vce trainer

# microsoft.examlabs.ms-500.v2021-01-16.by.albie.112q.vce

MS-500

ExamCollection

**MS-500**

**Microsoft 365 Security Administration**

**Version 13.0**

| | |
|---|---|
| Score: | 800/1000 |
| Version: | n/A |
| Time Limit: | 0 Minutes |

# Implement and manage identity and access (5 questions)

## *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 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?

- ☐ Yes
- ☐ No

## *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 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?

- ☐ Yes
- ☐ No

## *Question 18*

**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?

- ☐ Yes
- ☐ No

***Question 19***

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.)


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.

**Answer Area**

**User1:**

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

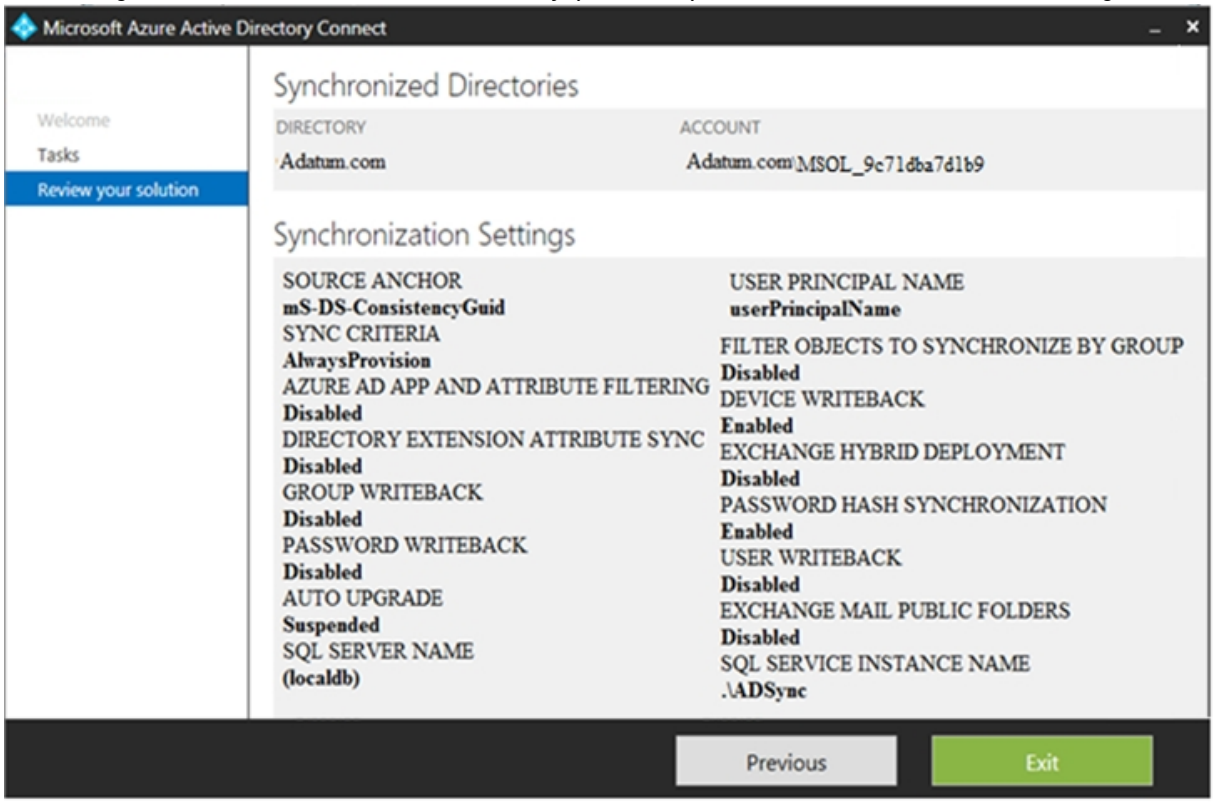
**User2:**

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

## *Question 20*

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.

