

# Exam Questions MS-102

Microsoft 365 Administrator Exam

<https://www.2passeasy.com/dumps/MS-102/>



### NEW QUESTION 1

- (Exam 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 2

- (Exam Topic 1)

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

- A. 1
- B. 4
- C. 7
- D. 31

**Answer: B**

#### Explanation:

References:

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

### NEW QUESTION 3

- (Exam Topic 1)

You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

New	Conditions	Device state (preview)
<p><b>Info</b></p> <p>Name: Policy1 ✓</p> <p><b>Assignments</b></p> <p>Users and groups: 0 users and groups selected</p> <p>Cloud apps: 1 app included</p> <p>Conditions: 0 conditions selected</p> <p><b>Access controls</b></p> <p>Grant: Block access</p> <p>Session: 0 controls selected</p> <p><b>Enable policy</b></p> <p>On Off</p>	<p><b>Info</b></p> <p>Sign-in risk: Not configured</p> <p>Device platforms: Not configured</p> <p>Locations: Not configured</p> <p>Client apps (preview): Not configured</p> <p>Device state (preview): Not configured</p>	<p><b>Info</b></p> <p>Configure: Yes No</p> <p>Include Exclude</p> <p>Select the device state condition used to exclude devices from policy.</p> <p><input type="checkbox"/> Device Hybrid Azure AD joined</p> <p><input type="checkbox"/> Device marked as compliant</p>

- A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

Suggested Answer

References: <https://docs.microsoft.com/en-us/intune/create-conditional-access-intune>

**NEW QUESTION 4**

- (Exam Topic 2)

You need to meet the technical requirement for the EU PII data. What should you create?

- A. a retention policy from the Security & Compliance admin center.
- B. a retention policy from the Exchange admin center
- C. a data loss prevention (DLP) policy from the Exchange admin center
- D. a data loss prevention (DLP) policy from the Security & Compliance admin center

**Answer:** A

**Explanation:**

References:

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

EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

**NEW QUESTION 5**

- (Exam 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 6**

- (Exam 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 7**

- (Exam Topic 3)

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements. To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role group:

▼
Reviewer
Global reader
Data Investigator
Compliance Management

Tool:

▼
Exchange admin center
SharePoint admin center
Microsoft 365 admin center
Microsoft 365 security center

