

MS-500.VCEplus.premium.exam.63q

Number: MS-500  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1.0



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

MS-500

Microsoft 365 Security Administration (beta)



Version 1.0

## Testlet 1

### 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 members name

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

What should you do to meet the security requirements?

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

**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:**

**Testlet 2**

#### **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 range 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
Group 1	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

**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
- Integrate Windows Defender and Windows Defender ATP on domain-joined servers

- 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 want 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 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:**

### Testlet 3

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

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktops 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 Intune Configuration

The devices enrolled in Intune 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	Not applicable	GroupA
Device6	Windows 10	Enabled	None



The device compliance policies in Intune 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	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

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 implement 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

<b>ADGroup1:</b>	None	V
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

<b>ADGroup2:</b>	None	V
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

**Correct Answer:**

#### Answer Area

<b>ADGroup1:</b>	None	V
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

<b>ADGroup2:</b>	None	V
	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**

A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.

**Yes**

**No**

☐
☐

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

A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.

Yes

☐

No

☒

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:**

**Question Set 4**

**QUESTION 1**

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

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

You have a Microsoft 365 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 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 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 [\(earn more\)](#)

- ☒ 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 [\(earn more\)](#)

- ☐ 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 [\(earn more\)](#)

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 [\(earn more\)](#)

- ☐ 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.

