

Exam Questions MS-102

Microsoft 365 Administrator Exam

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



NEW QUESTION 1

- (Exam Topic 1)

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Seattle:

▼
6 months
18 months
24 months
30 months
5 years

New York:

▼
6 months
18 months
24 months
30 months
5 years

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet> March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date

References:

<https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10>

NEW QUESTION 2

- (Exam Topic 1)

You need to create the Microsoft Store for Business. Which user can create the store?

- A. User2
- B. User3
- C. User4
- D. User5

Answer: C

Explanation:

References:

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

NEW QUESTION 3

- (Exam 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=o>

NEW QUESTION 4

- (Exam Topic 3)

You need to configure the compliance settings to meet the technical requirements. What should you do in the Microsoft Endpoint Manager admin center?

- A. From Compliance policies, modify the Notifications settings.
- B. From Locations, create a new location for noncompliant devices.
- C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
- D. Modify the Compliance policy settings.

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 5)

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 Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

- A. Yes
- B. no

Answer: B

NEW QUESTION 8

- (Exam Topic 5)

You have a Microsoft 365 tenant.

Company policy requires that all Windows 10 devices meet the following minimum requirements:

- > Require complex passwords.
- > Require the encryption of data storage devices.
- > Have Microsoft Defender Antivirus real-time protection enabled.

You need to prevent devices that do not meet the requirements from accessing resources in the tenant. Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a configuration policy
- B. a compliance policy
- C. a security baseline profile
- D. a conditional access policy
- E. a configuration profile

Answer: BD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 9

- (Exam Topic 5)

Your company has a Microsoft E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance. What should you use?

- A. eDiscovery
- B. Information governance
- C. Compliance Manager
- D. Data Subject Requests (DSRs)

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001>

NEW QUESTION 10

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure AD.

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

- A. From the Microsoft Entra admin center, create a conditional access policy
- B. From the Microsoft 365 admin center, configure the Modern authentication settings.
- C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
- D. From Multi-Factor Authentication, configure the service settings.

Answer: A

Explanation:

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authenticati>

NEW QUESTION 10

- (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 14

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data. What should you do in the Microsoft 365 compliance center?

- A. Create a Data Subject Request (DSR)
- B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data
- C. Create an assessment based on the EU GDPR assessment template
- D. Create an assessment based on the Data Protection Baseline assessment template

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan>

NEW QUESTION 16

- (Exam Topic 5)

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 19

- (Exam Topic 5)

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.

What should you create in Microsoft Endpoint Manager?

- A. an app configuration policy
- B. an app
- C. a device configuration profile
- D. a device compliance policy

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune>

NEW QUESTION 20

- (Exam Topic 5)

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.

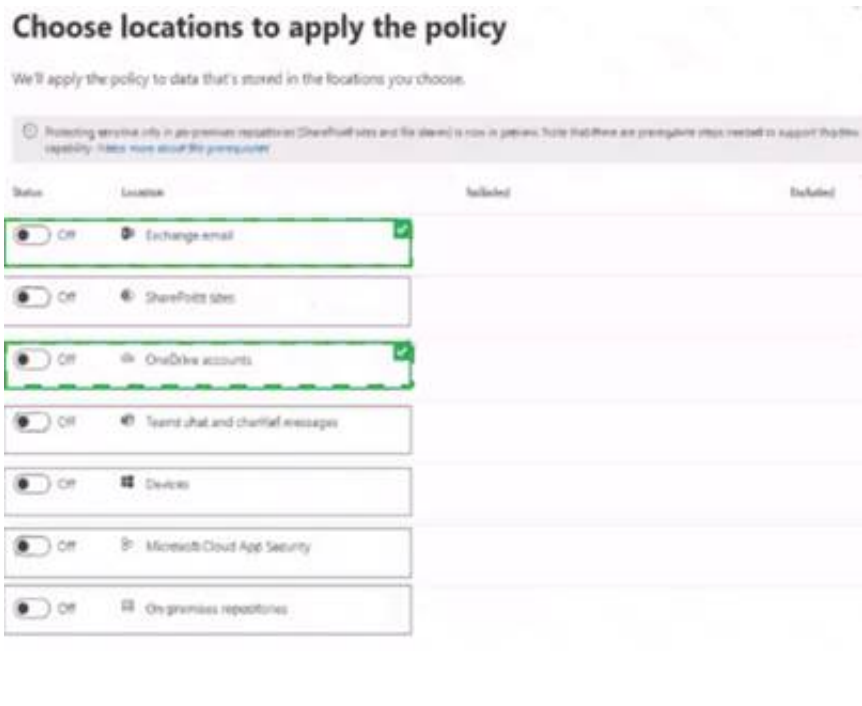
Protecting sensitive info in on-premises repositories (SharePoint sites and file stores) is now in preview. Take that, these are prerequisite steps needed to support this new capability. [Take more about the prerequisite](#)

