



Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator

NEW QUESTION 1

- (Exam Topic 1)

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

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

Set the frequency to:

One time	v
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Set the frequency to:

One time	v
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

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 v Access reviews v Export Refresh

Assignment type

All v

Search

Q 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)

Which IP address space should you include in the MFA configuration?

- A. 131.107.83.0/28
- B. 192.168.16.0/20
- C. 172.16.0.0/24
- D. 192.168.0.0/20

Answer: B

NEW QUESTION 5

- (Exam Topic 2)

You need to configure threat detection for Active Directory. The solution must meet the security requirements.

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

- Configure the Directory services setting in Azure ATP
- Download and install the ATA Gateway on DC1, DC2, and DC3
- Download and install the Azure ATP sensor package on DC1, DC2, and DC3
- Configure a site-to-site VPN
- Create a workspace in Azure ATP
- Download and install the ATA Center on Server1

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- Configure the Directory services setting in Azure ATP
- Download and install the ATA Gateway on DC1, DC2, and DC3
- Download and install the Azure ATP sensor package on DC1, DC2, and DC3
- Configure a site-to-site VPN
- Create a workspace in Azure ATP
- Download and install the ATA Center on Server1

Answer Area

Create a workspace in Azure ATP

Download and install the Azure ATP sensor package on DC1, DC2, and DC3

Configure the Directory services setting in Azure ATP

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)

What should User6 use to meet the technical requirements?

- A. Supervision in the Security & Compliance admin center
- B. Service requests in the Microsoft 365 admin center
- C. Security & privacy in the Microsoft 365 admin center
- D. Data subject requests in the Security & Compliance admin center

Answer: B

NEW QUESTION 8

- (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.

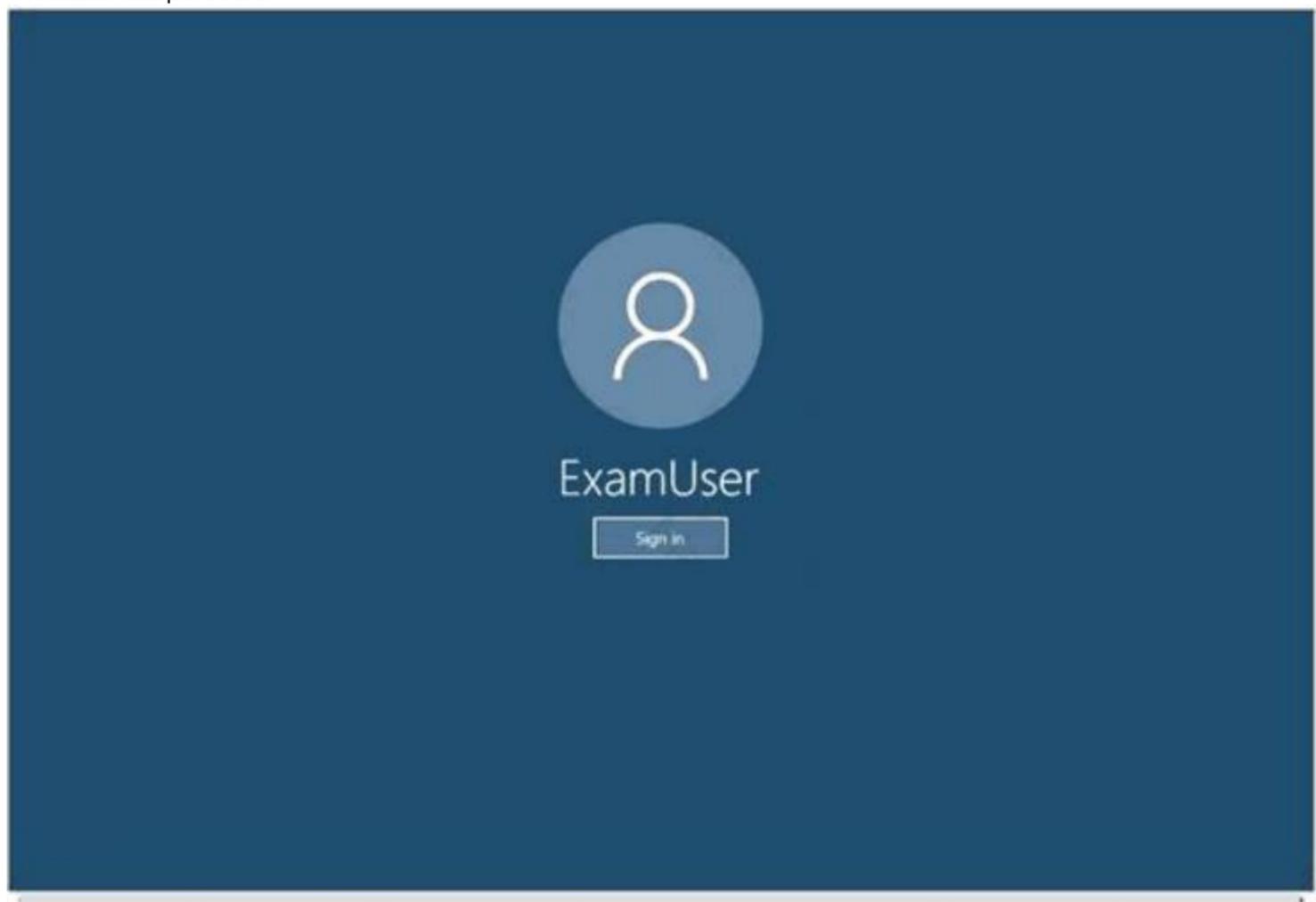
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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.

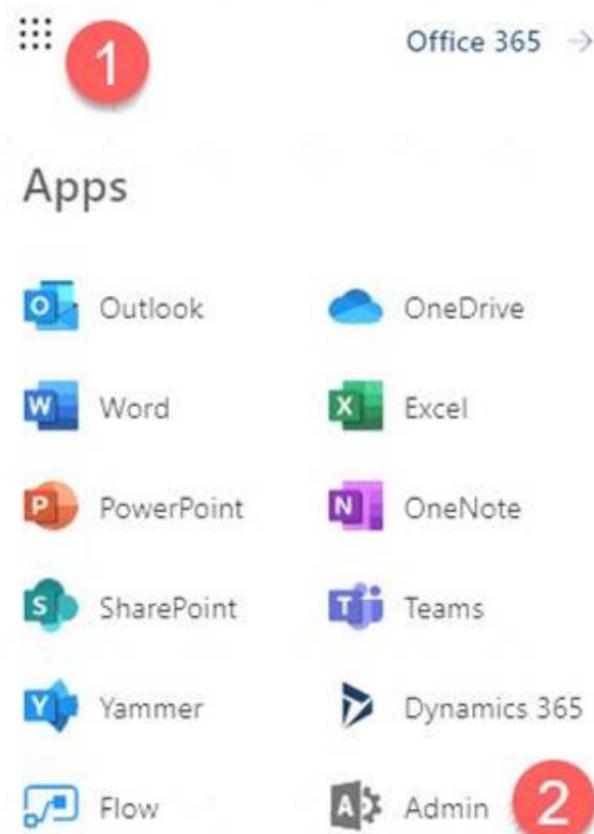
➤ In the details pane, click More options.

➤ Under Retention Policy, click Update.

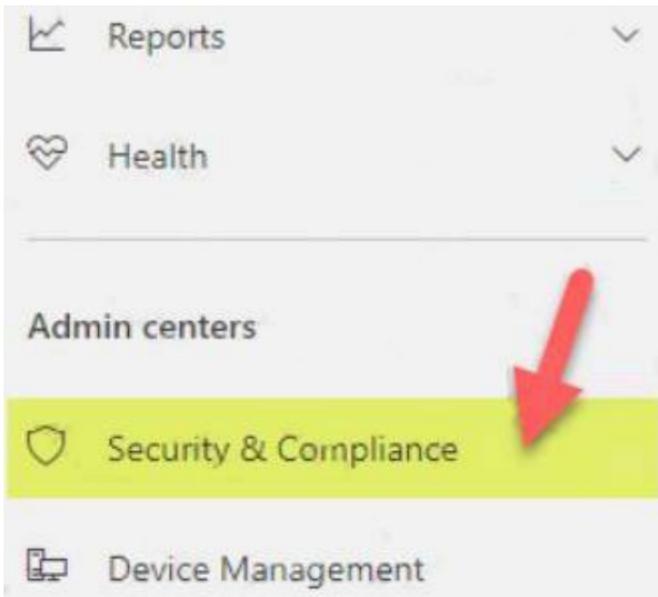
➤ In Bulk Assign Retention Policy, select the retention policy you want to apply to the mailboxes, and then click Save.

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

* 1. Navigate to the Office 365 Admin Centers

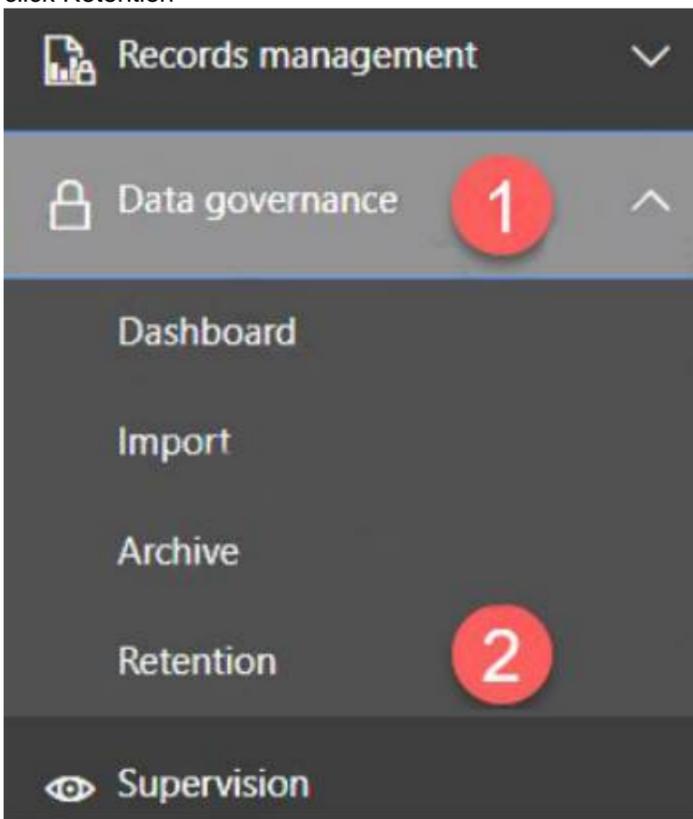


* 2. From the list of available Admin Centers, click on Security & Compliance



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

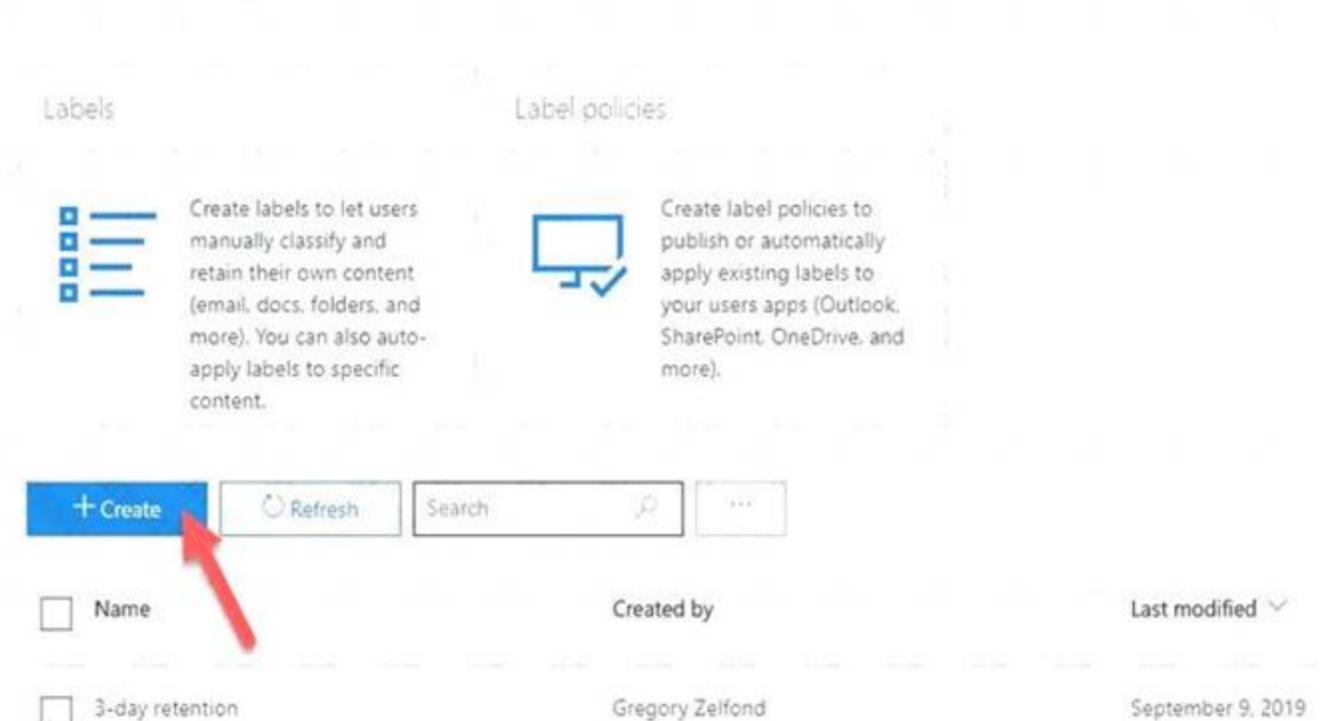
Now that we are in the Security & Compliance Admin Center, we are ready to create and publish a Retention Policy on a SharePoint site. Under Data Governance, click Retention



* 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](#)



* 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 * 1

Description 2

3

* 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 1

For this long... days 1

Retain the content based on 2

Do you want us to delete it after this time? Yes No 3

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 years

Need more options?
 Use advanced retention settings

4

* 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 type="checkbox"/>	Exchange email		
<input type="checkbox"/>	SharePoint sites		
<input type="checkbox"/>	OneDrive accounts		
<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

✔ 1 group added

Choose groups

^ Groups (1) Clear all

Finance Team

FinanceTeam@sharepointmaven.com

* 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.

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

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name: Retain for 2 days, then delete Edit

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

Applies to content in these locations: SharePoint sites Edit

Settings Edit

Retention period: Keep content, and delete it if it's older than 2 days

⚠ Content that's currently older than this will be deleted after you turn on the policy.

Buttons: Back, Save for later, **Create this policy**, Cancel

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 9

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You create an attack surface reduction policy that uses an application control profile as shown in the following exhibit.

Microsoft Endpoint Manager admin center

Home > Endpoint security > Attack surface reduction >

Create profile

Application control

Basics Configuration settings Scope tags Assignments Review + create

Summary

Basics

Name: ApplicationControlPolicy1
 Description: ...
 Platform: Windows 10 and later

Configuration settings

App locker application control: Enforce Components, Store Apps, and Smartlocker
 Turn on Windows SmartScreen: Yes

Scope tags

...

Assignments

Included groups: Group1
 Excluded groups: Group2

Buttons: Previous, **Create**

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.

When only a member of Group1 connects to a site that is identified as dangerous by application control, [answer choice]

<input type="text"/>	▼
the site will open without warning	
the site will be blocked from opening	
the member will receive a security warning	

When only a member of Group2 connects to a site that is identified as dangerous by application control, [answer choice]

<input type="text"/>	▼
the site will open without warning	
the site will be blocked from opening	
the member will receive a security warning	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: the member will receive a security warning. Group1 is included in the policy so SmartScreen will be enabled. SmartScreen will display a warning. Box 2: the site will open without warning. Group2 is excluded from the policy so SmartScreen will not be enabled. Therefore, no warning will be displayed.

