



**Microsoft**

**Exam Questions MS-500**

Microsoft 365 Security Administrator

### NEW QUESTION 1

- (Exam Topic 1)

You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

- A. Synchronization Service Manager
- B. Azure AD Connect wizard
- C. Synchronization Rules Editor
- D. IdFix

**Answer: B**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization>

### NEW QUESTION 2

- (Exam Topic 1)

An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.

Exchange Administrator - Members

+ Add member

X Remove member

✓

-

Access reviews

↓

Export

↺

Refresh

Assignment type

All

▼

Search

🔍

Search by members name

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

- A. Change the Assignment Type for Admin2 to Permanent
- B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
- C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
- D. Change the Assignment Type for Admin1 to Eligible

**Answer: D**

### NEW QUESTION 3

- (Exam Topic 2)

How should you configure Azure AD Connect? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

User sign-in settings:

▼

Password Synchronization with single-sign on

Pass-through authentication with single sign-on

Federation with Active Director Federation Services (AD FS)

Device options:

▼

Hybrid Azure AD Join

Enable Device writeback

Disable Device writeback

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

User sign-in settings:

	▼
Password Synchronization with single-sign on	
Pass-through authentication with single sign-on	
Federation with Active Director Federation Services (AD FS)	

Device options:

	▼
Hybrid Azure AD Join	
Enable Device writeback	
Disable Device writeback	

#### NEW QUESTION 4

- (Exam Topic 2)

You need to create Group2.

What are two possible ways to create the group?

- A. an Office 365 group in the Microsoft 365 admin center
- B. a mail-enabled security group in the Microsoft 365 admin center
- C. a security group in the Microsoft 365 admin center
- D. a distribution list in the Microsoft 365 admin center
- E. a security group in the Azure AD admin center

**Answer:** CE

#### NEW QUESTION 5

- (Exam Topic 3)

Which policies apply to which devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

NEW QUESTION 6

- (Exam Topic 3)

You are evaluating which devices are compliant in Intune.

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input type="radio"/>
Device6 is compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device2 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device5 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device6 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 7

- (Exam Topic 3)

You need to meet the technical requirements for User9. What should you do?

- A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
- B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
- C. Assign the Security administrator role to User9
- D. Assign the Global administrator role to User9

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access>

NEW QUESTION 8

- (Exam Topic 3)

Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ADGroup1:	<table><tbody><tr><td>None</td><td><input checked="" type="checkbox"/></td></tr><tr><td>User1 and User2 only</td><td><input type="checkbox"/></td></tr><tr><td>User2 and User4 only</td><td><input type="checkbox"/></td></tr><tr><td>User3 and User4 only</td><td><input type="checkbox"/></td></tr><tr><td>User1, User2, User3, and User4</td><td><input type="checkbox"/></td></tr></tbody></table>	None	<input checked="" type="checkbox"/>	User1 and User2 only	<input type="checkbox"/>	User2 and User4 only	<input type="checkbox"/>	User3 and User4 only	<input type="checkbox"/>	User1, User2, User3, and User4	<input type="checkbox"/>
None	<input checked="" type="checkbox"/>										
User1 and User2 only	<input type="checkbox"/>										
User2 and User4 only	<input type="checkbox"/>										
User3 and User4 only	<input type="checkbox"/>										
User1, User2, User3, and User4	<input type="checkbox"/>										
ADGroup2:	<table><tbody><tr><td>None</td><td><input checked="" type="checkbox"/></td></tr><tr><td>User1 and User2 only</td><td><input type="checkbox"/></td></tr><tr><td>User2 and User4 only</td><td><input type="checkbox"/></td></tr><tr><td>User3 and User4 only</td><td><input type="checkbox"/></td></tr><tr><td>User1, User2, User3, and User4</td><td><input type="checkbox"/></td></tr></tbody></table>	None	<input checked="" type="checkbox"/>	User1 and User2 only	<input type="checkbox"/>	User2 and User4 only	<input type="checkbox"/>	User3 and User4 only	<input type="checkbox"/>	User1, User2, User3, and User4	<input type="checkbox"/>
None	<input checked="" type="checkbox"/>										
User1 and User2 only	<input type="checkbox"/>										
User2 and User4 only	<input type="checkbox"/>										
User3 and User4 only	<input type="checkbox"/>										
User1, User2, User3, and User4	<input type="checkbox"/>										

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#suppor>

NEW QUESTION 9

- (Exam Topic 3)

You are evaluating which finance department users will be prompted for Azure MFA credentials. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

YES, YES, NO.

Named locations can't have a private IP range, look at

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

"User IP address The IP address that is used in policy evaluation is the public IP address of the user. For devices on a private network, this IP address is not the client IP of the user's device on the intranet, it is the address used by the network to connect to the public internet."

NEW QUESTION 10

- (Exam Topic 4)

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

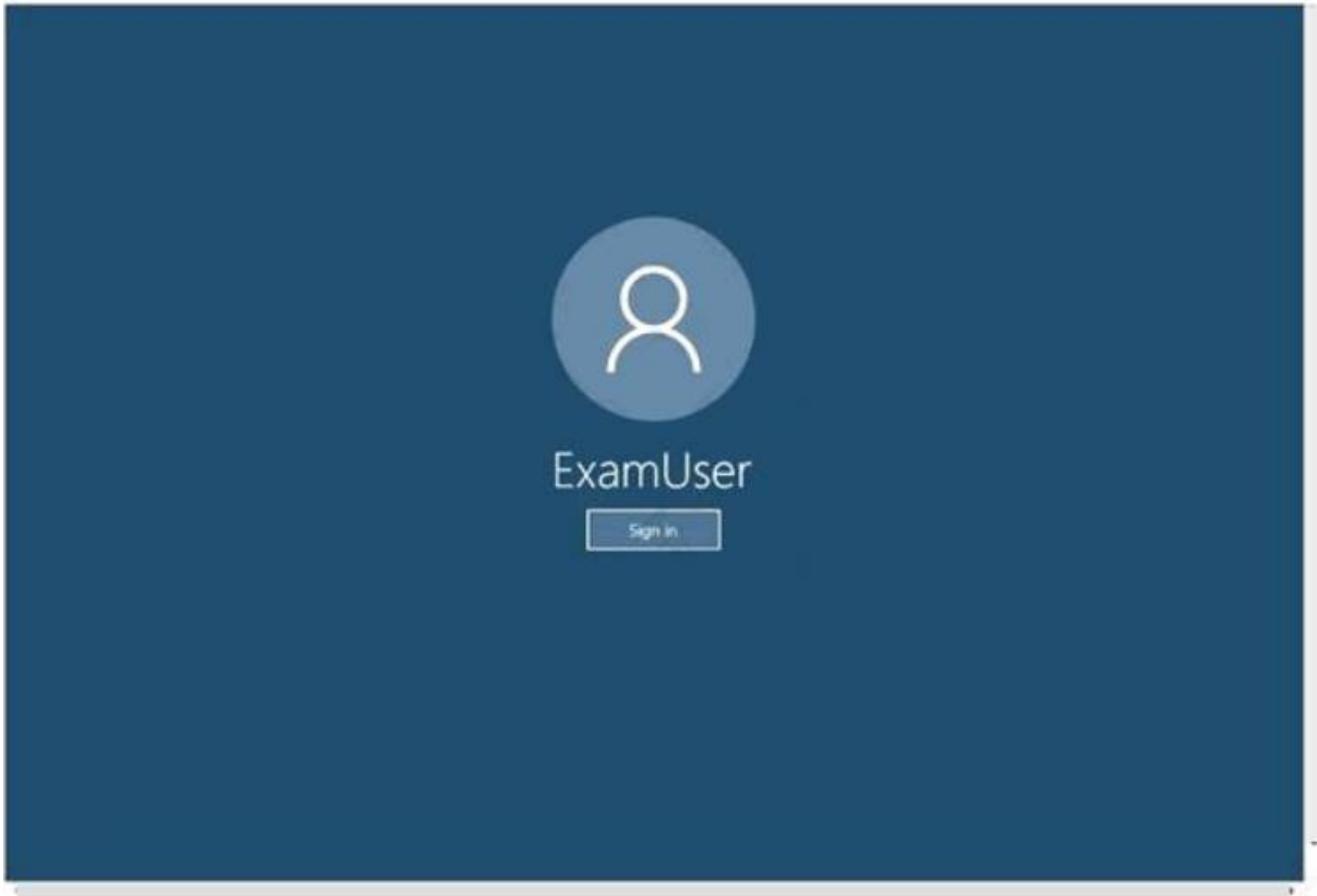
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:



To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username: admin@LODSe244001@onmicrosoft.com Microsoft 365 Password: &=Q8v@2qGzYz

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support only: Lab instance: 11032396

You need to ensure that email messages in Exchange Online and documents in SharePoint Online are retained for eight years.

To complete this task, sign in to the Microsoft Office 365 admin center.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

NB: For our purposes, the retention period will be 8 years. For retaining email messages in Exchange Online:

Step 1: Create a retention tag

- \* 1. Navigate to the Exchange Admin Center
- \* 2. Navigate to Compliance management > Retention tags, and then click Add +
- \* 3. Select one of the following options:

➤ Applied automatically to entire mailbox (default): Select this option to create a default policy tag (DPT).

You can use DPTs to create a default deletion policy and a default archive policy, which applies to all items in the mailbox.

➤ Applied automatically to a specific folder: Select this option to create a retention policy tag (RPT) for a default folder such as Inbox or Deleted Items.

➤ Applied by users to items and folders (Personal): Select this option to create personal tags. These tags allow Outlook and Outlook on the web (formerly known as Outlook Web App) users to apply archive or deletion settings to a message or folders that are different from the settings applied to the parent folder or the entire mailbox.

- \* 4. The New retention tag page title and options will vary depending on the type of tag you selected. Complete the following fields:

➤ Name: Enter a name for the retention tag. The tag name is for display purposes and doesn't have any impact on the folder or item a tag is applied to. Consider that the personal tags you provision for users are available in Outlook and Outlook on the web.

➤ Apply this tag to the following default folder: This option is available only if you selected Applied automatically to a specific folder.

➤ Retention action: Select one of the following actions to be taken after the item reaches its retention

period:

➤ Delete and Allow Recovery: Select this action to delete items but allow users to recover them using the Recover Deleted Items option in Outlook or Outlook on the web. Items are retained until the deleted item retention period configured for the mailbox database or the mailbox user is reached.

➤ Permanently Delete: Select this option to permanently delete the item from the mailbox database.

➤ Move to Archive: This action is available only if you're creating a DPT or a personal tag. Select this action to move items to the user's In-Place Archive.

➤ Retention period: Select one of the following options:

➤ Never: Select this option to specify that items should never be deleted or moved to the archive.

➤ When the item reaches the following age (in days): Select this option and specify the number of days to retain items before they're moved or deleted. The retention age for all supported items except Calendar and Tasks is calculated from the date an item is received or created. Retention age for Calendar and Tasks items is calculated from the end date.

➤ Comment: User this optional field to enter any administrative notes or comments. The field isn't displayed to users.

Step 2: Create a retention policy

- \* 1. Navigate to Compliance management > Retention policies, and then click Add +
- \* 2. In New Retention Policy, complete the following fields:

➤ Name: Enter a name for the retention policy.

➤ Retention tags: Click Add + to select the tags you want to add to this retention policy. A retention policy can contain the following tags:

➤ One DPT with the Move to Archive action.

➤ One DPT with the Delete and Allow Recovery or Permanently Delete actions.

➤ One RPT per default folder such as Inbox to delete items.

➤ Any number of personal tags.

Step 3: Apply a retention policy to mailbox users

After you create a retention policy, you must apply it to mailbox users. You can apply different retention policies to different set of users.

➤ Navigate to Recipients > Mailboxes.

➤ In the list view, use the Shift or Ctrl keys to select multiple mailboxes.

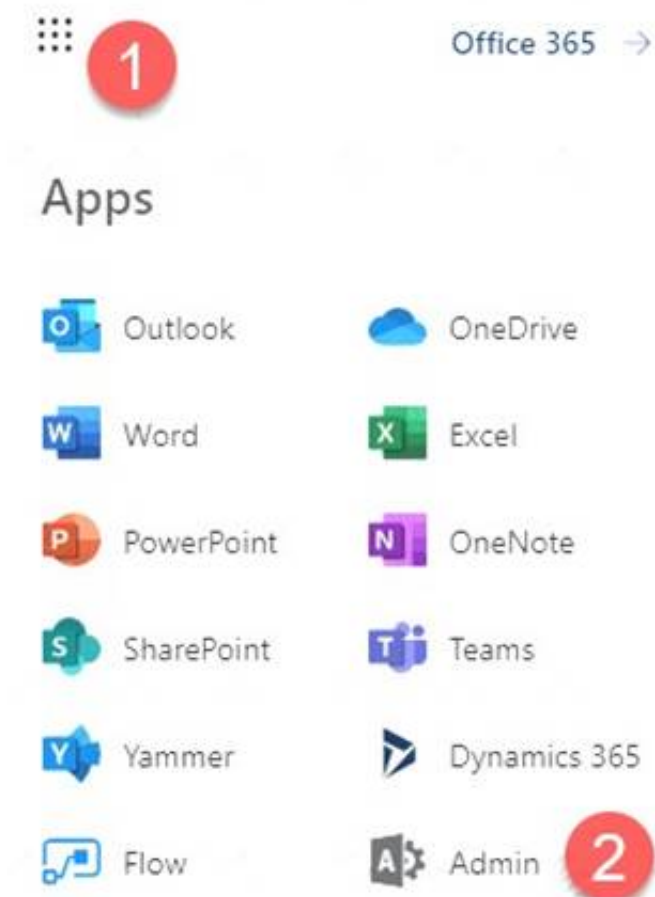
➤ In the details pane, click More options.

➤ Under Retention Policy, click Update.

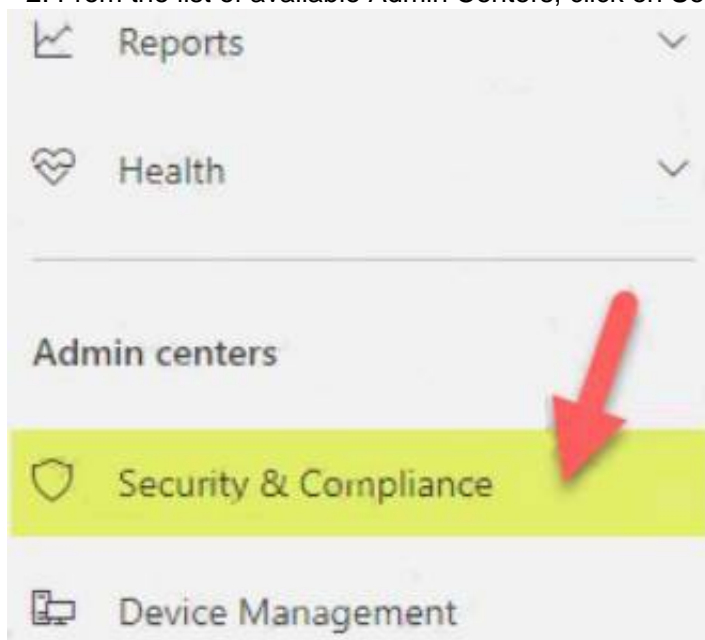
➤ In Bulk Assign Retention Policy, select the retention policy you want to apply to the mailboxes, and then click Save.

For retaining documents in SharePoint Online Access Security & Compliance Admin Center

- \* 1. Navigate to the Office 365 Admin Centers

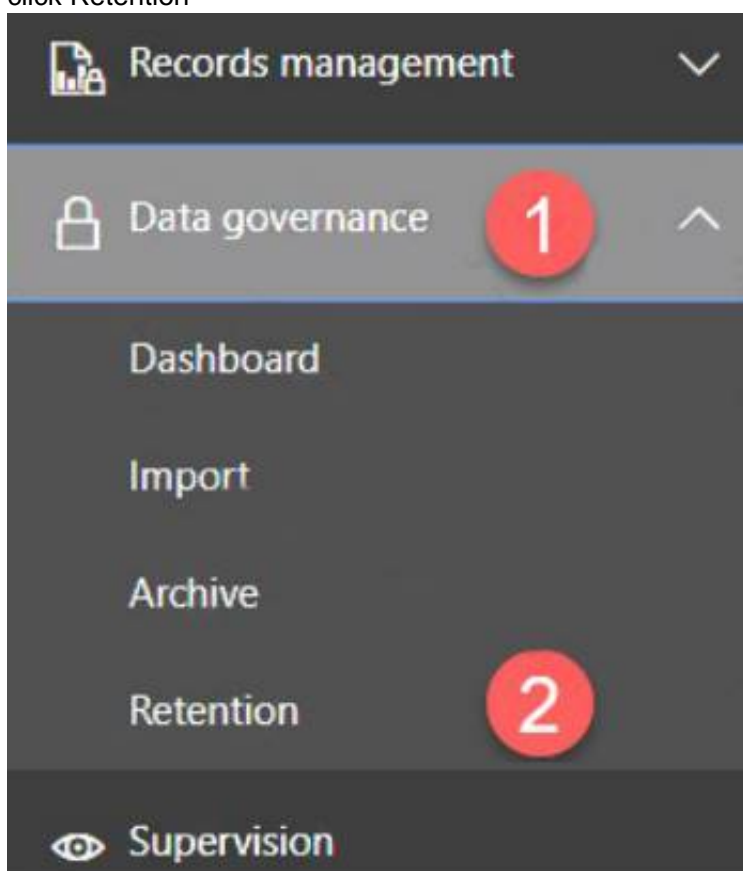


\* 2. From the list of available Admin Centers, click on Security & Compliance



How to create and publish a Retention Policy on a SharePoint site

Now that we are in the Security & Compliance Admin Center, we are ready to create and publish a Retention Policy on a SharePoint site. Under Data Governance, click Retention



\* 1. Hit Create button to create new Retention Policy

Home > Retention

Email, documents, Skype and Teams conversations. Your users generate a lot of content every day. Take control of it by setting up retention policies to get rid of what you don't. [Learn more about retention](#)

### Labels

Create labels to let users manually classify and retain their own content (email, docs, folders, and more). You can also auto-apply labels to specific content.

### Label policies

Create label policies to publish or automatically apply existing labels to your users apps (Outlook, SharePoint, OneDrive, and more).

+ Create

Refresh

Search

...

Name	Created by	Last modified
3-day retention	Gregory Zelfond	September 9, 2019

\* 2. Give your policy a name and description. Hit Next

Create a policy to retain what you want and get rid of what you don't.

Name your policy

Settings

Choose locations

Review your settings

## Name your policy

Name \*

Retain for 2 days, then delete

Description

This policy retains documents for 2 days after they were last modified and then deletes them

Next

Cancel

\* 3. On the next screen is where you set up the logic. You can configure how many days, months, or years to retain the content for, specify whether you want the math (retention period) to be calculated from the Created Date or Last Modified Date. Lastly, you can also specify whether you want to keep or delete content after the Retention period expires. Hit Next



Create a policy to retain what you want and get rid of what you don't.

**Name your policy**

Settings

Choose locations

Review your settings

## Decide if you want to retain content, delete it, or both

Do you want to retain content?

☒ Yes, I want to retain it

For this long... 2 days

Retain the content based on when it was last modified

Do you want us to delete it after this time?

☒ Yes ☐ No

At this time, creating a policy to delete Teams content that's less than 30 days old is not supported. If you want this policy to apply to Teams content, specify a retention period that's equal to or more than 30 days.

☐ No, just delete content that's older than

1 years

Need more options?

☐ Use advanced retention settings

Back Next Cancel

\* 4. On the next screen, you get to choose where to apply the policy. You can apply it to email (Exchange), SharePoint sites, OneDrive accounts as well as Office 365 Groups.

Create a policy to retain what you want and get rid of what you don't.

**Name your policy**

Settings

Choose locations

Review your settings

## Choose locations

The policy will apply to content that's stored in the locations you choose.

☐ Apply policy only to content in Exchange email, public folders, Office 365 groups, OneDrive and SharePoint documents

☒ Let me choose specific locations.

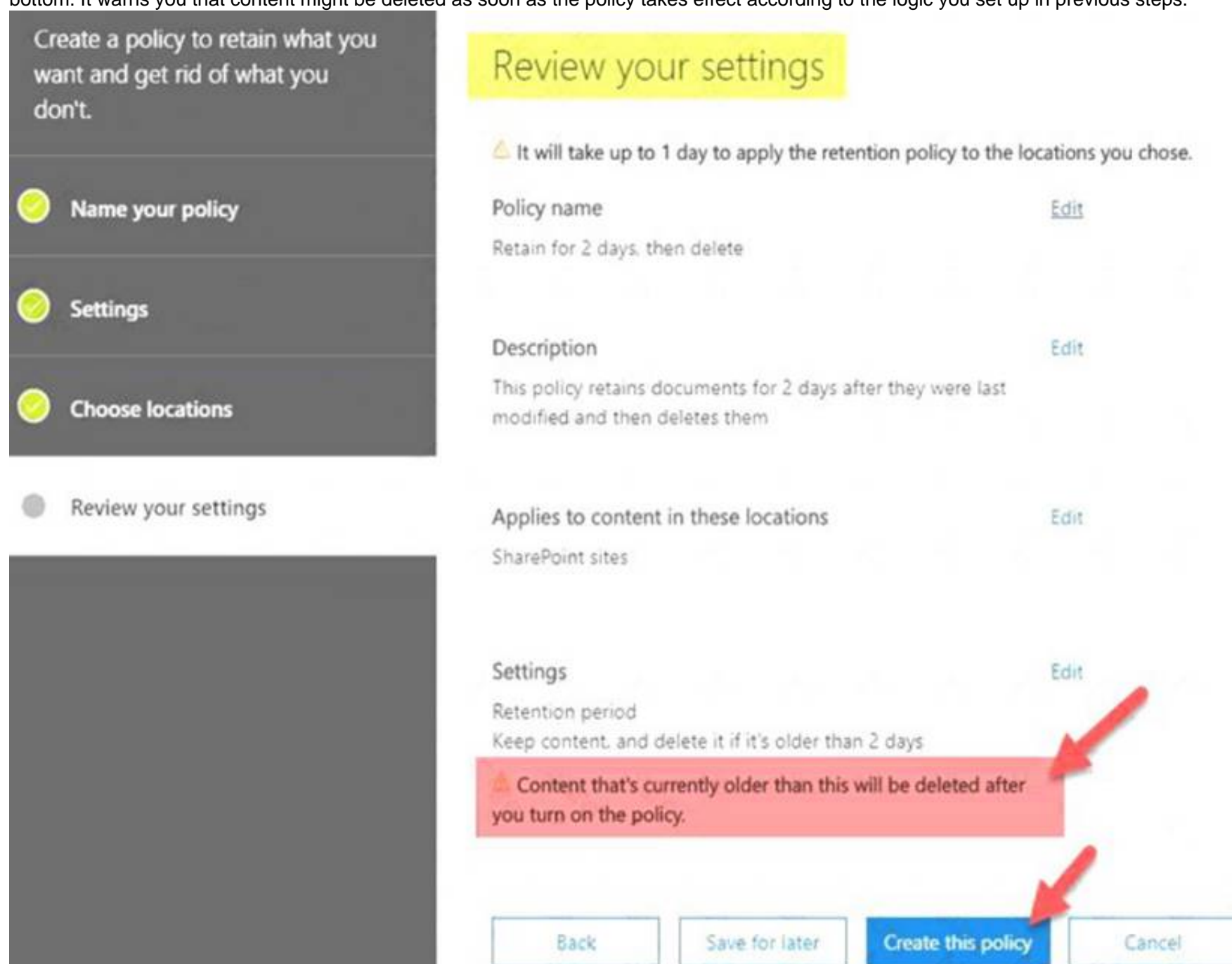
Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	Exchange email	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	SharePoint sites	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	OneDrive accounts	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Office 365 groups	All Choose groups	None Exclude groups

\* 5. In my case, I applied a policy to a single Office 365 Group Site

## Edit locations



\* 6. On a final screen, you need to review and confirm the settings and click Create this policy button. It is imperative to note the message you get to see at the bottom. It warns you that content might be deleted as soon as the policy takes effect according to the logic you set up in previous steps.