**Answer Area**

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

| | |
|---|---|
| be overwritten<br>be synced to Active Directory<br>be subject to the Active Directory password policy | V |

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

| | |
|---|---|
| an object will be provisioned in the Computers container<br>an object will be provisioned in the RegisteredDevices container<br>the device object in Azure will be deleted during synchronization | V |

## *Case Study (5 questions)*

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:

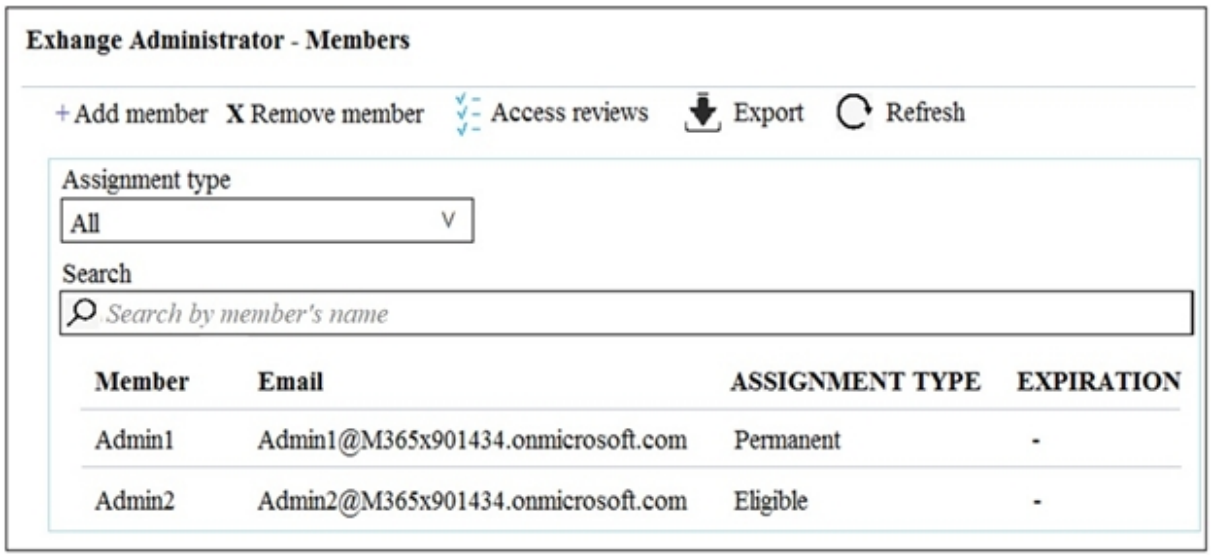
- User administrators will work from different countries
- User administrators will use the Azure Active Directory admin center
- Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

**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.




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**

## 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?

- ☐ Sign-ins
- ☐ Azure AD Identity Protection
- ☐ Authentication methods
- ☐ Access review

## 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.

Set the frequency to:

| | |
|---|---|
| One time<br>Weekly<br>Monthly | V |

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

| | |
|---|---|
| Upon completion settings<br>Advanced settings<br>Programs<br>Reviewers | V |

## 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 device compliance policy
- ☐ an access review
- ☐ a user risk policy
- ☐ a sign-in 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?

- ☐ Synchronization Service Manager
- ☐ Azure AD Connect wizard
- ☐ Synchronization Rules Editor
- ☐ IdFix

***Case Study (5 questions)***

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:

| 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.

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

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

## *Question 6*

You need to create Group2.

What are two possible ways to create the group?

- ☐ an Office 365 group in the Microsoft 365 admin center
- ☐ a mail-enabled security group in the Microsoft 365 admin center
- ☐ a security group in the Microsoft 365 admin center
- ☐ a distribution list in the Microsoft 365 admin center
- ☐ a security group in the Azure AD admin center

## Question 7

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

- ☐ 131.107.83.0/28
- ☐ 192.168.16.0/20
- ☐ 172.16.0.0/24
- ☐ 192.168.0.0/20

## Question 8

HOTSPOT

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

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

**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 set to accountEnabled Equals true
- A dynamic membership rule set to userType Equals Member