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?vi>

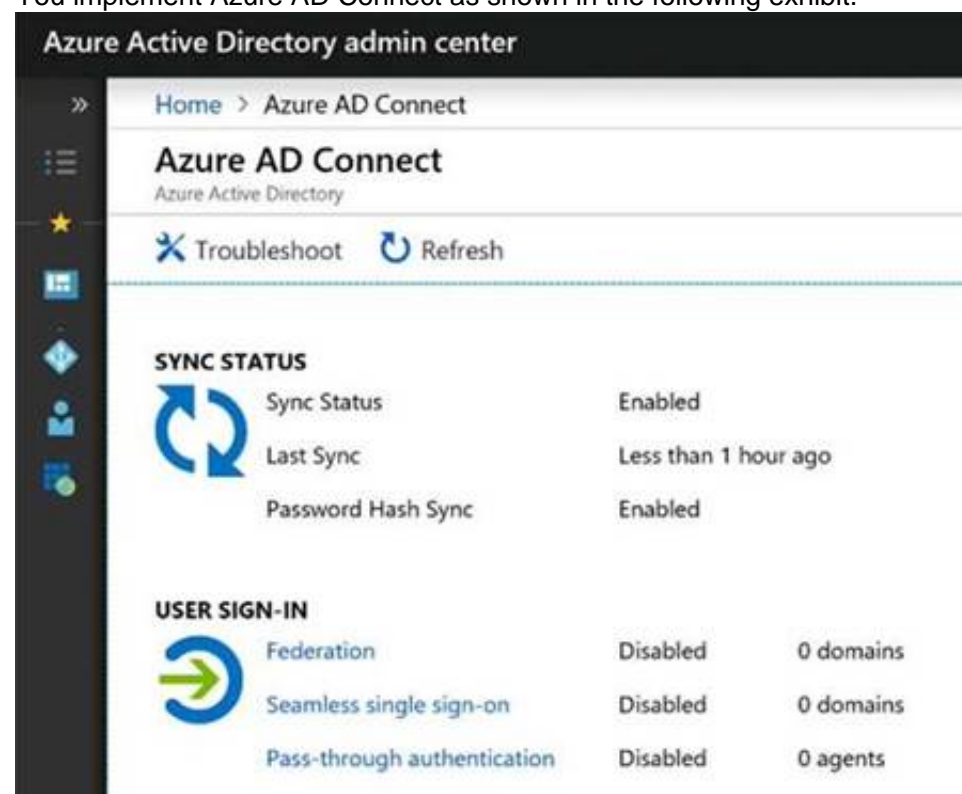
**NEW QUESTION 8**

- (Exam 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.

▼
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].

▼
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 9

- (Exam 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. pointer (PTR)

**Answer:** A

#### 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>

#### NEW QUESTION 10

- (Exam 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 10

- (Exam Topic 5)

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 11

- (Exam Topic 5)

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 12

- (Exam Topic 5)

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 named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD. Solution: From the on-premises Active Directory domain, you assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

This is not a permissions issue. The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

NEW QUESTION 17

- (Exam Topic 5)  
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 22

- (Exam Topic 5)  
You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. A user named User1 stores documents in Microsoft OneDrive. You need to place the contents of User1’s OneDrive account on an eDiscovery hold. Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

https://

<div>onedrive.live.com/</div> <div>contoso.onmicrosoft.com/</div> <div>contoso.sharepoint.com/</div> <div>contoso-my.sharepoint.com/</div>	<div>User1</div> <div>Sites/User1</div> <div>contoso_onmicrosoft_com/User1</div> <div>personal/User1_contoso_onmicrosoft_com</div>
--	--

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds>

**NEW QUESTION 26**

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:

- > Name: AutoLabel1
- > Label to auto-apply: Sensitivity1
- > Rules for SharePoint Online sites: Rule1-SPO
- > Choose locations where you want to apply the label: Site1 Rule1-SPO is configured as shown in the following exhibit.

**Edit rule**

Name \*

Rule1-SPO

Description

Rule1 description

^ Conditions

We'll apply this policy to content that matches these conditions.

^ Content contains sensitive info types

Default
All of these

Sensitive info types

IP Address
Accuracy 85 to 100
Instance count 2 to Any

Add

Create group

+ Add condition

Save Cancel

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
Sensitivity1 is applied to File1.docx.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 27**

- (Exam Topic 5)

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 32

- (Exam Topic 5)

You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment. You have the devices shown in the following table.

Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

You plan to enable co-management.

You need to identify which devices support co-management without requiring the installation of additional software.

Which devices should you identify?

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

Answer: D

### NEW QUESTION 34

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	Not applicable
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD)

What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action 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.

**Actions**

Disable BitLocker.

Disable TPM.

Switch to UEFI.

Upgrade to Windows 10 Enterprise.

**Answer Area**

Device1:

Action

Device2:

Action

Device3:

Action

- A. Mastered
- B. Not Mastered

Answer: A

### Explanation:

**Actions**

Disable BitLocker.

Disable TPM.

Switch to UEFI.

Upgrade to Windows 10 Enterprise.

**Answer Area**

Device1:

Disable BitLocker.

Device2:

Switch to UEFI.

Device3:

Upgrade to Windows 10 Enterprise.

### NEW QUESTION 39

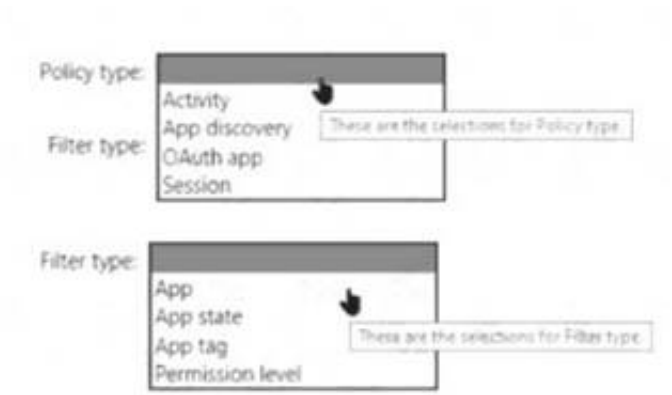
- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.

