used for privacy settings". At the bottom right of the page, there is a blue "Feedback" button.

Go to <https://account.microsoft.com/profile>

To build your profile

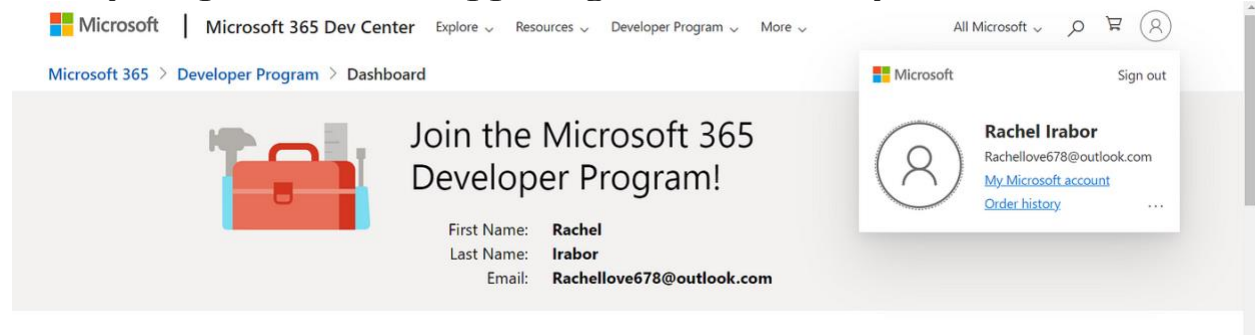
The main reason for this is to avoid FNU and LNU as your First and Last Name in your Microsoft 365 Developer Account



The graphic features a red toolbox with a blue handle and a blue bag on the left side. To the right of the toolbox, the text reads: "Join the Microsoft 365 Developer Program!". Below this, the following information is listed: "First Name: Rachel", "Last Name: Irabor", and "Email: Rachellove678@outlook.com".

If you are having issue with what your name is showing on aka.ms/M365DevAccount

Click your profile on the upper right hand side of your Screen.



The screenshot shows the Microsoft 365 Dev Center dashboard. At the top, there is a navigation bar with the Microsoft logo, "Microsoft 365 Dev Center", and links for "Explore", "Resources", "Developer Program", and "More". On the right, there are links for "All Microsoft", a search icon, a shopping cart icon, and a user profile icon. Below the navigation bar, the breadcrumb trail reads "Microsoft 365 > Developer Program > Dashboard". The main content area features a red toolbox icon and the heading "Join the Microsoft 365 Developer Program!". Below this, the user's details are listed: "First Name: Rachel", "Last Name: Irabor", and "Email: Rachellove678@outlook.com". A user profile dropdown menu is open on the right, showing the user's name "Rachel Irabor", email "Rachellove678@outlook.com", and links for "My Microsoft account" and "Order history".

Create a Microsoft 365 Dev Account



The screenshot shows the Microsoft 365 Dev Center dashboard. It features a red toolbox icon and the heading "Join the Microsoft 365 Developer Program!". Below this, the user's details are listed: "First Name: Rachel", "Last Name: Irabor", and "Email: Rachellove678@outlook.com".



Please answer a few questions to help us customize your Developer Program experience.

Country/Region *

Nigeria

Company *

Sweet Addiction

Language preference *

English

I accept the [terms and conditions](#) of the Microsoft 365 Developer

Fill in your details

You can use any name for your Company



What is your primary focus as a developer? * (Choose only one)

- Applications to be sold in market
- Custom solutions for my own customers
- Applications for internal use at my company
- Personal projects

[Next](#) [Back](#)

Click on **Next**



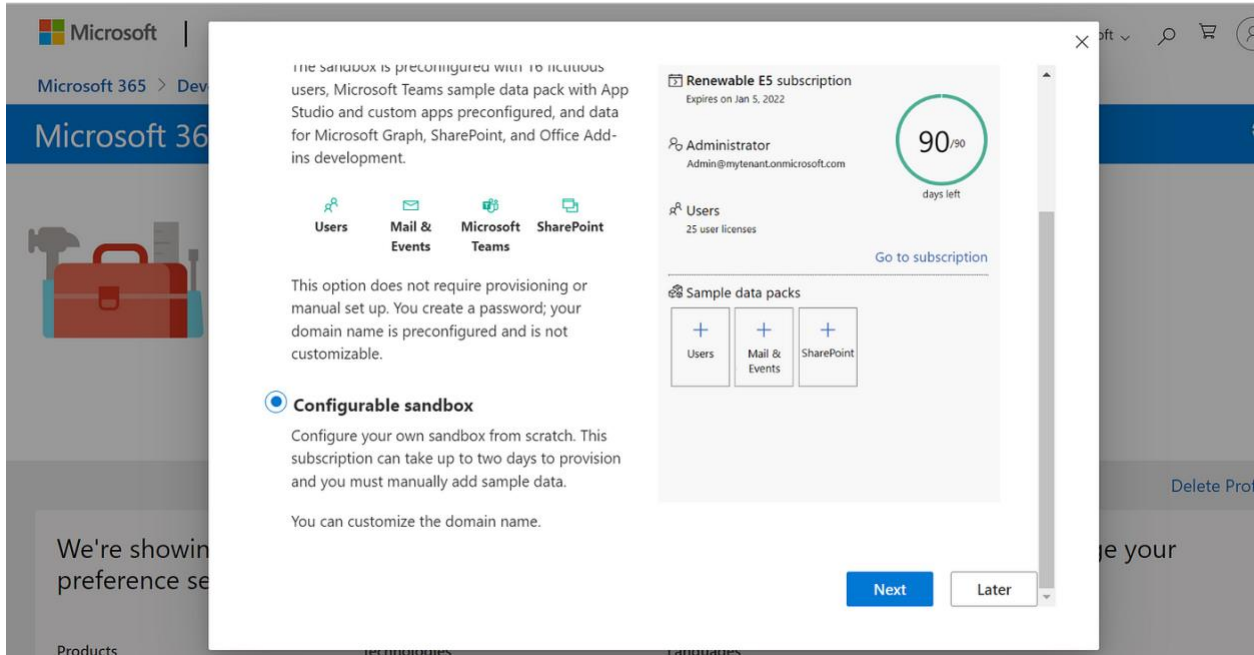
What areas of Microsoft 365 development are you interested in? We will show you resources, tools, and training to help you get started.

- SharePoint Framework (SPFx)
- Microsoft Graph
- Microsoft Teams
- Office Add-ins
- Outlook
- Microsoft identity platform
- Power Platform

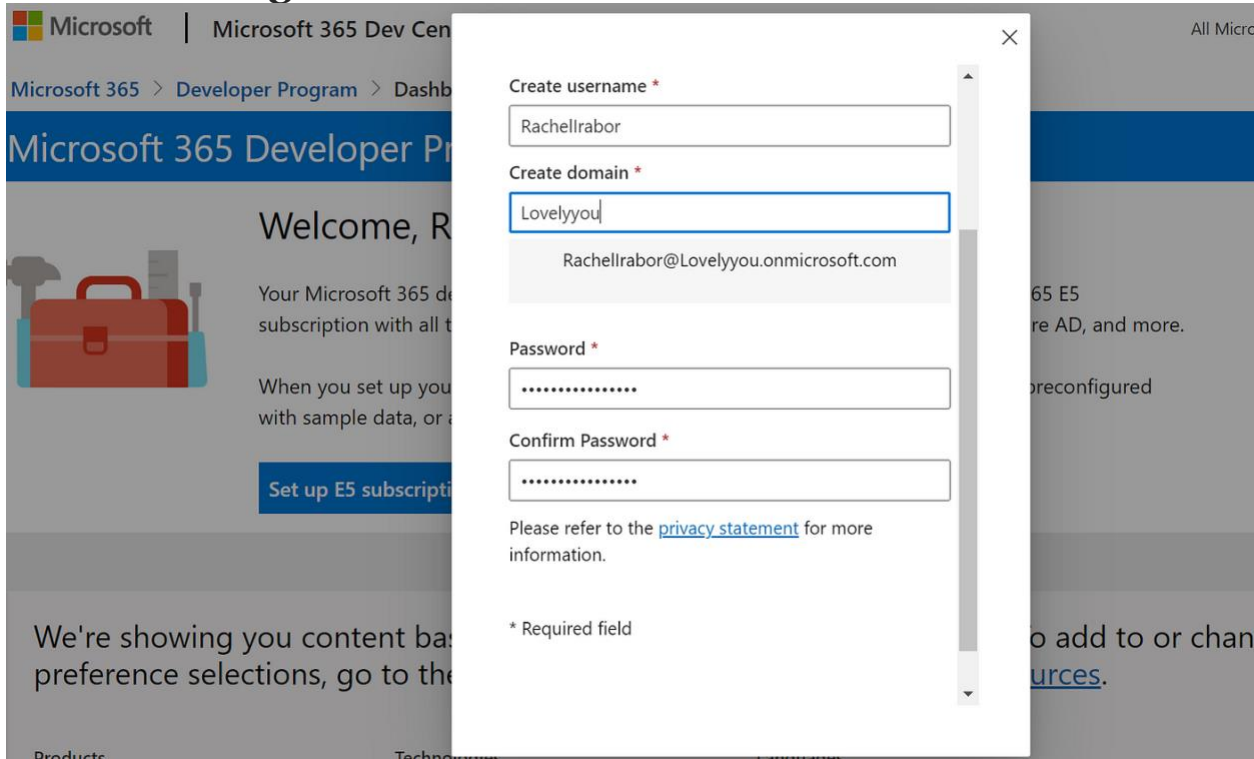
[Save](#) [Back](#)

Select everything on your Screen

Click on **Save**



Click on **Configurable sandbox**

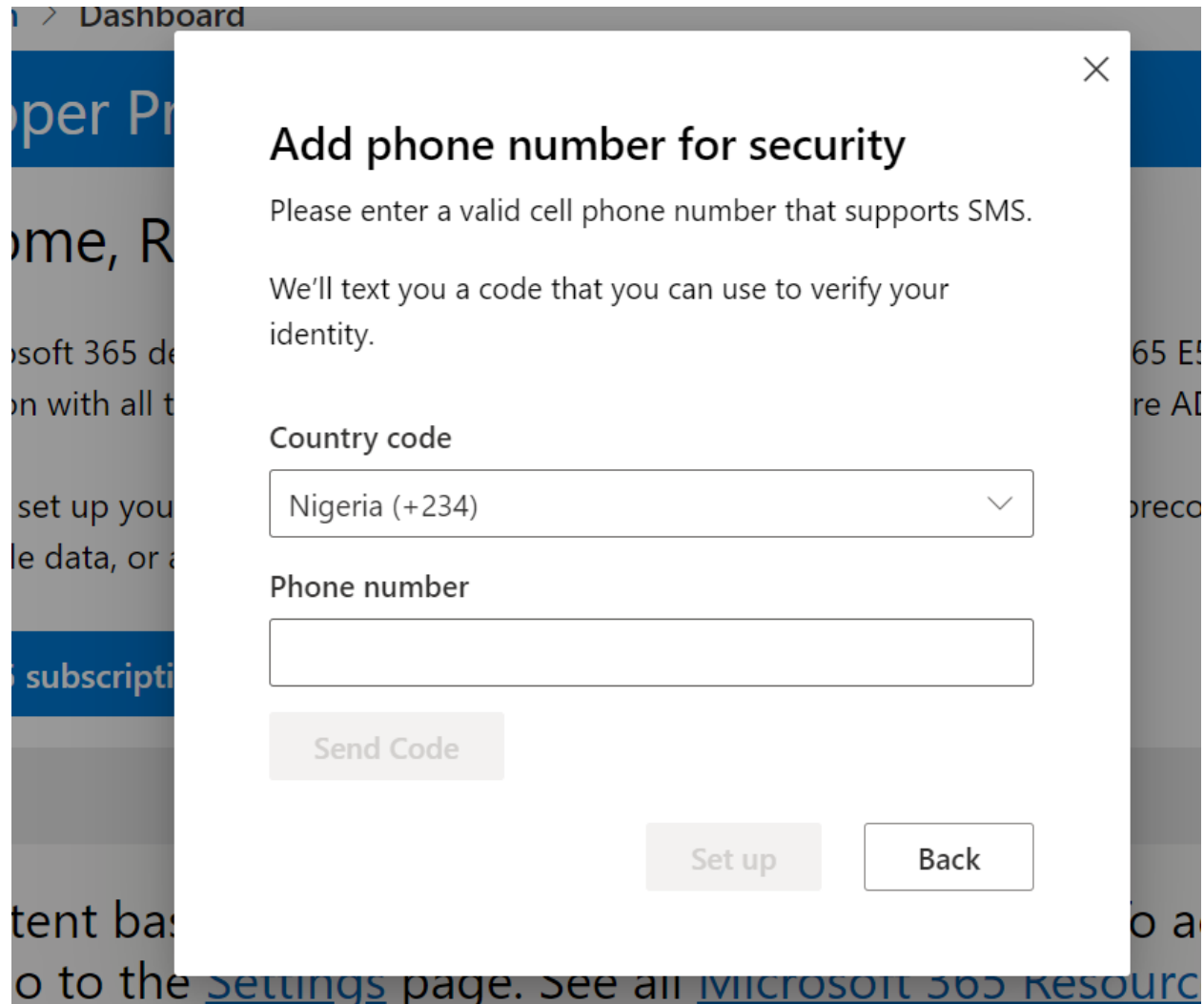


Here you have to use a domain name that is available

Create your Username, Domain

Password and confirm password.

