

MS-500.prepaway.premium.exam.147q

Number: MS-500
Passing Score: 800
Time Limit: 120 min
File Version: 7.0



MS-500

Microsoft 365 Security Administration

Version 7.0

Implement and manage identity and access

Testlet 1

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

Overview

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements

Fabrikam identifies the following issues:

- Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.
- Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes

Fabrikam plans to implement the following changes:

- Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory
- Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration

Fabrikam identifies the following application requirements for managing workload applications:

- User administrators will work from different countries
- User administrators will use the Azure Active Directory admin center

- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements

Fabrikam identifies the following security requirements:

- Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
- Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement
- Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
- Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
- Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
- The location of the user administrators must be audited when the administrators authenticate to Azure AD
- Email messages that include attachments containing malware must be delivered without the attachment
- The principle of least privilege must be used whenever possible

QUESTION 1

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

Exchange Administrator - Members			
+ Add member X Remove member Access reviews Export Refresh			
Assignment type All ▼			
Search Search by member's 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?

- Change the Assignment Type for Admin2 to **Permanent**
- From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
- From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
- Change the Assignment Type for Admin1 to **Eligible**

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

You need to recommend a solution for the user administrators that meets the security requirements for auditing.

Which blade should you recommend using from the Azure Active Directory admin center?

- A. Sign-ins
- B. Azure AD Identity Protection
- C. Authentication methods
- D. Access review

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 3

HOTSPOT

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.

Hot Area:

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	

Correct Answer:

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	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

You need to recommend a solution to protect the sign-ins of Admin1 and Admin2.

What should you include in the recommendation?

- A. a device compliance policy
- B. an access review
- C. a user risk policy
- D. a sign-in risk policy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 5

You need to resolve the issue that generates the automated email messages to the IT team.

Which tool should you run first?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

Implement and manage identity and access

Testlet 2

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment

Internal Network Infrastructure

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements

Planned Changes

Litware plans to implement the following changes:

- Migrate the email system to Microsoft Exchange Online
- Implement Azure AD Privileged Identity Management

Security Requirements

Litware identifies the following security requirements:

- Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
- Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
- Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
- Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
- Implement a permanent eligible assignment of the Compliance administrator role for User1
- Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
- Prevent access to Azure resources for the guest user accounts by default
- Ensure that all domain-joined computers are registered to Azure AD

Multi-factor authentication (MFA) Requirements

Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.

You identify the following requirements for testing MFA:

- Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must **NOT** be used on the Chicago office internal network.
- If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
- Any disruption of legitimate authentication attempts must be minimized.

General Requirements

Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

QUESTION 1

You need to create Group2.

What are two possible ways to create the group?

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

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

Which IP address space should you include in the Trusted IP 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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

HOTSPOT

How should you configure Group3? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Group type:

	▼
An Office 365 group in the Microsoft 365 admin center	
A security group in Active Directory Users and Computers	
A security group in the Azure Active Directory admin center	

Group membership criteria:

	▼
A dynamic distribution list	
A dynamic membership rule with an Advanced rule set to All users	
A dynamic membership rule with a Simple rule set to userType Equals User	

Correct Answer:

Answer Area

Group type:

	▼
An Office 365 group in the Microsoft 365 admin center	
A security group in Active Directory Users and Computers	
A security group in the Azure Active Directory admin center	

Group membership criteria:

	▼
A dynamic distribution list	
A dynamic membership rule with an Advanced rule set to All users	
A dynamic membership rule with a Simple rule set to userType Equals User	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

HOTSPOT

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.

Hot Area:

Answer Area

User sign-in settings:

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

Device options:

	▼
Hybrid Azure AD Join	
Enable Device writeback	
Disable Device writeback	

Correct Answer:

Answer Area

User sign-in settings:

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

Device options:

	▼
Hybrid Azure AD Join	
Enable Device writeback	
Disable Device writeback	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

You need to create Group3.

What are two possible ways to create the group?

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Implement and manage identity and access

Testlet 3

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea**"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	<i>Not applicable</i>	GroupA
Device6	Windows 10	Enabled	<i>None</i>

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	<i>None</i>
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	<i>None</i>

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management

QUESTION 1

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ADGroup1:	None	✓
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

ADGroup2:	None	✓
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

Correct Answer:

Answer Area

ADGroup1:	None	✓
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

ADGroup2:	None	✓
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 2

HOTSPOT

You are evaluating which finance department users will be prompted for Azure MFA credentials.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	☐	☐
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	☐	☐
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	☐	☐

Correct Answer:

Answer Area

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	☐	☒
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	☒	☐
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	☒	☐

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Which user passwords will User2 be prevented from resetting?

- A. User6 and User7
- B. User4 and User6
- C. User4 only
- D. User7 and User8
- E. User8 only

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

Which role should you assign to User1?

- A. Global administrator
- B. User administrator
- C. Privileged role administrator
- D. Security administrator

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Implement and manage identity and access

Question Set 4

QUESTION 1

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 is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Azure AD app and attribute filtering settings.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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 is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled

- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps>

QUESTION 3

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 is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Click the **Exhibit** tab.)

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

- ☒ 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

trusted ips [\(learn more\)](#)

- ☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

--

verification options [\(learn more\)](#)

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 [\(learn more\)](#)

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

In contoso.com, you create the users shown in the following table.

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My Apps portal	

Correct Answer:

Answer Area

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My Apps portal	

Section: (none)

Explanation

Explanation/Reference:

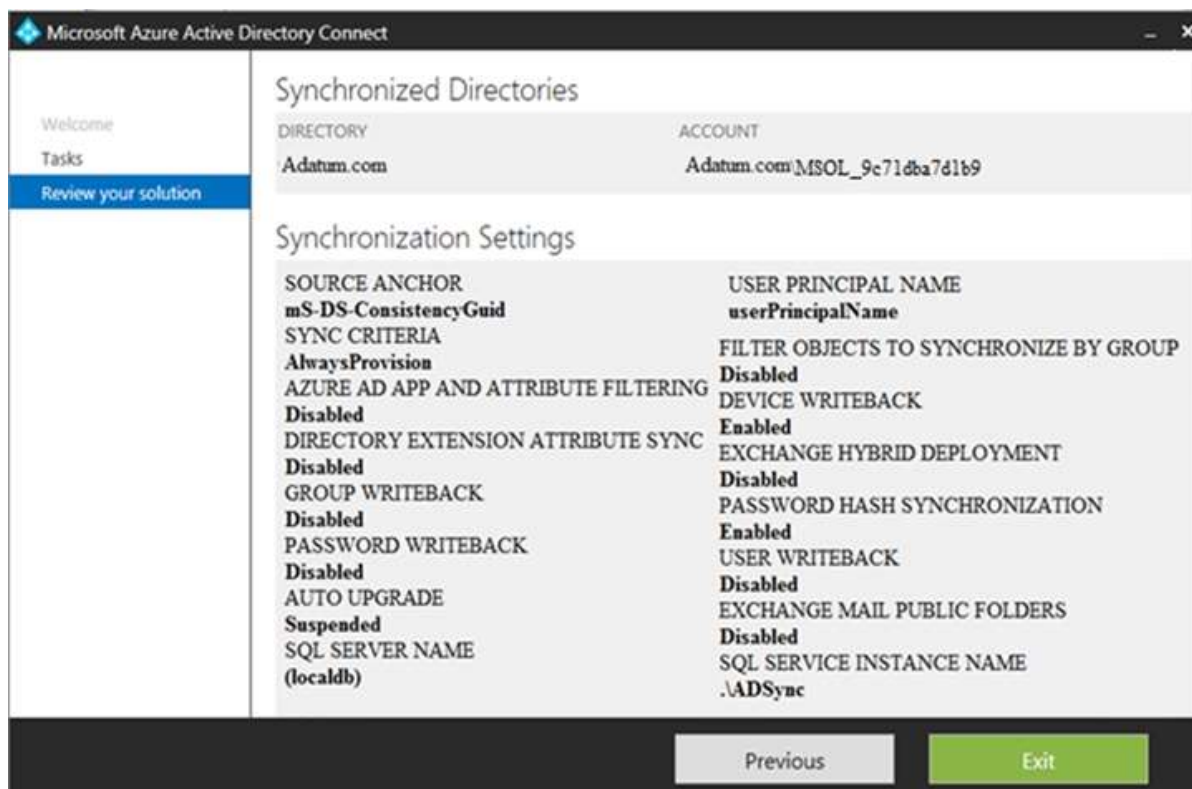
References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

QUESTION 5

HOTSPOT

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.

Hot Area:

Answer Area

If you reset a password in Azure AD of a synced user, the password will [answer choice].

be overwritten	V
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	V
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

Correct Answer:

Answer Area

If you reset a password in Azure AD of a synced user, the password will [answer choice].

be overwritten	V
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	V
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 6

You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.

You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network.

What should you do first?

- A. From the Azure Active Directory admin center, create a new certificate
- B. Enable Application Proxy in Azure AD
- C. From Active Directory Administrative Center, create a Dynamic Access Control policy
- D. From the Azure Active Directory admin center, configure authentication methods

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10>

QUESTION 7

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user.

You plan to assign the Reports reader role to the user.

You need to view the permissions of the Reports reader role.

Which admin center should you use?

- A. Azure Active Directory
- B. Cloud App Security
- C. Security & Compliance
- D. Microsoft 365

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

You have a Microsoft 365 E5 subscription.

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

What should you use to achieve the goal?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Your company has a Microsoft 365 subscription.

The company does not permit 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 Endpoint Manager
- 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 Endpoint Manager

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

HOTSPOT

You have a Microsoft 365 E5 subscription.

Users and device objects are added and removed daily. Users in the sales department frequently change their device.

You need to create three following groups:

Name	Requirement
Group1	All the devices of users where the Department attribute is set to Sales
Group2	All the users where the Department attribute is set to Sales
Group3	All the devices where the deviceOwnership attribute is set to Company.

The solution must minimize administrative effort.

What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Groups that have assigned membership:

	▼
0	
1	
2	
3	

Groups that have dynamic membership:

	▼
0	
1	
2	
3	

Correct Answer:

Answer Area

Groups that have assigned membership:	▼ 0 1 2 3
Groups that have dynamic membership:	▼ 0 1 2 3

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Group 1 has to be assigned because you can't create a device group based on the device owners' attributes.

Group 2 can be dynamic because a user does have a department attribute.

Group 3 can be dynamic because a device does have a deviceownership attribute.

References:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md>

QUESTION 11

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

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

What should you include in the configuration?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 12
HOTSPOT

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	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user 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 change

You need to identify how the policy affects User1 and User2.

What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Must change their password:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 nor User2	

Prompted for MFA:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 nor User2	

Correct Answer:

Answer Area

Must change their password:

User1 only

User2 only

Both User1 and User2

Neither User1 nor User2

Prompted for MFA:

User1 only

User2 only

Both User1 and User2

Neither User1 nor User2

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

HOTSPOT

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 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.

Hot Area:

Answer Area

User1:

	▼
Blocked	
Can sign in without MFA	
Prompted for MFA	

User2:

	▼
Blocked	
Can sign in without MFA	
Prompted for MFA	

Correct Answer:

Answer Area

User1:

	▼
Blocked	
Can sign in without MFA	
Prompted for MFA	

User2:

	▼
Blocked	
Can sign in without MFA	
Prompted for MFA	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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

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

You need to view Azure AD Connect events.

You use the Security event log on Server1.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 15

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 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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 16

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 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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 17

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 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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 18

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 Security & Compliance admin center, download a report.
- B. From Azure Log Analytics, query the logs.
- C. From the Security & Compliance admin center, perform an audit log search.
- D. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

HOTSPOT

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

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

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

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

Name	Assignment type
UserA	Permanent
UserB	Eligible
UserC	Eligible

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

- Maximum activation duration: 1 hour
- Notifications: Disable

- Incident/Request ticket: Disable
- Multi-Factor Authentication: Disable
- Require approval: Enable
- Selected approver: No results

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	☐	☐
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	☐	☐
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	☐	☐

Correct Answer:

Answer Area

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	☒	☐
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	☒	☐
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	☐	☒

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>**QUESTION 21****HOTSPOT**

You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to recommend an Azure AD Privileged Identity Management (PIM) solution that meets the following requirements:

- Administrators must be notified when the Security administrator role is activated.
- Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days.

Which Azure AD PIM setting should you recommend configuring for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Administrators must be notified when the Security administrator role is activated:

	▼
Alerts	
Roles	
Access reviews	

Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days:

	▼
Alerts	
Roles	
Access reviews	

Correct Answer:

Answer Area

Administrators must be notified when the Security administrator role is activated:

	▼
Alerts	
Roles	
Access reviews	

Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days:

	▼
Alerts	
Roles	
Access reviews	

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new>

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?tabs=new>

QUESTION 22

SIMULATION

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.

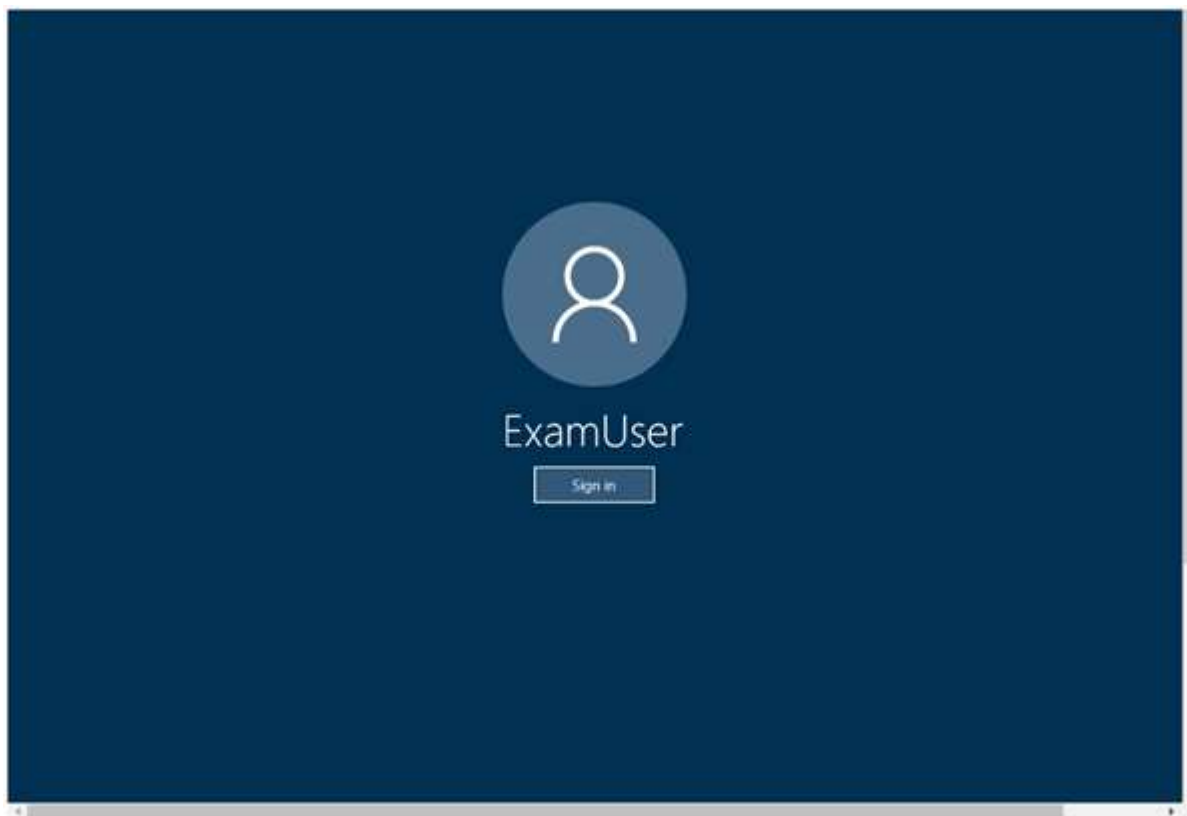
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 purposes 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.

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. In the Exchange Administration Center (EAC), navigate to **Permissions > Admin Roles**.
2. Select the group: **Organization Management** and then click on **Edit**.
3. In the **Members** section, click on **Add**.
4. Select the users, USGs, or other role groups you want to add to the role group, click on **Add**, and then click on **OK**.
5. 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-Organization-Management-to-the-account-that-is-performing-a-Public-Folder-migration->

<https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo>

QUESTION 23

SIMULATION

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.

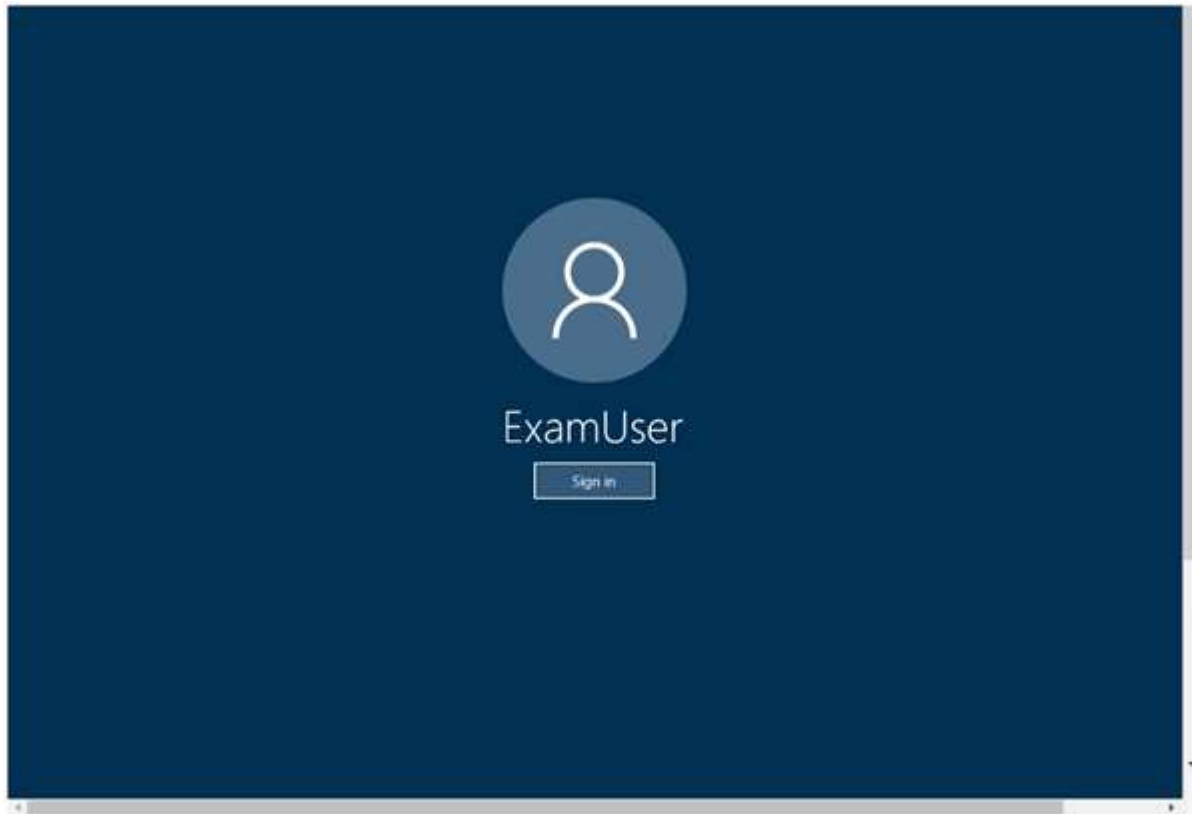
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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 purposes only:

Lab instance: 11032396

You need to ensure that each user can join up to five devices to Azure Active Directory (Azure AD).

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. After signing into **the Microsoft 365 admin center**, click **Admin centers > Azure Active Directory > Devices**.
2. Navigate to **Device Settings**.
3. Set the **Users may join devices to Azure AD** setting to **All**.
4. Set the **Additional local administrators on Azure AD joined devices** setting to **None**.
5. Set the **Users may register their devices with Azure AD** setting to **All**.
6. Leave the **Require Multi-Factor Auth to join devices** setting on its default setting.
7. Set the **Maximum number of devices** setting to **5**.
8. Set the **Users may sync settings and app data across devices** setting to **All**.
9. Click the **Save** button at the top left of the screen.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/use-your-free-azure-ad-subscription-in-office-365?view=o365-worldwide>

QUESTION 24**SIMULATION**

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.

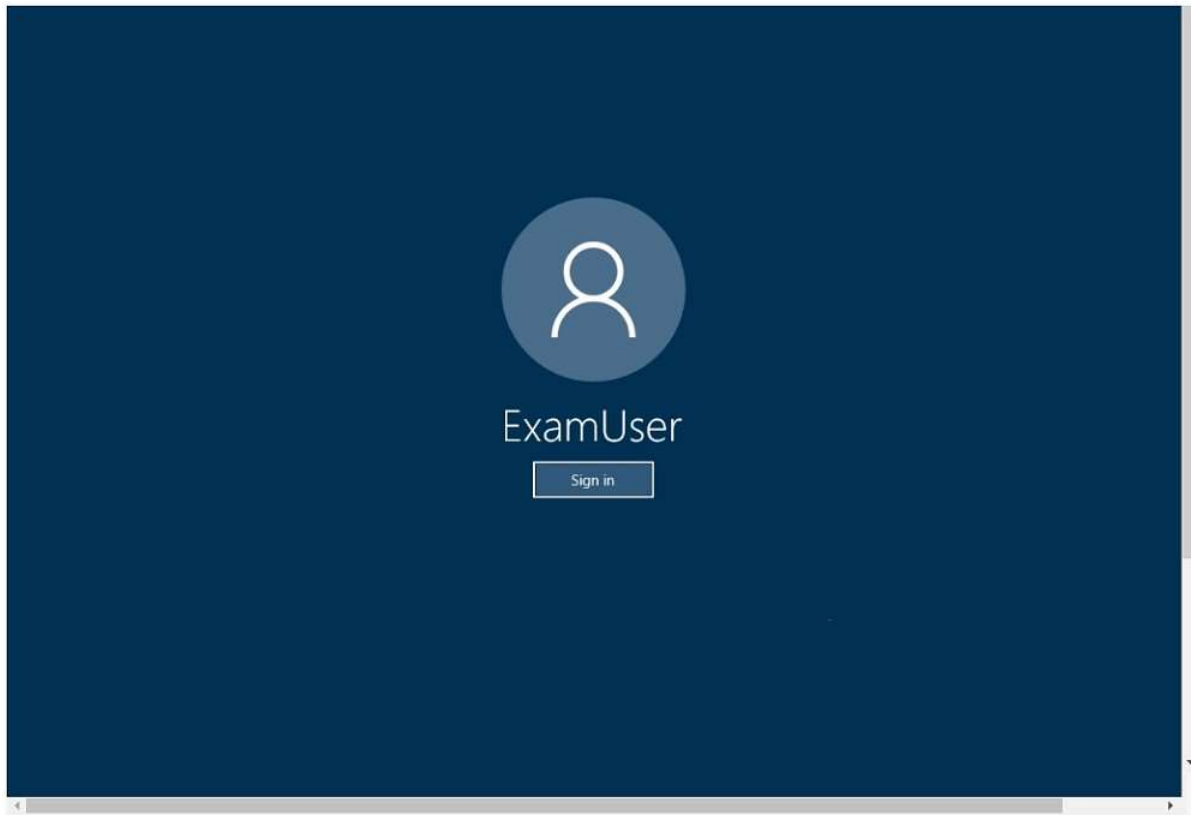
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 have 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 purposes only:

Lab instance: 11032396

You need to ensure that group owners renew their Office 365 groups every 180 days.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Set group expiration

1. Open the Azure AD admin center with an account that is a global administrator in your Azure AD organization.
2. Select **Groups**, then select **Expiration** to open the expiration settings.

Home > Contoso > Groups - Expiration

Groups - Expiration

Contoso - Azure Active Directory

Save Discard

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

Group lifetime (in days) * ⓘ 180

Email contact for groups with no owners * admin@contoso.com ✓

Enable expiration for these Office 365 groups ⓘ All Selected None

Left sidebar menu:

- All groups
- Deleted groups
- Diagnose and solve problems
- Settings
 - General
 - Expiration**
 - Naming policy
- Activity
 - Access reviews
 - Audit logs
 - Bulk operation results (Preview)
- Troubleshooting + Support
 - New support request

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

Reference:

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

Implement and manage threat protection

Testlet 1

Overview

Fabrikam, Inc. is a manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements

Fabrikam identifies the following issues:

- Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.
- Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes

Fabrikam plans to implement the following changes:

- Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory
- Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration

Fabrikam identifies the following application requirements for managing workload applications:

- User administrators will work from different countries
- User administrators will use the Azure Active Directory admin center
- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements

Fabrikam identifies the following security requirements:

- Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
- Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement
- Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
- Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
- Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
- The location of the user administrators must be audited when the administrators authenticate to Azure AD
- Email messages that include attachments containing malware must be delivered without the attachment
- The principle of least privilege must be used whenever possible

QUESTION 1**HOTSPOT**

You need to recommend an email malware solution that meets the security requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Policy to create:

ATP safe attachments	V
ATP Safe Links	
Exchange Online Anti-spam	
Exchange Online Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

Correct Answer:

Answer Area

Policy to create:

ATP safe attachments	V
ATP Safe Links	
Exchange Online Anti-spam	
Exchange Online Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

HOTSPOT

You install Azure ATP sensors on domain controllers.

You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.

You need to meet the security requirements for Azure ATP reporting.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Policy to edit:

	▼
Default Domain Controllers Policy	
Default Domain Policy	
A local policy on one domain controller	

Audit setting to configure:

	▼
Audit User Account Management	
Audit Computer Account Management	
Audit Other Account Management Events	
Audit Security Group Management	

Correct Answer:

Answer Area

Policy to edit:

	▼
Default Domain Controllers Policy	
Default Domain Policy	
A local policy on one domain controller	

Audit setting to configure:

	▼
Audit User Account Management	
Audit Computer Account Management	
Audit Other Account Management Events	
Audit Security Group Management	

Section: (none)

Explanation

Explanation/Reference:

References:

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

Implement and manage threat protection

Testlet 2

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment

Internal Network Infrastructure

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements

Planned Changes

Litware plans to implement the following changes:

- Migrate the email system to Microsoft Exchange Online
- Implement Azure AD Privileged Identity Management

Security Requirements

Litware identifies the following security requirements:

- Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
- Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
- Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
- Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
- Implement a permanent eligible assignment of the Compliance administrator role for User1
- Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
- Prevent access to Azure resources for the guest user accounts by default
- Ensure that all domain-joined computers are registered to Azure AD

Multi-factor authentication (MFA) Requirements

Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.

You identify the following requirements for testing MFA:

- Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must **NOT** be used on the Chicago office internal network.
- If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
- Any disruption of legitimate authentication attempts must be minimized.

General Requirements

Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

QUESTION 1

DRAG DROP

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.

Select and Place:

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

Correct Answer:

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

You need to enable and configure Microsoft Defender ATP to meet the security requirements. What should you do?

