

# Microsoft

## Exam Questions MS-102

Microsoft 365 Administrator Exam



**NEW QUESTION 1**

DRAG DROP - (Topic 6)  
 DRAG DROP

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2. You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	<ul style="list-style-type: none"> <li>• Manage service requests.</li> <li>• Purchase new services.</li> <li>• Manage subscriptions.</li> <li>• Monitor service health.</li> </ul>
Group2	<ul style="list-style-type: none"> <li>• Assign licenses.</li> <li>• Add users and groups.</li> <li>• Create and manage user views.</li> <li>• Update password expiration policies.</li> </ul>

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

**Roles**

- Billing Administrator
- Global Administrator
- Helpdesk Administrator
- License Administrator
- Service Support Administrator
- User Administrator

**Answer Area**

Group1:

Group2:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Billing admin manage service request Purchase new services Etc.

Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.

Box 2: User admin User admin

Assign the User admin role to users who need to do the following for all users:

- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health

**NEW QUESTION 2**

- (Topic 6)

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.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Service Administrator role.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

You need to assign the Security Administrator role. Reference:

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

**NEW QUESTION 3**

- (Topic 6)

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

- A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
- B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
- C. From the Microsoft 365 admin center, modify Organization information.
- D. From the Microsoft 365 admin center, modify Help desk information.

**Answer:** A

**Explanation:**

Reference:

<https://systemcenterdudes.com/intune-company-portal-customization/>

**NEW QUESTION 4**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant

You create a data loss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.

To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

## Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> Off	Exchange email	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	SharePoint sites	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Off	OneDrive accounts	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Teams chat and channel messages	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Devices	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Microsoft Cloud App Security	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	On-premises repositories	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

## Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> Off	Exchange email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	SharePoint sites	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Off	OneDrive accounts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Teams chat and channel messages	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Devices	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Microsoft Cloud App Security	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	On-premises repositories	<input type="checkbox"/>	<input type="checkbox"/>

### NEW QUESTION 5

DRAG DROP - (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to automatically label the documents on Site1 that contain credit card numbers. 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**

- Create a sensitivity label.
- Create an auto-labeling policy.
- Create a sensitive information type.
- Wait 24 hours, and then turn on the policy.
- Publish the label.
- Create a retention label.
- Wait eight hours, and then turn on the policy.

**Answer Area**

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Actions**

- Create a sensitivity label.
- Create an auto-labeling policy.
- Create a sensitive information type.
- Wait 24 hours, and then turn on the policy.
- Publish the label.
- Create a retention label.
- Wait eight hours, and then turn on the policy.

**Answer Area**

- Create a sensitivity label.
- Publish the label.
- Create an auto-labeling policy.

### NEW QUESTION 6

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Install:

Server:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: The Azure AD Connect provisioning agent Install the Azure AD Connect provisioning agent

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

\* An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

**NEW QUESTION 7**

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

**NEW QUESTION 8**

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. Android Enterprise
- D. Windows 8.1

**Answer:** D

**NEW QUESTION 9**

- (Topic 6)

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.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

You need to assign the Security Administrator role. Reference:

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

**NEW QUESTION 10**

- (Topic 6)

You have a Microsoft 365 tenant.

You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.

What should you use?

- A. an attack surface reduction (ASR) policy
- B. an app configuration policy
- C. a device compliance policy
- D. a device configuration profile

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 10**

HOTSPOT - (Topic 6)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

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

Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (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.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

**NEW QUESTION 12**

- (Topic 6)

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.

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The question states that "all the user account synchronizations completed successfully". Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

**NEW QUESTION 17**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

On Monday, you create a new user named User1.

On Tuesday, User1 signs in for the first time and perform the following actions:

- Signs in to Microsoft Exchange Online from an anonymous IP address
- Signs in to Microsoft SharePoint Online from a device in New York City.
- Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections

Which types of sign-in risks will Azure AD Identity Protection detect for User1?

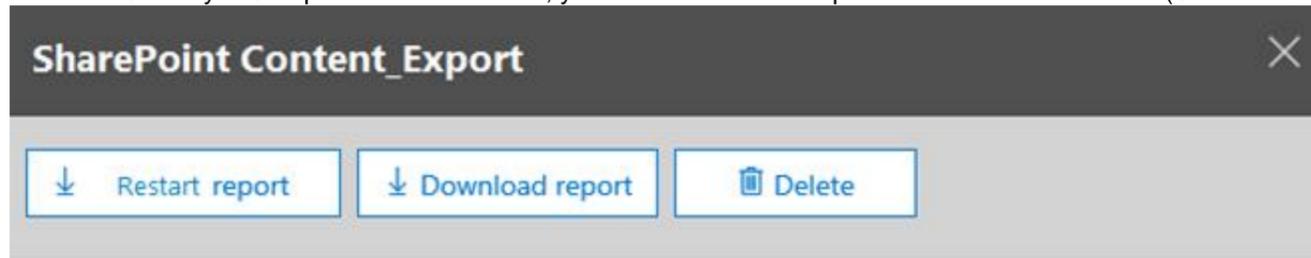
- A. anonymous IP address only
- B. anonymous IP address and atypical travel
- C. anonymous IP address, atypical travel, and unfamiliar sign-in properties
- D. unfamiliar sign-in properties and atypical travel only
- E. anonymous IP address and unfamiliar sign-in properties only

Answer: C

**NEW QUESTION 22**

- (Topic 6)

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



**Status:**

The export has completed. You can start downloading the results.

**Items included from the search:**

All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

**Exchange content format:**

One PST file for each mailbox.

**De-duplication for Exchange content:**

Not enabled.

**SharePoint document versions:**

Included

**Export files in a compressed (zipped) folder:**

Yes

**The export data was prepared within region:**

Default region

Close

Feedback

What will be excluded from the export?

- A. a 10-MB XLSX file
- B. a 5-MB MP3 file
- C. a 5-KB RTF file
- D. an 80-MB PPTX file

Answer: B

**Explanation:**

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide>

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

**NEW QUESTION 26**

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 28**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to compare the current Safe Links configuration to the Microsoft recommended configurations.

What should you use?

- A. Microsoft Purview
- B. Azure AD Identity Protection
- C. Microsoft Secure Score
- D. the configuration analyzer

**Answer:** C

**NEW QUESTION 32**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

- Retention period 7 years
  - Start the retention period based on: When items were created
- You need to prevent the removal of the label once the label is applied to an item. What should you select in the retention label settings?

- A. Retain items even if users delete
- B. Mark items as a record
- C. Mark items as a regulatory record
- D. Retain items forever

**Answer: B**

**NEW QUESTION 37**

- (Topic 6)

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

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1. To which resource can you apply Label1?

- A. Group1 only
- B. Group2 only
- C. Site1 only
- D. Group1 and Group2 only
- E. Group1, Group2, and Site1

**Answer: E**

**Explanation:**

Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory

Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.

In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.

When you configure a label policy, you can:

Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

**NEW QUESTION 40**

- (Topic 6)

You have a Microsoft E5 subscription.

You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time. What should you implement?

- A. Azure AD Privileged Identity Management (PIM)
- B. a conditional access policy
- C. a communication compliance policy
- D. Azure AD Identity Protection
- E. groups that have dynamic membership

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 44**

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365 and contains a mailbox named Mailbox1.

You plan to use Mailbox1 to collect and analyze unfiltered email messages.

You need to ensure that Defender for Office 365 takes no action on any inbound emails delivered to Mailbox1.

What should you do?

- A. Configure a retention policy for Mailbox1.
- B. Create a mail flow rule.
- C. Configure Mailbox1 as a SecOps mailbox.
- D. Place a litigation hold on Mailbox1.

**Answer: D**

**NEW QUESTION 48**

- (Topic 6)  
 You have a Microsoft 365 F5 subscription.  
 You plan to deploy 100 new Windows 10 devices.  
 You need to order the appropriate version of Windows 10 for the new devices. The version must meet the following requirements.  
 Be serviced for a minimum of 24 months.  
 Support Microsoft Application Virtualization (App-V) Which version should you identify?

- A. Window 10 Pro, version 1909
- B. Window 10 Pro, version 2004
- C. Window 10 Pro, version 1909
- D. Window 10 Enterprise, version 2004

**Answer: D**

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/windows/release-health/release-information>  
<https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations>

**NEW QUESTION 53**

- (Topic 6)  
 You have a Microsoft 365 subscription that contains the alerts shown in the following table.

Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

Which properties of the alerts can you modify?

- A. Status only
- B. Status and Comment only
- C. Status and Severity only
- D. Status, Severity, and Comment only
- E. Status, Severity, Comment and Category

**Answer: B**

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations>

**NEW QUESTION 55**

- (Topic 6)  
 You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online.  
 You need to enable unified labeling for Microsoft 365 groups. Which cmdlet should you run?