References:

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-re>  
<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-rete>  
<https://sharepointmaven.com/how-to-set-a-retention-policy-on-a-sharepoint-site/>

### NEW QUESTION 10

- (Exam Topic 4)

You have a hybrid Microsoft 365 environment.

All computers run Windows 10 Enterprise and have Microsoft Office 365 ProPlus installed. All the computers are joined to Active Directory.

You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft. What should you do?

- A. On Server1, run readinessreportcreator.exe
- B. Configure a registry on Server1
- C. Configure a registry on the computers

D. On the computers, run tdadm.exe

Answer: C

Explanation:

"To allow yourself and other administrators to identify the owners of Office files that have compatibility issues without revealing file names or specific locations, you can enable file obfuscation, which disguises Office file names, titles, and file paths. This setting is configured on the agent, which performs the obfuscation task before uploading data to the shared folder. The data that is stored on the local computer is not obfuscated."  
<https://docs.microsoft.com/en-us/deployoffice/compat/manage-the-privacy-of-data-monitored-by-telemetry-in-o>

NEW QUESTION 12

- (Exam Topic 4)

You have a Microsoft Defender for Endpoint deployment that has custom network indicators turned on. Microsoft Defender for Endpoint protects two computers that run Windows 10 as shown in the following table.

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender foe Endpoint has the device groups shown in the following table.

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp

Answer Area

Statements

YesNo

From a web browser on Computer1, you can open <http://www.contoso.com>.

From a web browser on Computer1, you can open <http://www.litwareinc.com/public>.

From a web browser on Computer2, you can open <http://www.litwareinc.com>.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

YesNo

From a web browser on Computer1, you can open <http://www.contoso.com>.

From a web browser on Computer1, you can open <http://www.litwareinc.com/public>.

From a web browser on Computer2, you can open <http://www.litwareinc.com>.

NEW QUESTION 17

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled. The security logs of the servers are collected by using a third-party SIEM solution. You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors. You need to ensure that you can detect when sensitive groups are modified and when malicious services are created. What should you do?

- A. Configure Event Forwarding on the domain controllers
- B. Configure auditing in the Office 365 Security & Compliance center.
- C. Turn on Delayed updates for the Azure ATP sensors.
- D. Enable the Audit account management Group Policy setting for the servers.

Answer: A

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding>

NEW QUESTION 20

- (Exam Topic 4)

Your on-premises network contains an Active Directory domain that syncs to Azure Active Directory (Azure AD) by using Azure AD Connect. The functional level of

the domain. You need to deploy Windows Hello for Business. The solution must meet the following requirements:

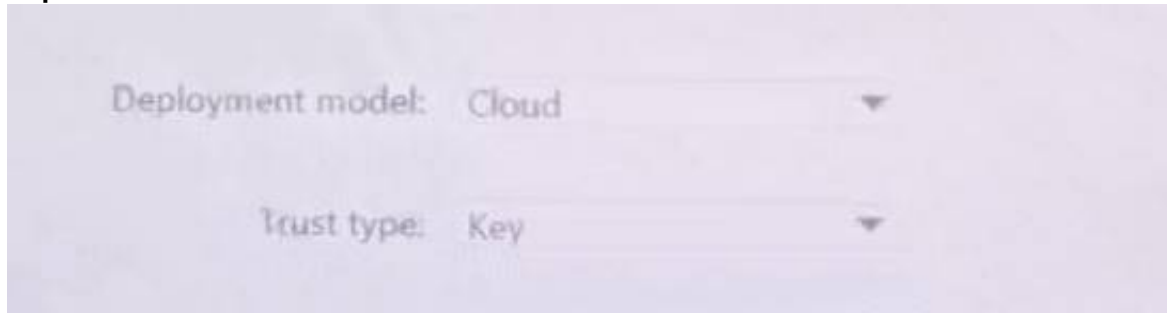
- Ensure that users can access Microsoft 365 services and on-premises resources.
- Minimize administrative efforts

How should you deploy Windows Hello for Business, and which type of trust should you use? To answer, select the appropriate options in the answer area.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 21

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that has Microsoft 365 Defender enabled.

You plan to deploy a third-party app named App1 that will receive alert data from Microsoft 365 Defender. Which format will Microsoft 365 Defender use to send the alert data to App1?

- A. JSON
- B. ZIP
- C. XML
- D. CSV

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts?view=o365-worldwide>

#### NEW QUESTION 26

- (Exam Topic 4)

Your company has a main office and a Microsoft 365 subscription.

You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.

What should you include in the configuration?

- A. a user risk policy
- B. a sign-in risk policy
- C. a named location in Azure Active Directory (Azure AD)
- D. an Azure MFA Server

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

#### NEW QUESTION 28

- (Exam Topic 4)

You have an Azure Sentinel workspace that has an Office 365 connector.

You are threat hunting events that have suspicious traffic from specific IP addresses. You need to save the events and the relevant query results for future reference.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



## Actions

Select the query result.

From the workspace, run an Azure Log Analytics query.

Add the query to favorites.

From Azure Monitor, run an Azure Log Analytics query.

Add a bookmark.

## Answer Area

- A. Mastered  
 B. Not Mastered

**Answer:** A

### Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/bookmarks>

## NEW QUESTION 31

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.

The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.

What should you do?

- A. Configure auditing in the Office 365 Security & Compliance center.  
 B. Turn off Delayed updates for the Azure ATP sensors.  
 C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.  
 D. Integrate SIEM and Azure ATP.

**Answer:** C

### Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>

## NEW QUESTION 36

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User 4.

Solution: You enable SSPR for Group3.

Does this meet the goal?

- A. Yes  
 B. No

**Answer:** B

### Explanation:

By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and Cloud application administrators. Therefore, we must enable SSPR for User3 by applying it to Group2 and not Group3 as User4 is in Group3. User4 would thus be affected if we enable it on Group3.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-p>



NEW QUESTION 37

- (Exam Topic 4)

You need to ensure that a user named Grady Archie can monitor the service health of your Microsoft 365 tenant. The solution must use the principle of least privilege.

To complete this task, sign in to the Microsoft 365 portal.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You need to assign the Service Administrator role to Grady Archie.

- In the Microsoft 365 Admin Center, type Grady Archie into the Search for users, groups, settings or tasks search box.
- Select the Grady Archie user account from the search results.
- In the Roles section of the user account properties, click the Edit link.
- Select the Customized Administrator option. This will display a list of admin roles.
- Select the Service admin role.
- Click Save to save the changes. Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/view-service-health>

NEW QUESTION 39

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

You implement Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

From PIM, you review the Application Administrator role and discover the users shown in the following table.

Name	Assignment type
UserA	Permanent
UserB	Eligible
UserC	Eligible

The Application Administrator role is configured to use the following settings in PIM:

- Maximum activation duration: 1 hour
- Notifications: Disable
- Incident/Request ticket: Disable
- Multi-Factor Authentication: Disable
- Require approval: Enable
- Selected approver: No results

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	<input checked="" type="radio"/>	<input type="radio"/>
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 41

- (Exam Topic 4)

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

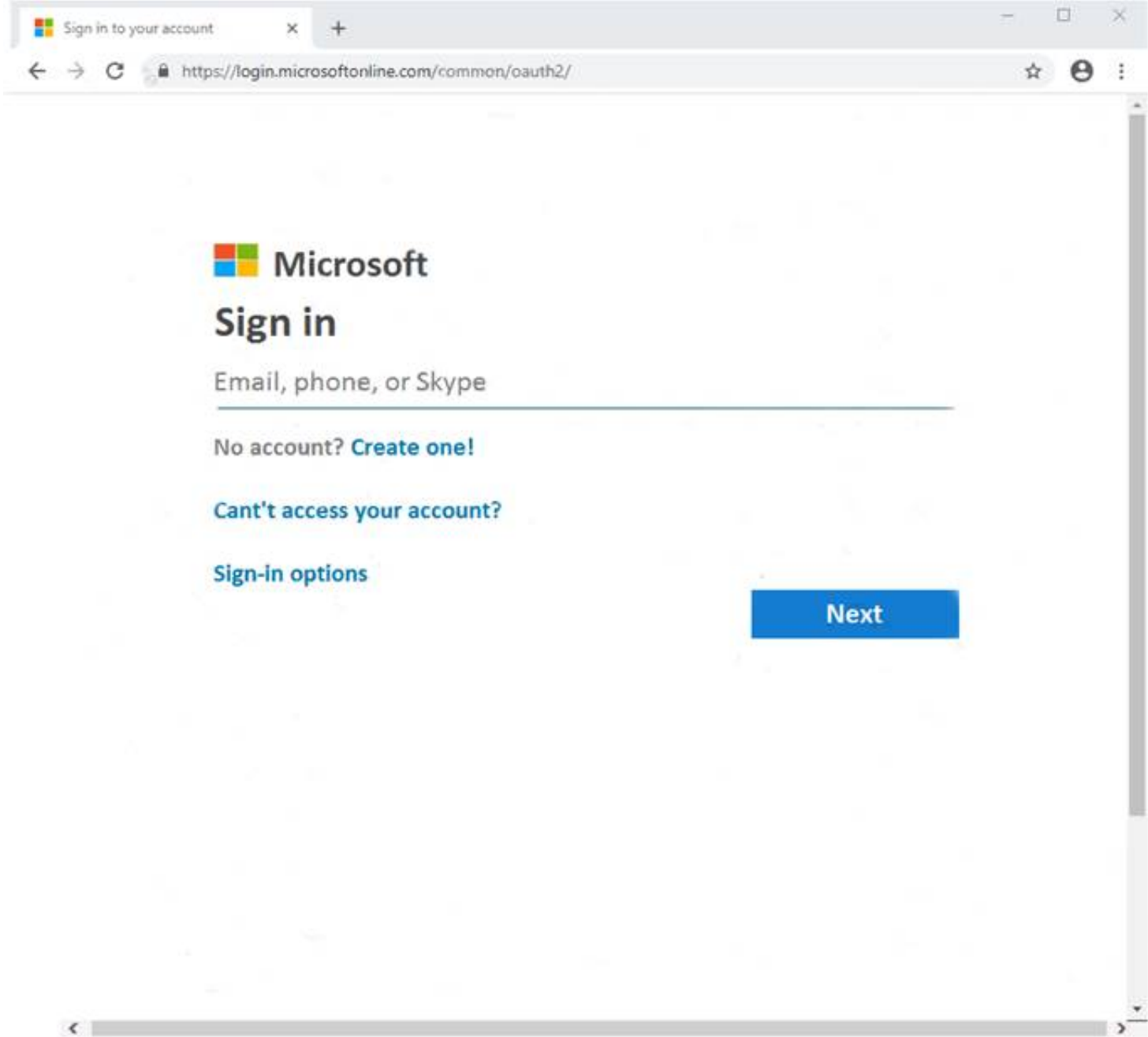
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



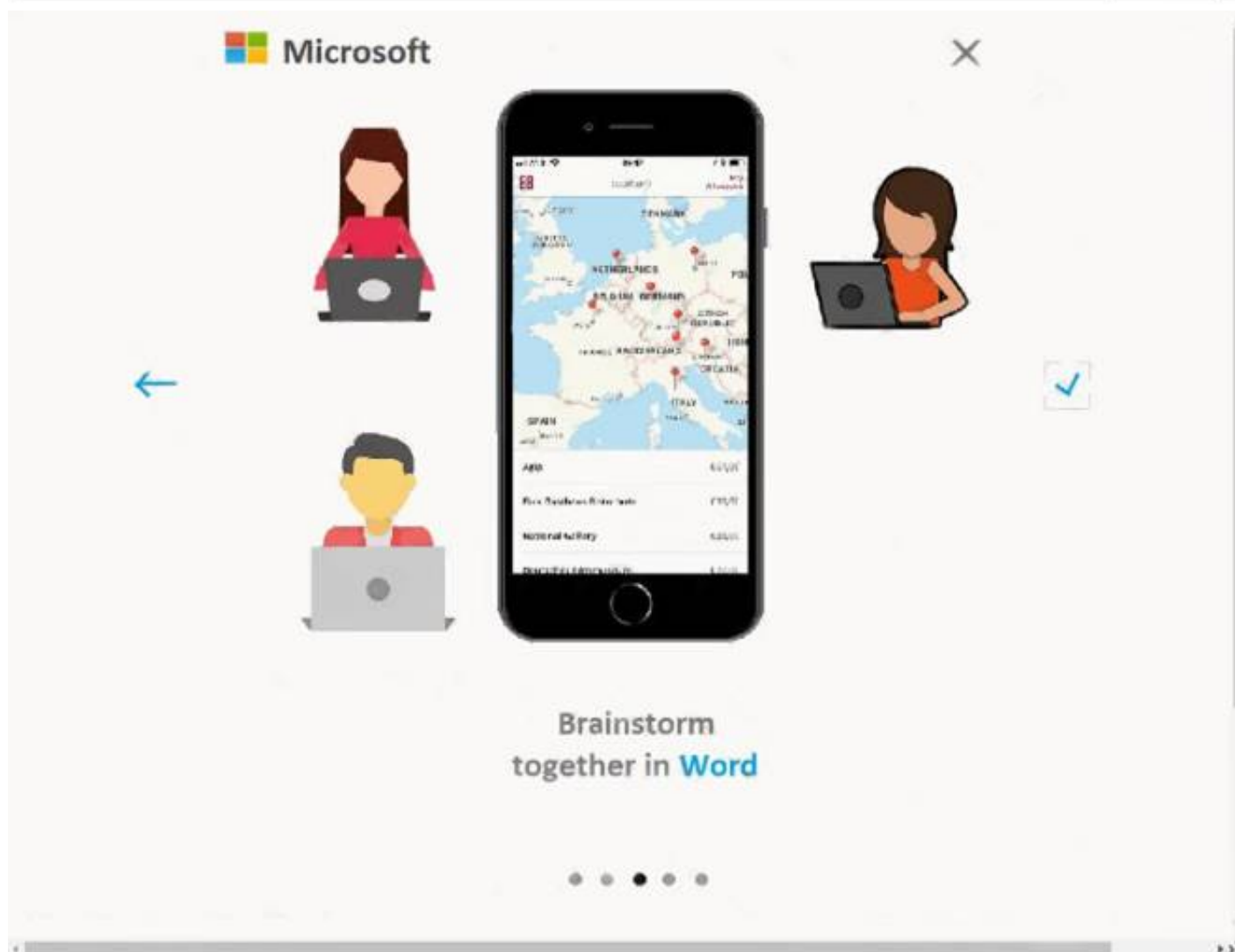
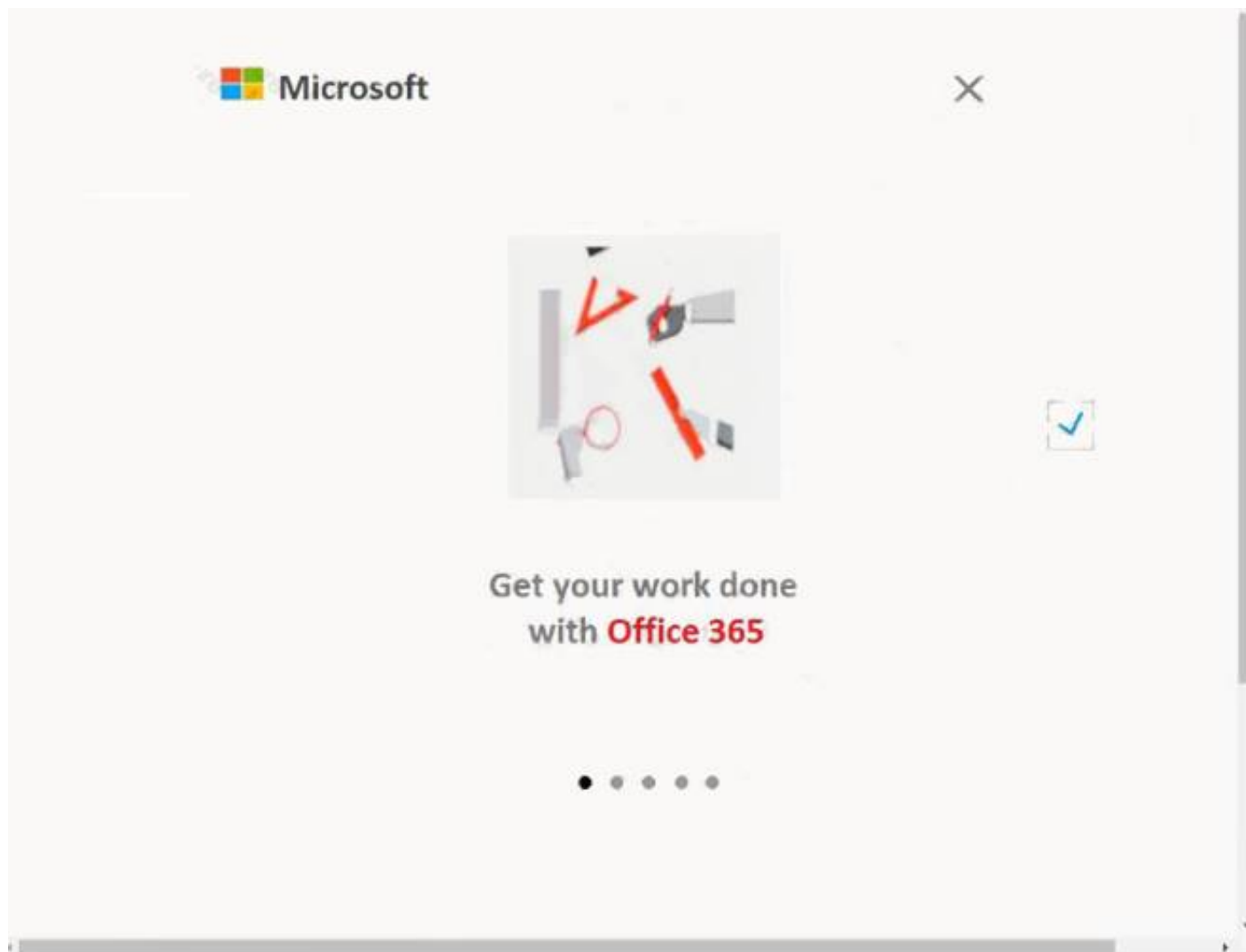
Use the following login credentials as needed:

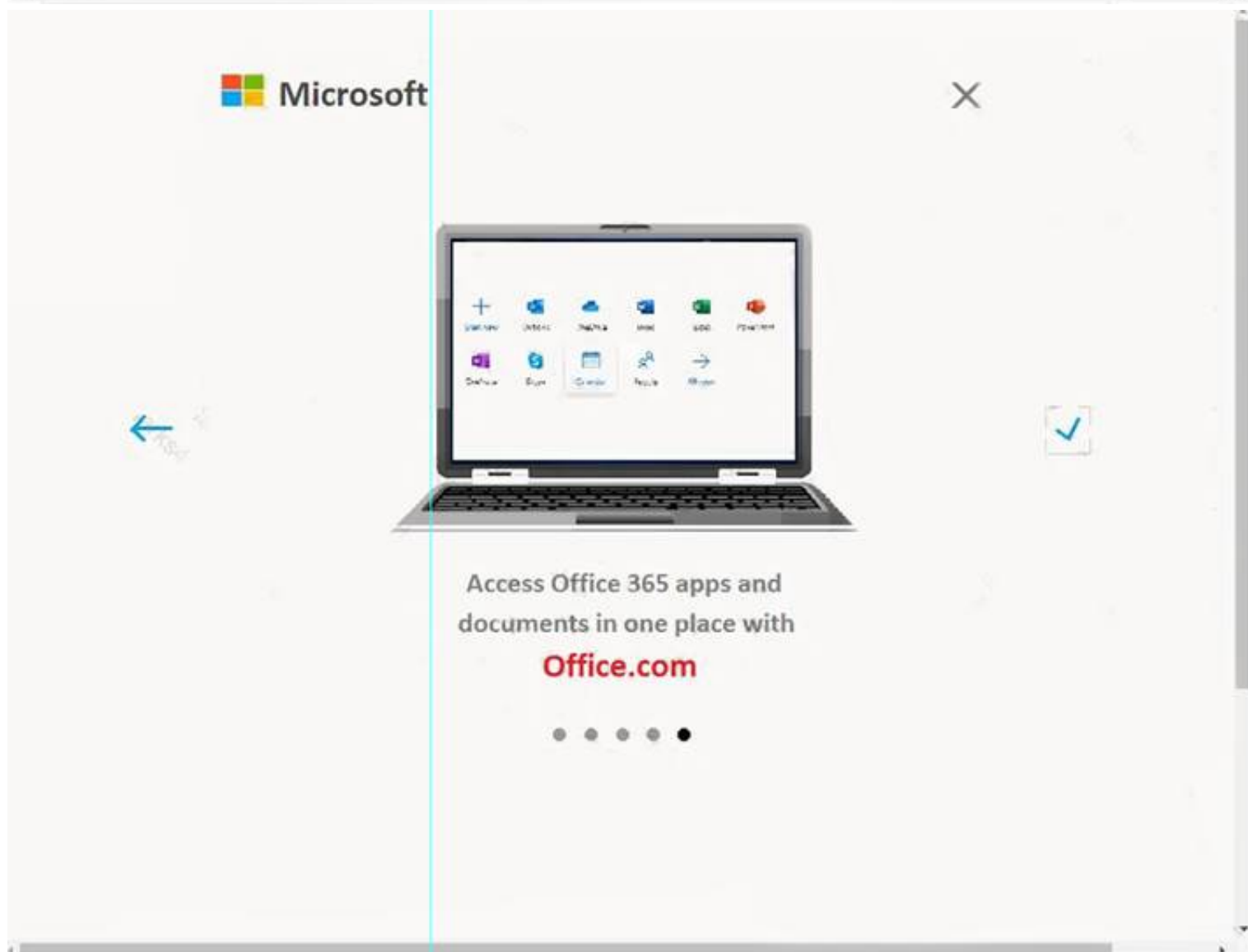
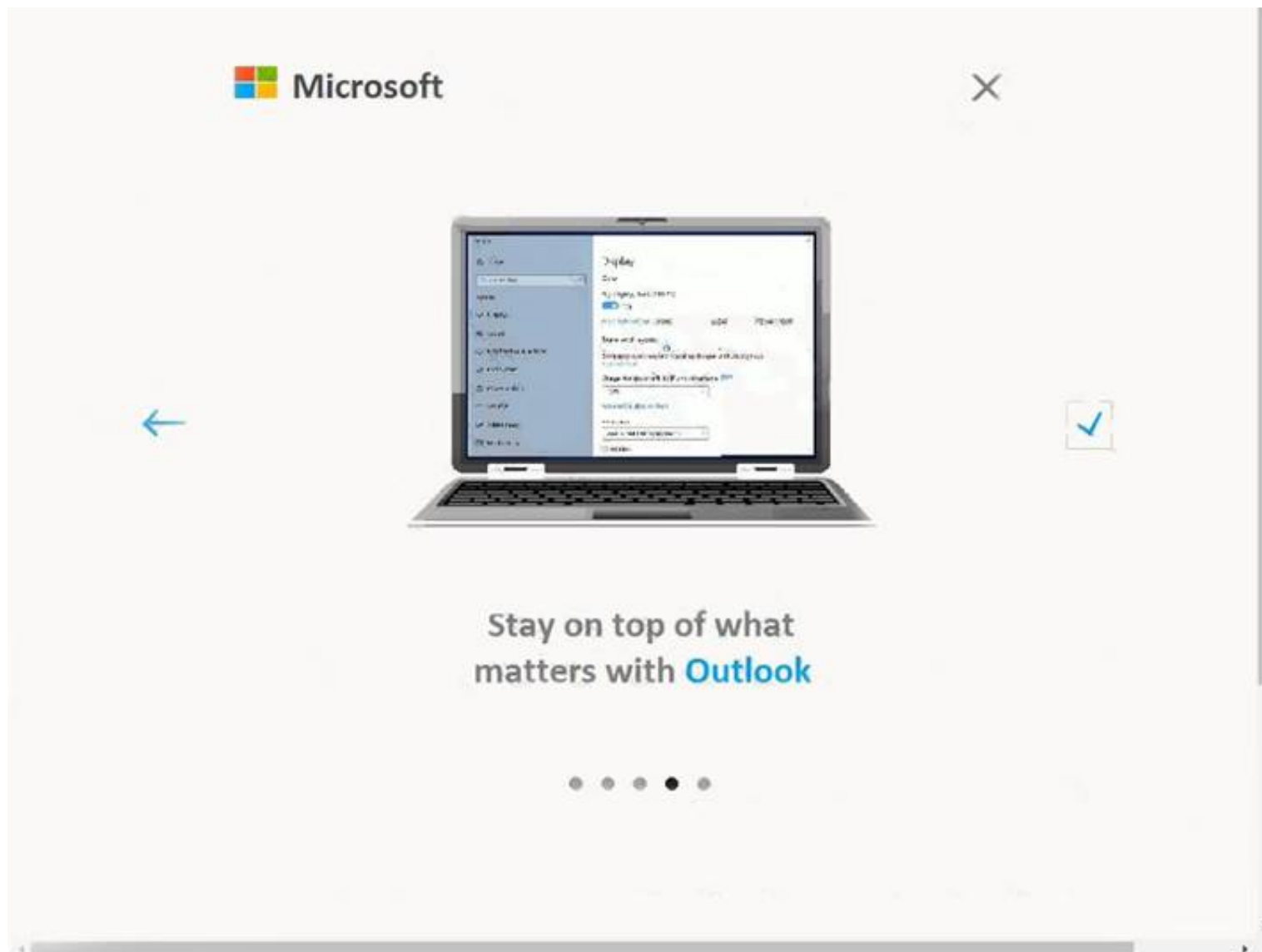
To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username: admin@LODSe00019@onmicrosoft.com Microsoft 365 Password: #HSP.ug?\$p6un

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support only: Lab instance: 11122308







Microsoft Office Home

office.com/tauthui2

Contoso electronics Office 365

Good morning

Install Office

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

**Excel**

Sales Results Overview  
lodse000198.sharepoint.co...