NEW QUESTION 10

- (Exam Topic 4)

You have a Microsoft 365 subscription for a company named Contoso, Ltd. All data is in Microsoft 365. Contoso works with a partner company named Litware, Inc. Litware has a Microsoft 365 subscription. You need to allow users at Contoso to share files from Microsoft OneDrive to specific users at Litware. Which two actions should you perform from the OneDrive admin center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Increase the permission level for OneDrive External sharing
- B. Modify the Links settings
- C. Change the permissions for OneDrive External sharing to the least permissive level
- D. Decrease the permission level for OneDrive External sharing
- E. Modify the Device access settings
- F. Modify the Sync settings

Answer: BD

Explanation:

References:
<https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>

NEW QUESTION 10

- (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:

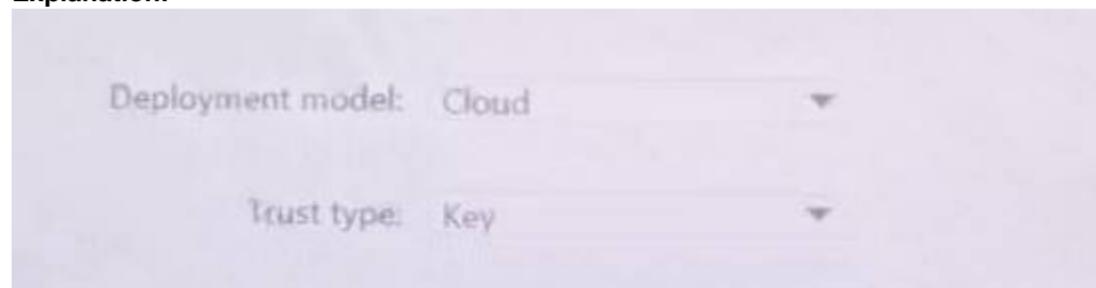
- Ensure that users can access Microsoft 365 services and on-premises resources.
- Minimize administrative efforts

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 13

- (Exam Topic 4)

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 User5. Solution: You assign the eDiscovery Manager role to Admin1, and then create an eDiscovery case. Does this meet the goal?

- A. Yes

B. No

Answer: A

Explanation:

References:

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

NEW QUESTION 16

- (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.

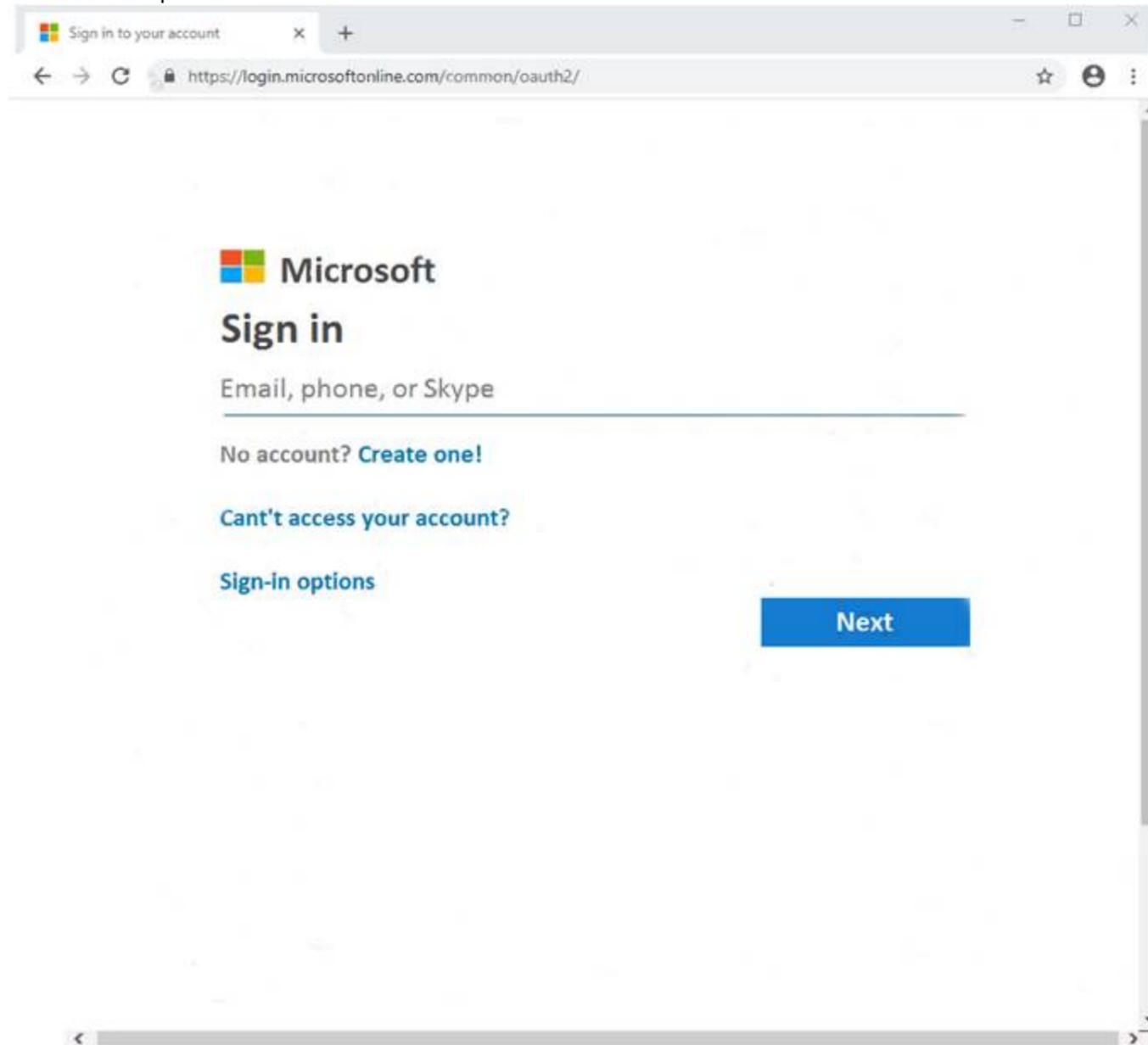
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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



Get your work done
with **Office 365**

● ● ● ● ●

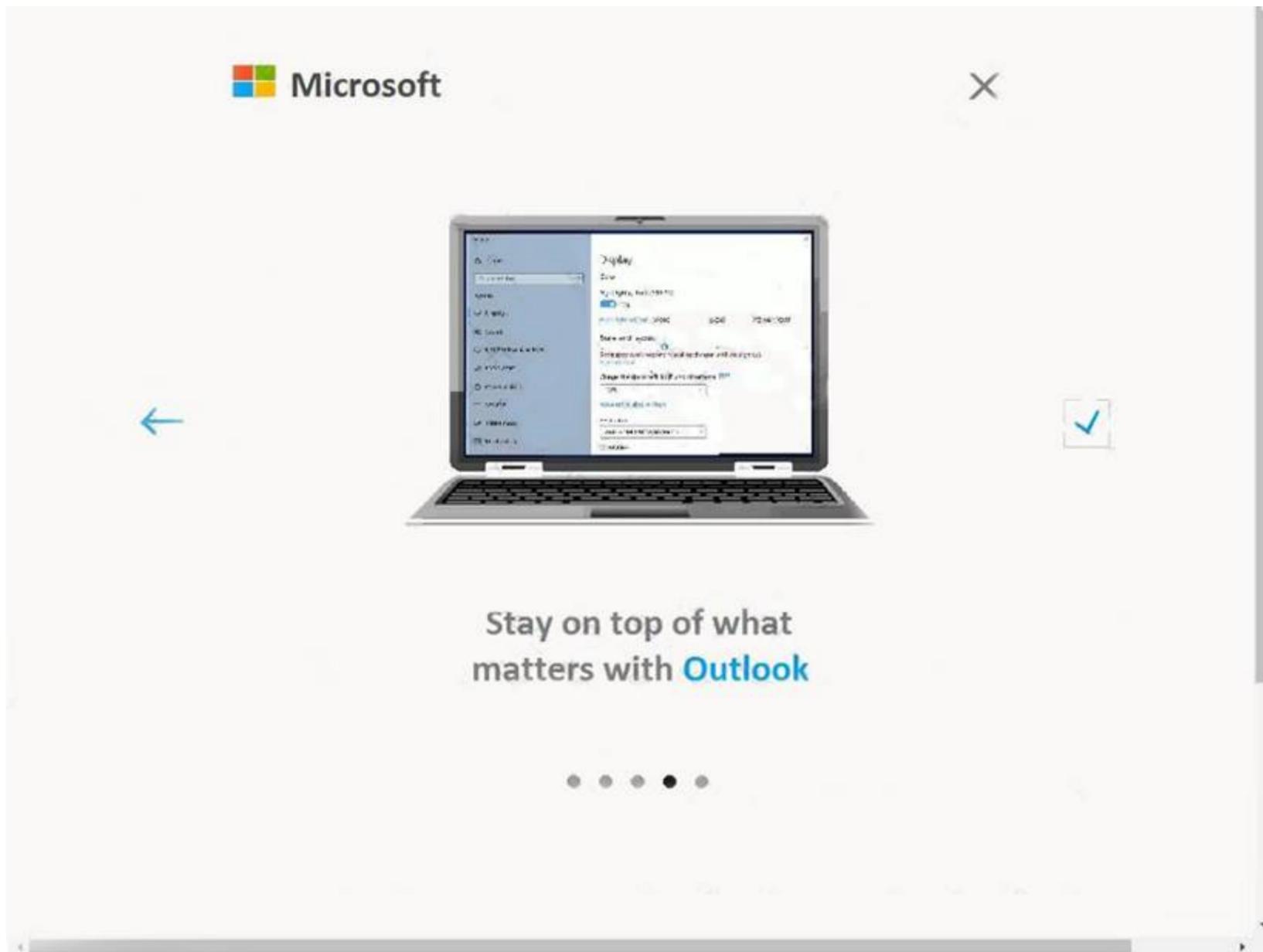
Microsoft



←

Brainstorm
together in **Word**

● ● ● ● ●



Microsoft

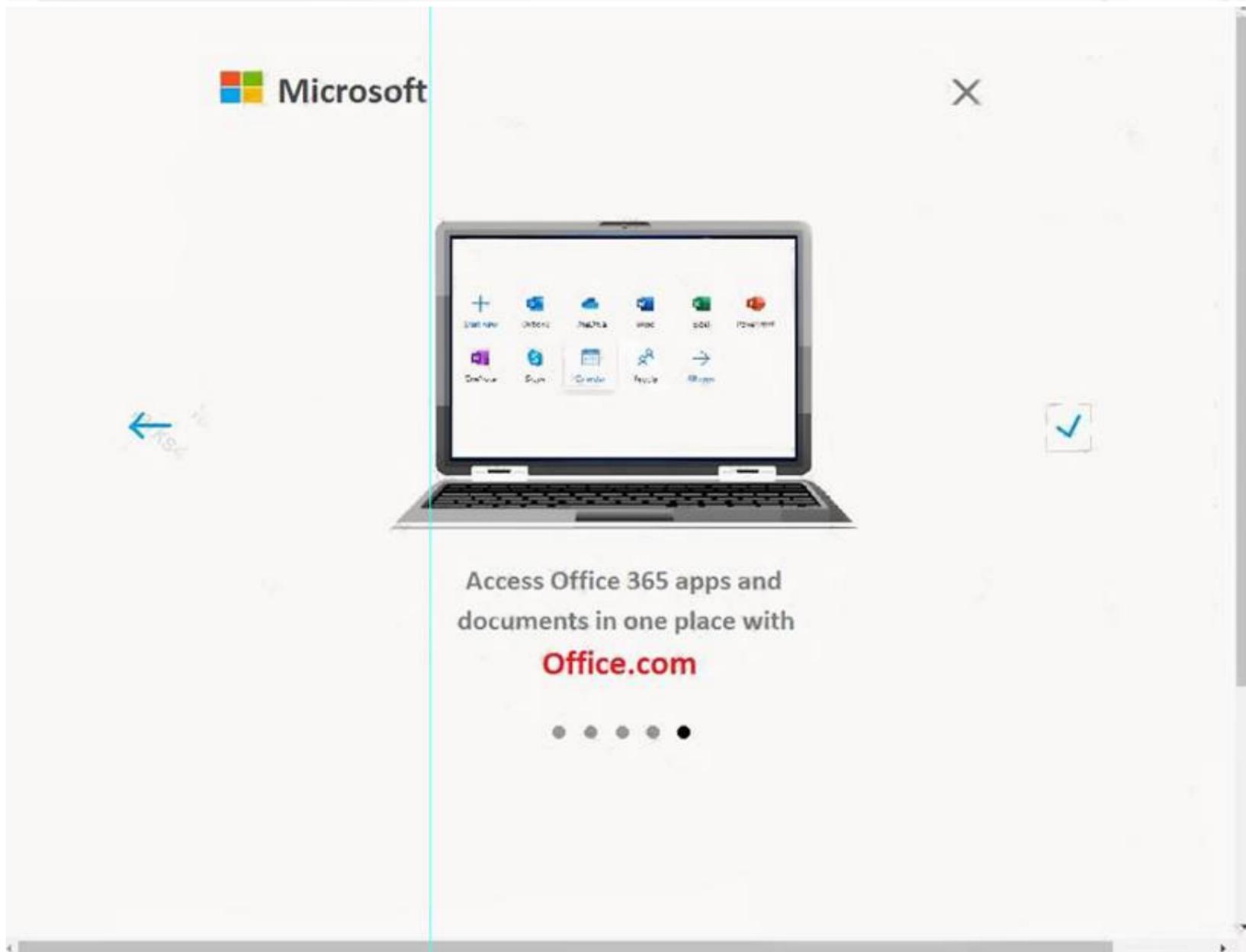


Stay on top of what matters with **Outlook**

Navigation icons: back, forward, search, refresh, close, checkmark

Progress indicator: 5 dots, 4th dot active

Vertical scrollbar on the right



Microsoft



Access Office 365 apps and documents in one place with **Office.com**

Navigation icons: back, forward, search, refresh, close, checkmark

Progress indicator: 5 dots, 5th dot active

Vertical scrollbar on the right

Microsoft Office Home
office.com/7a1rhu12

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
Intearted Team Sales Process
Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15
Word
Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