- A. set-unifiedGroup
- B. Set-Labelpolicy
- C. Execute-AzureAdLabelSync
- D. Add-UnifiedGroupLinks

**Answer: C**

**NEW QUESTION 60**

- (Topic 6)  
 Your network contains an Active Directory forest named Contoso. Local. You have a Microsoft 365 subscription.  
 You plan to implement a directory synchronization solution that will use password hash synchronization.  
 From the Microsoft 365 admin center, you successfully verify the contoso.com domain name.  
 You need to prepare the environment for the planned directory synchronization solution. What should you do first?

- A. From Active Directory Domains and Trusts, add contoso.com as a UPN suffix.
- B. From the Microsoft 365 admin center verify the Contos
- C. Local domain name.
- D. From the public DNS zone of contoso.com, add a new mail exchanger (MX) record.
- E. From Active Directory Users and Computers, modify the UPN suffix for all users.

**Answer: A**

**NEW QUESTION 61**

HOTSPOT - (Topic 6)  
 HOTSPOT  
 You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	<b>None</b>

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	<b>None</b>
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Add apps to the private store:

▼

- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:

▼

- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Add apps to the private store:

▼

- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:

▼

- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

**NEW QUESTION 62**

- (Topic 6)

You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.

You need to prevent the members of Group1 from communicating with the members of Group2 by using Microsoft Teams. The solution must comply with regulatory requirements and must not affect other user in the tenant.

What should you use?

- A. information barriers
- B. communication compliance policies
- C. moderated distribution groups
- D. administrator units in Azure Active Directory (Azure AD)

**Answer:** A

**NEW QUESTION 65**

- (Topic 6)

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create an Azure AD tenant.

You plan to sync the on-premises Active Directory to Azure AD.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.

What should you include in the recommendation?

- A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
- B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
- C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
- D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

**Answer:** A

**Explanation:**

Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.

Reference:

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

**NEW QUESTION 70**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.

What is the longest time range that can be included in the report?

- A. 1 day
- B. 7 days
- C. 30 days
- D. 90 days

**Answer:** C

**Explanation:**

View email security reports in the Microsoft 365 Defender portal

The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security>

**NEW QUESTION 75**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policy to create in Microsoft Endpoint Manager:

	▼
An app configuration policy	
An app protection policy	
A conditional access policy	
A device compliance policy	

Minimum number of required policies:

	▼
1	
2	
3	
5	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Policy to create in Microsoft Endpoint Manager:

	▼
An app configuration policy	
An app protection policy	
A conditional access policy	
A device compliance policy	

Minimum number of required policies:

	▼
1	
2	
3	
5	

**NEW QUESTION 78**

- (Topic 6)

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.

Your network contains an Active Directory domain. You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to the Microsoft Entra tenant. All the other user accounts synchronized successfully.

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.

Solution: From Microsoft Entra Connect, you modify the filtering settings. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 82**

HOTSPOT - (Topic 6)

HOTSPOT

You have a new Microsoft 365 E5 tenant. Enable Security defaults is set to Yes.

A user signs in to the tenant for the first time.

Which multi-factor authentication (MFA) method can the user use, and how many days does the user have to register for MFA? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

MFA method:

Number of days:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Notification to Microsoft Authenticator app

Do users have 14 days to register for Azure AD Multi-Factor Authentication?

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Box 2: 14

Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they'll be required to register before they can complete the sign-in process.

**NEW QUESTION 87**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

- A. From Policy in the Azure portal, select Compliance, and then assign a policy
- B. From Compliance Manager, create an assessment
- C. From the Microsoft J6i compliance center, create an audit retention policy.
- D. From the Microsoft 365 admin center enable the Productivity Score.

**Answer:** B

**NEW QUESTION 88**

HOTSPOT - (Topic 6)

You have several devices enrolled in Microsoft Endpoint Manager

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

The device limit restrictions in Endpoint manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager

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

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
 Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll an unlimited number of devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 90**

- (Topic 6)

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint Online site. What should you do?

- A. From the SharePoint Online site, create an alert.
- B. From the SharePoint Online admin center, modify the sharing settings.
- C. From the Microsoft 365 Defender portal, create an alert policy.
- D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

**Answer:** D

**NEW QUESTION 95**

- (Topic 6)

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.

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You raise the forest functional level to Windows Server 2016.

You copy the Group

Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

- A. yes
- B. No

**Answer:** B

**NEW QUESTION 97**

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

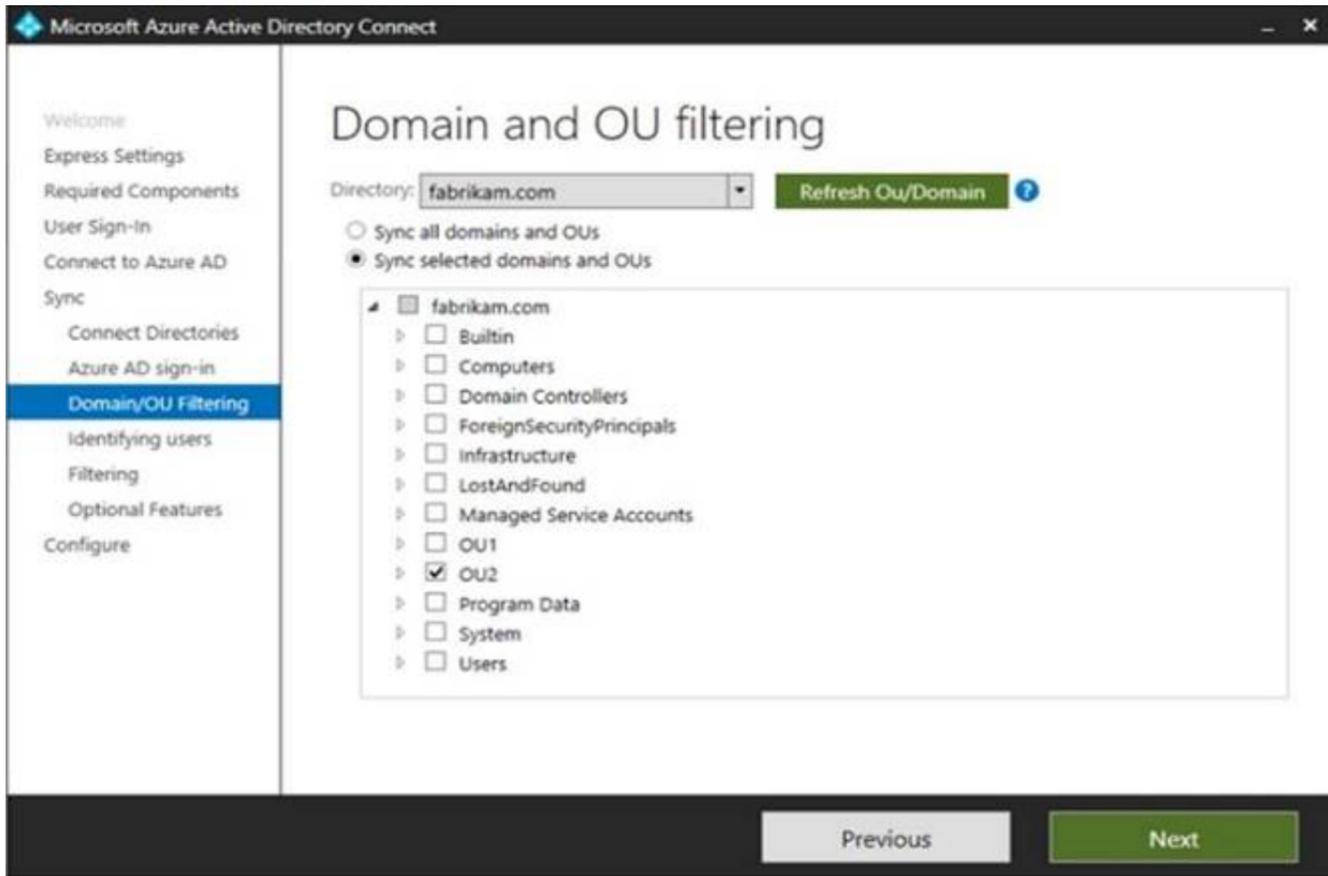
Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group - Global	OU1
User3	User	OU2
Group2	Security Group - Global	OU2

The groups have the members shown in the following table.