- A. Configure port mirroring
- B. Create the `ForceDefenderPassiveMode` registry setting
- C. Download and install the Microsoft Monitoring Agent
- D. Run `WindowsDefenderATPOnboardingScript.cmd`

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Implement and manage threat protection

Testlet 3

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea**"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	<i>Not applicable</i>	GroupA
Device6	Windows 10	Enabled	<i>None</i>

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	<i>None</i>
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	<i>None</i>

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management

QUESTION 1

HOTSPOT

You are evaluating which devices are compliant in Endpoint Manager.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Device2 is compliant.	☐	☐
Device5 is compliant.	☐	☐
Device6 is compliant.	☐	☐

Correct Answer:

Answer Area

Statements	Yes	No
Device2 is compliant.	☒	☐
Device5 is compliant.	☐	☒
Device6 is compliant.	☒	☐

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

HOTSPOT

Which policies apply to which devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

DevicePolicy1:	None
	Device1 only
	Device3 only
	Device2 and Device3 only
	Device1 and Device3 only
	Device1, Device2, and Device3

DevicePolicy2:	None
	Device4 only
	Device2 and Device4 only
	Device2, Device3, and Device 4 only

Correct Answer:

Answer Area

DevicePolicy1:	None
	Device1 only
	Device3 only
	Device2 and Device3 only
	Device1 and Device3 only
	Device1, Device2, and Device3

DevicePolicy2:	None
	Device4 only
	Device2 and Device4 only
	Device2, Device3, and Device 4 only

Section: (none)

Explanation

Explanation/Reference:

Implement and manage threat protection

Question Set 4

QUESTION 1

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Endpoint Manager has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

- Protected apps: App1
- Exempt apps: App2
- Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Yes No

From Device1, User1 can copy data from App1 to App3.

☐☐

From Device2, User1 can copy data from App1 to App2.

☐☐

From Device2, User1 can copy data from App1 to App3.

☐☐

Correct Answer:

Answer Area

Yes No

From Device1, User1 can copy data from App1 to App3.

☐☒

From Device2, User1 can copy data from App1 to App2.

☒☐

From Device2, User1 can copy data from App1 to App3.

☒☐

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

You have a Microsoft 365 tenant.

You have 500 computers that run Windows 10.

You plan to monitor the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP) after the computers are enrolled in Microsoft Intune.

You need to ensure that the computers connect to Windows Defender ATP.

How should you prepare Intune for Windows Defender ATP?

- A. Configure an enrollment restriction
- B. Create a device configuration profile
- C. Create a conditional access policy
- D. Create a Windows Autopilot deployment profile

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/intune/advanced-threat-protection>

QUESTION 3

HOTSPOT

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 Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). Microsoft 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
Microsoft Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Microsoft 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.

Hot Area:

Answer Area

Statements

Yes

No

User1 can run an antivirus scan on Device1.

☐
☐

User2 can collect an investigation package from Device2.

☐
☐

User3 can isolate Device1.

☐
☐

Correct Answer:

Answer Area

Statements

Yes

No

User1 can run an antivirus scan on Device1.

☒☐

User2 can collect an investigation package from Device2.

☐☒

User3 can isolate Device1.

☐☒

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1.

How long after the Azure ATP cloud service is updated will Sensor1 be updated?

- A. 7 days
- B. 24 hours
- C. 1 hour
- D. 48 hours
- E. 12 hours

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

QUESTION 5

DRAG DROP

You have a Microsoft 365 subscription. All users use Microsoft Exchange Online.

Microsoft 365 is configured to use the default policy settings without any custom rules.

You manage message hygiene.

Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each option 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.

Select and Place:**Options**

ATP quarantine

The Junk Email folder of a user's mailbox

The Focused Inbox experience in a user's mailbox.

Answer Area

Messages that contain word-filtered content:

option

Messages that are classified as phishing:

option

Correct Answer:**Options**

ATP quarantine

The Junk Email folder of a user's mailbox

The Focused Inbox experience in a user's mailbox.

Answer Area

Messages that contain word-filtered content:

The Junk Email folder of a user's mailbox

Messages that are classified as phishing:

ATP quarantine

Section: (none)**Explanation****Explanation/Reference:****QUESTION 6**

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create?

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

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:**

References:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files#BKMK_ModQuarantineTime

QUESTION 7

Your company has 500 computers.

You plan to protect the computers by using Microsoft Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.

You need to recommend a remediation solution that meets the following requirements:

- Microsoft Defender ATP administrators must manually approve all remediation for the executives
- Remediation must occur automatically for all other users

What should you recommend doing from Microsoft Defender Security Center?

- A. Configure 20 system exclusions on automation allowed/block lists
- B. Configure two alert notification rules
- C. Download an offboarding package for the computers of the 20 executives
- D. Create two machine groups

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 8

You have a Microsoft 365 Enterprise E5 subscription.

You use Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You need to integrate Microsoft Office 365 Threat Intelligence and Microsoft Defender ATP.
Where should you configure the integration?

- A. From the Microsoft 365 admin center, select **Settings**, and then select **Services & add-ins**.
- B. From the Security & Compliance admin center, select **Threat management**, and then select **Explorer**.
- C. From the Microsoft 365 admin center, select **Reports**, and then select **Security & Compliance**.
- D. From the Security & Compliance admin center, select **Threat management** and then select **Threat tracker**.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-office-365-ti-with-wdatp>

QUESTION 9

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

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

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

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

What should you do?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 10

You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com.

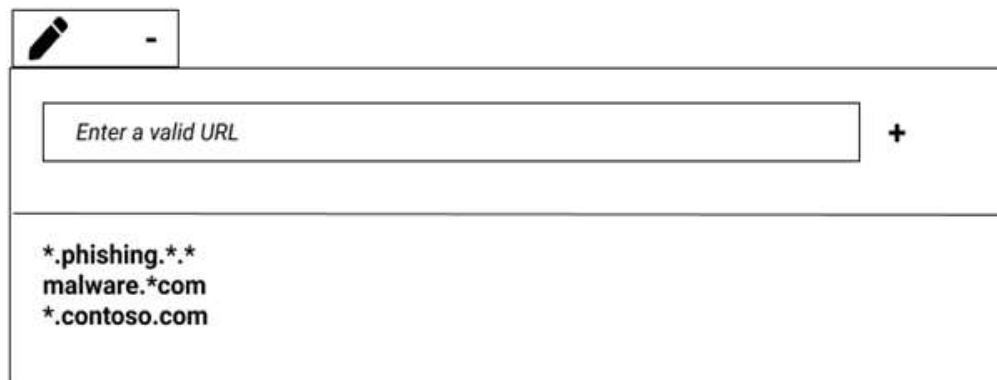
You create a safe links policy, as shown in the following exhibit.

Safe links policy for your organization

Settings that apply to content across Office 365

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.

Block the following URLs:



Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- ☒ Office 365 ProPlus, Office for iOS and Android
- ☒ Office Online of above applications

For the locations selected above:

- ☒ Do not track when users click safe links:
- ☒ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

- A. fabrikam.phishing.fabrikam.com
- B. malware.fabrikam.com

- C. fabrikam.contoso.com
- D. www.malware.fabrikam.com

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list-with-atp>

QUESTION 11

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of litwareinc.com.

You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.

Links

Choose the kind of link that's selected by default when users share items.

Default link type

☒ Shareable: Anyone with the link

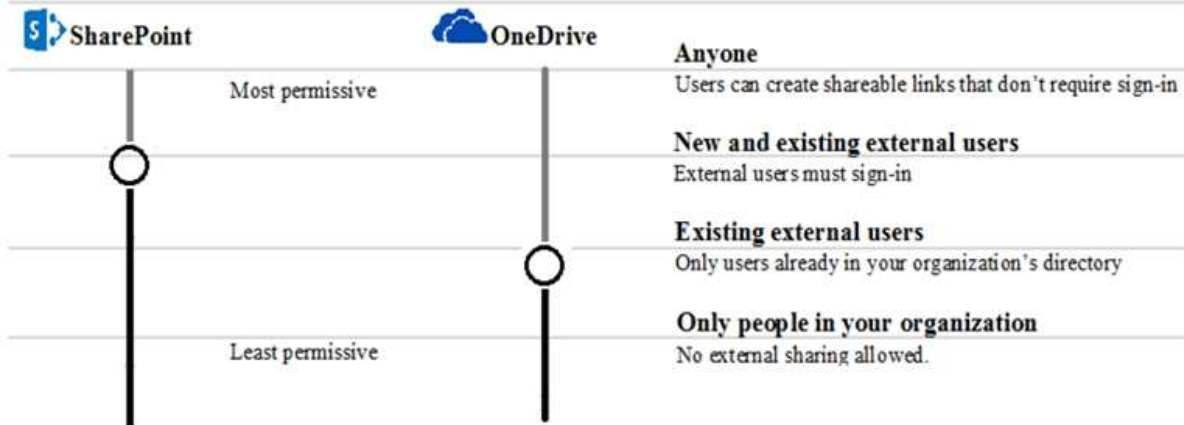
☐ Internal: Only people in your organization

☐ Direct: Specific people

Advanced settings for shareable links

External sharing

Users can share with:



Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

☒ Allow or block sharing with people on specific domains
Allow only these domains: Contoso.com, Adatum.com

[Add domains](#)

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.

Hot Area:

Answer Area

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice].

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

Correct Answer:

Answer Area

A user who has an email address of user1@fabrikam.com [answer choice].

	▼
cannot access OneDrive content	
can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

If a new guest user is created for user2@contoso.com [answer choice].

	▼
the user cannot access OneDrive content	
the user can access OneDrive content after a link is created	
must be added to a group before the user can access shared files	

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

QUESTION 12

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

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

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

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

What should you do?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 13

Several users in your Microsoft 365 subscription report that they received an email message without the attachment.

You need to review the attachments that were removed from the messages.

Which two tools can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. the Exchange admin center
- B. the Azure ATP admin center
- C. Outlook on the web
- D. the Security & Compliance admin center
- E. Microsoft Azure Security Center

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files>

QUESTION 14

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

You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.

Which type of device configuration profile should you use?

- A. Endpoint protection
- B. Device restrictions
- C. Identity protection
- D. Windows Defender ATP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

QUESTION 15

DRAG DROP

You have a Microsoft 365 E5 subscription.

All computers run Windows 10 and are onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You create a Microsoft Defender ATP machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

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.

Select and Place:

Actions

From Microsoft Defender Security Center, create a role.

From Microsoft Defender Security Center, configure the permissions for MachineGroup1.

From the Azure portal, create an RBAC role.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Azure Cloud Shell, run the Add-MsolRoleMember cmdlet.



Answer Area



Correct Answer:

Actions

From the Azure portal, create an RBAC role.

From Azure Cloud Shell, run the Add-MsolRoleMember cmdlet.



Answer Area

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Microsoft Defender Security Center, create a role.

From Microsoft Defender Security Center, configure the permissions for MachineGroup1.



Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

You have a hybrid Microsoft Exchange Server organization. All users have Microsoft 365 E5 licenses.

You plan to implement an Advanced Threat Protection (ATP) anti-phishing policy.

You need to enable mailbox intelligence for all users.

What should you do first?

- A. Configure attribute filtering in Microsoft Azure Active Directory Connect (Azure AD Connect)
- B. Purchase the ATP add-on
- C. Select **Directory extension attribute sync** in Microsoft Azure Active Directory Connect (Azure AD Connect)
- D. Migrate the on-premises mailboxes to Exchange Online

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies>

QUESTION 17
HOTSPOT

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.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2

You register devices in contoso.com as shown in the following table.

Name	Platform	Member of	Microsoft Intune managed
Device1	Windows 10	GroupA	Yes
Device2	iOS	GroupB	No

You create app protection policies in Intune as shown in the following table.

Name	Platform	Management state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	With enrollment	Group2
Policy3	iOS	Apps on Intune managed devices	GroupA
Policy4	iOS	Apps on Intune managed devices	GroupB

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	☐	☐
When User2 uses Device1, Policy2 applies.	☐	☐
When User2 uses Device2, Policy4 applies.	☐	☐

Correct Answer:

Answer Area

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	☐	☒
When User2 uses Device1, Policy2 applies.	☒	☐
When User2 uses Device2, Policy4 applies.	☐	☒

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/intune/apps/app-protection-policy>

QUESTION 19

DRAG DROP

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

You purchase a cloud app named App1 that supports session controls.

You need to ensure that access to App1 can be reviewed in real time.

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

Select and Place:

Actions

From the Azure Active Directory admin center, register App1.

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

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

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

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

From the Device Management admin center, add an App1.

Answer Area

Correct Answer:**Actions**

--

--

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

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

--

From the Device Management admin center, add an App1.

Answer Area

From the Azure Active Directory admin center, register App1.

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

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

Section: (none)**Explanation****Explanation/Reference:**

References:

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

QUESTION 20

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view ATP reports in the Threat management dashboard.

Which role provides User1 with the required role permissions?

- A. Security reader
- B. Message center reader

- C. Compliance administrator
- D. Information Protection administrator
- E. Service administrator
- F. Exchange administrator

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 21

You have a Microsoft 365 Enterprise E5 subscription.

You use Microsoft Defender Advanced Threat Protection (Microsoft 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 Office 365 Advanced Threat Protection (ATP)
- C. Create a Conditional Access App Control policy for accessing Office 365
- D. Integrate Office 365 Threat Intelligence and Microsoft Defender ATP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 22

You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.

Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.

You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.

The email addresses that you intend to spoof belong to the Executive group members.

What should you do first?

- A. From the Azure ATP admin center, configure the primary workspace settings
- B. From the Microsoft Azure portal, configure the user risk policy settings in Azure AD Identity Protection
- C. Enable MFA for the Research group members
- D. Migrate the Executive group members to Exchange Online

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 23

You have a Microsoft 365 E5 subscription.

You implement Advanced Threat Protection (ATP) safe attachments policies for all users.

User reports that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.

What should you do from ATP?

- A. Set the action to **Block**
- B. Add an exception
- C. Add a condition
- D. Set the action to **Dynamic Delivery**

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing>

QUESTION 24

HOTSPOT

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.

Hot Area:

Answer Area

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	

Correct Answer:

Answer Area

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	

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 25

HOTSPOT

You have a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) deployment that has the custom network indicators turned on. Microsoft Defender ATP protects two computers that run Windows 10 as shown in the following table.

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender ATP has the machine groups shown in the following table.

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp
Last	Ungrouped machines (default)	None

From Microsoft Defender Security Center, you create the URLs/Domains indicators shown in the following table.

URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	☐	☐
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	☐	☐
From a web browser on Computer2, you can open http://www.litwareinc.com.	☐	☐

Correct Answer:

Answer Area

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	☐	☒
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	☒	☐
From a web browser on Computer2, you can open http://www.litwareinc.com.	☐	☒

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

SIMULATION

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.

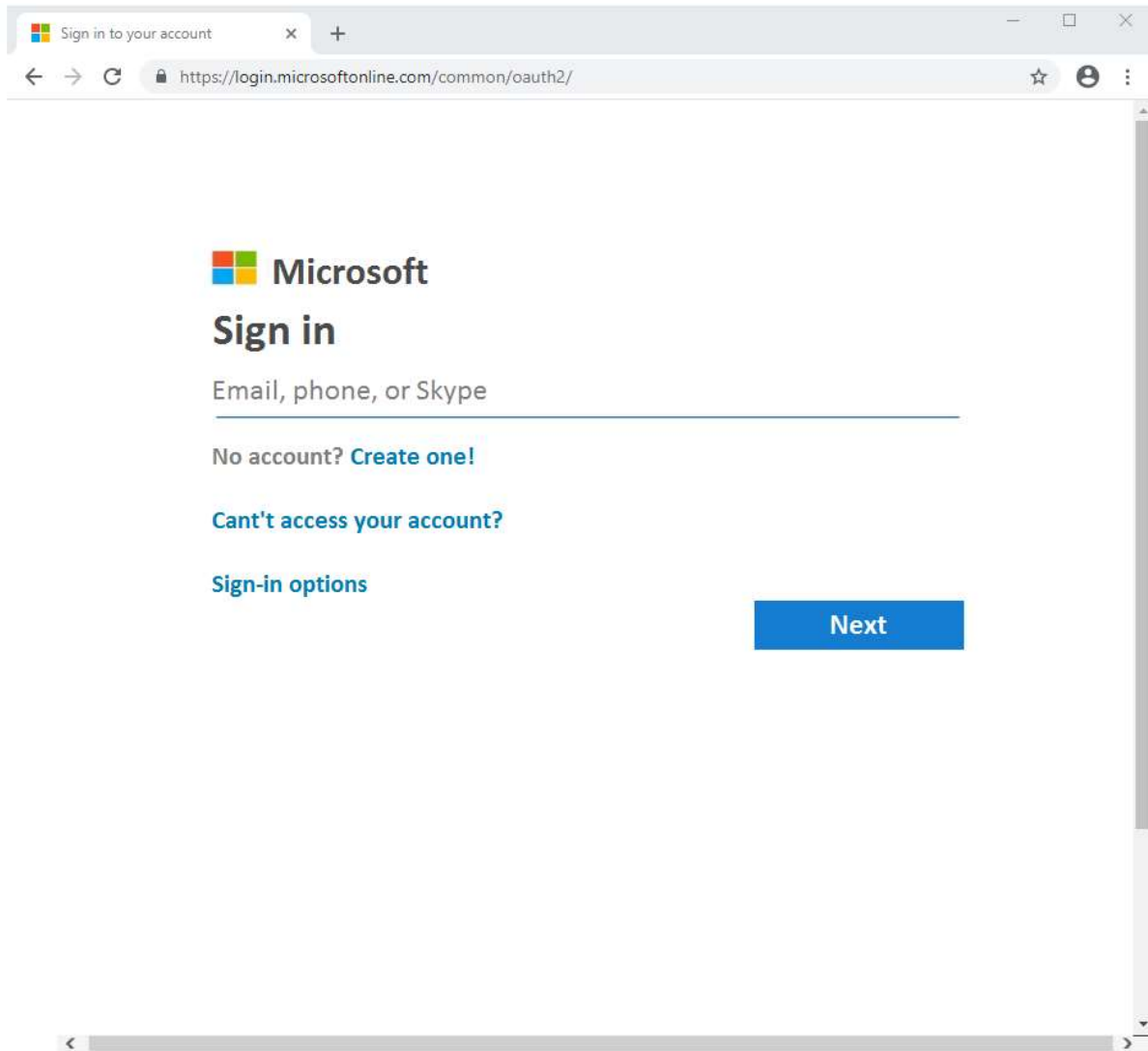
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 have 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.

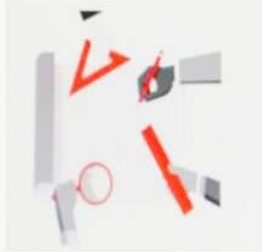
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home | office.com/?auth=2

Contoso electronics | Office 365

Good morning | Install Office

Start new

Outlook

OneDrive

Word

Excel

PowerPoint

OneNote

Skype

Calendar

People

All apps

Recommended

Excel

You edited this Jan 15

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart
lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15

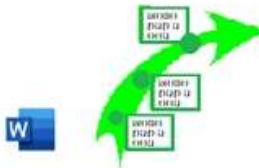


Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Ad Slogans



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](#) →

Recent Pinned Shared with me Discover



OneDrive



No recent folders

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

[Go to OneDrive](#) →

SharePoint

Frequent sites Following

- Sales and Marketing
- Retail
- Communication Site

[Go to SharePoint](#) →

SharePoint

Frequent sites Following

- Contoso Landings
- Contoso Web 3
- Executive Corner

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

You need to ensure that 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.

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

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.

Active users

Add a user	Add multiple users	Multi-factor authentication	Refresh	Export Users	...
Display name ↑	Username		Licenses		
Elise Mens			Office 365 E3		
info			Office 365 F1		
Rudy Mens			Microsoft Flow Free, Off		

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](#) 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

☐	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Elise Mens		Disabled
☐	info		Disabled
☐	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: Sign-in allowed users

Multi-Factor Auth status: Any

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
☐ Elise Mens		Disabled
☐ info		Disabled
☒ Rudy Mens		Disabled

Rudy Mens

quick steps

Enable

Manage user settings

Reference:

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

QUESTION 27 SIMULATION

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.

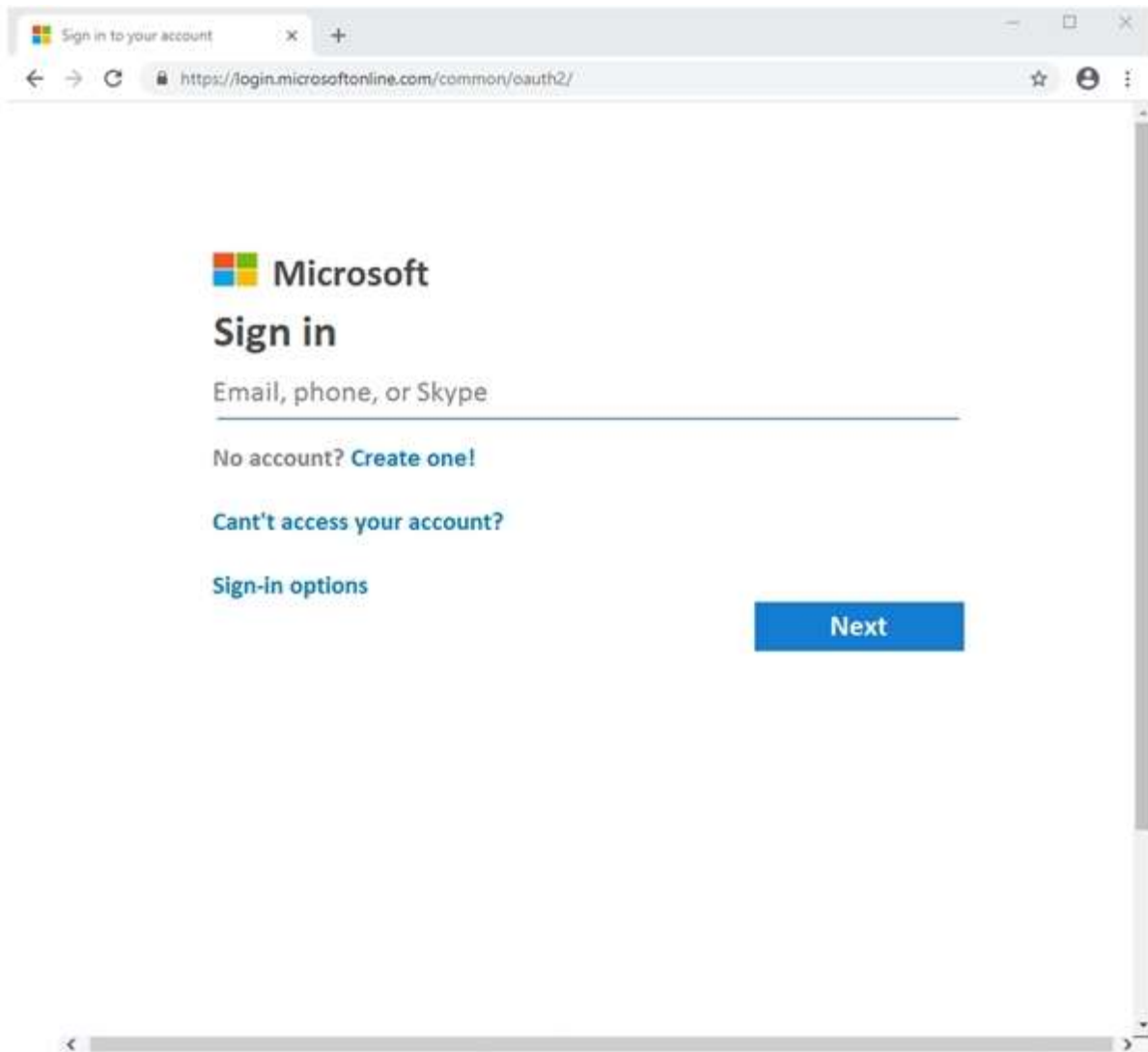
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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.

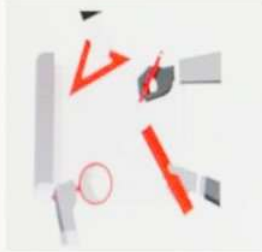
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home

Contoso electronics Office 365

Good morning

Install Office

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15

Excel

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

You edited this Jan 15

Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

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 →

Recent Pinned Shared with me Discover



OneDrive



No recent folders

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

Go to OneDrive →

SharePoint

Frequent sites Following

SM Sales and Marketing

R Retail

Cs Communication Site

SharePoint

Frequent sites Following

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

Go to SharePoint →

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

You need to ensure that all links to malware.contoso.com within documents stored in Microsoft Office 365 are blocked when the documents are accessed from Office 365 ProPlus applications.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. After signing in to the Microsoft 365 admin center, navigate to **Threat management**, choose **Policy > Safe Links**.
2. In the **Policies that apply to the entire organization** section, select **Default**, and then choose **Edit** (the Edit button resembles a pencil).



3. In the **Block the following URLs** section, add the malware.contoso.com link.
4. In the **Settings that apply to content except email** section, select all the options.
5. Choose **Save**.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide>

QUESTION 28

SIMULATION

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.

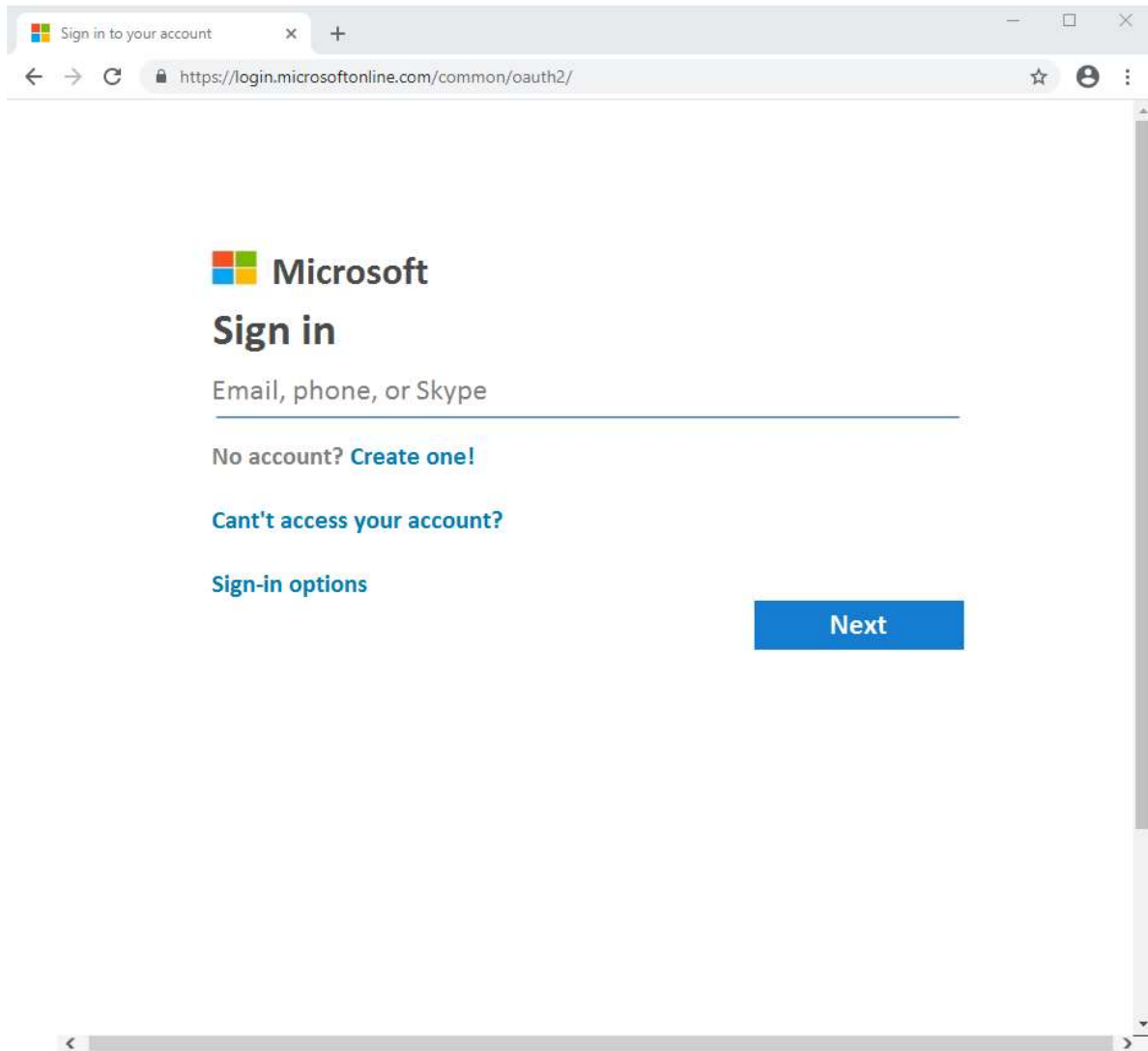
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 have 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.