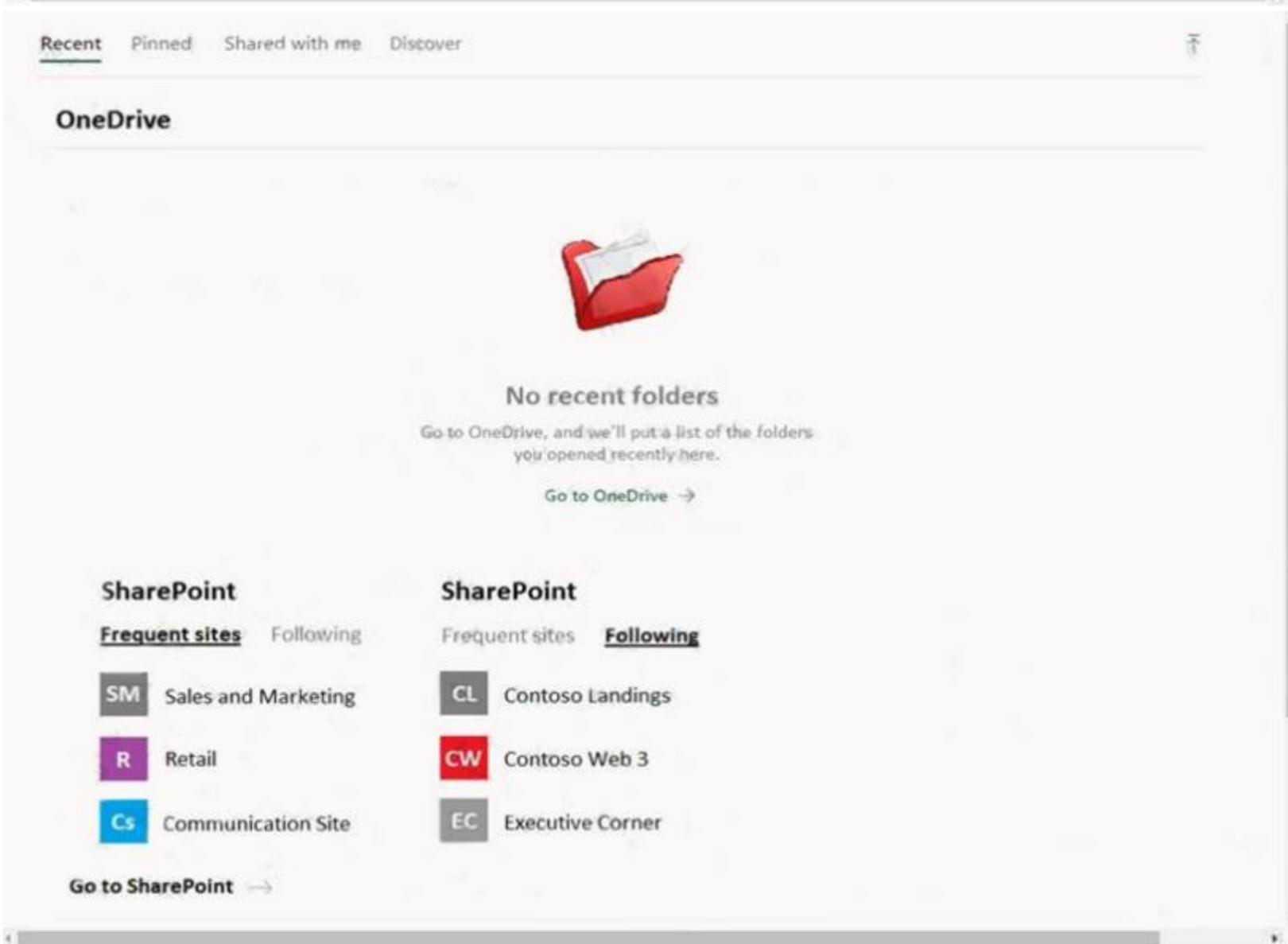
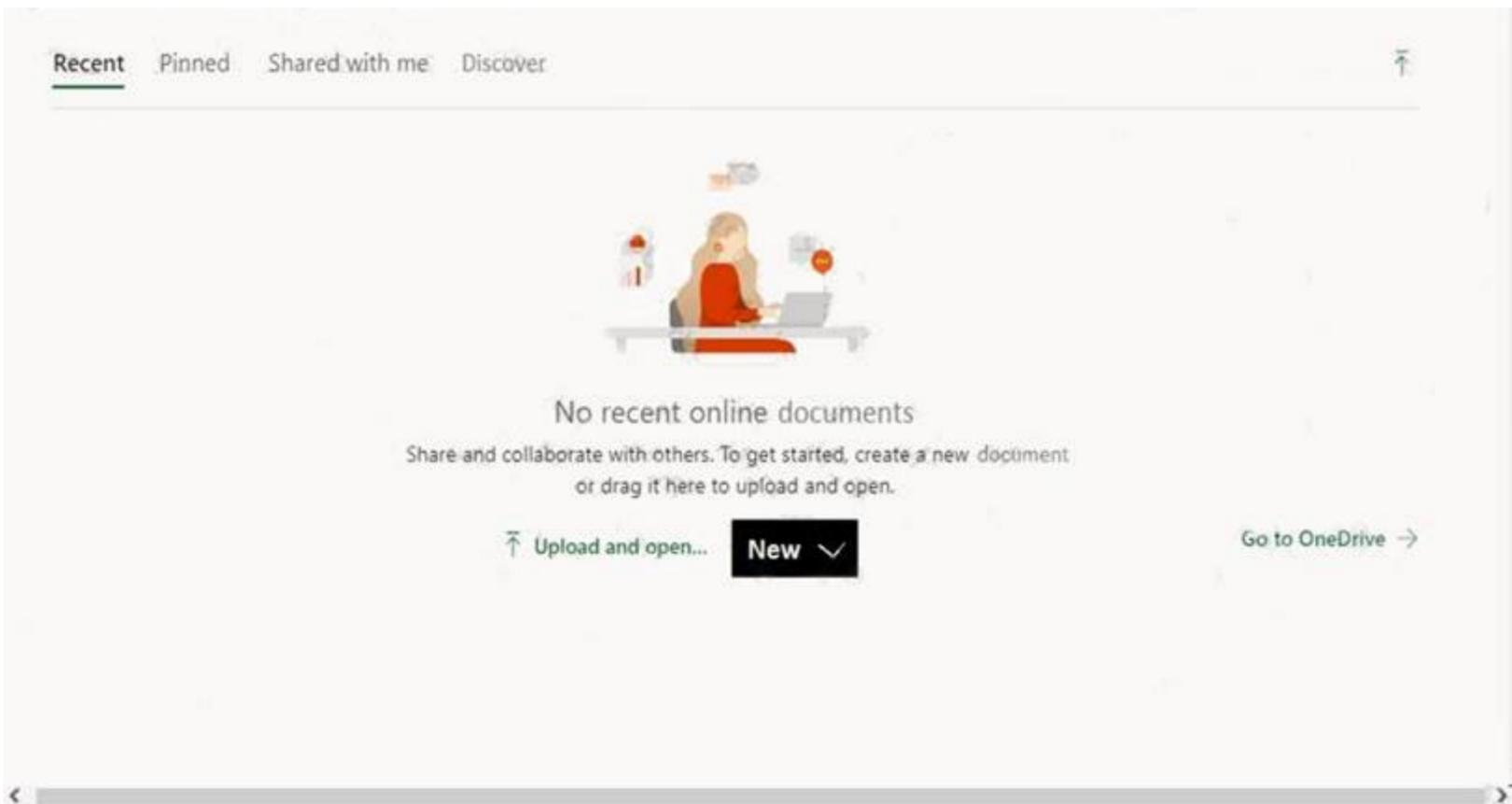
Recommended

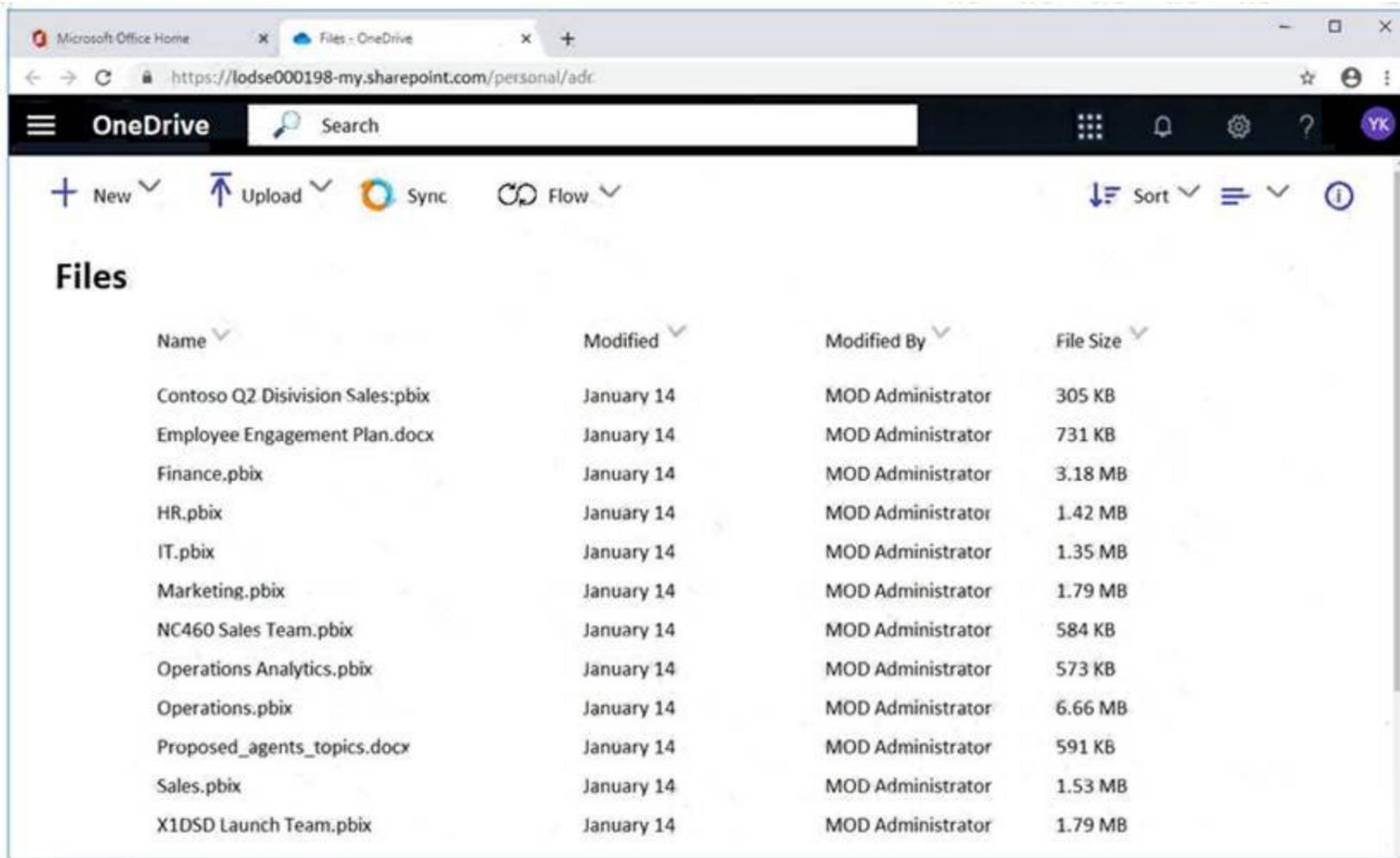
You edited this Jan 15
Excel
P and L Summary
lodse000198.sharepoint.co...

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





You need to ensure that a user named Allan Deyoung uses multi-factor authentication (MFA) for all authentication requests. To complete this task, sign in to the Microsoft 365 admin center.

- A. Mastered
- B. Not Mastered

Answer: A

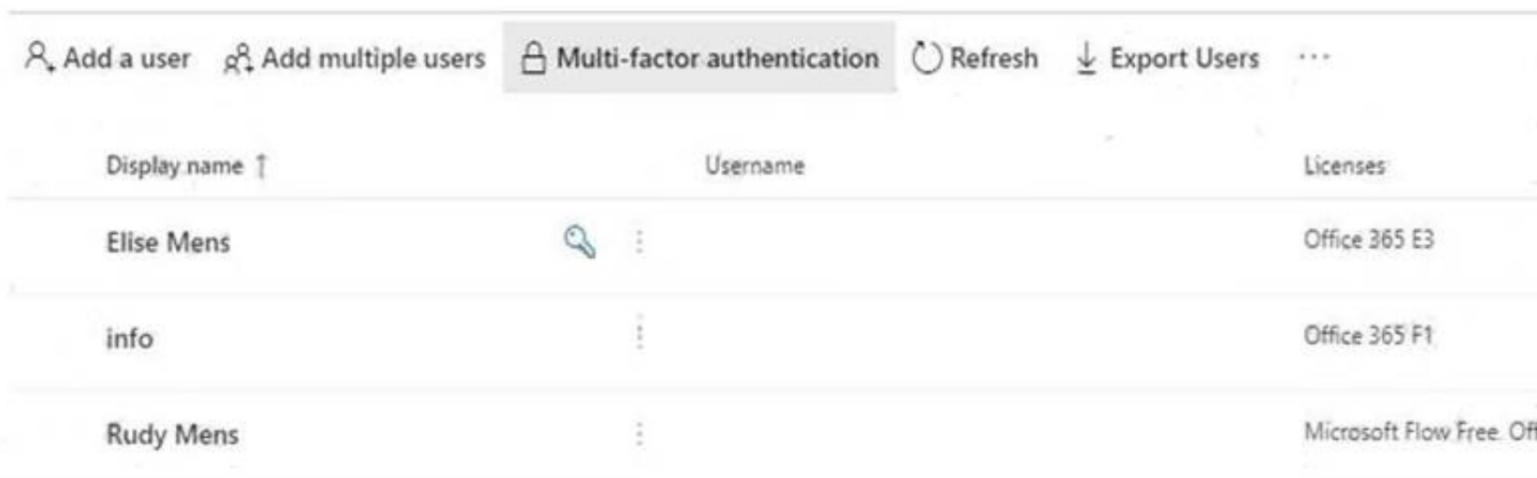
Explanation:

- * 1. Open the Admin Center and go to Users > Active Users
- * 2. Open Multi-factor authentication

Don't select any user yet, just open the Multi-factor authentication screen. You will find the button in the toolbar.

LazyAdmin.nl

Active users



* 3. Open the Service settings Before we start enabling MFA for the users, we first go through the service settings. The button to the settings screen doesn't stand out, but it's just below the title

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to get started. Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

View: Sign-in allowed users Multi-Factor Auth status: Any

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Elise Mens		Disabled
<input type="checkbox"/>	info		Disabled
<input type="checkbox"/>	Rudy Mens		Disabled

* 4. Setup MFA Office 365

A few settings are important here:

- > Make sure you check the App password. Otherwise, users can't authenticate in some applications (like the default mail app in Android).
- > Also, take a look at the remember function. By default, it is set to 14 days.

multi-factor authentication

users service settings

app passwords

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication

- Allow users to remember multi-factor authentication on devices they trust
 Days before a device must re-authenticate (1-60):

save

* 5. Enable MFA for Office 365 users

After you have set the settings to your liking click on save and then on users (just below the title Multi-factor authentication).

You see the list of your users again. Here you can select single or multiple users to enable MFA.

At the moment you enable Office 365 MFA for a user it can get the setup screen as soon as the users browse to one of the Office 365 products.

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

View: Multi-Factor Auth status:

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Elise Mens		Disabled
<input type="checkbox"/>	info		Disabled
<input checked="" type="checkbox"/>	Rudy Mens		Disabled

Rudy Mens

quick steps

Enable

Manage user settings

Reference:

<https://lazyadmin.nl/office-365/how-to-setup-mfa-in-office-365/>

NEW QUESTION 17

- (Exam Topic 4)

You have a Microsoft 365 E3 subscription.

You plan to audit all Microsoft Exchange Online user and admin activities.

You need to ensure that all the Exchange audit log records are retained for one year. What should you do?

- A. Modify the retention period of the default audit retention policy.
- B. Create a custom audit retention policy.
- C. Assign Microsoft 365 Enterprise E5 licenses to all users.
- D. Modify the record type of the default audit retention policy.

Answer: C

Explanation:

Reference:

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

NEW QUESTION 20

- (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 23

- (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 28

- (Exam Topic 4)

You have a Microsoft 365 Enterprise E5 subscription.

You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You plan to use Microsoft Office 365 Attack simulator.

What is a prerequisite for running Attack simulator?

- A. Enable multi-factor authentication (MFA)
- B. Configure Advanced Threat Protection (ATP)
- C. Create a Conditional Access App Control policy for accessing Office 365
- D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

NEW QUESTION 31

- (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 35

- (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 Nock sharing with people on specific domains and add contoso.com.
- B. From the External sharing settings for OneDriv
- 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 OneDriv
- 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 39

- (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.

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 41

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	Exchangeltem	MailboxLogin	None	90 Days
20	AuditRetention2	Exchangeltem	Send, MailltemsAccessed	User1	9 Months
30	AuditRetention3	Sharepoint	None	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	None	10 Years

The users perform the following actions:

- > User1 renames a Microsoft SharePoint Online site.
- > User2 sends an email message.

How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1 renames a SharePoint site:

90 days
6 months
9 months
1 year
10 years

User2 sends an email message:

90 days
6 months
9 months
1 year
10 years

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated with medium confidence

Reference:

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

NEW QUESTION 43

- (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.

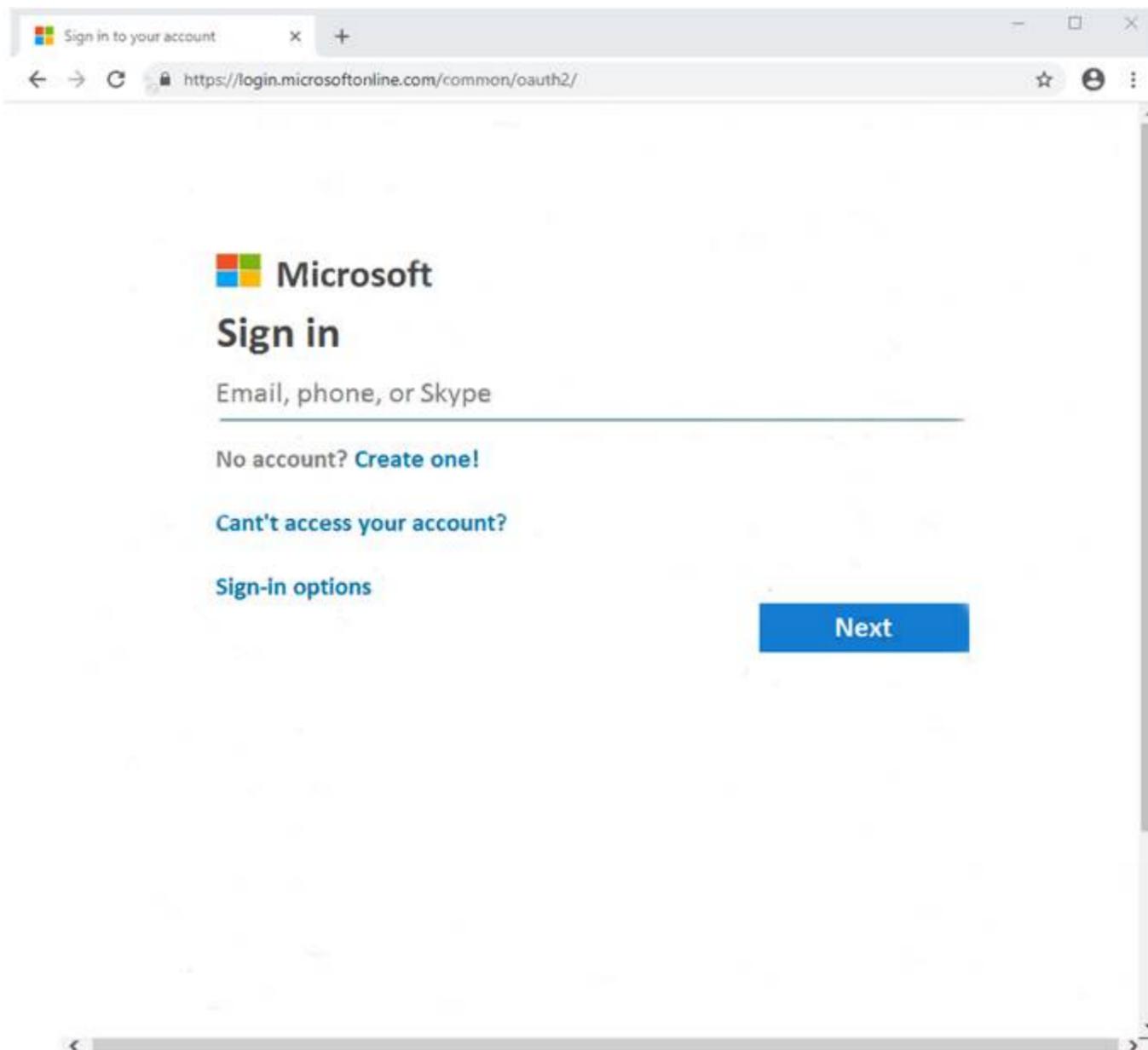
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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