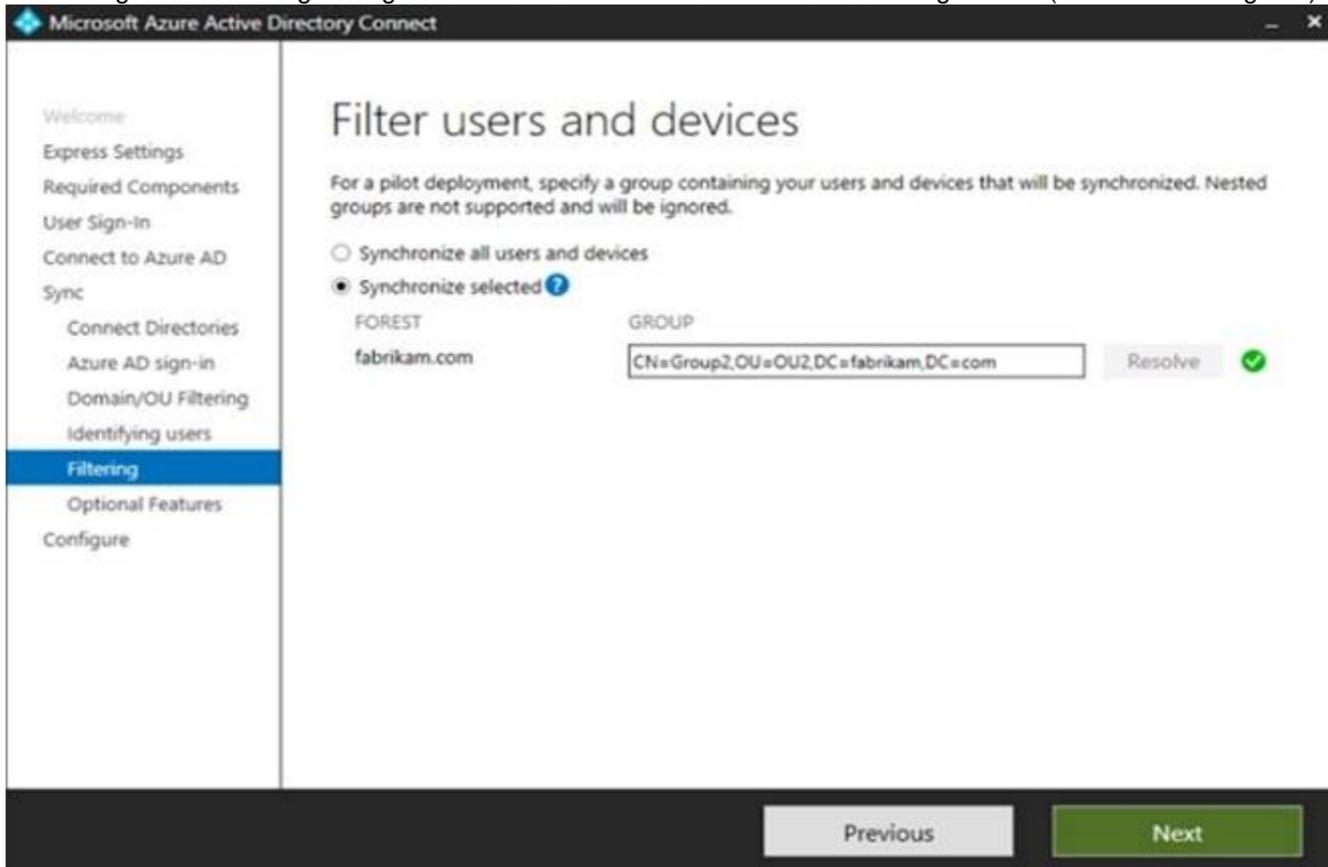
Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



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
User2 will synchronize to Azure AD.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group2 will synchronize to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>
User3 will synchronize to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: No

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.

User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.

Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

**NEW QUESTION 100**

- (Topic 6)

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

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort. What should you do first?

- A. From the Microsoft 365 admin center, create a mail-enabled security group.
- B. From the Microsoft 365 Defender portal, create a device group.
- C. From the Microsoft Endpoint Manager admin center, create a device category.
- D. From the Azure Active Directory admin center, create a dynamic device group.

**Answer: B**

**Explanation:**

Reference:

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

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

**NEW QUESTION 104**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations: Name: Policy1

Assignments:

- Users and groups: Group1

- Cloud apps or actions: All cloud apps

? Access controls:

? Grant, require multi-factor authentication

? Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

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

NOTE: Each correct selection is worth one point.

**Statements**

**Yes No**

Admin1 can set Enable policy for Policy1 to **On**.

Admin2 can set Enable policy for Policy1 to **Off**.

Admin3 can set Users and groups for Policy1 to **All users**.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

? Conditional Access policies can be enabled in report-only mode.

? During sign-in, policies in report-only mode are evaluated but not enforced.

? Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

? Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

**NEW QUESTION 105**

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You need to meet the following requirements:

- Report a Microsoft 365 service issue.
- Request help on how to add a new user to an Azure AD tenant.

What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Features	Answer Area
Message center	To report issues regarding a Microsoft 365 service: <input type="text"/>
New service request	To request help on how to add a new user to the tenant: <input type="text"/>
Product feedback	
Service health	

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Features	Answer Area
Message center	To report issues regarding a Microsoft 365 service: <input type="text" value="New service request"/>
New service request	To request help on how to add a new user to the tenant: <input type="text" value="Message center"/>
Product feedback	
Service health	

**NEW QUESTION 107**

- (Topic 6)

You have a Microsoft 365 tenant and a LinkedIn company page.

You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.

Where can you store data from the LinkedIn connector?

- A. a Microsoft OneDrive for Business folder
- B. a Microsoft SharePoint Online document library
- C. a Microsoft 365 mailbox
- D. Azure Files

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide>

**NEW QUESTION 112**

- (Topic 6)

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	None

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Delete User2 and User4 only.
- B. Reset the password of User4 only
- C. Reset the password of any user in Azure AD.
- D. Delete User1, User2, and User4 only.
- E. Reset the password of User2 and User4 only.
- F. Delete any user in Azure AD.

**Answer: AE**

**Explanation:**

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below). Only on users who are non-admins or in any of the following limited admin roles:

- Directory Readers
- Guest Inviter
- Helpdesk Administrator
- Message Center Reader
- Reports Reader
- User Administrator Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles>

**NEW QUESTION 116**

HOTSPOT - (Topic 6)

HOTSPOT

Assessment	Score	Status	Progress	Actions	Completed	Group	Provider	Standard
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input checked="" type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input checked="" type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 118**

HOTSPOT - (Topic 6)

You have a Microsoft 365 tenant that contains the groups shown in the following table.

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

You plan to create a compliance policy named Compliance1. You need to identify the groups that meet the following requirements:  
 ? Can be added to Compliance1 as recipients of noncompliance notifications  
 ? Can be assigned to Compliance1  
 To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Can be added to Compliance1 as recipients of noncompliance notifications:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

▼
Group1 and Group4 only
Group3 and Group4 only
Group1, Group2 and Group3 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

**NEW QUESTION 120**

- (Topic 6)

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.

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the filtering settings.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 122**

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

? Opening files in Microsoft SharePoint that contain malicious content

? Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

### Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

### NEW QUESTION 124

HOTSPOT - (Topic 6)  
HOTSPOT

Your network contains an on-premises Active Directory domain. You have a Microsoft 365 E5 subscription. You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

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

### Answer Area

Tool:

▼
<input type="checkbox"/> AccessChk
<input type="checkbox"/> Azure AD Connect
<input type="checkbox"/> Active Directory Explorer
<input type="checkbox"/> IdFix

Required group membership:

▼
<input type="checkbox"/> Domain Admins
<input type="checkbox"/> Domain Users
<input type="checkbox"/> Server Operators
<input type="checkbox"/> Enterprise Admins

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.

The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Windows Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.

Incorrect:

\* AccessChk

Box 2: Enterprise Admins

IdFix permissions requirements

The user account that you use to run IdFix must have read and write access to the AD DS domain.

If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.

\* Enterprise Admins

The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.

Incorrect:

\* Domain Admins

Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

\* Server Operator

Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.

\* Domain Users - too few permissions

The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

#### NEW QUESTION 125

- (Topic 6)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

A. Yes

B. No

**Answer: A**

#### NEW QUESTION 128

- (Topic 6)

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant includes a user named User1.

You enable Azure AD Identity Protection.

You need to ensure that User1 can review the list in Azure AD Identity Protection of users flagged for risk. The solution must use the principle of least privilege.

To which role should you add User1?

A. Security Reader

B. Global Administrator

C. Owner

D. User Administrator

**Answer: A**

#### NEW QUESTION 133

HOTSPOT - (Topic 6)

You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.

```

Select Administrator Windows PowerShell
Name           : Retention1
Priority        : 200
RecordTypes     : {MicrosoftTeams}
Operations      : {}
UserIds         : {}
RetentionDuration : ThreeMonths

Name           : Retention2
Priority        : 150
RecordTypes     : {MicrosoftTeams}
Operations      : {teamcreated}
UserIds         : {User1@sk200628outlook.onmicrosoft.com}
RetentionDuration : SixMonths

Name           : Retention3
Priority        : 100
RecordTypes     : {}
Operations      : {}
UserIds         : {User2@sk200628outlook.onmicrosoft.com}
RetentionDuration : TwelveMonths

PS C:\>
    
```

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 User1 creates a team in Microsoft Teams, the event is [answer choice]

If User2 adds a channel in Microsoft Teams, the event is [answer choice]

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

If User1 creates a team in Microsoft Teams, the event is [answer choice]

If User2 adds a channel in Microsoft Teams, the event is [answer choice]

**NEW QUESTION 138**

- (Topic 6)

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.