Status	Location	Included	Excluded
<input 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 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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 24

- (Exam Topic 5)
HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:

▼

Rule1 tip only
Rule2 tip only
Rule3 tip only
Rule1 tip and Rule2 tip only
Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

▼

Rule1 tip only
Rule3 tip only
Rule4 tip only
Rule1 tip and Rule4 tip only
Rule1 tip, Rule3 tip, and Rule4 tip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Rule1 tip only
File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.

Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.

Box 2: Rule1 tip only

Note: User Override support

The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).

It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also

overrides any other rules that the content matched. Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp> <https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips>

NEW QUESTION 27

- (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 31

- (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: 

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

ASR2: 

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

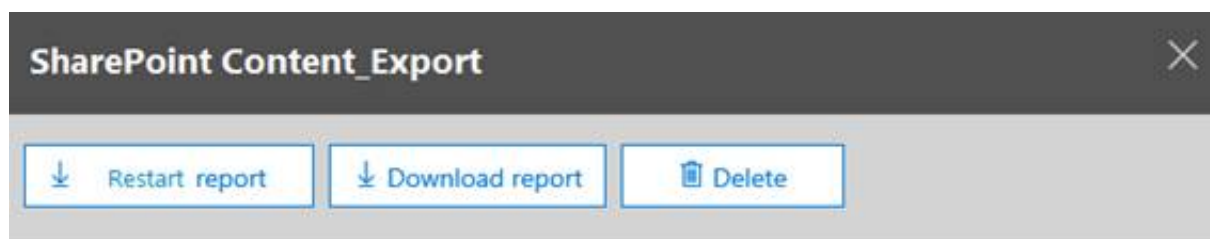
Reference:

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

NEW QUESTION 34

- (Exam Topic 5)

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=o3> <https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

NEW QUESTION 36

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft 365 compliance policies to meet the following requirements:

- > Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
- > Report on shared documents that contain PII. What should you create?

- A. an alert policy
- B. a data loss prevention (DLP) policy
- C. a retention policy
- D. a Microsoft Cloud App Security policy

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

NEW QUESTION 41

- (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 42

- (Exam Topic 5)

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 44

- (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 polio/ 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 46

- (Exam Topic 5)

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 50

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: No

Box 2: Yes

Box 3: No Reference:

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

NEW QUESTION 52

- (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 Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com.

Does this meet the goal?

- A. Yes
B. No

Answer: A

Explanation:

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 54

- (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 59

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.

From Azure AD Identity Protection, you enable a sign-in risk policy.

Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.

What should you configure?

- A. the Tenant restrictions settings in Azure AD
- B. a trusted location
- C. a Conditional Access policy exclusion
- D. the Microsoft 365 network connectivity settings

Answer: B

Explanation:

There are two types of risk policies in Azure Active Directory (Azure AD) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:

Sign-in risk policy User risk policy

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-> <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION 61

- (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 65

- (Exam Topic 5)

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs. D18912E1457D5D1DDCBD40AB3BF70D5D

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a sensitive information type
 B. a sensitivity label
 C. a supervision policy
 D. a retention label

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

NEW QUESTION 67

- (Exam Topic 5)

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments 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: C

NEW QUESTION 72

- (Exam Topic 5)

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

Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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 has their cache cleared on close.	<input type="radio"/>	<input type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>
User3 has Cursor movement set to Visual.	<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/deployoffice/overview-office-cloud-policy-service>

NEW QUESTION 77

- (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 79

- (Exam Topic 5)

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

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress. Yes No

Show time limit error when installation takes longer than specified number of minutes.