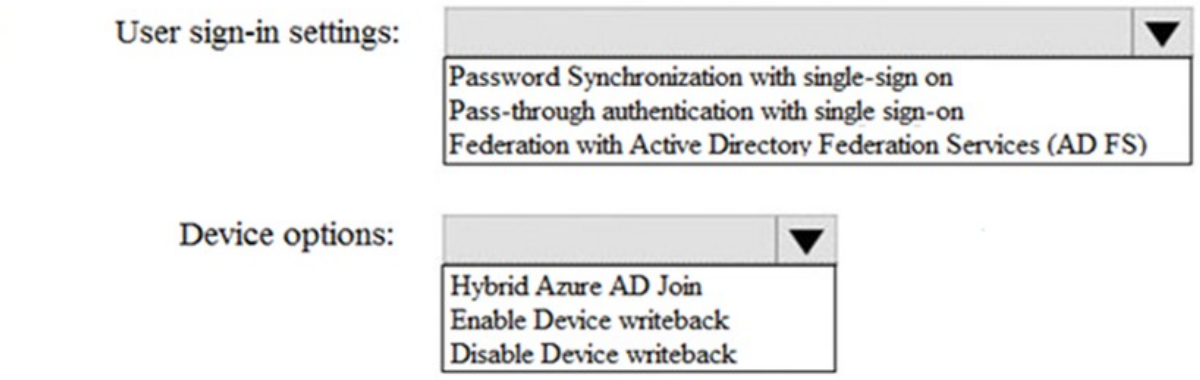
## Question 9

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.

**Answer Area**




## Question 10

You need to create Group3.

What are two possible ways to create the group?

- ☐ an Office 365 group in the Microsoft 365 admin center
- ☐ a mail-enabled security group in the Microsoft 365 admin center
- ☐ a security group in the Microsoft 365 admin center
- ☐ a distribution list in the Microsoft 365 admin center
- ☐ a security group in the Azure AD admin center

***Case Study (5 questions)***

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 | *Not applicable* | GroupA |
| Device6 | Windows 10 | Enabled | *None* |

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 | *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 enable and configure Azure AD Privileged Identity Management

## *Question 11*

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.

**Answer Area**

**ADGroup1:**

| |
|---|
| None<br>User1 and User2 only<br>User2 and User4 only<br>User3 and User4 only<br>User1, User2, User3, and User4 |

**ADGroup2:**

| |
|---|
| None<br>User1 and User2 only<br>User2 and User4 only<br>User3 and User4 only<br>User1, User2, User3, and User4 |

## Question 12

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.

**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. | ○ | ○ |

## Question 13

Which user passwords will User2 be prevented from resetting?

- ☐ User6 and User7
- ☐ User4 and User6
- ☐ User4 only
- ☐ User7 and User8
- ☐ User8 only

## Question 14

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

- ☐ Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
- ☐ Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
- ☐ Assign the Security administrator role to User9
- ☐ Assign the Global administrator role to User9

## *Question 15*

Which role should you assign to User1?

- ☐ Global administrator
- ☐ User administrator
- ☐ Privileged role administrator
- ☐ Security administrator

# Implement and manage threat protection (5 questions)

## *Question 56*

You have an Azure Sentinel workspace.

You need to manage incidents based on alerts generated by Microsoft Cloud App Security.

What should you do first?

- ☐ From the Cloud App Security admin center, configure security extensions.
- ☐ From the Cloud App Security admin center, configure app connectors.
- ☐ From the Cloud App Security admin center, configure log collectors.
- ☐ From the Microsoft 365 compliance center, add and configure a data connector.

## *Question 57*

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?

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

## Question 58

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.

- ☐ the Exchange admin center
- ☐ the Azure ATP admin center
- ☐ Outlook on the web
- ☐ the Security & Compliance admin center
- ☐ Microsoft Azure Security Center

## Question 59

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

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

Which type of device configuration profile should you use?

- ☐ Endpoint protection
- ☐ Device restrictions
- ☐ Identity protection
- ☐ Windows Defender ATP

## Question 60

DRAG DROP

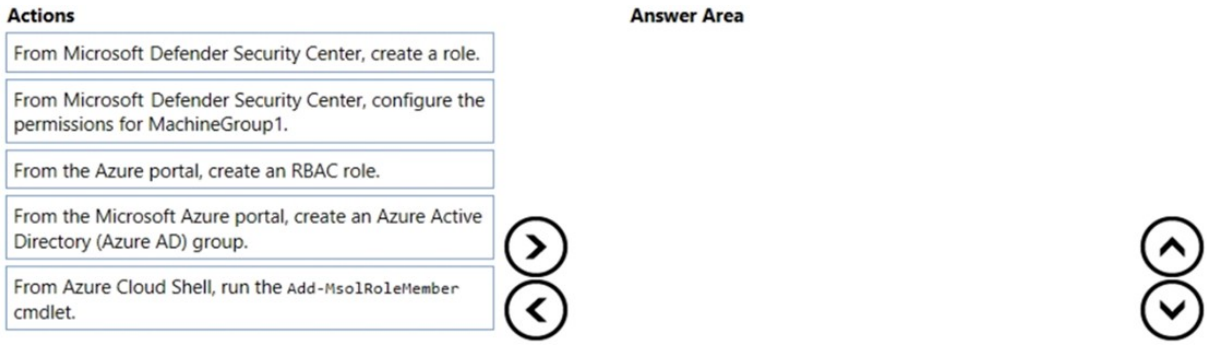
You have a Microsoft 365 E5 subscription.