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

Answer Area

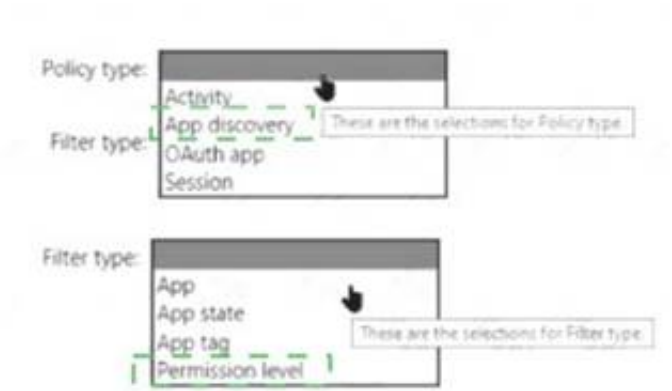


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 41

- (Exam Topic 5)

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 46

- (Exam Topic 5)

You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

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

NOTE: Each correct selection is worth one point.

In Azure:

<input type="checkbox"/>	Add and configure the Diagnostics settings for the Azure Activity Log.
<input type="checkbox"/>	Add and configure an Azure Log Analytics workspace.
<input type="checkbox"/>	Add an Azure Storage account and Azure Cognitive Search
<input type="checkbox"/>	Add an Azure Storage account and a file share.

On the computers:

<input type="checkbox"/>	Create an event subscription.
<input type="checkbox"/>	Modify the membership of the Event Log Readers group.
<input type="checkbox"/>	Enroll in Microsoft Endpoint Manager.
<input type="checkbox"/>	Install the Microsoft Monitoring Agent.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer

NEW QUESTION 49

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 tenant.

You need to create a custom Compliance Manager assessment template.

Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Application:

Microsoft Excel
Microsoft Forms
Microsoft Word
Visual Studio Code

File format:

csv
dbx
docx
dotx
json
xlsx
xltx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-create?view=o365>

#### NEW QUESTION 50

- (Exam Topic 5)

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

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

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

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

Name	Assigned to
Policy1	Group3
Policy2	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
Device1 is compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 55

- (Exam Topic 5)

HOTSPOT

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

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs. The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:

- > Users or workload identities assignments: All users
- > Cloud apps or actions assignment: App1
- > Conditions: Include all trusted locations
- > Grant access: Require multi-factor authentication

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
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	<input type="radio"/>	<input type="radio"/>
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

\* 131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1’s MFA status is disabled. The MFA requirement in the conditional access policy will override the user’s MFA status of disabled. Therefore, User1 must use MFA.

Box 2: Yes.

\* 131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.

Box 3: No.

IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24

Reference:

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

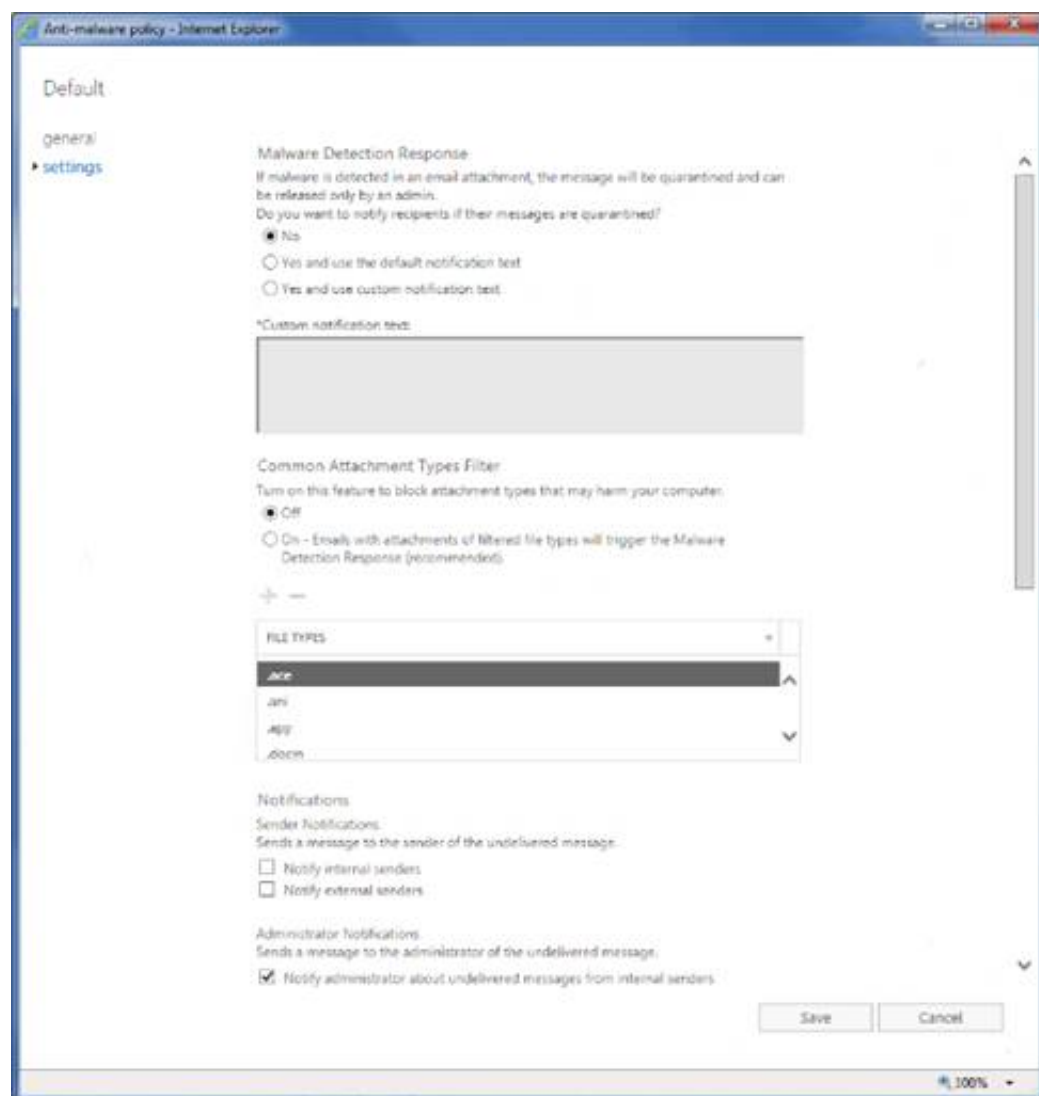
NEW QUESTION 59

- (Exam Topic 5)

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

The subscription has a single anti-malware policy as shown in the following exhibit.





An email message that contains text and two attachments is sent to User1. One attachment is infected with malware. How will the email message and the attachments be processed?

- A. Both attachments will be remove
- B. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
- C. The email message will be quarantined, and the message will remain undelivered.
- D. Both attachments will be remove
- E. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed.'
- F. The malware-infected attachment will be remove
- G. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

**Answer:** C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o36>

## NEW QUESTION 63

- (Exam Topic 5)

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: 

Role

Group2: 

Role

- 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

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles>

**NEW QUESTION 68**

- (Exam Topic 5)

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 71**

- (Exam Topic 5)

HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped devices (default)	Not applicable

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.

Settings > Endpoints > computer1



computer1

### Device summary

Risk level ⓘ

None

### Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

Use the drop-down menus to select the answer choice that completes each statement.  
 NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of [answer choice].

▼

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

▼

Group1 only

Group1 and Group2 only

Group1, Group2, Group3, and Group4

Ungrouped devices

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Box 1: Group3 and Group4 only Computer1 has no Demo Tag.

Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

### NEW QUESTION 75

- (Exam Topic 5)

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

- A. a custom detection rule
- B. an allowed/blocked list rule
- C. an alert suppression rule
- D. an indicator

**Answer: D**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators>

### NEW QUESTION 80

- (Exam Topic 5)

Your network contains an Active Directory domain named adatum.com that is synced to Azure AD. The domain contains 100 user accounts.

The city attribute for all the users is set to the city where the user resides.

You need to modify the value of the city attribute to the three-letter airport code of each city. What should you do?

- A. From Windows PowerShell on a domain controller, run the Gec-ADUser and Sec-ADUser cmdlets.
- B. From Azure Cloud Shell, run the Gec-ADUser and Sec-ADUser cmdlets.
- C. From Windows PowerShell on a domain controller, run the Gec-MgUser and Updace-MgUser cmdlets.
- D. From Azure Cloud Shell, run the Gec-MgUser and Update-MgUser cmdlets.