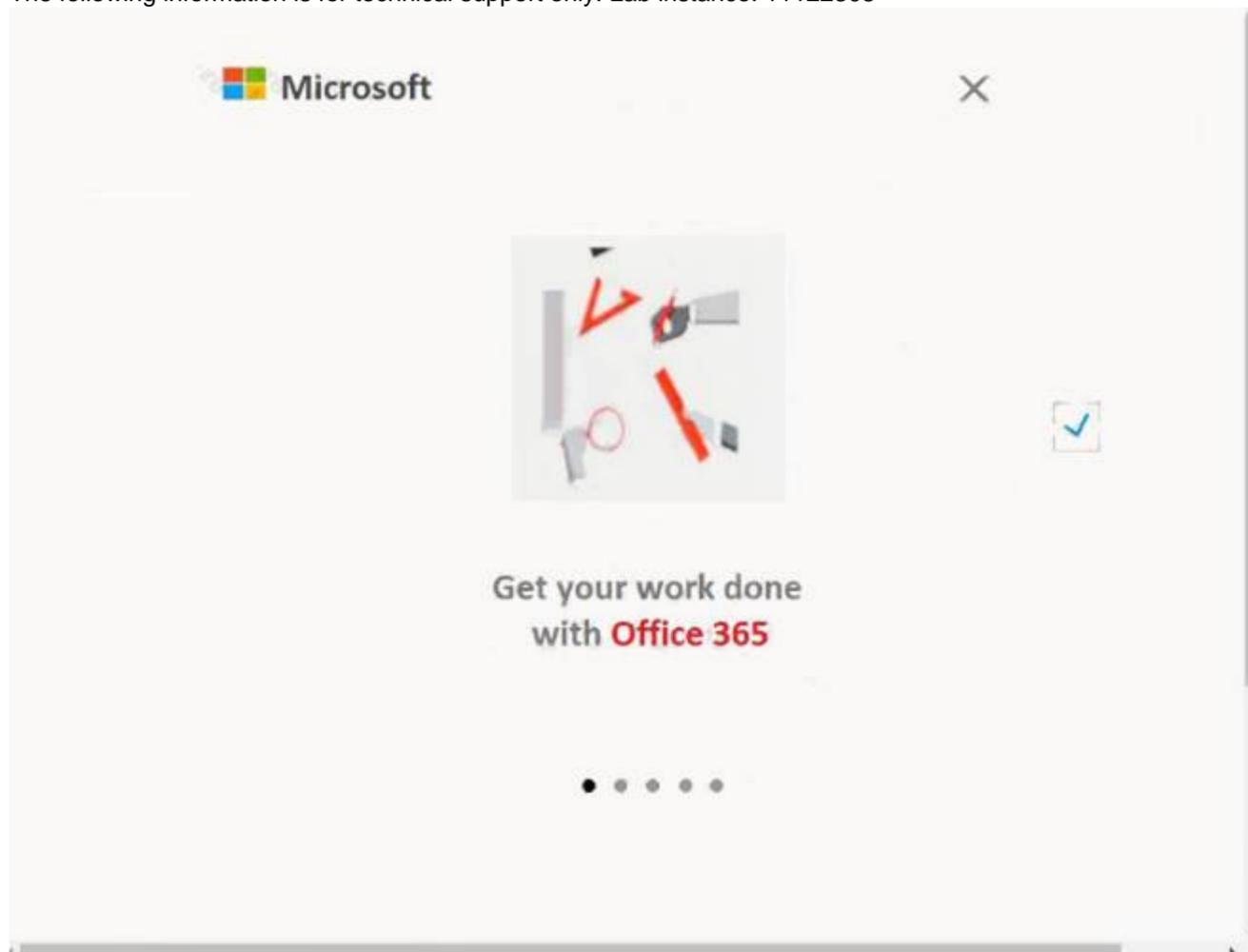
Use the following login credentials as needed:

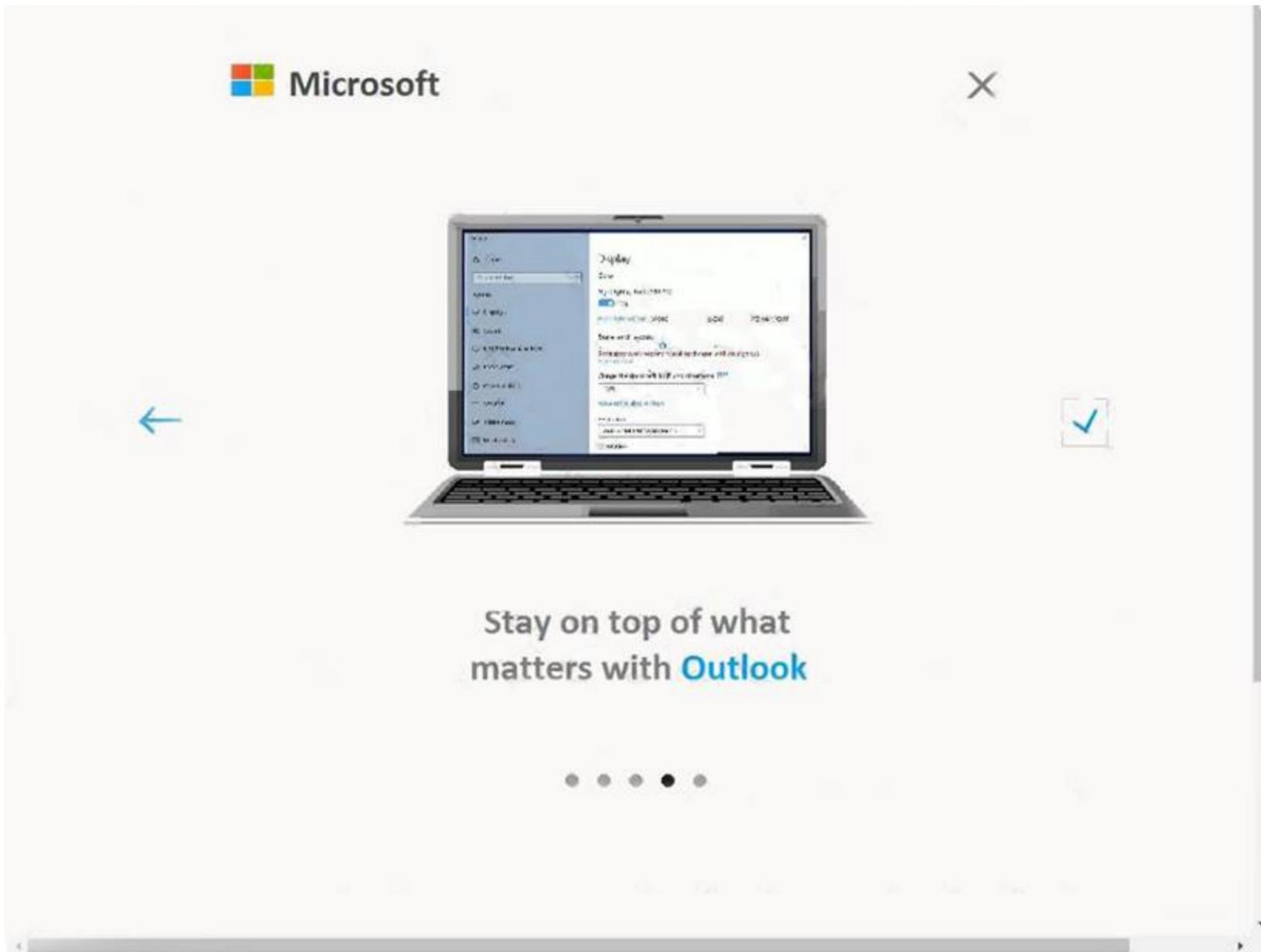
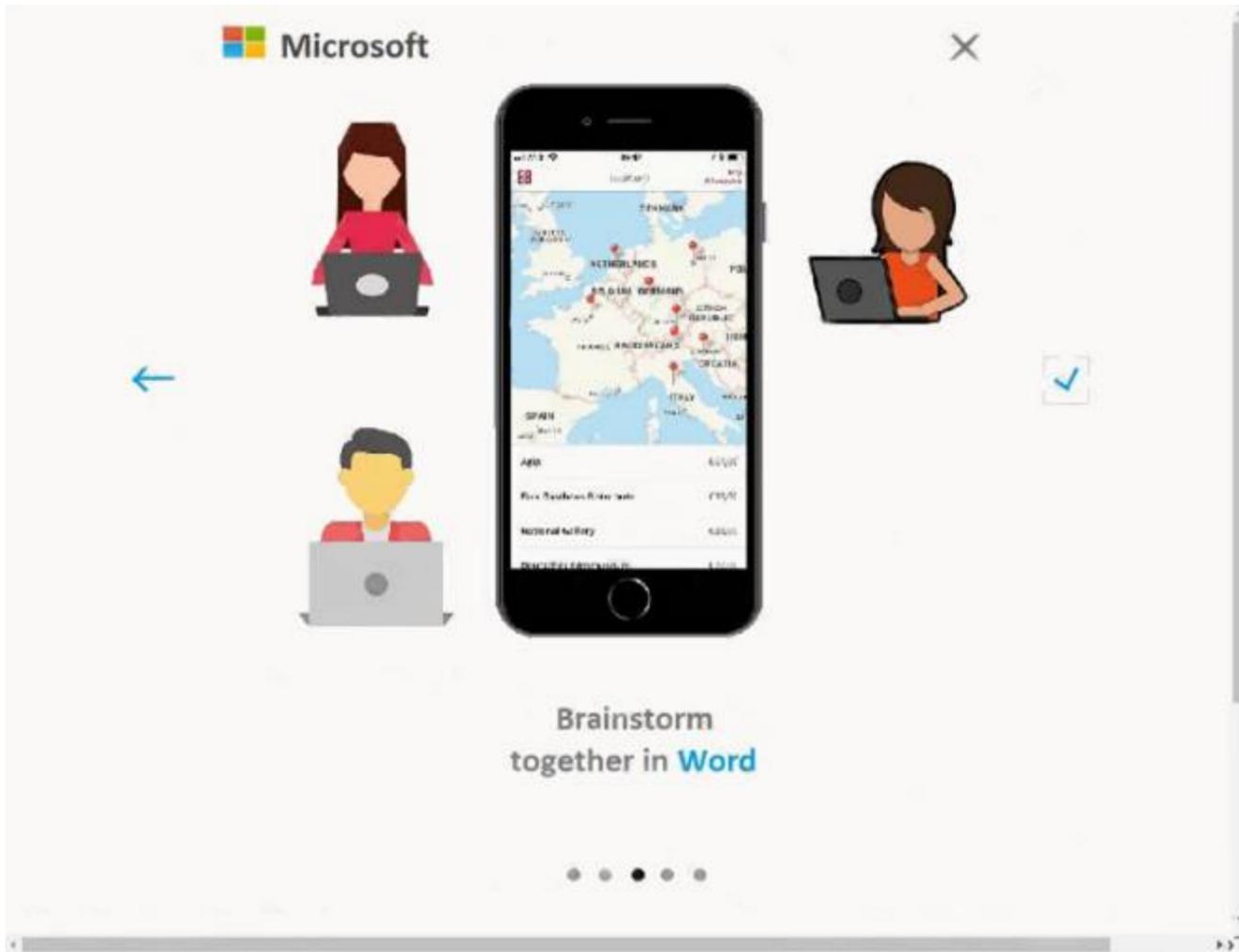
To enter your username, place your cursor in the Sign in box and click on the username below.

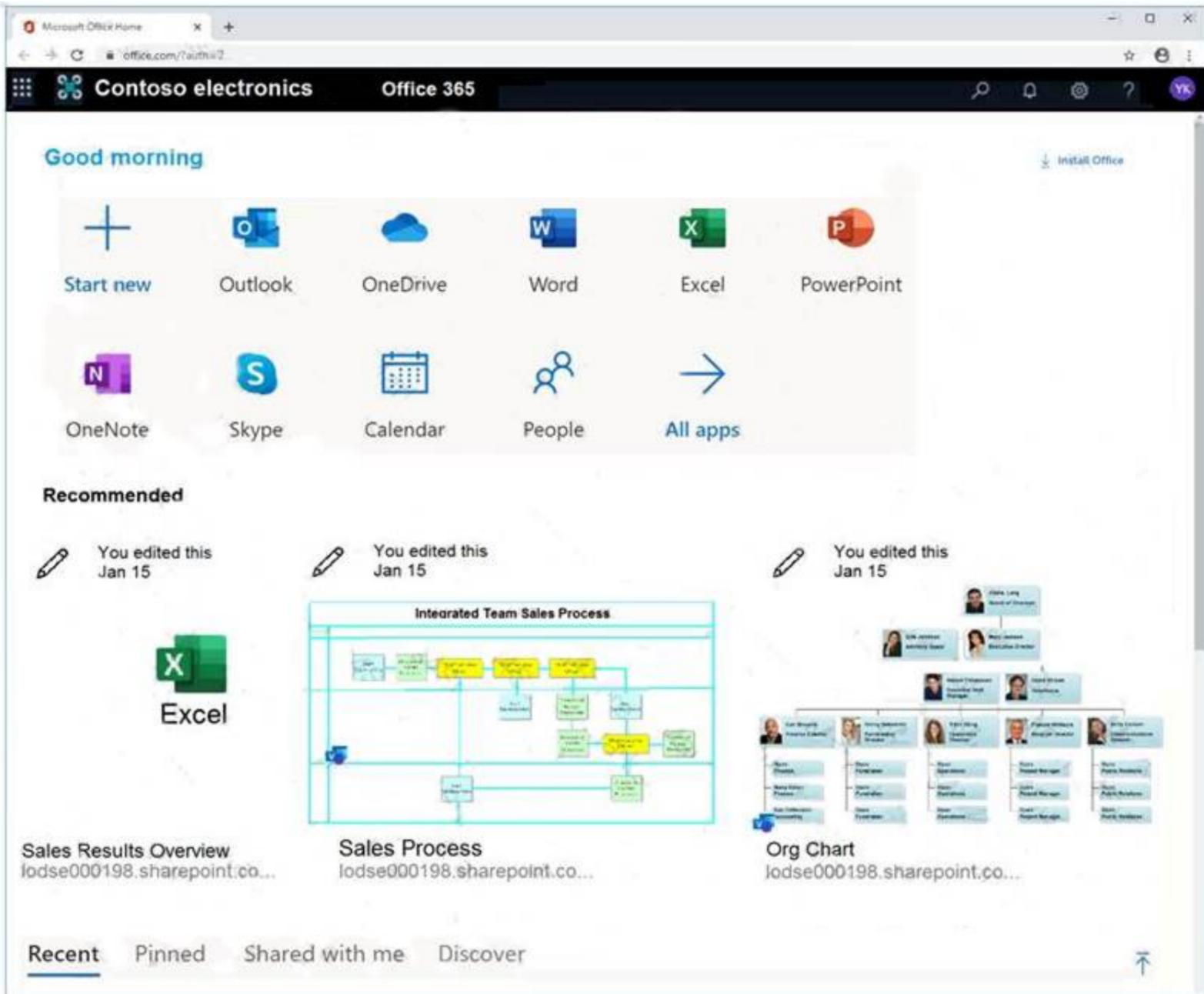
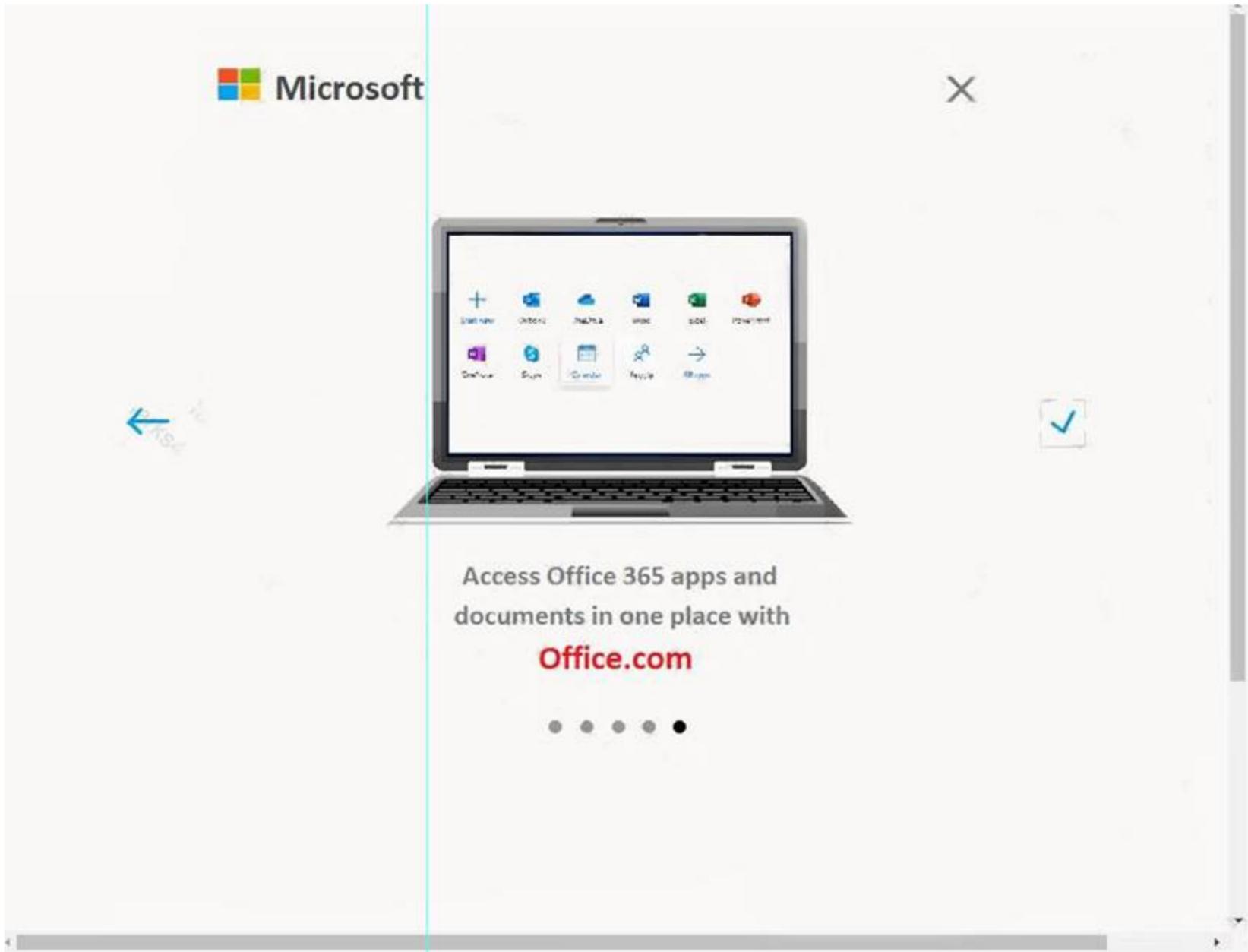
To enter your password, place your cursor in the Enter password box and click on the password below. Microsoft 365 Username: admin@LODSe00019@onmicrosoft.com Microsoft 365 Password: #HSP.ug?\$p6un