You edited this Jan 15

**Excel**

Sales Process  
lodse000198.sharepoint.co...

You edited this Jan 15

**Word**

Org Chart  
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

## Recommended

You edited this Jan 15

**Excel**

P and L Summary  
lodse000198.sharepoint.co...

You edited this Jan 15

**Word**

Contoso Electronics Outdoor...  
lodse000198.sharepoint.co...

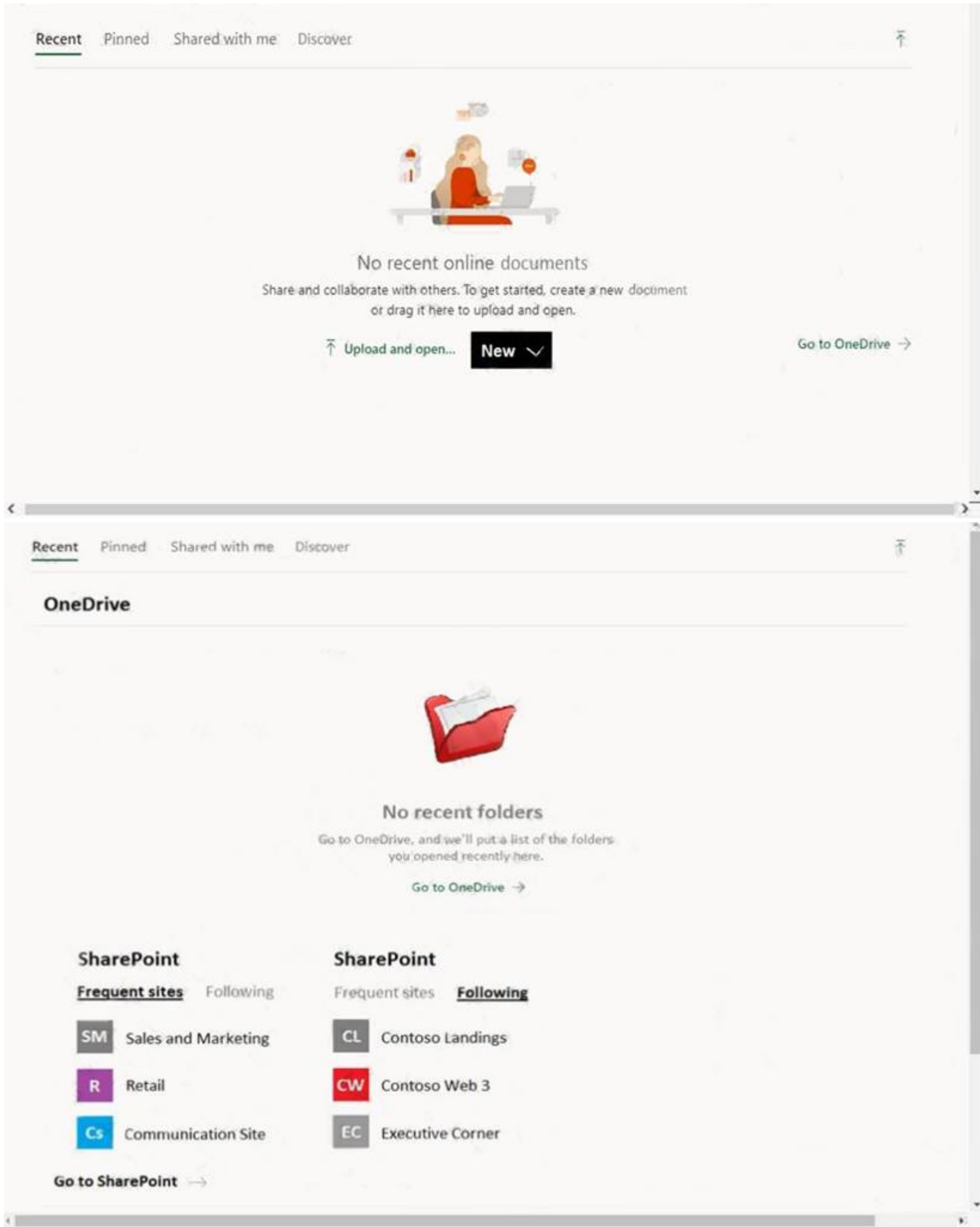
You edited this Jan 15

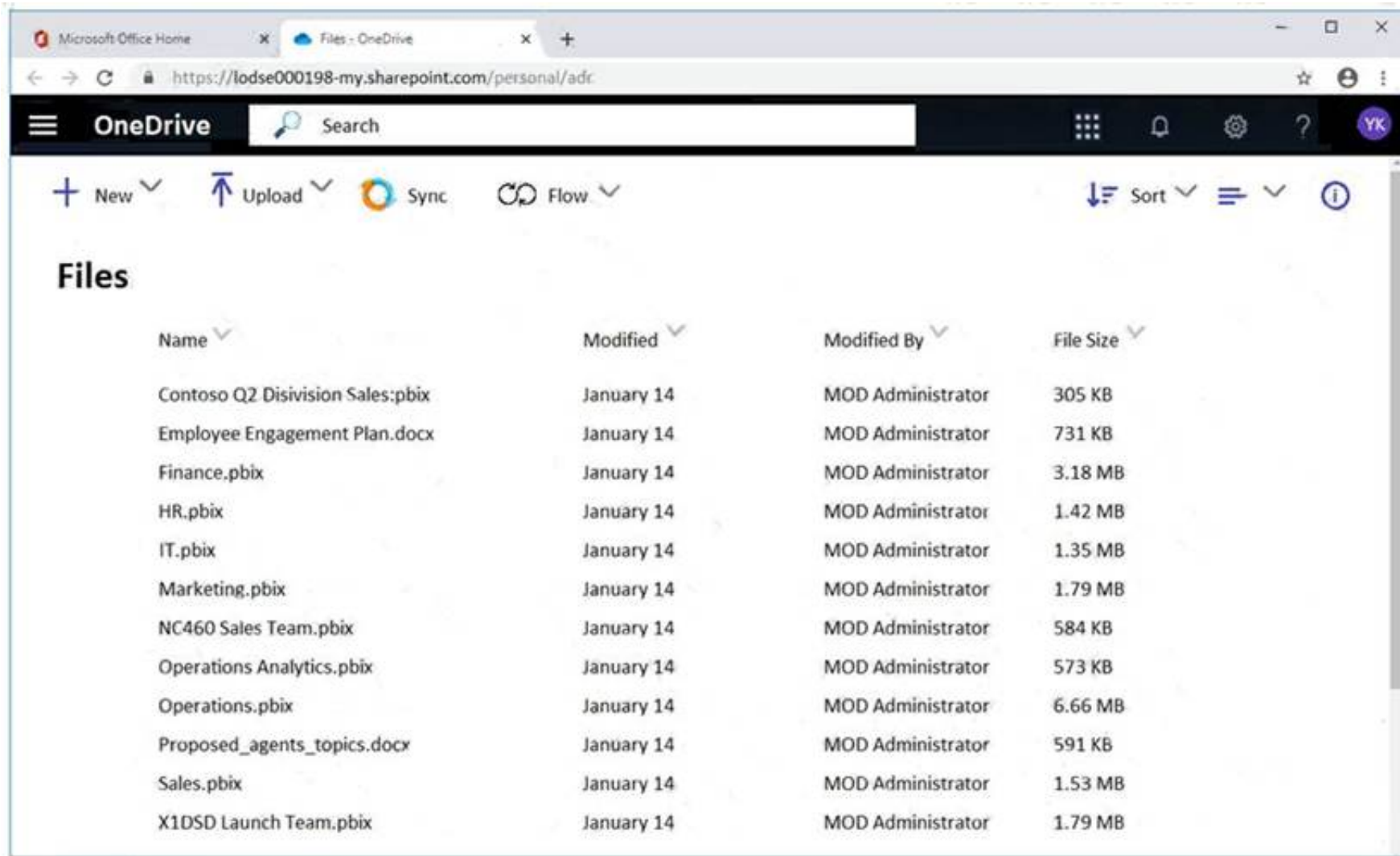
**Word**

AD Slogans  
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover







Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

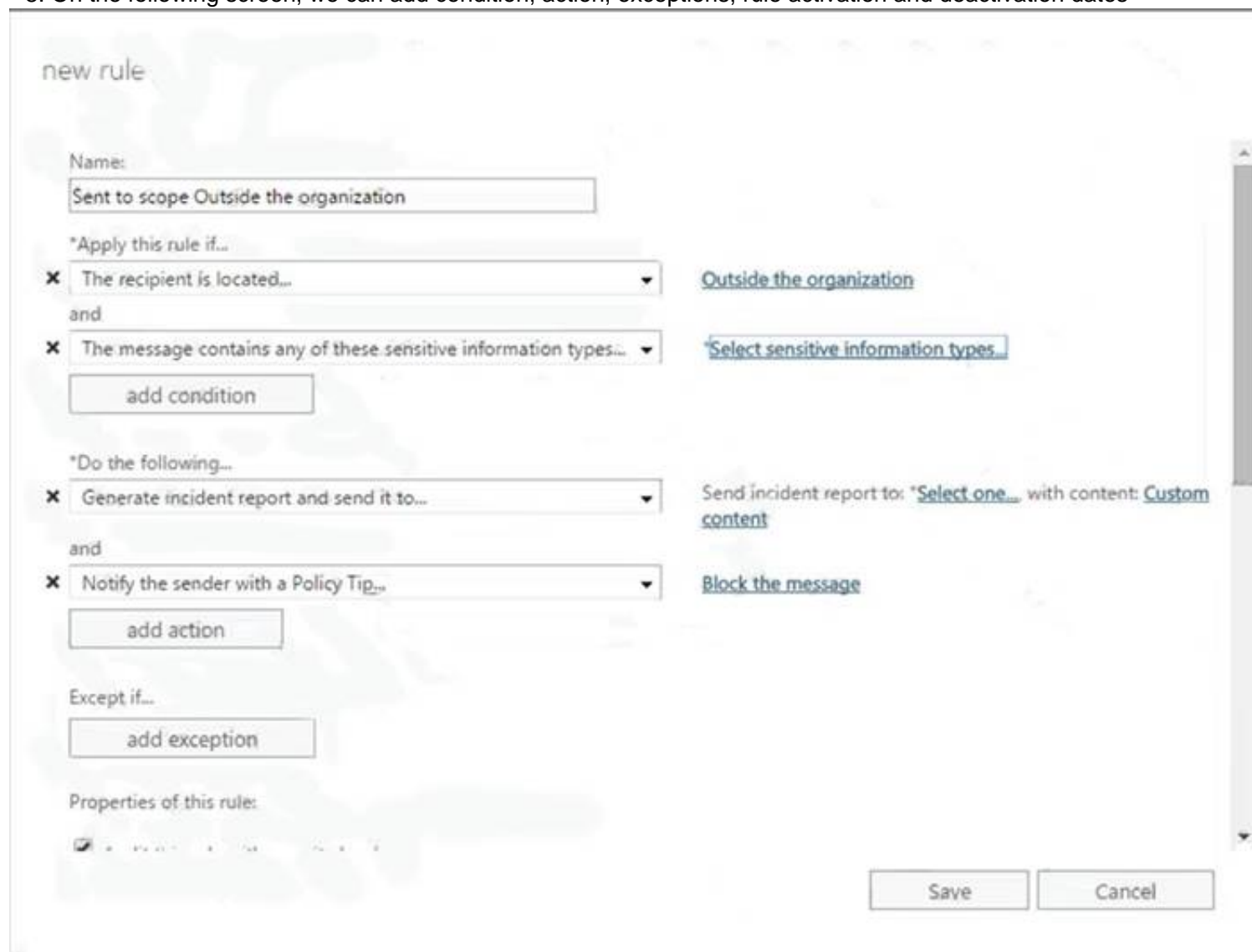
You need to prevent any email messages that contain data covered by the U.K. Data Protection Act from being sent to recipients outside of your organization, unless the messages are sent to an external domain named adatum.com.  
 To complete this task, sign in to the Microsoft 365 admin center.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

- \* 1. After signing into the Microsoft 365 admin center, navigate to Compliance Management in the Exchange Admin center.
- \* 2. Click on "Data Loss Prevention" option.
- \* 3. To add a new custom DLP policy, Click on (+) plus button to get the context menu
- \* 4. Click on "New Custom DLP policy" option, a new window appears where you have to enter policy name, description, state and mode of the requirement details. Click on save button to create policy and continue...
- \* 5. You will be back to the "Data Loss Prevention" screen with newly added policy information.
- \* 6. Double click on the added row to open the policy details, click on rules option in left part of the screen as depicted
- \* 7. Click on (+) plus button to add a new rule. Select the "Block messages with sensitive information" rule.
- \* 8. On the following screen, we can add condition, action, exceptions, rule activation and deactivation dates



**new rule**

Name:

\*Apply this rule if...

☒ The recipient is located...

and

☒ The message contains any of these sensitive information types...

\*Do the following...

☒ Generate incident report and send it to...

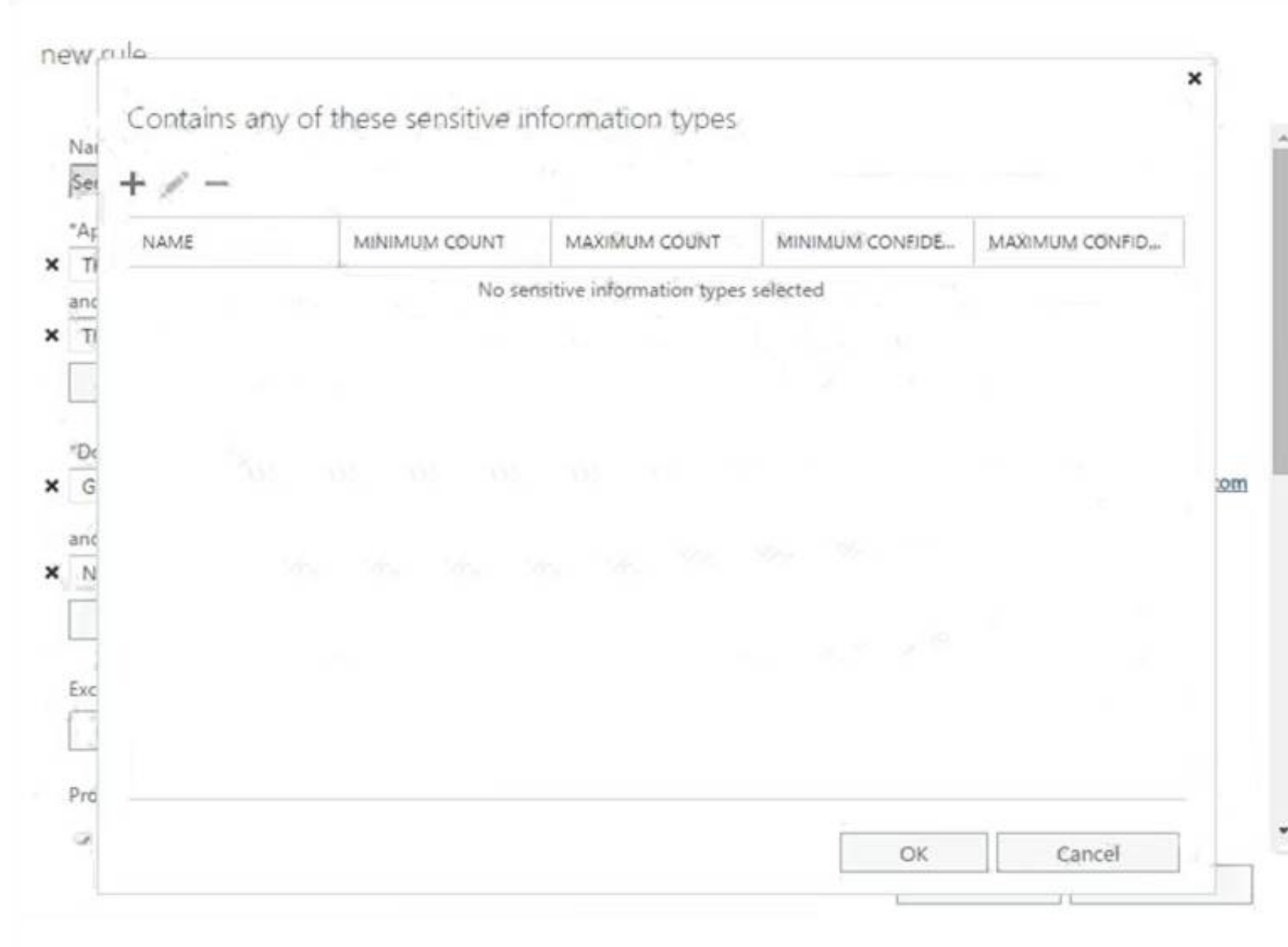
and

☒ Notify the sender with a Policy Tip...

Except if...

Properties of this rule:

\* 9. Click on "Select Sensitive information Types" to specify the sensitive information details.



\* 10. Click on (+) plus button and add the following Sensitive information Types:

- > U.K. National Insurance Number (NINO)
- > U.S. / U.K. Passport Number
- > SWIFT Code

\* 11. Click on Ok

\* 12. Add an exception for recipients in the adatum.com domain

\* 13. Add recipients for incident reports and click ok

\* 14. Click save

\* 15. Click save

Reference:

<https://events.collab365.community/configure-data-loss-prevention-policies-in-exchange-online-in-office-365/>

#### NEW QUESTION 44

- (Exam Topic 4)

You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1. You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1. What should you do first?

- A. From the Azure Active Directory admin center, assign a role group to Admin1.
- B. From the Microsoft 365 admin center, assign a role to Admin1.
- C. From Security & Compliance admin center, assign a role group to Admin1.

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

#### NEW QUESTION 46

- (Exam Topic 4)

You need to ensure that administrators can publish a label that adds a footer to email messages and documents. To complete this task, sign in to the Microsoft Office 365 portal.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

You need to configure a Sensitivity label.

- > Go to the Security & Compliance Admin Center.
- > Navigate to Classification > Sensitivity labels.
- > Click on + Create a label to create a new label.

- Give the label a name and description then click Next.
- Leave the Encryption option as None and click Next.
- On the Content Marking page, tick the checkbox Add a footer.
- Click the Customize Text link and add the footer text and click Save (for the question, it doesn't matter what text you add).
- Click Next.
- Leave the Auto-labeling for Office apps off and click Next.
- Click the Submit button to save your changes.
- The label is now ready to be published. Click the Done button to exit the page and create the label.

#### NEW QUESTION 51

- (Exam Topic 4)

You have a Microsoft 365 subscription.

A user reports that changes were made to several files in Microsoft OneDrive.

You need to identify which files were modified by which users in the user's OneDrive. What should you do?

- A. From the Azure Active Directory admin center, open the audit log
- B. From the OneDrive admin center, select Device access
- C. From Security & Compliance, perform an eDiscovery search
- D. From Microsoft Cloud App Security, open the activity log

**Answer:** D

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/activity-filters>

#### NEW QUESTION 52

- (Exam Topic 4)

Your company has a Microsoft 365 subscription.

The company does not permit users to enroll personal devices in mobile device management (MOM). Users in the sales department have personal iOS devices. You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant. The users must be prevented from backing up the app's data to iCloud.

What should you create?

- A. a device compliance policy in Microsoft Endpoint Manager
- B. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
- C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
- D. an app protection policy in Microsoft Endpoint Manager

**Answer:** D

#### NEW QUESTION 53

- (Exam Topic 4)

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the roles shown in the following table:

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP contains the machine groups shown in the following table:

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 56

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

You configure the Security Operator role in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.

### Edit role setting - Security Operator

Privileged Identity Management | Azure AD roles

**Activation** Assignment Notification

Activation maximum duration (hours)  

3

On activation, require ☐ None  
☒ Azure MFA

You add assignments to the Security Operator role as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

Which users can activate the Security Operator role?



- A. User2 only
- B. User3 only
- C. Used and User2 only
- D. User2 and User3 only
- E. User1,User2, and User3

**Answer:** D

#### NEW QUESTION 57

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You create a data loss prevention (DLP) policy and select Use Notifications to inform your users and help educate them on the proper use of sensitive info.

Which apps will show the policy tip?

- A. Outlook on the web and Outlook Win32 only
- B. Outlook Win32 and Outlook for iOS and Android only Outlook Win32 only
- C. Outlook for iOS and Android only
- D. Outlook on the web, Outlook Win32, and Outlook for iOS and Android
- E. Outlook on the web only

**Answer:** A

#### NEW QUESTION 60

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Compliance administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure Active Directory (Azure AD) Identity Protection. You need to identify which users can perform the following actions:

- > Configure a user risk policy.
- > View the risky users report.