Click on **Continue**



The screenshot shows a dialog box with a close button (X) in the top right corner. The title is "Add phone number for security". Below the title, there is a message: "Please enter a valid cell phone number that supports SMS. We'll text you a code that you can use to verify your identity." There are two input fields: "Country code" with a dropdown menu showing "Nigeria (+234)" and a "Phone number" field. Below the "Country code" field is a "Send Code" button. At the bottom of the dialog are "Set up" and "Back" buttons.

Add your **Phone number** and **Country code**

Click on **Send code**

Enter the Code then click on **Set up**

[Microsoft 365](#) > [Developer Program](#) > [Dashboard](#)

Microsoft 365 Developer Program

Your Microsoft 365 developer subscriptions

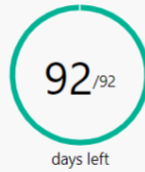
To learn more about how to work with your subscription, see [Build Microsoft 365 solutions](#).

🌐 Domain name
lovelyou.onmicrosoft.com

📅 **Renewable E5** subscription
Expires on Aug 21, 2022

👤 Administrator
Rachellrabor@lovelyou.onmicrosoft.com

👥 Users
25 user licenses



[Go to subscription](#)

Pre-Lab Setup of the Microsoft 365 Tenant

Enable Microsoft 365 audit log

In this setup task, you'll enable the Audit log capability in Microsoft 365. Although documentation indicates that audit log is turned on by default, most lab tenants don't have this feature enabled, and it can take several hours for this to take effect. It's beneficial to enable this feature, as Microsoft 365 uses audit logs for user insights and activities identified in policies and analytics insights.

1. Open Microsoft Edge. In the address bar, enter <https://admin.microsoft.com>.
2. Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).
3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.
4. Under Admin centers, select **Compliance**. A new browser page opens to the welcome page of the Microsoft Purview compliance portal.
5. From the left navigation panel of the Microsoft Purview compliance portal, select **Show all**.
6. In the left navigation panel, under solutions, select **Audit**. Note: the audit functionality is also accessible through the Microsoft 365 Defender home page.
7. Verify that the **Search** tab is selected (underlined).
8. Once you land on the Audit page, wait 2-3 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start recording user and admin activity. Select **Start recording user and admin activity**. Once auditing is enabled, the blue bar disappears. If the blue bar is not present, then auditing is already enabled, and no further action is required.
9. Return to the home page of the Microsoft Purview compliance portal by selecting **Home** from the left navigation panel.

Microsoft Defender for Cloud Apps file monitoring

In this setup task, you will enable file monitoring in Microsoft Defender for Cloud Apps.

1. Open the browser tab for the Microsoft 365 admin center. If you previously closed it, open a new browser tab and in the address bar, enter <https://admin.microsoft.com> and from the left navigation pane of the Microsoft 365 admin center, select **Show all**.
2. Under Admin centers, select **Security**. A new browser page opens to the welcome page of the Microsoft 365 Defender portal.
3. From the left navigation panel, select **Files**, which is listed under Cloud apps.
4. If not already enabled, you'll need to select **Enable file monitoring** and select the box next to where it says **Enable file monitoring** then select **Save**.
5. From the left navigation panel, under cloud apps, select **Files** to return to the files page. If you successfully enabled file monitoring, you should see the filter options on the top of the page. It may take some time for files from the pre-configured lab tenant to be displayed.

Pre-Lab setup of the Azure Cloud Slice Subscription

For this setup you are using the Azure Cloud Slice environment which is separate than the Microsoft 365 tenant provided. Logout of the Microsoft 365 Tenant and login using the Azure Cloud Slice credentials.

Azure virtual machine

Check that a VM has already been created. If not, then set it up now. You will use the VM as part of the NSG demo.

1. Open Microsoft Edge. In the address bar, enter <https://portal.azure.com> and sign in with the Azure credentials provided by the authorized lab hoster (ALH). This bring you to the Azure services home page.
2. In the blue search box at the top of the page, enter **Virtual Machines** then select **Virtual Machines** from the search results.
3. If a VM is already listed then skip the steps that follow, otherwise you'll need to create one. Select **Create**, then from the drop-down menu, select **Azure Virtual machine**. Configure the following parameters (if a parameter is not listed, leave the default value).
 - i. Resource group: Select **Create new** and enter **LabsSC900**, then select **OK**.

- ii. Virtual machine name: enter **SC900-WinVM**.
 - iii. Availability options: From the drop down, select **No infrastructure redundancy required**.
 - iv. Image: From the drop down select **Windows 11 Pro, version 22H2 - x64 Gen2** (or any Windows 10 or Window 11 image listed).
 - v. Size: select **See all sizes** and select **Standard_B1s** then select **Select** at the bottom of the page.
 - vi. Username: enter **SC900-VM-User**
 - vii. Password: enter a password and write it down, you will need it later!!!!
 - viii. Confirm password: re-enter the password.
 - ix. Public inbound ports: **None**.
 - x. Licensing: select where it says, "I confirm I have an eligible Windows 10/11 license with multi-tenant hosting rights." A checkmark should appear.
 - xi. Select **Next: Disks**
 - xii. OS disk type: from the drop-down, select **Standard SSD**.
 - xiii. Select **Next: Networking**
 - xiv. NIC network security group: select **None**. You will create an NSG as part of the demo, so don't do it here!
 - xv. Delete public IP and NIC when VM is deleted: select the box so a checkmark appears.
 - xvi. Select **Review + create**, then when validation passes, select **Create**.
 - xvii. Once the VM deployment is complete, select **Home** from the top of the page.
4. Keep the Azure browser tab open to continue with the pre-demo setup.

Network security group

Check that an NSG has already been created. If the NSG has not been created set it up now, but do not associate any interface to it nor create any rules. Those steps will be done as part of the NSG demo.

1. In the blue search bar on the top of the page, enter **Network security groups** groups. From the results, select **Network security groups** (do not select Network security groups classic).
2. Select **Create network security group**. On the Basics tab of the Create network security group page, specify the following settings:

- i. Subscription: Leave the default value (this is the Azure subscription provided by the authorized lab hoster)
- ii. Resource group: **LabsSC900**
- iii. Name: **NSG-SC900**
- iv. Region: leave the default.
- v. Select **Review + create** then select **Create**.
- vi. Once the deployment is complete (this happens very quickly), select **Go to resource**.

Microsoft Defender for Cloud

The objective here is simply to access Microsoft Defender to Cloud for the first time. This is important because it can take up to 24 hours for Defender for Cloud to reflect an initial secure score.

1. Open the Home-Microsoft Azure tab in your browser.
2. In the blue search bar enter **Microsoft Defender for Cloud**, then from the results list, select **Microsoft Defender for Cloud**.
3. If this is the first time you enter Microsoft Defender for Cloud with your subscription, you may land on the Getting started page, and may be prompted to upgrade. Scroll to the bottom of the page and select **Skip**. You'll be taken to the Overview page.
4. All subscriptions have foundational CSPM enabled by default, which provides a secure score, but it can take up to 24 hours for Defender for Cloud to reflect an initial secure score.
5. Select **Home** from the top of the page.
6. Keep the browser tab open to continue with the pre-demo setup.

Microsoft Sentinel

Check to that an instance of Microsoft Sentinel has already been created. If not, then set it up now as you will need it as part of the walk-through demo on Microsoft Sentinel.

1. Open the Home-Microsoft Azure tab in your browser.

2. In the search box, in the blue bar on the top of the page next to where it says Microsoft Azure, enter **Microsoft Sentinel** then select **Microsoft Sentinel** from the search results.
3. From the Microsoft Sentinel page, select **Create Microsoft Sentinel**.
4. From the Add Microsoft Sentinel to a workspace page, select **Create a new workspace**.
5. From the basics tab of the Create Log Analytics workspace, enter the following:
 - i. Subscription: Leave the default.
 - ii. Resource group: select **Create New**, then enter the name **SC900-Sentinel-RG** then select **OK**.
 - iii. Name: **SC900-LogAnalytics-workspace**.
 - iv. Region: **East US** (A different default region may be selected based on your location).
 - v. Select **Review + Create** (no tags will be configured).
 - vi. Verify the information you entered then select **Create**.
 - vii. It may take a minute or two for the new workspace to be listed, if you still don't see it, select **Refresh**, then select **Add**.
6. Once the new workspace is added, the Microsoft Sentinel | News & guides page will display, indicating that the Microsoft Sentinel free trial is activated. Select **OK**.

Review

In this setup, you enabled the audit log capability in your Microsoft 365 tenant and you also created verified that a VM was preconfigured in your Azure Cloud Slice environment. You also prepared your Defender for Cloud and Microsoft Sentinel environment.

Lab: Explore Microsoft Entra ID

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft Entra.
- Module: Describe the function and identity types of Microsoft Entra ID.
- Unit: Describe the types of identities.

Lab scenario

In this lab, you'll access Microsoft Entra ID (previously referred to as Azure Active Directory). Additionally, you'll create a user and configure the different settings, including adding licenses.

Estimated Time: 10-15 minutes

Task 1

As a subscriber to Microsoft 365 you're already using Microsoft Entra ID (previously referred to as Azure AD). In this task, you'll learn how to create a new user in Microsoft Entra ID and explore some of services that can be managed at the user level.

1. Open the Microsoft Edge browser. In the address bar, enter admin.microsoft.com and sign in with the Microsoft 365 credentials provided by your authorized lab hoster (ALH).
 - i. In the Sign-in window, enter admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your ALH) then select **Next**.
 - ii. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.
 - iii. When prompted to stay signed- in, select **Yes**.
2. Under Admin centers, select **Identity** (you may need to select **Show all** and scroll down). A new browser page opens to the overview page of the Microsoft Entra admin center. Here you will see basic information about your Contoso tenant. If you scroll down the main window you will also see information about alerts, my feed, feature highlights, and more.

3. From the left navigation pane, expand **Users** then select **All users**. Notice that your tenant is already configured with users.
4. From the top of the page, select **+ New user** then from the drop-down box, select **Create new user**.
5. You are now in the **basics** tab of the create new user page. Populate the fields as follows:
 - i. User principal name: **sara**.
 - ii. Mail nickname: leave the default, which is set to derive from user principal name.
 - iii. Display name: **Sara Perez**.
 - iv. Password: uncheck the box that says auto-generate password and enter a temporary password that adheres to the password requirements and make note of it, as you will need it to complete the subsequent task.
 - v. Account enabled: Leave the checkmark to ensure the account is enabled.
 - vi. At the bottom of the page, select **Next: Properties**.
6. Here you will configure a few of the fields in the **Properties** tab.
 - i. First name: Sara
 - ii. Last name: Perez
 - iii. User types: Leave the default to **Member**, but note that from the drop-down you have the option to select guest.
 - iv. Usage location: Choose the country/region where you are located. Note that to get to the usage location field, you will need to scroll down on the page as it is the last field on the page. **NOTE:** if you don't do this, you will not be able assign a license in a subsequent step.
 - v. Select **Next: Assignments**.
7. You are now on the **Assignments** tab where you add a group assignment and view the available options for adding a role.
 - i. Select **Add group**.

- ii. The window that opens shows all the available groups.
 - iii. Notice the list of available groups. From the list, select **Operations**. From the bottom of the page, select the **Select** button. It may take a few seconds but you should see the operations group showup on the assignments page.
 - iv. From the top of the page, select **Add role**. A window opens that shows all the available directory roles. View the available options, but don't add any new roles. Close this page by selecting the **X** on the top right corner of the directory roles page.
 - v. From the bottom of the page, select **Review + create**. A summary of the settings will be displayed. From the bottom of the page, select **Create**.
8. You are returned to the users page. After a few seconds, Sara Perez will be listed. You may need to select the **refresh** icon on the top of the page.
9. From the user list, select the user you created, **Sara Perez**. The **Overview** page opens.
10. The left navigation panel shows the various options that can be configured for the user. View the available options.
11. From the left navigation panel, select **Licenses**. Notice that there are no license assignments found for this user. NOTE: Licenses can only be assigned if a usage location was configured. If you did not set the usage location, go back to that step in the previous task.
 - i. To add a license select **+ Assignments** from the top of the main window.
 - ii. Under Select licenses, select **Office 365 E3** and **Windows 10/11 Enterprise E3** then select the **Save** button on the bottom of the screen. A notification on the top right corner of the screen should show that license assignments succeeded.
 - iii. Select the **X** on the top right of the screen to close the License assignments window.
 - iv. Select the **Refresh icon** at the top of the page to confirm the license assignments.

12. Return to the Microsoft Entra admin center by selecting **Home** from the left navigation panel or from the top-left of the screen (the bread-crumb), above where it says Sara Perez | Licenses.
13. You have successfully created and configured a user in Microsoft Entra ID.
14. Sign out of all the open browser tabs. Sign out by selecting the user icon next to the email address on the top right corner of the screen then selecting **Sign out**. Close all the browser windows.