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







Recommended

You edited this
Jan 15

You edited this
Jan 15

You edited this
Jan 15



Excel

P and L Summary

[lodse000198.sharepoint.co...](#)



Contoso Electronics Outdoor...

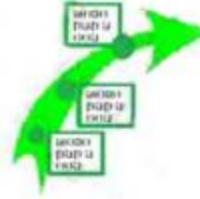
[lodse000198.sharepoint.co...](#)



AD Slogans

[lodse000198.sharepoint.co...](#)

Ad Slogans



Recent

Pinned

Shared with me

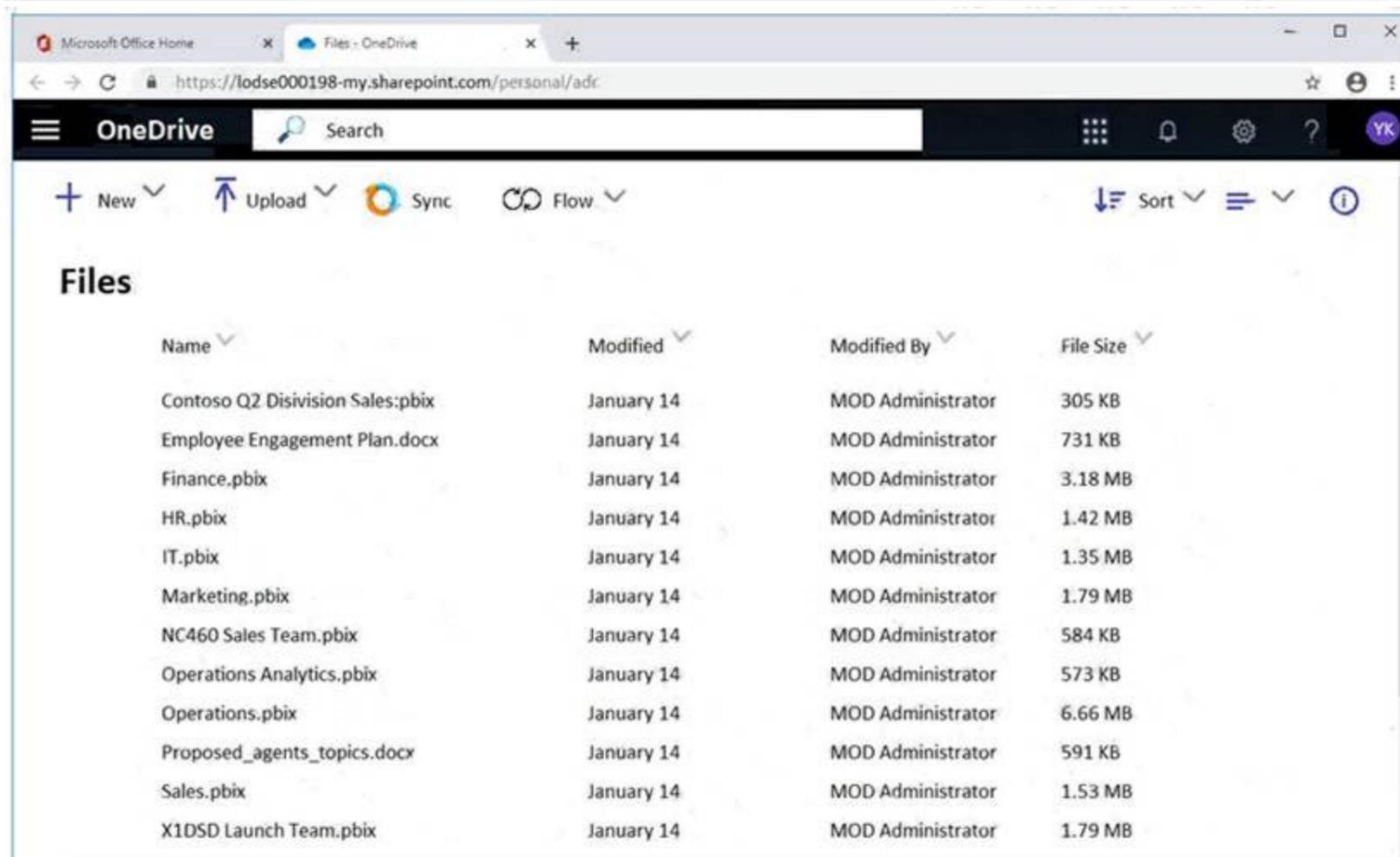
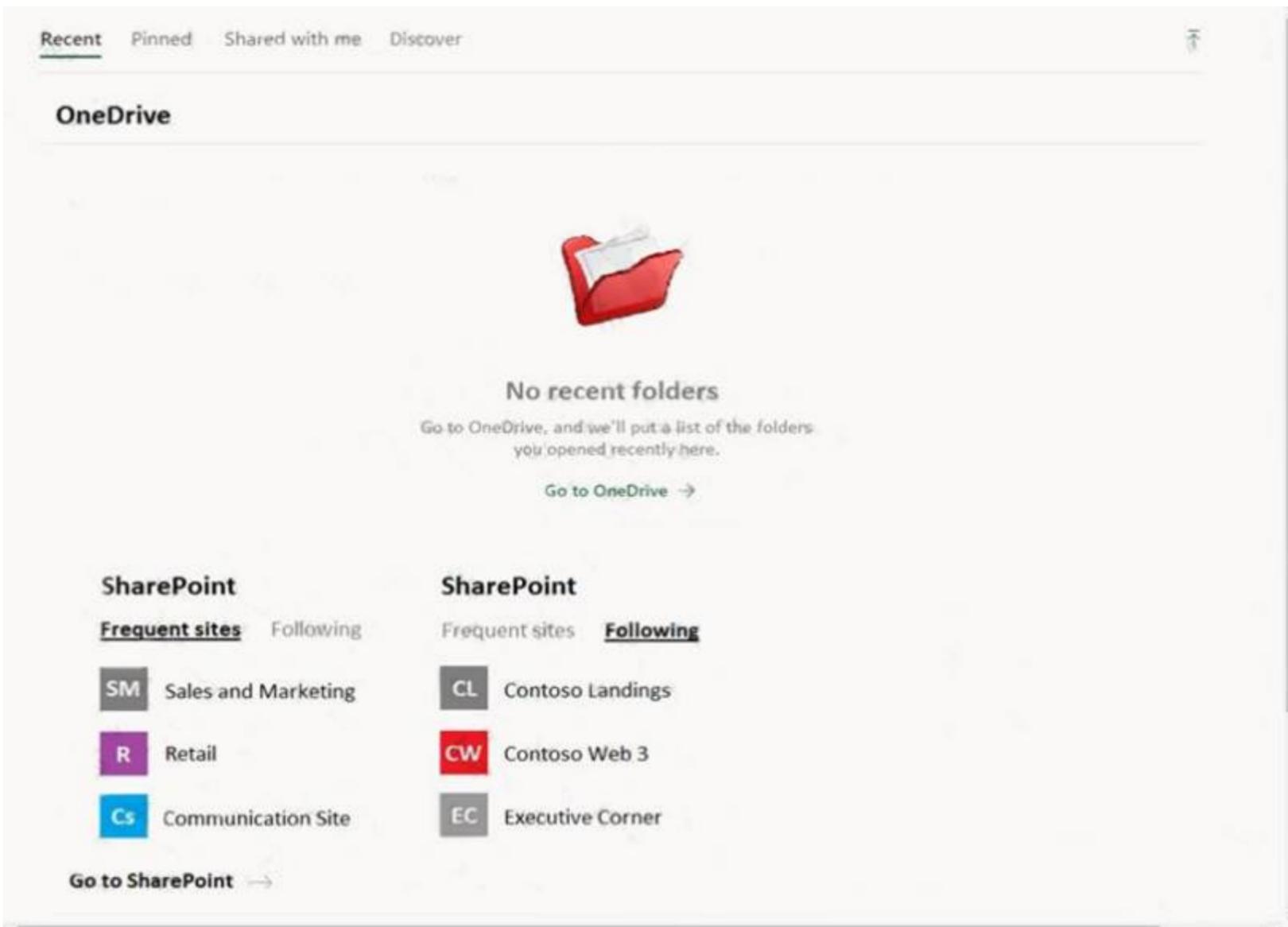
Discover

Recent Pinned Shared with me Discover

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



You need to ensure that a user named Allan Deyoung receives incident reports when email messages that contain data covered by the U.K. Data Protection Act are sent outside of your organization.
 To complete this task, sign in to the Microsoft 365 admin center.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. In the Security & Compliance Center > left navigation > Data loss prevention > Policy > + Create a policy.
- * 2. Choose the U.K. Data Protection Act template > Next.
- * 3. Name the policy > Next.
- * 4. Choose All locations in Office 365 > Next.
- * 5. At the first Policy Settings step just accept the defaults,
- * 6. After clicking Next, you'll be presented with an additional Policy Settings page Deselect the Show policy tips to users and send them an email notification

option.
 Select the Detect when content that's being shared contains option, and configure the number instances to be 10.
 Select the Send incident reports in email option.
 Select the Choose what to include in the report and who receives it link to add Allan Deyoung as a recipient.

* 7. > Next

* 8. Select the option to turn on the policy right away > Next.

* 9. Click Create to finish creating the policy. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwid> <https://docs.microsoft.com/en-us/microsoft-365/compliance/what-the-dlp-policy-templates-include?view=o365>

NEW QUESTION 48

- (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:

User2:

User3:

- 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 53

- (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 56

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses insider risk management and contains the users shown in the following table.

Name	Role group
Admin1	Insider Risk Management
Admin2	Insider Risk Management Admins
Admin3	Insider Risk Management Analysts
Admin4	Insider Risk Management Investigators

Which users can use Content explorer?

- A. Admin1 and Admin2 only
- B. Admin4 only
- C. Admin2 and Admin3 only
- D. Admin1, Admin2, Admin3, and Admin4
- E. Admin1 and Admin4 only

Answer: D

NEW QUESTION 61

- (Exam Topic 4)

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

You need to ensure that User1 can use the Microsoft 365 compliance center to search audit logs and identify which users were added to Microsoft 365 role groups.

The solution must use the principle of least privilege.

To which role group should you add User1?

- A. Security Reader
- B. View-Only Organization Management
- C. Organization Management
- D. Compliance Management

Answer: C

NEW QUESTION 66

- (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 71

- (Exam Topic 4)

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains two users named User1 and User2.

You need to assign Role Based Access Control (RBAC) roles to User1 and User2 to meet the following requirements:

- > Use the principle of least privilege
- > Enable User1 to view sync errors by using Azure AD Connect Health
- > Enable User2 to configure Azure Active Directory Connect Health Settings Which two roles should you assign?

- A. The Monitoring Readers role in Azure AD Connect Health to User1
- B. The Security reader role in Azure AD to User 1
- C. The Reports reader role in Azure AD to User 1
- D. The Contributor role in Azure AD Connect Health to User 2
- E. The Monitoring Contributor role in Azure Connect Health to User 2
- F. The Security operator role in Azure AD to User2

Answer: BD

NEW QUESTION 72

- (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 73

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search. What should you do from the Security & Compliance admin center?

- A. From Search & investigation, create a guided search.
- B. From Events, create an event.
- C. From Alerts, create an alert policy.
- D. From Search & Investigation, create an eDiscovery case.

Answer: C

Explanation:

References:

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

NEW QUESTION 74

- (Exam Topic 4)

Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed.

You have a Microsoft Azure subscription.

You are deploying Azure Advanced Threat Protection (ATP)

You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016. You need to integrate the VPN and Azure ATP.

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

On VPN1:

Configure an authentication provider.	V
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	V
1723	
1813	
8080	
8531	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn>

NEW QUESTION 77

- (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 create a conditional access policy for User1, User2, and User3, Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr>

NEW QUESTION 81

- (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 83

- (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.