Which users should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Configure a user risk policy:

	▼
User1 only	
User1 and User3 only	
User3 and User4 only	
User1, User3, and User4 only	
User1, User2, User3, and User4	

View the risky users report:

	▼
User1 only	
User3 and User4 only	
User1, User2, and User3 only	
User1, User3, and User4 only	
User1, User2, User3, and User4	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

#### NEW QUESTION 64

- (Exam Topic 4)

You have a Microsoft 365 subscription named contofco.com

You need to configure Microsoft OneDrive for Business external sharing to meet the following requirements:

- Enable file sharing for users that have a Microsoft account
- Block file sharing for anonymous users. What should you do?

- A. From Advanced settings for external sharing, select Allow or No sharing with people on specific domains and add contoso.com.
- B. From the External sharing settings for OneDrive

- C. select Existing external users.
- D. From the External sharing settings for OneDrive, select New and existing external users.
- E. From the External sharing settings for OneDrive, select Only people in your organization.
- F. select Only people in your organization.

**Answer: C**

**Explanation:**

Reference:

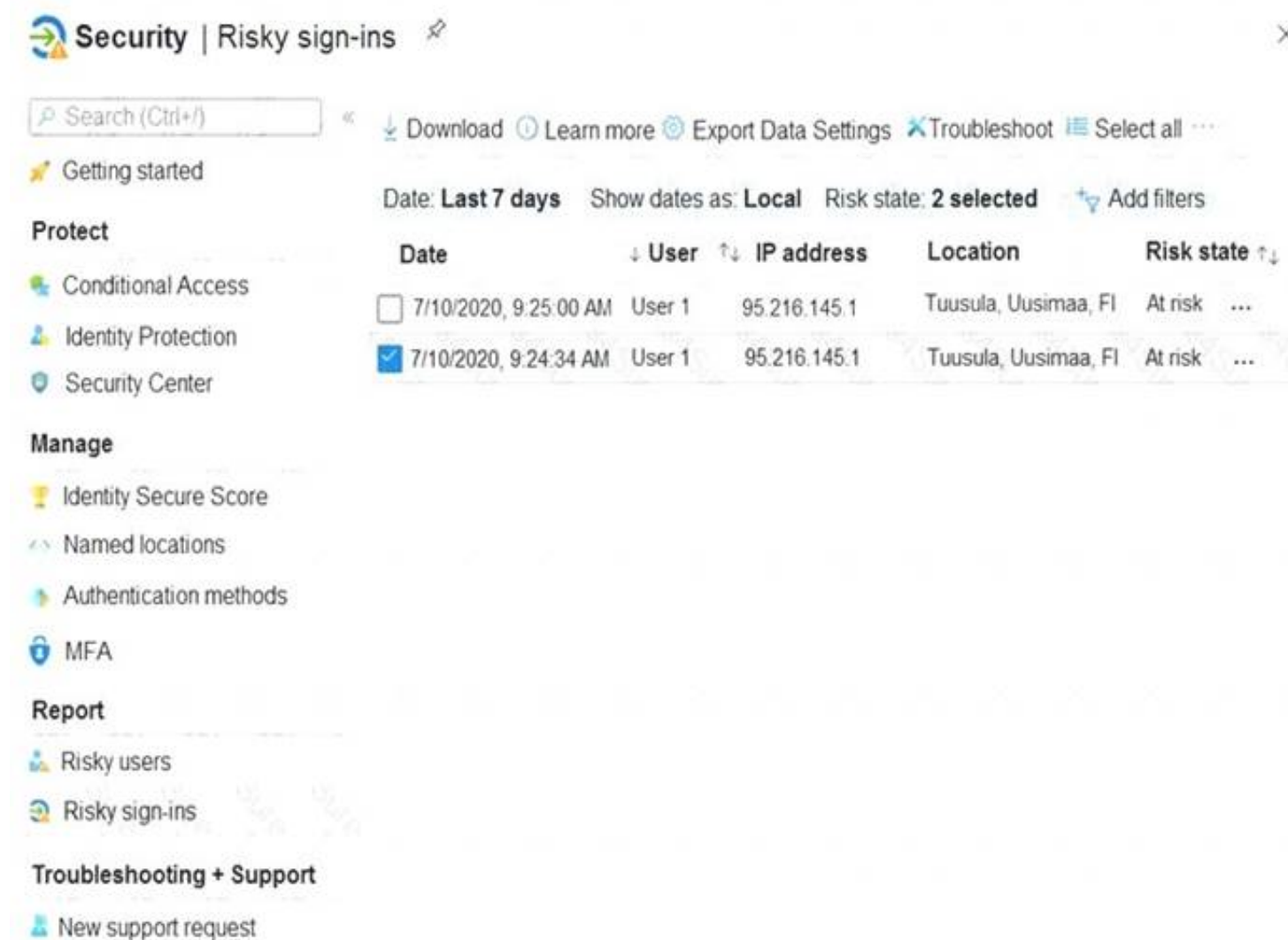
<https://www.sharepointdiary.com/2020/09/enable-external-sharing-in-onedrive-for-business.html>

**NEW QUESTION 66**

- (Exam Topic 4)

You have a Microsoft 365 tenant.

From the Azure Active Directory admin center, you review the Risky sign-ins report as shown in the following exhibit.



**Security | Risky sign-ins**

Search (Ctrl+/) Download Learn more Export Data Settings Troubleshoot Select all

Getting started

**Protect**

- Conditional Access
- Identity Protection
- Security Center

**Manage**

- Identity Secure Score
- Named locations
- Authentication methods
- MFA

**Report**

- Risky users
- Risky sign-ins

**Troubleshooting + Support**

- New support request

Date: Last 7 days Show dates as: Local Risk state: 2 selected Add filters

Date	User	IP address	Location	Risk state
7/10/2020, 9:25:00 AM	User 1	95.216.145.1	Tuusula, Uusimaa, FI	At risk
7/10/2020, 9:24:34 AM	User 1	95.216.145.1	Tuusula, Uusimaa, FI	At risk

You need to ensure that you can see additional details including the risk level and the risk detection type. What should you do?

- A. Purchase Microsoft 365 Enterprise E5 licenses.
- B. Activate an instance of Microsoft Defender for Identity.
- C. Configure Diagnostic settings in Azure Active Directory (Azure AD).
- D. Deploy Azure Sentinel and add a Microsoft Office 365 connector.

**Answer: A**

**NEW QUESTION 67**

- (Exam Topic 4)

You have a Microsoft 365 E5 Subscription named contOSO.C0rn. You create a user named User'.

You Need to ensure that User1 can change Status of Microsoft Defender for Identity health alerts. The solution must use principle of the least principle. What should you do?

- A. From the Microsoft 365 admin center, add user' to the Azure ATP contoso.com Administrators group.
- B. From the Microsoft 365 Defender portal, assign user' the Security Operator role.
- C. From the Microsoft 365 admin center, add user' to the Azure ATP contoso.com users group.
- D. From the Microsoft admin center, assign user1 the Hybrid Identity Administrator role.

**Answer: B**

**NEW QUESTION 71**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription

You need to ensure that users who are assigned the Exchange administrator role have time-limited permissions and must use multi factor authentication (MFA) to request the permissions.

What should you use to achieve the goal?

- A. Microsoft 365 user management
- B. Microsoft Azure AD group management
- C. Security & Compliance permissions
- D. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management

Answer: D

NEW QUESTION 72

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. Azure AD Identity Protection alerts for contoso.com are configured as shown in the following exhibit.

Save

Discard

Download

Alert on user risk level at or above

Low

Medium

High

Emails are sent to the following users. ⓘ

INCLUDED

1 selected

>

Add additional emails to receive alert notifications (Preview). ⓘ

A user named User1 is configured to receive alerts from Azure AD Identity Protection. You create users in contoso.com as shown in the following table.

Name	Role
User2	Security reader
User3	User administrator
User4	None
User5	None

The users perform the sign-ins shown in the following table.

Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User2 receives three email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>
User3 receives two email alerts from Azure AD Identity Protection.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

User1 will receive the two alerts classified as medium or higher.

Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as Low.

Box 2: No

User2 will receive the two alerts classified as medium or higher.

Email alerts are sent to all global admins, security admins and security readers

Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as Low.

Box 3: No

User3 will not receive alters.

Email alerts are sent to all global admins, security admins and security readers. Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure>

### NEW QUESTION 73

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains 1,000 user mailboxes.

An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.

You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.

Solution: You modify the permissions of the mailbox of User5, and then create an eDiscovery case. Does this meet the goal?

A. Yes

B. No

**Answer: B**

#### Explanation:

References:

<https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-201>

### NEW QUESTION 75

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Cloud Apps enabled. You need to create an alert in Defender for Cloud Apps when source code is shared externally.

Which type of policy should you create?

A. Cloud Discovery anomaly detection

B. file

C. access

D. activity

**Answer: B**

### NEW QUESTION 76

- (Exam Topic 4)

You have a Microsoft 365 E5 tenant that contains three users named User1, User2, and User3. You need to assign roles or role groups to the users as shown in the following table.

User	Role or role group
User1	SharePoint admin
User2	Data Investigator
User3	User admin

What should you use to assign a role or role group to each user? To answer, drag the appropriate tools to the correct roles or role groups. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Tools**

Azure Defender for Servers

Compliance Manager

Microsoft 365 admin center

Security & Compliance admin center

Trust Center

**Answer Area**

User1: 

Tool

User2: 

Tool

User3: 

Tool

A. Mastered

B. Not Mastered

**Answer: A**

#### Explanation:

Graphical user interface, text, application, chat or text message Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-co>



NEW QUESTION 79

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.

You use the Application event log on Server1. Does that meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

NEW QUESTION 80

- (Exam Topic 4)

You have a Microsoft 365 subscription. All users use Microsoft Exchange Online. Microsoft 365 is configured to use the default policy settings without any custom rules. You manage message hygiene.

Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each location may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Locations

ATP quarantine

The Junk Email folder of a user's mailbox

The Clutter folder a user's mailbox

Messages that contain word-filtered content:

Messages that are classified as phishing:

Answer Area

Location

Location

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Locations

ATP quarantine

The Junk Email folder of a user's mailbox

The Clutter folder a user's mailbox

Messages that contain word-filtered content:

Messages that are classified as phishing:

Answer Area

The Junk Email folder of a user's mailbox

The Junk Email folder of a user's mailbox

NEW QUESTION 82

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You need to ensure that all users who are assigned the Exchange administrator role have multi-factor authentication (MFA) enabled by default.

What should you use to achieve the goal?

- A. Security & Compliance permissions
- B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- C. Microsoft Azure AD group management
- D. Microsoft Office 365 user management

Answer: B

NEW QUESTION 85

- (Exam Topic 4)

You have a Microsoft 365 subscription that include three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

You create an alert policy named Policy1 as shown in the following exhibit.



Policy1

Edit policy

Delete policy

Status	<input checked="" type="checkbox"/> On	
Description	Policy1 description	Edit
Severity	<input checked="" type="radio"/> Low	
Category	Threat management	

Conditions	Activity is Copied file and File name is Like any of File1.docx	
Aggregation	Aggregated	Edit
Threshold	10 activities	
Window	60 minutes	
Scope	All users	

Email recipients	prvi@sk180920.onmicrosoft.com	
Daily notifications limit	Do not send email notifications	Edit

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
 NOTE: Each correct selection is worth one point.

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

▼

Policy1 will not be triggered

Policy1 will be triggered after 45 minutes

Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

▼

Policy1 will not be triggered

Policy1 will be triggered within 20 minutes

Policy1 will be triggered within 45 minutes

Policy1 will be triggered after 60 minutes

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

NEW QUESTION 87

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription. Contoso.com contains the groups shown in the following table.

Name	Type
Group1	Office 365
Group2	Distribution list
Group3	Mail-enabled security
Group4	Security

You plan to create a supervision policy named Policy1.

You need to identify which groups can be supervised by using Policy1. Which groups should you identify?

- A. Group1 and Group4 only
- B. Group1 only
- C. Group1, Group3, and Group4 only

- D. Group2 and Group3 only
- E. Group1, Group2, and Group3 only

**Answer:** E

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/configure-supervision-policies?view=o365-worldwide>

**NEW QUESTION 92**

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1. You need to ensure that User1 can review Conditional Access policies.

Solution: You assign User1 the Application Administrator role. Does this meet goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 93**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You need to enable auditing for all Microsoft Exchange Online users. What should you do?

- A. From the Exchange admin center, create a journal rule
- B. Run the Set-MailboxDatabase cmdlet
- C. Run the Set-Mailbox cmdlet
- D. From the Exchange admin center, create a mail flow message trace rule.

**Answer:** C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

**NEW QUESTION 94**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them. When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets \*Mailbox\* command. Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/setadmindauditlogconfig>

**NEW QUESTION 98**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1.

The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1. For User1, you select Confirm user compromised.

User1 can still sign in.

You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.

Solution: From the Access settings, you select Block access for User1. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate>

**NEW QUESTION 103**

- (Exam Topic 4)

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription. You need to allow a user named User1 to view ATP reports in the Threat management dashboard. Which role provides User1 with the required role permissions?

- A. Security reader
- B. Message center reader
- C. Compliance administrator
- D. Information Protection administrator

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-areneeded>

**NEW QUESTION 104**

- (Exam Topic 4)

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

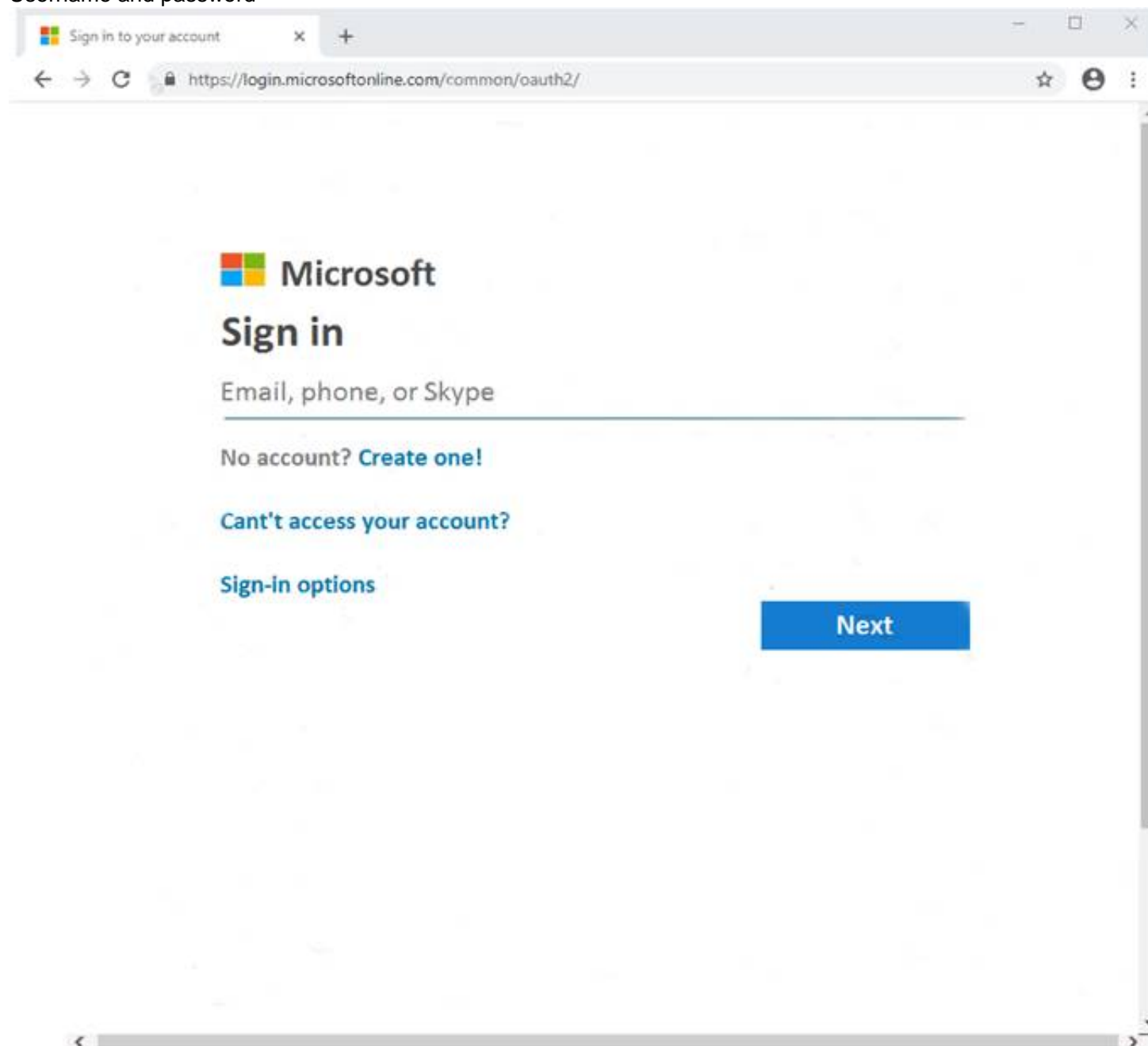
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:

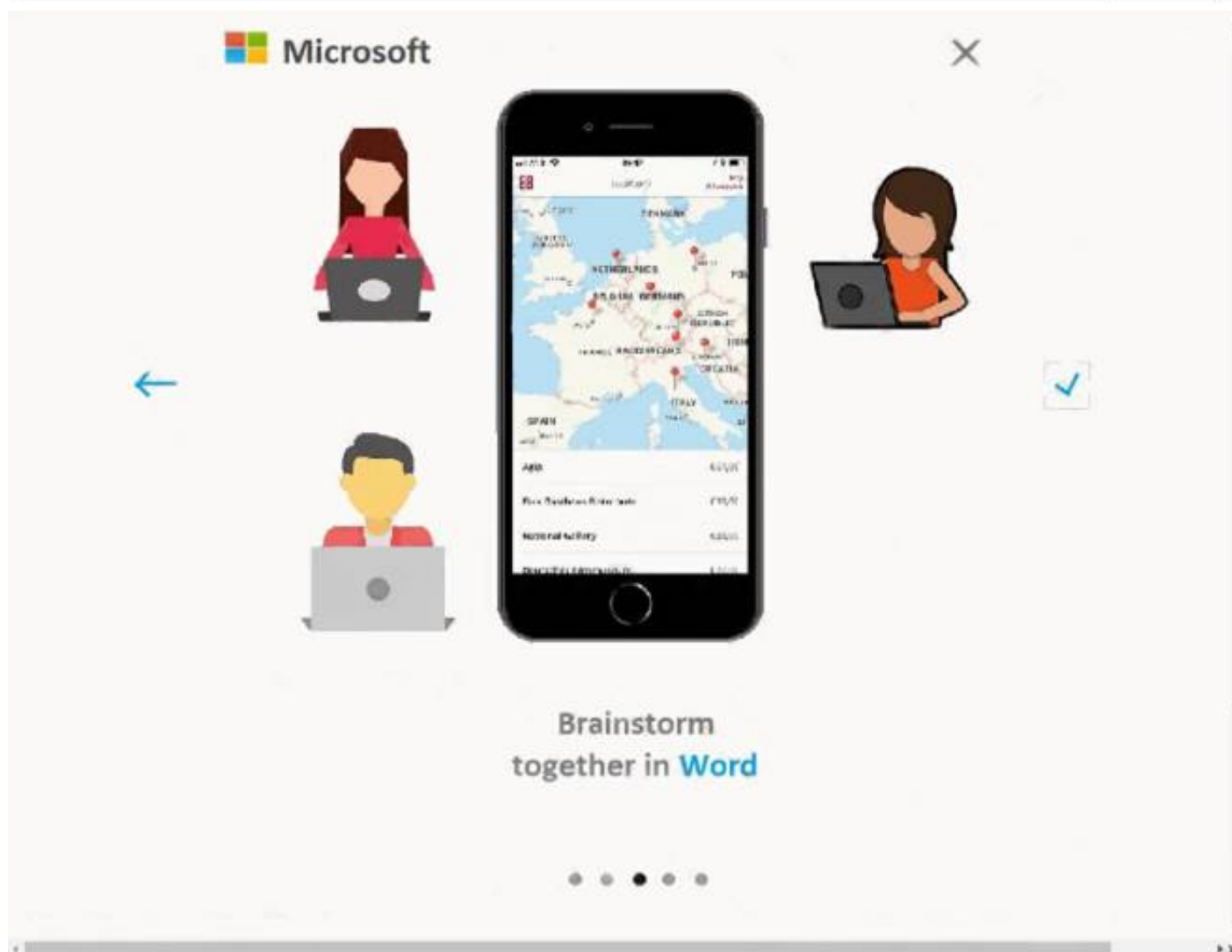
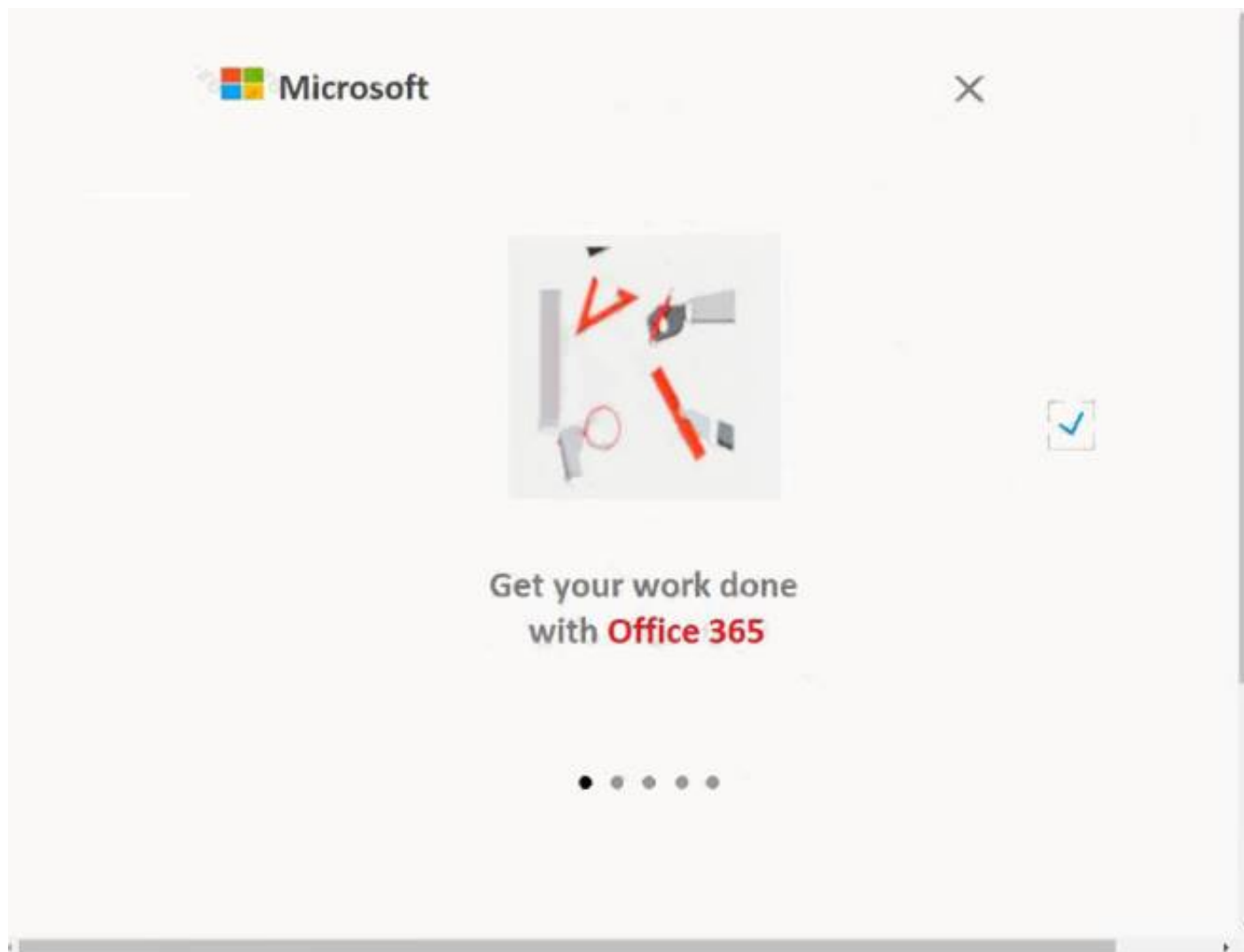
To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username:

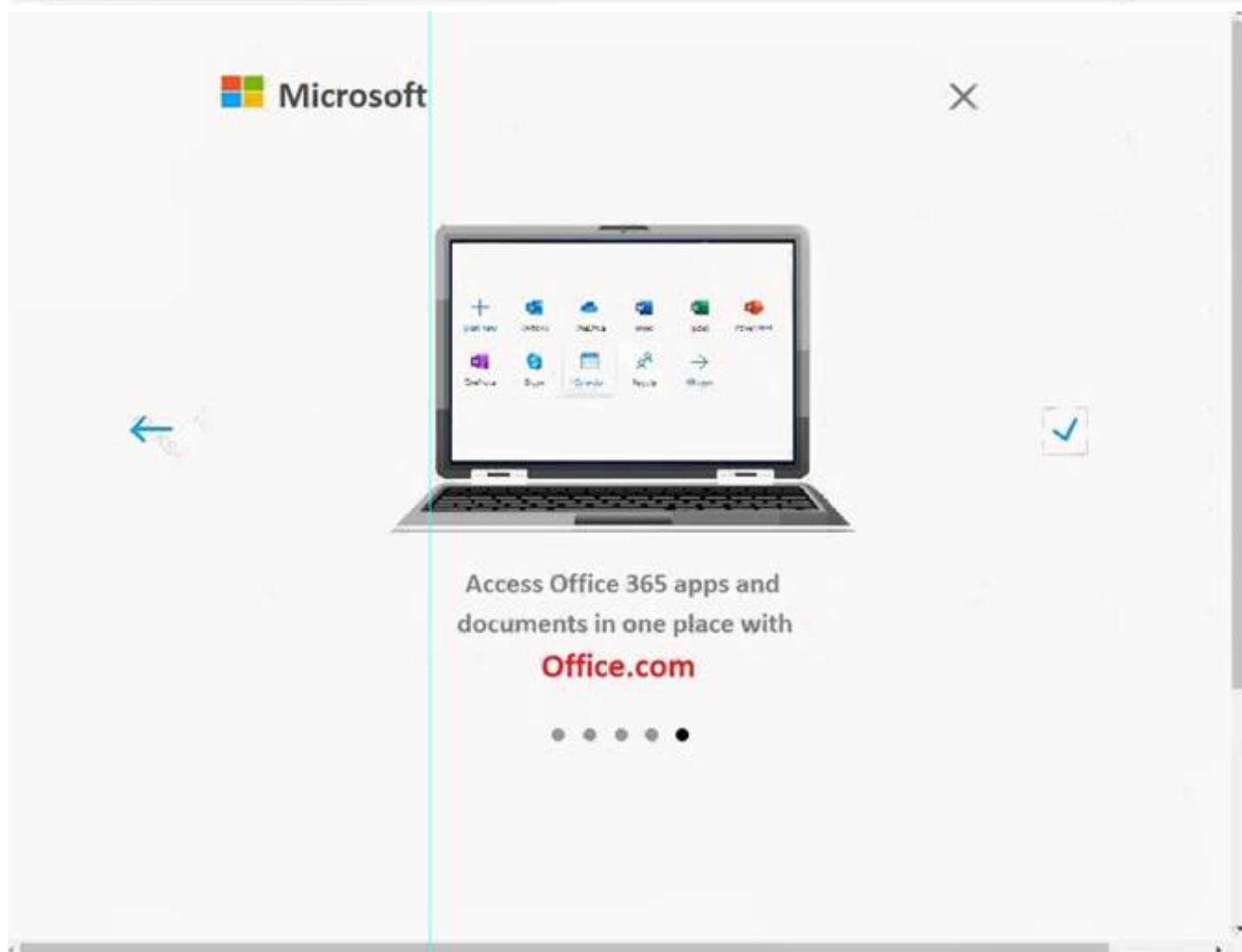
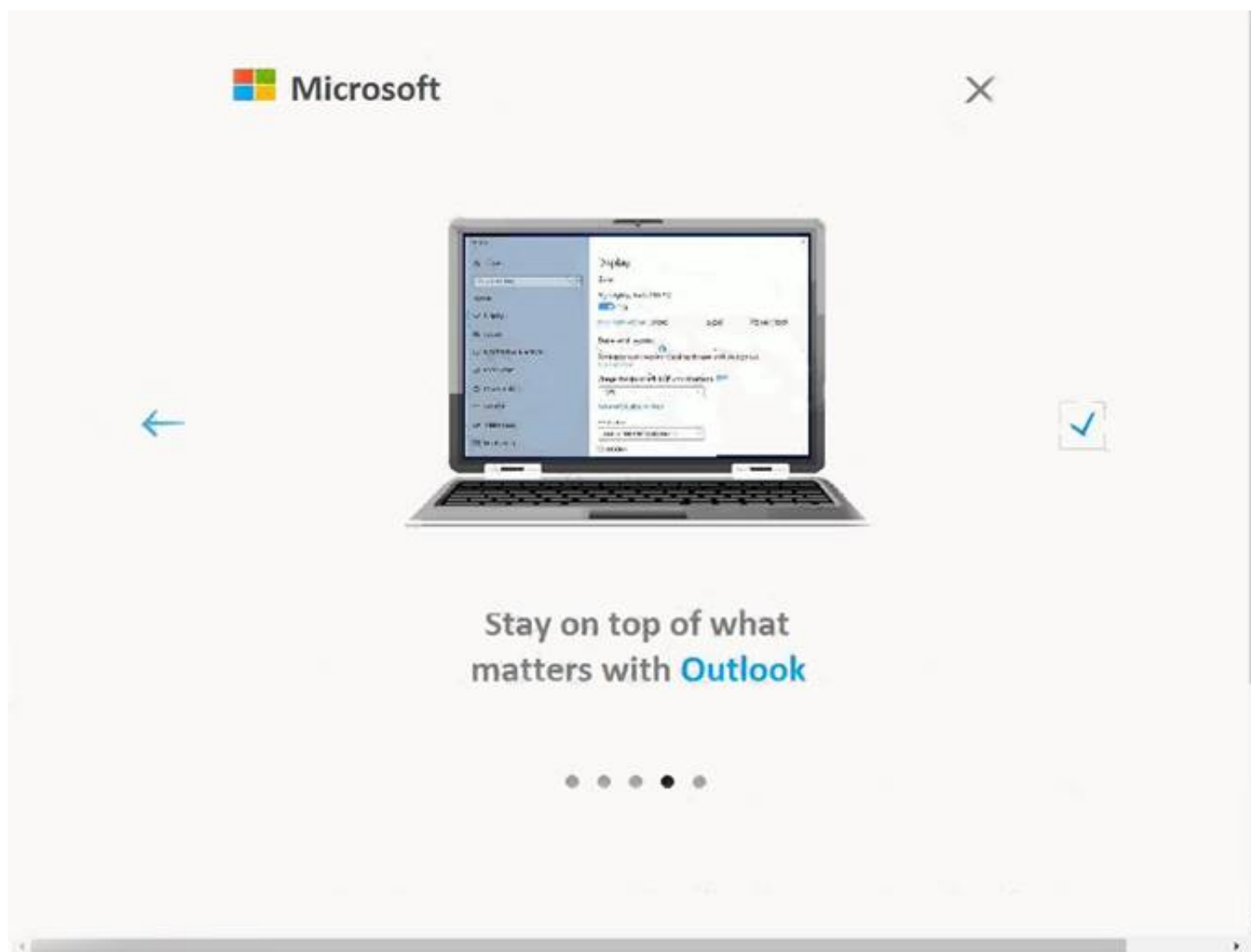
admin@LODSe00019@onmicrosoft.com Microsoft 365 Password: #HSP.ug?\$p6un

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support only: Lab instance: 11122308







Microsoft Office Home

office.com/7a9thui2

Contoso electronics Office 365

Good morning

Install Office

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview  
 lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process  
 lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart  
 lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

## Recommended

You edited this Jan 15

Excel

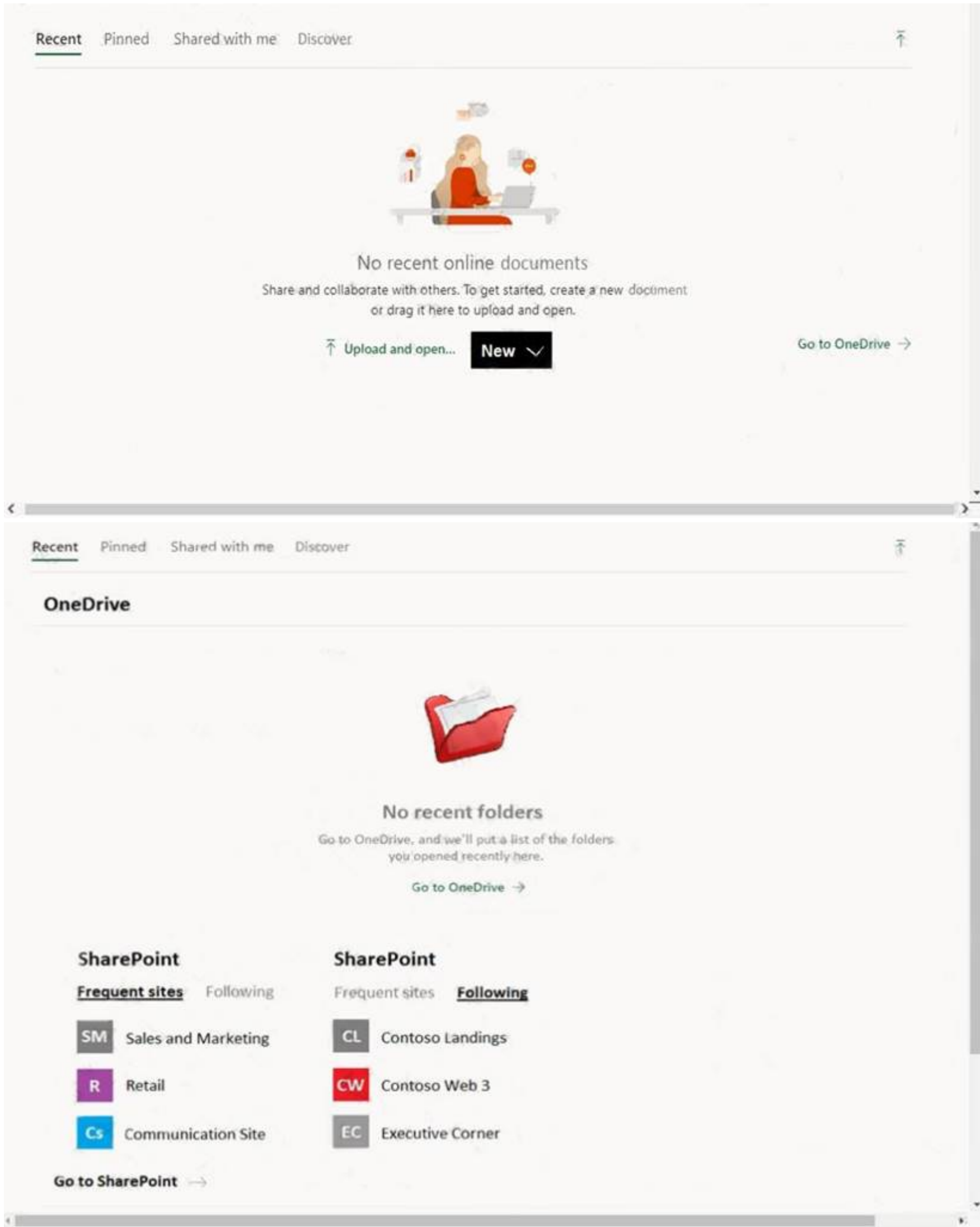
P and L Summary  
 lodse000198.sharepoint.co...

You edited this Jan 15

Contoso Electronics Outdoor...

AD Slogans  
 lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover



Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

You plan to create a script to automate user mailbox searches. The script will search the mailbox of a user named Allan Deyoung for messages that contain the word injunction.

You need to create the search that will be included in the script. To complete this task, sign in to the Microsoft 365 admin center.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create a CSV file that contains information about the searches you want to run

The comma separated value (CSV) file that you create in this step contains a row for each user that want to search. You can search the user's Exchange Online mailbox (which includes the archive mailbox, if it's enabled) and their OneDrive for Business site. Or you can search just the mailbox or the OneDrive for Business site. You can also search any site in your SharePoint Online organization. The script that you run in Step 3 will create a separate search for each row in the CSV file.

\* 1. Copy and paste the following text into a .txt file using NotePad. Save this file to a folder on your local computer. You'll save the other scripts to this folder as well. ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate  
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad\_contoso\_onmicrosoft\_com,(OR legal),1/1/2000,12/31/2005  
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad\_contoso\_onmicrosoft\_com,(OR legal),1/1/2006,12/31/2010  
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad\_contoso\_onmicrosoft\_com,( OR legal),1/1/2011,3/21/2016  
,https://contoso.sharepoint.com/sites/contoso,,,3/21/2016  
,https://contoso-my.sharepoint.com/personal/davidl\_contoso\_onmicrosoft\_com,,1/1/2015,  
,https://contoso-my.sharepoint.com/personal/janets\_contoso\_onmicrosoft\_com,,1/1/2015,

The first row, or header row, of the file lists the parameters that will be used by New-ComplianceSearch cmdlet to create a new Content Searches. Each parameter name is separated by a comma. Make sure there aren't any spaces in the header row. Each row under the header row represents the parameter values for each search. Be sure to replace the placeholder data in the CSV file with your actual data.

\* 2. Open the .txt file in Excel, and then use the information in the following table to edit the file with information for each search.



Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see <a href="#">Keyword queries and search conditions for Content Search</a> .
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

\* 3. Save the Excel file as a CSV file to a folder on your local computer. The script that you create in Step 3 will use the information in this CSV file to create the searches.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-search> Keyword queries and search conditions for Content Search

<https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365>

#### NEW QUESTION 109

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	User principal name (UPN)	Member of
User1	User1@contoso.com	Group1
User2	User2@contoso.com	Group2
User3	User3@contoso.com	Group2

Group1 is member of a group named Group3.

The Azure Active Directory (Azure AD) tenant contains the Windows 10 devices shown in the following table.

Name	Join type	Owner	Member of
Device1	Azure AD-registered	User3	Group4
Device2	Azure AD-joined	User2	Group5

Microsoft Endpoint Manager has the devices shown in the following table.

Name	Enrolled by UPN
Device1	User1@contoso.com
Device2	User2@contoso.com

Microsoft Endpoint Manager contains the compliance policies shown in the following table.

Name	Assignment
Policy1	Group3
Policy2	Group4
Policy3	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

#### Answer Area

Statements	Yes	No
Policy1 applies to Device1.	<input type="radio"/>	<input type="radio"/>
Policy2 applies to Device1.	<input type="radio"/>	<input type="radio"/>
Policy3 applies to Device2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Statements	Yes	No
Policy1 applies to Device1.	<input checked="" type="radio"/>	<input type="radio"/>
Policy2 applies to Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Policy3 applies to Device2.	<input type="radio"/>	<input checked="" type="radio"/>

#### NEW QUESTION 111

- (Exam Topic 4)

You need to ensure that unmanaged mobile devices are quarantined when the devices attempt to connect to Exchange Online. To complete this task, sign in to the Microsoft 365 portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

You need to configure the Exchange ActiveSync Access Settings.

- > Go to the Exchange admin center.
- > Click on Mobile in the left navigation pane.
- > On the Mobile Device Access page, click the Edit button in the Exchange ActiveSync Access Settings area.
- > Select the Quarantine option under When a mobile device that isn't managed by a rule or personal exemption connects to Exchange.
- > Optionally, you can configure notifications to be sent to administrators and a message to be sent to the mobile device user when a device is quarantined.
- > Click Save to save the changes.

#### NEW QUESTION 114

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Configuration
DC1	Domain controller
Server1	Member server

You plan to implement Azure Advanced Threat Protection (ATP) for the domain. You install an Azure ATP standalone sensor on Server1. You need to monitor the domain by using Azure ATP. What should you do?

- A. Configure port mirroring for DC1.
- B. Configure port mirroring for Server 1.
- C. Install the Microsoft Monitoring Agent on Server1.
- D. Install the Microsoft Monitoring Agent on DC1.

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-port-mirroring>

#### NEW QUESTION 115

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports. The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.  
 Solution: You recommend modifying the licenses assigned to User5. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

#### NEW QUESTION 118

- (Exam Topic 4)

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. Four Windows 10 devices are joined to the tenant as shown in the following table.

Name	Has TPM	BitLocker Drive Encryption (BitLocker) -protected C drive	BitLocker Drive Encryption (BitLocker) -protected D drive
Device1	Yes	Yes	No
Device2	Yes	No	Yes
Device3	No	Yes	Yes
Device4	No	No	No

On which devices can you use BitLocker To Go and on which devices can you turn on auto-unlock? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

BitLocker To Go:

Device3 only
Device1 and Device2 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Auto-unlock:

Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

BitLocker To Go:

Device3 only
Device1 and Device2 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Auto-unlock:

Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

#### NEW QUESTION 119

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports. The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User5. Does this meet the goal?

- A. Yes
- B. No



Answer: B

#### NEW QUESTION 123

- (Exam Topic 4)

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

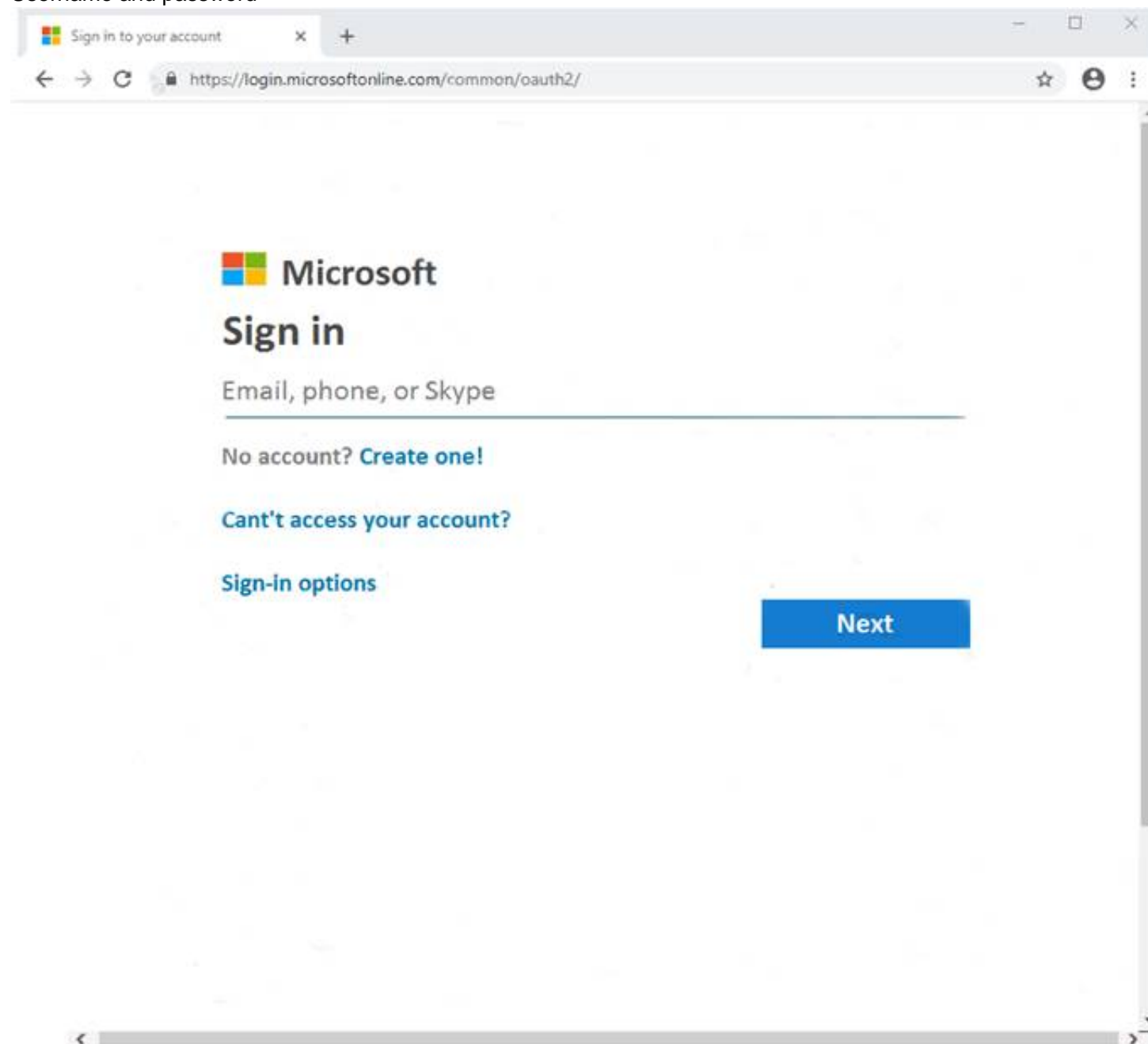
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