Task 2

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

1. Open Microsoft Edge.
2. In the address bar, enter <https://login.microsoft.com>.
3. Sign in as sara@WWLxZZZZZ.onmicrosoft.com, (where ZZZZZZ is your unique tenant ID provided by your ALH)
4. Enter the temporary password you set in the previous task.
5. You are now prompted to Update your password. In the Current password field, enter the temporary password from the previous task.
6. In the New password field, enter a new password, confirm the password, then select **Sign in**. Make note of your new password as you will need it for the subsequent lab exercise on SSPR.
7. You should now be successfully signed-in to Microsoft 365.
8. Sign out by selecting the icon on the top right corner of the Microsoft 365 window that is shown as a circle with the letters SP (next to the question mark icon), then selecting **Sign out**, then close the browser.

Review

In this lab, you started your initial exploration of Azure AD. Since subscribers to Microsoft 365 are automatically using Azure AD, you found that you access Azure AD features and services through either the Microsoft 365 admin portal or through the Azure portal. Whichever approach you prefer to get to the same place. You also walked

through the process of creating a new user and the different setting that can be configured, including groups to which the user can be assigned, the availability of roles, and assigning of user licenses.

Lab: Microsoft Entra self-service password reset

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities 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.

Estimated Time: 15-20 minutes

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).
 - i. In the Sign-in window, enter admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your ALH) then select **Next**.
 - ii. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.
 - iii. When prompted to stay signed- in, select **Yes**.
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."
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 (SMS only)** 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 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 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 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 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. This task requires that you have access to a mobile device where you can receive text messages or a personal email account that you can access

1. Open the Microsoft Edge and in the address bar enter <https://login.microsoft.com>.
2. Sign in as Sara Perez.
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 is for the Phone authentication method, if you don't have a mobile device with you that is capable of receiving text messages, skip to the next step. You're prompted to enter a phone number. Ensure the option **Text me a code** is enabled. Enter the phone number where you can receive a text code and select the **Next button**. A new window opens indicating a code was sent to the phone you entered. Enter the code you received and select **Next**. A window opens indicating Success and showing your Default sign-in method. Select **Done**.
 - i. Alternatively, you can set up a different method as shown on the bottom left of the window. If you choose to set up a different method, select **I want to set up a different method**, a pop-up window shows up, asking Which method would you like to use? From the drop-down, select your preferred method, **Email**, then select the **Confirm** button. Enter the email you would like to use then select **Next**. A new window opens indicating a code was sent to the email you entered. Access the email you entered to obtain the code. Enter the code you received and select **Next**. A window opens indicating Success and showing your Default sign-in method. 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 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.microsoftonline.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. Leave the default setting **Text my mobile phone**. You're prompted to enter your mobile phone number. Once you've entered it, select the **Text button**. If during the registration you selected email, the Get back into your account window will that indicate you'll receive an email containing a verification code at your alternate email address. Select **Email**.
8. Enter the verification code then press **Next**.
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@WWLxZZZZ.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 in the Office portal.
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.
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 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 ID
- 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.

Estimated Time: 30 minutes

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.

1. Open Microsoft Edge. In the address bar, enter <https://entra.microsoft.com>, and sign in with your admin credentials.
 - i. In the Sign-in window, enter admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.
 - ii. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.
 - iii. When prompted to stay signed- in, select **Yes**.
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**. IMPORTANT, make a note of the new password, as you'll need it in a subsequent task, to be able to sign in as the user.
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 Azure AD.

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. 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 **MFA Test Policy**.
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. In the search bar, enter **Azure**. From the search results that appear under the search box, select **Microsoft Admin Portals**, then press **Select** at the bottom of the page. Notice the warning.
13. 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.
14. Now you'll set the access controls. Under Grant, select **0 controls selected**.
15. The Grant window opens. Ensure **Grant access** is selected and then select **Require multifactor authentication**. Scroll down a bit on the right window and under the section For multiple controls, leave the default **Require all the selected controls**. Press **Select** at the bottom of the page.
16. At the bottom of the page, Under Enable policy, select **On**, then select **Create**.
17. From the left navigation pane select **Policies**. The MFA Pilot policy 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).
18. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting **Sign out**. Then close all the browser windows

Task 3

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 requires the user to go through MFA when accessing any of the Microsoft Admin Portals, including the Azure portal. To use MFA, the user must first register the authentication method that will be used for MFA, for example a code sent to a mobile device or an authenticator application.

1. Open Microsoft Edge. In the address bar, enter <https://login.microsoftonline.com>.
 - i. Sign in as DebraB@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.
 - ii. Enter the password you noted in the earlier task. Select **Sign in**.
 - iii. Since the password provided when you, as the admin, reset the password is temporary you need to update your password (this is not part of the MFA policy). 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.
 - iv. When prompted to stay signed- in, select **Yes**. You should be successfully logged in to your Microsoft 365 account. MFA was not required for this application as it is not part of the policy.
2. Now you'll attempt to sign in to an application that meets the criteria for MFA. Open a new browser tab and enter <https://portal.azure.com>.
3. You'll see a window indicating, More information required. Select **Next**. Note, this will initiate the MFA registration process, as this is the first time you're accessing the cloud app that that was identified in the conditional access policy. This registration process is required only once. An alternative to having the user go through the registration process is to have the admin configure the authentication method to use.
4. In the Keep your account secure window, you have the option to select the method to use for MFA. Microsoft Authenticator is one option. For expediency in this lab exercise, you'll choose a different method. Select **I want to setup a**

different method. From the Chose a different method pop-up window, select the **drop-down arrow** and select **Phone** then select **Confirm**.

5. In the window that opens, ensure your country is selected then enter mobile phone number you wish to use. Ensure that **Text me a code** is selected, then press **Next**. You'll receive a text message on your phone with a code that you'll need to enter where it says enter code. Enter the code you received, then press **Next**. Once confirmed, the screen will display, "SMS verified. Your phone was registered successfully". Select **Next**. then select **Done**. this completes the one-time registration process.
6. You should now be able to access the Azure portal. The Azure portal is a Microsoft Admin portal and therefore requires multi-factor authentication, per the conditional access policy that was created.
 - i. If you get a message indicating that your sign-in timed out you, enter the password and select **Sign in**.
 - ii. You'll see a window that requires you to verify your identity. Select where it says Text =X XXXXXXXX to receive a code on your mobile phone, enter the code and select **Verify**.
 - iii. If you're prompted to stay signed in, select **No**.
7. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting sign out. Then the close all the browser windows.

Review

In this lab, you went through the process of setting up a conditional access policy that requires users to go through MFA when they access any Microsoft Admin portal. Then, as a user you went through the registration process for MFA and saw the impact of the conditional access policy that required you to use MFA when accessing the Azure portal.

Lab: Explore Privileged Identity management

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft Entra
- Module: Describe the identity protection and governance capabilities of Microsoft Entra
- Unit: Describe the capabilities of Privileged Identity Management

Lab scenario

In this lab, you'll explore some of the basic functionality of Privileged Identity Management (PIM). PIM does require Microsoft Entra ID P2 licensing. In this lab, you, as the admin, will configure one of your users, Diego Siciliani, with a Microsoft Entra user administrator role, through Privileged ID management (PIM). With user admin privileges, Diego will be able to create users and groups manage licenses, and more. Both the admin and the user, Diego, must be configured for Microsoft Entra ID P2 licensing.

Estimated Time: 45-60 minutes

Task 1

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

1. Open Microsoft Edge. In the address bar, enter <https://entra.microsoft.com>.
2. Sign in with the Microsoft 365 admin credentials provided by your ALH.
 - i. In the Sign-in window, enter admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your ALH) then select **Next**.
 - ii. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.
 - iii. When prompted to stay signed- in, select **Yes**.

3. From the left navigation panel, expand **Identity**, expand **Users**, then select **All users**.
4. Select **Diego Siciliani** from the list of users.
5. Select **Reset password** from the top of the page. Since you haven't previously signed in as Diego, you don't know his password, and will need to reset the password.
6. When the password reset window opens, select **Reset Password**. IMPORTANT, make a note of the new password, as you'll need it in a subsequent task, to be able to sign in as the user.
7. From the left navigation panel, select **Home** to return the home page for the Microsoft Entra admin center.
8. Keep the browser page open, as you'll need it in the subsequent task.

Task 2

In this task you, as the admin, will assign Diego an Azure AD role in Privileged Identity Management.

1. Open the browser tab for the home page of the Microsoft Entra admin center.
2. From the left navigation panel, under "Identity", expand **Identity Governance**, then select **Privileged Identity Management**.
3. You are now in the Privileged Identity Management quick start page. Review the information on the Get started page. Select **Manage**.
4. You're now in the Contoso Roles page. In the search bar, on the top of the page, enter **user**. From the search results, select **User Administrator**.
5. From the top of the page, select **+ Add assignments**.
6. In the Add assignments page, ensure that **Membership** is underlined. Here you'll configure the membership settings for the user administrator role in PIM.
7. Leave the Scope type to its default value, Directory.
8. Under Select members, select **No member selected**. This opens the Select a member window.

9. In the search bar, enter **Diego**. From the search results, select **Diego Siciliani** then press **Select** on the bottom of the page.
10. Under Select members, you'll see 1 Member(s) selected and the name and email of the selected member(s), Deigo Siciliani. From the bottom of the Add assignments page, select **Next**.
11. You're now in the Setting page. Leave the Assignment type to the default setting, Eligible.
12. If the Permanently eligible box is checked, select **Permanently eligible**, to remove the checkmark.
13. In the Assignment start fields, keep the default date and time, which is today and the current time.
14. In the Assignment end fields, change the date to today's date (note the default setting is one year from the today, so you need to change the year). For the time, set the time to two hours from the current time. After you have set the time field for the time when the Assignment ends, press the tab key on your keyboard and select **Assign** on the bottom of the page.
15. This takes you back the Assignments window. After a few second you should see Diego Siciliani listed in the User Administrator table, along with the details of the assignment. If after a few seconds you still don't see the update, select **Refresh** from the top of the page.
16. From the top of the page, select **Settings**.
17. In the Role setting details for User Administrator, notice the different options. Note that the setting to "Require justification on activation" is set to yes, and "On activation, require Azure MFA" is also set to yes. You'll see both of these in the next task when Diego activates the role. Also note that "Require approval to activate" is set to No. Leave all the settings to their default values. Close the page by selecting the **X** on the top right corner of the screen.
18. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting **Sign out**. Then the close all the browser windows.

Task 3

In this task you, as Diego Siciliani, will sign in to Microsoft Entra admin center, to access the Privileged Identity Management capability of Microsoft Entra to activate your assignment as User administrator. Once activated you'll make some configuration changes to an existing user. Note: For this task, you'll need access to a mobile device to which you have immediate access and can receive text messages.

1. Open Microsoft Edge. In the address bar of the browser, enter **Entra.microsoft.com**.
2. Sign in as Diego Siciliani.
 - i. In the Sign-in window, enter **DiegoS@WWLxZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.
 - ii. Enter the temporary password that you noted from the previous task and select **Sign in**. Select **Sign in**.
 - iii. Since the password you entered was only a temporary password, you need to update now. Enter the current password, enter a new password, then confirm the new password. Make note of this new password as you will need to complete the task.
 - iv. When prompted to stay signed- in, select **Yes**.
3. You should be successfully logged in to Microsoft Entra admin center.
4. From the left navigation panel, expand **Identity Governance** then select **Privileged Identity Management**.
5. From the left navigation panel, select **My roles**. You're now seeing information for your eligible assignments. You'll see that you, Diego, are assigned the User administrator role.
6. In the last column of the table, labeled action, select **Activate**.
7. You'll see a warning icon indicating Additional verification required. Select **Click to continue**. Recall that the PIM settings for the User administrator role require multi-factor authentication. Additionally, since Diego's contact information for use with MFA (authentication methods) was not previously configured, he must register his information, to be able to use MFA. Although he will have to do MFA anytime he signs in as a user admin, within the assignment period, the MFA registration process is required only once.
8. You're notified that more information is required, select **Next**.

9. Enter your password.
10. From the bottom left of the Microsoft Authenticator window, select **I want to setup a different method**.
11. You're prompted to Choose a different method. Next to where it says Authenticator app, select the down arrow key. Select **Phone** and then select **Confirm**.
12. You're prompted to enter a phone number you would like to use. Ensure the country is correct, for your telephone number's country code. Enter your phone number, ensure that **Text me a code** is selected, then select **Next**.
13. Enter the 6 digit code you received on your phone and select **Next**.
14. You'll see a notification that your phone was registered successfully. Select **Next**, then select **Done**.
15. You're asked if you want to stay signed in. Select **Yes**.
16. The Activate User Administrator window appears. You're required to enter a reason for the activation. In the box that appears, enter any reason you want (max of 500 characters), then select **Activate**.
17. You'll see the status (3 stages of progress), as the activation is processed.
18. Once the activation is completed you're returned to the My roles | Azure AD roles page, where you'll see a notification stating you have activated a role. Select **Click here** to view your active roles. If you notice the end time is different than what was originally configured, select the refresh key on the top of the page (it may take a few minutes to refresh).
19. Return to the home page of the Microsoft Entra admin center by selecting **Home** from the left navigation panel.
20. As an Azure AD user administrator you can create users and groups, manage licenses, and more. From the left navigation panel, expand **Identity**, select **Users**, then select **All users**.
21. From the users list, select **Bianca Pisani**.
22. From the left navigation panel, select **Licenses**.