Your network contains an Active Directory forest. You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

- A. Yes
- B. No

Answer: B

**NEW QUESTION 141**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.

Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Device1	Android	User1	Yes
Device2	Android	User1	No
Device3	iOS	User1	No
Device4	Windows 10	User2	Yes
Device5	Windows 10	User2	No
Device6	iOS	User2	Yes

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

- A. Device1, Device4, and Device6
- B. Device2, Device3, and Device5
- C. Device1, Device2, Device3, and Device6
- D. Device1, Device2, Device4, and Device5

**Answer:** C

**Explanation:**

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

**NEW QUESTION 143**

HOTSPOT - (Topic 6)

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

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

At 08:00. you create an incident notification rule that has the following configurations:

- Name: Notification!
- Notification settings
  - o Notify on alert severity: Low
  - o Device group scope: All (3)
  - o Details: First notification per incident
- Recipients: User1@contoso.com, User2@contoso.com

At 08:02. you create an incident notification rule that has the following configurations:

- Name: Notification
- Notification settings
  - o Notify on alert severity: Low. Medium
  - o Device group scope: DeviceGroup1, DeviceGroup2
- Recipients: User1@contoso.com

in Microsoft 365 Defender, alerts are logged as shown in the following table.

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

For each of the following statements, select Yes if the statement is true. Otherwise, select No1.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input checked="" type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input checked="" type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 147**

DRAG DROP - (Topic 6)

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

Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune-managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must minimize administrative effort.

What should you use to onboard each type of device? To answer, drag the appropriate onboarding methods to the correct device types. Each onboarding method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Onboarding method**

- A local script
- Group Policy
- Integration with Microsoft Defender for Cloud
- Microsoft Intune
- Virtual Desktop Infrastructure (VDI) scripts

**Device Type**

Corporate:

BYOD:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Onboarding method**

- A local script
- Group Policy
- Integration with Microsoft Defender for Cloud
- Microsoft Intune
- Virtual Desktop Infrastructure (VDI) scripts

**Device Type**

Corporate: Microsoft Intune

BYOD: Integration with Microsoft Defender for Cloud

**NEW QUESTION 152**

- (Topic 6)

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.

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: You run idfix.exe and export the 10 user accounts.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

The question states that "all the user account synchronizations completed successfully". If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.

It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

**NEW QUESTION 153**

HOTSPOT - (Topic 6)

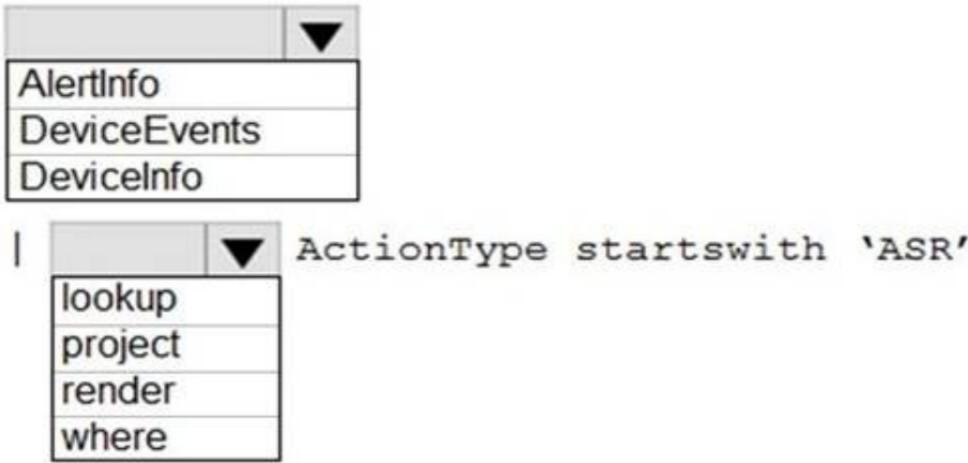
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.

You need to find the ASR rules that match the activities on the devices.

How should you complete the Kusto query? To answer, select the appropriate options in the answer area.

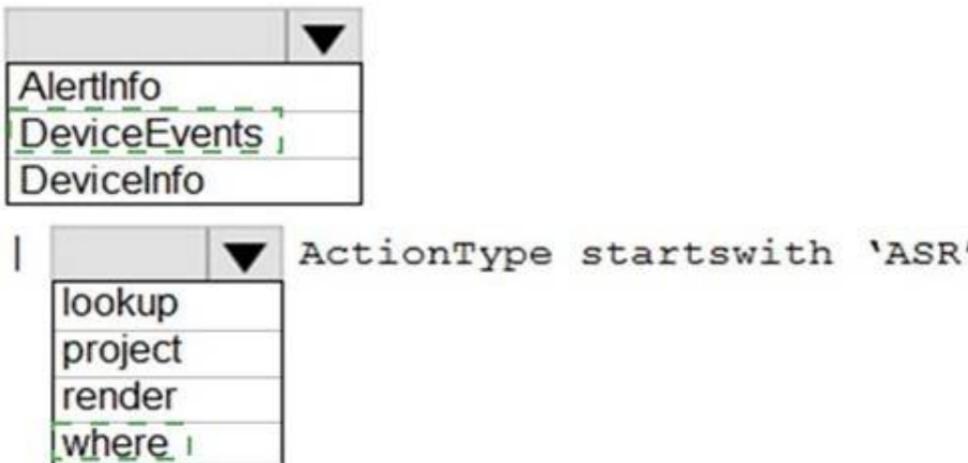
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 156**

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.

**Domains**

+ Add domain Buy domain Refresh		
Domain name ↑	Status	Choose columns
<input type="checkbox"/> contoso221018.onmicrosoft.com (Default)	Healthy	
<input type="checkbox"/> contoso.com	Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	No services selected	

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**

An administrator can create usernames that contain the [answer choice].

Exchange Online can receive inbound email messages sent to the [answer choice].

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

An administrator can create usernames that contain the [answer choice].

Exchange Online can receive inbound email messages sent to the [answer choice].

**NEW QUESTION 158**

- (Topic 6)

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft Intune. You plan to use Endpoint analytics to identify hardware issues. You need to enable Windows health monitoring on the devices to support Endpoint analytics. What should you do?

- A. Configure the Endpoint analytics baseline regression threshold.
- B. Create a configuration profile.
- C. Create a Windows 10 Security Baseline profile
- D. Create a compliance policy.

**Answer: B**

**NEW QUESTION 160**

- (Topic 6)

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels | Label policies | Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label | Publish labels | Refresh

Name	Order	Created by	Last modified
Label1	0 - highest	Pvi	04/24/2020
Label2	1	Pvi	04/24/2020
Label3	0 - highest	Pvi	04/24/2020
Label4	0 - highest	Pvi	04/24/2020
Label5	5	Pvi	04/24/2020
Label6	0 - highest	Pvi	04/24/2020

Which labels can users apply to content?

- A. Label1, Label2, and Label5 only
- B. Label3, Label4, and Label6 only
- C. Label1, Label3, Label2, and Label6 only
- D. Label1, Label2, Label3, Label4, Label5, and Label6

**Answer: C**

**NEW QUESTION 165**

- (Topic 6)

You have the sensitivity labels shown in the following exhibit.

Home > sensitivity

**Labels**

Label policies

Auto-labeling(preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label    Publish labels    Refresh

Name ↑	Order	Created by	Last modified
Label1	0-highest	Pri	04/24/2020
- Label2	1	Pri	04/24/2020
Label3	0-highest	Pri	04/24/2020
Label4	0-highest	Pri	04/24/2020
- Label5	5	Pri	04/24/2020
Label6	0-highest	Pri	04/24/2020

Which labels can users apply to content?

- A. Label3, Label4, and Label6 only
- B. Label1, Label2, Label3, Label4, Label5, and Label6
- C. Label1, Label2, and Label5 only
- D. Label1, Label3, Label4, and Label6 only

**Answer:** D

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

**NEW QUESTION 166**

HOTSPOT - (Topic 6)

Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 device group

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
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 167**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:

- Create a sensitive info type named SIT1 based on a regular expression.
- Add a watermark to all new documents that are matched by SIT1.

Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



**NEW QUESTION 169**

FILL IN THE BLANK - (Topic 6)

You have a Microsoft 365 tenant.

You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.

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

Answer Area

Save the audit logs to:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Save the audit logs to:

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

**NEW QUESTION 174**

- (Topic 6)

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

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

You have a Microsoft 365 subscription.

From the Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**NEW QUESTION 175**

- (Topic 6)

You have a Microsoft 365 E5 tenant. Users store data in the following locations:

- ? Microsoft Teams
- ? Microsoft OneDrive
- ? Microsoft Exchange Online
- ? Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.