Show custom message when time limit error occurs. Yes No

Allow users to collect logs about instalation errors. Yes No

Only show page to devices provisioned by out-of-box experience (OOBE) Yes No

Block device use until all apps and profiles are installed Yes No

You assign the policy to Group1.

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
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 84

- (Exam Topic 5)

You have a Microsoft 365 subscription.

From 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 Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 86

- (Exam Topic 5)

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

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager. To which devices can you deploy Microsoft 365 Apps for enterprise?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 89

- (Exam Topic 5)

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

NEW QUESTION 93

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.

You deploy a third-party antivirus solution to the devices. You need to ensure that the devices are marked as compliant.

Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 10 compliance policy
 Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

NEW QUESTION 95

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

- A. Microsoft Exchange Online only
- B. Microsoft Teams only
- C. Microsoft Exchange Online and SharePoint Online only
- D. Microsoft Teams and SharePoint Online only
- E. Microsoft Teams, Exchange Online, and SharePoint Online

Answer: A

Explanation:

Privileged access management

Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon. Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management-solution-overview> <https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management>

NEW QUESTION 97

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings:

* 1. Assignments

- > Users or workload identities: Group1
- > Cloud apps or actions: Office 365 SharePoint Online
- > Conditions

- Filter for devices: Exclude filtered devices from the policy

- Rule syntax: device.displayName -startsWith "Device"

* 2. Access controls

> Grant

- Grant: Block access

> Session: 0 controls selected

* 3. Enable policy: On

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 access Site1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

User1 is member of Group1 and has Device1. Device1 is not Azure AD joined.

Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.

Box 2: Yes

User2 is member of Group1 and has devices Device2 and Device3. Device2 is Azure AD joined.

Device2 is excluded from CAPolicy1 (which would block access to Site1). Box 3: Yes

User2 is member of Group1 and has devices Device2 and Device3. Device3 is Android and is Azure AD registered.

Device3 is excluded from CAPolicy1 (which would block access to Site1).

Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join>

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

NEW QUESTION 98

- (Exam Topic 5)

HOTSPOT

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

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.

How should you complete the membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

(user.userType) and (user.department)

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: -eq "Guest"

Dynamic membership rules for groups in Azure Active Directory Supported expression operators

The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

* Equals

-eq

* Contains

-contains

* Etc.

Box 2: -contains "Support" Incorrect:

* -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notin operators.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

NEW QUESTION 102

- (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. Android

B. CentOS Linux

C. iOS

D. Window 10

Answer: D

Explanation:

Reference:

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

NEW QUESTION 105

- (Exam Topic 5)

HOTSPOT

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

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	Not applicable

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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

If a high-severity incident is triggered for Device1, an incident email notification will be sent.

Yes

☐

No

☐

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

☐
☐

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.

Box 2: No

Computer1 does not belong to either Group1 or Group2 Box 3: Yes

Device3 belongs to both Group1 and Group2. Note: Understanding alert severity

Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.

The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue>

NEW QUESTION 106

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription 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 publish a sensitivity label named Label1. To which groups can you publish Label1?

- A. Group1 only
- B. Group1 and Group2 only
- C. Group1 and Group4 only
- D. Group1, Group2, and Group3 only
- E. Group1 Group2, Group3, and Group4

Answer: A

Explanation:

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.