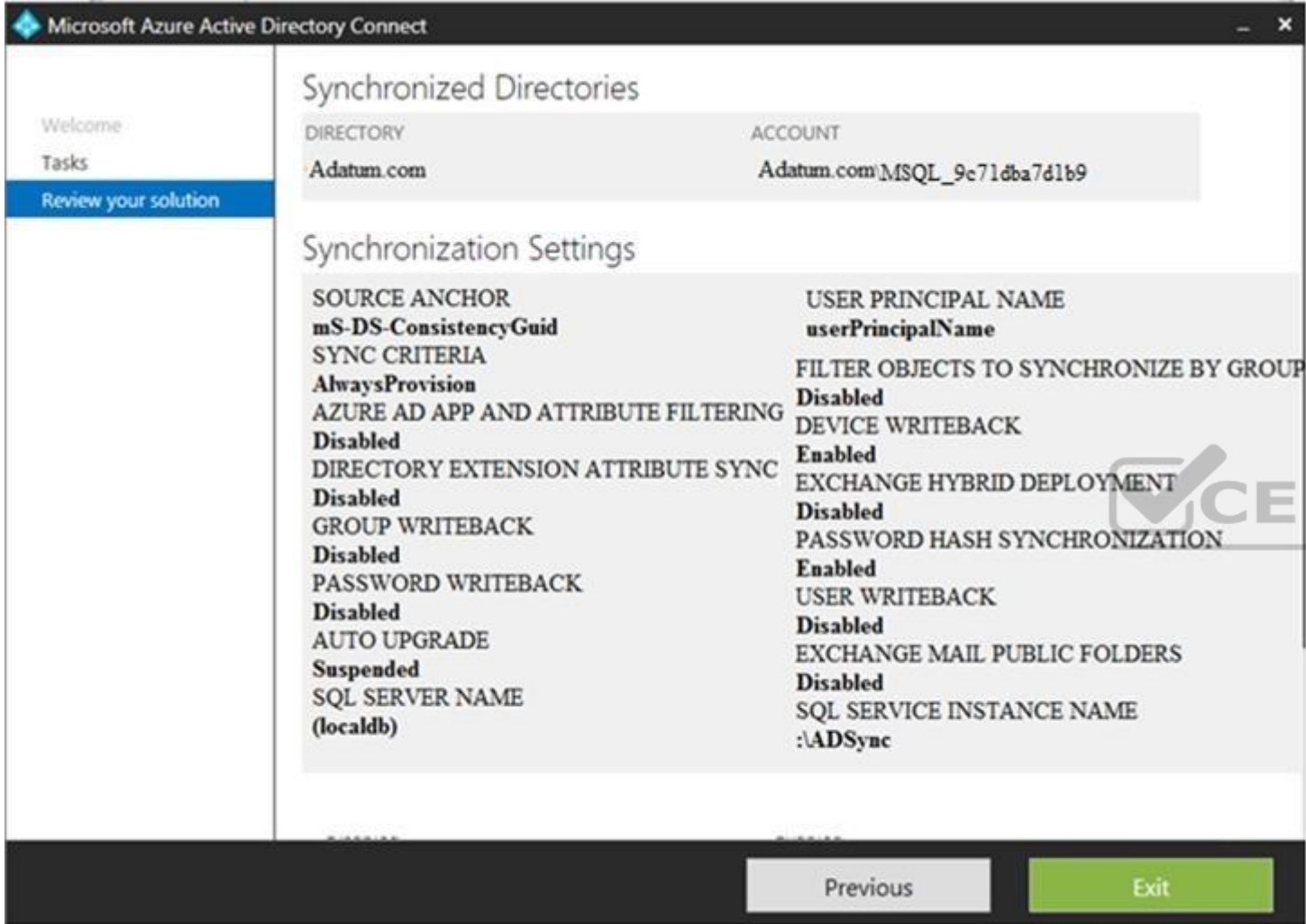


Hot Area:  
Correct Answer:

Section: [none]  
Explanation  
Explanation/Reference:

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, 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, 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 see 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 subscription.

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

What should you use to achieve the goal?

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

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

**QUESTION 9** Your company has a Microsoft 365 subscription.

The company forbids users to enroll personal devices in mobile device management (MDM).

Users in the sales department have personal iOS devices.

You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.

The users must be prevented from backing up the app's data to iCloud.

What should you create?

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

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**



## Testlet 1

### 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

### 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	
Anti-spam	
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	
Anti-spam	
Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

Section: [none]



Explanation  
Explanation/Reference:



## Testlet 2

### 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 range 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
Group 1	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

**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
- Integrate Windows Defender and Windows Defender ATP on domain-joined servers
- 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:**

**Correct Answer:**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

**QUESTION 2** You need to implement Windows 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:**

**Testlet 3**

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

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktops 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 Intune Configuration

The devices enrolled in Intune 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	Not applicable	GroupA
Device6	Windows 10	Enabled	None

The device compliance policies in Intune 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	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

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 implement Azure AD Privileged Identity Management

#### QUESTION 1

##### HOTSPOT

You are evaluating which devices are compliant in Intune.

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

**NOTE:** Each correct selection is worth one point.

**Hot Area:**

### Answer Area

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

Correct Answer:

### Answer Area

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

Section: [none]  
Explanation

Explanation/Reference:



#### Question Set 4

**QUESTION 1** 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

**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 2** You have a Microsoft 365 Enterprise E5 subscription.

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

What is a prerequisite for running Attack simulator?

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



**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

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

**QUESTION 3** 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 address that you intend to spoof belongs to the Executive group members.

What should you do first?

- A. From Azure ATP admin center, configure the primary workspace settings
- B. From the Microsoft Azure portal, configure the user risk 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 4** 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 5**

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 6**  
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 Intune 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.

<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

**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.

<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>

**Section:** [none]

**Explanation**

**Explanation/Reference:**

**QUESTION 7** 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 8

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

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

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

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

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

**NOTE:** Each correct selection is worth one point.

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 9** 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 10

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 location may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

**Select and Place:**

**Correct Answer:**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

**QUESTION 11** You have a Microsoft 365 subscription.

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

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

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

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

**Correct Answer: D**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

#### QUESTION 12

Your company has 500 computers.

You plan to protect the computers by using Windows 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:

- Windows 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 Windows 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 Set 1

### QUESTION 1

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

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

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

You add CompanyConfidential to a global policy.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

### QUESTION 2

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

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

You have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

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

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

Solution: You modify the encryption settings of the label.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

### QUESTION 3

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

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

You have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.

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

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

Solution: You modify the content expiration settings of the label.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

#### QUESTION 4

##### 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	<u>Group1@contoso.com</u>
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	<u>Group4@contoso.com</u>



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	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 only	



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 only	



Section: [none]

Explanation

Explanation/Reference:

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

### QUESTION 5

HOTSPOT

You have the Microsoft 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.