What is the minimum number of retention policies that you should create?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: C**

**Explanation:**

Reference:

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

**NEW QUESTION 176**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table.

You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	None	Default

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Device 1:

No profiles
Profile1 only
Profile4 only
Profile1 and Profile4 only
Profile1, Profile1, and Profile4 only

Device 2:

No profiles
Profile1 only
Profile2 only
Profile3 only
Profile1 and Profile2 only
Profile2 and Profile3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1:

No profiles
Profile1 only
Profile4 only
Profile1 and Profile4 only
Profile1, Profile1, and Profile4 only

Device 2:

No profiles
Profile1 only
Profile2 only
Profile3 only
Profile1 and Profile2 only
Profile2 and Profile3 only

**NEW QUESTION 178**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint. You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

- A. a Microsoft Defender for Endpoint baseline profile
- B. an update policy for iOS
- C. a device configuration profile
- D. a mobile device management (MDM) security baseline profile

Answer: D

**NEW QUESTION 179**

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

- Use a file plan to manage retention labels.
- Identify, monitor, and automatically protect sensitive information.
- Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Solutions	Answer Area
Data loss prevention	Identify, monitor, and automatically protect sensitive information:
Information governance	Capture employee communications for examination by designated reviewers:
Insider risk management	Use a file plan to manage retention labels:
Records management	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Solutions	Answer Area
Data loss prevention	Identify, monitor, and automatically protect sensitive information: Data loss prevention
Information governance	Capture employee communications for examination by designated reviewers: Insider risk management
Insider risk management	Use a file plan to manage retention labels: Information governance
Records management	

**NEW QUESTION 181**

HOTSPOT - (Topic 6)

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Android devices in Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can enroll iOS devices in Endpoint Manager.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 186**

HOTSPOT - (Topic 6)

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

? Assignments: All users

? Controls: Require Azure AD multifactor authentication registration

? Enforce Policy: On

? On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:

▼

- August 6
- August 17
- August 19
- September 3
- September 5

User2:

▼

- August 8
- August 17
- August 19
- August 21
- September 7

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: August 19

Note: Security defaults will trigger a 14 day grace period for registration after a user's first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.

Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period. Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi- Factor Authentication, then the user must be able to pass that MFA request.

Box 2: August 21

**NEW QUESTION 191**

**HOTSPOT - (Topic 6)**

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1. What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

Action:

- Add User1 to the subscription as an active user.
- For Group1, change the Privacy setting to Public.
- For Group1, select Allow external senders to email this group.
- Invite User1 to collaborate with your organization as a guest.

Portal:

- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Invite User1 to collaborate with your organization as a guest.

To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.

Navigate with your Web browser to <https://admin.microsoft.com>. On the left pane, click on "Users", then click "Guest Users".

On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at <https://aad.portal.azure.com>.

On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain.dot.com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.

Box 2: The Microsoft Entra admin center

Microsoft Entra admin center unites Azure AD with family of identity and access products

Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).

**NEW QUESTION 195**

HOTSPOT - (Topic 6)

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

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
  - Priority: 0
  - Include these users, groups and domains
    - o Users: User3
    - o Groups: Group1
  - Exclude these users, groups and domains
    - o Groups: Group2
  - Message limits
    - o Set a daily message limit 100
- Name: AntiSpam2
  - Priority: 1
  - Include these users, groups and domains
    - o Users: User1
    - o Groups: Group2
  - Exclude these users, groups and domains
    - o Users: User3
  - Message limits
    - o Set a daily message limit 50

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 200**

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You need to access service health alerts from a mobile phone.

What should you use?

- A. the Microsoft Authenticator app
- B. the Microsoft 365 Admin mobile app
- C. Intune Company Portal
- D. the Intune app

**Answer:** B

**NEW QUESTION 202**

HOTSPOT - (Topic 6)

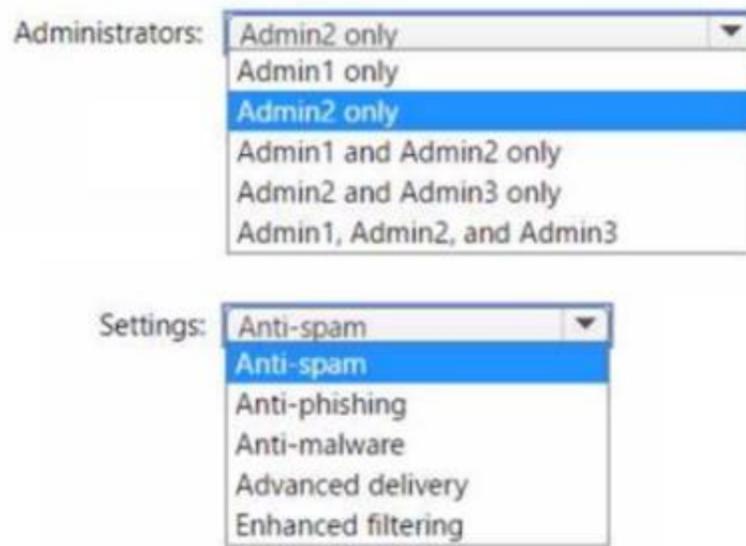
You have a Microsoft 365 E5 subscription that contains a user named User1 and the administrators shown in the following table.

User1 reports that after sending 1,000 email messages in the morning, the user is blocked from sending additional emails. You need to identify the following:

- Which administrators can unblock User1
- What to configure to allow User1 to send at least 2,000 emails per day without being blocked

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

**Answer Area**

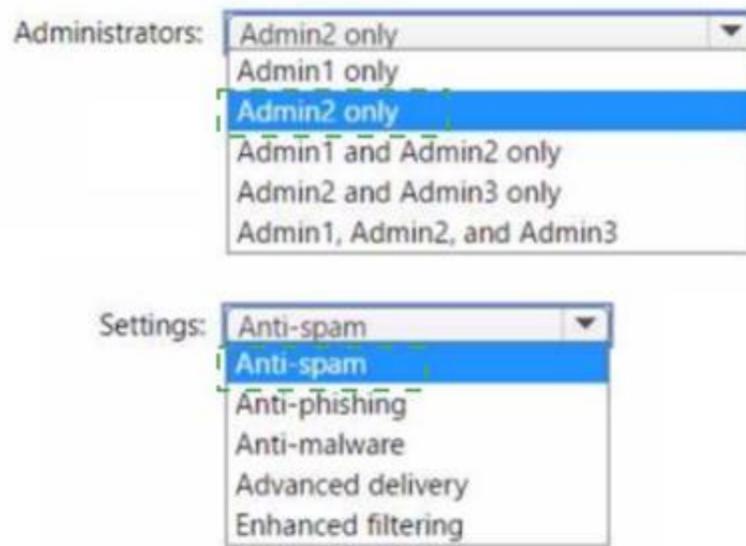


- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**



**NEW QUESTION 206**

- (Topic 6)

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

- A. Enable auditing.
- B. Enable Microsoft 365 usage analytics.
- C. Create an Insider risk management policy.
- D. Create a communication compliance policy.

**Answer:** A

**Explanation:**

Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Note: Permissions alert policies

Example: Elevation of Exchange admin privilege

Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview> <https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

**NEW QUESTION 207**

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.

Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com.

You plan to install Azure AD Connect on a member server and implement pass-through authentication.

You need to prepare the environment for the planned implementation of pass-through authentication.

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

NOTE: Each correct selection is worth one point.

- A. From a domain controller install an Authentication Agent
- B. From the Microsoft Entra admin center, configure an authentication method.
- C. From Active Directory, Domains and Trusts add a UPN suffix
- D. Modify the email address attribute for each user account.
- E. From the Microsoft Entra admin center, add a custom domain name.
- F. Modify the User logon name for each user account.

**Answer:** ABE

**Explanation:**

Deploy Azure AD Pass-through Authentication Step 1: Check the prerequisites

Ensure that the following prerequisites are in place. In the Entra admin center

\* 1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.

(E) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.

(A) In your on-premises environment

\* 1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.

\* 2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is supported.

\* 3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.

\* 4. Etc.

(B) Step 2: Enable the feature

Enable Pass-through Authentication through Azure AD Connect.

If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.

Incorrect:

Not C: From Active Directory Domains and Trusts, add a UPN suffix Not D. Modify the email address attribute for each user account. Not F. Modify the User logon name for each user account.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start>

**NEW QUESTION 212**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that contain

Personally Identifiable Information (PII). Report on shared documents that contain PII. What should you create?

- A. a data loss prevention (DLP) policy
- B. a retention policy
- C. an alert policy
- D. a Microsoft Defender for Cloud Apps policy

**Answer:** A

**Explanation:**

Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

? From the Security & Compliance tab of your browser, click Home.

? Click Data loss prevention > Policy.

? Click + Create a policy.

? In Start with a template or create a custom policy, click Custom > Custom policy > Next.

? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens

? Etc.

Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment>

**NEW QUESTION 213**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.

You need to implement passwordless authentication. The solution must support all the devices.

Which authentication method should you use?

- A. Windows Hello
- B. FIDO2 compliant security keys
- C. Microsoft Authenticator app

Answer: C

**NEW QUESTION 218**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription. You need to meet the following requirements:

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance portal? To answer,

select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**



- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection

All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files

without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.

To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:

In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.

Note: Encryption of data at rest

Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.

BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology. Box 2: Settings

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

- \* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
- \* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
- \* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
- \* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
- \* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

**NEW QUESTION 219**

- (Topic 6)

You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that User1 can place a hold on all mailbox content. What permission should you assign to User1?

- A. the Information Protection administrator role from the Azure Active Directory admin center.
- B. the eDiscovery Manager role from the Microsoft 365 compliance center.
- C. the Compliance Management role from the Exchange admin center.
- D. the User management administrator role from the Microsoft 365 admin center.