**Answer:** A

**Explanation:**

The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.

You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.

Note:

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

- \* 1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
- \* 2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.

Other incorrect answer options you may see on the exam include the following:

- \* 1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
- \* 2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.
- \* 3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
- \* 4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets. Reference:

<https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser>

**NEW QUESTION 82**

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action. To which location can the policy be applied?

- A. OneDrive accounts
- B. Exchange email
- C. Teams chat and channel messages
- D. SharePoint sites

**Answer:** B

**NEW QUESTION 84**

- (Exam Topic 5)

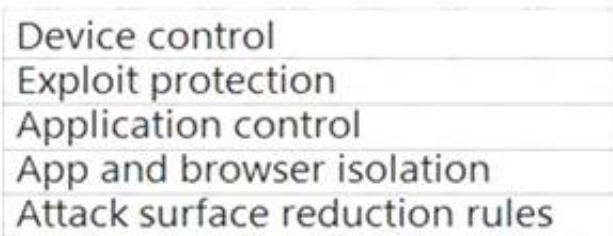
You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.

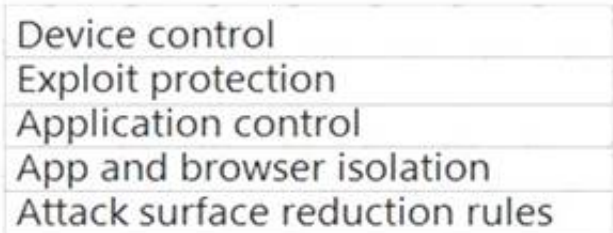
You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard.

ASR2 will be used to configure Microsoft Defender SmartScreen.

Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ASR1: 

ASR2: 

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application, chat or text message Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

**NEW QUESTION 88**

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record



Site1 contains the files shown in the following table.

Name	Label
File1	None
File2	Retention1
File3	Retention2
File4	Retention3

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Rename:

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

Delete:

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Rename:

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

Delete:

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

## NEW QUESTION 91

- (Exam Topic 5)

Your on-premises network contains an Active Directory domain. You have a Microsoft 365 subscription.

You need to sync the domain with the subscription. The solution must meet the following requirements: On-premises Active Directory password complexity policies must be enforced.

Users must be able to use self-service password reset (SSPR) in Azure AD.

What should you use?

- A. password hash synchronization
- B. Azure AD Identity Protection
- C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- D. pass-through authentication

Answer: D

Explanation:

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.

This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.

Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.

Password writeback is supported in environments that use the following hybrid identity models: Password hash synchronization

Pass-through authentication

Active Directory Federation Services Reference:

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

## NEW QUESTION 93

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

- A. Ubuntu Linux
- B. macOS
- C. iOS
- D. Android

**Answer:** B

**Explanation:**

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices Note:  
 There are several versions of this question in the exam. The question has two possible correct answers:

- > Windows 10
- > macOS

Other incorrect answer options you may see on the exam include the following:

- > Android Enterprise
- > Windows 8.1 Reference:

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

**NEW QUESTION 97**

- (Exam Topic 5)

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Not configured	15	Yes

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

Name	Assigned to
Policy2	Group2
Policy3	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.

**Answer Area**

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as noncompliant after 15 days.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

**NEW QUESTION 102**

- (Exam Topic 5)

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

Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

- Word files created by using Windows devices must be encrypted automatically.
- If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
- For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of policy should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type may be used

once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.  
 NOTE: Each correct selection is worth one point.

**Policy Types**

App configuration policy
App protection policy
Compliance policy
Conditional Access policy

**Answer Area**

Device1:
Device2:
Device3:

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

**Policy Types**

App configuration policy
App protection policy
Compliance policy
Conditional Access policy

**Answer Area**

Device1: App protection policy
Device2: Conditional Access policy
Device3: Compliance policy

#### NEW QUESTION 105

- (Exam Topic 5)

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 106

- (Exam Topic 5)

HOTSPOT

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

Name	Role
User1	Global admin
User2	None
User3	None

You provision the private store in Microsoft Store for Business.

You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Can add apps to the private store:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Can assign apps from Microsoft Store for Business:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business> <https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-rol>

**NEW QUESTION 108**

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

- > Deploy a VPN connection by using a VPN device configuration profile.
- > Configure security settings by using an Endpoint Protection device configuration profile. You support the management tasks.