23. Notice how Bianca has no licenses assigned. From the top of the page, select **+** **Assignments**.
24. From the select licenses list, select **Office 365 E3** and **Windows 10 Enterprise E3**.
25. From the bottom of the page, select **Save**. You'll see a brief notification on the top right of page indicating licenses were successfully assigned.
26. Close out of the updated license assignments page, by selecting the **X** on the top right corner of the page.
27. Sign out by selecting on the user icon next to the email address on the top right corner of the screen and selecting **Sign out**. Then close all the browser windows.
28. The duration of the User Administrator role is limited to the time that was configured.

Review

In this lab; you, explored PIM. You, as the admin, configured Diego with user admin privileges for a specified amount of time. Then you, as Diego, walked through the process of activating the user admin privileges and configuring user settings. Recall that PIM requires Azure AD Premium P2 licensing.

Lab: Explore Azure Network Security Groups (NSGs)

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the basic security capabilities in Azure
- Unit: Describe Azure Network Security groups

Lab scenario

In this lab, you'll explore the function of network security groups in Azure. You'll do this by creating a network security group (NSG) and assigning the NSG to the interface of a pre-existing virtual machine (VM). Once configured you'll observe the default inbound and outbound rules, create new rules, and test those rules. In this lab, the VM you'll use with the NSG is created for you, so you'll first view some of the information associated with that VM.

Estimated Time: 30-45 minutes

Task 1

In this task, you'll view some of the parameters associated with the VM that that was created for use with this lab.

1. Open Microsoft Edge. In the address bar, enter <https://portal.azure.com>.
2. Sign in with your admin credentials.
 - i. In the Sign-in window, enter the username provided by your lab hosting provider then select **Next**.
 - ii. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.
 - iii. If prompted to stay signed- in, select **Yes**.
3. On the top of the page, underneath where it says Azure Services, select **Virtual Machines**. If you don't see it listed, then in the search box, in the blue bar on the

top of the page next to where it says Microsoft Azure, enter **Virtual Machines** then select **Virtual Machines** from the search results.

4. From the Virtual machines page, select the VM listed **SC900-WinVM**.
5. You're now in the SC900-WinVM page. Note some of the basic information about the VM.
6. From the left navigation panel, select **Network Settings**. The essentials sections of the main window shows the network interface for the VM. Note how there is nothing listed next to Network security group, as there is not NSG assigned to the interface.
7. Keep this tab open.

Task 2

In this task, you'll create a network security group, assign the network interface of the VM to that NSG, and create a new inbound rule for RDP traffic.

1. From the open Azure tab, *right-click* on the **Home** link at the top of the page and select **Open link in new tab** to open another page to Azure services.
2. In the blue search bar on the top of the page, enter **Network security groups** and, from the results, select **Network security groups**. Do not select *Network security groups (classic)*.
3. From the center of the page, select the blue button labeled **Create network security group**. Alternatively, you can select **+ Create** from the top of Network security groups page.
4. On the Basics tab of the Create network security group page, specify the following settings:
 - i. Subscription: Leave the default value (this is the Azure subscription provided by the authorized lab hoster)
 - ii. Resource group: **LabsSC900**
 - iii. Name: **NSG-SC900**
 - iv. Region: leave the default.
 - v. Select **Review + create** then select **Create**.
5. Once the deployment is complete, select **Go to resource**.

6. You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there are default inbound and outbound rules that are included with every NSG, as shown on the page. Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.
7. From the left navigation pane on the NSG-SC900 page, under Settings, select **Network interfaces**.
 - i. Select **Associate**.
 - ii. In the field for network interface associations, select the **down-arrow**, select **sc900-winvmXXX**, then select **OK** on the bottom of the window. Once the interface is associated to the NSG, it will show up on the list. The NSG is now assigned to the network interface of your VM.
8. Switch back to the **SC900-WinWM - Microsoft Azure** tab on the browser. Refresh the page. Next to where it says Network security group, you should now see the name of the NSG you just created. If you still don't see it, wait another minute and then refresh the page again.
9. From the left navigation panel, select **Connect**. From the main window, next to where it shows the port number 3389, select **Check access**. The check access function sends signals (traffic) to the default RDP port 3389 of the VM to check if it is accessible. It may take a minute, but you will see Not accessible. This is expected, because the DenyAllInBound NSG rule denies all inbound traffic to the VM.
10. Switch back to the **NSG-SC900 - Microsoft Azure** tab on the browser.
11. From the left navigation pane, select **Inbound security rules**. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer so you need to set up a rule to allow inbound RDP traffic (traffic on port 3389). Recall that you cannot remove the default rules, but you can override them by creating rules with higher priorities.

12. From the top of the page, select **Add**. On the Add inbound security rule window, specify the following settings:
 - i. Source: **Any**
 - ii. Source port ranges: *
 - iii. Destination: **Any**
 - iv. Service: **RDP**
 - v. Action: **Allow**
 - vi. Priority: **1000**. Rules with lower numbers have higher priority and are processed first.
 - vii. Name: Leave the default name or create your own descriptive name.
 - viii. Note the warning sign at the bottom of the page. We're using RDP only for testing purposes and to demonstrate the functionality of the NSG.
 - ix. Select **Add**
13. Once the rule is provisioned, it will appear on the list of inbound rules (you may need to refresh the screen).
14. Leave this browser tab open.

Task 3

In this task, you'll test the newly created inbound NSG rule to confirm that you can establish a remote desktop (RDP) connection to the VM. Once inside the VM you'll work to check outbound connectivity to the Internet from the VM.

1. Open the SC900-WinVM – Microsoft Azure Tab on your browser.
2. Select **Connect** from the left navigation panel.
3. Select **check access** (verify the port is set to 3389). The status should show as "Accessible".
4. Now connect directly to the VM by clicking **Select** in the box that says Native RDP.
 - i. From the Native RDP window that opens, select **Download RDP file**.
 - ii. If a download warning appears, select **Keep**, then on the pop-up window that appears, select **Open file**.
 - iii. A Remote Desktop Connection window opens; select **Connect**.

- iv. You'll be prompted for your credentials. Enter the Username and Password for the VM (refer to the resources tab on the lab instruction panel).
 - v. A Remote Desktop connection window opens indicating: *The identity of the remote computer cannot be verified. Do you want to connect anyway?* Select **Yes**.
5. You're now connected to the VM. In this case you were able to connect to the VM because the inbound traffic rule you created allows inbound traffic to the VM via RDP. After a few seconds on the Welcome screen you may see a window to Choose privacy settings for your device, select **Accept**. If the Networks window appears, select **No**.
6. With the VM in the RDP session up and running, test outbound connectivity to the Internet from the VM.
 - i. From the open VM, select **Microsoft Edge** to open the browser. Since this is the first time you open Microsoft Edge, you may get a pop-up window, select **Start without your data**, then select **Continue without this data**, then select **Confirm and start browsing**.
 - ii. Enter www.bing.com in the browser address bar and confirm you're able to connect to the search engine.
 - iii. Once you've confirmed that you can access www.bing.com, close the browser window in the VM, but leave the VM up.
7. Minimize the VM by selecting the underscore _ in the blue tab that shows the VM's IP address. This brings you back to the SC900-WinVM | Connect page.
8. Keep the browser tab open; you'll use it the next task.

Task 4

In the previous task you confirmed that you could establish an RDP connection to the VM. Once in the VM you also confirmed that you could establish an outbound connection to the Internet. The outbound Internet traffic was allowed because the default outbound rules for NSG allow outbound Internet traffic. In this task, you'll go through the process of creating a custom outbound rule to block outgoing Internet traffic and test that rule.

1. You should be on the SC900-WinVM | Connect page. From the left navigation panel, select **Networking**. If you previously closed the browser tab, select the

blue search bar on the top of the page and select Virtual machines, then select the VM, **SC900-WinVM**, then select **Networking**.

2. Select the **Outbound port rules** tab. You'll see the default outbound rules. Note the default rule "AllowInternetOutBound". This rule allows all outbound Internet traffic. You cannot remove the default rule, but you can override it by creating a rule with higher priority. From the right side of the page, select **Add outbound port rule**.
3. On the Add outbound security rule page, specify the following settings:
 - i. Source: **Any**
 - ii. Source port ranges: *
 - iii. Destination: **Service Tag**
 - iv. Destination service tag: **Internet**
 - v. Service: **Custom** (leave the default)
 - vi. Destination port ranges: * (be sure to put an asterisk in the destination port ranges field)
 - vii. Protocol: **Any**
 - viii. Action: **Deny**
 - ix. Priority: **1000**
 - x. Name: Leave the default name or create your own descriptive name.
 - xi. Select **Add**
4. Once the rule is provisioned, it will appear on the list of outbound rules. Although it appears on the list, it will take a few minutes to take effect (wait a few minutes before continuing with the next steps).
5. Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).
6. Open the Microsoft Edge browser in your VM and enter www.bing.com. The page should not display. If you're able to connect to the internet and you verified that all the parameters for the outbound rule were properly set, it's likely because it takes a few minutes for the rule to take effect. Close the browser, wait a few minutes and try again. Azure subscriptions in the lab environment may experience longer than normal delays.

7. Close the remote desktop connection, by selecting the **X** on the top center of the page where the IP address is shown. A pop-up window appears indicating Your remote session will be disconnected. Select **OK**.
8. From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.
9. Keep the Azure tab open on your browser.

Review

In this lab, you walked through the process of setting up a network security group (NSG), associating that NSG to the network interface of a virtual machine, and adding new rules to the NSG to allow inbound RDP traffic and to block outbound Internet traffic.

Lab: Explore Microsoft Defender for Cloud

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the security management capabilities of Azure
- Unit: Describe cloud security posture management

Lab scenario

In this lab, you'll explore Microsoft Defender for Cloud. NOTE: the Azure subscription provided by the Authorized Lab Host (ALH) limits access and may experience longer than normal delays.

Estimated Time: 30 minutes

Task 1

In this task, you'll do a high-level walk-through of some of the capabilities of Microsoft Defender for Cloud

1. You should be on the home page for Azure services. If you previously closed the browser, open Microsoft Edge. In the address bar, enter **portal.azure.com**, and sign in with your admin credentials.
2. In the blue search bar enter **Microsoft Defender for Cloud**, then from the results list, select **Microsoft Defender for Cloud**.
3. If this is the first time you enter Microsoft Defender for Cloud with your subscription you may land on the Getting started page, and may be prompted to upgrade. Scroll to the bottom of the page and select **Remind me later** (or **Skip**). You'll be taken to the Overview page.
4. From the Overview page of Microsoft Defender for Cloud, notice the information available on the page (if you see 0 assessed resources and active recommendations, refresh the browser page, it may take a few minutes). Information on the top of the page includes the number of Azure subscriptions, the number of Assessed resources, the number of active recommendations, and

any security alerts. On the main body of the page, there are cards representing Security posture, Regulatory compliance, Insights, and more. Note: The Microsoft Defender for Cloud default policy initiative, which would normally have to be assigned by the admin, has already been assigned as part of the Azure subscription setup. The secure score, however, will show as 0% because there can be up to a 24 hour delay for Azure to reflect an initial score.

5. From the top of the page, select **Assessed resources**.
 - i. This brings you to the **Inventory** page that lists the current resources. Select the virtual machine resource, **sc900-winwm**. This resource is associated with the virtual machine you used in the previous lab.
 - ii. The Resource health page for the VM provides a list of recommendations. From the available list, select any item from the list that shows an **unhealthy** status.
 - iii. Note the detailed description. Select the drop-down arrow next to Remediation steps. Note how remediation instructions (or links to instructions) are provided along with the option to take action. Exit the window without taking any action.
 - iv. Return to the Microsoft Defender for Cloud overview page, by selecting **Microsoft Defender for Cloud | Overview** from the top of the page, above where it says Resource health.

6. From the left navigation panel, select **Recommendations**.
 - i. Verify, the **All recommendations** tab is selected (underlined). Note the dashboard view that shows Active recommendations by severity, Resource health, and more.
 - ii. From the list, select an item. In the page that opens, you'll see a description and additional information that may include remediation steps, affected resources, and more. Exit out this page, by selecting the **X** on top-right corner of the screen.

7. From the main left navigation panel, select **Regulatory compliance**. **NOTE:** If you see that there is no subscription to calculate compliance for, its because there may be up to a 24 hour delay for information to appear. Move to Task 2. If you do see information then proceed with the steps that follow.
 - i. The regulatory compliance page provides a list of compliance controls based on the Microsoft cloud security benchmark (verify that Microsoft cloud security benchmark tab is selected/underlined). Under each control

domain is a subset of controls and for each control there are one or more assessments. Each assessment provides information including description, remediation, and affected resources.