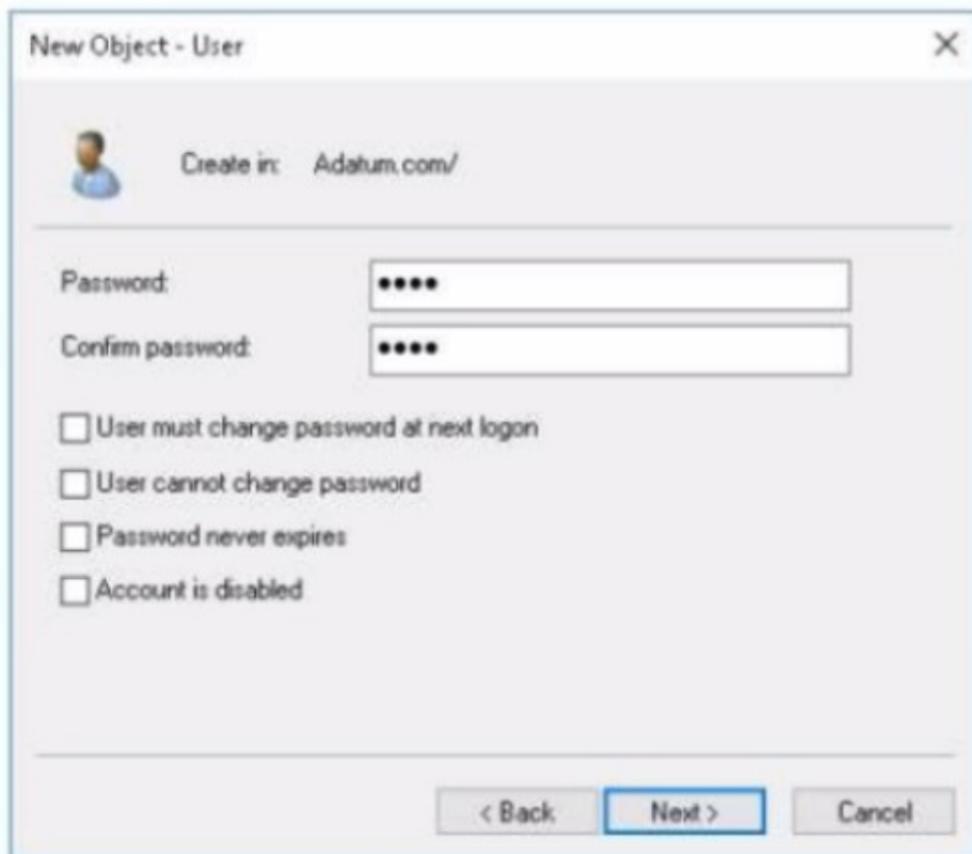
**Answer: B**

**NEW QUESTION 221**

HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password write back is disabled.

You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



The Azure AD password policy is configured as shown in the following exhibit. Password policy

Set the password policy for all users in your organization. Days before passwords expire 90

Days before a user is notified about 14 expiration

You confirm that User1 is synced to Azure AD.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can sign in to Azure AD.	<input type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Statements	Yes	No
User1 can sign in to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 222**

HOTSPOT - (Topic 6)

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self- service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:  Phone number and email address  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

User2:  Phone number and email address  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

User3:  Security questions only  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

User1:  Phone number and email address  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

User2:  Phone number and email address  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

User3:  Security questions only  
 Email address only  
 Phone number only  
 Security questions only  
 Phone number and email address

**NEW QUESTION 223**

- (Topic 6)

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso. The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**NEW QUESTION 228**

- (Topic 6)

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

- A. Device 1, Device2, and Device3 only
- B. Device3 only
- C. Device2 and Device3 only
- D. Device1, Device2, Devices and Device4

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements>

**NEW QUESTION 232**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

The Microsoft Secure Score for the tenant is shown in the following exhibit.

**Microsoft Secure Score**

Overview Improvement actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

↓ Export 12 items 🔍 Search ⌵ Filter ☰ Group by ▾

Applied filters:

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for...	+15.25%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	+1.69%	0/1

You plan to enable Security defaults for Azure Active Directory (Azure AD). Which three improvement actions will this affect?

- A. Require MFA for administrative roles.

- B. Ensure all users can complete multi-factor authentication for secure access
- C. Enable policy to block legacy authentication
- D. Enable self-service password reset
- E. Use limited administrative roles

**Answer:** ABC

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

**NEW QUESTION 235**

HOTSPOT - (Topic 6)

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.

In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

**Device limit restrictions**

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.

Users may register their devices with Azure AD ⓘ

All  None

[Learn more on how this setting works](#)

Require Multi-Factor Auth to join devices ⓘ

Yes  No

Maximum number of devices per user ⓘ

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
User1 can enroll only five devices in Intune.	<input type="radio"/>	<input type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 can enroll all the devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Statements	Yes	No
User1 can enroll only five devices in Intune.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll all the devices in Intune.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 240**

- (Topic 6)

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics. Which devices can you monitor by using Endpoint analytics?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

**NEW QUESTION 244**

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	None	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	None	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
App3 can be installed automatically for UserGroup1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input checked="" type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input checked="" type="radio"/>
App3 can be installed automatically for UserGroup1.	<input checked="" type="radio"/>	<input type="radio"/>

**NEW QUESTION 248**

- (Topic 6)

You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

- A. 3
- B. 5
- C. 4
- D. 1

**Answer: D**

**NEW QUESTION 250**

HOTSPOT - (Topic 5)

You are evaluating the use of multi-factor authentication (MFA).

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
Users will have 14 days to register for MFA after they sign in for the first time.	<input type="radio"/>	<input type="radio"/>
Users must use the Microsoft Authenticator app to complete MFA.	<input type="radio"/>	<input type="radio"/>
After registering, users must use MFA for every sign-in.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	<input checked="" type="radio"/>	<input type="radio"/>
Users must use the Microsoft Authenticator app to complete MFA.	<input checked="" type="radio"/>	<input type="radio"/>
After registering, users must use MFA for every sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 255**

- (Topic 5)

You need to configure just in time access to meet the technical requirements. What should you use?

- A. entitlement management
- B. Azure AD Privileged Identity Management (PIM)
- C. access reviews
- D. Azure AD Identity Protection

**Answer:** B

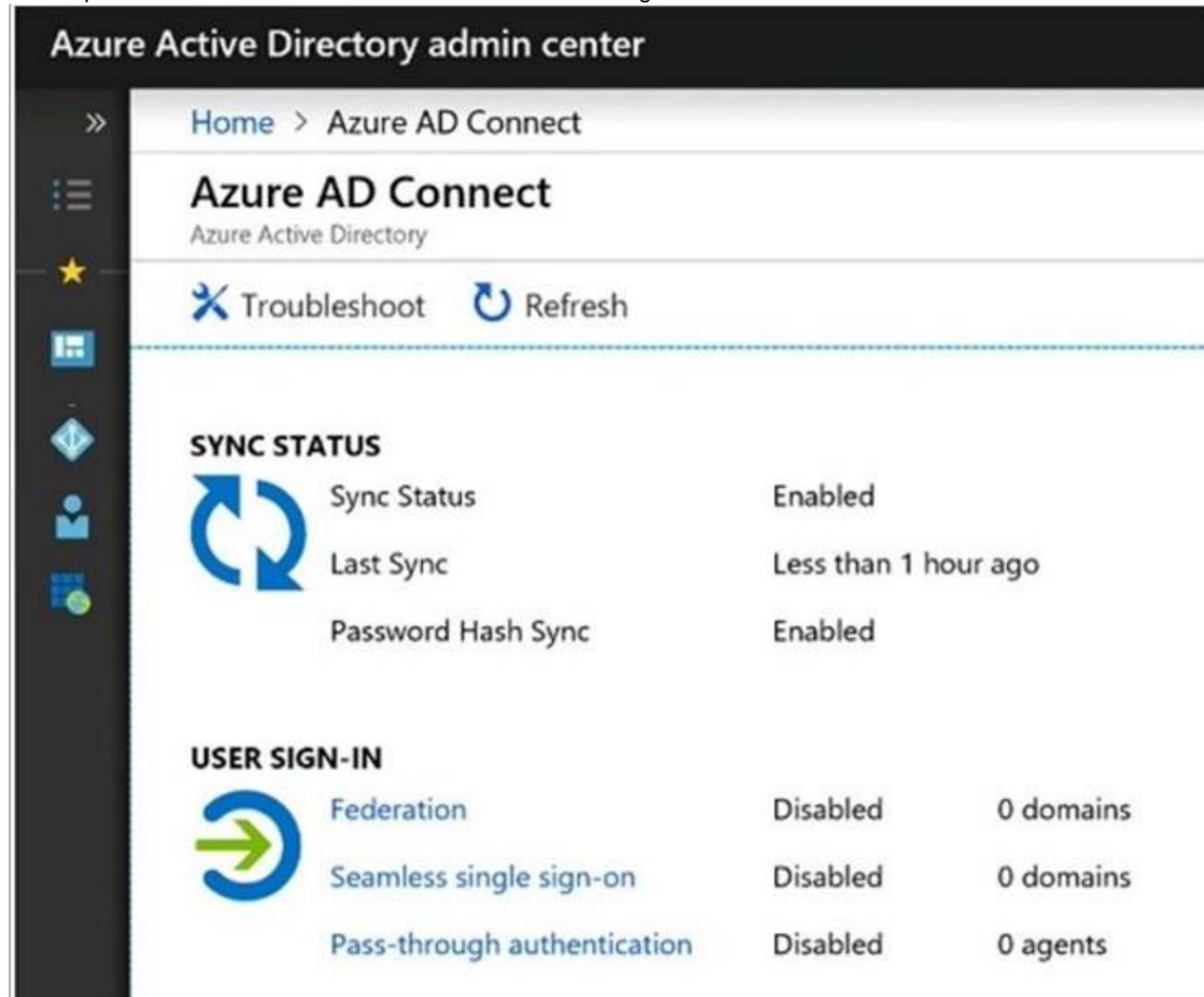
**NEW QUESTION 259**

HOTSPOT - (Topic 4)

HOTSPOT

You create the Microsoft 365 tenant.