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.




## Case Study (2 questions)

**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 50*

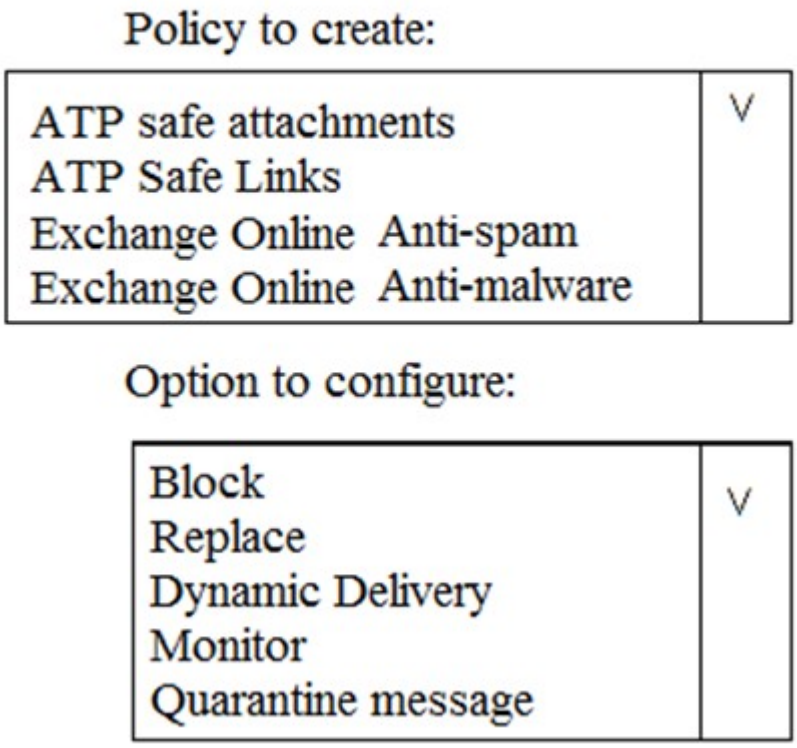
HOTSPOT

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.

**Answer Area**



## *Question 51*

HOTSPOT

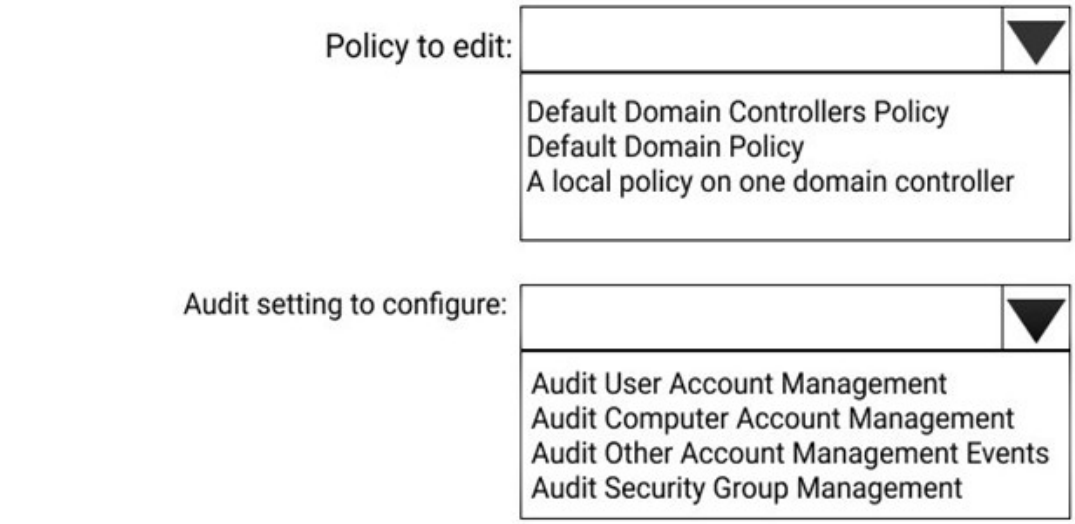
You install Azure ATP sensors on domain controllers.

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.

**Answer Area**



***Case Study (2 questions)***

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:

| 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.