- ii. Let's explore one of the control domains areas. Select (expand) **NS. Network Security**. A list of controls related to network security is displayed.
- iii. Select **NS-10. Ensure Domain Name System (DNS) security**. Note the list of automated assessments (which include automated assessments for AWS) and how each assessment line item provides information including the resource type, failed resources and compliance stations. Select the assessments listed. Here you see information including a description, Remediation steps, and Affected resources.
- iv. Select the **X** on the top-right corner of the screen to close the page.
- v. Select **Overview** from the left navigation panel to return to the Microsoft Defender for Cloud Overview page.
- vi. Keep the Microsoft Defender for Cloud overview page open, you'll use in the next task.

Task 2

Recall that Microsoft Defender for Cloud is offered in two modes: without enhanced security features (free) and with enhanced security features that are available through the Microsoft Defender for Cloud plans. In this task, you discover how to enable/disable the various Microsoft Defender for Cloud plans.

1. From the Microsoft Defender for Cloud overview page, select the **Environment settings** from the left navigation panel.
2. Select the **Expand all** box then select the **MOC Subscription--lodXXXXXXXXX** subscription listed next to the yellow key icon.
3. On the Defender plans page, notice how you can select Enable all or select individual Defender plans.
 - i. Verify that CSPM status is set to **On**, if not, set it now.
 - ii. Enable the plan for Servers. Select **On** for the Servers line item, then select **Save** from the top of the page.
4. From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.
5. Keep the Azure tab open on your browser.

Review

In this lab, you explored Microsoft Defender for Cloud.

Lab: Explore Microsoft Sentinel

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the security capabilities of Microsoft Sentinel
- Unit: Describe threat detection and mitigation capabilities in Microsoft Sentinel

Lab scenario

, you'll walk through the process of creating a Microsoft Sentinel instance. You'll also set up the permissions to ensure access to the resources that will get deployed to support Microsoft Sentinel. Once this basic setup is done you'll walk through the steps for connecting Microsoft Sentinel to your data sources, set up a workbook, and do a brief walk-through of some of key capabilities available in Microsoft Sentinel.

Estimated Time: 45-60 minutes

Task 1

Create a Microsoft Sentinel instance

1. You should be at the home page for Azure services. If you previously closed the browser, open Microsoft Edge. In the address bar, enter **portal.azure.com**, and sign in with your admin credentials.
2. In the blue search box on the top of the page, enter **Microsoft Sentinel** then select **Microsoft Sentinel** from the search results.
3. From the Microsoft Sentinel page, select **Create Microsoft Sentinel**.
4. From the Add Microsoft Sentinel to a workspace page, select **Create a new workspace**.
5. From the basics tab of the Create Log Analytics workspace, enter the following:
 - i. Subscription: leave the default, this is the Azure subscription provided by the Authorized Lab Host (ALH).

- ii. Resource group: select **SC900-Sentinel-RG**. If this resource group is not listed create it by selecting **Create new**, enter **SC900-Sentinel-RG**, then select **OK**.
 - iii. Name: **SC900-LogAnalytics-workspace**.
 - iv. Region: **East US** (A different default region may be selected based on your location)
 - v. Select **Review + Create** (no tags will be configured).
 - vi. Verify the information you entered then select **Create**.
 - vii. It may take a minute or two for the new workspace to be listed, if you still don't see it, select **Refresh**, then select **Add**.
6. Once the new workspace is added, the Microsoft Sentinel | News & guides page will display, indicating that the Microsoft Sentinel free trial is activated. Select **OK**. Note the three steps listed on the Get started page.
 7. Keep this page open, as you'll use it in the next task.

Task 2

With the Microsoft Sentinel instance created, it is important that users that will have responsibility to support Microsoft Sentinel have the necessary permissions. This is done by assigning the designated user the required role permissions. In this task, you'll view the available, built-in Microsoft Sentinel roles.

1. In the blue search box, enter **resource groups** then select **Resource groups** from the search results.
2. From the Resource groups page, select the resource group that you created with Microsoft Sentinel, **SC900-Sentinel-RG**. Working at the resource group level will ensure that any role that is selected will apply to all the resources that are part of the Microsoft Sentinel instance that was created in the previous task.
3. From the SC900-Sentinel-RG page, select **Access control (IAM)** from the left navigation panel.
4. From the Access control page, select **View my access**. For the Azure subscription provided to you by the Authorized Lab Host, a role has been defined that will give you access to manage all necessary resources, as shown in the description. It is important, however, to understand the available Sentinel specific roles. Close the assignments window by selecting the **X** on the top-right corner of the window.

5. From the Access control page, select the **Roles** tab on the top of the page/
 - i. In the search box, enter **Microsoft Sentinel** to view the built-in roles associated with Microsoft Sentinel.
 - ii. From any of the roles listed, select **view** to view the details of that role. As a best practice you should assign the least privilege required for the role.
 - iii. Close the window by selecting the **X** on the top-right corner of the window.
6. From the access control page, close the window by selecting the **X** on the top-right corner of the window.
7. From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.
8. Keep the Azure tab open on your browser.

Task 3

The purpose of this task is to walk you through the steps involved in connecting to a data source. Many data connectors are deployed as part of a Microsoft Sentinel solution together with related content like analytics rules, workbooks and playbooks. The Microsoft Sentinel Content hub is the centralized location to discover and manage out-of-the-box (built-in) content. In this step, you'll use the content hub to deploy the Microsoft Defender for Cloud solution for Microsoft Sentinel. This solution allows you to ingest Security alerts reported in Microsoft Defender for Cloud.

1. From the Azure services home page, select Microsoft Sentinel, then select the instance you created, **SC900-LogAnalytics-workspace**.
2. From the left navigation panel, select **Content hub**.
3. Take a moment to scroll down to see the long list of available solutions and the options to filter the list. For this task, you're looking for **Microsoft Defender for Cloud**. Select it from the list. In the side window that opens, read the description then select **Install**. Once the installation is completed, the status column in the main window will show as installed.
4. Once again, select **Microsoft Defender for Cloud** from the list. From the window on the right, select **Manage**.

5. On the right side of the the Microsoft Defender for Cloud page is the description and notes associated with the solution from Content Hub and what is included as part of this solution. On the main window are the components of the solution. In this case there are two data connectors and one data rule. The orange triangle indicates that some configuration is needed. Select the box next to where it says **Subscription-based Microsoft Defender for Cloud (Legacy)**. A window opens on the right side of the page. Select **Open connector page**.
6. Note the configuration instructions. Select the box next to the name of the subscription then select **Connect**. A pop-up window may appear indicating that only subscriptions you have Security Reader permissions on will start streaming Microsoft Defender for Cloud alerts. Select **OK**. The status will move to connected. The connector is now enabled, although it may take some time for the connector to show up in the data connectors page.
7. Now view information about the analytics rule. From the top of the page (in the breadcrumb) select **Microsoft Defender for Cloud**. De-select the box next to where it says Microsoft Defender for Cloud, as you have already configured the connector (it may take some time for the warning icon to disappear). Select the box next to where it says, **Detect CoreBackUp Deletion Activity from related security alerts**. This brings up the Analytics Rules page. Again, select the **Detect CoreBackUp Deletion Activity from related security alerts** rule. A window that opens on the right, that provides information about the rule and what it does. Select **Create rule**.
 - i. Although the details of the rule logic are beyond the scope of the fundamentals, go through each tab in the rule creation to view the type of information that can be configured
 - ii. When you reach the Review + create tab, select **Save**.
8. Return to the Sentinel page by selecting **Microsoft Sentinel | Content hub** from the bread-crumbs at the top of the page, above where it says Analytics rules.
9. Keep this page open, as you'll use it in the next task.

Task 4

In this task, you'll walk through some of the options available in Sentinel.

1. From the left navigation panel, select **Hunting**. From the top of the page, select the **Queries** tab. Read the description of what is a hunting query. Hunting queries

can be added through the Content hub. Any queries previously installed would be listed here. Select **Go to content hub**. The content hub lists content that includes queries either as part of a solution or as a standalone query. Scroll down to see the available options. Close the Content hub by selecting the **X** on the top-right corner of the window.

2. From the left navigation panel, select **MITRE ATT&CK**. MITRE ATT&CK is a publicly accessible knowledge base of tactics and techniques that are commonly used by attackers. With Microsoft Sentinel you can view the detections already active in your workspace, and those available for you to configure, to understand your organization's security coverage, based on the tactics and techniques from the MITRE ATT&CK® framework. Select any cell from the matrix and note the information available on the right side of the screen. **Note:** You may need to select the "<<" at the far-right side of the window to see the information panel.
3. From the left navigation panel, select **Community**. The community page includes Cybersecurity insights and updates from Microsoft Research, a link to a list of Microsoft Sentinel Blogs, a link to Microsoft Sentinel Forums, links the the latest editions to the Microsoft Sentinel Hub, and more. Explore this at will.
4. From the left navigation panel, select **Analytics**. There should be two active rules, one that is available by default and the rule you created in the previous task. Select the default rule **Advanced Multistage Attack Detection**. Note the detailed information. Microsoft Sentinel uses Fusion, a correlation engine based on scalable machine learning algorithms, to automatically detect multistage attacks (also known as advanced persistent threats) by identifying combinations of anomalous behaviors and suspicious activities that are observed at various stages of the kill chain. On the basis of these discoveries, Microsoft Sentinel generates incidents that would otherwise be difficult to catch. **Note:** You may need to select the "<<" at the far-right side of the window to see the information panel.
5. From the left navigation panel, select **Automation**. Here you can create simple automation rules, integrate with existing playbooks, or create new playbooks. Select **+ Create** then select **Automation rule**. Note the window that opens on the right side of the screen and the options available to create conditions and actions. Select **Cancel** from the bottom of the screen.
6. From the left navigation panel, select **Workbooks**. Read the description of the Microsoft Sentinel workbook. Workbooks can be added through the Content hub. Any workbooks previously installed would be listed here. Select **Go to**

content hub. The content hub lists content that includes workbooks either as part of a solution or as a standalone workbook. Scroll down to see the available options.

7. Close the window by selecting the **X** on the top-right corner of the window.
8. From the top left corner of the window, just below the blue bar, select **Home** to return to the home page of the Azure portal.
9. Sign out and close all the open browser tabs.

Review

In this IV you walked through the steps for connecting Microsoft Sentinel to data sources, you set up a workbook, and walked several options available in Microsoft Sentinel.

Lab: Explore Microsoft Defender for Cloud Apps

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the threat protection capabilities of Microsoft 365
- Unit: Describe Microsoft Defender for Cloud Apps

Lab scenario

In this lab, you'll explore the capabilities of Microsoft Defender for Cloud Apps. You'll walk through the information available on the Cloud Discovery dashboard, the Cloud app catalog, capabilities available to investigate findings, and ways to control impact to your organization through policies. Note: An organization must have a license to use Microsoft Defender for Cloud Apps that is a user-based subscription service.

Estimated Time: 15-20 minutes

Task 1 - Explore Cloud discovery

Explore Cloud Discovery.

1. Open Microsoft Edge. In the address bar, enter **admin.microsoft.com**.
2. Sign in with your admin credentials for the Microsoft 365 tenant.
 - i. In the Sign in window, enter admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.
 - ii. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.
 - iii. When prompted to stay signed- in, select **Yes**. This takes you to the Microsoft 365 admin center page.
3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.
4. Under Admin centers, select **Security**. A new browser page opens to the welcome page of the Microsoft 365 Defender portal.

5. If this is the first time you visit the Microsoft 365 Defender portal, you may get a pop-up window to take a quick tour. Close this.
6. From the left navigation panel, select **Cloud apps** to expand the list then select **Cloud Discovery**. This takes you to the Dashboard view. Note the information available on the dashboard. From the dashboard view, you can select different tabs from the top of the page.
7. Select **Discovered apps**. The discovered apps window provides a more detailed view of the discovered apps, including risk score, traffic, number of users and more.
 - i. From any item on the list, select the **ellipses** in the actions' column of the table. Note the various options available, including the ability to tag an app as sanctioned or unsanctioned. Select the **ellipses**, again, to close the actions box.
 - ii. Selecting a specific line item opens a details page for the specific app. Select an item from the list and review the information available on the overview page. For the selected item, select the **Cloud app usage** tab to see more detailed information, including **Usage, Users, IP, Addresses, and Alerts**. When you're done exploring the details page, return to discovered apps page, by selecting **Cloud Discovery** from the bread crumb on the top of the page. If you select Cloud discovery from the left navigation panel, it will take you back to the dashboard view.
 - iii. From the top of the page, select the **IP addresses** tab. Here you'll find data including number of transactions, amount of traffic and upload amounts, by IP address. Note that you can also filter by specific IP address or export the data for further analysis.
 - iv. From the top of the page select **Users**. This is the same type of information provided when you select IP addresses, but instead it's listed for individual users. Here again, you filter by specific user and export data for further analysis.
8. The information provided in the Cloud Discovery page and the related tabs are based on either snap-shot reports from traffic logs you manually upload from your firewalls and proxies or from continuous reports that analyze all logs that are forwarded from your network using Cloud App Security. To see where this is set up, select **Actions** on the top-right corner of the page.
 - i. Select the first option, **Create Cloud Discovery snapshot report** then select **Next**. Here you would fill in the requested details and upload traffic

logs to generate and upload a report. Select **Quit** and if prompted with Are you sure, select **Quit** again. The data you're seeing for your lab tenant came from a Snapshot report, you can see this information on the top of the Cloud Discovery window.