**Hot Area:**

**Correct Answer:**

**Section:** [none]

**Explanation**

**Explanation/Reference:**

## QUESTION 6

### 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	10.10.0.0/16	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



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: 30

Within timeframe: 1 minutes

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

Edit and preview results

ACTIVITIES MATCHING ALL OF THE FOLLOWING

IP address

Raw IP address

equals

10.10.0.0/24

-

OR

194.25.2.0/24

-

+

Activity type

equals

Download file

User

From group

equals

Applicaition(Cloud App Security)

as

Actor only

+

Alerts

☒ Create alert Use your organization's default settings
 

Daily alert limit 5

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:**

**Correct Answer:**

**Section:** [none]

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

**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 8** You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

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

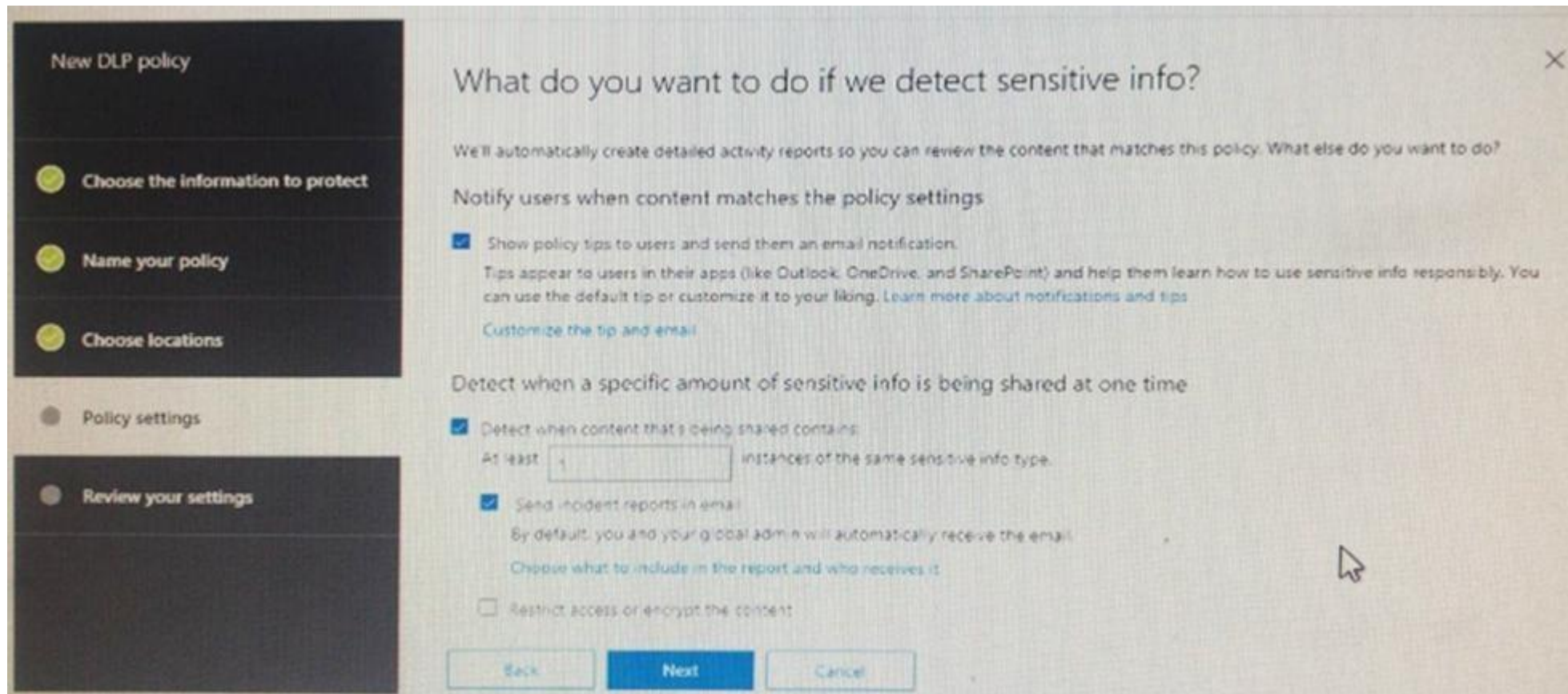
What should you do?

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

**Correct Answer:** B  
**Section:** [none]  
**Explanation**

**Explanation/Reference:**

**QUESTION 9**  
You create a data loss prevention (DLP) policy as shown in the following shown:



What is the effect of the policy when a user attempts to send an email messages 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 10** You have a Microsoft 365 subscription.

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

Which type of site collection should you create first?

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

**Correct Answer:** C

**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 11****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:****Correct Answer:**

**Section:** [none]

**Explanation****Explanation/Reference:**

Reference:

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





## Question Set 1

### QUESTION 1

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 2

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 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... ▾ 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 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].

cannot recover the file	▼
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

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 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].

cannot recover the file	▼
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

Section: [none]

Explanation

Explanation/Reference:

QUESTION 3 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:**

**Correct Answer:**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 4

You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution.