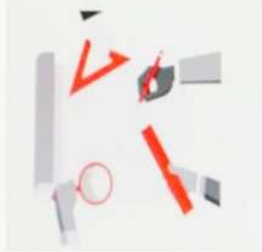
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home | office.com/7a4uthx2

Contoso electronics | Office 365

Good morning | Install Office

Start new | Outlook | OneDrive | Word | Excel | PowerPoint

OneNote | Skype | Calendar | People | All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent | Pinned | Shared with me | Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Ad Slogans



AD Slogans

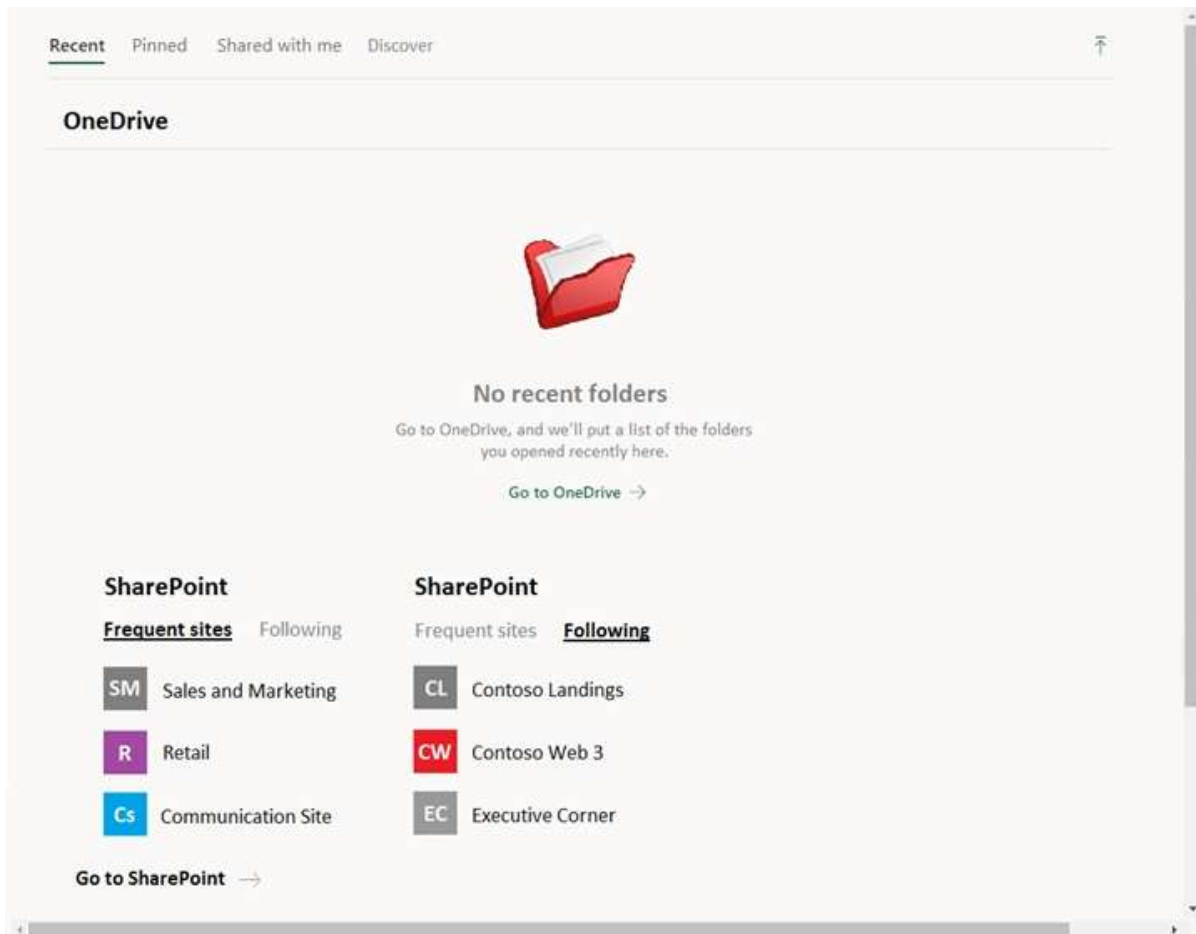
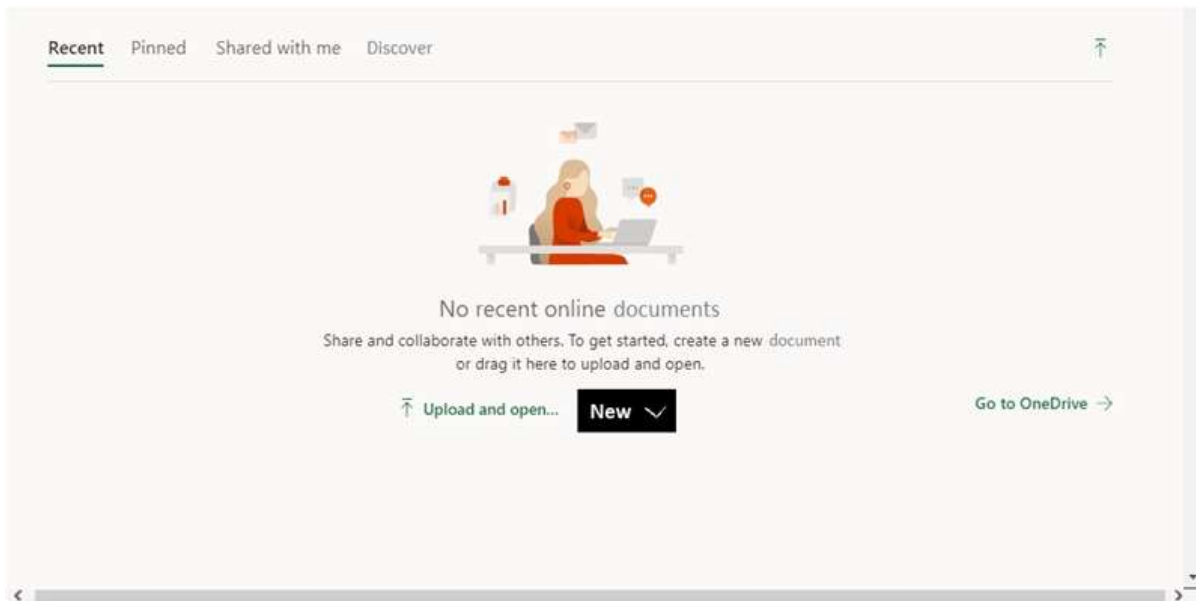
lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



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

You need to protect against phishing attacks. The solution must meet the following requirements:

- Phishing email messages must be quarantined if the messages are sent from a spoofed domain.
- As many phishing email messages as possible must be identified.

The solution must apply to the current SMTP domain names and any domain names added later.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. After signing in to the Microsoft 365 admin center, select **Security, Threat Management, Policy**, then **ATP Anti-phishing**.
2. Select **Default Policy** to refine it.
3. In the **Impersonation** section, select **Edit**.
4. Go to **Add domains to protect** and select the toggle to automatically include the domains you own.
5. Go to **Actions**, open the drop-down **If email is sent by an impersonated user**, and choose the **Quarantine message** action.
- Open the drop-down **If email is sent by an impersonated domain** and choose the **Quarantine message** action.
6. Select **Turn on impersonation safety tips**. Choose whether tips should be provided to users when the system detects impersonated users, domains, or unusual characters. Select **Save**.
7. Select **Mailbox intelligence** and verify that it's turned on. This allows your email to be more efficient by learning usage patterns.
8. Choose **Add trusted senders and domains**. Here you can add email addresses or domains that shouldn't be classified as an impersonation.
9. Choose **Review your settings**, make sure everything is correct, select **Save**, then **Close**.

Reference:

https://support.office.com/en-us/article/protect-against-phishing-attempts-in-microsoft-365-86c425e1-1686-430a-9151-f7176cce4f2c#ID0EAABAAA=Try_it!

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#example-anti-phishing-policy-to-protect-a-user-and-a-domain>

QUESTION 29

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

Name	Configuration
DC1	Domain controller
Server1	Member server

You plan to implement Azure Advanced Threat Protection (ATP) for the domain.

You install an Azure ATP standalone sensor on Server1.

You need to monitor the domain by using Azure ATP.

What should you do?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 30

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 31

SIMULATION

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.

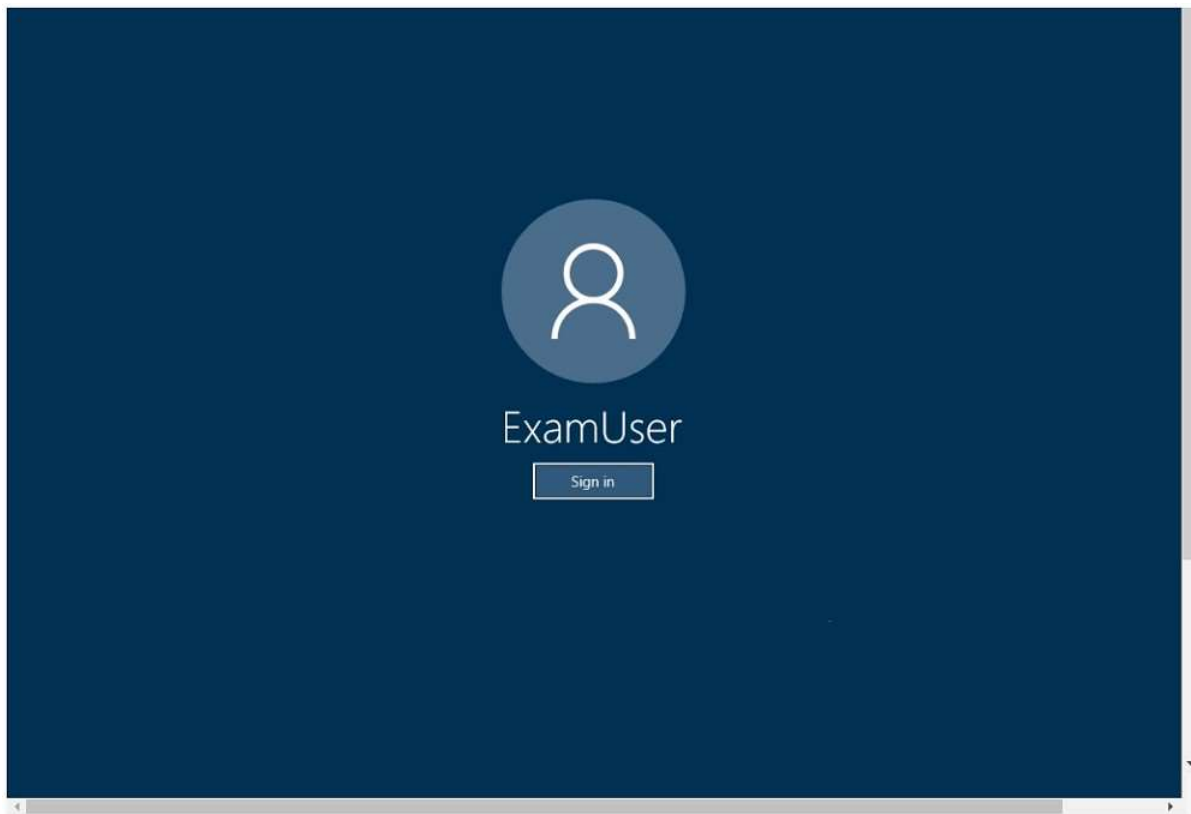
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 purposes only:

Lab instance: 11032396

You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA).

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

Correct Answer: See explanation below.

Section: (none)

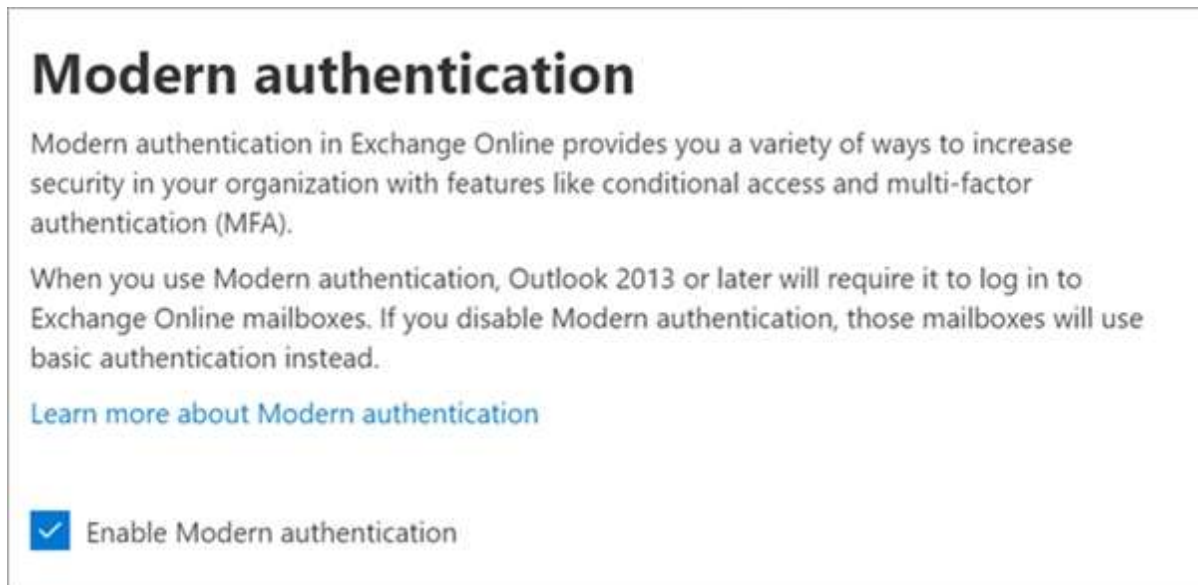
Explanation

Explanation/Reference:

Explanation:

Enable Modern authentication for your organization

1. To enable modern authentication, from the admin center, select **Settings** > **Settings** and then in the **Services** tab, choose **Modern authentication** from the list.
2. Check the **Enable modern authentication** box in the **Modern authentication** panel.



Enable multi-factor authentication for your organization

1. In the admin center, select **Users** and **Active Users**.
 2. In the **Active Users** section, Click on **multi-factor authentication**.
 3. On the **Multi-factor authentication** page, select **user** if you are enabling this for one user or select **Bulk Update** to enable multiple users.
 4. Click on **Enable** under **Quick Steps**.
 5. In the Pop-up window, Click on **Enable Multi-Factor Authentication**.
- After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide>

Implement and manage information protection

Testlet 1

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

Overview

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment

Network Infrastructure

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements

Fabrikam identifies the following issues:

- Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.
- Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements

Planned Changes

Fabrikam plans to implement the following changes:

- Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory
- Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration

Fabrikam identifies the following application requirements for managing workload applications:

- User administrators will work from different countries
- User administrators will use the Azure Active Directory admin center
- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements

Fabrikam identifies the following security requirements:

- Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed
- Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement
- Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations
- Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory
- Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location
- The location of the user administrators must be audited when the administrators authenticate to Azure AD
- Email messages that include attachments containing malware must be delivered without the attachment
- The principle of least privilege must be used whenever possible

QUESTION 1

You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.

What should you include in the recommendation? (Choose two). Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create an access review
- B. Assign the Global administrator role to User1
- C. Assign the Guest inviter role to User1
- D. Modify the External collaboration settings in the Azure Active Directory admin center

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Implement and manage information protection

Question Set 2

QUESTION 1

HOTSPOT

You have a Microsoft 365 subscription.

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

- Send notifications to users if they attempt to send attachments that contain EU social security numbers
- 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.

Hot Area:

Answer Area

Policies:

1	V
2	
3	

Rules:

1	V
2	
3	
4	

Correct Answer:

Answer Area

Policies:

1	V
2	
3	

Rules:

1	V
2	
3	
4	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

QUESTION 3

You create a data loss prevention (DLP) policy as shown in the following exhibit:

New DLP policy

What do you want to do if we detect sensitive info?

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

☒ Show policy tips to users and send them an email notification.

Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)

[Customize the tip and email](#)

Detect when a specific amount of sensitive info is being shared at one time.

☒ Detect when content that's being shared contains:

At least instances of the same sensitive info type.

☒ Send incident reports in email

By default, you and your global admin will automatically receive the email.

[Choose what to include in the report and who receives it](#)

☐ Restrict access or encrypt the content

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

What is the effect of the policy when a user attempts to send an email message that contains sensitive information?

- A. The user receives a notification and can send the email message
- B. The user receives a notification and cannot send the email message
- C. The email message is sent without a notification
- D. The email message is blocked silently

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

QUESTION 4

You have a Microsoft 365 subscription.

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

Which type of site collection should you create first?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bb-b944-448d-b83d-8fec4abcc24c>

QUESTION 5

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

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

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

Which type of Cloud App Security policy should you create?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 6

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.

You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	✓
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	✓
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Correct Answer:

Answer Area

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	✓
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	✓
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 7

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

You add CompanyConfidential to a global policy.

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

You need to ensure that the external recipients can open protected email messages sent to them.

You create a new label in the global policy and instruct the user to resend the email message.

Does that meet the goal?

A. Yes

B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

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

You need to ensure that the external recipients can open protected email messages sent to them.

You modify the encryption settings of the label.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

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

You need to ensure that the external recipients can open protected email messages sent to them.

You modify the content expiration settings of the label.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office 365	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1.

You need to apply Policy1.

To which groups can you apply Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On-premises Active Directory groups:

Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	V
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12, Group13, and Group14	

Correct Answer:

Answer Area

On-premises Active Directory groups:

Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	V
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12, Group13, and Group14	

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/prepare>

QUESTION 11

HOTSPOT

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:

- Rule1:
- Conditions: Label1, Detect content that's shared with people outside my organization

- Actions: Restrict access to the content for external users
 - User notifications: Notify the user who last modified the content
 - User overrides: On
 - Priority: 0
- Rule2:
 - Conditions: Label1 or Label2
 - Actions: Restrict access to the content
 - Priority: 1
- Rule3:
 - Conditions: Label2, Detect content that's shared with people outside my organization
 - Actions: Restrict access to the content for external users
 - User notifications: Notify the user who last modified the content
 - User overrides: On
 - Priority: 2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
External users can access File1	☐	☐
The users in contoso.com can access File2	☐	☐
External users can access File3	☐	☐

Correct Answer:

Statements	Yes	No
External users can access File1	☒	☐
The users in contoso.com can access File2	☐	☒
External users can access File3	☐	☒

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 13

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

- A. Run the `Set-SPOTenant` cmdlet and specify the `-ConditionalAccessPolicy` parameter.
- B. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
- D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps>

<https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

QUESTION 14

HOTSPOT

You have the Microsoft Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.

Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

You have the Azure Information Protection policies shown in the following table.

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User1 types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	☐	☐
If User1 types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	☐	☐
If User1 types "product2" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	☐	☐

Correct Answer:

Answer Area

Statements	Yes	No
If User1 types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	☐	☒
If User1 types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	☒	☐
If User1 types "product2" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	☐	☒

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

HOTSPOT

Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com.

The company has the offices shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/24	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

The tenant contains the users shown in the following table.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

You create the Microsoft Cloud App Security policy shown in the following exhibit.

Create filters for the policy

Act on:

☐ **Single activity:**
 Every activity that matches the filters

☒ **Repeated activity:**
 Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

☐ In a single app
☐ Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR

equals

From group equals

as

Alerts

☒ Create alert Use your organization's default settings
 Daily alert limit

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

Yes

No

In the Montreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

☐☐

In the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.

☐☐

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

☐☐

Correct Answer:

Answer Area

Statements

Yes

No

In the Montreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

☒☐

In the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.

☒☐

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

☐☒

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

A user stores the following files in Microsoft OneDrive:

- File.docx
- ImportantFile.docx
- File_Important.docx

You create a Microsoft Cloud App Security file policy Policy1 that has the filter shown in the following exhibit.

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING

Edit and preview results

X

File name

contains words

File

Apply to:

all files

Apply to:

all file owners

To which files does Policy1 apply?

- A. File_Important.docx only
- B. File.docx, ImportantFile.docx, and File_Important.docx
- C. File.docx only
- D. ImportantFile.docx only
- E. File.docx and File_Important.docx only

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 17

SIMULATION

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.

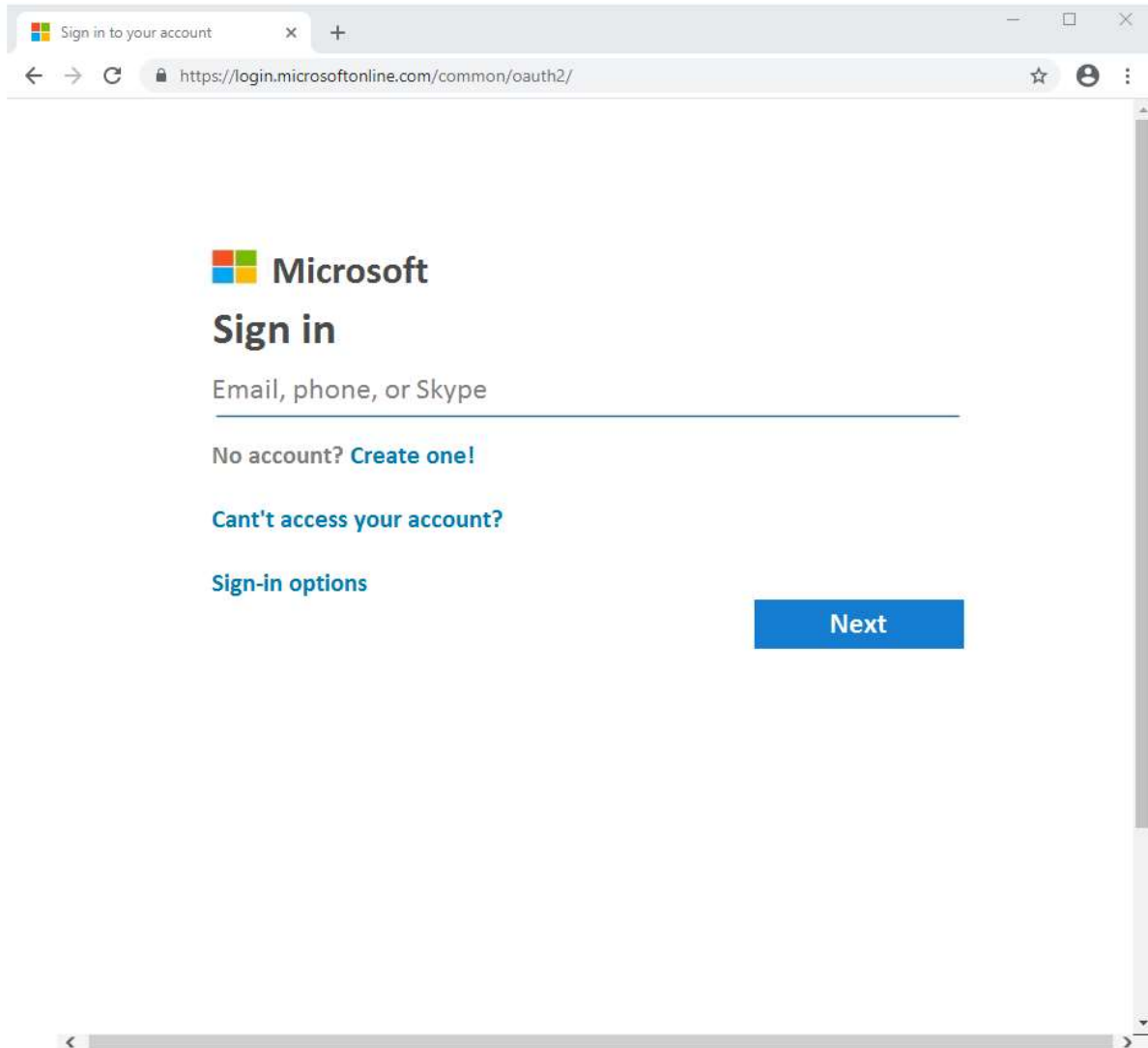
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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:

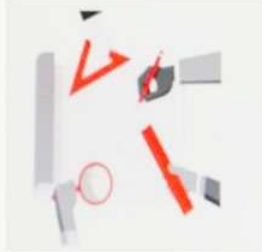
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home: office.com/?auth=2