You implement 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**

During Project1, sales department users can access [answer choice] applications by using SSO.

Dropdown menu options:
 

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

Dropdown menu options:
 

- both on-premises and in the cloud
- in the cloud only
- on-premises only

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: only on-premises

In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.

In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Azure Active Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active Directory. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.

Box 2: in the cloud only

**NEW QUESTION 260**

- (Topic 4)

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

- A. host (A)
- B. host information
- C. text (TXT)
- D. alias (CNAME)

**Answer: D**

**Explanation:**

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

Text (TXT)

Mail exchanger (MX)

incorrect answer options you may see on the exam include the following: alias (CNAME)

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

<https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider>

**NEW QUESTION 263**

- (Topic 4)

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.

Which authentication strategy should you implement for the pilot projects?

- A. pass-through authentication
- B. pass-through authentication and seamless SSO
- C. password hash synchronization and seamless SSO
- D. password hash synchronization

**Answer: C**

**Explanation:**

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.

Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

Fabrikam does NOT plan to implement identity federation.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

**NEW QUESTION 264**

- (Topic 3)

You need to configure Office on the web to meet the technical requirements. What should you do?

- A. Assign the Global reader role to User1.
- B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
- C. Configure an auto-labeling policy to apply the sensitivity labels.
- D. Assign the Office apps admin role to User1.

**Answer: B**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide>

**NEW QUESTION 267**

HOTSPOT - (Topic 3)

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.

What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure:  ▼

Device configuration profiles
Enrollment restrictions
The mobile device management (MDM) user scope
The mobile application management (MAM) user scope

Group:  ▼

UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Configure:  ▼

Device configuration profiles
Enrollment restrictions
The mobile device management (MDM) user scope
The mobile application management (MAM) user scope

Group:  ▼

UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

**NEW QUESTION 269**

- (Topic 3)

You need to create the Safe Attachments policy to meet the technical requirements. Which option should you select?

- A. Replace
- B. Enable redirect
- C. Block
- D. Dynamic Delivery

Answer: D

Explanation:

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md>

**NEW QUESTION 274**

HOTSPOT - (Topic 2)

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Minimum number of data sources:  ▼

1
3
6

Minimum number of log collectors:  ▼

1
3
6

- A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker>

**NEW QUESTION 275**

HOTSPOT - (Topic 2)

You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

From the Security & Compliance admin center, perform a search by using:

Audit log
Data governance events
DLP policy matches
eDiscovery

Filter by:

Activity
Detail
Item
User agent

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results>

**NEW QUESTION 277**

- (Topic 1)

On which server should you use the Defender for identity sensor?

- A. Server1
- B. Server2
- C. Server3
- D. Server4
- E. Servers5

**Answer:** A

**Explanation:**

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

**NEW QUESTION 281**

- (Topic 2)

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

**Answer:** C

**Explanation:**

References:

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

This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

**NEW QUESTION 284**

- (Topic 2)

You need to protect the U.S. PII data to meet the technical requirements. What should you create?

- A. a data loss prevention (DLP) policy that contains a domain exception
- B. a Security & Compliance retention policy that detects content containing sensitive data

- C. a Security & Compliance alert policy that contains an activity
- D. a data loss prevention (DLP) policy that contains a user override

**Answer:** A

**NEW QUESTION 285**

- (Topic 1)

On which server should you install the Azure ATP sensor?

- A. Server 1
- B. Server 2
- C. Server 3
- D. Server 4
- E. Server 5

**Answer:** A

**Explanation:**

References:

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

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

**NEW QUESTION 287**

HOTSPOT - (Topic 1)

You need to meet the Intune requirements for the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

▼
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

▼
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/intune/windows-enroll>

**NEW QUESTION 291**

- (Topic 1)

You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

- A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- C. From the Intune admin center, add User1 as a device enrollment manager.
- D. From the Intune admin center, configure the Enrollment restrictions.

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

**NEW QUESTION 296**

- (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named site1. You need to ensure that site1 meets the following requirements:

- Retains all data for 10 years
- Prevents the sharing of data outside the organization

Which two items should you create and apply to site1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. a retention policy

- B. a sensitive info type
- C. a data loss prevention (DLP) policy
- D. a sensitivity label
- E. a retention label
- F. a retention label policy

**Answer:** CE

**NEW QUESTION 301**

DRAG DROP - (Topic 6)

You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune. You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices. Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions		Answer Area
Create an app configuration policy		
Link the account to Intune		
Create a Microsoft account	➤	⬆
Configure a mobile device management (MDM) push certificate	⬅	⬇
Add the app		
Create a Google account		
Assign the app		

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Actions		Answer Area
Create an app configuration policy		Create a Google account
Link the account to Intune		
Create a Microsoft account	➤	Link the account to Intune
Configure a mobile device management (MDM) push certificate	⬅	Add the app
Add the app		
Create a Google account		Assign the app
Assign the app		

**NEW QUESTION 305**

- (Topic 6)

You have a Microsoft 365 E5 subscription. You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event. You need to reduce false positives for impossible travel when the users sign in from the corporate network. What should you configure?

- A. exclusion groups
- B. multi-factor authentication (MFA)
- C. named locations

D. user risk policies

**Answer: C**

**NEW QUESTION 308**

- (Topic 6)

You have a Microsoft 365 E5 tenant.

You plan to deploy a monitoring solution that meets the following requirements:

? Captures Microsoft Teams channel messages that contain threatening or violent language.

? Alerts a reviewer when a threatening or violent message is identified.

What should you include in the solution?

- A. Data Subject Requests (DSRs)
- B. Insider risk management policies
- C. Communication compliance policies
- D. Audit log retention policies

**Answer: C**

**NEW QUESTION 313**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to create Conditional Access policies to meet the following requirements:

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must be blocked from signing in from outside the United States and Canada.

Only users in the R&D department must be blocked from signing in from both Android and iOS devices.

Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

What is the minimum number of Conditional Access policies you should create?

- A. 3
- B. 4
- C. 5
- D. 6
- E. 7
- F. 8

**Answer: B**

**Explanation:**

\* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.

One Policy.

\* Only users in the R&D department must be blocked from signing in from both Android and iOS devices.

One Policy.

\* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.

All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.

One policy

\* All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android One Policy

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>

**NEW QUESTION 317**

- (Topic 6)

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select System, and then you select About to view information about the system.

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

**Explanation:**

Reference:

<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808>

**NEW QUESTION 322**

HOTSPOT - (Topic 6)

You have Microsoft 365 subscription.

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

## Policy1

[Edit policy](#) [Delete policy](#)

Status  On

### Name your alert

Description: Add a description  
 Severity:  Low  
 Category: Threat management  
 Policy contains tags: -

### Create alert settings

Conditions: Activity is FileMalwareDetected  
 Aggregation: Aggregated  
 Scope: All users  
 Threshold: 20  
 Window: 2 hours  
 Severity:  Low

### Set your recipients

Recipients: User1@sk220912outlook.onmicrosoft.com  
 Daily notification limit: 100

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**

Policy1 will trigger an alert if malware is detected in [answer choice].

SharePoint or OneDrive only  
 Exchange Online only  
 SharePoint only  
 SharePoint or OneDrive only  
 Exchange Online, SharePoint, or OneDrive

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5  
 5  
 12  
 20  
 100

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Answer Area**

Policy1 will trigger an alert if malware is detected in [answer choice].

SharePoint or OneDrive only  
 Exchange Online only  
 SharePoint only  
**SharePoint or OneDrive only**  
 Exchange Online, SharePoint, or OneDrive

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5  
**5**  
 12  
 20  
 100

**NEW QUESTION 327**

- (Topic 6)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to ensure that users can select a department when they enroll their device in Intune. What should you create?