- ii. To see the option for continuous reports, select the **Actions** on the top-right corner of the page and from the drop-down select **Configure automatic upload**. There are no data sources connected, but this is where you would add a data source. Select **Add a data source** then select the drop-down arrow in the **Select appliance** field to see the types of appliances that you can connect as a data source. Select **Cancel** to exit,
 - iii. From the left navigation panel, select **Cloud discovery** to return to Cloud discovery page.
9. You can connect to apps directly by setting up app connectors that will provide you with greater visibility and control over your cloud apps. From the top-right corner of the screen, select **Actions** then select **Cloud Discovery Settings**. From the left side of the screen, under Connected apps, select **App connectors**.
 - i. On the Connected apps page, select **Office 365** from the list to view the detailed information available and then select the vertical ellipses on the right side of the screen and select **View App connector settings** to return to the App connectors page. If Office 365 is showing a connection error, it's most likely because Audit is not turned on. If audit is enabled, go to the vertical ellipses on the right side of the line item, and select **Edit settings**. To reconnect, select **Connect Office 365** on the bottom of the page. The page should now show that Office 365 is connected. Select **Done**. The status will now show with a yellow warning sign, indicating there is no recent status. It will take some time for status to update as the retroactive scan time period differs per app, and lab tenants may experience longer than normal delays.
 - ii. Now you'll set up a new app connector. Select **+Connect an app** and from the drop-down list select **Microsoft Azure**. From the Microsoft Azure pop-up window, select **Connect Microsoft Azure** then select **Done**. You'll see a connected status (if you don't see it, refresh the browser). Select **Microsoft Azure** to view the detailed information on scanning users, data, and activities. Return to the Cloud Discovery dashboard by selecting **Cloud Discovery** under Cloud Apps from the left-most navigation panel.
10. Keep this page open, as you'll use it in the next task.

Task 2 - Explore the Cloud app catalog

Cloud Discovery analyzes your traffic logs against the Microsoft Defender for Cloud Apps cloud app catalog of over 31,000 cloud apps. The apps are ranked and scored based on more than 80 risk factors to provide you with ongoing visibility into cloud use, Shadow IT, and the risk Shadow IT poses to your organization. In this task, you'll explore the capabilities of the Cloud app catalog.

1. From the left navigation panel, select **Cloud app catalog**.
2. The Cloud app catalog enables you to choose apps that fit your organization's security requirements. Admins can do basic filtering of apps as shown on the top of the page, which includes whether the app is sanctioned, unsanctioned, or has no tag, risk score, Compliance risk factor, and security risk factor. For example, filtering by compliance risk factor lets you search for a specific standards, certification, and compliance that the app may comply with. Examples include HIPAA, ISO 27001, SOC 2, and PCI-DSS. Select **Compliance risk factor** to view the available options. You can further filter by risk score, by moving the sliders on the risk score on the top of the page. If you moved the slide, be sure to set it so the range is set at 0 to 10.
3. Admins can also search for apps by category. For example, in the search for category field enter **Social network**, then select **Social network**. Select any item from the list for a detailed view. Hovering your mouse over any topics for a given category will show an information icon that you can select to get more information about that topic.
4. Keep this page open, as you'll use it in the next task.

Task 3 - Explore the Activity log and Files

Explore ways in which you can investigate the recorded activities with the activity log and files.

1. From the left navigation panel, select **Activity Log**. Here you get visibility into all the activities from your connected apps. You may not see any data listed as it can take several hours to perform retroactive scans once audit is enabled and lab tenants may experience longer than normal delays. Note the available filter options and the option to create new a policy from search.

2. To provide data protection, Microsoft Defender for Cloud Apps gives you visibility into all the files from your connected apps, for example all the files stored in SharePoint and Salesforce. From the left navigation pane, select and explore the **Files** option.
 - i. The ability to scan files must be enabled as part of the Information protection settings of Microsoft 365 Cloud apps. Select **Enable file monitoring** and select the box next to where it says **Enable file monitoring** then select **Save**.
 - ii. Return to files by selecting **Files**, listed under cloud apps, from the left navigation panel. As noted, it can take several days for files to display, once file monitoring is enabled it's worth noting that once files are listed you can filter data by app, owner, access level, file type, and matched policy. Also, you create a new policy from search and export of the data.
3. Keep this page open, as you'll use it in the next task.

Task 4 - Explore Policies

In this task, you'll explore the policies in Microsoft Defender for Cloud Apps.

1. From the left navigation panel, select **Policies** then select **Policy management**. The listed policies provide information on the number of alerts generated by the policy, severity, etc. Selecting any line item provides more detailed information about the policy.
 - i. Note that you can also create a policy. Select **+ Create policy** to view the types of policies you can create. Select **Activity policy** to view the different options available for creating the policy. Select **Cancel** to exit out of the configuration window.
 - ii. Note that you can also have the option to export policy information.
2. From the left navigation panel, select **Policy templates**. To create a policy from one of the available templates, select the **+** on the right side of a template line item. View the different configuration options for the policy. Select **Cancel** to exit out of the page.
3. Close the browser window.

Review

In this lab, you explored the capabilities of Microsoft Defender for Cloud Apps. You walked through information available on the Cloud Discovery dashboard, the Cloud app catalog, capabilities available to investigate findings, and ways to control impact to your organization through policies.

Lab: Explore the Microsoft 365 Defender portal

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the threat protection capabilities of Microsoft 365
- Unit: Describe the Microsoft 365 Defender portal

Lab scenario

In this lab, you'll explore the Microsoft 365 Defender portal by walking through the content displayed on the landing page. You'll also explore the options on the navigation panel that provide quick access to functionality that is part of Microsoft's Extended Detection and Response (XDR) solution: Microsoft Defender for Endpoints, and Microsoft Defender for Office 365 (email and collaboration). Lastly you'll also explore how Microsoft Secure Score can help an organization improve its security posture.

Estimated Time: 10-15 minutes

Task 1

Explore the Microsoft 365 Defender landing page.

1. Open Microsoft Edge. In the address bar, enter **admin.microsoft.com**.
2. Sign in with your admin credentials.
 - i. In the Sign-in window, enter **admin@WWLxZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.
 - ii. Enter the admin password provided by your lab hosting provider. Select **Sign in**.
 - iii. When prompted to stay signed- in, select **Yes**. This takes you to the Microsoft 365 admin center page.

3. From the left navigation pane of the Microsoft 365 admin center, under Admin centers, select **Security**. If you don't see Security listed, select **Show all**, then select **Security**. A new browser page opens to the welcome page of the Microsoft 365 Defender portal.
4. If this is the first time you visit the Microsoft 365 Defender portal, you may get a pop-up window to take a quick tour. It is recommended that you complete the tour. Select **Take a quick tour**. Read the description provided in each pop-up window, then select **Next**. Continue through the tour until you get to the end, then select **Done**.
5. The welcome page of the Microsoft 365 Defender portal, shows many of the common cards that security teams need. The composition of cards and data is dependent on the user role. Scroll through the page to view the default set of cards for your role as global admin.
6. The cards displayed can be customized to your preference. Select **+ Add cards**. A Window opens that displays any cards that are available to add to your home page. You may already have all cards displayed in which case you will see the note, "You already have all the cards on your home page." Close the window by select the **X** on top-right corner of the window.
7. Selecting the ellipses on the top-right of any card will provide more actions you can take.
8. You can also move the cards around. Hover your mouse cursor over the title bar of any card, when you'll get a cross shaped cursor select the card and move it to your desired location.
9. Selecting the title of a card will take you to additional information for that topic. You'll explore this in the next task.
10. The left navigation panel provides links/access to information that is part of Microsoft's Extended Detection and Response (XDR solution) which includes incidents & alerts, hunting, action center, threat analytics, secure score and more. It also includes quick access to Microsoft Defender for Endpoint (the links listed under Endpoints), Defender for Office for 365 (links listed under Email and Collaboration), Microsoft Defender for Cloud Apps (links under Cloud apps). Explore these options by selecting some of the links. To return to the home page of the Microsoft 365 Defender portal, select **Home** on the left navigation panel.
11. Keep the browser window open.

Task 2

In this task, you'll explore how Microsoft Secure Score can help an organization improve its security posture.

1. From the Welcome page of the Microsoft 365 Defender portal, select **Microsoft Secure Score**, from the title bar of the card (the text will turn blue). Alternatively, you can select **Secure score** from the left navigation panel.
2. The Microsoft Secure Score page opens to the Overview tab. Microsoft Secure Score is a measurement of an organization's security posture. Your organization's secure score is shown as a percentage, along with the number of points you've achieved out of the total possible points and broken down by category. Select **Include**, next to where it says Your secure score. A small window opens that allows you to include the achievable score, Planned score, and Current license score in the breakdown of your organization's secure score. Select **Include** again to close the window.
3. The overview page also includes top improvement actions, comparison score, history, and additional resources.
4. Select **Recommended actions** from the top of the page. Notice the information available in the table.
5. Select the first items from the list and review the available information. In the window that opens, note the status options available. Select the **Implementation** tab to view information related to implementation. Select the **X** at the top right corner to close this window.
6. Select the **History** tab from the top of the page. For each activity listed there is a brief statement that provides context. Select an item from the history table. On the top-right of the details page, under History, select **X events** (where X is a number). The action history window opens and provides more information. Select **Close** on the bottom of the page, then select the **X** on the top-right corner of the details page to return to the History page.
7. From the top of the page, select **Metrics & trends**. Note the available information. From the top-right corner of the page, select the **calendar icon**. You can narrow down the view to a custom date range. Selecting the **filter icon**, allows you to filter the view by Identity and/or apps. Close the window and select **Home** from the left navigation panel to return to the Microsoft 365 Defender home page.

8. Close all the open browser tabs.

Review

In this lab, you explored the Microsoft 365 Defender portal by walking through the content displayed on the landing page, you explored the options on the navigation panel that provides quick access to functionality that is part of Microsoft's Extended Detection and Response (XDR) solution, Microsoft Defender for Endpoints, and Microsoft Defender for Office 365 (email and collaboration). Lastly you explored how Microsoft Secure Score can help an organization improve its security posture.

Lab: Explore the Service Trust Portal

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft compliance
- Module: Describe the compliance management capabilities at Microsoft
- Unit: Explore the Service Trust Portal

Lab scenario

In this lab, you'll explore the features and content available from the Service Trust Portal. You'll also visit the Trust Center to view information about Privacy at Microsoft.

Estimated Time: 10-15 minutes

Task 1

In this task, you'll explore the Service Trust portal and the different types of content available, you'll learn how to access reports, and how to save reports to your library.

1. Open Microsoft Edge.
2. In the address bar, enter **aka.ms/STP**. This will bring you to the landing page for the Service Trust Portal. The Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.
3. To access some of the resources on the Service Trust Portal, you must sign in as an authenticated user with your Microsoft cloud services account and review and accept the Microsoft Non-Disclosure Agreement for Compliance Materials. On the top, right hand corner of the landing page for the Service Trust Portal, you'll see the option to Sign in. **Sign in**, using your admin credentials and, if prompted, select **Agree** to accept the Microsoft Non-Disclosure Agreement for Compliance Materials.
4. Scroll down on the page and notice the different categories of information available. From the Certifications, Regulations, and Standards category select **ISO/IEC**.

5. Note the description on the top of the page and available applicable documents. Select the **ellipsis** under the More Options header for first document on the list. Note the different options.
6. Select **Save to Library**. A window will pop up asking if you want to subscribe to this document. Select **Yes**. A window will pop up for notification settings, note the different settings. Select **Save**.
7. To verify that the document has been saved, scroll up to the top of the page and select **My Library**. For any document on the My Library page, select the ellipsis to view the available options.
8. From the top of the My Library page, select **Service Trust Portal** to return to the Service Trust Portal home page.
9. From the Service Trust Portal home page, scroll down to the **Industry and Regional Resources** category. Note the available tiles. Select **Financial Services**. Scroll down to see all the available regions and countries. Select the tile for any country to view the applicable documents.
10. To return the Service Trust Portal home page, select the link **Service Trust Portal** at the top of the page.
11. From the Service Trust Portal home page, scroll down to the **Resource for your Organization** category. Select **Resources for your Organization**. Note that any documents listed here are based on your organization's subscription and permissions.
12. To return the Service Trust Portal home page, select the link **Service Trust Portal** at the top of the page.

Task 2

In this task, you'll visit the Trust Center and navigate to information that describes Privacy at Microsoft.

1. From the Service Trust Portal home page, scroll down to the **Reports, Whitepapers, and Artifacts** category. Select **Privacy and Data Protection**.
2. In addition to listing all applicable documents, there is a description of the category followed by a link to Learn more. Select **Learn more**.

3. A new browser page opens to the Microsoft Trust Center where you find more information, including information about privacy and much more. Explore the contents of this page and navigate through different links.
4. Close all the open browser tabs.

Review

In this lab, you explored some of the options available under the Service Trust Portal and how to use the My Library feature to save documents for future review. Additionally, you visited the Trust Center to access and review information about privacy at Microsoft.