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

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2 and Device3

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure> <https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos>

**NEW QUESTION 109**

- (Exam Topic 5)

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 114**

- (Exam Topic 5)

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

Name	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

You have labels in Microsoft 365 as shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

The content in Microsoft 365 is assigned labels as shown in the following table.

Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

You have labels in Microsoft 365 as shown in the following table.

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

**Answer Area**

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input type="radio"/>
Admin2 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input type="radio"/>
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 116**

- (Exam Topic 5)

HOTSPOT

			Progress	actions	Review			
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 119

- (Exam Topic 5)

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:

Graphical user interface, text, application Description automatically generated

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy

#### NEW QUESTION 121

- (Exam Topic 5)

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-t>

#### NEW QUESTION 125

- (Exam Topic 5)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to identify the settings that are below the Standard protection profile settings in the preset security policies.

What should you use? 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 130

- (Exam Topic 5)

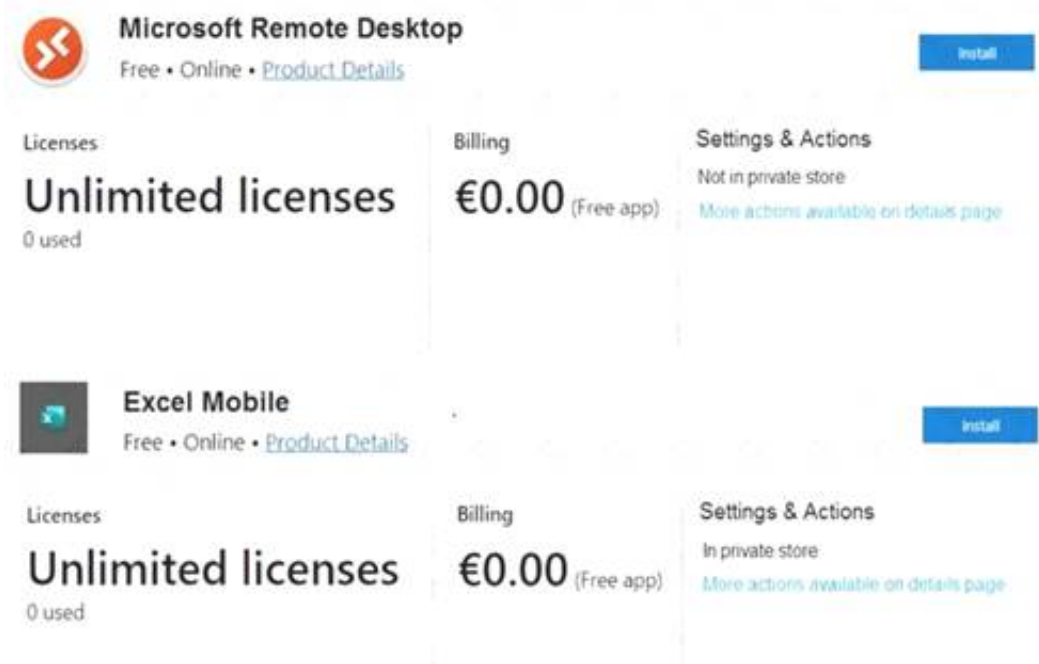
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.

The Products & services settings in Microsoft Store for Business are 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.

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	<input type="radio"/>	<input type="radio"/>
User4 can manage the Microsoft Remote Desktop app from the private store.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

NEW QUESTION 135

- (Exam Topic 5)

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 140

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.



Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

- > MDM user scope: Some
- > Groups: Group1
- > MAM user scope: Some
- > Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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 Device1 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

NEW QUESTION 142

- (Exam Topic 5)

Your company has multiple offices.

You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator. You need to ensure that the local administrators can manage only the devices in their respective office. What should you use?

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

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

NEW QUESTION 146

- (Exam Topic 5)

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 147

- (Exam Topic 5)

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 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 150

- (Exam Topic 5)

You have device compliance policies shown in the following table.

Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

The device compliance state for each policy is shown in the following table.

Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

NOTE: Each correct selection is worth one point.

#### Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	<input type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

#### Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input checked="" type="radio"/>	<input type="radio"/>

### NEW QUESTION 153

- (Exam Topic 5)

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:

Graphical user interface, text, application, chat or text message Description automatically generated

Reference:

<https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manage>

### NEW QUESTION 155

- (Exam Topic 5)

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

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

All the devices are onboarded To Microsoft Defender for Endpoint

You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

- Detect operating system vulnerabilities.

Answer Area

Detect operating system vulnerabilities

▼
Device1 only  
Device1 and Device2 only  
Device1, Device2, and Device3 only  
Device1, Device2, and Device4 only  
Device1, Device2, Device3 and Device4

Perform a configuration assessment of the operating system

▼
Device1 only  
Device1 and Device2 only  
Device1, Device2, and Device3 only  
Device1, Device2, and Device4 only  
Device1, Device2, Device3 and Device4

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

#### Answer Area

Detect operating system vulnerabilities

▼

Device1 only

Device1 and Device2 only

Device1, Device2, and Device3 only

Device1, Device2, and Device4 only

Device1, Device2, Device3 and Device4

Perform a configuration assessment of the operating system

▼

Device1 only

Device1 and Device2 only

Device1, Device2, and Device3 only

Device1, Device2, and Device4 only

Device1, Device2, Device3 and Device4

#### NEW QUESTION 157

- (Exam Topic 5)

Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD). Password hash synchronization is disabled.

You plan to implement co-management.

You need to configure Azure AD Connect and the domain to support co-management. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To configure Azure AD Connect:

Configure hybrid Azure AD join.

Enable device writeback.

Enable password hash synchronization.

To configure the domain:

Add an alternative UPN suffix.

Register a service connection point.

Register a service principal name (SPN).

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To configure Azure AD Connect:

Configure hybrid Azure AD join.

Enable device writeback.

Enable password hash synchronization.

To configure the domain:

Add an alternative UPN suffix.

Register a service connection point.

Register a service principal name (SPN).

#### NEW QUESTION 161

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.

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

NOTE: Each correct selection is worth one point.

- A. a data loss prevention (DLP) policy
- B. a sensitivity label policy
- C. a Microsoft Cloud App Security file policy
- D. a communication compliance policy
- E. a retention label policy

Answer: AD

#### NEW QUESTION 163

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

In the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices. You enable device clean-up rules.

What can you configure as the minimum number of days before a device is removed automatically?

- A. 10
- B. 30
- C. 45
- D. 90

Answer: D



#### NEW QUESTION 165

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

- A. Microsoft Store for Business
- B. Apple Business Manager
- C. Apple iTunes Store
- D. Apple Configurator

**Answer:** B

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios>

#### NEW QUESTION 169

- (Exam Topic 5)

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

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings: ➤ Show app and profile configuration progress: Yes

➤ Allow users to collect logs about installation errors: Yes

➤ Assignments: Group2

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status>

#### NEW QUESTION 171

- (Exam Topic 5)

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:

➤ Password Hash Sync: Enabled

➤ Pass-through authentication: Enabled

You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.

Which users should you identify?

- A. none
- B. User1 only
- C. User1 and User2 only

D. User1, User2, and User3

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 175**

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

- > Name: Case1
  - > Included content: Group1, User1, Site1
  - > Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders
- The investigation for Case1 completes, and you close the case.

What occurs after you close Case1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Holds are turned off for:

User1 only

All locations

Site1 and Group1 only

Holds are placed on a delay hold for:

30 days

90 days

120 days

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/close-or-delete-case?view=o365-worldwide>

**NEW QUESTION 177**

- (Exam Topic 5)

HOTSPOT

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

- > Contoso.com
- > East.contoso.com

The forest contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	East.contoso.com
User3	Fabrikam.com

The forest syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)

## PROVISION FROM ACTIVE DIRECTORY



### Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

### Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Disabled

## USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

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 authenticate to Azure AD by using a username of user1@contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can authenticate to Azure AD by using a username of user2@contoso.com.	<input type="radio"/>	<input type="radio"/>
User3 can authenticate to Azure AD by using a username of user3@contoso.com.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

### Explanation:

Box 1: Yes

The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.

Box 2: No

The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.

Box 3: No

The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

## NEW QUESTION 181

- (Exam Topic 5)

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

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.