- A. scope tags
- B. device configuration profiles
- C. device categories
- D. device compliance policies

**Answer: C**

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

**NEW QUESTION 332**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant. You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege. Which type of policy should you create and which Microsoft 365 compliance center role is required to create the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Policy type:  
 Alert  
 Threat  
 Compliance

Role:  
 Quarantine  
 Security Administrator  
 Organization Configuration  
 Communication Compliance Admin

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Policy type:  
 Alert  
 Threat  
 Compliance

Role:  
 Quarantine  
**Security Administrator**  
 Organization Configuration  
 Communication Compliance Admin

**NEW QUESTION 336**

- (Topic 6)

Your network contains an Active Directory forest named contoso.local. You purchase a Microsoft 365 subscription. You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months. You need to prepare for the planned move to Microsoft 365. What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Purchase a third-party X.509 certificate.

- B. Create an external forest trust.
- C. Rename the Active Directory forest.
- D. Purchase a custom domain name.

**Answer:** D

**Explanation:**

The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on-premise Active Directory if it's a routable domain name, for example, contoso.com.

If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.

Incorrect:

Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization>

**NEW QUESTION 339**

- (Topic 6)

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do first?

- A. From the Exchange admin center create a mail flow rule.
- B. From Microsoft 365 Defender, start a message trace.
- C. From Microsoft Defender for Cloud Apps, create an activity policy.
- D. From the Microsoft Purview compliance portal, create a label and a label policy.

**Answer:** D

**NEW QUESTION 343**

- (Topic 6)

You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.

You purchase 100 Microsoft 365 Business Voice add-on licenses.

You need to ensure that the members of a group named Voice are assigned a Microsoft 365 Business Voice add-on license automatically.

What should you do?

- A. From the Microsoft 365 admin center, modify the settings of the Voice group.
- B. From the Licenses page of the Microsoft 365 admin center, assign the licenses.
- C. From the Microsoft Entra admin center, modify the settings of the Voice group.

**Answer:** C

**NEW QUESTION 348**

- (Topic 6)

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You need to configure Microsoft Defender ATP on the computers. What should you create from the Endpoint Management admin center?

- A. a device configuration profile
- B. an update policy for iOS
- C. a Microsoft Defender ATP baseline profile
- D. a mobile device management (MDM) security baseline profile

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 352**

- (Topic 6)

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

Corporate policy states that user passwords must not include the word Contoso. What should you do to implement the corporate policy?

- A. From Azure AD Identity Protection, configure a sign-in risk policy.
- B. From the Microsoft Entra admin center, create a conditional access policy.
- C. From the Microsoft 365 admin center, configure the Password policy settings.
- D. From the Microsoft Entra admin center, configure the Password protection settings.

**Answer:** D

**NEW QUESTION 353**

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription.

You need to create two groups named Group1 and Group2. The solution must meet the following requirements:

- Group1 must be mail-enabled and have an associated Microsoft SharePoint Online site.
  - Group2 must support dynamic membership and role assignments but must NOT be mail-enabled.
- Which types of groups should you create? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Group1: 

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

Group2: 

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Group1: 

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

Group2: 

- Distribution
- Dynamic distribution
- Microsoft 365
- Security

**NEW QUESTION 355**

- (Topic 6)

You have a Microsoft 365 subscription.

You need to identify which administrative users performed eDiscovery searches during the past week.

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

- A. Perform a content search
- B. Create a supervision policy
- C. Create an eDiscovery case
- D. Perform an audit log search

**Answer:** D

**NEW QUESTION 357**

- (Topic 6)

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

Name	Type
Label1	Sensitivity
Label2	Retention

You have the items shown in the following table.

Name	Stored in	Description
File1	Microsoft SharePoint	File document that has Label1 applied
File2	Microsoft Teams channel	File document that has Label2 applied
Mail1	Microsoft Exchange Online	Email message that has Label1 applied
Mail2	Microsoft Exchange Online	Email message that has Label2 applied

Which items can you view in Content explorer?

- A. File1 only
- B. File1 and File2 only
- C. File1 and Mail! only

- D. File2 and Mail2 only
- E. File1, File2, Mail1, and Mail2

**Answer: C**

**NEW QUESTION 362**

HOTSPOT - (Topic 6)  
 HOTSPOT

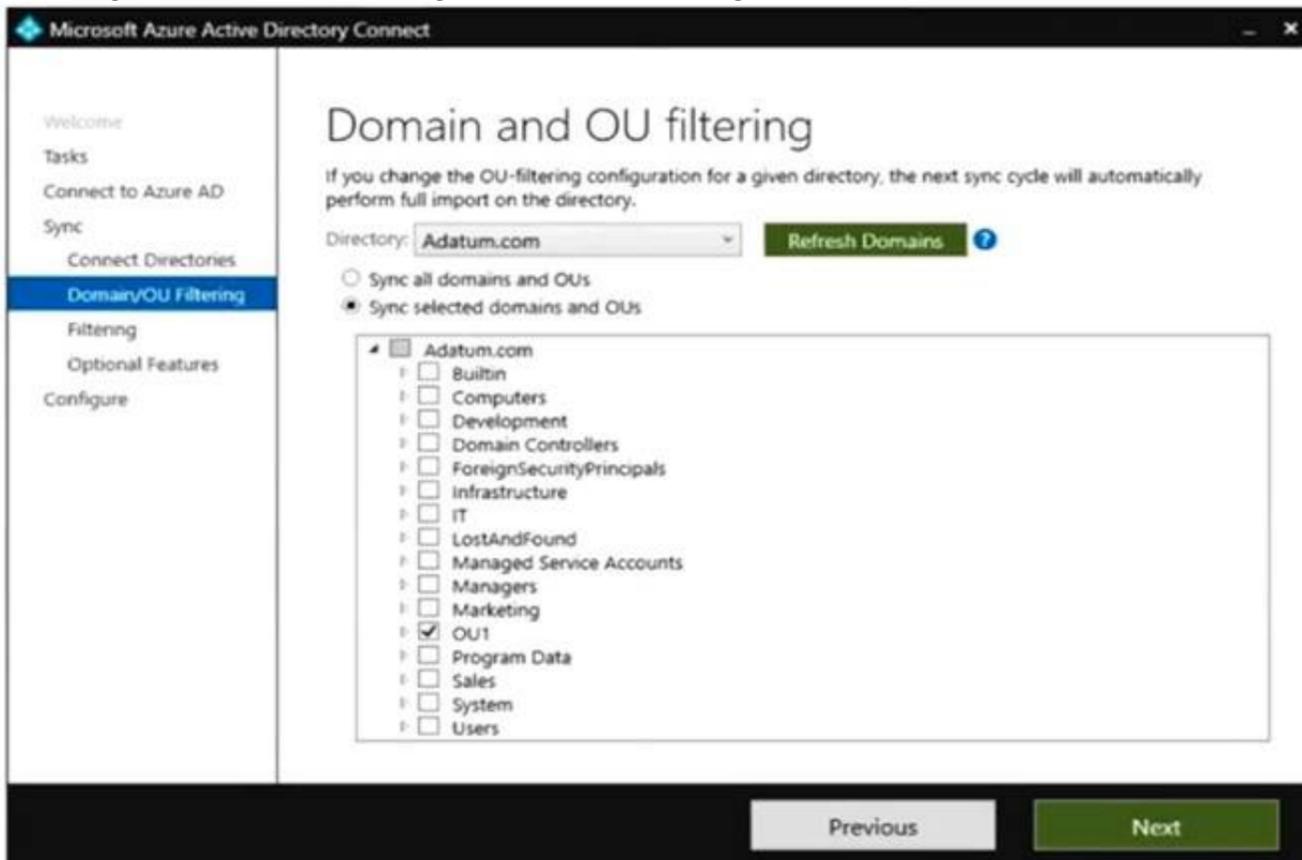
Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription. The domain contains the users shown in the following table.

Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.

Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect. You configure Domain and OU filtering as shown in the following exhibit.



You configure Filter users and devices as shown in the following exhibit.



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

**Answer Area**

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User2 syncs to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>
Group2 syncs to Azure AD.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Answer Area**

Statements	Yes	No
User1 syncs to Azure AD.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User2 syncs to Azure AD.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group2 syncs to Azure AD.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**NEW QUESTION 366**

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You have an Azure AD tenant named contoso.com that contains the following users:

- Admin1
- Admin2
- User1

Contoso.com contains an administrative unit named AIM that has no role assignments. User1 is a member of AU1. You create an administrative unit named AU2 that does NOT have any members or role assignments. 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
You can add Admin1 as a member of AU1.	<input type="radio"/>	<input type="radio"/>
You can add User1 as a member of AU2.	<input type="radio"/>	<input type="radio"/>
You can assign Admin2 the User administrator role for AU1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

You can add Admin1 as a member of AU1.

Yes

No

You can add User1 as a member of AU2.

You can assign Admin2 the User administrator role for AU1.

NEW QUESTION 367

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions and Answers in PDF Format

### **MS-102 Practice Exam Features:**

- \* MS-102 Questions and Answers Updated Frequently
- \* MS-102 Practice Questions Verified by Expert Senior Certified Staff
- \* MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The MS-102 Practice Test Here](#)**