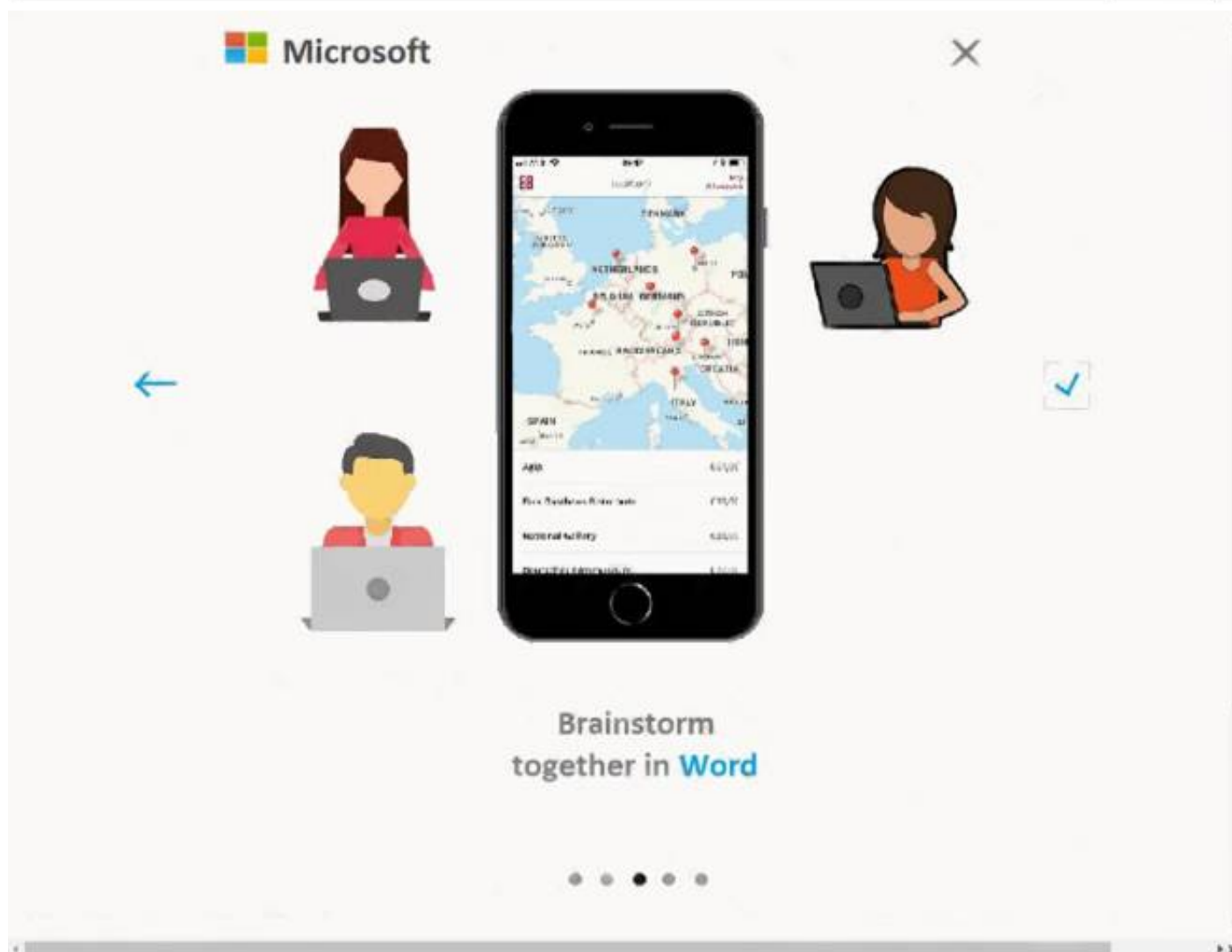
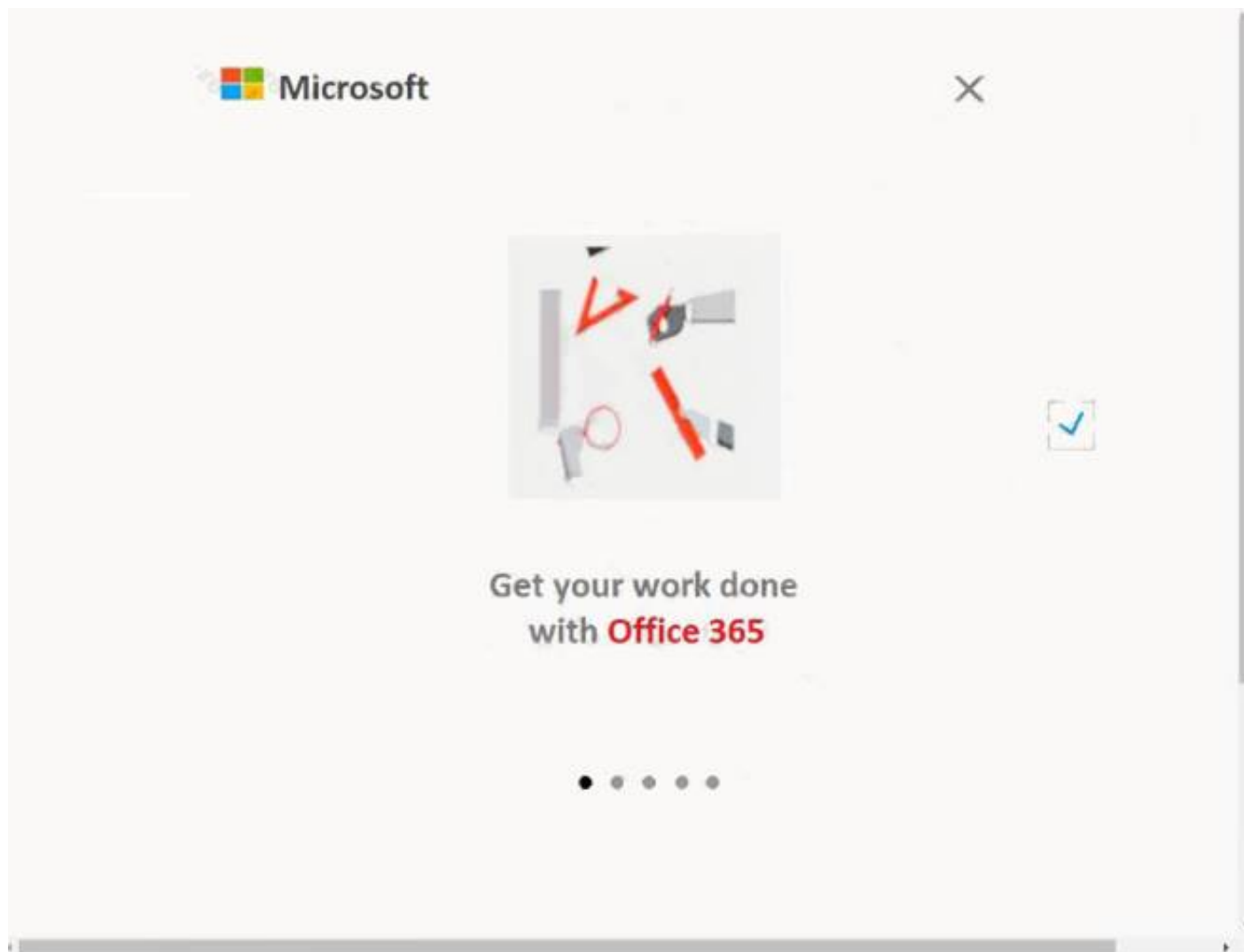
To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username:

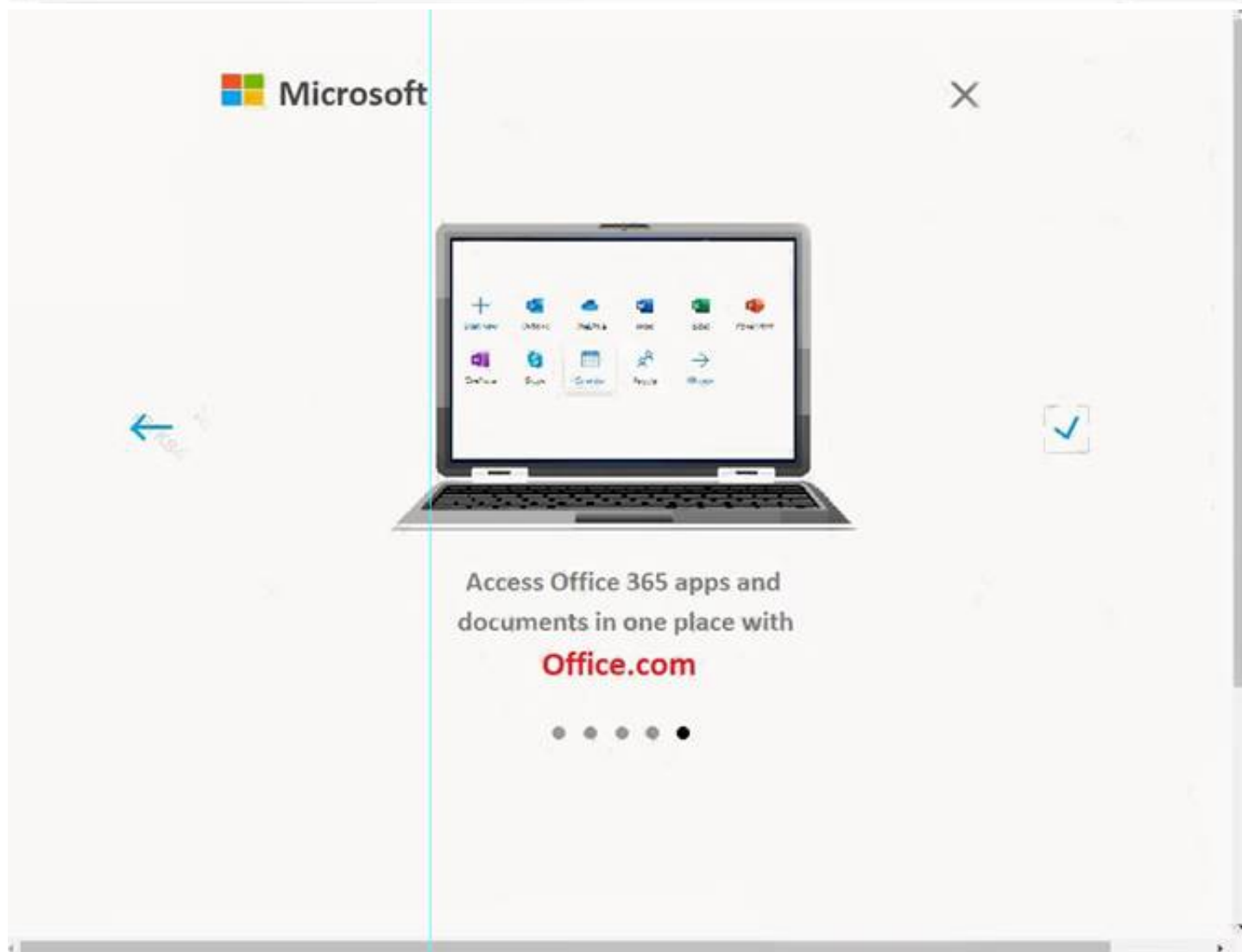
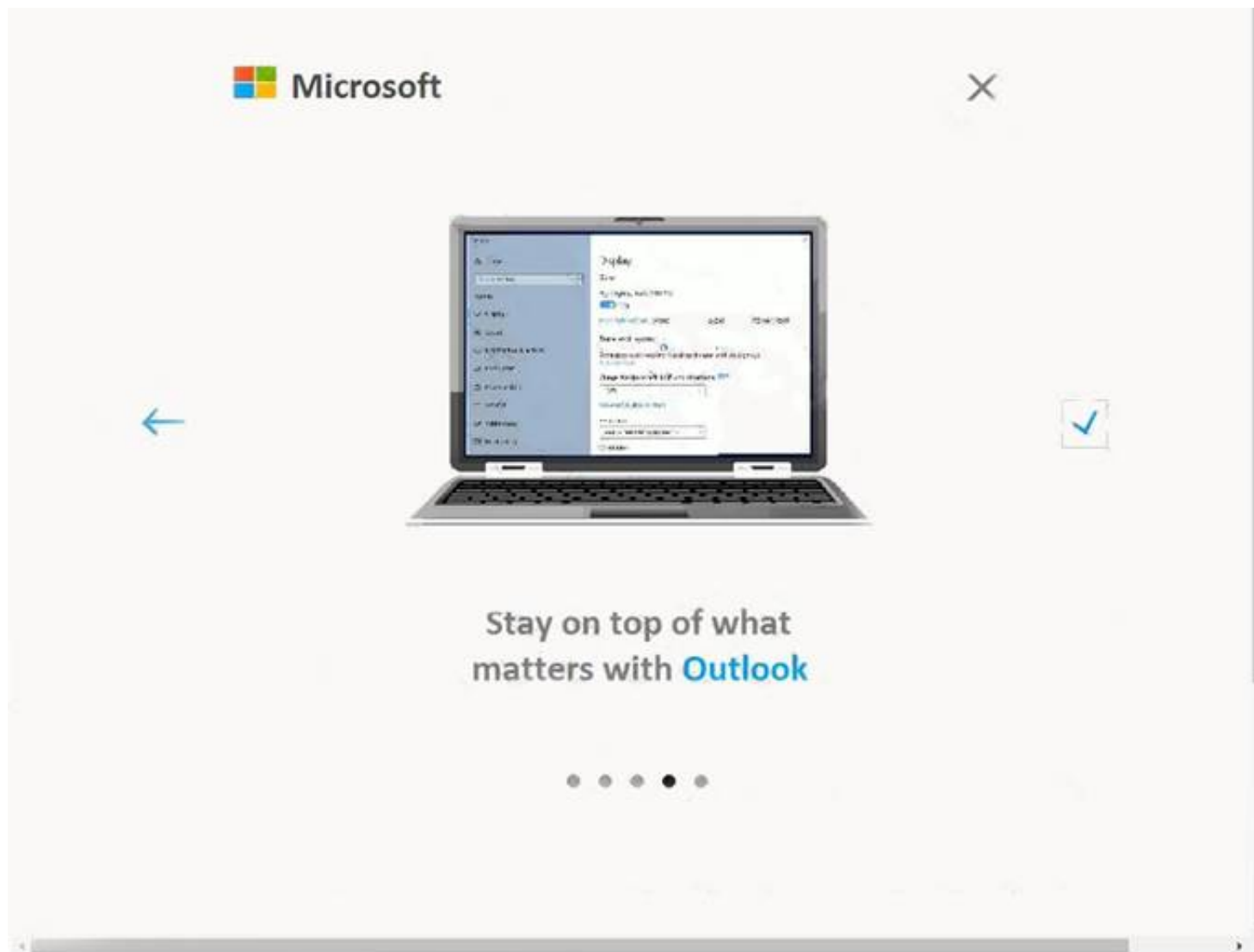
admin@LODSe00019@onmicrosoft.com Microsoft 365 Password: #HSP.ug?\$p6un

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support only: Lab instance: 11122308







Microsoft Office Home

Contoso electronics Office 365

Good morning

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview  
lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process  
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart  
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

## Recommended

You edited this Jan 15

Excel

P and L Summary  
lodse000198.sharepoint.co...

You edited this Jan 15


Contoso Electronics Outdoor...  
lodse000198.sharepoint.co...

You edited this Jan 15

AD Slogans  
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

RecentPinnedShared with meDiscover



No recent online documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.


Upload and open...

New

Go to OneDrive →

RecentPinnedShared with meDiscover

OneDrive



No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

Go to OneDrive →

SharePoint

Frequent sitesFollowing

SM

Sales and Marketing

R

Retail

Cs

Communication Site

Go to SharePoint →

SharePoint

Frequent sitesFollowing

CL

Contoso Landings

CW

Contoso Web 3

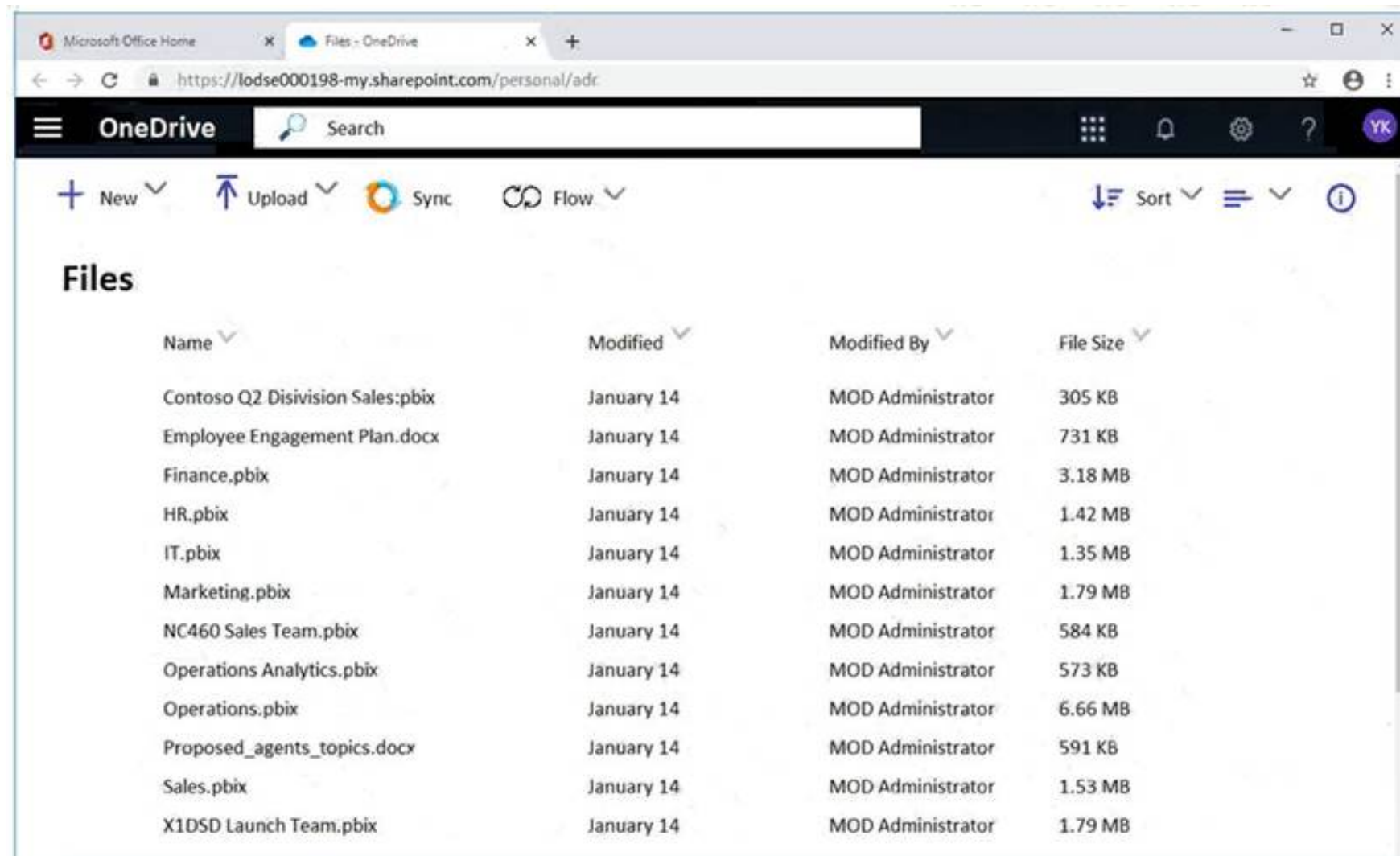
EC

Executive Corner

Guaranteed success with Our exam guides

visit - <https://www.certshared.com>





Name	Modified	Modified By	File Size
Contoso Q2 Disivision Sales.pbix	January 14	MOD Administrator	305 KB
Employee Engagement Plan.docx	January 14	MOD Administrator	731 KB
Finance.pbix	January 14	MOD Administrator	3.18 MB
HR.pbix	January 14	MOD Administrator	1.42 MB
IT.pbix	January 14	MOD Administrator	1.35 MB
Marketing.pbix	January 14	MOD Administrator	1.79 MB
NC460 Sales Team.pbix	January 14	MOD Administrator	584 KB
Operations Analytics.pbix	January 14	MOD Administrator	573 KB
Operations.pbix	January 14	MOD Administrator	6.66 MB
Proposed_agents_topics.docx	January 14	MOD Administrator	591 KB
Sales.pbix	January 14	MOD Administrator	1.53 MB
X1DSD Launch Team.pbix	January 14	MOD Administrator	1.79 MB

You need to ensure that all the email messages in the mailbox of a user named Allan Deyoung are retained for a period of 90 days, even if the messages are deleted.

To complete this task, sign in to the Microsoft 365 admin center.

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

- \* 1. Navigate to the Exchange Admin Center
- \* 2. Navigate to Compliance management > Retention tags, and then click Add +
- \* 3. Select the Applied automatically to entire mailbox (default) option.
- \* 4. The New retention tag page title and options will vary depending on the type of tag you selected. Complete the following fields:  
 Name: Enter a name for the retention tag.  
 Retention action: Select Delete and Allow Recovery option.  
 Retention period: Select When the item reaches the following age (in days) option.  
 Comment: User this optional field to enter any administrative notes or comments. The field isn't displayed to users.
- \* 5. Navigate to Compliance management > Retention policies, and then click Add +
- \* 6. In New Retention Policy, complete the following fields: Name: Enter a name for the retention policy.  
 Retention tags: Click Add + to select the tags you want to add to this retention policy. After you create a retention policy, you must apply it.
- \* 1. Navigate to Recipients > Mailboxes.
- \* 2. In the list view, select the mailbox to which you want to apply the retention policy, and then click Edit.
- \* 3. In User Mailbox, click Mailbox features.
- \* 4. In the Retention policy list, select the policy you want to apply to the mailbox, and then click Save. Reference:  
<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-re> <https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-rete>

#### NEW QUESTION 127

- (Exam Topic 4)

You have multiple Microsoft 365 subscriptions.

You need to build an application that will retrieve the Microsoft Secure Score data of each subscription. What should you use?

- A. the Microsoft Defender for Endpoint API
- B. the Microsoft Graph Security API
- C. the Microsoft Office 365 Management API
- D. the Azure Monitor REST API

**Answer: C**

#### NEW QUESTION 130

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that contains a user named User1.

The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1. For User1, you select Confirm user compromised.

User1 can still sign in.

You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.

Solution: You configure the sign-in risk policy to block access when the sign-in risk level is high. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate>

**NEW QUESTION 133**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

Some users are required to use an authenticator app to access Microsoft SharePoint Online.

You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.

What should you do?

- A. From the Azure Active Directory admin center, view the sign-ins.
- B. From the Security & Compliance admin center, download a report.
- C. From the Azure Active Directory admin center, view the authentication methods.
- D. From the Azure Active Directory admin center, view the audit logs.

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

**NEW QUESTION 134**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1.

You have a Data Subject Request (DSR) case named Case1 that searches Site1. You create a new sensitive information type.

You need to ensure that Case1 returns all the documents that contain the new sensitive information type. What should you do?

- A. From the Security & Compliance admin center, create a new Search by ID List.
- B. From Site1, modify the search dictionary.
- C. From the Security & Compliance admin center, create a new Guided search.
- D. From Site1, initiate a re-indexing of Site1.

**Answer:** D

**NEW QUESTION 139**

- (Exam Topic 4)

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

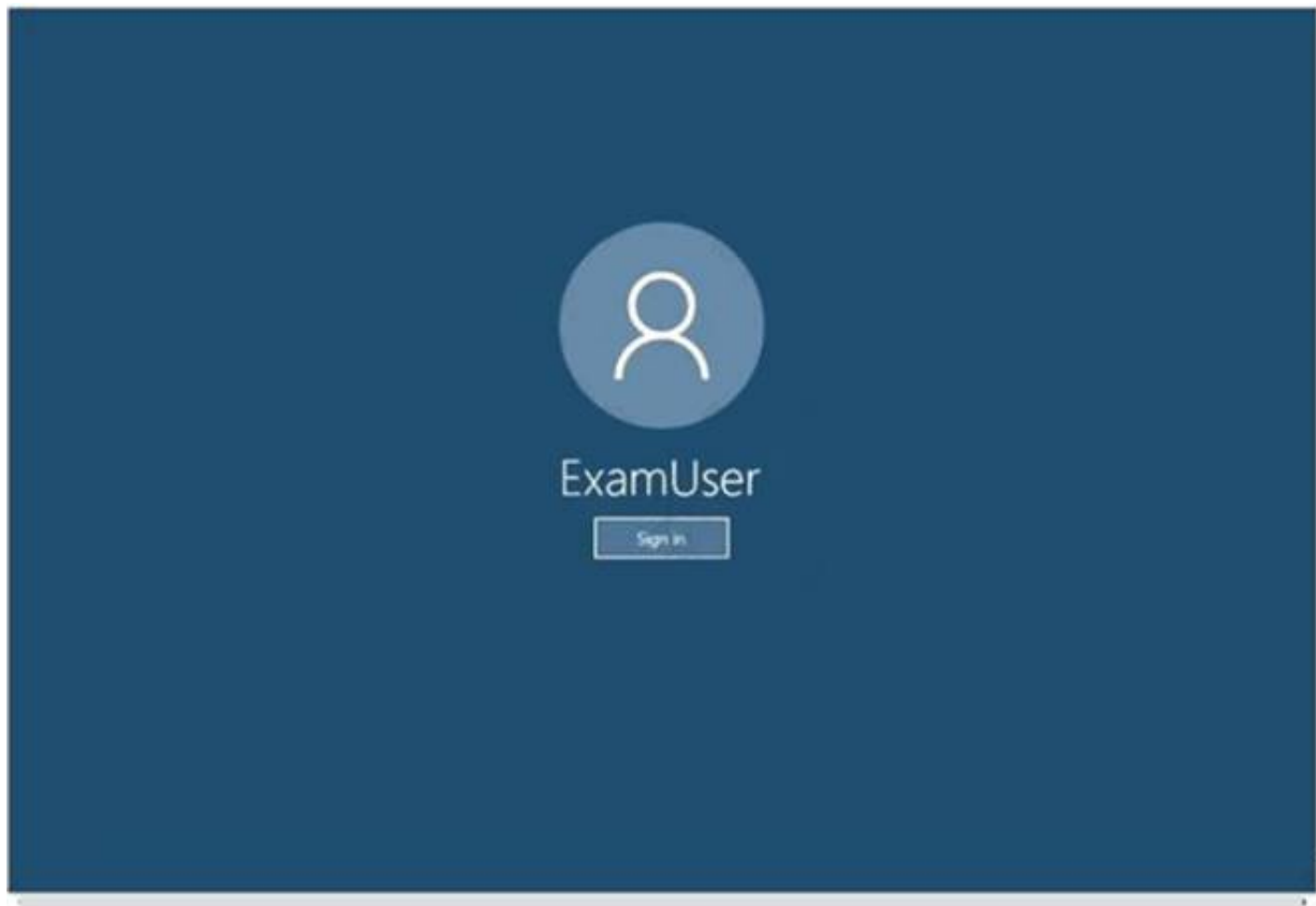
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username:

admin@LODSe244001@onmicrosoft.com Microsoft 365 Password: &=Q8v@2qGzYz

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support only: Lab instance: 11032396

You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA). To complete this task, sign in to the Microsoft Office 365 admin center.