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

Integrated Team Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Excel

Org Chart

Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15

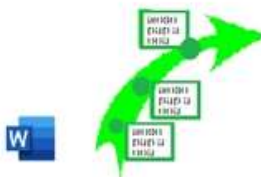


Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Ad Slogans



AD Slogans

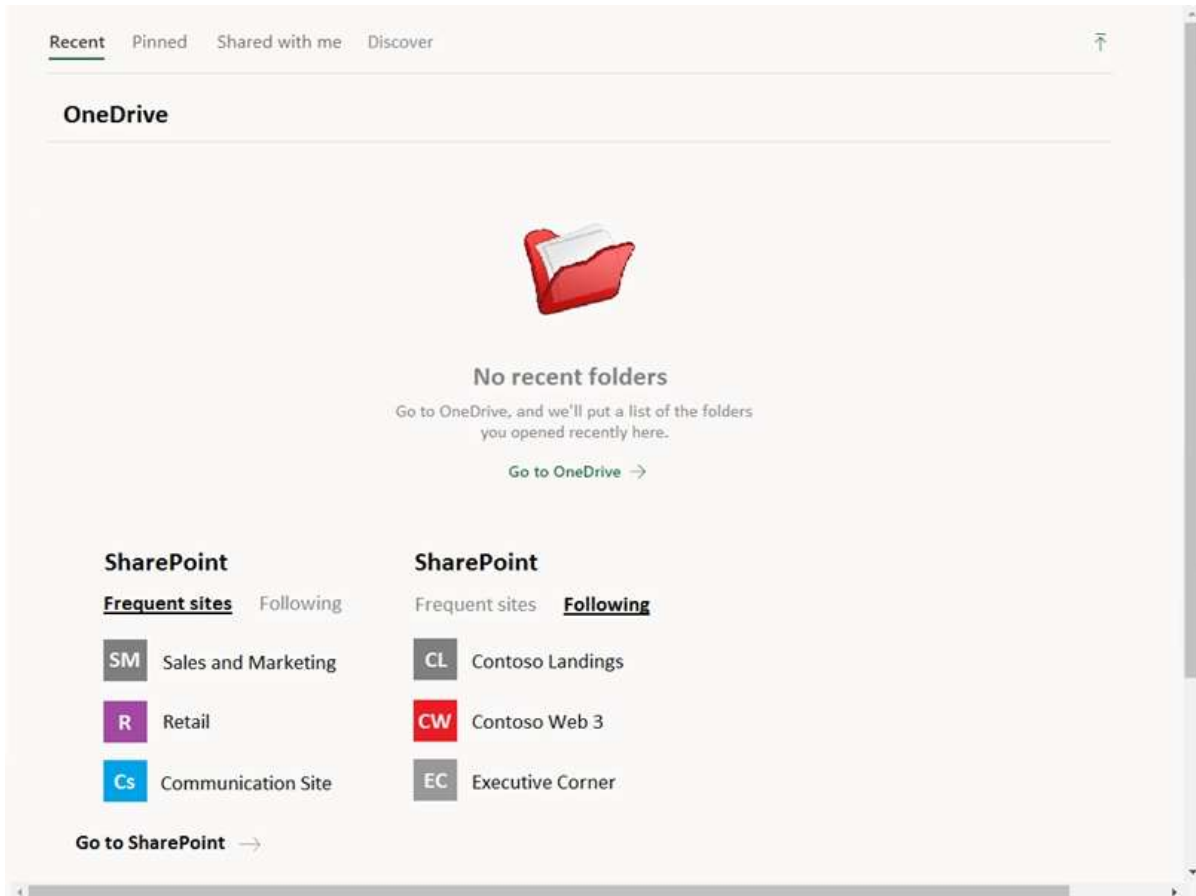
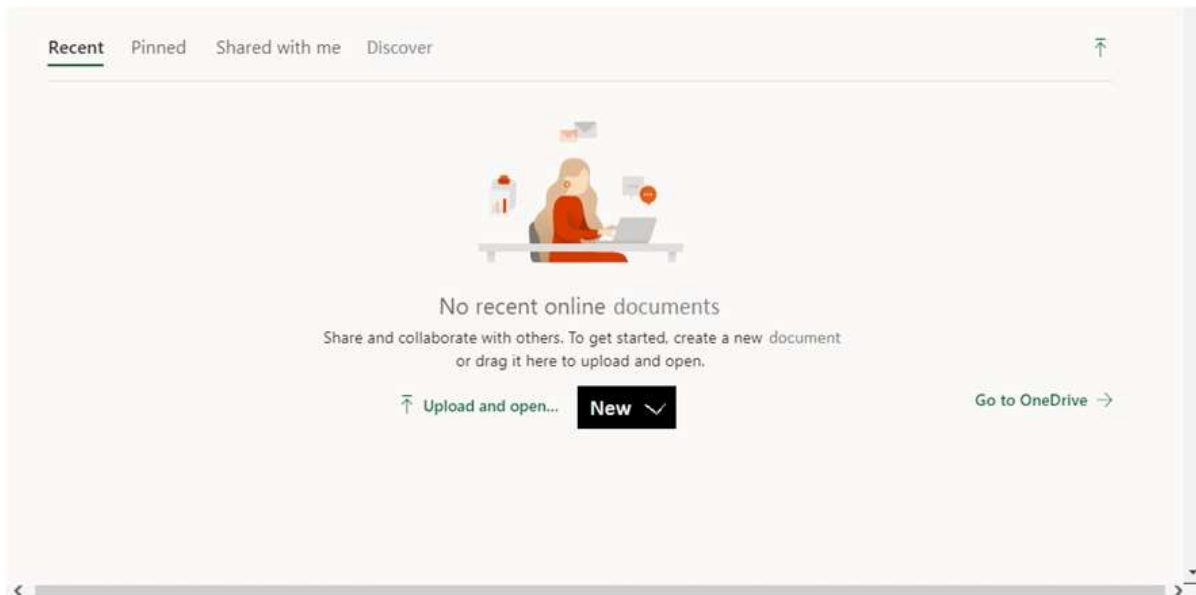
lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



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

You need to create an Azure Information Protection label to meet the following requirements:

- Content must expire after 21 days.
- Offline access must be allowed for 21 days only.
- Documents must be protected by using a cloud key.
- Authenticated users must be able to view content only.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. If you haven't already done so, open a new browser window and sign in to the Azure portal. Then navigate to the **Azure Information Protection** pane.
For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.
2. From the **Classifications > Labels** menu option: On the **Azure Information Protection - Labels** pane, select the label you want to change.
 - On the **Label** pane, locate **Set permissions for documents and emails containing this label**, and select **Protect**.
3. Select **Protection**.
4. On the **Protection** pane, select **Azure (cloud key)**.
5. Select **Set permissions** to define new protection settings in this portal.
6. If you selected **Set permissions** for **Azure (cloud key)**, this option lets you select users and usage rights. To specify the users that you want to be able to open protected documents and emails, select **Add permissions**. Then on the **Add permissions** pane, select the first set of users and groups who will have rights to use the content that will be protected by the selected label:
 - Choose **Select from the list** where you can then add all users from your organization by selecting **Add <organization name> - All members**. This setting excludes guest accounts. Or, you can select **Add any**

authenticated users, or browse the directory.

When you choose all members or browse the directory, the users or groups must have an email address. In a production environment, users and groups nearly always have an email address, but in a simple testing environment, you might need to add email addresses to user accounts or groups.

- Change the **File Content Expiration** setting to 21 days.
- Change the **Allow offline access** setting to 21 days.

When you have finished configuring the permissions and settings, click **OK**.

This grouping of settings creates a custom template for the Azure Rights Management service. These templates can be used with applications and services that integrate with Azure Rights Management.

7. Click **OK** to close the **Protection** pane and see your choice of **User defined** or your chosen template display for the **Protection** option in the **Label** pane.

8. On the **Label** pane, click **Save**.

9. On the **Azure Information Protection** pane, use the **PROTECTION** column to confirm that your label now displays the protection setting that you want:

- A check mark if you have configured protection.
- An x mark to denote cancellation if you have configured a label to remove protection.
- A blank field when protection is not set.

When you clicked **Save**, your changes are automatically available to users and services. There's no longer a separate publish option.

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection>

QUESTION 18

SIMULATION

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.

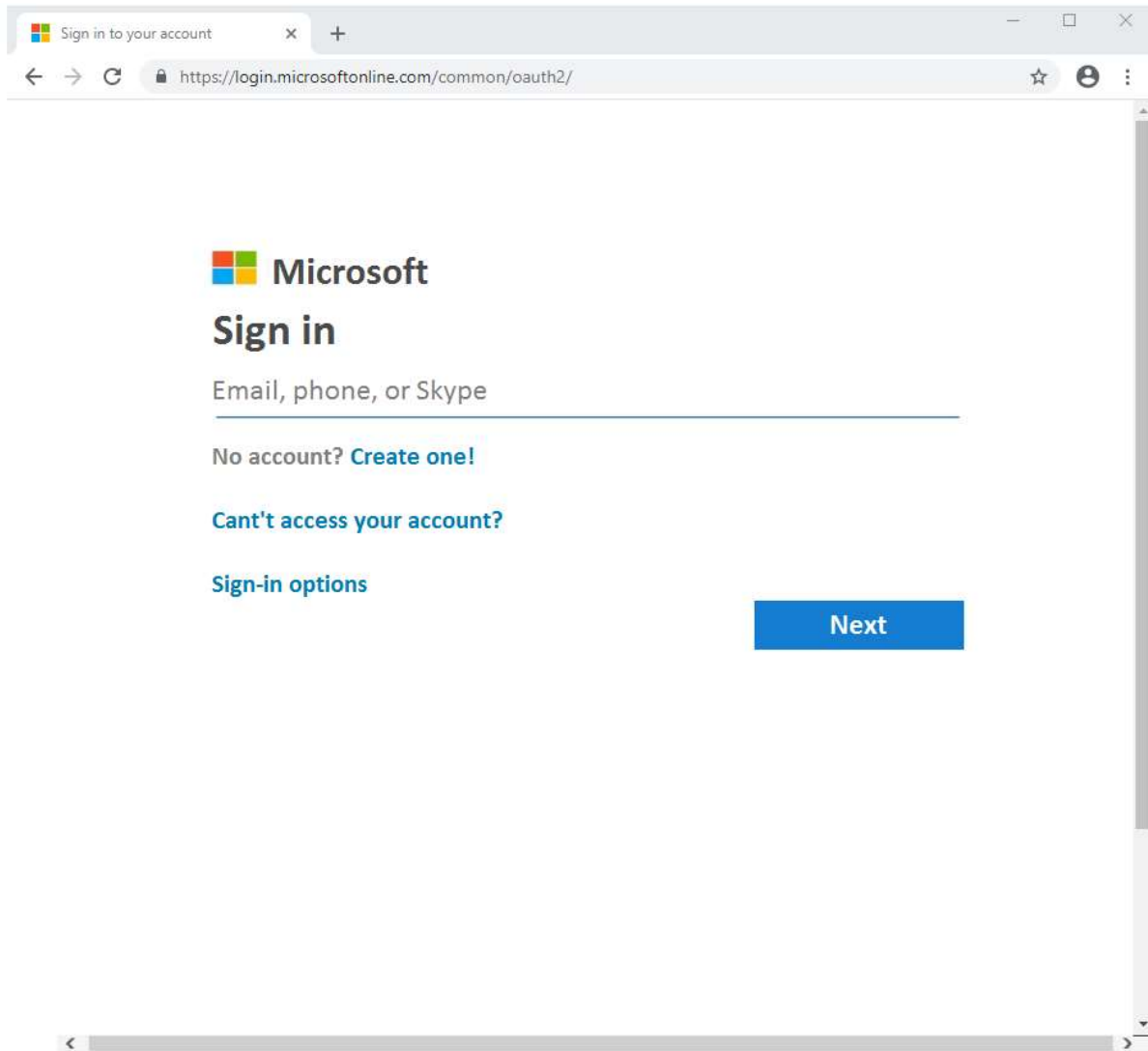
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 have 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.

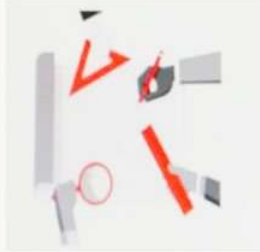
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home x +

office.com/?auth=2

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



Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15



Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Ad Slogans



AD Slogans

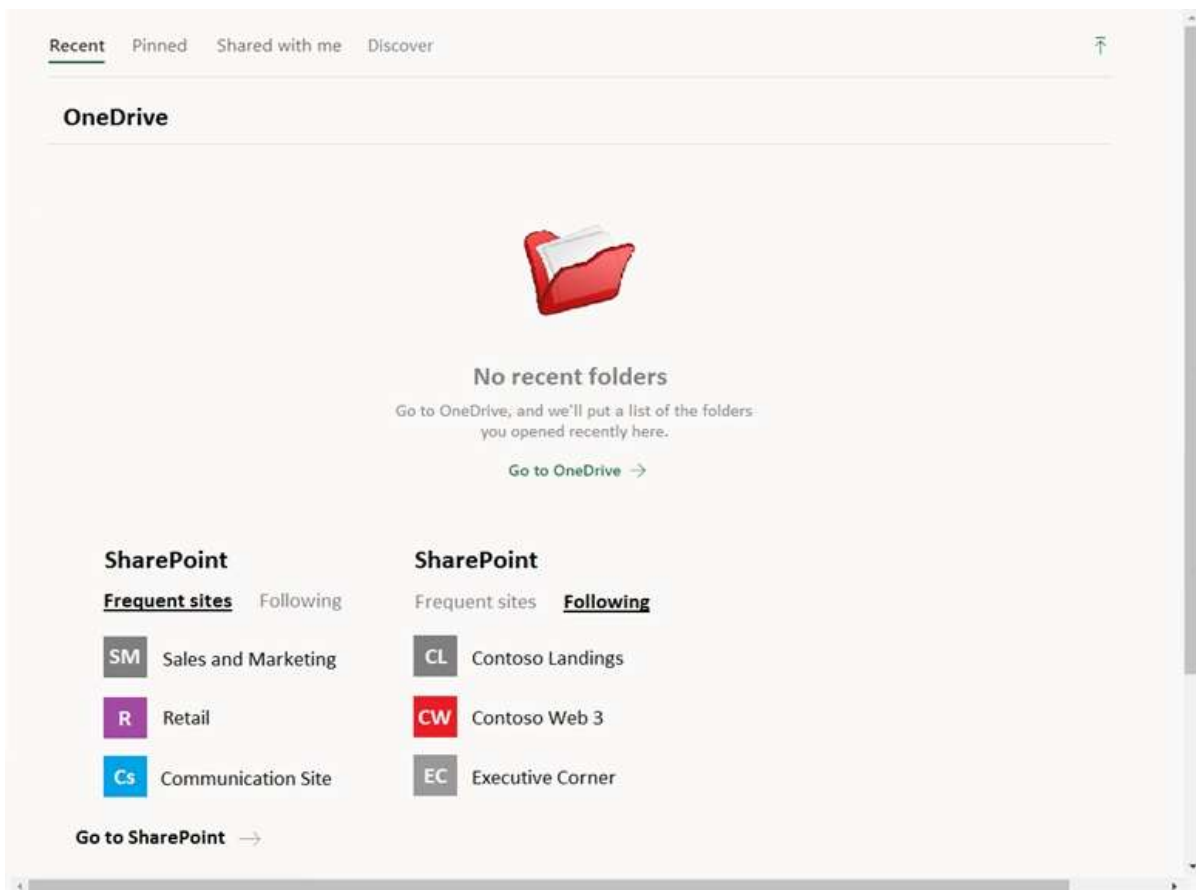
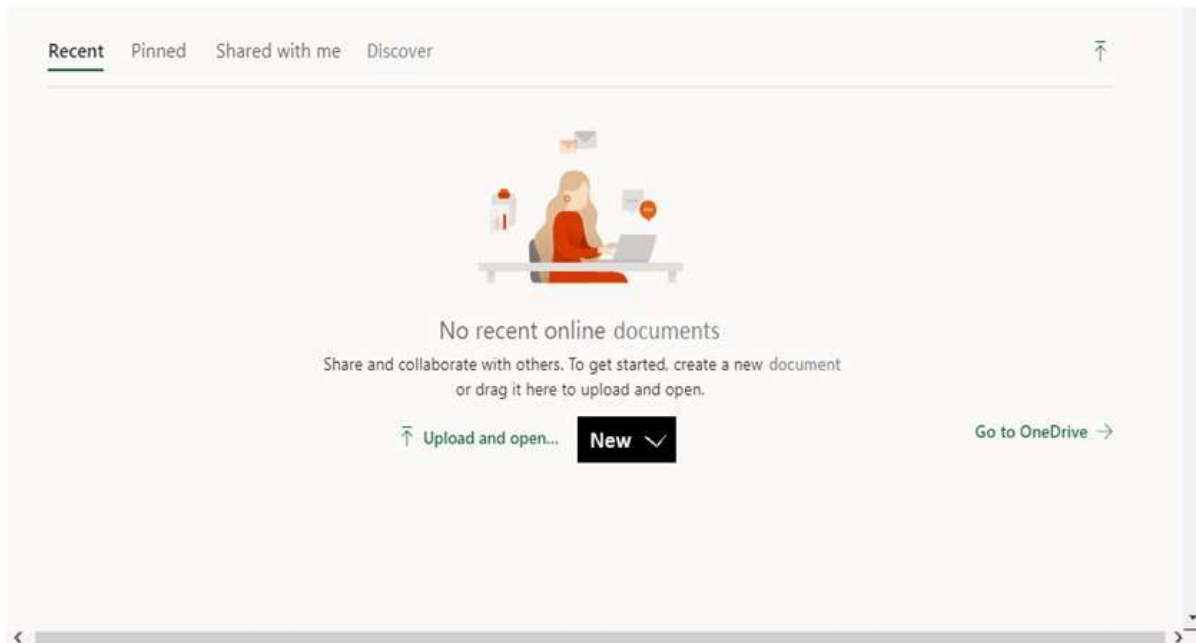
lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



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

You need to ensure that a user named Allan Deyoung can perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations. The solution must use the principle of least privilege.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. After signing in to the Microsoft 365 admin center, navigate to the Security & Compliance Center.
2. In the left pane of the security and compliance center, select **Permissions**, and then select the checkbox next to **eDiscovery Manager**.
3. On the **eDiscovery Manager** flyout page, do one of the following based on the eDiscovery permissions that you want to assign.

To make a user an eDiscovery Manager: Next to **eDiscovery Manager**, select **Edit**. In the **Choose eDiscovery Manager** section, select the **Choose eDiscovery Manager** hyperlink, and then select **+ Add**. Select the user (or users) you want to add as an eDiscovery manager, and then select **Add**. When you're finished adding users, select **Done**. Then, on the **Editing Choose eDiscovery Manager** flyout page, select **Save** to save the changes to the eDiscovery Manager membership.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide>

QUESTION 19

SIMULATION

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.

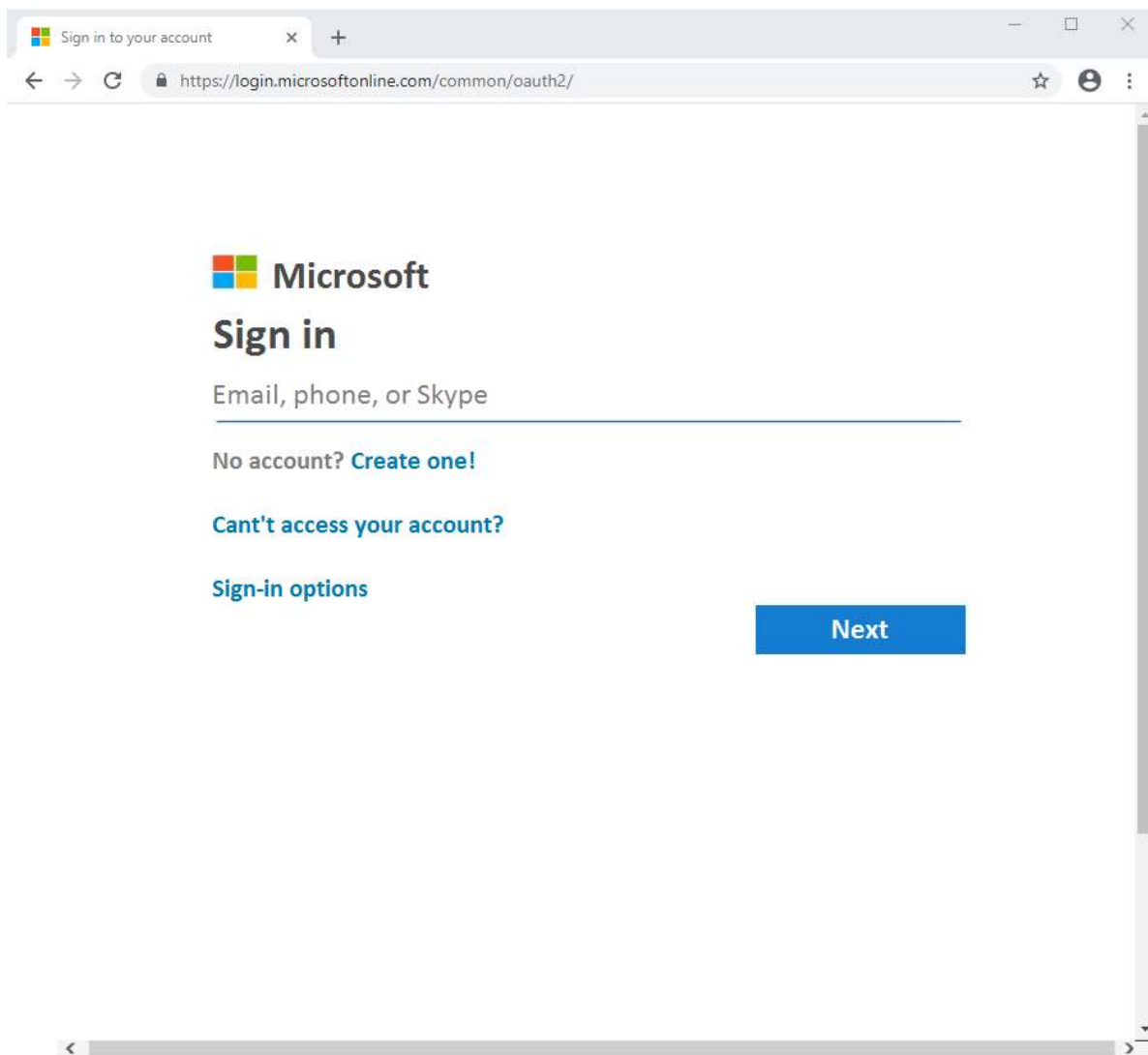
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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



The screenshot shows a web browser window with the address bar displaying "https://login.microsoftonline.com/common/oauth2/". The page content includes the Microsoft logo, the text "Sign in", a text input field labeled "Email, phone, or Skype", and several links: "No account? Create one!", "Can't access your account?", and "Sign-in options". A blue "Next" button is positioned to the right of the input field. The browser's address bar also shows a tab titled "Sign in to your account".

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:

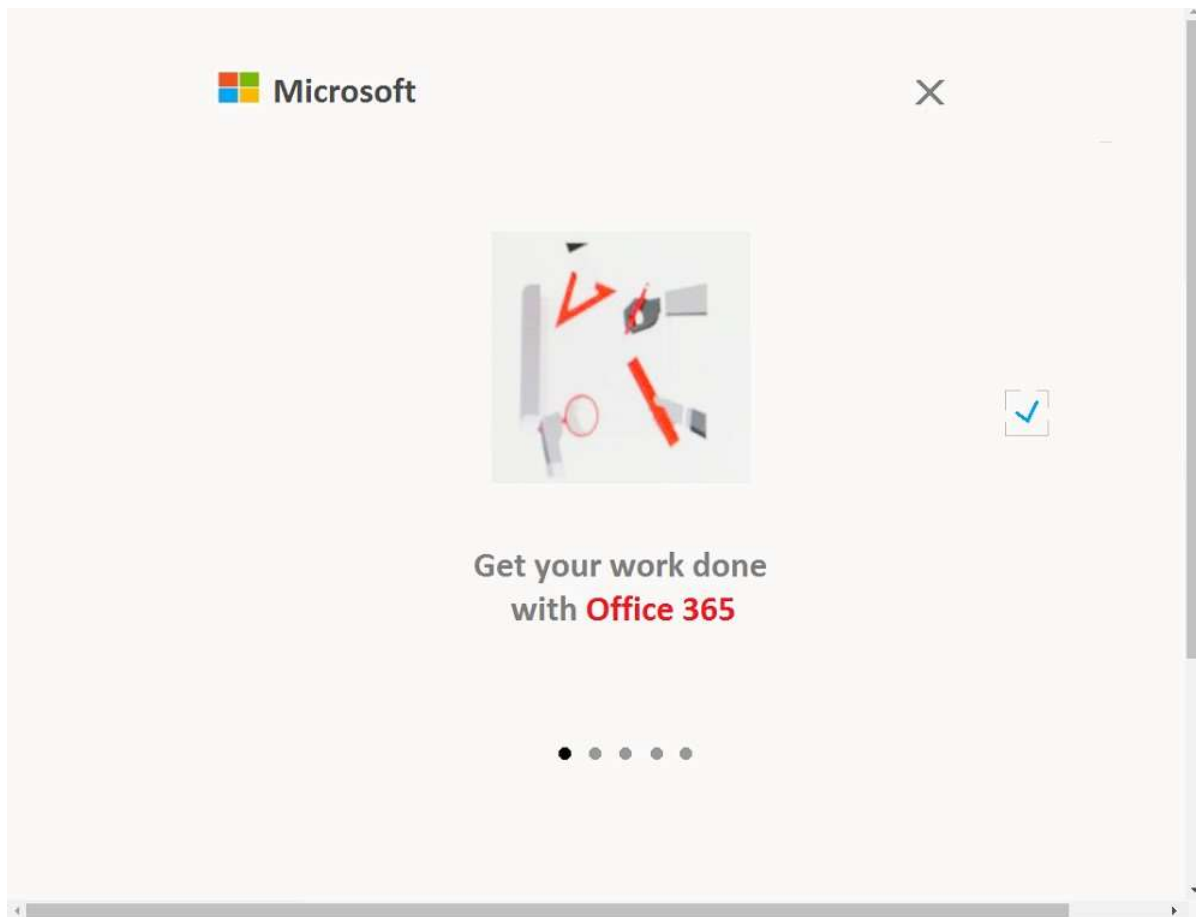
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308





Brainstorm
together in **Word**





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





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



Microsoft Office Home

office.com/tautiv2

Contoso electronics

Office 365

Good morning

Install Office

Start new

Outlook

OneDrive

Word

Excel

PowerPoint

OneNote

Skype

Calendar

People

All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview

lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process

lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

Org Chart

lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover

Recommended

 You edited this Jan 15

 You edited this Jan 15

 You edited this Jan 15



Excel

P and L Summary

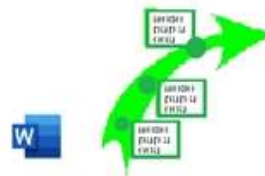
lodse000198.sharepoint.co...