Lab: Explore the Microsoft Purview compliance portal & Compliance Manager

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft compliance
- Module: Describe the compliance management capabilities in Microsoft Purview
- Unit: Describe the Microsoft Purview compliance portal

Lab scenario

In this lab, you'll explore the Microsoft Purview compliance portal home page and ways in which the capabilities of Compliance Manager can help organizations improve their compliance posture.

Estimated Time: 30-45 minutes

Task 1

Explore the Microsoft Purview compliance portal home page and learn to customize the card view and the navigation panel.

1. Open Microsoft Edge. In the address bar, enter **admin.microsoft.com**.
2. Sign in with your admin credentials.
 - i. In the Sign in window, enter **admin@WWLxZZZZZZ.onmicrosoft.com** (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider) then select **Next**.
 - ii. Enter the admin password that should be provided by your lab hosting provider. Select **Sign in**.
 - iii. When prompted to stay signed- in, select **Yes**. This takes you to the Microsoft 365 admin center page.
3. From the left navigation pane of the Microsoft 365 admin center, select **Show all**.

4. Under Admin centers, select **Compliance**. A new browser page opens to the welcome page of the Microsoft Purview compliance portal.
5. The card section on the home page shows you, at a glance, how your organization is doing with your compliance posture, what solutions are available for your organization, and more.
6. From the main window, scroll down to view the different cards. The cards available on the home screen and the position of the cards can be changed to accommodate each administrator's preference.
7. Placing your mouse cursor over the title bar of any card turns the title bar grey. When you see the cursor turn into a cross shape, you can move the card to your desired location.
8. On the title bar of every card, you'll also see an ellipsis that provides actions you can take. Select the ellipses on the Solution catalog and select **Remove**.
9. You can add cards, by selecting **+ Add cards**. The Add cards to your home page window opens. Place your mouse cursor over the card shown in this window and drag it over to the location on your home screen where you want the card to be positioned.
10. From the left navigation panel of the Microsoft Purview compliance portal home page, notice the items listed under Solutions.
11. As the compliance admin, there may be a set of solutions that you manage for our organization and as such, you may want to have only those solutions listed in the navigation panel that you see. To customize to your preferences select **Customize navigation**.
12. From the window labeled Customize your navigation pane, note how you can select the items you want to have appear on the navigation panel and de-select the items you don't want to see. For the purpose of these labs, keep all items selected and hit **Save** on the bottom of the window.
13. Leave the browser tab open.

Task 2

Learn about your organization's compliance posture through Compliance Manager.

1. From the left navigation panel of the Microsoft Purview compliance portal, select **Compliance Manager**. Alternatively, you can select Compliance Manager on the title bar of the Compliance Manager card.
2. From the top of the Compliance Manager page, ensure **Overview** is selected (underlined). Scroll down to see all the information available on the page. Information on this page includes your compliance score, your points achieved, and Microsoft managed points achieved. You'll see Key improvement actions, Solutions that affect your score and compliance score breakdown by categories.
3. From the top of the Overview page, select **Improvement actions**. These are actions that can improve the organization's compliance score. Note that as improvement actions are taken, points may take up to 24 hours to update. Notice the available filters.
4. From the list of improvement actions, select **Enable self-service password reset**. Review the available information for the improvement action. The left side of the window provides a brief overview about the implementation, test status, and more. To the right of the overview is the details page from which you can select implementation, testing, the related standards and regulatory requirements, and documents. Each of these tabs provides more detailed information for the improvement action.
5. Exit out of this improvement action by selecting **Improvement Actions** from the breadcrumb on the top-left of the page. You're now back on the improvement actions page.
6. From the top of the page, select **Solutions**. On this page, you'll see how solutions contribute to your score and their remaining opportunity for improvement.
7. From the top of the page, select **Assessments**. On this page, you'll see the Data Protection Baseline for Microsoft 365. This is a default baseline assessment Microsoft provides in Compliance Manager for Microsoft 365. This baseline assessment has a set of controls for key regulations and standards for data protection and general data governance. Compliance Manager becomes more helpful as you add your own assessments to meet your organization's particular needs.
8. Select **Data Protection Baseline**. Notice the information available on the progress tab. You can also view information on the Controls, your improvement actions, and Microsoft actions.

9. From the top-left of the page, above where it says Assessments (the breadcrumb), select **Assessments** to return to the assessments page. Before leaving the assessments tab, note that you can add your own assessments.
10. From the top of the page, select **Regulations**. This page lists the regulations available to your organization. You can also create assessments from the available templates. Select one of the premium templates from the list. You will see specific information about that regulation including controls, your improvement actions, and Microsoft action. From the top-right corner of the window, select the **ellipses** to see the option for **+ Create assessment**, that allows you to create an assessment based on the template. Return to the regulations page by select **Regulations** from the bread-crumbs at the top of the page.
11. From the top of the page, select **Alerts**. Here you can view and manage alerts for events that can affect your organization's compliance score. If there is an alert listed, select it to view the information about the associated alert policy.
12. From the left navigation panel, select **Home** to return to the landing page of the Microsoft Purview compliance portal.
13. Keep the browser tab open.

Review

In this lab, you explored the Microsoft Purview compliance portal home page and ways in which the capabilities of Compliance Manager can help organizations improve their compliance posture.

Lab: Explore sensitivity labels in Microsoft Purview

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft compliance
- Module: Describe information protection and data lifecycle management in Microsoft Purview
- Unit: Describe sensitivity labels

Lab scenario

In this lab, you'll explore the capabilities of sensitivity labels. You'll go through the settings for existing sensitivity labels that have been created and the corresponding policy to publish the label. Then you'll see how to apply a label and the impact of that label, from the perspective of a user.

Estimated Time: 20-25 minutes

Task 1

In this task, you'll gain an understanding of what sensitivity labels can do by going through the process of creating a new label and creating a policy to publish the label.

1. Open the browser tab for home page of Microsoft Purview. If you previously closed it, open a browser tab and enter <https://admin.microsoft.com>. Sign in with the admin credentials for the Microsoft 365 tenant provided by the authorized lab hoster (ALH). From the left navigation pane of the Microsoft 365 admin center, select **Show all** then select **Compliance**. A new browser page opens to the welcome page of the Microsoft Purview compliance portal.
2. In the left navigation panel, under solutions, expand **Information protection** then select **Overview**. Note the warning at the top of the page and scroll down to view the information available.
 - i. On the Overview page, you may see a yellow information box indicating that your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. Select **Turn on now**. Once you do this,

there can be a delay for the setting to propagate through the system and there are additional steps that must be completed to protect Teams, SharePoint sites, and Microsoft 365 Groups.

3. From the left navigation panel, select **Labels**.
 - i. On the Labels page, you may see a yellow information box indicating that your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. Select **Turn on now**. Once you do this, there can be a delay for the setting to propagate through the system and there are additional steps that must be completed to protect Teams, SharePoint sites, and Microsoft 365 Groups.
4. Some labels have been preconfigured in your Microsoft 365 lab tenant, for your convenience. Select the label named **Confidential-Finance**. A window opens that provides information about this label. Note the settings for this label. Select **Edit label** (it may also show as a pencil icon) at the top of the page to view some of the basic configuration settings. If you don't see this option, select the ellipsis.
 - i. Configuration starts with providing a name and description for your label. Don't change anything. Select **Next** at the bottom of the page.
 - ii. Review the scope for this label. Don't change anything. Select **Next** at the bottom of the page.
 - iii. This next screen is where you can choose protection settings for the labeled items. This label is configured to support content marking. Don't change anything. Select **Next** at the bottom of the page.
 - a. On the content markings page, take note of the information box on the top of the page. Don't change any settings. Select **Next** on the bottom of the page.
 - iv. You are now in the Auto-labeling for files and emails window. Read the description of auto-labeling on the top of the page and the information box below it. Also take note that this label is set for auto-labeling for specific conditions. Don't change any settings. Select **Next** on the bottom of the page.
 - v. This window defines protection settings for teams, groups, and sites that have this label applied. This is not enabled, select **Next** on the bottom of the page.
 - vi. This window is a preview feature to automatically apply this label to schematized data assets in Microsoft Purview Data Map (such as SQL,

Synapse, and more) that contain the sensitive info types you choose. This feature is not enabled. Select **Cancel** at the bottom of the page to exit the label configuration wizard and return to the Information Protection page.

5. From the left navigation panel, select **Label policies**. It is through label policies that sensitivity labels can be published. The Microsoft 365 tenant has been configured with some label policies, for your convenience.
6. Select **Confidential-Finance Policy**. A window opens that provides information about the policy. Select **Edit policy** from the top of the window. Here you will walk through the settings without changing anything.
 - i. Review the description for "Choose sensitivity labels to publish". Notice the label that is listed. Don't change any settings. Select **Next** on the bottom of the page.
 - ii. Review the description for "Assign admin units". The Admin units are set to the full directory, don't change any settings. Select **Next**.
 - iii. Review the description for "Publish to users and groups". Notice this label is available to all users. Don't change any settings. Select **Next** on the bottom of the page.
 - iv. Review the policy settings. Don't change any settings. Select **Next** on the bottom of the page.
 - v. Review the description for "Apply a default label to documents." Don't change any settings. Select **Next** on the bottom of the page.
 - vi. Review the description for "Apply a default label to emails" and "Inherit label from attachments". Don't change any settings. Select **Next** on the bottom of the page.
 - vii. Review the description for "Apply a default label to meetings and calendar events". Don't change any settings. Select **Next** on the bottom of the page.
 - viii. Review the description for "Apply a default label to Power BI content". Don't change any settings. Select **Next** on the bottom of the page.
 - ix. The last configuration option is to name your policy. Since you're editing the policy, the name field is greyed out. Select **Next** on the bottom of the page.
 - x. Review the policy settings. Select **Cancel** to discard any changes and return to the Label policies page.

7. From the left navigation panel, under Information protection, select Auto-labeling. Review the description. Note that you create auto-labeling policies to automatically apply sensitivity labels to email messages or OneDrive and SharePoint files that contain sensitive info. No auto-label policies have been preconfigured in our tenant. To create a new auto-label policy, select **Create auto-label policy**. Here you will walk through the steps to create a new policy.
 - i. You start by choosing the information you want this label applied to. Note the available options. Select **Medical and health** then select one of the available templates. Select **Next**.
 - ii. You can name your auto-label policy or use the default name. Select **Next**.
 - iii. You can assign the admin units to which this policy applies. Leave the default set to full directory and select **Next**.
 - iv. Note the available locations where you want to apply the label. Leave the defaults and select **Next**.
 - v. You can set up common or advanced rules that define what the content the label is applied to. Leave the default set to Common rules and select **Next**.
 - vi. You can define rules for content in all locations. The label will be applied to content that matches rules defined on this page. For the template you selected, you should see a line item. Expand it to view the conditions that apply. Leave all the default settings and select **Next**.
 - vii. Choose a label to auto-apply by selecting **Choose a label**. Choose a label then select **Add**. Select **Next**.
 - viii. Additional settings can be configured for email. Leave the defaults and select **Next**.
 - ix. You can decide to test the policy now or later. Select **Leave policy turned off** then select **Next**.
 - x. Review the settings and select **Create policy** then select **Done**.
8. From the left navigation panel, select **Home** to return to the Microsoft Purview compliance portal.
9. Keep this page open, you'll use it in the next task.

Task 2

In this task, you'll go through the process of applying a sensitivity label to a Microsoft Word document and then view the content marking (watermark) that is generated by

the label. NOTE: When using Microsoft Word online, you may experience a delay before the option to select Sensitivity labels appears on the top ribbon. It is recommended that you complete all remaining labs and then return back to this task.

1. From the Microsoft Purview compliance portal home page, select the **app launcher icon**, next to where it says Contoso Electronics. Select the **Word icon**.
2. Under Create new, select **Blank document**, then enter some text on the page. On the top of the page, select the down-arrow, next to where it says Document - Saved, and in the File Name box enter, **Test-label** then press **Enter** on your keyboard.
3. On the far right of top menu bar (also referred to as the ribbon) is a down arrow, select it, then select **Classic Ribbon**. This will make it easier to identify the sensitivity icon. Select **Sensitivity**, located next to the microphone icon. From the drop-down menu, select **Confidential-Finance**.
4. From the top menu bar, select **View**, then select **Reading view**.
5. Notice how the document includes the watermark-Confidential FINANCIAL DATA..
6. Close the Microsoft Word tabs that are open on your browser to exit from Word, but keep the the browser tab to the Microsoft Purview home page open.

Review

In this lab, you'll explore the capabilities of sensitivity labels. You'll go through the settings for existing sensitivity labels that have already been created and the corresponding policy to publish the label. Then you'll see how to apply a label.

Lab: Explore insider risk management in Microsoft Purview

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft compliance
- Module: Describe the insider risk capabilities in Microsoft Purview
- Unit: Describe insider risk management

Lab scenario

In this lab, you'll walk through the process of setting up an insider risk policy, along with the basic prerequisites to configure and use insider risk management policies. Note: this lab will only provide visibility into what is required for setting up Insider risk management and options associated with creating a policy. This lab does not include a task to trigger the policy, as the number of events that would need to occur to trigger a policy and the time required are outside of the scope of this exercise.