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

### Answer Area

Device1:

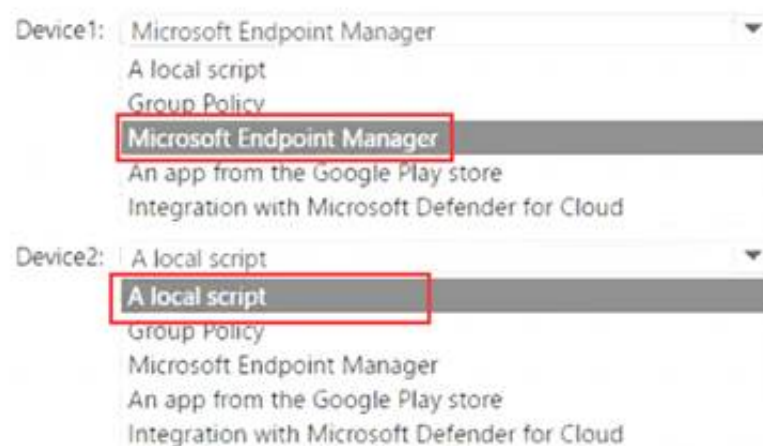
Device2:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area



#### NEW QUESTION 186

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

- A. 1
- B. 2
- C. 5
- D. 10

**Answer:** C

**Explanation:**

You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq>

#### NEW QUESTION 187

- (Exam Topic 5)

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#>

#### NEW QUESTION 192

- (Exam Topic 5)

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. advanced hunting
- B. security reports
- C. digital certificate assessment
- D. device discovery
- E. attack surface reduction (ASR)

**Answer:** BE

**Explanation:**

B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting

The Microsoft 365 Defender portal (<https://security.microsoft.com>) provides easy access to information about detected threats and actions to address those



threats.

The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created. The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.

The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab.

The Reports section includes reports that show threats detected and their status. E: What can you expect from Microsoft Defender for Endpoint P1?

Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:

- Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks.
- (E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.
- Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.

The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL backing	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
APIs, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts**		✓

\*\*Includes Targeted Attack Notifications (TAN) and Experts On Demand (EOD). Customers must apply for TAN. EOD is available for purchase as an add-on.

Incorrect:

Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.

Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1> <https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-plan>

### NEW QUESTION 193

- (Exam Topic 5)

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1. You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:

- Assign licenses to users.
- Procure apps from Microsoft Store.
- Manage private store availability for all items.

The solution must use the principle of least privilege.

Which Microsoft Store for Business role should you assign to User1?

- A. Basic Purchaser
- B. Device Guard signer
- C. Admin
- D. Purchaser

**Answer: C**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview>

### NEW QUESTION 197

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription.

You deploy the anti-phishing policy 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

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

Add trusted senders and domains

Enable domains to protect

Enable users to protect

Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Add trusted senders and domains

Enable intelligence for impersonation protection

Enable spoof intelligence

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Enable users to protect  
Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.  
User impersonation protection  
User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.  
You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section).  
When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender's email address, the action for impersonated users is applied to the message.  
Box 2: Add trusted senders and domains  
Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren't applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.  
Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

NEW QUESTION 201

- (Exam Topic 5)  
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:

Call to phone

Email message

Security questions

Text message to phone

Notification to Microsoft Authenticator app

Number of days:

7

14

30

60

- 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.  
Reference:  
<https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work-remotely-secure-sign-in> <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure>

#### NEW QUESTION 205

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

##### Review your settings

**Name** [Edit](#)  
Retention1

**Description for admins** [Edit](#)

**Description for users** [Edit](#)

**File plan descriptors** [Edit](#)

Reference Id:1  
Business function/department Legal  
Category: Compliance  
Authority type: Legal

**Retention** [Edit](#)

7 years  
Retain only  
Based on when it was created

[Back](#) [Create this label](#) [Cancel](#)

When users attempt to apply Retention1, the label is unavailable. You need to ensure that Retention1 is available to all the users. What should you do?

- A. Create a new label policy
- B. Modify the Authority type setting for Retention!
- C. Modify the Business function/department setting for Retention 1.
- D. Use a file plan CSV template to import Retention1.

**Answer:** A

#### **Explanation:**

Reference:

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

#### NEW QUESTION 210

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-102 Product From:

<https://www.2passeasy.com/dumps/MS-102/>

## Money Back Guarantee

### 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