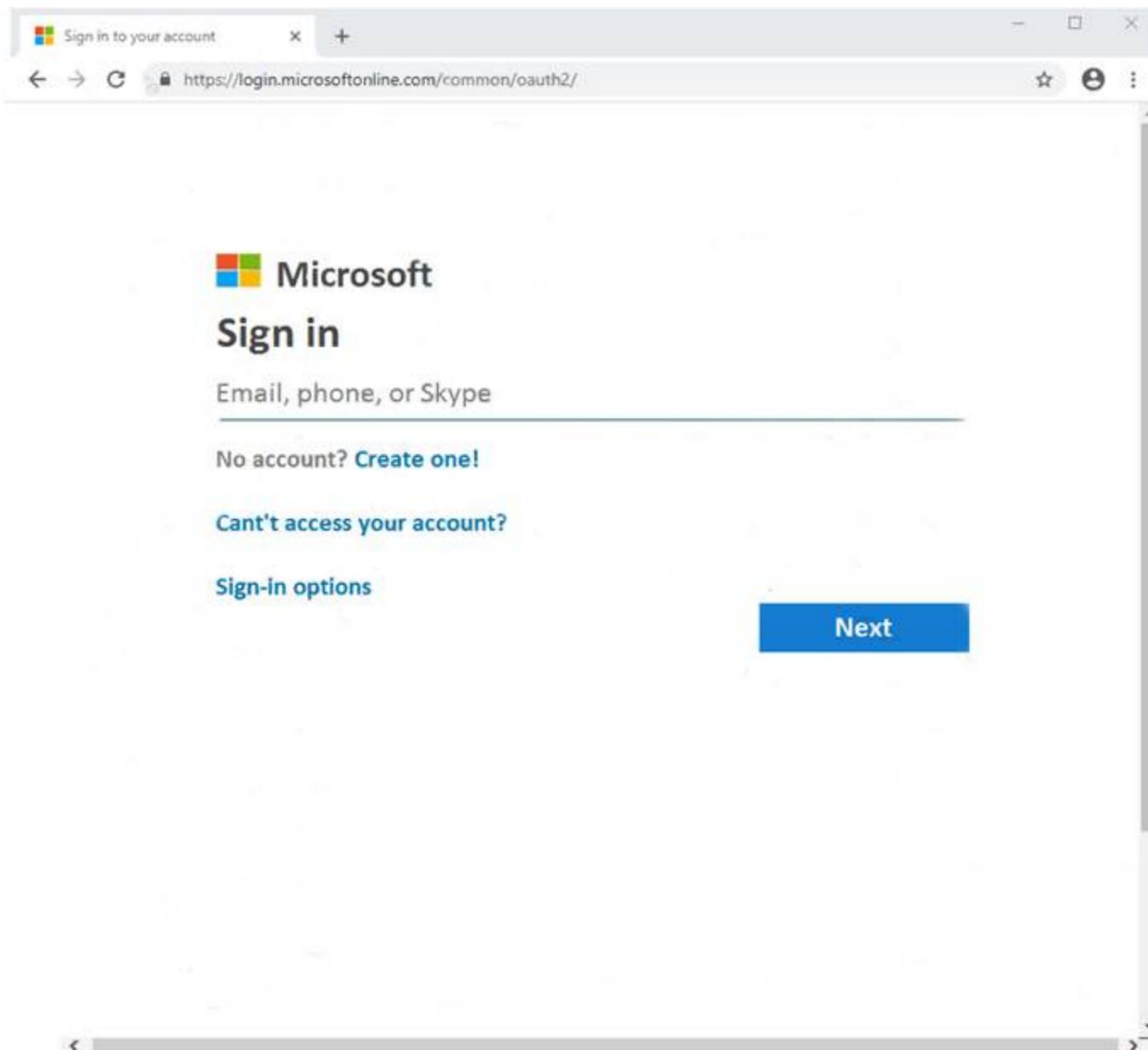
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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



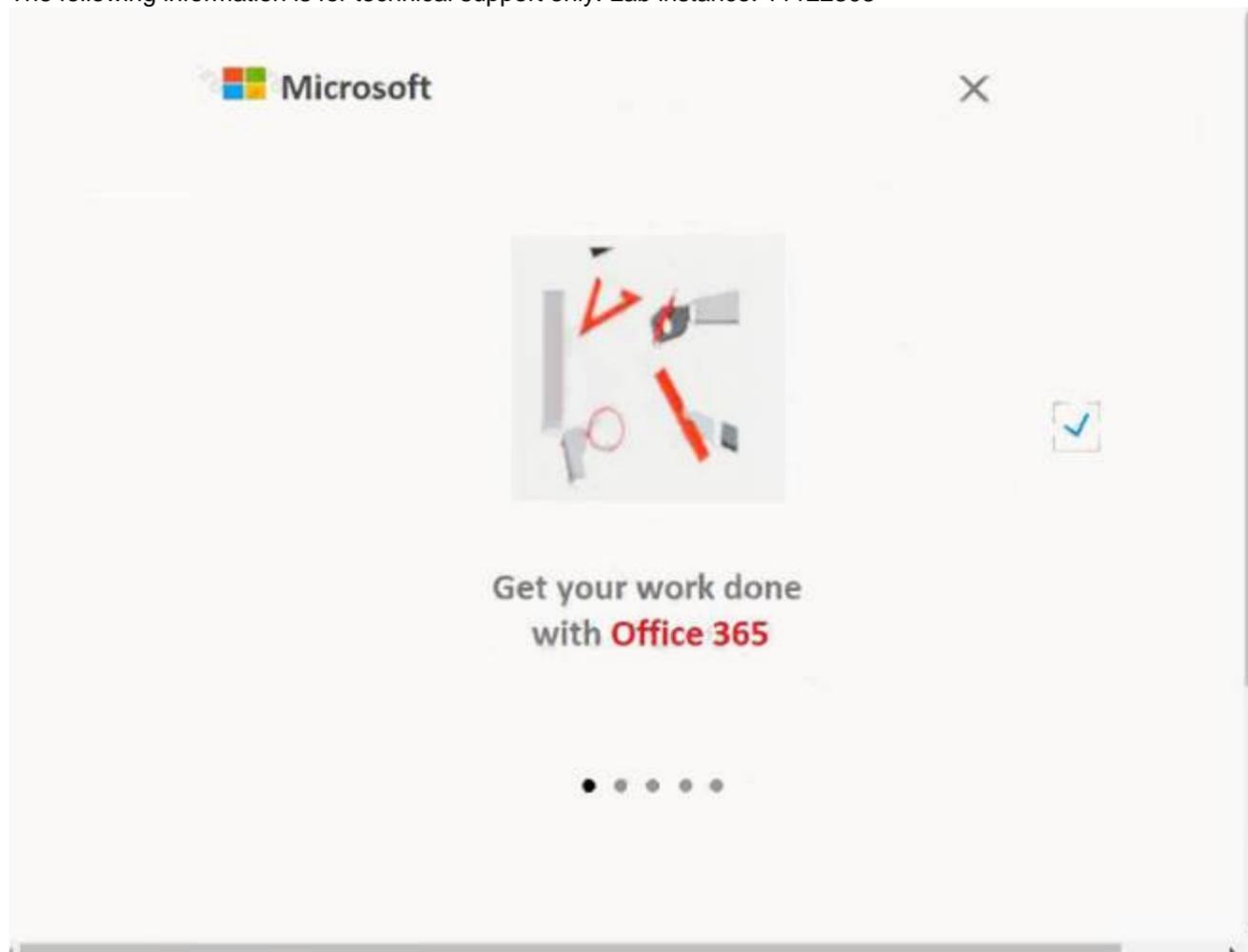
Use the following login credentials as needed:

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



Brainstorm together in **Word**

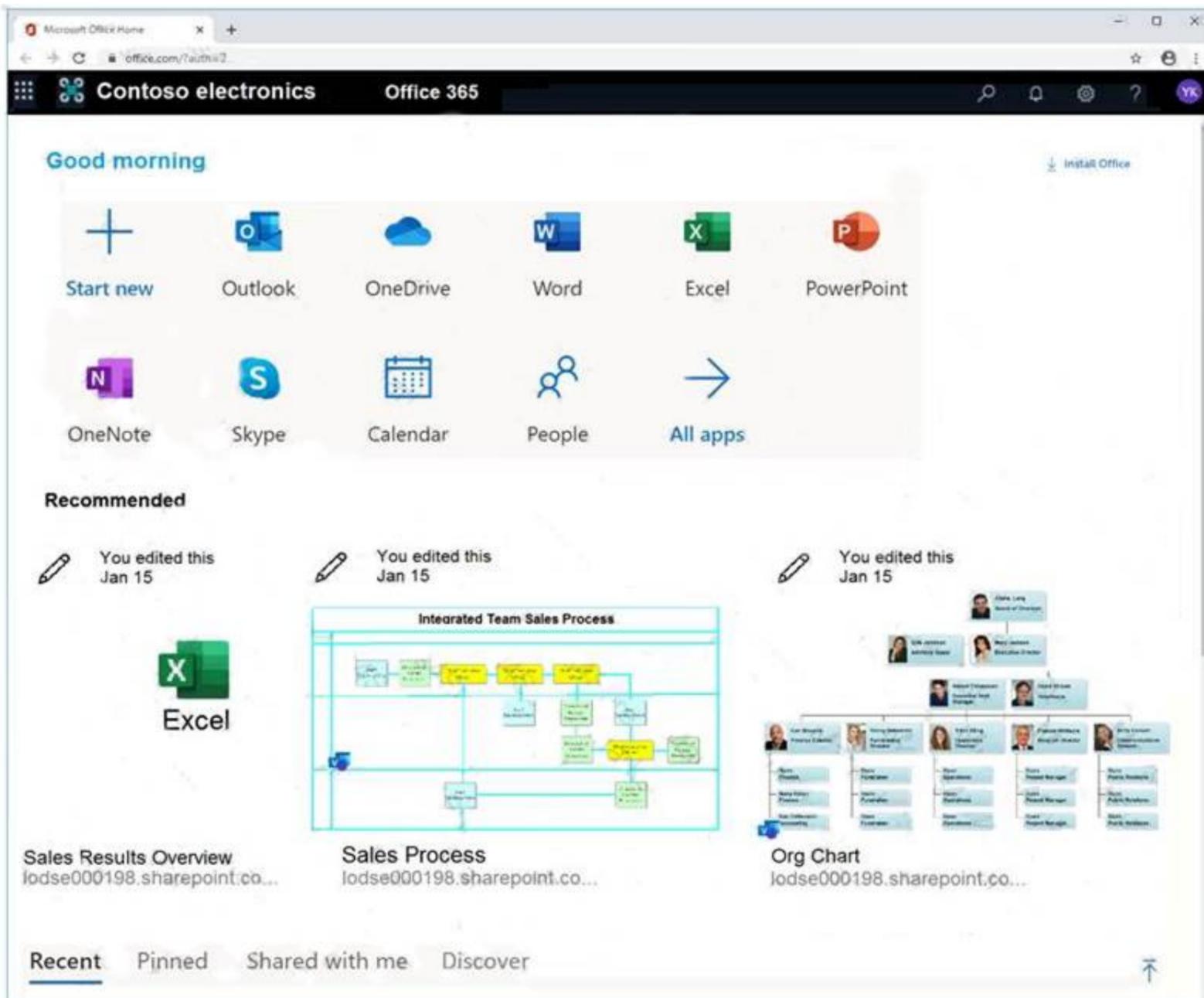
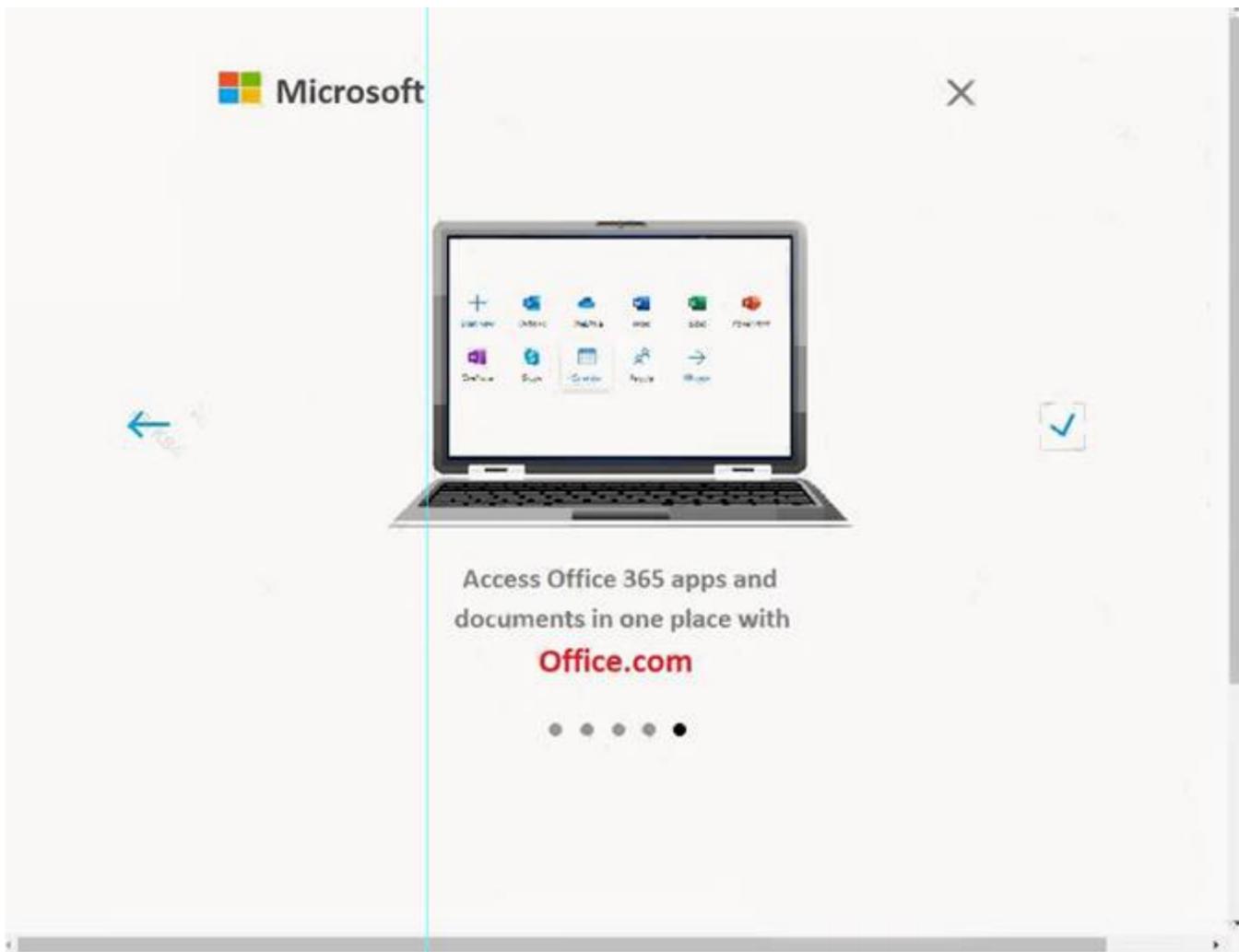
This advertisement features the Microsoft logo at the top left. The central image shows a smartphone displaying a map of Europe with several red location pins. To the left of the phone are two icons of people sitting at laptops, and to the right is one icon of a person at a laptop. A blue arrow points left from the phone, and a blue checkmark icon is on the right. Below the phone, the text reads "Brainstorm together in Word". At the bottom, there are five small circles, with the third one from the left being filled, indicating the current slide in a sequence.

Microsoft



Stay on top of what matters with **Outlook**

This advertisement features the Microsoft logo at the top left. The central image shows a laptop displaying the Outlook email interface, with a list of emails on the left and a selected email on the right. A blue arrow points left from the laptop, and a blue checkmark icon is on the right. Below the laptop, the text reads "Stay on top of what matters with Outlook". At the bottom, there are five small circles, with the fourth one from the left being filled, indicating the current slide in a sequence.



Recommended

 You edited this
Jan 15

 You edited this
Jan 15

 You edited this
Jan 15



Excel

P and L Summary

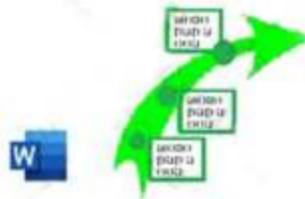
[lodse000198.sharepoint.co...](#)



Contoso Electronics Outdoor...