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

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

## Question 52

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.

| Actions | Answer Area |
| --- | --- |
| 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 | |

## Question 53

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

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

***Case Study (2 questions)***

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 | *Not applicable* | GroupA |
| Device6 | Windows 10 | Enabled | *None* |

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 | *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 enable and configure Azure AD Privileged Identity Management

## Question 54

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.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Device2 is compliant. | ○ | ○ |
| Device5 is compliant. | ○ | ○ |
| Device6 is compliant. | ○ | ○ |

## Question 55

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.

**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

# Implement and manage information protection (5 questions)

## *Question 99*

**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?

- ☐ Yes
- ☐ No

## *Question 100*

HOTSPOT

You have a Microsoft 365 subscription.

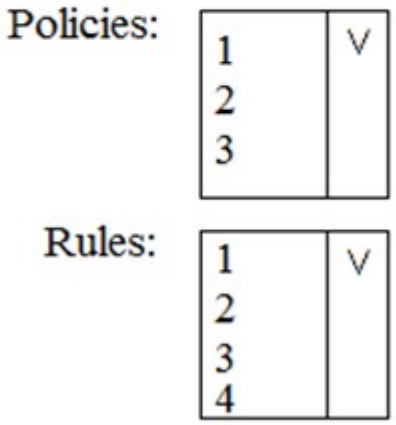
You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain EU Social Security Numbers (SSN) or Equivalent ID.
- 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.

**Answer Area**




## *Question 101*

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

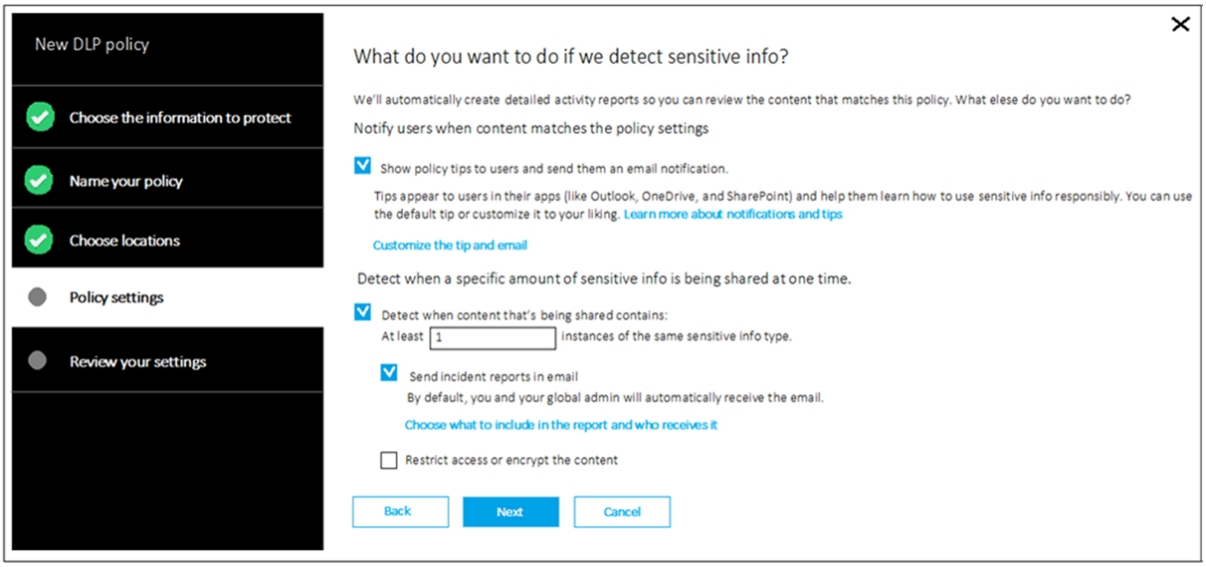
You need to prevent the users from downloading, printing, and syncing files.

What should you do?

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

## Question 102

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




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

- ☐ The user receives a notification and can send the email message
- ☐ The user receives a notification and cannot send the email message
- ☐ The email message is sent without a notification
- ☐ The email message is blocked silently

## Question 103

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?

- ☐ Records Center
- ☐ eDiscovery Center
- ☐ Enterprise Search Center
- ☐ Document Center

## *Case Study (0 questions)*

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

## Manage governance and compliance features in Microsoft 365 (0 questions)

### *Case Study (0 questions)*

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 | *Not applicable* | GroupA |
| Device6 | Windows 10 | Enabled | *None* |

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 | *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 enable and configure Azure AD Privileged Identity Management