Reference:

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

NEW QUESTION 110

- (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:	<input type="checkbox"/> Configure hybrid Azure AD join. <input type="checkbox"/> Enable device writeback. <input type="checkbox"/> Enable password hash synchronization.
To configure the domain:	<input type="checkbox"/> Add an alternative UPN suffix. <input type="checkbox"/> Register a service connection point. <input type="checkbox"/> Register a service principal name (SPN)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To configure Azure AD Connect:	<input checked="" type="checkbox"/> Configure hybrid Azure AD join. <input checked="" type="checkbox"/> Enable device writeback. <input checked="" type="checkbox"/> Enable password hash synchronization.
To configure the domain:	<input checked="" type="checkbox"/> Add an alternative UPN suffix. <input checked="" type="checkbox"/> Register a service connection point. <input checked="" type="checkbox"/> Register a service principal name (SPN)

NEW QUESTION 114

- (Exam Topic 5)

Your company has offices in five cities. The company has a Microsoft 365 tenant.

Each office is managed by a local administrator. You plan to deploy Microsoft Intune.

You need to recommend a solution to manage resources in intune that meets the following requirements: ➤ Local administrators must be able to manage only the resources in their respective office.

- Local administrators must be prevented from managing resources in other offices.
- Administrative effort must be minimized.

What should you include in the recommendation?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 117

- (Exam Topic 5)

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

You need to be notified when a single user downloads more than 50 files during any 60-second period. What should you configure?

- A. a session policy
- B. a file policy
- C. an activity policy
- D. an anomaly detection policy

Answer: D

NEW QUESTION 121

- (Exam Topic 5)

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.

▼

AlertInfo

DeviceEvents

DeviceInfo

▼

ActionType startswith 'ASR'

lookup

project

render

where

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction>

NEW QUESTION 123

- (Exam Topic 5)

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:

Graphical user interface, application, table Description automatically generated

Reference:

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

NEW QUESTION 128

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.

From Microsoft Defender Security Center, you perform a security investigation.

You need to run a PowerShell script on the device to collect forensic information. Which action should you select on the device page?

- A. Initiate Live Response Session
 B. Initiate Automated Investigation
 C. Collect investigation package
 D. Go hunt

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwid>

NEW QUESTION 130

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You discover that some external users accessed center for a Microsoft SharePoint site. You modify the sharePoint sharing policy to prevent sharing, outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security \$ Compliance admin center you create a threat management policy. Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 135

- (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 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 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>

NEW QUESTION 137

- (Exam Topic 5)

DRAG DROP

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

- > Block emails that contain financial data.
- > Display the following policy tip text: Message blocked.

From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

- > Use the following location: Exchange email.
- > Display the following policy tip text: Message contains sensitive data.
- > When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result 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.

Results	Answer Area
The email will be blocked, and the user will receive the policy tip: Message blocked.	When the user sends an email that contains financial data and health records:
The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.	When the user sends an email that contains only financial data:
The email will be allowed, and the user will receive the policy tip: Message blocked.	
The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.	
The email will be allowed, and a message policy tip will NOT be displayed.	

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.

If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers>

NEW QUESTION 139

- (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 141

- (Exam Topic 5)

Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component 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

An app configuration policy

An app protection policy

A compliance policy

A configuration profile

Answer Area

Company-owned devices:

Solution

Personal devices:

Solution

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application, Word Description automatically generated

NEW QUESTION 142

- (Exam Topic 5)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.

You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

- A. Delete the workspace.
- B. Create a workspace.
- C. Onboard a new device.
- D. Offboard the test devices.

Answer: B

Explanation:

Storage locations

Understand where Defender for Cloud stores data and how you can work with your data:

* Machine information

- Stored in a Log Analytics workspace.

- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace>

NEW QUESTION 147

- (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 148

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.

Which policy should you use?

- A. a retention policy
- B. a retention label policy
- C. an auto-labeling policy
- D. an insider risk policy

Answer: C

Explanation:

Reference:

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

NEW QUESTION 151

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

Review your settings and finish

Name

Sensitivity1

Display name

Sensitivity1

Description for users

Sensitivity1

Scope

File.Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns

None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

Auto-labeling policy

Edit Policy

Delete Policy

Policy name

Auto-labeling policy

Description

Label in simulation

Sensitivity1

Info to label

IP Address

Apply to content in these locations

Exchange email All

Rules for auto-applying this label

Exchange email 1 rule

Mode

On

Comment

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	Not applicable	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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 the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<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>

NEW QUESTION 154

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains the following user:

- > Name: User1
- > UPN: user1@contoso.com
- > Email address: user1@marketing.contoso.com
- > MFA enrollment status: Disabled

When User1 attempts to sign in to Outlook on the web by using the user1@marketing.contoso.com email address, the user cannot sign in. You need to ensure that User1 can sign in to Outlook on the web by using user1@marketing.contoso.com. What should you do?