- A. Mastered
- B. Not Mastered

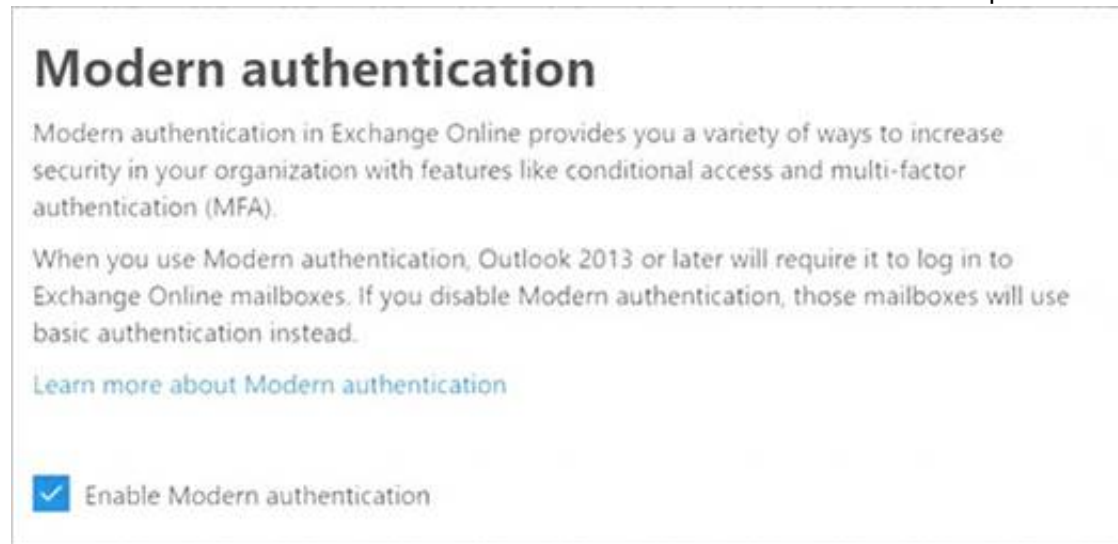
**Answer:** A

**Explanation:**

Enable Modern authentication for your organization

\* 1. To enable modern authentication, from the admin center, select Settings > Settings and then in the Services tab, choose Modern authentication from the list.

\* 2. Check the Enable modern authentication box in the Modern authentication panel.



Enable multi-factor authentication for your organization

\* 1. In the admin center, select Users and Active Users.

\* 2. In the Active Users section, Click on multi-factor authentication.

\* 3. On the Multi-factor authentication page, select user if you are enabling this for one user or select Bulk Update to enable multiple users.

\* 4. Click on Enable under Quick Steps.

\* 5. In the Pop-up window, Click on Enable Multi-Factor Authentication.

After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authenticati>

**NEW QUESTION 142**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Azure Active Directory (Azure AD) Privileged identity Management (PIM). A user named User1 is eligible for the User Account Administrator role. You need User1 to request to activate the User Account Administrator role. From where should User1 request to activate the role?

- A. the My Access portal
- B. the Microsoft 365 Defender portal
- C. the Azure Active Directory admin center
- D. the Microsoft 365 admin center

Answer: B

### NEW QUESTION 145

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains the folders shown in the following table.

Name	File in folder
Folder1	File1
Folder2	File2

At 09:00, you create a Microsoft Cloud App Security policy named Policy1 as shown in the following exhibit.

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING

Edit and preview results

×

App

equals

Microsoft SharePoint...

+

Apply to:

selected folders

Currently supports Box, SharePoint, Dropbox, OneDrive.

**Folder1** (Microsoft SharePoint Online) ×

[Add more folder\(s\)](#)

Apply to:

all file owners

Inspection method

None

Alerts

☒ Create an alert for each matching file [Restore default settings](#)

Daily alert limit

5

☐ Send alert as email ⓘ

☐ Send alert as text message ⓘ

[Save as default settings](#)

☐ Send alerts to Flow  
[Create a playbook in Flow](#)

After you create Policy1, you upload files to Site1 as shown in the following table.

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
File1 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File3 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>
File9 triggers an alert from Policy1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A



**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

**NEW QUESTION 148**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.

Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
From PowerShell, run Remove-SPOUserProfile	
Delete Litware.docx from the Recycle Bin of Site2.	
From PowerShell, run Set-SPOSite.	
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

Actions	Answer Area
From PowerShell, run Remove-SPOUserProfile	Delete Litware.docx from Customers.
Delete Litware.docx from the Recycle Bin of Site2.	Delete Litware.docx from the Recycle Bin of Site2.
From PowerShell, run Set-SPOSite.	Delete Litware.docx from the Recycle Bin of SiteCollection1.
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

**NEW QUESTION 152**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You need to include a custom sensitive information type in Data Subject Request (DSR) cases.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Connect to the Security & Compliance admin center

Connect to the Security & Compliance admin center by using a remote PowerShell session

Export the current rules as a JSON file

Upload the file

Export the current rules as an XML file

Modify the file

Answer Area

>

<

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/compliance/customize-a-built-in-sensitive-information-type?vie>

NEW QUESTION 153

- (Exam Topic 4)  
You have a Microsoft 365 tenant.  
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.  
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Save the audit logs to:

Azure Data Lake Storage Gen2

Azure Files

Azure Log Analytics

Azure Active Directory admin center blade to use to view the saved audit logs:

Audit logs

Identity Governance

Logs

Sign-ins

Usage & insights

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-ana>

NEW QUESTION 157

- (Exam Topic 4)  
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 contains 100 users and has dynamic user membership. All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online. You create a sensitivity label named Label and publish Label 1 as

the default label for Group1. You need to ensure that the users in Group1 must apply Label1 to their email and documents. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Install the Azure Information Protection unified labeling client on the Windows 10 devices.
- B. From the Microsoft 365 Compliance center, modify the settings of the Label1 policy.
- C. Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices.
- D. From the Microsoft 365 Compliance center, create an auto-labeling policy.
- E. From the Azure Active Directory admin center, set Membership type for Group1 to Assigned.

**Answer:** DE

#### NEW QUESTION 158

- (Exam Topic 4)

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

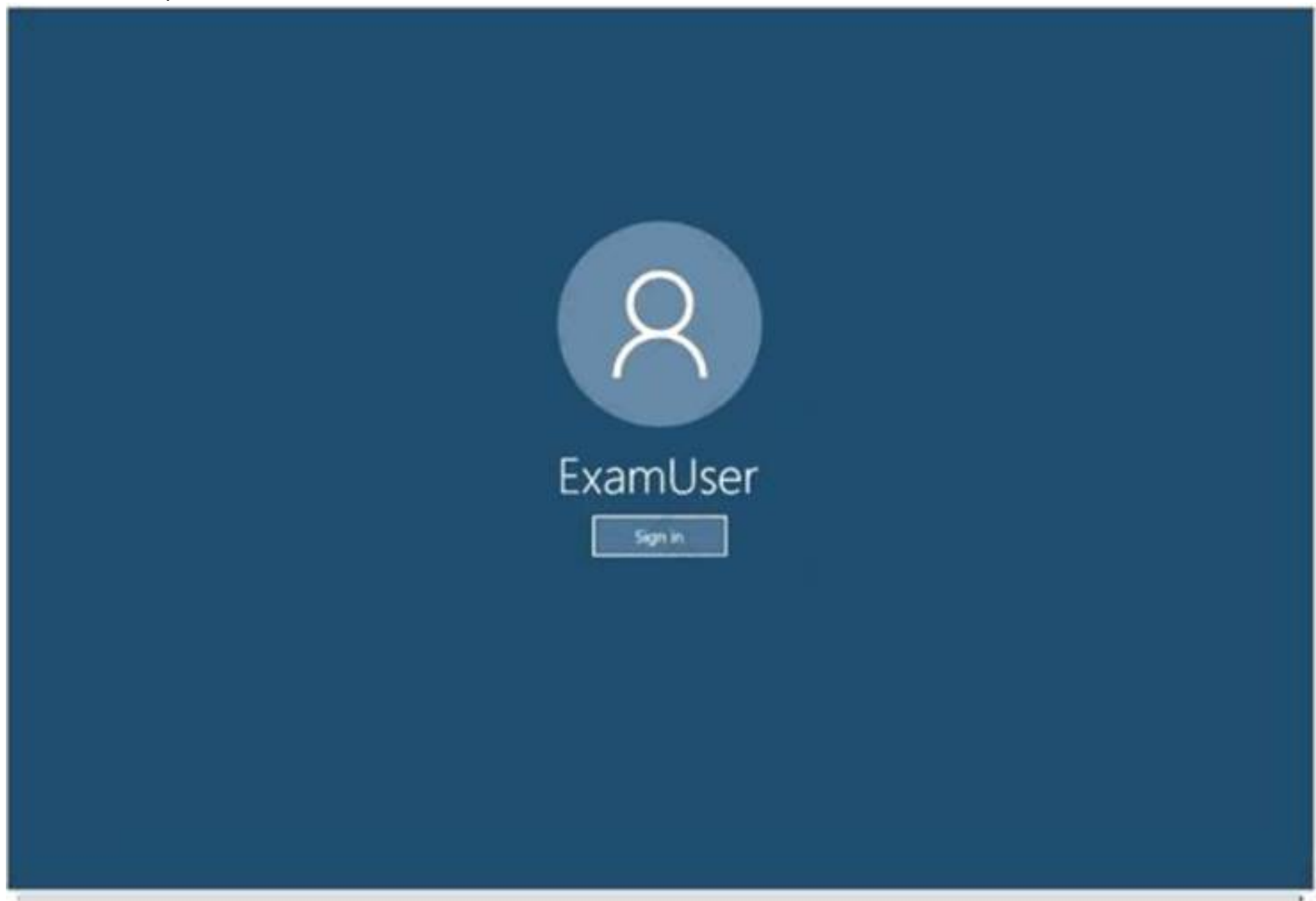
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username: admin@LODSe244001@onmicrosoft.com Microsoft 365 Password: &=Q8v@2qGzYz

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support only: Lab instance: 11032396

You need to ensure that group owners renew their Office 365 groups every 180 days. To complete this task, sign in to the Microsoft Office 365 admin center.

- A. Mastered
- B. Not Mastered

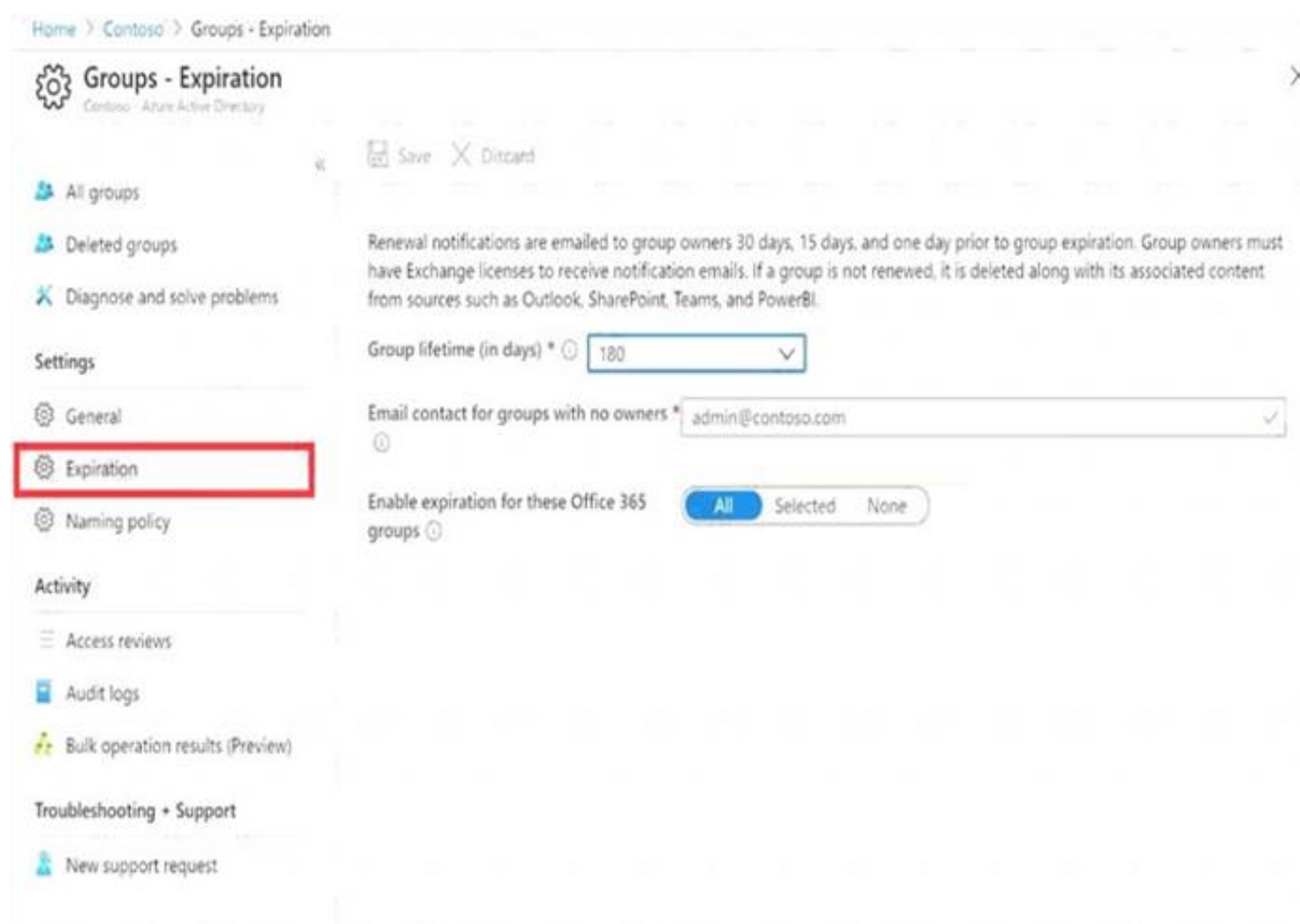
**Answer:** A

#### Explanation:

Set group expiration

\* 1. Open the Azure AD admin center with an account that is a global administrator in your Azure AD organization.

\* 2. Select Groups, then select Expiration to open the expiration settings.



\* 3. On the Expiration page, you can:

- Set the group lifetime in days. You could select one of the preset values, or a custom value (should be 31 days or more).
- Specify an email address where the renewal and expiration notifications should be sent when a group has no owner.
- Select which Office 365 groups expire. You can set expiration for:
- All Office 365 groups
- A list of Selected Office 365 groups
- None to restrict expiration for all groups

Save your settings when you're done by selecting Save. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-lifecycle>

#### NEW QUESTION 159

- (Exam Topic 4)

Your company has a Microsoft 365 subscription that includes a user named User1. You suspect that User1 sent email messages to a competitor detailing company secrets.

You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted. What should you include in the recommendation?

- A. Enable In-Place Archiving for the mailbox of User1
- B. From the Security & Compliance, perform a content search of the mailbox of User1
- C. Place a Litigation Hold on the mailbox of User1
- D. Configure message delivery restrictions for the mailbox of User1

**Answer: C**

#### NEW QUESTION 160

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription and 5,000 users.

You create several alert policies that are triggered every time activities match rules.

You need to create an alert policy that is triggered when the volume of matched activities becomes unusual. What should you do first?

- A. Enable Microsoft Office 365 auditing.
- B. Enable Microsoft Office 365 analytics.
- C. Enable Microsoft Office 365 Cloud App Security.
- D. Deploy a Microsoft Office 365 add-in to all the users.

**Answer: B**

#### NEW QUESTION 165

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1.

User1 needs to be able to create Data Subject Requests (DSRs) in the Microsoft 365 compliance center. To which role or role group should you add User1?

- A. the Compliance Data Administrator role
- B. the Data Investigator role
- C. the eDiscovery Manager role
- D. the Records Management role group

**Answer: C**



#### NEW QUESTION 168

- (Exam Topic 4)

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E5 license. How long will auditing data be retained?

- A. 30 days
- B. 90 days
- C. 365 days
- D. 5 years

**Answer:** B

#### Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

#### NEW QUESTION 169

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1.

The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1. For User1, you select Confirm user compromised.

User1 can still sign in.

You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.

Solution: You configure the user risk policy to block access when the user risk level is medium and higher. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 174

- (Exam Topic 4)

You have a Microsoft 365 subscription that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

You have a custom compliance manager template named Regulation1. You have the assessments shown in the following table.

Name	Score	Status	Group	Product	Regulation
Assessment1	1200	Incomplete	Group1	Microsoft 365	Regulation1
Assessment2	900	Incomplete	Group2	Microsoft 365	Regulation2

Assessment1 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Enable multi-factor authentication for admins	Failed high risk	+27 points	0/27	Technical
Enable multi-factor authentication for non-admins	Failed high risk	+27 points	0/27	Technical

Assessment2 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Establish a threat intelligence program	None	+9 points	0/9	Operational
Configure a privileged access policy	Failed high risk	+15 points	0/15	Technical

You perform the following actions:

➤ Enable multi-factor authentication (MFA) for all users.

➤ Configure a privileged access policy.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	<input type="radio"/>	<input type="radio"/>
The Assessment1 score will increase by only 54 points.	<input type="radio"/>	<input type="radio"/>
The Assessment2 score will increase by only 78 points.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o>

**NEW QUESTION 179**

- (Exam Topic 4)

You have a Microsoft 365 subscription and a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) subscription.

You have devices enrolled in Microsoft Endpoint Manager as shown in the following table:

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You integrate Microsoft Defender ATP and Endpoint Manager.

You plan to evaluate the Microsoft Defender ATP risk level for the devices. You need to identify which devices can be evaluated.

Which devices should you identify?

- A. Device1 and Device2 only
- B. Device1 only
- C. Device1 and Device3 only
- D. Device2 and Device3 only

**Answer:** B

**Explanation:**

Microsoft Defender ATP supports Windows 10, Windows Server, macOSX, and Linux D18912E1457D5D1DDCBD40AB3BF70D5D

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/evaluation-lab> <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/minimumrequireme>

**NEW QUESTION 180**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy. You need to configure the retention duration for the attachments in quarantine. Which type of threat management policy should you create?

- A. Anti-malware
- B. DKIM
- C. Anti-spam
- D. ATP anti-phishing

**Answer:** A

**NEW QUESTION 185**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Teams and contains a user named User1. You configure information barriers.

You need to identify which information barrier policies apply to User1. Which cmdlet should you use?

- A. Get-InformationBarrierRecipientStatus
- B. Get-InformationBarrierPoliciesApplicationStatus
- C. Get-InformationBarrierPolicy
- D. Get-OrganizationSegment

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/office365/troubleshoot/information-barriers/information-barriers-troubleshooti>

**NEW QUESTION 188**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

Your company uses Jamf Pro to manage macOS devices.

You plan to create device compliance policies for the macOS devices based on the Jamf Pro data. You need to connect Microsoft Endpoint Manager to Jamf Pro. What should you do first?

- A. From the Azure Active Directory admin center, add a Mobility (MDM and MAM) application.
- B. From the Endpoint Management admin center, add the Mobile Threat Defense connector.
- C. From the Endpoint Management admin center, configure Partner device management.
- D. From the Azure Active Directory admin center, register an application.

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf>

**NEW QUESTION 189**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.local that has a forest functional level of Windows Server 2008 R2.

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to install Azure AD Connect and enable single sign-on (SSO).

You need to prepare the domain to support SSO. The solution must minimize administrative effort. What should you do?

- A. Raise the forest functional level to Windows Server 2016.
- B. Modify the UPN suffix of all domain users.
- C. Populate the mail attribute of all domain users.
- D. Rename the domain.

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchro>

**NEW QUESTION 194**

- (Exam Topic 4)

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.

From the workspace, you plan to create a scheduled query rule that will use a custom query. The rule will be used to generate alerts when inbound access to Office 365 from specific user accounts is detected.

You need to ensure that when multiple alerts are generated by the rule, the alerts are consolidated as a single incident per user account.

What should you do?

- A. From Set rule logic, map the entities.
- B. From Analytic rule details, configure Severity.
- C. From Set rule logic, set Suppression to Off.
- D. From Analytic rule details, configure Tactics.

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/map-data-fields-to-entities>

**NEW QUESTION 196**

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes a user named User1.

You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.

You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.

Which type of Cloud App Security policy should you create?

- A. an app permission policy
- B. an activity policy
- C. a Cloud Discovery anomaly detection policy
- D. a session policy

**Answer:** D

**NEW QUESTION 200**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy to quarantine malware. You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create from the Security&Compliance admin center?

- A. ATP anti-phishing
- B. DKIM
- C. Anti-spam
- D. Anti-malware

**Answer:** D

**NEW QUESTION 203**

- (Exam Topic 4)

HOTSPOT

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD) as shown in the following exhibit.



## PROVISION FROM ACTIVE DIRECTORY



### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

### Azure AD Connect sync

Sync Status	Enabled
Last Sync	4.00 hours ago
Password Hash Sync	Enabled

## USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	1 agent

The synchronization schedule is configured as shown in the following exhibit.

```
Administrator: Windows PowerShell
PS C:\> Get-ADSyncScheduler

AllowedSyncCycleInterval       : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 00:30:00
CustomizedSyncCycleInterval    :
NextSyncCyclePolicyType        : Delta
NextSyncCycleStartTimeInUTC     : 1/28/2020 3:47:41 PM
PurgeRunHistoryInterval        : 7.00:00:00
SyncCycleEnabled               : True
MaintenanceEnabled             : True
StagingModeEnabled             : False
SchedulerSuspended             : False
SyncCycleInProgress            : False

PS C:\>
```

Use the drop-down menus to select the answer choice that answers each question based on the information presented in the graphic.  
 NOTE: Each correct selection is worth one point.

Which employees can authenticate by using Azure AD?

▼

☐ Only employees who have an Azure AD user account
 ☐ Employees who have an Azure AD user account and a synced on-premises account
 ☐ Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

▼

☐ Fix the synchronization server and install Azure AD Connect in staging mode
 ☐ Fix the synchronization server and install an additional authentication agent
 ☐ Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
 ☐ Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Which employees can authenticate by using Azure AD?

▼

☐ Only employees who have an Azure AD user account
 ☒ Employees who have an Azure AD user account and a synced on-premises account
 ☐ Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

▼

☐ Fix the synchronization server and install Azure AD Connect in staging mode
 ☒ Fix the synchronization server and install an additional authentication agent
 ☐ Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
 ☐ Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet



**NEW QUESTION 206**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

User	Security group	Azure Active Directory (Azure AD) role
User1	ADGroup1	Security administrator
User2	ADGroup2	Application administrator
User3	ADGroup3	User administrator

You have the devices shown in the following table.