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

Ad Slogans



AD Slogans

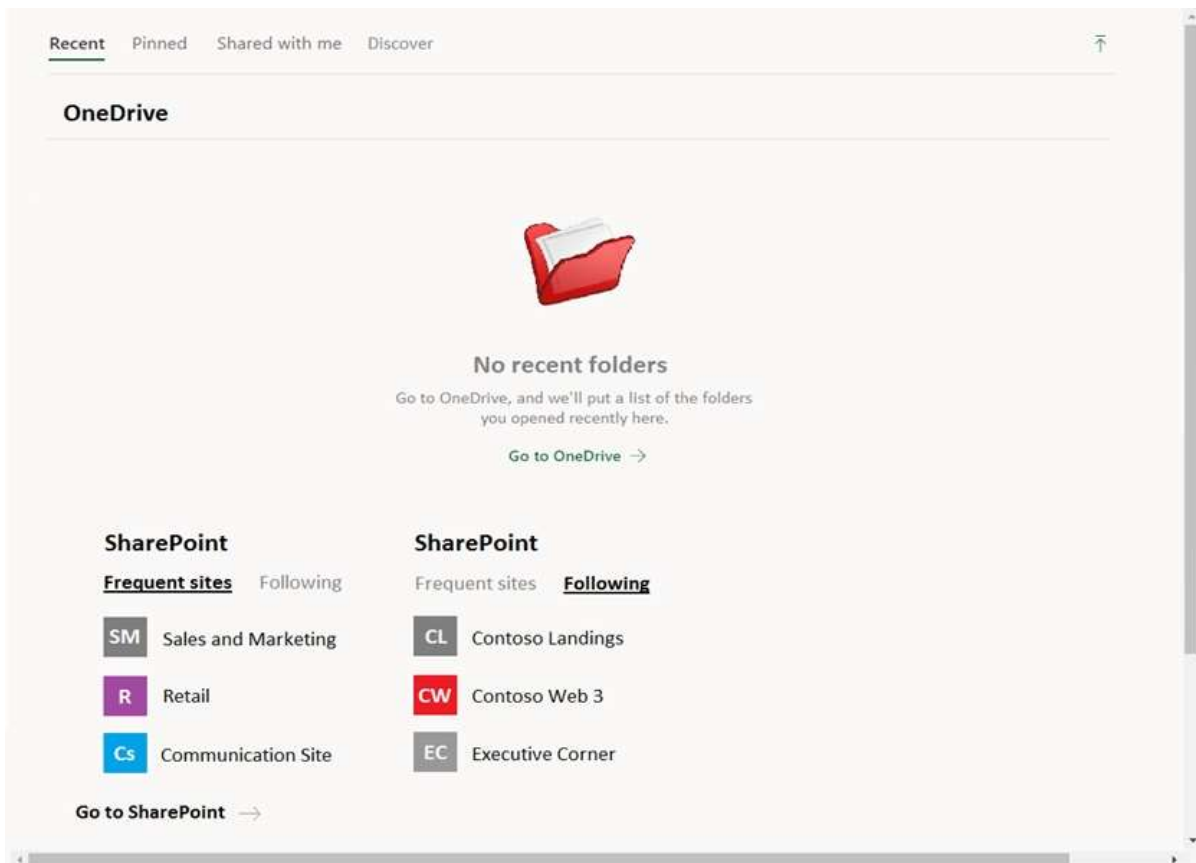
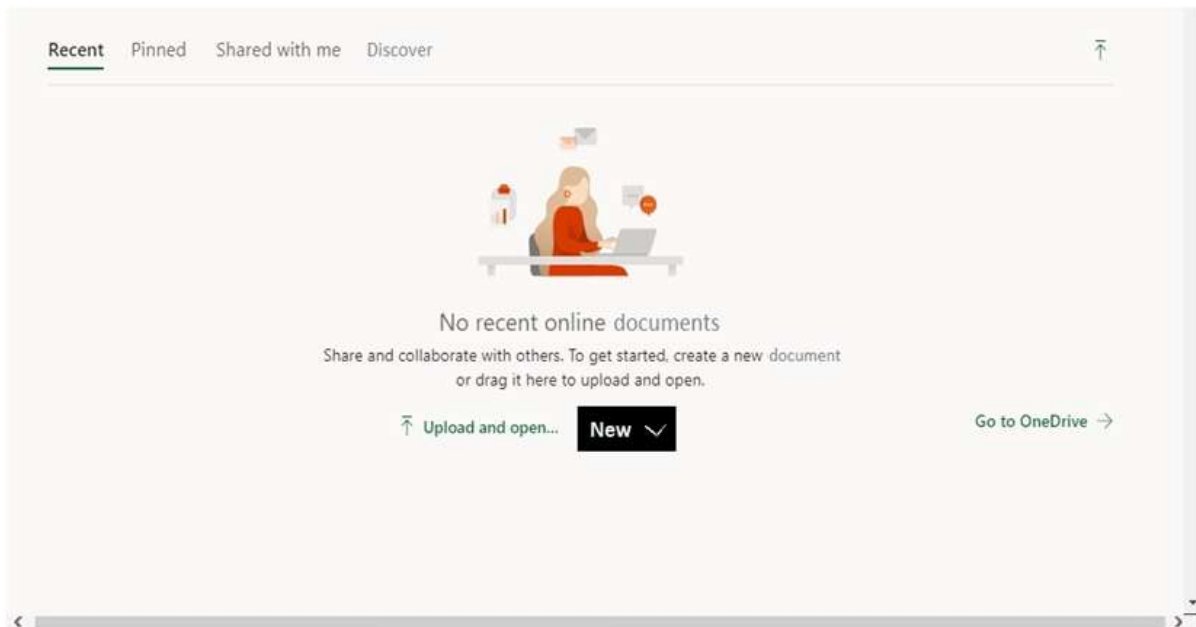
lodse000198.sharepoint.co...

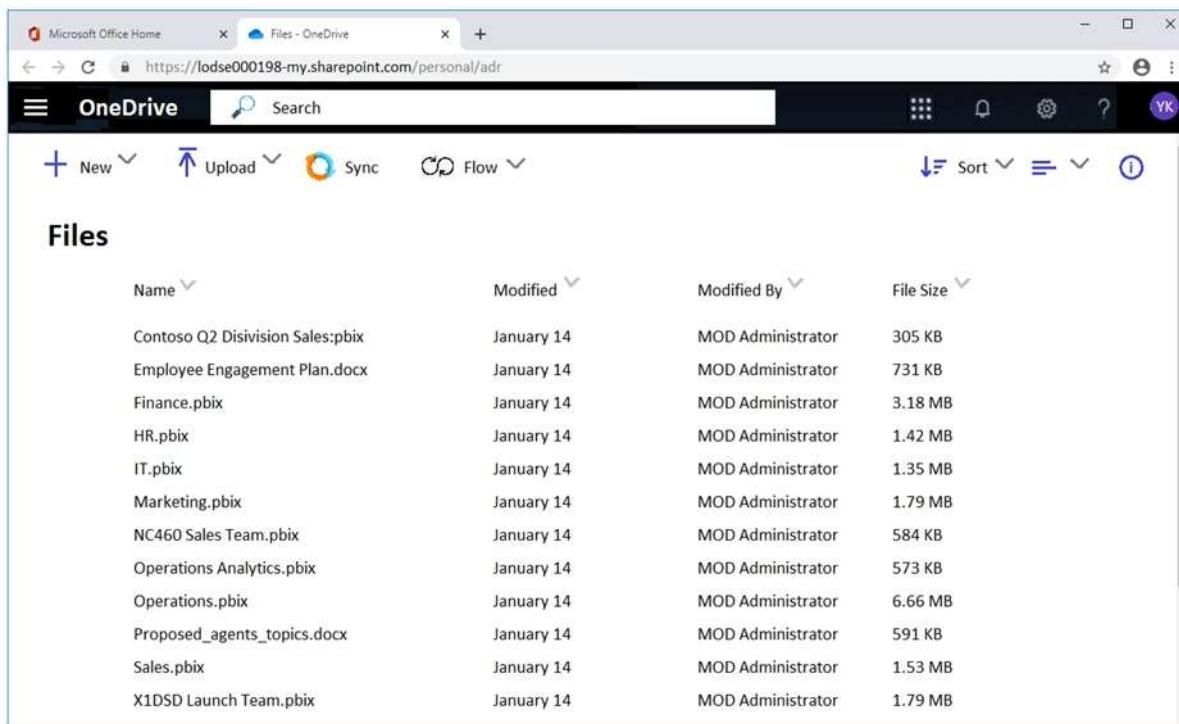
Recent

Pinned

Shared with me

Discover





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

You need to prevent any email messages that contain data covered by the U.K. Data Protection Act from being sent to recipients outside of your organization, unless the messages are sent to an external domain named adatum.com.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

new rule

Name:
Sent to scope Outside the organization

*Apply this rule if...

✕ The recipient is located... [Outside the organization](#)

and

✕ The message contains any of these sensitive information types... [Select sensitive information types...](#)

add condition

*Do the following...

✕ Generate incident report and send it to... Send incident report to: [Select one...](#) with content: [Custom content](#)

and

✕ Notify the sender with a Policy Tip... [Block the message](#)

add action

Except if...

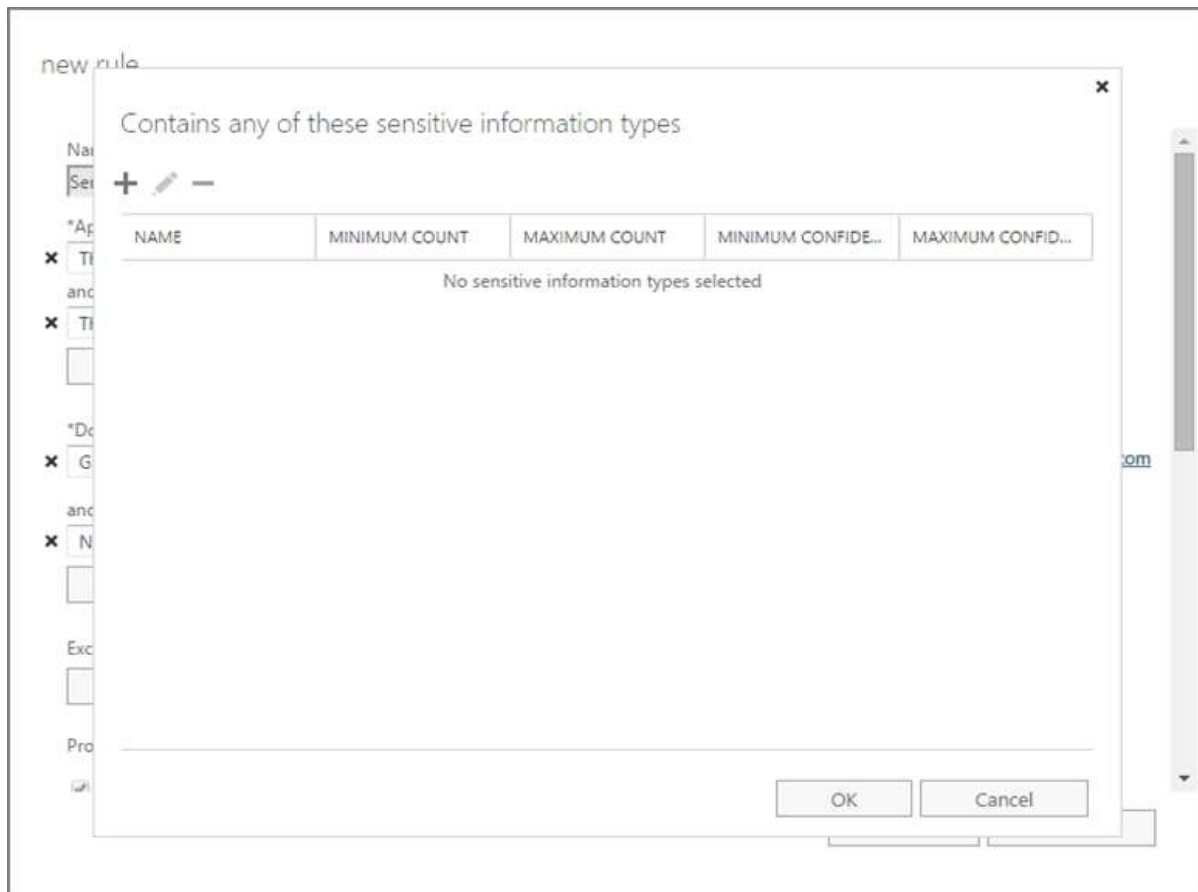
add exception

Properties of this rule:

Save Cancel

9. Click on “Select Sensitive information Types” to specify the sensitive information details.



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

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

11. Click on Ok

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

13. Add recipients for incident reports and click ok

14. Click save

15. Click save

Reference:

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

QUESTION 20

SIMULATION

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.

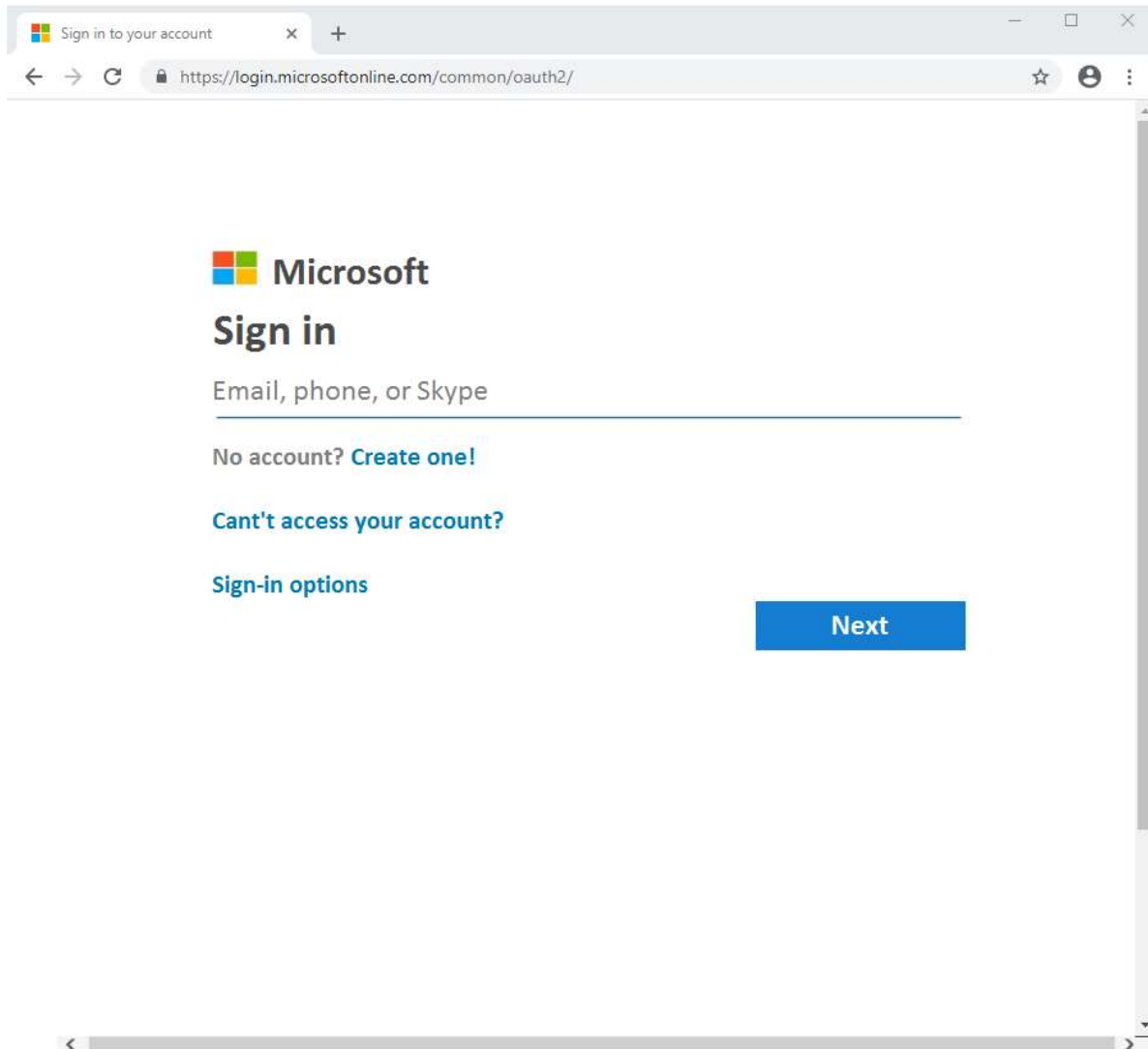
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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

A screenshot of a web browser window showing the Microsoft Sign in page. The browser's address bar displays the URL "https://login.microsoftonline.com/common/oauth2/". The page features the Microsoft logo at the top left, followed by the text "Sign in". Below this is a text input field labeled "Email, phone, or Skype". Underneath the input field are three links: "No account? Create one!", "Can't access your account?", and "Sign-in options". A blue "Next" button is positioned to the right of the input field. The browser window includes standard navigation buttons (back, forward, refresh) and window controls (minimize, maximize, close) at the top.

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.

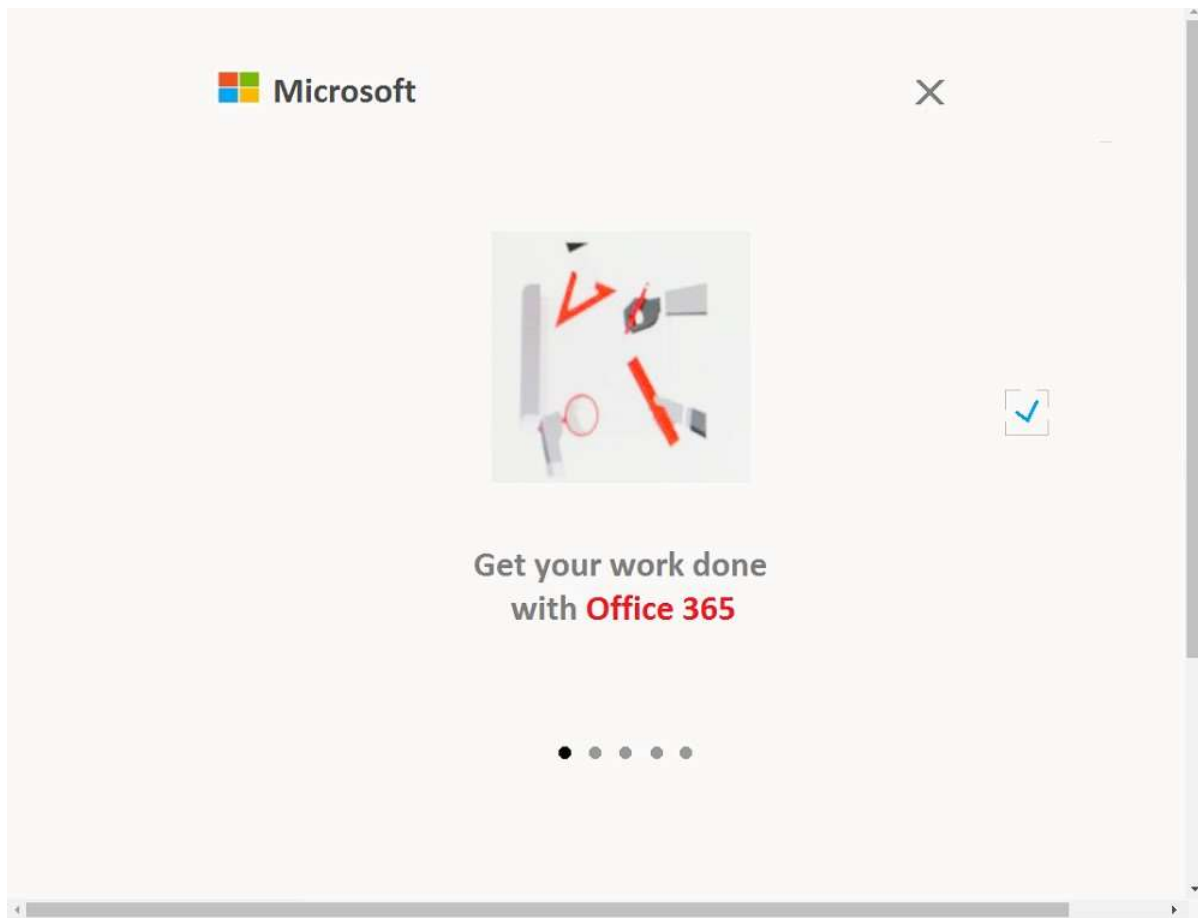
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308





Brainstorm
together in **Word**





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





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



Microsoft Office Home x + office.com/?auth=2

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

Sales Process

lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15

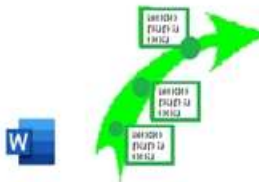


Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Ad Slogans



AD Slogans

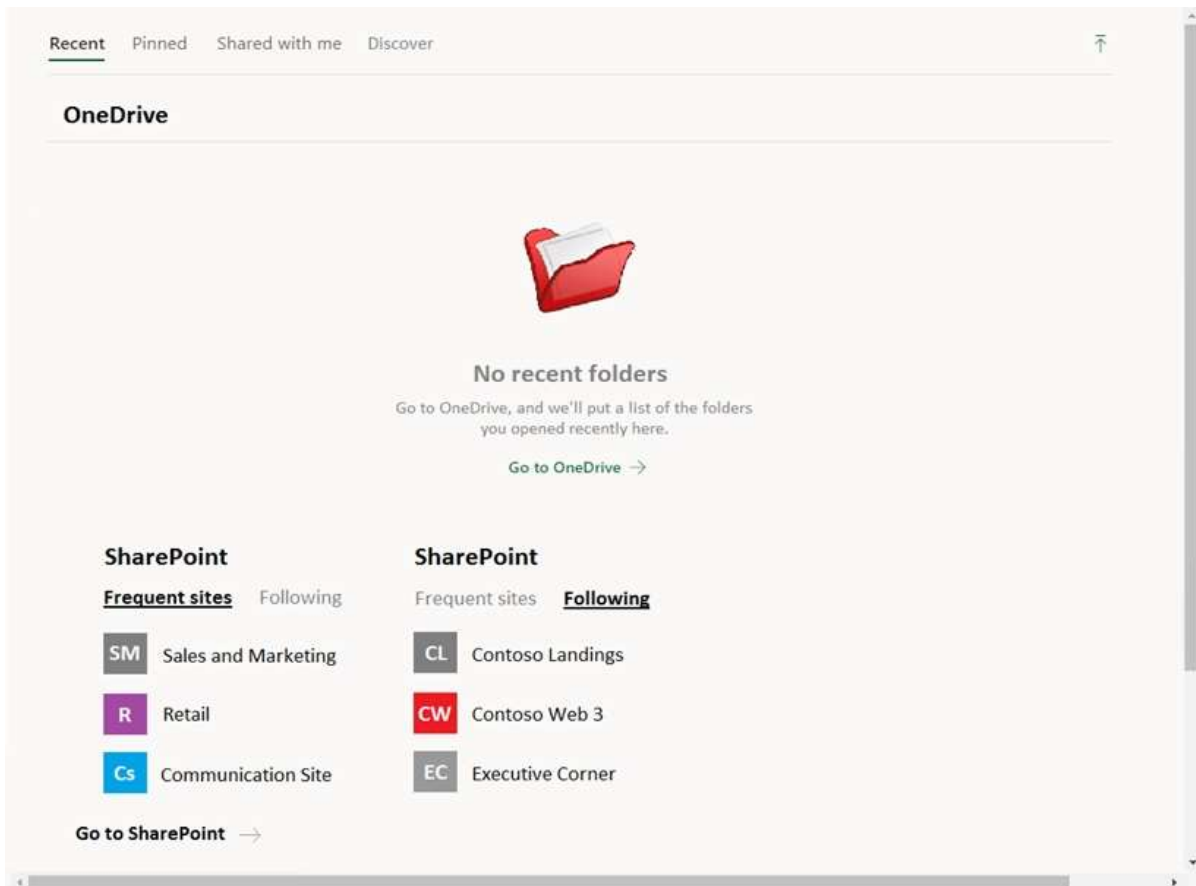
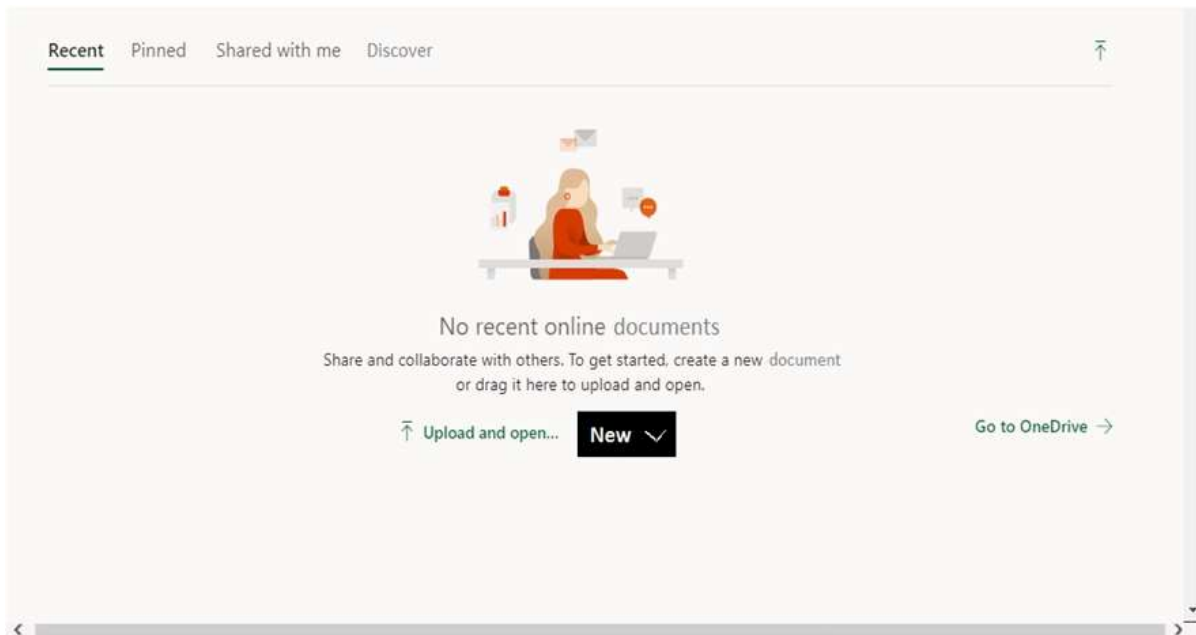
lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



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

You need to 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.

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

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-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/what-the-dlp-policy-templates-include?view=o365-worldwide>

QUESTION 21

SIMULATION

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.

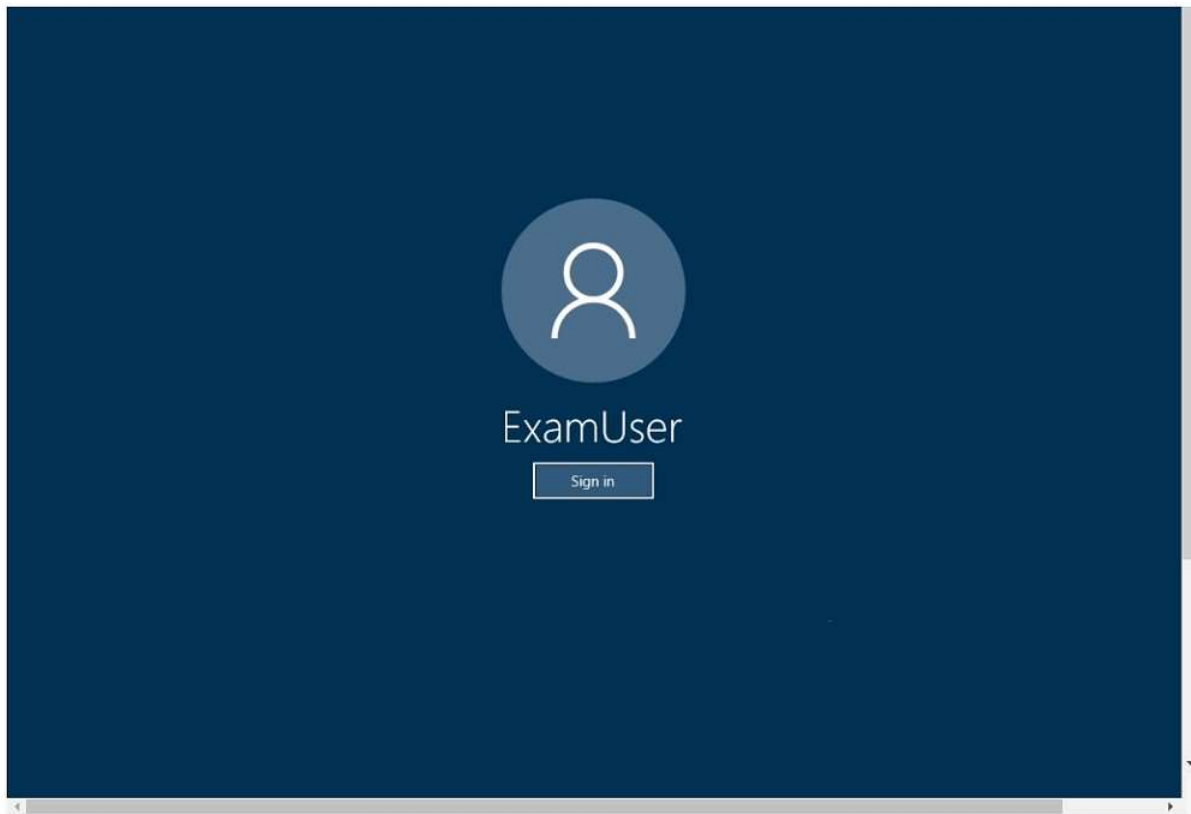
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 purposes only:

Lab instance: 11032396

You need to ensure that a global administrator is notified when a document that contains U.S. Health Insurance Portability and Accountability Act (HIPAA) data is identified in your Microsoft 365 tenant.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. In the Security & Compliance Center > left navigation > **Data loss prevention** > **Policy** > **+ Create a policy**.
2. Choose the U.S. Health Insurance Portability and Accountability Act (HIPAA) 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 decrease the number of instances to 1.
 - Select the **Send incident reports in email** option.
7. > **Next**
8. Select the option to turn on the policy right away > **Next**.
9. Click **Create** to finish creating the policy.