- A. Assign an MFA registration policy to User1.
- B. Reset the password of User1.
- C. Add an alternate email address for User1.
- D. Modify the UPN of User1.

Answer: D

Explanation:
Microsoft’s recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN’s to match.
Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.

Configure the Azure AD multifactor authentication registration policy

Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.

Reference:

<https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname>

NEW QUESTION 155

- (Exam Topic 5)

You purchase a new computer that has Windows 10, version 21H1 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

- A. Install all the feature updates released since version 21H1 and the latest quality update only.
- B. Install the latest feature update and all the quality updates released since version 21H1.
- C. Install the latest feature update and the latest quality update only.
- D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

Answer: C

NEW QUESTION 158

- (Exam Topic 5)

HOTSPOT

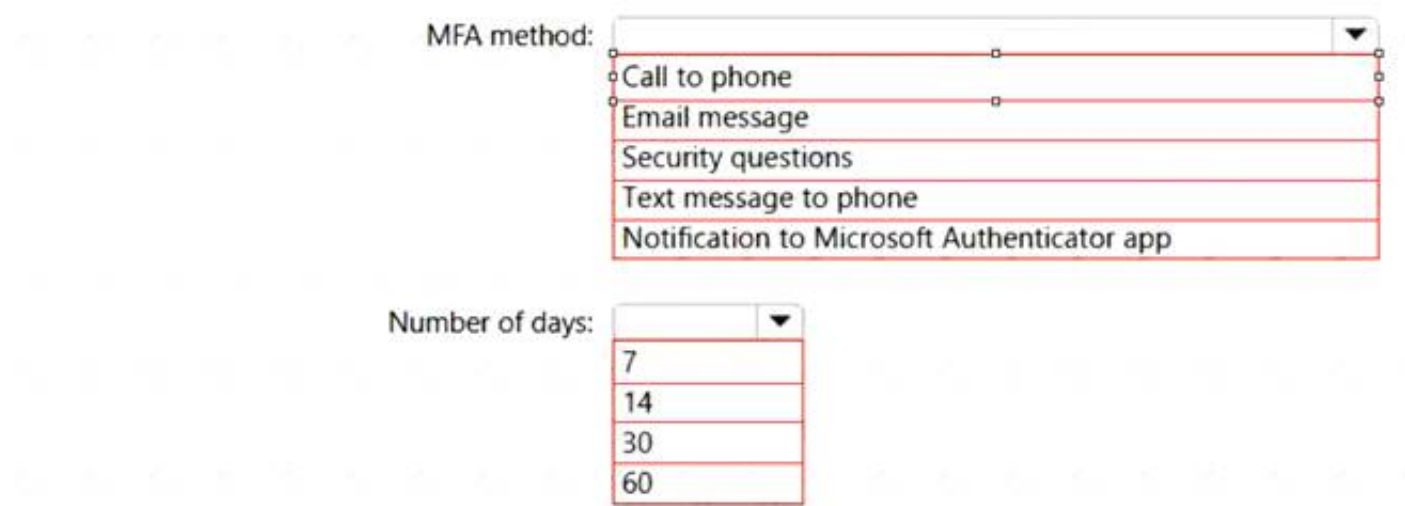
You have a new Microsoft 365 E5 tenant. Enable Security defaults is set to Yes.

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



The screenshot shows a configuration interface for MFA. It has two main sections: 'MFA method:' and 'Number of days:'. The 'MFA method:' section has a dropdown menu that is open, showing a list of options: 'Call to phone', 'Email message', 'Security questions', 'Text message to phone', and 'Notification to Microsoft Authenticator app'. The 'Number of days:' section has a dropdown menu that is also open, showing a list of options: '7', '14', '30', and '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 160

.....

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