Name	Operating system	Onboarded to Microsoft Defender for Endpoint
Device1	Windows 10	Yes
Device2	Windows 8.1	Yes
Device3	Windows 10	Yes

You have the Microsoft Defender for Endpoint portal roles shown in the following table.

Name	Assigned to
Role1	ADGroup1
Role2	ADGroup2
Role3	ADGroup3

You have the Microsoft Defender for Endpoint device groups shown in the following table.

Name	Remediation level	Rank	Role	Members
Group1	Full - remediate threats automatically	1	Role1	OS: Windows 10
Group2	Semi - require approval for all folders	2	Role2	OS: Windows 8.1
Group3	Semi - require approval for all folders	3	Role3	OS: Windows 10

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can manage alerts for Device2.	<input type="radio"/>	<input type="radio"/>
User3 can manage alerts for Device3.	<input type="radio"/>	<input type="radio"/>
The Remediation level for Device3 is Semi - require approval for all folders.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Statements	Yes	No
User1 can manage alerts for Device2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can manage alerts for Device3.	<input type="radio"/>	<input checked="" type="radio"/>
The Remediation level for Device3 is Semi - require approval for all folders.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 208**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Office 365 enabled. You need to review the zero-hour auto purge (ZAP) configuration for the subscription.

Which two threat policies should you review? Each correct answer presents part of the solution NOTE: Each correct selection is worth one point,

- A. Safe links Built-in protection (Microsoft)  
B. Office365 AntiPhish Default (Default)  
C. Anti-spam outbound policy (Default)  
D. Anti-malware (Default) Default  
E. Anti-spam inbound policy

F. Safe attachments Built-in protection (Microsoft)

**Answer:** CD

#### NEW QUESTION 209

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User 4.

Solution: You enable SSPR for Group2.

Does this meet the goal?

A. Yes

B. No

**Answer:** A

#### Explanation:

By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and Cloud application administrators.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-p>

#### NEW QUESTION 212

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 500 Windows 10 devices. The subscription uses Microsoft Defender for Endpoint and is integrated with Microsoft Endpoint Manager. All the devices have Defender for Endpoint deployed.

You create a Conditional Access policy as shown in the following table.

Setting	Value
Assignments: User and groups	All users
Assignments: Cloud apps or actions	All cloud apps
Access controls: Grant	Grant access: Require device to be marked as compliant

You need to ensure that devices that have a machine risk score of high are blocked. What should you do in Microsoft Endpoint Manager?

A. Apply a security baseline to all the devices.

B. Apply an endpoint detection and response policy to the subscription.

C. Configure the Compliance policy settings.

D. Apply a compliance policy to all the devices.

**Answer:** B

#### NEW QUESTION 216

- (Exam Topic 4)

You have a Microsoft 365 subscription.

All computers run Windows 10 Enterprise and are managed by using Microsoft Intune. You plan to view only security-related Windows telemetry data.

You need to ensure that only Windows security data is sent to Microsoft. What should you create from the Intune admin center?

A. a device configuration profile that has device restrictions configured

B. a device configuration profile that has the Endpoint Protection settings configured

C. a device configuration policy that has the System Security settings configured

D. a device compliance policy that has the Device Health settings configured

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry>

#### NEW QUESTION 218

- (Exam Topic 4)

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings: ➤ Assignments: Include Group1, Exclude Group2  
➤ Conditions: Sign in risk of Low and above  
➤ Access: Allow access, Require password multi-factor authentication

You need to identify how the policy affects User1 and User2.  
What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

User1: 

Blocked

Can sign in without MFA

Prompted for MFA

User2: 

Blocked

Can sign in without MFA

Prompted for MFA

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1: 

Blocked

Can sign in without MFA

Prompted for MFA

User2: 

Blocked

Can sign in without MFA

Prompted for MFA

NEW QUESTION 222

- (Exam Topic 4)  
You have a Microsoft 365 subscription.  
Some users access Microsoft SharePoint Online from unmanaged devices. You need to prevent the users from downloading, printing, and synching files. What should you do?

- A. Run the Set-SPODataConnectionSetting cmdlet and specify the AssignmentCollection parameter
- B. From the SharePoint admin center, configure the Access control settings
- C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
- D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Answer: B

NEW QUESTION 223

- (Exam Topic 4)  
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	Security administrator
User3	Security operator
User4	User administrator

You need to identify which user can enable Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) roles. Which user should you identify?

- A. User1
- B. User4
- C. User3
- D. User2

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/rbac>

**NEW QUESTION 228**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You create and run a content search from the Security & Compliance admin center. You need to download the results of the content search.

What should you obtain first?

- A. an export key
- B. a password
- C. a certificate
- D. a pin

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results>

**NEW QUESTION 230**

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1. You plan to use Compliance Manager.

You need to ensure that User1 can assign Compliance Manager roles to users. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Compliance Manager Assessor
- B. Global Administrator
- C. Portal Admin
- D. Compliance Manager Administrator

**Answer:** C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/working-with-compliance-manager?view=o365-wo>

**NEW QUESTION 233**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them. When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-Mailbox -Identity "User1" -AuditEnabled \$true command. Does that meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>



NEW QUESTION 236

- (Exam Topic 4)

You company has a Microsoft 365 E5 subscription and a hybrid Azure active Directory named contoso.com. Contoso.com includes the following users:

Custom smart lockout

Lockout threshold 10

Lockout duration in seconds 60

Custom banned passwords

Enforce custom list Yes No

Custom banned password list Contoso

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit

You configure Password protection for Contoso.com as shown in the following exhibit.

Answer Area

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input type="radio"/>
User2 can change his password to CONT0\$0C0NT0\$0.	<input type="radio"/>	<input type="radio"/>
User3 can change his password to myCONT0\$0c0mp1exPWD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can change his password to CONT0\$0C0NT0\$0.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can change his password to myCONT0\$0c0mp1exPWD.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 240

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Configuration
DC1	Domain controller
Server1	Member server

You plan to implement Microsoft Defender for Identity for the domain. You install a Microsoft Defender for Identity standalone sensor on Server 1. You need to monitor the domain by using Microsoft Defender for Identity. What should you do?

- A. Configure port mirroring for DC1.
- B. Install the Microsoft Monitoring Agent on DC1.
- C. Configure port mirroring for Server1.
- D. Install the Microsoft Monitoring Agent on Server 1.

Answer: A

NEW QUESTION 242

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Permanent role assignment
User1	Global Administrator
User2	Security Administrator
User3	Privileged Role Administrator
User4	None

The User Administrator role is configured in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.

User Administrator

Save

Discard

Activations

Maximum activation duration (hours)

4

Notifications

Send email notifying admins of activation

Enable

Disable

Incident/Request ticket

Require incident/request ticket number during activation

Enable

Disable

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation

Enable

Disable

Require approval

Require approval to activate this role

Enable

Disable

If no approvers are selected, Privileged Role Administrators will be approvers by default.

SELECTED APPROVER

ACTION

No results

Select approvers

No approver selected

You make User4 eligible for the User Administrator role.  
For each of the following statements, select Yes if the statement is true. Otherwise, select No.  
NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input type="radio"/>
User2 receives an email notification when User4 activates the User Administrator role.	<input type="radio"/>	<input type="radio"/>
User3 receives an email notification when User4 requests activation of the User Administrator role.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Y,Y,Y

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications>

**NEW QUESTION 245**

- (Exam Topic 4)

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

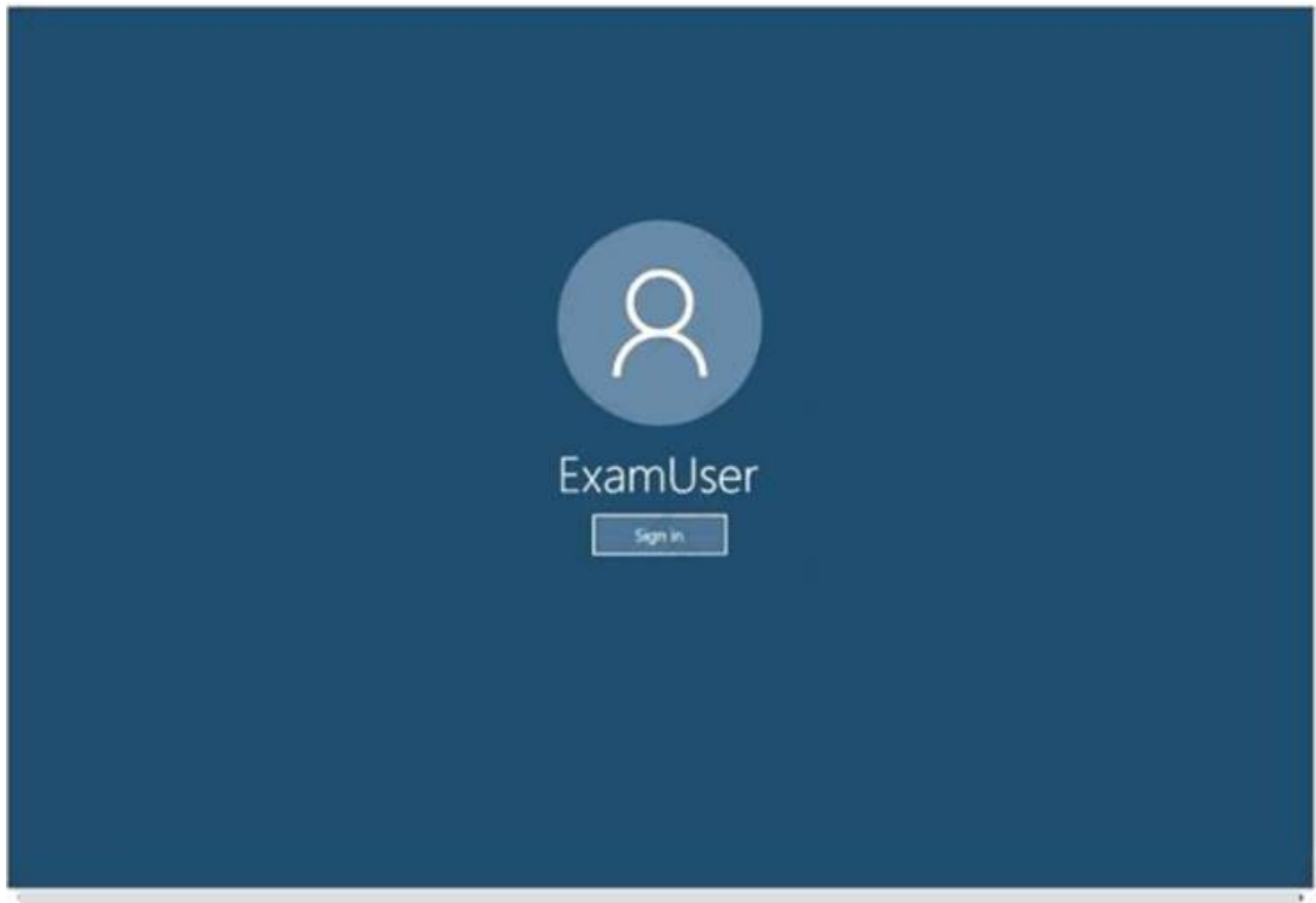
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username:

admin@LODSe244001@onmicrosoft.com Microsoft 365 Password: &=Q8v@2qGzYz

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support only: Lab instance: 11032396

You need to ensure that SharepointAdmins@contoso.com receives an alert when a user establishes a sync relationship to a document library from a computer that is a member of an Active Directory (AD) domain.

To complete this task, sign in to the Microsoft Office 365 admin center.

A. Mastered

B. Not Mastered

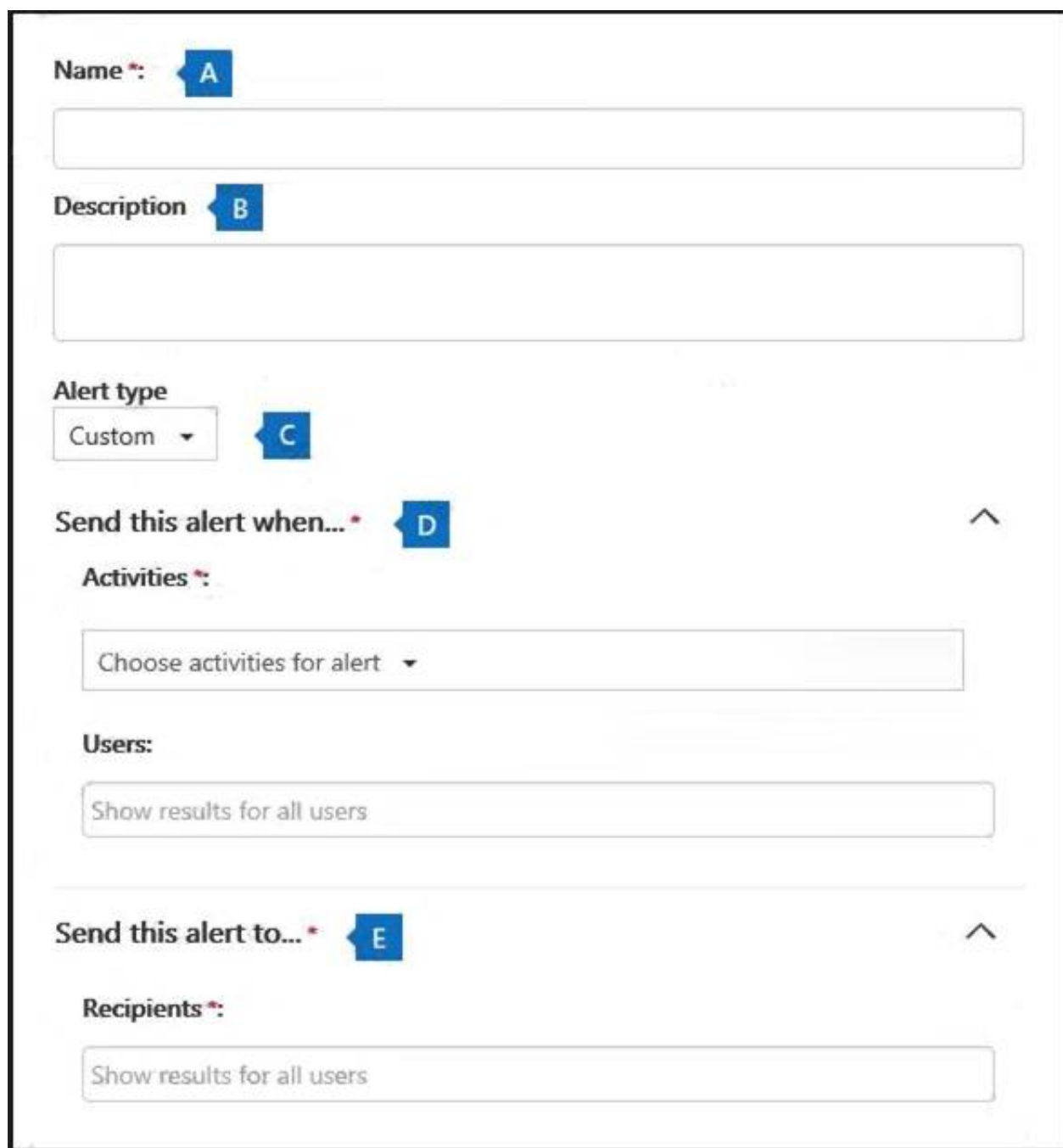
**Answer: A**

**Explanation:**

\* 1. Navigate to Manage Alerts in the Security & Compliance Center.

\* 2. On the Activity alerts page, click + New.

The flyout page to create an activity alert is displayed.



\* 3. Complete the following fields to create an activity alert:

\* a. Name - Type a name for the alert. Alert names must be unique within your organization.

\* b. Description (Optional) - Describe the alert, such as the activities and users being tracked, and the users that email notifications are sent to. Descriptions provide a quick and easy way to describe the purpose of the alert to other admins.

\* c. Alert type - Make sure the Custom option is selected.

\* d. Send this alert when - Click Send this alert when and then configure these two fields:

➤ Activities - Click the drop-down list to display the activities that you can create an alert for. This is the same activities list that's displayed when you search the Office 365 audit log. You can select one or more specific activities or you can click the activity group name to select all activities in the group. For a description of these activities, see the "Audited activities" section in Search the audit log. When a user performs any of the activities that you've added to the alert, an email notification is sent.

➤ Users - Click this box and then select one or more users. If the users in this box perform the activities that you added to the Activities box, an alert will be sent. Leave the Users box blank to send an alert when any user in your organization performs the activities specified by the alert.

\* e. Send this alert to - Click Send this alert, and then click in the Recipients box and type a name to add a user's who will receive an email notification when a user (specified in the Users box) performs an activity (specified in the Activities box). Note that you are added to the list of recipients by default. You can remove your name from this list.

\* 4. Click Save to create the alert.

The new alert is displayed in the list on the Activity alerts page.

Activity alerts			
Name	Recipients	Status ▲	Date modified
Executive mailbox alert	compliance@contoso.com	On	2016-06-08 14:42:02
SharePoint upload alert	admin@contoso.com	Off	2016-06-08 14:23:39
External sharing alert	admin@contoso.com	Off	2016-06-08 14:24:08

The status of the alert is set to On. Note that the recipients who will receive an email notification when an alert is sent are also listed.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-activity-alerts?view=o365-worldwide>

## NEW QUESTION 250

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. All the devices in the tenant are managed by using Microsoft Intune.

You purchase a cloud app named App1 that supports session controls. You need to ensure that access to App can be reviewed in real time.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



### Answer Area

#### Actions

From the Azure Active Directory admin center, register App1.

From the Cloud App Security admin center, create an access policy.

From the Cloud App Security admin center, create an app discovery policy.

From the Device Management admin center, create an app configuration policy.

From the Azure Active Directory admin center, create a conditional access policy.

From the Device Management admin center, add an App1.







- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

References:

<https://docs.microsoft.com/en-us/cloud-app-security/access-policy-aad>

#### NEW QUESTION 252

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Group	Role
User1	Group1	User administrator
User2	Group1	Security operator
User3	Group2	Security reader
User4	None	Global administrator

You enable self-service password reset for Group1 and configure security questions as the only authentication method for self-service password reset. You need to identify which user must answer security questions to reset his password. Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

**Answer:** B

#### NEW QUESTION 256

- (Exam Topic 4)

An administrator plans to deploy several Azure Advanced Threat Protection (ATP) sensors.

You need to provide the administrator with the Azure information required to deploy the sensors. What information should you provide?

- A. an Azure Active Directory Authentication Library (ADAL) token
- B. the public key
- C. the access key
- D. the URL of the Azure ATP admin center

**Answer:** D

#### Explanation:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/workspace-portal>

#### NEW QUESTION 260

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.

You need to implement a data loss prevention (DLP) solution that meets the following requirements:

- Email messages that contain a single customer identifier can be sent outside your company.
- Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.

Which two components should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. a sensitive information type
- B. a sensitivity label
- C. a retention label
- D. a DLP policy
- E. a mail flow rule

**Answer:** AD

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-entity-definitions?view=>

**NEW QUESTION 261**

- (Exam Topic 4)

You have a hybrid Microsoft 365 deployment that contains the Windows 10 devices shown in the following table.

Name	Trusted Platform Module (TPM) version	Joined to	Microsoft Intune enrolled
Device1	v2.0	Active Directory	Yes
Device2	v2.0	Azure Active Directory (Azure AD)	Yes
Device3	v1.3	Azure Active Directory (Azure AD)	Yes

You assign a Microsoft Endpoint Manager disk encryption policy that automatically and silently enables BitLocker Drive Encryption (BitLocker) on all the devices. Which devices will have BitLocker enabled?

- A. Device 1, Device2, and Device3
- B. Device2 only
- C. Device1 and Device2 only
- D. Device2 and Device3 only

**Answer:** B

**Explanation:**

To silently enable BitLocker, the device must be Azure AD Joined or Hybrid Azure AD Joined and the device must contain TPM (Trusted Platform Module) 2.0.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

**NEW QUESTION 262**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.

Which type of site collection should you create first?

- A. Records Center
- B. Compliance Policy Center
- C. eDiscovery Center
- D. Enterprise Search Center
- E. Document Center

**Answer:** C

**Explanation:**

Reference:

<https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bbb9>

**NEW QUESTION 265**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.

You use the System event log on Server1. Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

References:

<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

#### NEW QUESTION 267

- (Exam Topic 4)

Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them. Solution: You modify the encryption settings of the label.

Does this meet the goal?

A. Yes

B. No

**Answer: B**

#### NEW QUESTION 268

- (Exam Topic 4)

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user named User1. You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege. Which role should you assign to User1?

A. the View-Only Audit Logs role in the Security & Compliance admin

B. the Security reader role in the Azure Active Directory admin center

C. the View-Only Audit Logs role in the Exchange admin center

D. the Compliance Management role in the Exchange admin center

**Answer: C**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?vi>

#### NEW QUESTION 270

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.

You use the Security event log on Server1. Does that meet the goal?

A. Yes

B. No

**Answer: B**

#### Explanation:

References:

<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

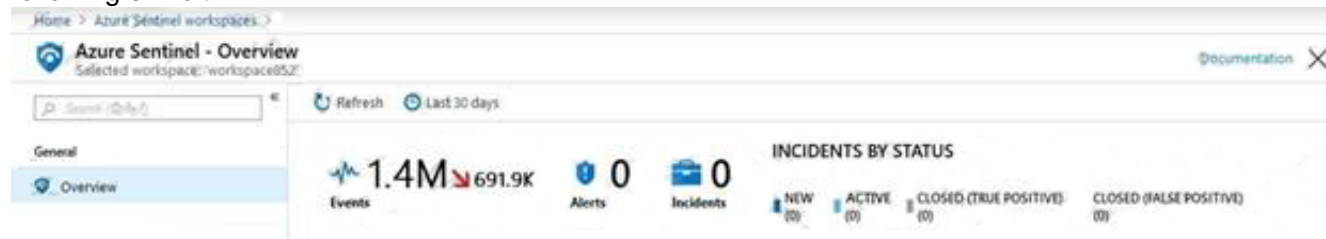
#### NEW QUESTION 271

- (Exam Topic 4)

You create an Azure Sentinel workspace.

You configure Azure Sentinel to ingest data from Azure Active Directory (Azure AD).

In the Azure Active Directory admin center, you discover Azure AD Identity Protection alerts. The Azure Sentinel workspace shows the status as shown in the following exhibit.



In Azure Log Analytics, you can see Azure AD data in the Azure Sentinel workspace.

What should you configure in Azure Sentinel to ensure that incidents are created for detected threats?

A. data connectors

B. rules

C. workbooks

D. hunting queries

**Answer: B**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom>

#### NEW QUESTION 275

- (Exam Topic 4)

You plan to add a file named ConfidentialHR.docx to a Microsoft SharePoint library.

You need to ensure that a user named Megan Bowen is notified when another user accesses ConfidentialHR.xlsx.

To complete this task, sign in to the Microsoft 365 portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

You need to configure an alert policy.

- Go to the Security & Compliance Admin Center.
- Navigate to Alerts > Alert Policies.
- Click on + New alert policy to create a new policy.
- Give the policy a name and select a severity level. For example: Medium.
- In the Category section, select Information Governance and click Next.
- In the Select an activity section, select Any file or folder activity.
- Click Add a condition and select File name.
- Type in the filename ConfidentialHR.xlsx and click Next.
- In the email recipients section, add Megan Bowen and click Next.
- Click Finish to create the alert policy.

**NEW QUESTION 277**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### MS-500 Practice Exam Features:

- \* MS-500 Questions and Answers Updated Frequently
- \* MS-500 Practice Questions Verified by Expert Senior Certified Staff
- \* MS-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* MS-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The MS-500 Practice Test Here](#)**