References:

<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-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/what-the-dlp-policy-templates-include?view=o365-worldwide>

Manage governance and compliance features in Microsoft 365

Testlet 1

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment

Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea**"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	<i>Not applicable</i>	GroupA
Device6	Windows 10	Enabled	<i>None</i>

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	<i>None</i>
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	<i>None</i>

The Mark devices with no compliance policy assigned as setting is set to **Compliant**.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

- Use the principle of least privilege
- Enable User1 to assign the Reports reader role to users
- Ensure that User6 approves Customer Lockbox requests as quickly as possible
- Ensure that User9 can enable and configure Azure AD Privileged Identity Management

QUESTION 1

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

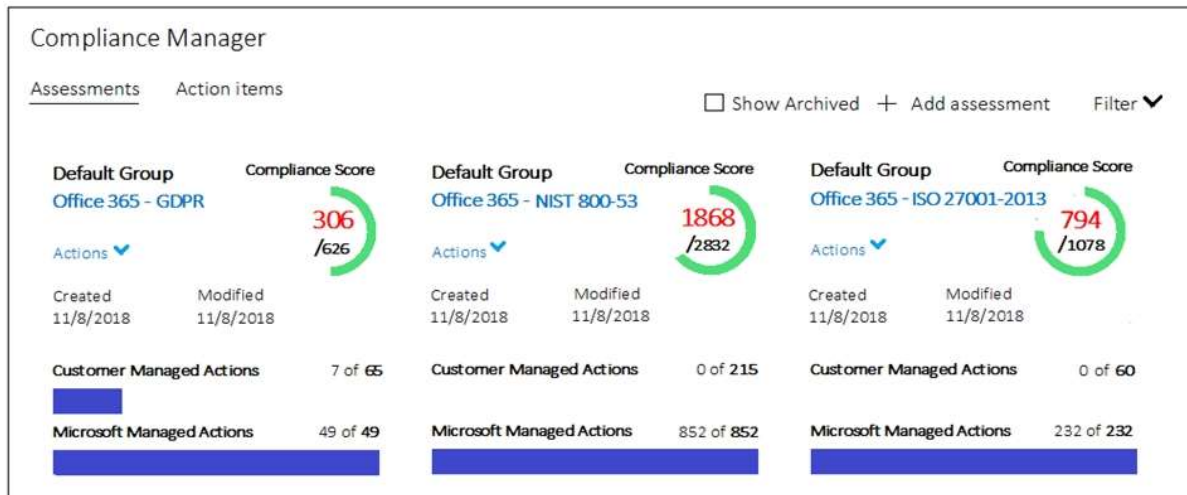
Manage governance and compliance features in Microsoft 365

Question Set 2

QUESTION 1

HOTSPOT

You view Compliance Manager 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.

Hot Area:

Answer Area

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	V
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	V
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

Correct Answer:

Answer Area

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	✓
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	✓
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud>

QUESTION 2

You have a Microsoft 365 subscription.

All computers run Windows 10 Enterprise and are managed by using Microsoft Endpoint Manager.

You plan to view only security-related Windows telemetry data.

You need to ensure that only Windows security data is sent to Microsoft.

What should you create from the Intune admin center?

- A. a device configuration profile that has device restrictions configured
- B. a device configuration profile that has the Endpoint Protection settings configured
- C. a device compliance policy that has the System Security settings configured
- D. a device compliance policy that has the Device Health settings configured

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 3

You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

You need to ensure that the users can use the new label to protect their email.

What should you do?

- A. Modify the priority order of label policies
- B. Wait six hours and ask the users to try again
- C. Create a label policy
- D. Create a new sensitive information type

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

You have a Microsoft 365 subscription that includes a user named Admin1.

You need to ensure that Admin1 can preserve all the mailbox content of users, including their deleted items.

The solution must use the principle of least privilege.

What should you do?

- A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.
- B. From the Exchange admin center, assign the Discovery Management admin role to Admin1.
- C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.
- D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

You have a hybrid Microsoft 365 environment.

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

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

What should you do?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Your company has a Microsoft 365 subscription that includes a user named User1.

You suspect that User1 sent email messages to a competitor detailing company secrets.

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

What should you include in the recommendation?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

You have a Microsoft 365 subscription.

Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.

You need to ensure that the labels will be available for manual assignment as soon as possible.

What should you do?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

DRAG DROP

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.

Select and Place:

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.	

Correct Answer:

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.	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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

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

You have a Microsoft 365 subscription.

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

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-Mailbox -Identity "User1" -AuditEnabled $true` command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 10

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

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

You have a Microsoft 365 subscription.

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

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-AuditConfig -Workload Exchange` command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps>

QUESTION 11

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

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

You have a Microsoft 365 subscription.

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

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox*` command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-adminauditlogconfig?view=exchange-ps>

QUESTION 12

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security & Compliance admin center, you create a label that designates personal data.

You need to auto-apply the new label to all the content in Site1.

What should you do first?

- A. From PowerShell, run `Set-ManagedContentSettings`.
- B. From PowerShell, run `Set-ComplianceTag`.
- C. From the Security & Compliance admin center, create a Data Subject Request (DSR).
- D. Remove Azure Information Protection from the Site1 files.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in-office-365>

QUESTION 13

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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 14

You have a Microsoft 365 E5 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 settings 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.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 15

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Search

Clear

Results

Activities

Show results for all activities ☒

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

Correct Answer:

Answer Area

Search

Clear

Results

Activities

	Date ▼	IP address	User	Activity	Item
Show results for all activities ▼					
x Clear all to show results for all activities					
Search					

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 16

You have a Microsoft 365 subscription.

You create and run a content search from the Security & Compliance admin center.

You need to download the results of the content search.

What should you obtain first?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 17**HOTSPOT**

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

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

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

Policy1

Edit policy

Delete policy

Status	☒ On	
Description	Policy1 description	
Severity	☒ Low	Edit
Category	Threat management	

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

	▼
Policy1 will not be triggered	
Policy1 will be triggered after 45 minutes	
Policy1 will be triggered after 60 minutes	

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

	▼
Policy1 will not be triggered	
Policy1 will be triggered within 20 minutes	
Policy1 will be triggered within 45 minutes	
Policy1 will be triggered after 60 minutes	

Correct Answer:

Answer Area

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

	▼
Policy1 will not be triggered	
Policy1 will be triggered after 45 minutes	
Policy1 will be triggered after 60 minutes	

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

	▼
Policy1 will not be triggered	
Policy1 will be triggered within 20 minutes	
Policy1 will be triggered within 45 minutes	
Policy1 will be triggered after 60 minutes	

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 18

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E5 license.

How long will auditing data be retained?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 19

HOTSPOT

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 sidebar contains three steps: 'Name your label' (completed with a green checkmark), 'Label settings' (completed with a green checkmark), and 'Review your settings' (selected with a grey circle). Below the sidebar is a large black redacted area. The main content area is titled 'Review your settings' and contains the following sections:

- 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' (highlighted in blue), 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.

Hot Area:

Answer Area

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.	

Correct Answer:

Answer Area

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.	

Section: (none)
Explanation

Explanation/Reference:

References:

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

QUESTION 20

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 21

You have a Microsoft 365 subscription.

You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.

What should you create first?

- A. A retention label in Microsoft Office 365
- B. A custom sensitive information type
- C. A Data Subject Request (DSR)
- D. A safe attachments policy in Microsoft Office 365

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool#more-information-about-using-the-dsr-case-tool>

QUESTION 22

You have a Microsoft 365 subscription.

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

You need to identify which files were modified by which users in the user's OneDrive.

What should you do?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 23

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the following exhibit. (Click the **Exhibit** tab.)

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

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 2 years ▾

Retain the content based on when it was last modified ▾ ⓘ

Do you want us to delete it after this time? ⓘ

☒ Yes ☐ No

☐ No, just delete content that's older than ⓘ

1 years ▾

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

You apply Retention1 to SharePoint sites and OneDrive accounts.

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.

Hot Area:

Answer Area

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be **[answer choice]**.

retained	▼
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in a Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

can recover the file until the Recycle Bin retention period expires	▼
can recover the file until January 1, 2021	
can recover the file until March 1, 2021	
can recover the file until May 1, 2021	

Correct Answer:

Answer Area

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be **[answer choice]**.

retained	▼
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in a Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

can recover the file until the Recycle Bin retention period expires	▼
can recover the file until January 1, 2021	
can recover the file until March 1, 2021	
can recover the file until May 1, 2021	

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

DRAG DROP

You have a Microsoft 365 subscription.

A customer requests that you provide her with all documents that reference her by name.

You need to provide the customer with a copy of the content.

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

Select and Place:

Actions

Close the case.

Regenerate a report.

View the results.

Export the results.

Create a Data Subject Request
(DSR) case.

Save the search.

Download the results.

Answer Area

Correct Answer:

Actions	Answer Area
Close the case.	Create a Data Subject Request (DSR) case.
Regenerate a report.	View the results.
View the results.	Save the search.
Export the results.	Export the results.
Create a Data Subject Request (DSR) case.	
Save the search.	
Download the results.	

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365>

QUESTION 25

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 admin center, create a label.
- D. From the SharePoint admin center, modify the records management settings.
- E. From the Security admin center, publish a label.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 26

You recently created and published several label policies in a Microsoft 365 subscription.

You need to view which labels were applied by users manually and which labels were applied automatically.

What should you do from the Security & Compliance admin center?

- A. From Search & investigation, select **Content search**
- B. From Data governance, select **Events**
- C. From Search & investigation, select **eDiscovery**
- D. From Reports, select **Dashboard**

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

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

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

You have a Microsoft 365 subscription.

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

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the `Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner` command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

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

QUESTION 28

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

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

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

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

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

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

Solution: You recommend assigning the Compliance Manager Reader role to User1.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 29

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

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

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

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

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

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

Solution: You recommend modifying the licenses assigned to User5.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 30

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

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

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

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

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

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

Solution: You recommend assigning the Compliance Manager Reader role to User5.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 31

You have a Microsoft 365 subscription.

You enable auditing for the subscription.

You plan to provide a user named Auditor with the ability to review audit logs.

You add Auditor to the Global administrator role group.

Several days later, you discover that Auditor disabled auditing.

You remove Auditor from the Global administrator role group and enable auditing.

You need to modify Auditor to meet the following requirements:

- Be prevented from disabling auditing
- Use the principle of least privilege
- Be able to review the audit log

To which role group should you add Auditor?

- A. Security reader
- B. Compliance administrator
- C. Security operator
- D. Security administrator

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center>

QUESTION 32

You have a Microsoft 365 subscription.

You have a team named Team1 in Microsoft Teams.

You plan to place all the content in Team1 on hold.

You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.

Which cmdlet should you use?

- A. Get-UnifiedGroup
- B. Get-MailUser
- C. Get-TeamMessagingSettings
- D. Get-TeamChannel

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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

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

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

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

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

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

Solution: You recommend removing User1 from the Compliance Manager Contributor role.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager>

QUESTION 34

You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1.

You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1.

What should you do first?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 35

HOTSPOT

You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.

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

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 1 years ▾

☐ No, just delete content that's older than ⓘ

1 years ▾

Delete the content based on when it was created ▾ ⓘ

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

Policy2 is configured as shown in the following exhibit.

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

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 3 years ▾

Retain the content based on when it was created ▾ ⓘ

Do you want us to delete it after this time?

☐ Yes ☒ No

☐ No, just delete content that's older than ⓘ

1 years ▾

Need more options?

☐ Use advanced retention settings ⓘ

Back Next Cancel

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

Hot Area:

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	☐	☐
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	☐	☐
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	☐	☐

Correct Answer:

Answer Area

	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	☒	☐
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019	☒	☐
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	☐	☒

Section: (none)

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence>

QUESTION 36

You have a Microsoft 365 subscription.

You need to enable auditing for all Microsoft Exchange Online users.

What should you do?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 37

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

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

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

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

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

Solution: You modify the permissions of the mailbox of User5, and then create an eDiscovery case.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019>

QUESTION 38

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

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

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

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

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

Solution: You start a message trace, and then create a Data Subject Request (DSR) case.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019>

QUESTION 39

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

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

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

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

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

Solution: You assign the eDiscovery Manager role to Admin1, and then create an eDiscovery case.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

References:

<https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019>

QUESTION 40

SIMULATION

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.

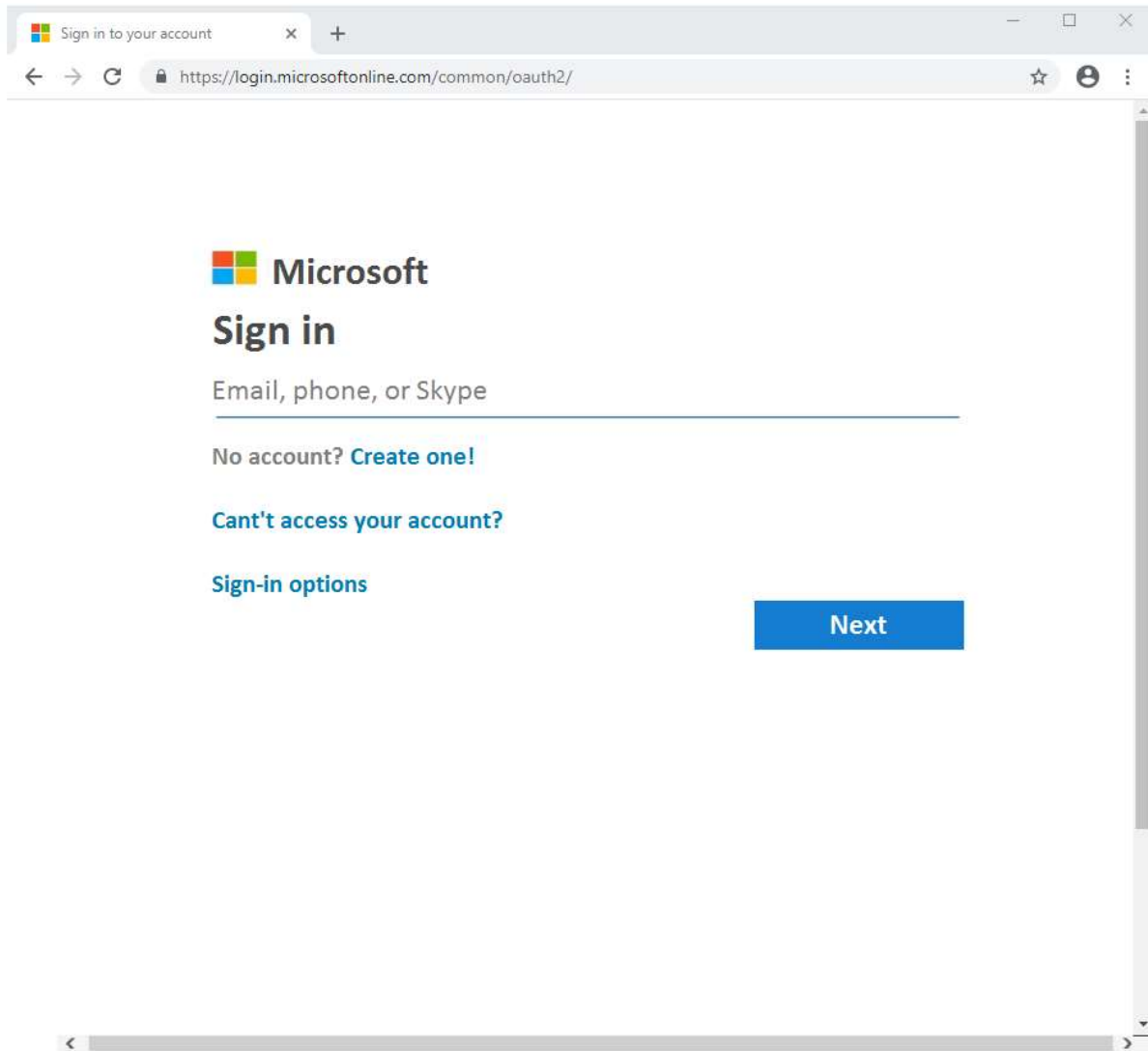
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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.

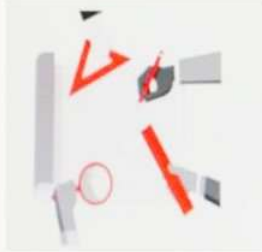
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home | office.com/tauth=2

Contoso electronics Office 365

Good morning Install Office

Start new

Outlook

OneDrive

Word

Excel

PowerPoint

OneNote

Skype

Calendar

People

All apps

Recommended

Excel

Sales Results Overview
lodse000198.sharepoint.co...

Sales Process
lodse000198.sharepoint.co...

Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15

You edited this Jan 15

You edited this Jan 15



Excel

P and L Summary

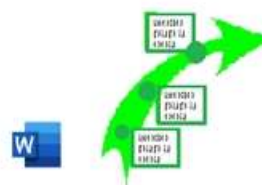
lodse000198.sharepoint.co...



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](#)

Recent Pinned Shared with me Discover



OneDrive



No recent folders

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

[Go to OneDrive](#)

SharePoint

Frequent sites Following

SM Sales and Marketing

R Retail

Cs Communication Site

SharePoint

Frequent sites Following

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

[Go to SharePoint](#)

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

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

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

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-retention-policy#step-3-apply-a-retention-policy-to-mailbox-users>

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-retention-policy>

QUESTION 41

SIMULATION

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.

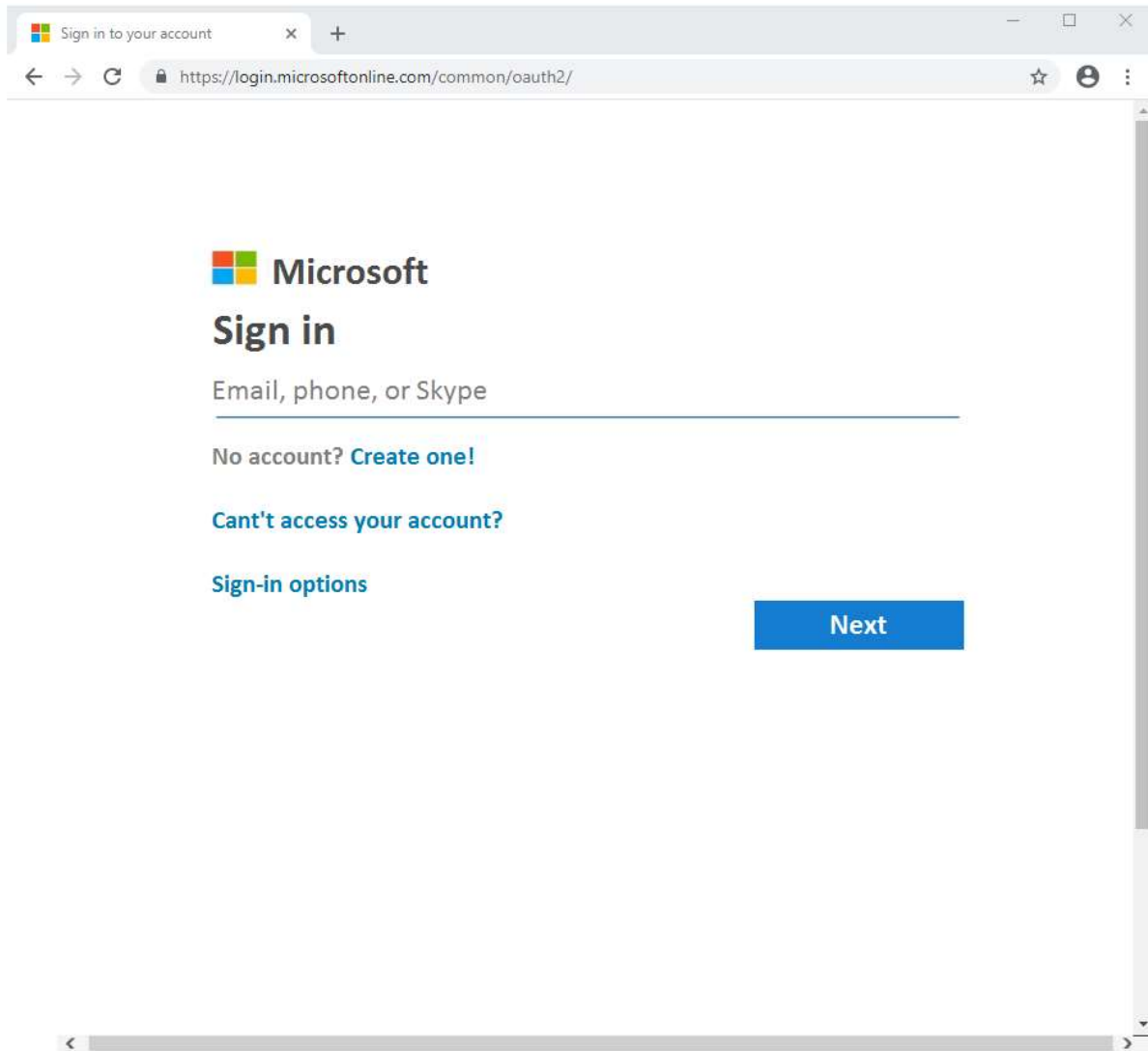
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 have 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.

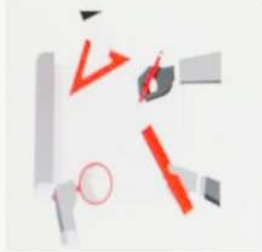
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home x + office.com/?auth=2

Contoso electronics Office 365

Good morning [Install Office](#)

Start new Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15

You edited this Jan 15

You edited this Jan 15



Excel

P and L Summary

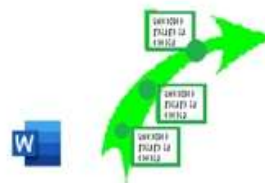
lodse000198.sharepoint.co...



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](#) →

Recent Pinned Shared with me Discover



OneDrive



No recent folders

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

[Go to OneDrive](#) →

SharePoint

Frequent sites Following

SM Sales and Marketing

R Retail

Cs Communication Site

SharePoint

Frequent sites Following

CL Contoso Landings

CW Contoso Web 3

EC Executive Corner

[Go to SharePoint](#) →

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

You need to create a retention policy that contains a data label. The policy must delete all Microsoft Office 365 content that is older than six months.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Creating Office 365 labels is a two-step process. The first step is to create the actual label which includes the name, description, retention policy, and classifying the content as a record. Once this is completed, the second step requires the deployment of a label using a labelling policy which specifies the specific location to publish and applying the label automatically.

To create an Office 365 label, following these steps:

1. Open *Security and Compliance Centre*;
2. Click on *Classifications*;
3. Click on *Labels*;
4. The label will require configuration including: name your label (*Name*), add a description for the admins (*Description for Admins*), add a description for the users (*Description for Users*);
5. Click *Next* once the configuration is completed;
6. Click *Label Settings* on the left-hand side menu;
7. The Label Settings will need to be configured. On this screen, you can toggle the *Retention* switch to either "on" or "off". If you choose "on", then you can answer the question "When this label is applied to content" with one of two options. The first option is to *Retain the Content*. From the pick boxes, you can choose the length of retention and upon the end of the retention, the action that will take place. The three actions are to delete the data, trigger an approval flow for review, or nothing can be actioned. The second option is to **not retain the data after a specified amount of time** or based on the age of the data; and

8. The label has now been created.

To create a label policy, follow these steps:

1. Open *Security and Compliance Centre*;
2. Click on *Data Governance, Retention*;
3. Choose *Label Policies* box at the top of the screen; and
4. There are now two options. The first is to *Publish Labels*. If your organization wants its end users to apply the label manually, then this is the option you would choose. Note that this is location based. **The second option is to Auto-apply Labels. With Auto-apply, you would have the ability to automatically apply a label when it meets the specified criteria.**

References:

<https://www.maadarani.com/office-365-classification-and-retention-labels/>

QUESTION 42

SIMULATION

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.