[lodse000198.sharepoint.co...](#)

AD Slogans



AD Slogans

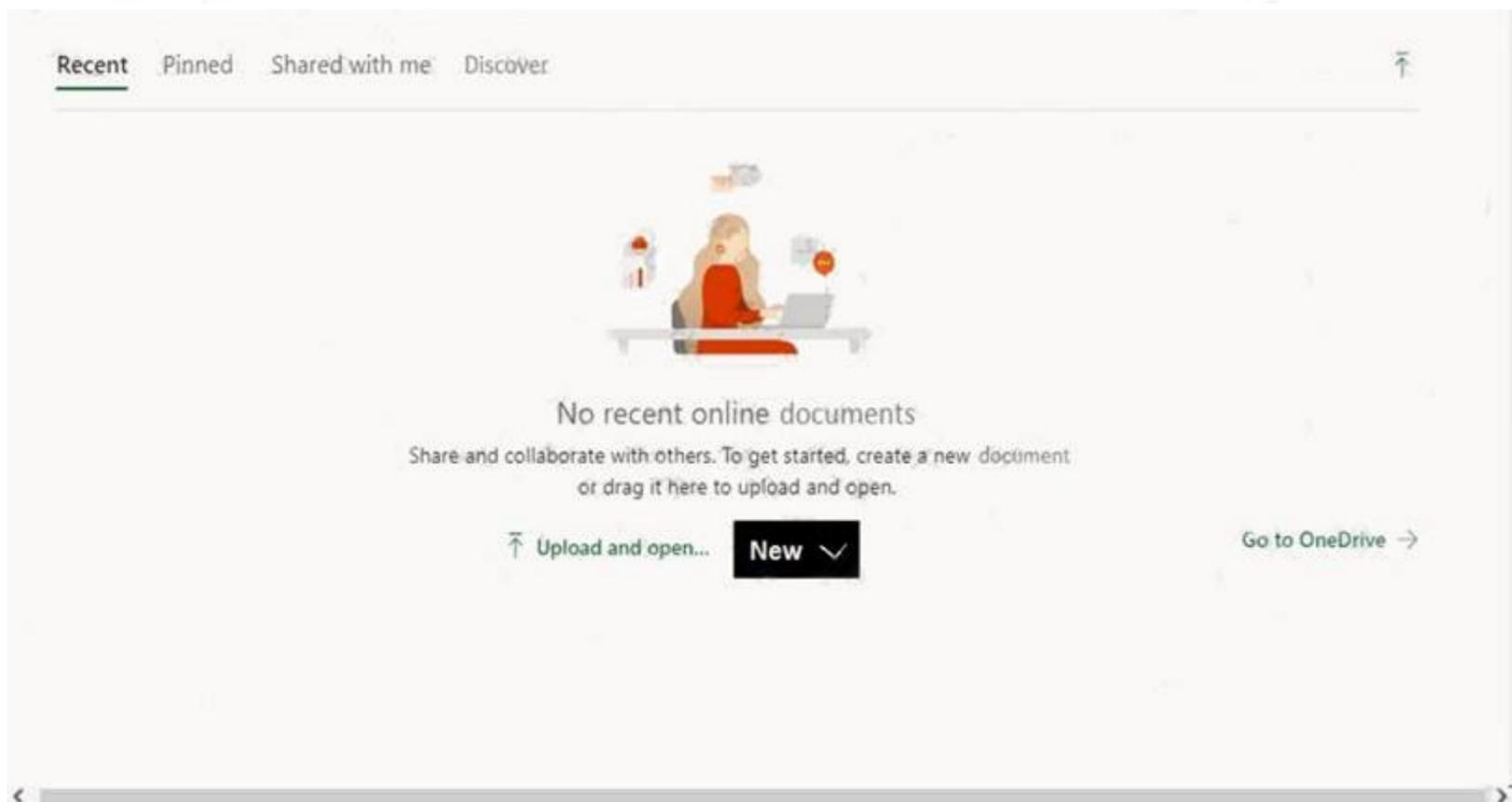
[lodse000198.sharepoint.co...](#)

Recent

Pinned

Shared with me

Discover



Recent Pinned Shared with me Discover

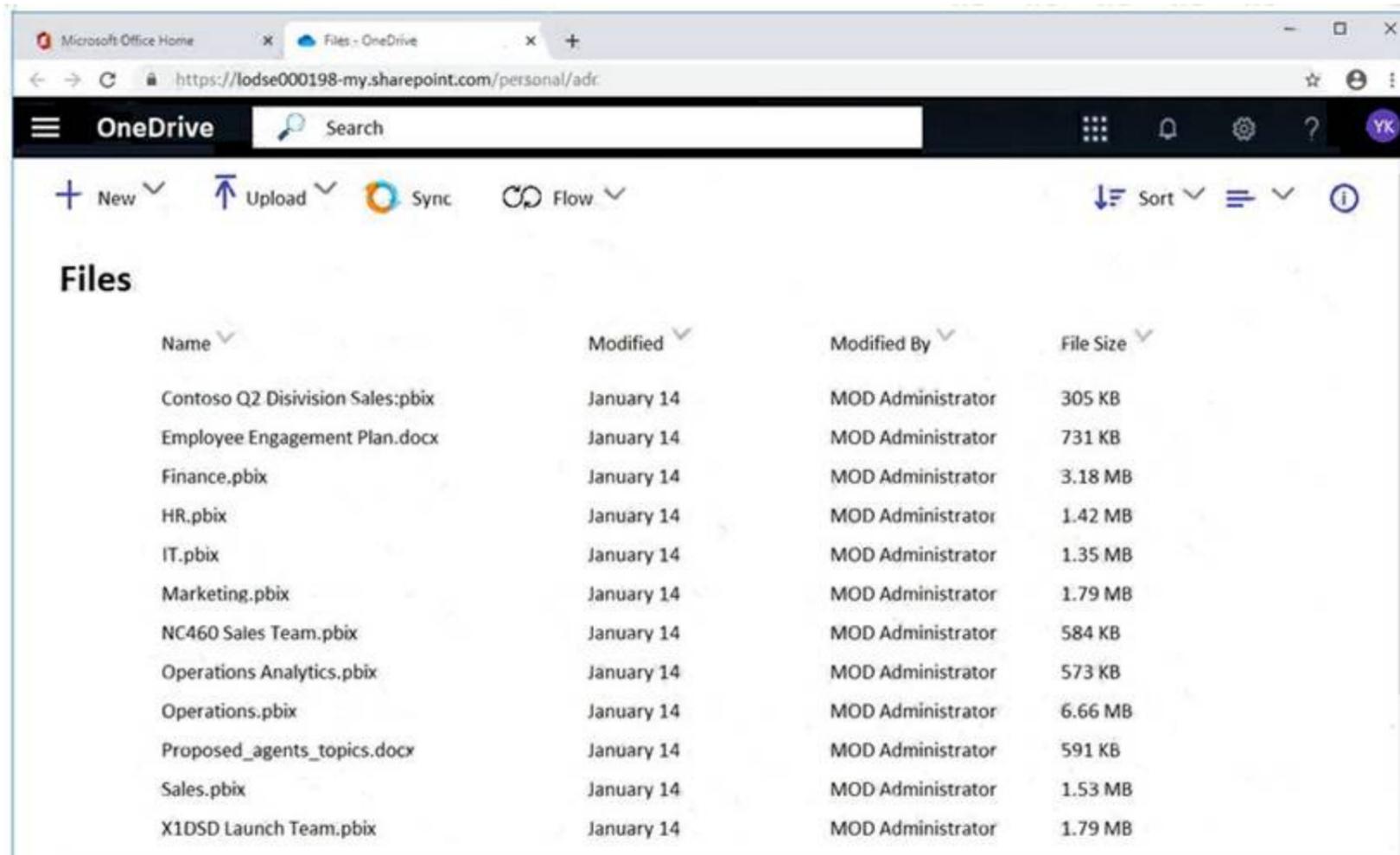
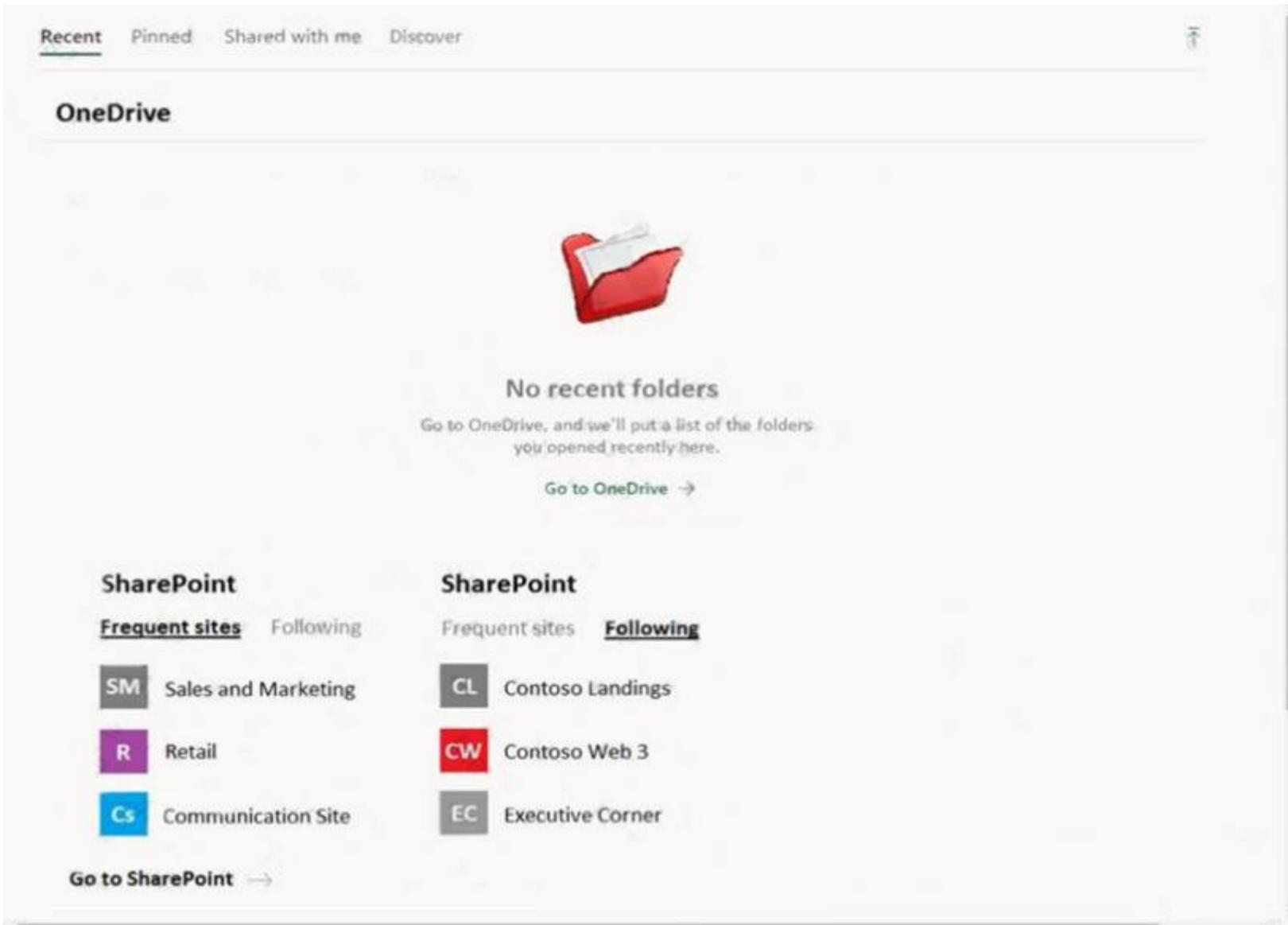


No recent online documents

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](#) 



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 88

- (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 92

- (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 95

- (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 100

- (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	Group	Role
User1	Microsoft Defender for Identity Contoso Users	None
User2	Microsoft Defender for Identity Contoso Viewers	None
User3	Not applicable	Security administrator
User4	Not applicable	Security operator

You discover that several security alerts are visible from the Microsoft Defender for Identity portal. You need to identify which users in contoso.com can close the security alerts.

Which users should you identify?

- A. User3 only
- B. User1 and User2 only
- C. User3 and User4 only
- D. User1 and User3 only
- E. User1 only

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/defender-for-identity/role-groups>

NEW QUESTION 103

- (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 106

- (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 111

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies. You need to identify the following:

- Rules that are applied without Triggering a policy alert
- The top 10 files that have matched DLP policies
- Alerts that are miscategorized

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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.

Reports	Answer Area
DLP policy matches	Rules that are applied without triggering a policy alert: <input type="text"/>
False positive and override	The top 10 files that have matched DLP policies: <input type="text"/>
Incident reports	Alerts that are miscategorized: <input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reports	Answer Area
DLP policy matches	Rules that are applied without triggering a policy alert: DLP policy matches
False positive and override	The top 10 files that have matched DLP policies: Incident reports
Incident reports	Alerts that are miscategorized: False positive and override

NEW QUESTION 113

- (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 116

- (Exam Topic 4)

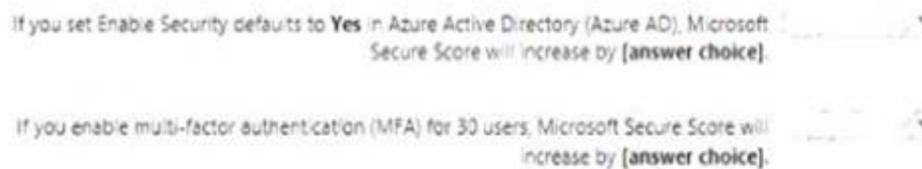
You have a Microsoft 365 subscription that contains 100 users.

Microsoft Secure Score for the subscription is shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area



If you set Enable Security defaults to **Yes** in Azure Active Directory (Azure AD), Microsoft Secure Score will increase by [answer choice].

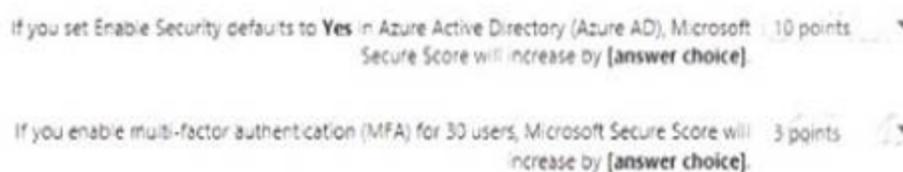
If you enable multi-factor authentication (MFA) for 30 users, Microsoft Secure Score will increase by [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



If you set Enable Security defaults to **Yes** in Azure Active Directory (Azure AD), Microsoft Secure Score will increase by [answer choice] 10 points.

If you enable multi-factor authentication (MFA) for 30 users, Microsoft Secure Score will increase by [answer choice] 3 points.

NEW QUESTION 120

- (Exam Topic 4)

Your company has a Microsoft 365 subscription.

The company forbids users to enroll personal devices in mobile device management (MDM). 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 conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
- B. an app protection policy in Microsoft Intune
- C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
- D. a device compliance policy in Microsoft Intune

Answer: B

NEW QUESTION 124

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You need to implement a policy to enforce the following requirements:

- If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint Online only from a web browser. The user must be prevented from downloading files or syncing files from SharePoint Online.
- If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files.

What should you create?

- A. a conditional access policy in Azure AD that has Client apps conditions configured
- B. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured
- C. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured
- D. a conditional access policy in Azure AD that has Session controls configured

Answer: A

NEW QUESTION 125

- (Exam Topic 4)

You have a Microsoft 365 description that contains a user named User1.

You need to that User1 can review registration and usage activity reports for Azure Multi-Factor Authentication (Azure MFA) for the subscription. The solution must meet the following requirements:

- Minimize Costs
- use the principle Of least privilege

What should you assign to user1?

License:

Role:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

License:

Role:

NEW QUESTION 130

- (Exam Topic 4)

You have a Microsoft 365 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs. You need to limit alert notifications to actionable DLP events.

What should you do?

- A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
- B. From the Cloud App Security admin center, apply a filter to the alerts.
- C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
- D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

Answer: D

Explanation:

References:

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

NEW QUESTION 131

- (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 135

- (Exam Topic 4)

You have a Microsoft 365 alert named Alert? as shown in the following exhibit.

View alerts

Severity	Alert name	Status	Category	Activity count	Last occurrence...
Medium	Alert2	Resolved	Data loss prevention	1	6 days ago

You need to manage the status of Alert2. To which status can you change Alert2?

- A. The status cannot be changed.
- B. investigating only
- C. Active or investigating only
- D. Investigating, Active, or Dismissed
- E. Dismissed only

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worl>

NEW QUESTION 140

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.

The screenshot shows the 'Review your settings' page for a retention label named 'Label1'. On the left, a progress bar indicates that 'Name your label' and 'Label settings' are completed, while 'Review your settings' is the current step. The main content area includes:

- Name:** Label1 (with an 'Edit' link)
- Descriptions for admins:** (with an 'Edit' link)
- Description for users:** (with an 'Edit' link)
- Retention:** 2 years, Retain and Delete, Based on when it was created, Use Label to classify content as a "Record" (with an 'Edit' link)

 At the bottom, there are three buttons: 'Back', 'Create this label', and 'Cancel'.

You publish Label1 to SharePoint sites.

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 you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

▼

never delete the file.

delete the file before January 1, 2021.

delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

▼

always remain in the library.

remain in the library until you delete the file.

be deleted automatically on March 15, 2021.

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 143

- (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 147

- (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 149

- (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 154

- (Exam Topic 4)

You have an on-premises Hyper-V infrastructure that contains the following:

- > An Active Directory domain
- > A domain controller named Server1
- > A member server named Server2

A security policy specifies that Server1 cannot connect to the Internet. Server2 can connect to the Internet. You need to implement Azure Advanced Threat Protection (ATP) to monitor the security of the domain.

What should you configure on each server? To answer, drag the appropriate components to the correct servers. Each component may only 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.