Estimated Time: 45-60 minutes

Task 1

In this task you, as the global administrator, will enable permissions for Insider Risk Management. Specifically, you'll add users to the Insider Risk Management role group to ensure that designated users can access and manage insider risk management features. It may take up to 30 minutes for the role group permissions to apply to users across the organization.

1. Open the browser tab for home page of Microsoft Purview. If you previously closed it, open a browser tab and enter <https://admin.microsoft.com>. Sign in with the admin credentials for the Microsoft 365 tenant provided by the authorized lab hoster (ALH). From the left navigation pane of the Microsoft 365 admin center, select **Show all** then select **Compliance**. A new browser page opens to the welcome page of the Microsoft Purview compliance portal.
2. From the left navigation panel, expand **Roles & scopes** then select **Permissions**.
3. Under Microsoft Purview solutions, select **Roles**.

4. In the search field type **Insider risk** then hit Enter on your keyboard. Notice the numerous roles that show up. Each of these has different access levels. Select **Insider risk management** and review the description. Scroll down to where it shows members and note that MOD Administrator and Megan Bowen are listed. Close the window by selectin the **X** on the top right of the window..
5. From the left navigation panel, select **Home** to return to the Microsoft Purview compliance portal page.
6. Keep this browser tab open, as you'll come back to it in a subsequent task.

Task 2 (NOTE: SKIP Task 2 if you did the setup lab task to enable the audit log.)

Insider risk management uses Microsoft 365 audit logs for user insights and activities identified in policies and analytics insights. In this task, you'll enable the Audit log search capability. Note: It may take several hours after you turn on audit log search before you can return results when you search the audit log. Although it can take several hours before you can search the audit log, it will not impact the ability to complete other tasks in this lab.

1. Select the browser tab labeled, **Home-Microsoft 365 compliance**. If you previously closed this browser tab, open Microsoft Edge, and in the address bar enter **compliance.microsoft.com** and sign in with your admin credentials.
2. In the left navigation panel, under solutions, select **Audit**.
3. Verify that the **New Search** tab is selected (underlined).
4. Once you land on the Audit page, wait 2-3 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start recording user and admin activity. Select **Start recording user and admin activity**. Once auditing is enabled, the blue bar disappears. If the blue bar is not present, then auditing is already enabled, and no further action is required.
5. Return to the home page of the Microsoft Purview compliance portal by selecting **Home** from the left navigation panel.
6. Keep this browser tab open, as you'll use it in the next task.

Task 3

In this task, you'll walk through the settings associated with the Insider Risk Management solution. Insider risk management settings apply to all insider risk management policies, regardless of the template you choose when creating a policy.

1. You should be on the Microsoft Purview compliance portal home page. If not, Open the browser tab **Home - Microsoft 365 compliance**.
2. From the left navigation panel under Solutions, select **Insider risk management**.
3. Before getting started with setting up a policy, there are some settings that an admin should be familiar with and configure to as needed for their organization. From the Insider Risk Management page, select the **setting cog icon** on the top-right corner of the Insider risk management window to access Insider Risk settings.
 - i. Verify you are in the **Privacy** tab: for users who perform activities matching your insider risk policies, this setting will determine whether to show their actual names or use anonymized versions to mask their identities. For the purpose of this walk-through, you can leave the default setting.
 - ii. Select the **Policy indicators** tab. Once a policy triggering event occurs, activities that map to the selected indicators are used in determining the risk score, for the user. Policy indicators selected here are included the Insider risk policy templates. Scroll to view all the indicators available and any associated information. Under **Office indicators**, select **Select all**, then select **Save** at the bottom of the page (you'll need to scroll down).
 - iii. Select the **Policy timeframes** tab. The timeframes you choose here go into effect for a user when they trigger a match for an insider risk policy. The Activation window determines how long policies will actively detect activity for users and is triggered when a user performs the first activity matching a policy. Past activity detection Determines how far back a policy should go to detect user activity and is triggered when a user performs the first activity matching a policy. Leave the default values.
 - iv. Select the **Intelligent detections** tab. Review the options here. Note the domains settings and how they relate to the indicators.
 - v. Explore other items listed in the settings and note that many are in preview.
4. To return to the Insider risk management overview, select **Insider risk management** from the top-left corner of the page, above where it says Settings.

5. Keep this browser tab open, as you'll use it in the next task.

Task 4

In this task, you'll walk through the settings for creating a policy. The objective is simply to get a sense of the various options and flexibility associated with creating a policy.

1. You should be on the Insider risk management page. If not already there, open the browser tab labeled, **Insider risk management - Microsoft 365 compliance**.
2. From the Insider risk management overview page, select the **Policies** tab then select **+ Create policy**. Configure each of the following policy tabs.
 - i. Policy template: Under the Data leaks category, select **Data leaks**. Read the details associated with this template. Under prerequisites, DLP policy is shown with a checkmark in a green circle to indicate that the prerequisite is satisfied. There's a DLP policy that was preconfigured for this lab tenant. Select **Next**.
 - ii. Name and description: enter a name, **SC900-InsiderRiskPolicy**, then select **Next**.
 - iii. Users and groups: Review the information box. Leave the default setting, **Include all users and groups**. Select **Next**.
 - iv. Content to prioritize: Per the description, Risk scores are increased for any activity that contains priority content, which in turn increases the chance of generating a high severity alert. For simplicity, select **I don't want to prioritize content right now**, then select **Next**.
 - v. Triggers: The triggering event determines when a policy will begin to assign risk scores to a user's activity. You can choose from an existing DLP policy or if the user performs an exfiltration activity. Select **User matches a data loss prevention (DLP) policy** then from the drop-down select **U.S. Financial Data**. Select **Next**.
 - vi. Indicators: Note that all the office indicators you selected in the previous task are selected (you can see this by selecting the down arrow key next to Office indicators), then select **Next**.
 - vii. On the Detection options page, leave all the default settings, but read the description associated with the various options and hover over the information icon to get more detailed information on a specific setting. Select **Next**.

- viii. On the page to Decide whether to use default or customer indicator thresholds, leave the default setting **Apply thresholds provided by Microsoft**, then select **Next**.
 - ix. Finish: review the settings, select **Submit**.
 - x. Review the description of what happens next then select **Done**.
3. You're back on the Policies tab of the Insider risk management page. The policy you created will be listed. If you don't see it, select the **Refresh** icon.
 4. As an admin, you can immediately start assigning risk scores to users based on activity detected by the policies you selected. This bypasses the requirement that a triggering event (like a DLP policy match) is detected first. An admin would do this by selecting the empty square next to the policy name to select the policy, then select **Start scoring activity for users**, which is shown above the policy table. A new window opens that requires the admin to populate the available fields. Leave the fields empty as you won't configure this option, but for more information on why an admin would want to do this, select **Why would I do this??**. Exit the window by selecting the **X** on the top right of the window.
 5. From the left navigation panel, select **Home** to return to the landing page of the Microsoft Purview compliance portal.
 6. Keep the browser tab open.

Review

In this lab, you walked through the process of setting up an insider risk policy, along with the basic prerequisites to configure and use insider risk management policies.

Lab: Explore the eDiscovery (Standard) workflow

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft compliance
- Module: Describe the eDiscovery and audit capabilities of Microsoft Purview
- Unit: Describe the eDiscovery solutions in Microsoft Purview

Lab scenario

In this lab you'll go through the steps required for setting up eDiscovery, including setting up role permissions, creating an eDiscovery case, creating an eDiscovery hold and creating a search query. Note: Licensing for eDiscovery (Standard) requires the appropriate organization subscription and per-user licensing. If you aren't sure which licenses support eDiscovery (Standard), visit [Get started with eDiscovery \(Standard\) in Microsoft Purview](#).

Estimated Time: 25-30 minutes

Task 1

To access eDiscovery (Standard) or be added as a member of an eDiscovery case, a user must be assigned the appropriate permissions. In this task, you as the global admin, will add specific users as members of the eDiscovery Manager role group.

1. Open the browser tab for home page of Microsoft Purview. If you previously closed it, open a browser tab and enter <https://admin.microsoft.com>. Sign in with the admin credentials for the Microsoft 365 tenant provided by the authorized lab hoster (ALH). From the left navigation pane of the Microsoft 365 admin center, select **Show all** then select **Compliance**. A new browser page opens to the welcome page of the Microsoft Purview compliance portal.
2. From the left navigation pane, expand (select the down arrow) **Roles & Scopes** then select **Permissions**.
3. Under Microsoft Purview solutions, select **Roles**.

4. In the search field, enter **eDiscovery** then hit Enter on your keyboard. Select **eDiscovery Manager**.
5. Select **Edit**. Notice how there are two subgroups, eDiscovery Manager and eDiscovery Administrator.
 - i. The "Manage eDiscovery Manager" page allows you to add users to the role of eDiscovery manager. For this lab, we'll add members to the eDiscovery Administrator subgroup so select **Next**.
 - ii. On the "Manage eDiscovery Administrator" page, select **Choose users** . Search for and select **MOD Administrator** and **Megan Bowen** then press **Select** at the bottom of the page, then select **Next** and then **Save**.
 - iii. On the "You successfully updated the role group" page, select **Done**.
6. Keep this browser tab open, as you'll use it in the next task.

Task 2

In this task you, as an eDiscovery Administrator (MOD admin is an eDiscovery administrator), will create a case to start using eDiscovery (Standard).

1. You should still be on the compliance portal roles page. If you closed the browser tab from the previous task, open a new browser tab and enter **compliance.microsoft.com**
2. From the left navigation panel, under Solutions, expand **eDiscovery** then select **Standard**.
3. From the top of the eDiscovery (Standard) page, select + **Create a case**.
4. In the New case window, enter a Case name, **SC900 Test Case** then select the **Save** at the bottom of the page.
5. The case should now appear on the list.
6. As the creator of the case and because you have eDiscovery Administrator privileges, you can begin to work with it.
7. Keep this browser tab open, as you'll use it in the subsequent task.

Task 3

Now that you've created an eDiscovery (Standard) case, you can begin to work with the case. In this task, you'll create an eDiscovery hold for the case for you created. Specifically, you'll create a hold for the exchange mailbox belonging to Adele Vance.

1. Open the eDiscovery (Standard) tab on your browser.
2. From the eDiscovery (Standard) page, select the case you created in the previous tab, **SC900 Test Case**.
3. From the Home page of the case, select the **Hold** tab then select **+Create**.
4. In the name field, enter **Test hold** then select **Next**.
5. In the Choose locations page, select toggle switch next to **Exchange mailboxes** to set the status to **On**.
6. Now select **Choose users, groups, or teams**. In the search box, enter **Adele** then press enter on your keyboard. From the search results select **Adele Vance**, then select **Done**.
7. From the Choose locations page, select **Next**. For expediency with the lab, no other locations will be included in this hold.
8. The Query conditions page enables you to create a hold, based on specific Keywords or Conditions that are satisfied, select **+ Add condition** to view the available options. Select **Next**. Without any conditions, the hold will preserve all content in the specified location.
9. Review your settings and select **Submit**, it may take a minute, then select **Done**. The Test hold should appear on the list. If you don't immediately see it, select **Refresh**
10. Keep this browser tab open, as you'll use it in the subsequent task.

Task 4

With a hold in place, you'll create a search query. Once your search is complete, the eDiscovery supports actions, such as exporting and downloading the results for future investigation. Note: Searches associated with an eDiscovery (Standard) case are not listed on the Content search page in the Microsoft Purview compliance portal. These searches are listed only on the Searches page of the associated eDiscovery (Standard) case.

1. Open the SC900 Test Case tab on your browser.
2. From the SC900 Test Case page, select **Searches**.
3. From the Search page, select + **New Search**.
4. In the Name field, enter **Test Hold – Sales Search**, then select **Next** from the bottom of the page.
5. In the Choose locations page, select **locations on hold** and unselect **Add App Content for On-Premises users**, as your lab environment has no on-premises users, then select **Next**.
6. The Query conditions page enables you to create a search, based on specific Keywords or Conditions that are satisfied, In the keyword field enter **Sales** select **Next**.
7. Review your settings and select **Submit**, it may take a minute, then select **Done**. The search should appear on the list. If you don't immediately see it, select **Refresh**
8. From the Searches window, select the search you created, **Test Hold - Sales Search**. A window that opens with the Summary tab selected. Once the search is complete the status will indicate that the search is completed. You'll see a Search statistics tab (if you don't see the Search statistics tab, the search may still be running and may take a few minutes to complete). Select the **Search statistics** tab and select the drop-down next to Search content. You can also view more information for the Condition report and Top locations.
9. From the bottom of the page, select **Actions**. Note the available options that include export options (the export options cannot be selected from within the lab platform provided by the authorized lab hoster, but are available in a production environment and are considered part of the standard workflow). Select **Close**.
10. Sign out and close all open browser windows.

Review

In this lab, you went through the steps required to get started with eDiscovery (Standard), including setting up the role permissions for eDiscovery and creating an eDiscovery case. With the case, created you went through elements of the eDiscovery (Standard) workflow by creating an eDiscovery hold and creating a search query.