**NOTE:** Each correct selection is worth one point.

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



**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 5** You recently created and published several labels 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 6

You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1.

You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1.

What should you do first?

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

**Correct Answer: C**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 7

##### 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:**

**Correct Answer:**

**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-orwhat-takes-precedence>

**QUESTION 8** 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**

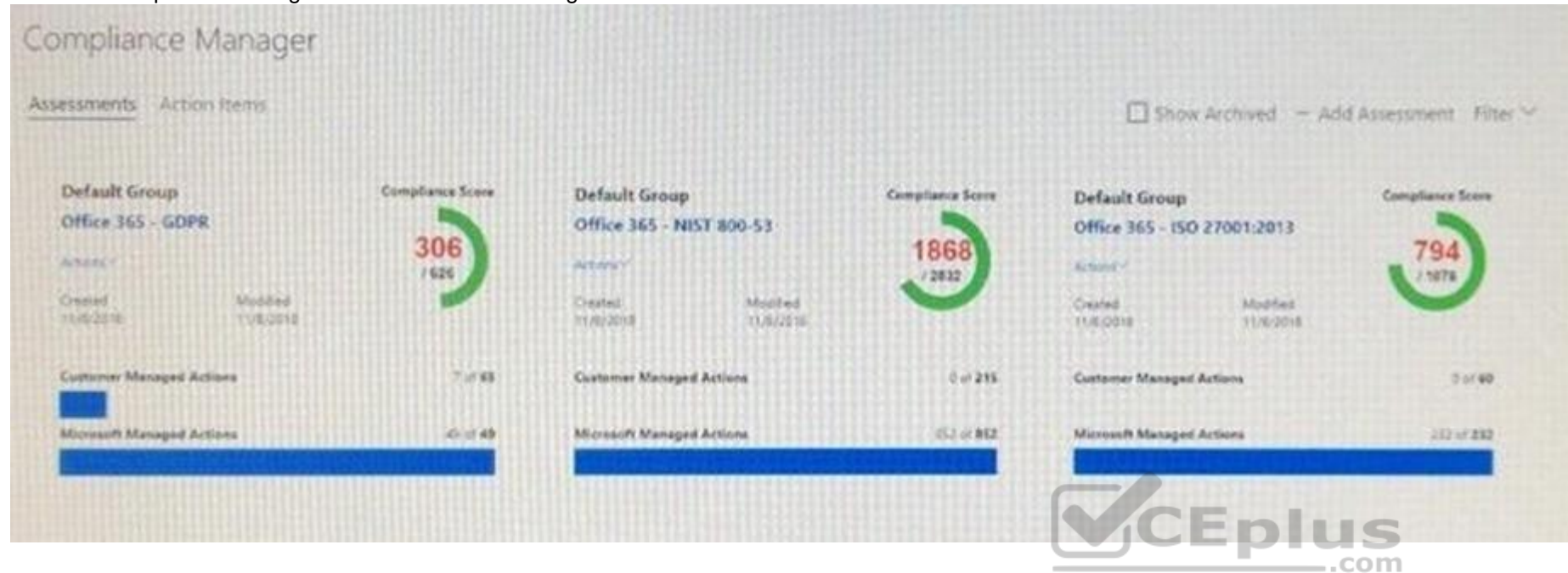
**Explanation/Reference:**

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

### QUESTION 9

#### 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	✓
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	

Correct Answer:

## 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	



Section: [none]  
Explanation

### Explanation/Reference:

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

**QUESTION 10** You have a Microsoft 365 subscription.

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

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

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

What should you create from the Intune admin center?

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

**Correct Answer: A**

Section: [none]

Explanation

### Explanation/Reference:

Reference:

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

**QUESTION 11**

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 12** 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 13** You have a hybrid Microsoft 365 environment.

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

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

What should you do?

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

**Correct Answer: C**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

**QUESTION 14** 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 15** 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 16**

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:**

**Correct Answer:**

**Section: [none]**

**Explanation**

**Explanation/Reference:**



## Testlet 2

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

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktops 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 Intune Configuration

The devices enrolled in Intune 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	Not applicable	GroupA
Device6	Windows 10	Enabled	None



The device compliance policies in Intune 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	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

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 implement 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:**