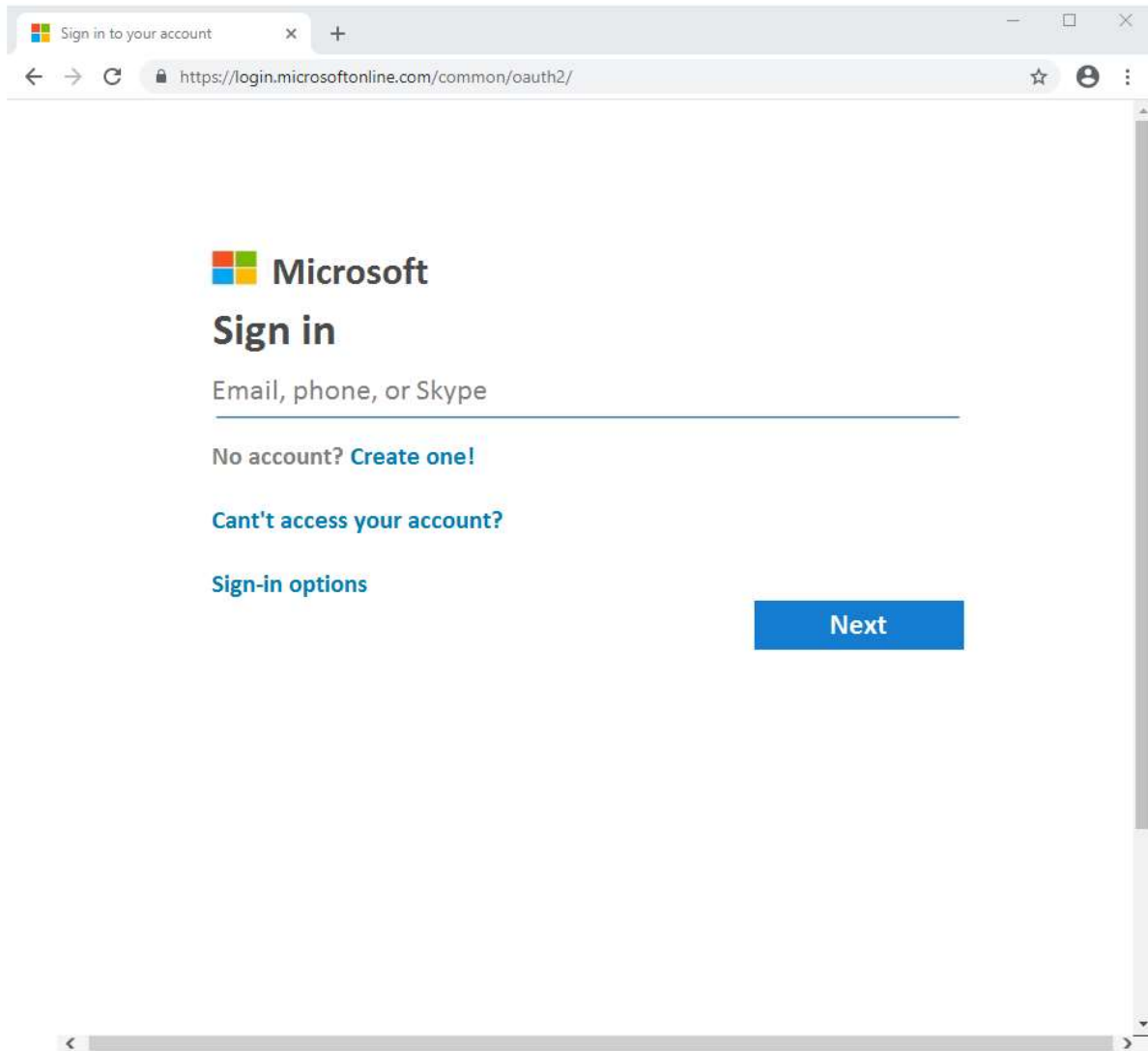
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 have 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.

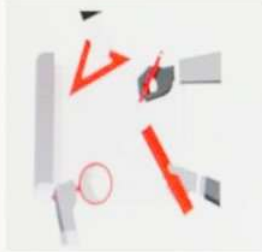
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home | office.com/?auth=2

Contoso electronics Office 365

Good morning [Install Office](#)

Start new

Outlook

OneDrive

Word

Excel

PowerPoint

OneNote

Skype

Calendar

People

All apps

Recommended

Excel

You edited this Jan 15

Sales Results Overview
lodse000198.sharepoint.co...

Sales Process
lodse000198.sharepoint.co...

Org Chart
lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15



Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Ad Slogans



AD Slogans

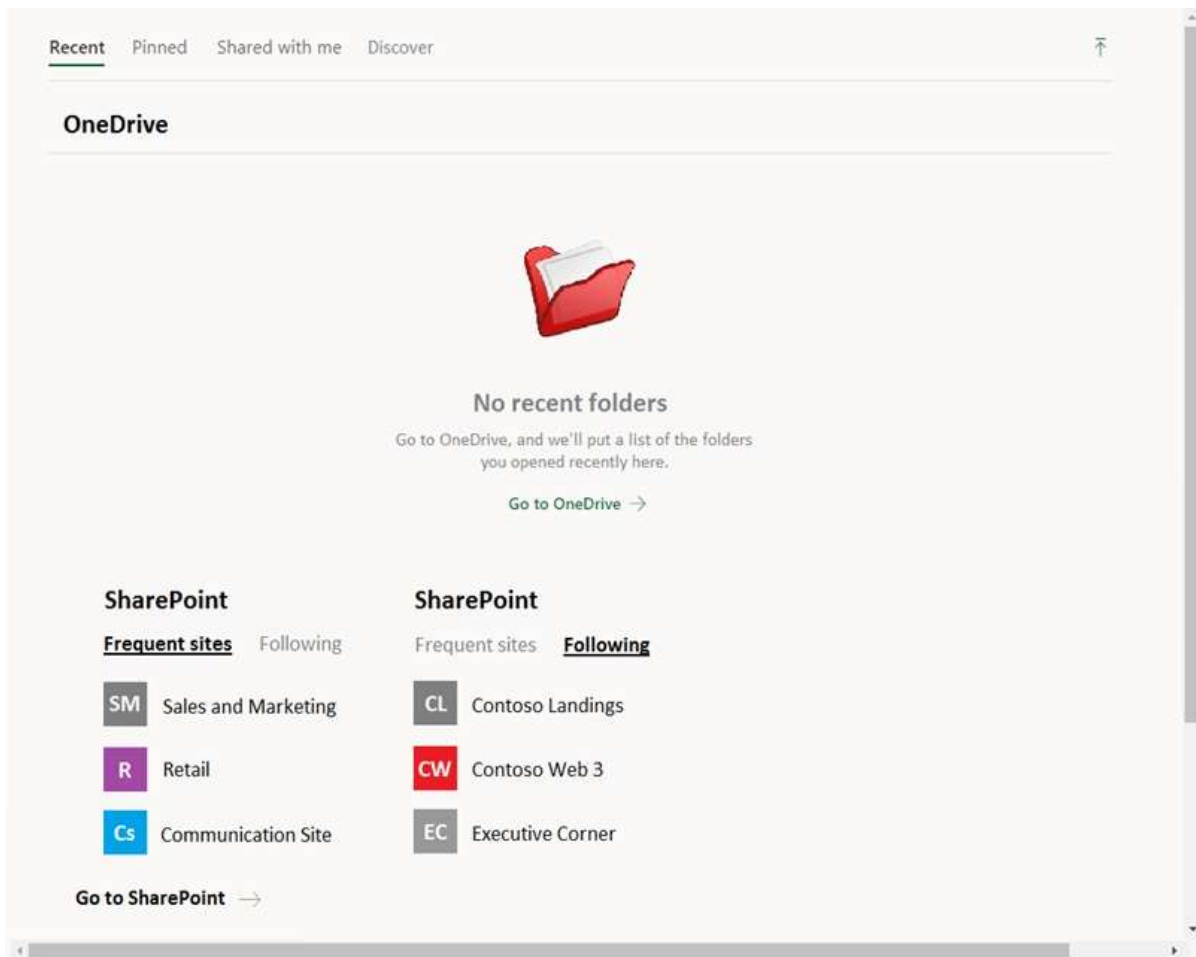
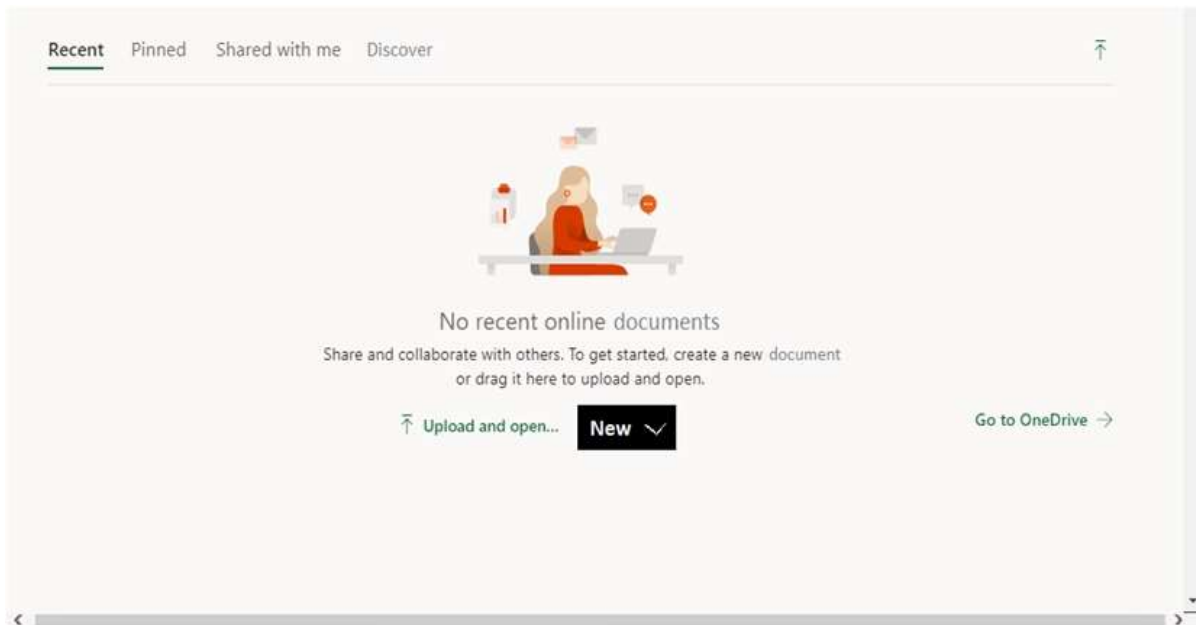
lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



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

You need to create an eDiscovery case that places a hold on the mailbox of a user named Allan Deyoung. The hold must retain email messages that have a subject containing the word merger or the word Contoso.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. Navigate to **eDiscovery** in the Security & Compliance Center, and then click **Create a case**.
2. On the **New Case** page, give the case a name, type an optional description, and then click **Save**. The case name must be unique in your organization.

New case

Enter a name and description

Give this case a friendly name so you can easily find it again later.

*Case name

Description

Save

Cancel

The new case is displayed in the list of cases on the **eDiscovery** page. You can hover the cursor over a case name to display information about the case, including the status of the case (**Active** or **Closed**), the description of the case (that was created in the previous step), and when the case was changed last and who changed it.

To create a hold for an eDiscovery case:

1. In the Security & Compliance Center, click **eDiscovery** > **eDiscovery** to display the list of cases in your organization.
2. Click **Open** next to the case that you want to create the holds in.
3. On the **Home** page for the case, click the **Hold** tab.

Home

Hold

Search

Export

Switch to Advanced eDiscovery

+ Create

Refresh

Search

Name

holdOne

HoldTwo

4. On the **Hold** page, click **Create**.
5. On the **Name your hold** page, give the hold a name. The name of the hold must be unique in your organization.

Name your hold

Name *

Enter a friendly name

Description

Enter a friendly description for your policy

Next Cancel

6. (Optional) In the **Description** box, add a description of the hold.
7. Click **Next**.
8. Choose the content locations that you want to place on hold. You can place mailboxes, sites, and public folders on hold.

Choose locations

Location

Include



Exchange email

None

[Choose users, groups, or teams](#)



Office 365 group email



Skype for Business



Teams messages



To-Do



Yammer conversations



SharePoint sites

None

[Choose sites](#)



OneDrive accounts



Office 365 group sites



Teams sites



Yammer networks



Exchange public folders

None



Back

Next

Cancel

- **Exchange email** - Click **Choose users, groups, or teams** and then click **Choose users, groups, or teams** again. to specify mailboxes to place on hold. Use the search box to find user mailboxes and distribution groups (to place a hold on the mailboxes of group members) to place on hold. You can also place a hold on the associated mailbox for a Microsoft Team, a Yammer Group, or an Office 365 Group. Select the user, group, team check box, click **Choose**, and then click **Done**.

Note

When you click **Choose users, groups, or teams** to specify mailboxes to place on hold, the mailbox picker that's displayed is empty. This is by design to enhance performance. To add people to this list, type a name (a minimum of 3 characters) in the search box.

9. After configuring a query-based hold, click **Next**.

10. Review your settings, and then click **Create this hold**.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-cases?view=o365-worldwide#step-4-place-content-locations-on-hold>

QUESTION 43

SIMULATION

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.

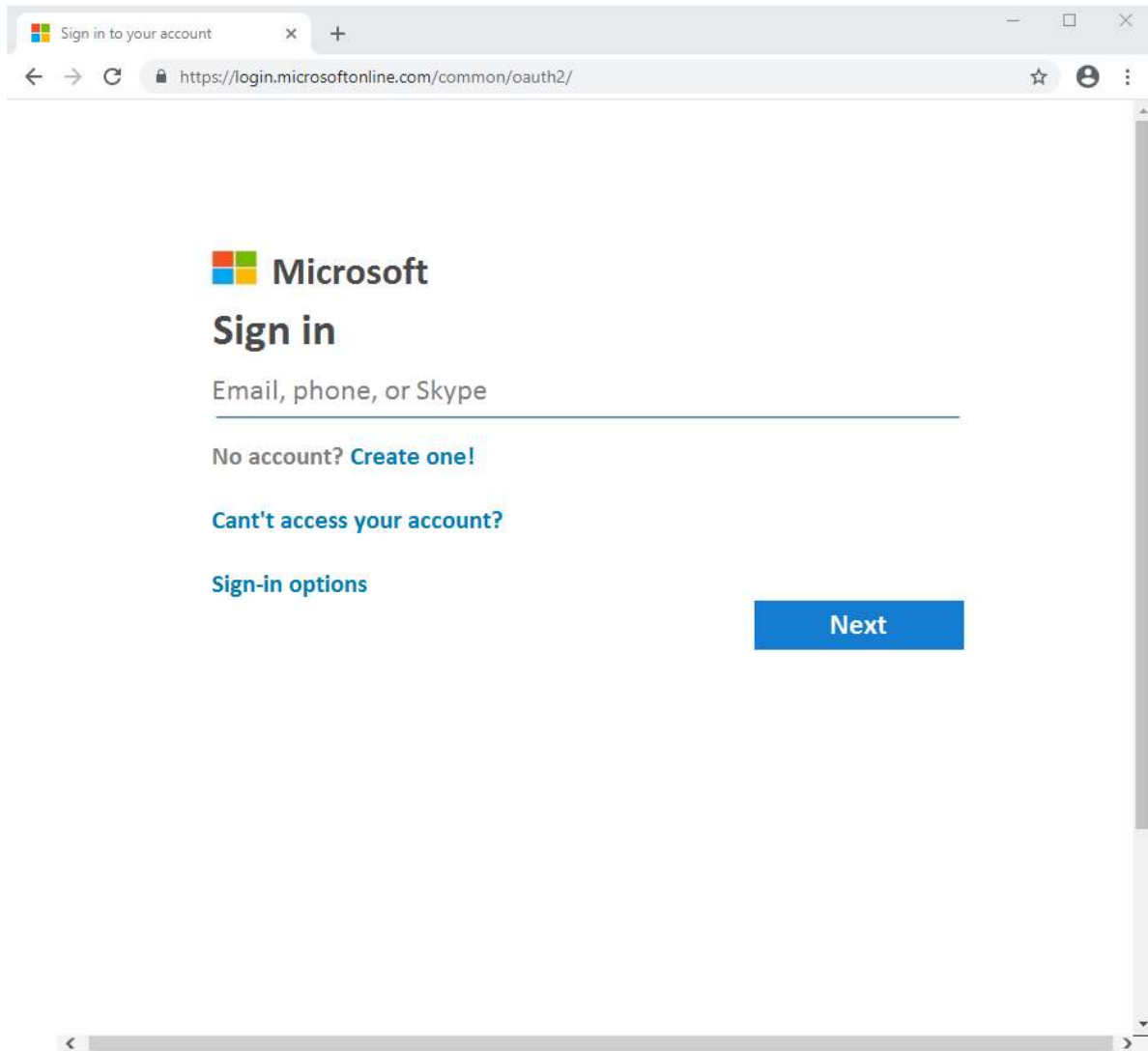
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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.

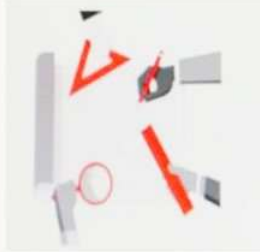
Microsoft 365 Username:
admin@LODSe00019.onmicrosoft.com

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 purposes only:

Lab instance: 11122308



Get your work done
with **Office 365**





Brainstorm
together in **Word**





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





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



Microsoft Office Home | office.com/auth=2

Contoso electronics Office 365

Good morning [Install Office](#)

Start new

Outlook OneDrive Word Excel PowerPoint

OneNote Skype Calendar People All apps

Recommended

You edited this Jan 15

Excel

Sales Results Overview
lodse000198.sharepoint.co...

You edited this Jan 15

Integrated Team Sales Process

Sales Process
lodse000198.sharepoint.co...

You edited this Jan 15

Org Chart

lodse000198.sharepoint.co...

Recent Pinned Shared with me Discover

Recommended

You edited this Jan 15



Excel

P and L Summary

lodse000198.sharepoint.co...

You edited this Jan 15

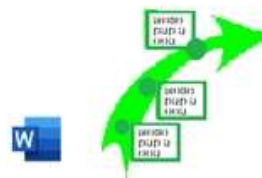


Contoso Electronics Outdoor...

lodse000198.sharepoint.co...

You edited this Jan 15

Ad Slogans



AD Slogans

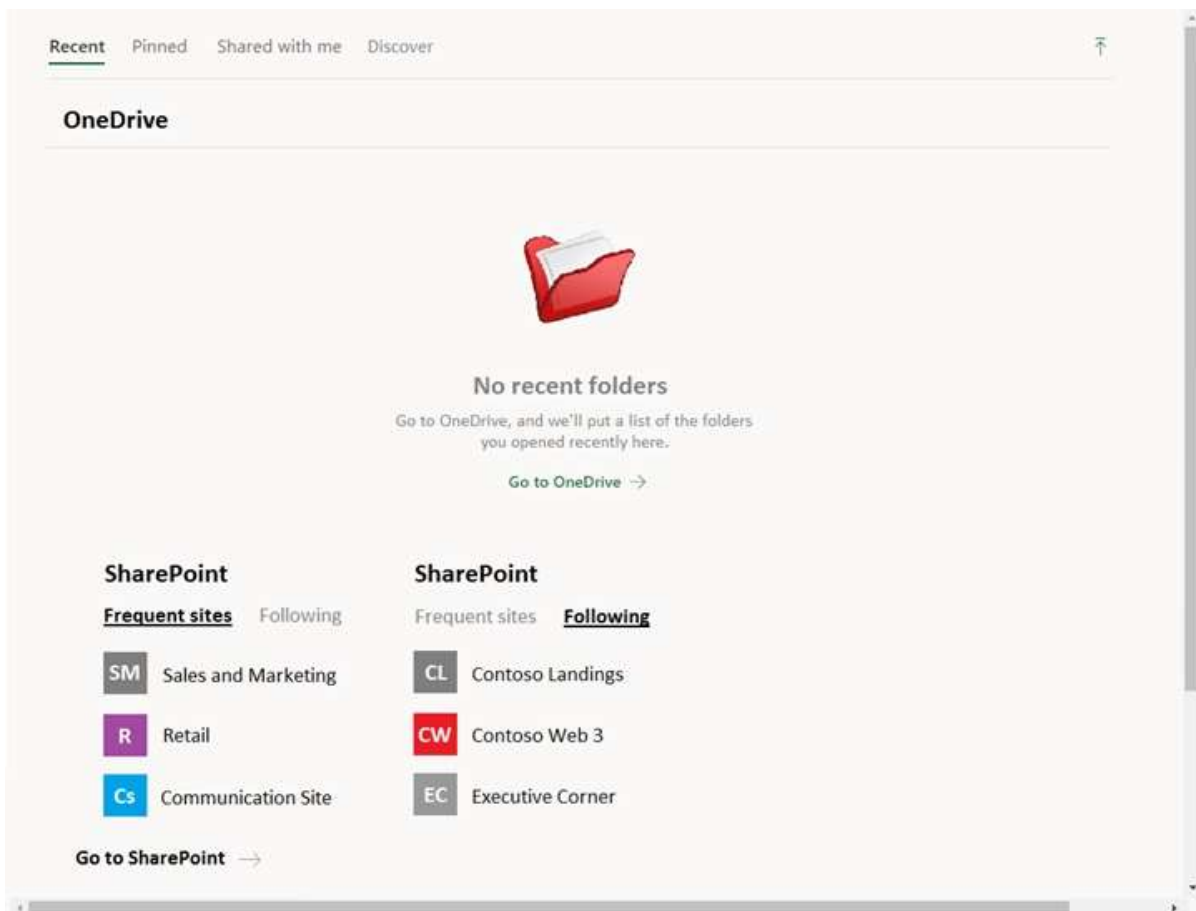
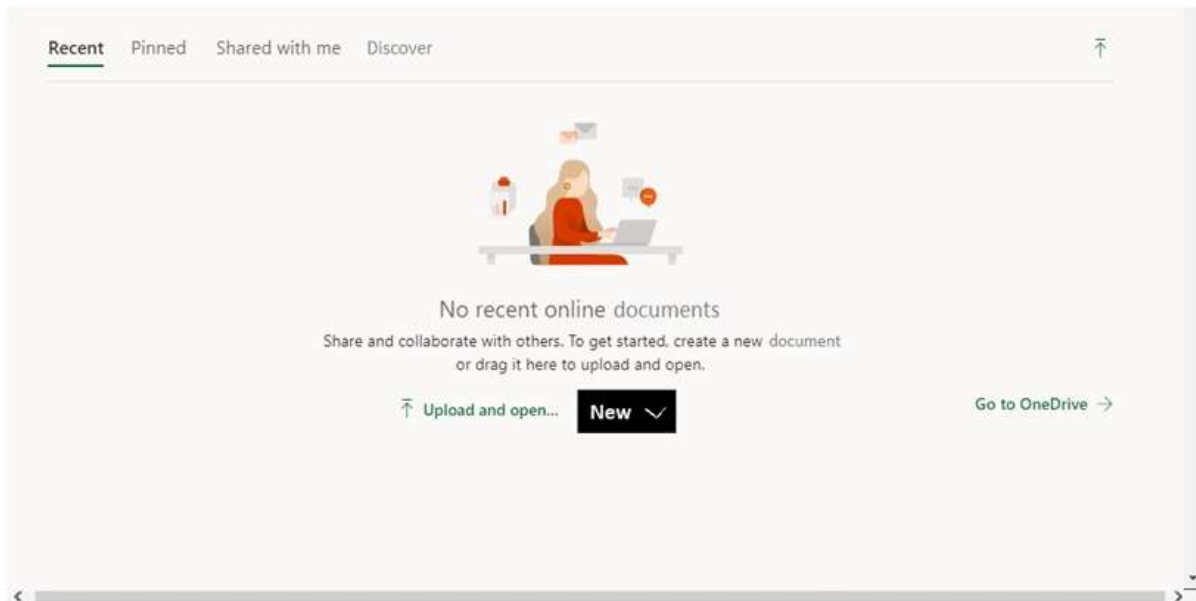
lodse000198.sharepoint.co...

Recent

Pinned

Shared with me

Discover



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

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

You need to create the search that will be included in the script.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

1. Copy and paste the following text into a .txt file using NotePad. Save this file to a folder on your local computer. You'll save the other scripts to this folder as well.

```
ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/
sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2000,12/31/2005
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/
sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2006,12/31/2010
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/
sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2011,3/21/2016
,https://contoso.sharepoint.com/sites/contoso,,3/21/2016
,https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com,,1/1/2015,
,https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com,,1/1/2015,
```

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

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

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

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

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-searches?view=o365-worldwide>

Keyword queries and search conditions for Content Search

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

QUESTION 44

You have a Microsoft 365 subscription.

You create a supervision policy named Policy1, and you designate a user named User1 as the reviewer.

What should User1 use to view supervised communications?

- A. a team in Microsoft Teams
- B. the Security & Compliance admin center
- C. Outlook on the web
- D. the Exchange admin center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

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

QUESTION 45

SIMULATION

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.

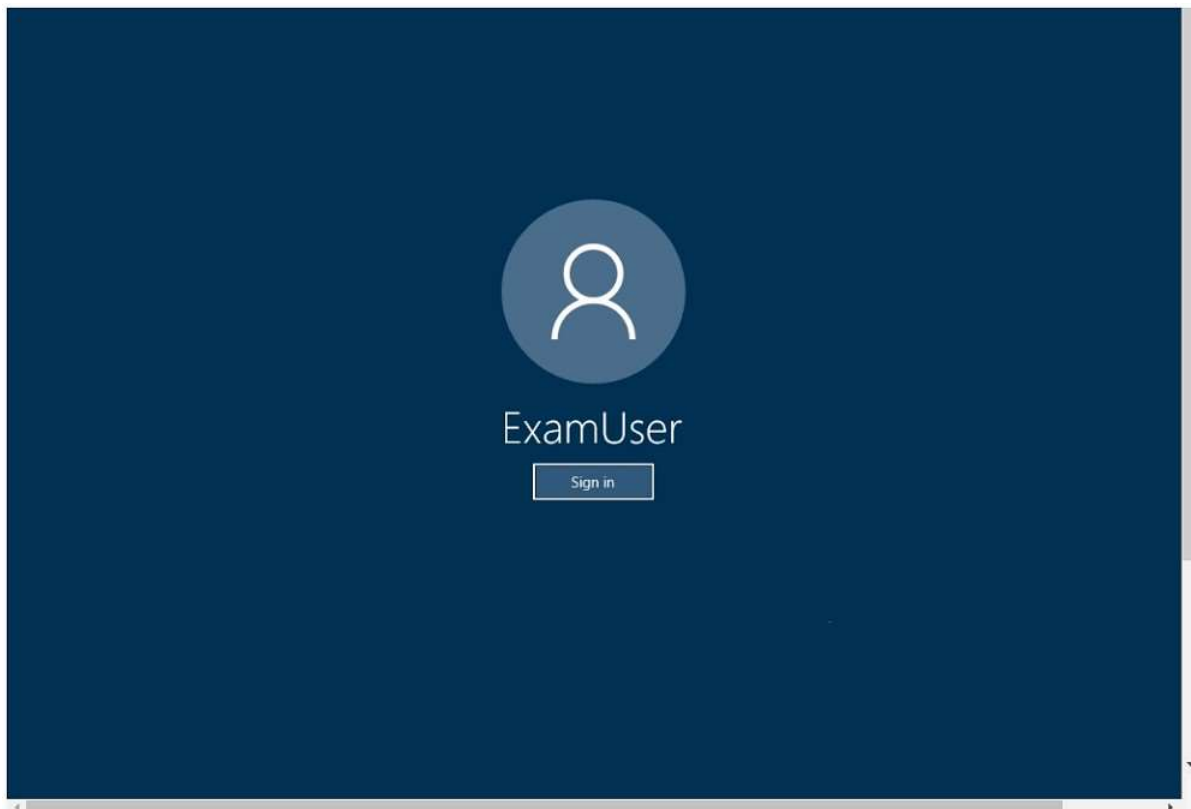
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 purposes only:

Lab instance: 11032396

You need to ensure that when users tag documents as classified, a classified watermark is applied to the documents.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. In the admin center, select the **Compliance** admin center.
2. Select **Classification > Sensitivity labels**.
3. Select **Create a label**, and when the warning appears, select **Yes**.
4. Enter a **Label name**, **Tooltip**, and **Description**. Select **Next**.
5. Turn on **Encryption**. Choose when you want to assign permissions, whether you want your users' access to the content to expire, and whether you want to allow offline access.
6. Select **Assign permissions > Add these email addresses or domains**.
7. Enter an email address or domain name (such as Contoso.org). Select **Add**, and repeat for each email address or domain you want to add.
8. Select **Choose permissions from preset or custom**.
9. Use the drop-down list to select preset permissions, such as **Reviewer** or **Viewer**, or select **Custom** permissions. If you chose **Custom**, select the permissions from the list. Select **Save > Save > Next**.
10. Turn on **Content marking**, and choose the markings you want to use.
11. For each marking that you choose, select **Customize text**. Enter the text you want to appear on the document, and set the font and layout options. Select **Save**, and then repeat for any additional markings. Select **Next**.
12. Optionally, turn on **Endpoint data loss prevention**. Select **Next**.
13. Optionally, turn on **Auto labeling**. Add a condition. For example, under **Detect content that contains**, select **Add a condition**. Enter the condition; for example, add a condition that if passport, Social Security, or other sensitive information is detected, the label will be added. Select **Next**.
14. Review your settings, and select **Create**. Your label has been created. Repeat this process for any additional labels you want.
15. By default, labels appear in Office apps in this order: **Confidential**, **Internal**, and **Public**. To change the order, for each label, select **More actions** (the ellipsis), and then move the label up or down. Typically, permissions are listed from the lowest to highest level of permissions.
16. To add a sub-label to a label, select **More actions**, then **Add sub level**.
17. When finished, choose **Publish labels > Choose labels to publish > Add**. Select the labels you want to publish, and then select **Add > Done > Next**.