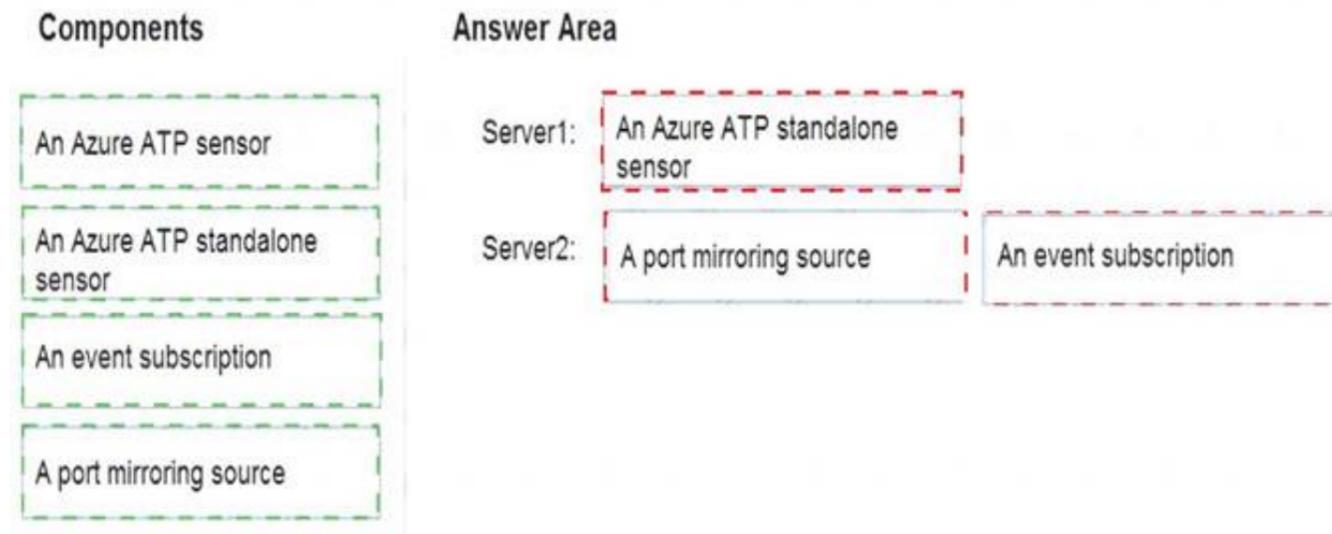
Components	Answer Area
An Azure ATP sensor	Server1: <input type="text"/> Component
An Azure ATP standalone sensor	Server2: <input type="text"/> Component <input type="text"/> Component
An event subscription	
A port mirroring source	

7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 156

- (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>

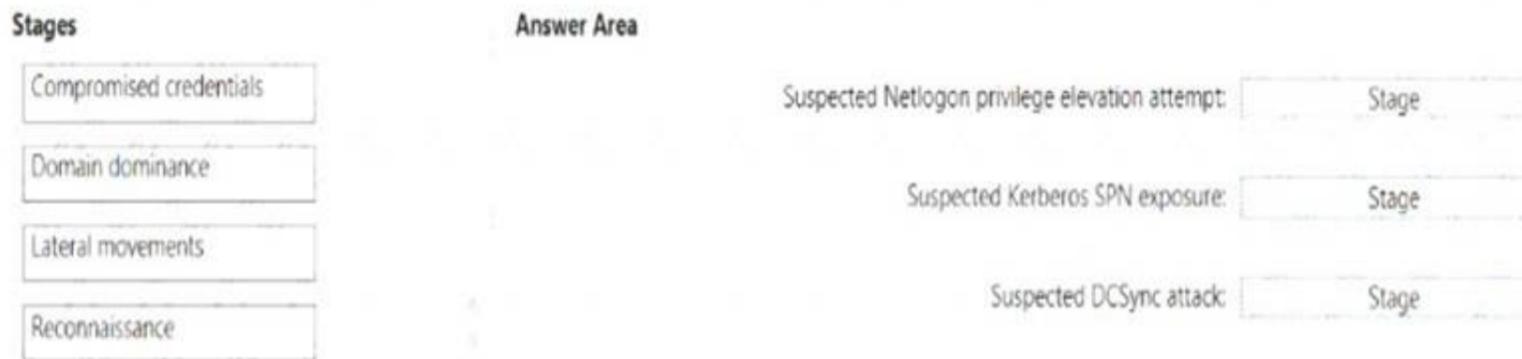
NEW QUESTION 158

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Identity. You receive the following alerts:

- Suspected Netlogon privilege elevation attempt
- Suspected Kerberos SPN exposure
- Suspected DCSync attack

To which stage of the cyber-attack kill chain does each alert map? To answer, drag the appropriate alerts to the correct stages. Each alert 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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 161

- (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 164

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 50 devices- The devices are enrolled in Microsoft Endpomt Manager and have Microsoft Defender for Endpoint enabled. You need to identify devices that have a pending offline scan. What should you do?

- A. From the Microsoft 365 Defender portal, review the Threat & Vulnerability Management dashboard.
- B. From the Microsoft 365 Defender portal, review the Threat analytics dashboard
- C. From the Microsoft Endpoint Manager admin center, review the Detected malware report
- D. From the Microsoft Endpoint Manager admin center, review the Antivirus agent status report.

Answer: A

NEW QUESTION 169

- (Exam Topic 4)

You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From the Cloud App Security admin center, create a file policy.
- B. From the SharePoint admin center, modify the Site Settings.
- C. From the SharePoint & Compliance admin center, create a label.
- D. From the SharePoint admin center, modify the records management settings.
- E. From the Security & Compliance admin center, publish a label.

Answer: CE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-l>

NEW QUESTION 172

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named Used. You need to assign User1 permissions to search Microsoft Office 365 audit logs. What should you use?

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

Answer: A

NEW QUESTION 177

- (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 181

- (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 182

- (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 184

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

- > Prevent any email messages that contain credit card numbers from being sent outside your organization
- > Block the external sharing of Microsoft OneDrive content that contains EU passport numbers
- > Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Policies:

1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>

Rules:

1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policies:

1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>

Rules:

1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>

NEW QUESTION 188

- (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.

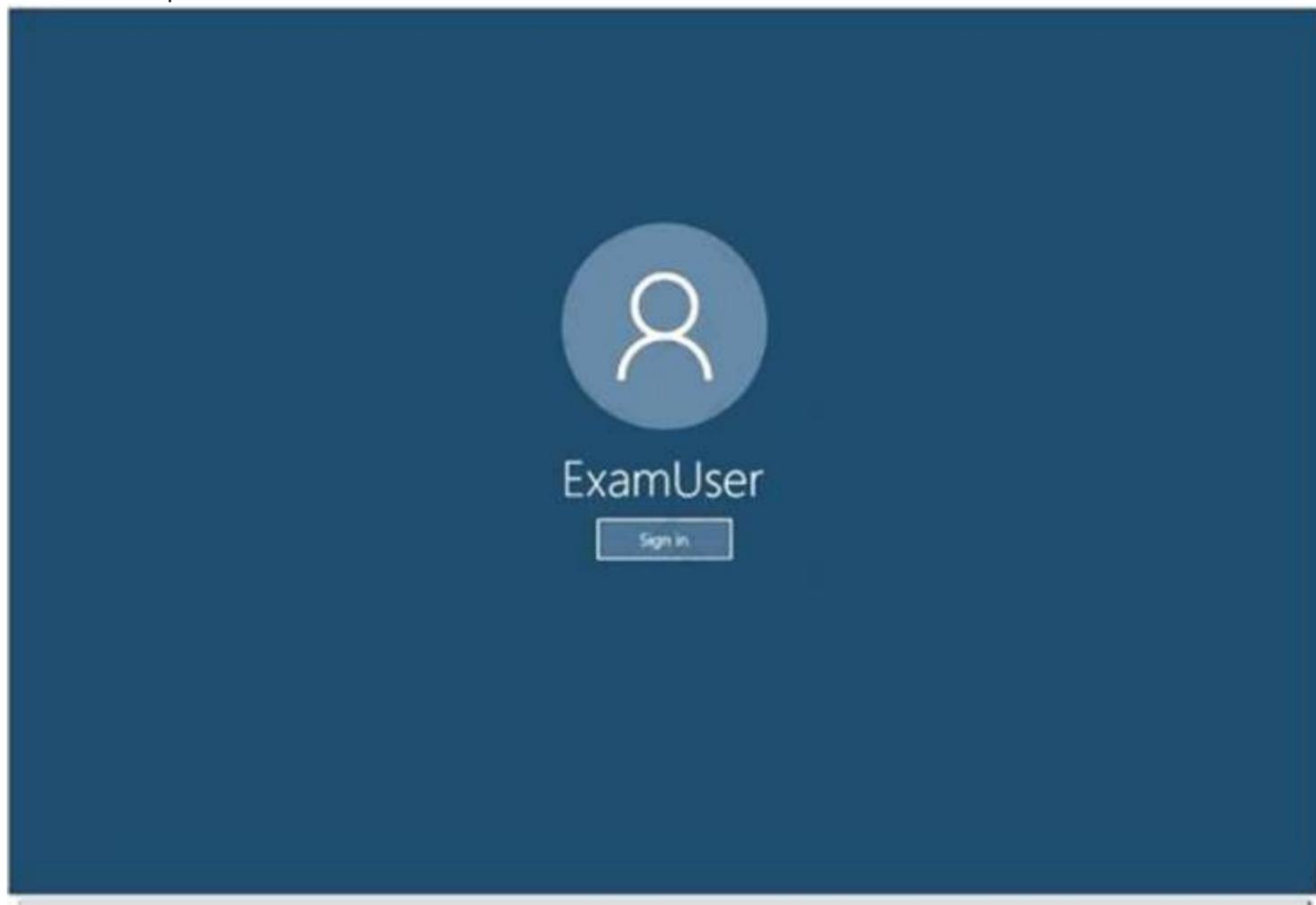
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 Lee Gu can manage all the settings for Exchange Online. The solution must use the principle of least privilege.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- In the Exchange Administration Center (EAC), navigate to Permissions > Admin Roles.
- Select the group: Organization Management and then click on Edit.
- In the Members section, click on Add.
- Select the users, USGs, or other role groups you want to add to the role group, click on Add, and then click on OK.
- Click on Save to save the changes to the role group. Reference:

<https://help.bittitan.com/hc/en-us/articles/115008104507-How-do-I-assign-the-elevated-admin-role-Organizatio> <https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo>

NEW QUESTION 192

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. On January 1, you create the sensitivity label shown in the following table.

Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

On January 2, you publish label to User1.
 On January 3. User 1 creates a Microsoft Word document named Doc1 and applies Label to the document. On January 4. User2 edits Doc1.
 On January 15, you increase the content expiry period for Label to 28 days. When will access to Doc1 expire for User2?

- A. January 23
- B. January 24
- C. January 25
- D. January 31

Answer: C

NEW QUESTION 193

- (Exam Topic 4)

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1. You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two actions should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 194

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.

You need to enable Microsoft Defender Exploit Guard (Microsoft Defender EG) on the devices. Which type of device configuration profile should you use?

- A. Endpoint protection
- B. Device restrictions
- C. Microsoft Defender for Endpoint
- D. identity protection

Answer: A

NEW QUESTION 197

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Sentinel to create incidents based on:

- Azure Active Directory (Azure AD) Identity Protection alerts
- Correlated events from the DeviceProcessEvents table

Which analytic rule types should you use for each incident type? To answer, drag the appropriate rule types to the correct incident types. Each rule type 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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 201

- (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 Directory Service 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 204

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible. What should you do?

- A. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning
- B. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
- C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy
- D. From the Security & Compliance admin center, create a label policy

Answer: D

Explanation:

References:

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

NEW QUESTION 205

- (Exam Topic 4)

You have several Conditional Access policies that block noncompliant devices from connecting to services. You need to identify which devices are blocked by which policies.

What should you use?

- A. the Device compliance report in the Microsoft Endpoint Manager admin center
- B. the Device compliance trends report in the Microsoft Endpoint Manager admin center

- C. Activity log in the Cloud App Security admin center
- D. the Conditional Access Insights and Reporting workbook in the Azure Active Directory admin center

Answer: D

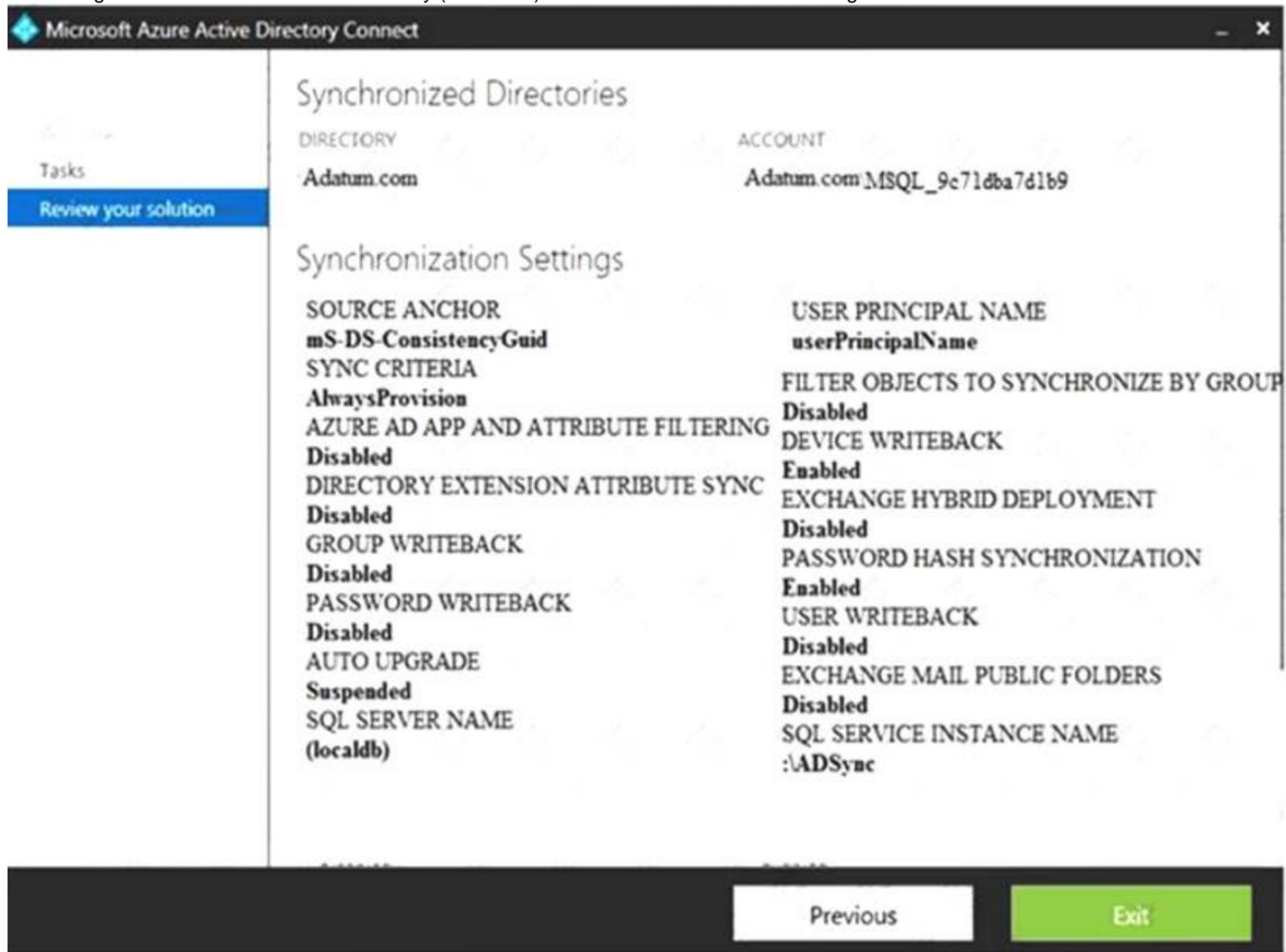
Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-re>

NEW QUESTION 206

- (Exam Topic 4)

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



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 you reset a password in Azure AD, the password will [answer choice].

be overwritten	▼
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	▼
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

NEW QUESTION 210

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains the groups shown in the following exhibit.

<input type="checkbox"/>	Name	Group type	Membership type	Email	Security enabled
<input type="checkbox"/>	 Group1	Microsoft 365	Assigned	Group1@sk220130.onmicrosoft.com	No
<input type="checkbox"/>	 Group2	Microsoft 365	Assigned	Group2@sk220130.onmicrosoft.com	Yes
<input type="checkbox"/>	 Group3	Distribution	Assigned	Group3@sk220130.onmicrosoft.com	No
<input type="checkbox"/>	 Group4	Mail enabled security	Assigned	Group4@sk220130.onmicrosoft.com	Yes
<input type="checkbox"/>	 Group5	Security	Assigned		Yes

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.

Answer Area

[Answer choice] can be assigned to receive noncompliance notifications generated by device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

[Answer choice] can be assigned device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

[Answer choice] can be assigned to receive noncompliance notifications generated by device compliance policies. Group1, Group2, Group3, Group4, and Group5

[Answer choice] can be assigned device compliance policies. Group1, Group2, Group3, and Group4 only

NEW QUESTION 211

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)