18. By default, the new label policy is applied to everyone. If you want to limit who the policy is applied to, select **Choose users or groups** > **Add**. Select who you want the policy to apply to, and then select **Add** > **Done** > **Next**.
19. If you want a default label for documents and email, select the label you want from the drop-down list. Review the remaining settings, adjust as needed, and then select **Next**.
20. Enter a **Name** and **Description** for your policy. Select **Next**.
21. Review your settings, then select **Publish**.

Reference:

<https://support.office.com/en-us/article/create-and-manage-sensitivity-labels-2fb96b54-7dd2-4f0c-ac8d-170790d4b8b9>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

QUESTION 46

SIMULATION

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.

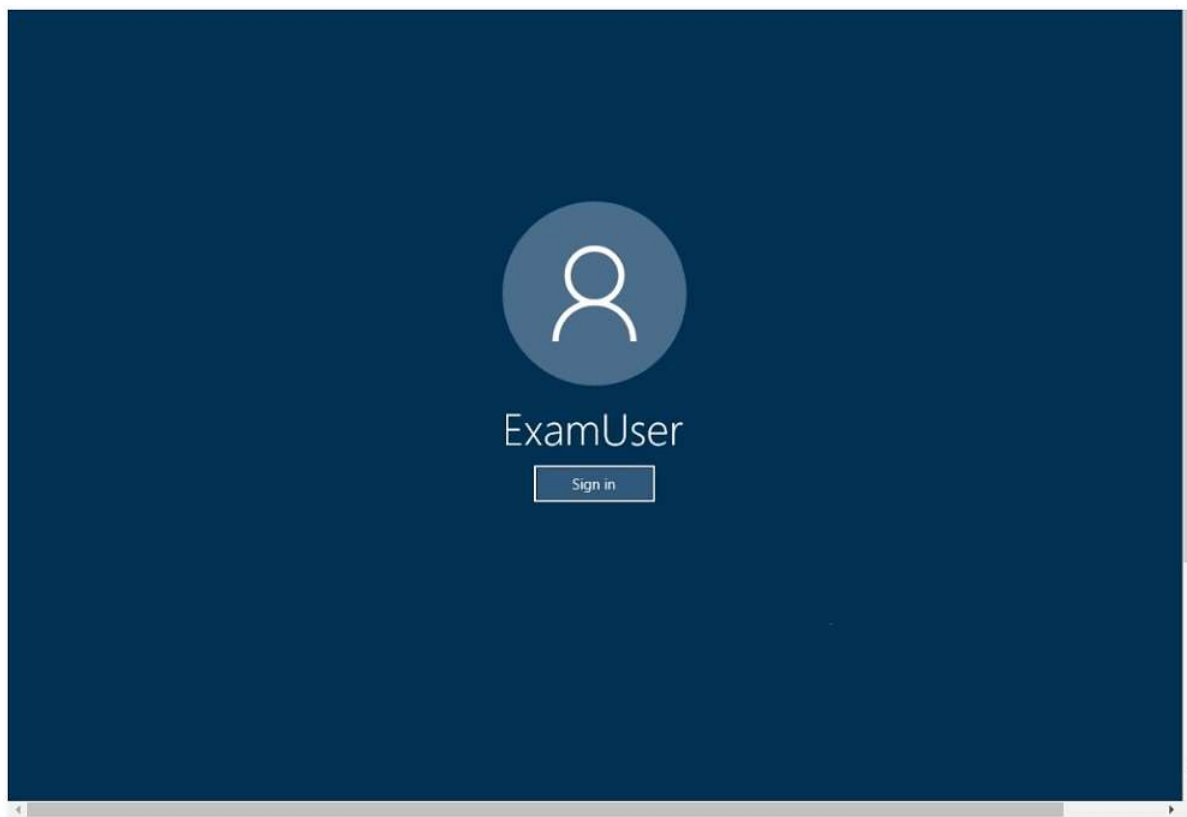
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 have 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 purposes 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.

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

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 DPT for voice mail messages 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

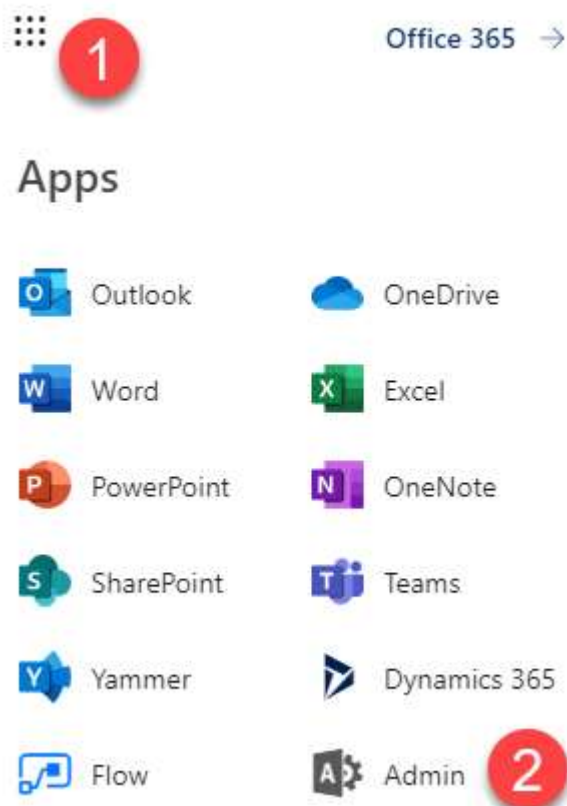
to different set of users.

1. Navigate to **Recipients > Mailboxes**.
2. In the list view, use the Shift or Ctrl keys to select multiple mailboxes.
3. In the details pane, click **More options**.
4. Under **Retention Policy**, click **Update**.
5. In **Bulk Assign Retention Policy**, select the retention policy you want to apply to the mailboxes, and then click **Save**.

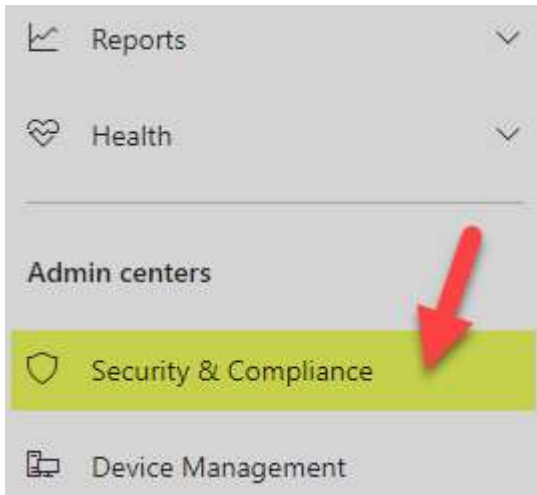
For retaining documents in SharePoint Online

Access Security & Compliance Admin Center

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



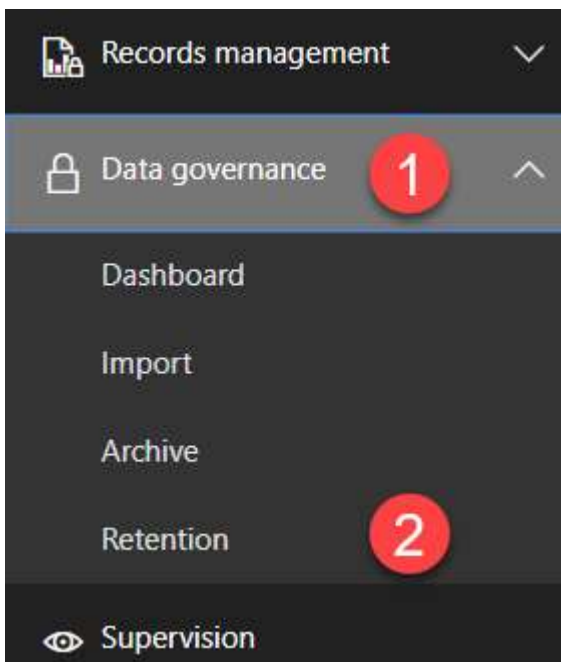
2. From the list of available Admin Centers, click on **Security & Compliance**



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

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

Under **Data Governance**, click **Retention**



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

Home > Retention

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

Labels



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

Label policies



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

+ Create

Refresh

Search

...

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

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

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

Name your policy

Settings

Choose locations

Review your settings

Name your policy

Name * ⓘ
Retain for 2 days, then delete

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

Next

Cancel

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

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

Name your policy

Settings

Choose locations

Review your settings

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

Do you want to retain content?

☒ Yes, I want to retain it

For this long... 2 days

Retain the content based on when it was last modified

Do you want us to delete it after this time?

☒ Yes ☐ No

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

☐ No, just delete content that's older than

1 years

Need more options?

☐ Use advanced retention settings

Back Next Cancel

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

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

Name your policy

Settings

Choose locations

Review your settings

Choose locations

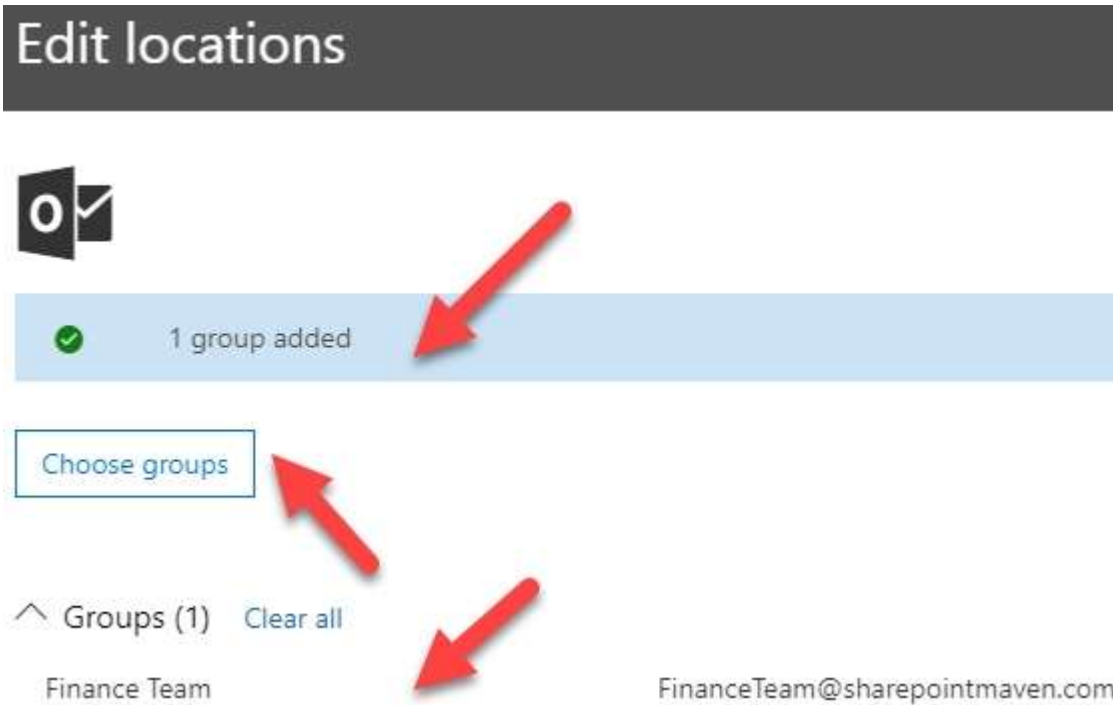
The policy will apply to content that's stored in the locations you choose.

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

☒ Let me choose specific locations

Status	Location	Include	Exclude
☒	Exchange email		
☒	SharePoint sites		
☒	OneDrive accounts		
☒	Office 365 groups	All Choose groups	None Exclude groups

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



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 [Edit](#)
Retain for 2 days, then delete

Description [Edit](#)
This policy retains documents for 2 days after they were last modified and then deletes them

Applies to content in these locations [Edit](#)
SharePoint sites

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.

[Back](#)
[Save for later](#)
[Create this policy](#)
[Cancel](#)

References:

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy#step-2-create-a-retention-policy>

<https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-retention-policy#use-the-eac-to-apply-a-retention-policy-to-multiple-mailboxes>

<https://sharepointmaven.com/how-to-set-a-retention-policy-on-a-sharepoint-site/>

QUESTION 47 SIMULATION

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.

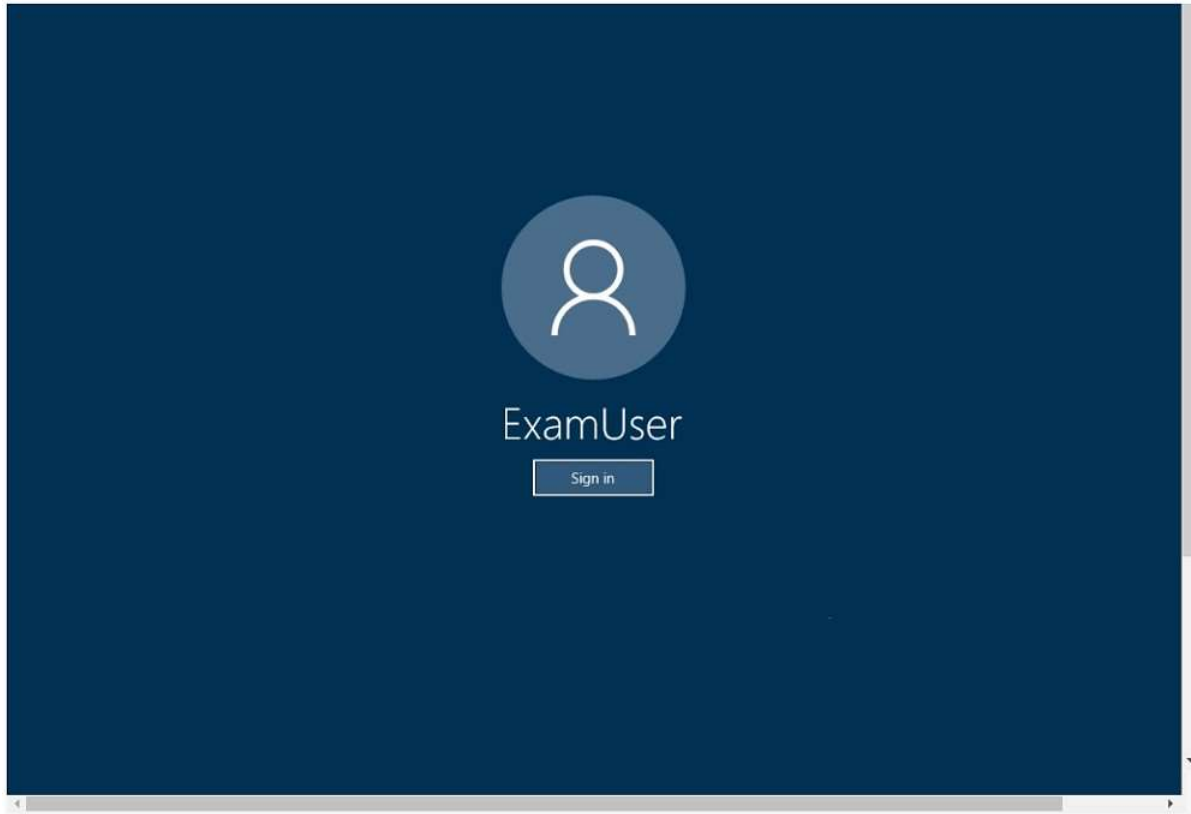
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 purposes only:

Lab instance: 11032396

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

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. Navigate to Manage Alerts in the Security & Compliance Center.
2. On the **Activity alerts** page, click **+ New**.

The flyout page to create an activity alert is displayed.

Name * A

Description B

Alert type
Custom C

Send this alert when... * D ^

Activities *

Choose activities for alert ▾

Users:

Show results for all users

Send this alert to... * E ^

Recipients *

Show results for all users

3. Complete the following fields to create an activity alert:
 - a. **Name** - Type a name for the alert. Alert names must be unique within your organization.
 - b. **Description** (Optional) - Describe the alert, such as the activities and users being tracked, and the users that email notifications are sent to. Descriptions provide a quick and easy way to describe the purpose of the alert to other admins.
 - c. **Alert type** - Make sure the **Custom** option is selected.
 - d. **Send this alert when** - Click **Send this alert when** and then configure these two fields:
 - **Activities** - Click the drop-down list to display the activities that you can create an alert for. This is the same

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

- **Users** - Click this box and then select one or more users. If the users in this box perform the activities that you added to the **Activities** box, an alert will be sent. Leave the **Users** box blank to send an alert when any user in your organization performs the activities specified by the alert.
 - e. **Send this alert to** - Click **Send this alert**, and then click in the **Recipients** box and type a name to add a user's who will receive an email notification when a user (specified in the **Users** box) performs an activity (specified in the **Activities** box). Note that you are added to the list of recipients by default. You can remove your name from this list.
4. Click **Save** to create the alert.

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

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

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

Reference:

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

QUESTION 48

SIMULATION

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.

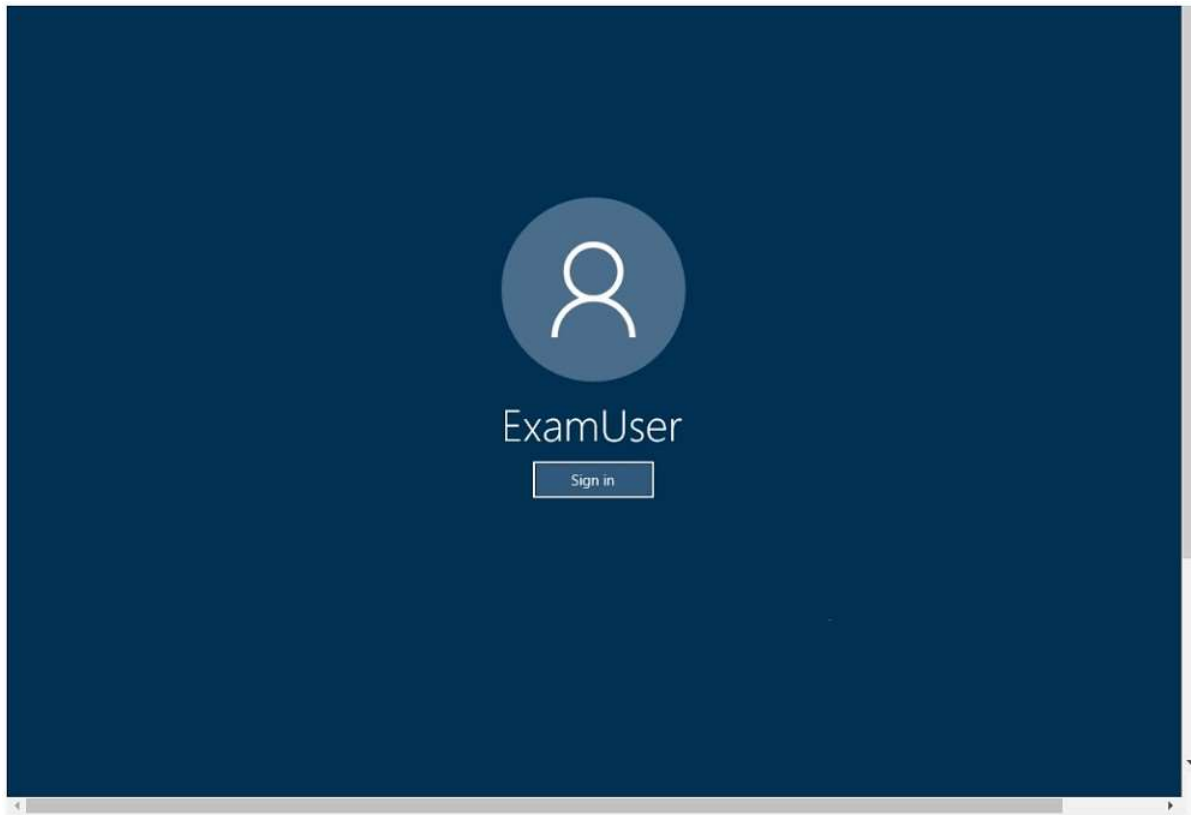
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external 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 purposes only:

Lab instance: 11032396

You need to create a case that prevents the members of a group named Operations from deleting email messages that contain the word IPO.

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

Correct Answer: See explanation below.

Section: (none)

Explanation

Explanation/Reference:

Explanation:

1. Navigate to the Security & Compliance Center.
2. In the Security & Compliance Center, click **eDiscovery** > **eDiscovery**, and then click **Create a case**.
3. On the **New Case** page, give the case a name, type an optional description, and then click **Save**. The case name must be unique in your organization.



The screenshot shows a 'New case' dialog box. At the top, there's a dark header with the text 'New case' and a close button (an 'X' in a square). Below the header, the main area is white. It starts with the instruction 'Enter a name and description' followed by a sub-instruction 'Give this case a friendly name so you can easily find it again later.' There are two input fields: a single-line text box labeled '*Case name' and a larger multi-line text box labeled 'Description'. At the bottom of the dialog, there are two buttons: a grey 'Save' button and a blue 'Cancel' button.

The new case is displayed in the list of cases on the **eDiscovery** page.

After you create a case, the next step is to add members to the case. The eDiscovery Manager who created the case is automatically added as a member. Members have to be assigned the appropriate eDiscovery permissions so they can access the case after you add them.

4. In the Security & Compliance Center, click **eDiscovery** > **eDiscovery** to display the list of cases in your organization.
5. Click the name of the case that you want to add members to.

The **Manage this case** flyout page is displayed.

Manage this case



Manage members

+ Add

— Remove

Search



^ Users (1)

Company Admin

Manage role groups

+ Add

— Remove

Search



^ Role Groups (0)

Manage case status

Name *

New case1

Description

test

Created

2018-03-22 15:15:16

Status

Closing

 Delete case

 Reopen case

Save

Close

Feedback

6. Under **Manage members**, click **Add** to add members to the case.

You can also choose to add a role group to the case. Under **Manage role groups**, click **Add**.

7. In the list of people or role groups that can be added as members of the case, click the check box next to the names of the people or role groups that you want to add.

8. After you select the people or role groups to add as members of the group, click **Add**.

In **Manage this case**, click **Save** to save the new list of case members.

9. Click **Save** to save the new list of case members.

You can use an eDiscovery case to create holds to preserve content that might be relevant to the case. You can place a hold on the mailboxes and OneDrive for Business sites of people who are custodians in the case. You can also place a hold on the group mailbox, SharePoint site, and OneDrive for Business site for an Office 365 Group. Similarly, you can place a hold on the mailboxes and sites that are associated with Microsoft Teams or Yammer Groups. When you place content locations on hold, content is held until you remove the hold from the content location or until you delete the hold.

To create a hold for an eDiscovery case:

1. In the Security & Compliance Center, click **eDiscovery** > **eDiscovery** to display the list of cases in your organization.

2. Click **Open** next to the case that you want to create the holds in.

3. On the **Home** page for the case, click the **Hold** tab.

Name
holdOne
HoldTwo

4. On the **Hold** page, click **Create**.

5. On the **Name your hold** page, give the hold a name. The name of the hold must be unique in your organization.

Name your hold

Name *

Description

Next **Cancel**

6. (Optional) In the **Description** box, add a description of the hold.
7. Click **Next**.
8. Choose the content locations that you want to place on hold. You can place mailboxes, sites, and public folders on hold.

Choose locations

Location

Include



Exchange email

None

[Choose users, groups, or teams](#)



Office 365 group email



Skype for Business



Teams messages



To-Do



Yammer conversations



SharePoint sites

None

[Choose sites](#)



OneDrive accounts



Office 365 group sites



Teams sites



Yammer networks



Exchange public folders

None

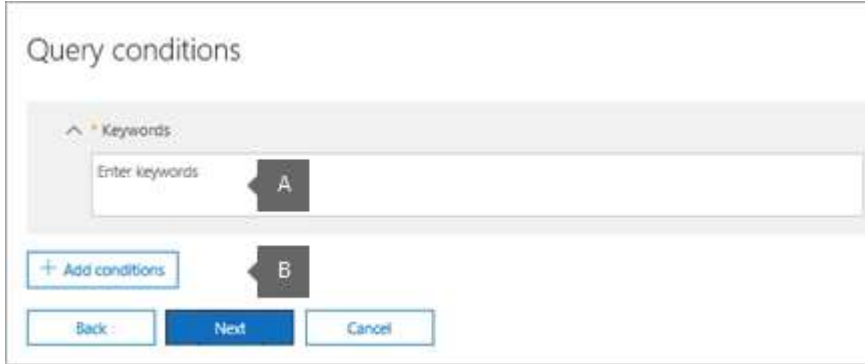


Back

Next

Cancel

a. **Exchange email** - Click **Choose users, groups, or teams** and then click **Choose users, groups, or teams** again. to specify mailboxes to place on hold. Use the search box to find user mailboxes and distribution groups (to place a hold on the mailboxes of group members) to place on hold. You can also place a hold on the associated mailbox for a Microsoft Team, a Yammer Group, or an Office 365 Group. Select the user, group, team check box, click **Choose**, and then click **Done**.



a. In the box under **Keywords**, type a search query in the box so that only the content that meets the search criteria is placed on hold. You can specify keywords, message properties, or document properties, such as file names. You can also use more complex queries that use a Boolean operator, such as **AND**, **OR**, or **NOT**. If you leave the keyword box empty, then all content located in the specified content locations will be placed on hold.

b. Click **Add conditions** to add one or more conditions to narrow the search query for the hold. Each condition adds a clause to the KQL search query that is created and run when you create the hold. For example, you can specify a date range so that email or site documents that were created within the date ranged are placed on hold. A condition is logically connected to the keyword query (specified in the keyword box) by the **AND** operator. That means that items have to satisfy both the keyword query and the condition to be placed on hold.

9. After configuring a query-based hold, click **Next**.

10. Review your settings, and then click **Create this hold**.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-cases?view=o365-worldwide>