Exam Questions MS-102

Microsoft 365 Administrator Exam

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

NEW QUESTION 1
- (Topic 6)
You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

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

Answer: A

Explanation:
Reference:
https://systemcenterdudes.com/intune-company-portal-customization/

NEW QUESTION 2
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 tenant
You create a data toss 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Choose locations to apply the policy

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

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

Status	Location	Included	Excluded
● Off	📧 Exchange email ✓		
● Off	🌐 SharePoint sites		
● Off	☁ OneDrive accounts ✓		
● Off	👥 Teams chat and channel messages		
● Off	⊞ Devices		
● Off	⊗ Microsoft Cloud App Security		
● Off	⊞ On-premises repositories		

NEW QUESTION 3
DRAG DROP - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to automatically label the documents on Site1 that contain credit card numbers. Which three actions should you perform in sequence? To answer, move the appropriate
actions from the list of actions to the answer area and arrange them in the correct order.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 4

- (Topic 6)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list.
You need to remove User1 from the Restricted entities list. What should you use?

A. the Exchange admin center
B. the Microsoft Purview compliance portal
C. the Microsoft 365 admin center
D. the Microsoft 365 Defender portal
E. the Microsoft Entra admin center

Answer: D

Explanation:
Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam
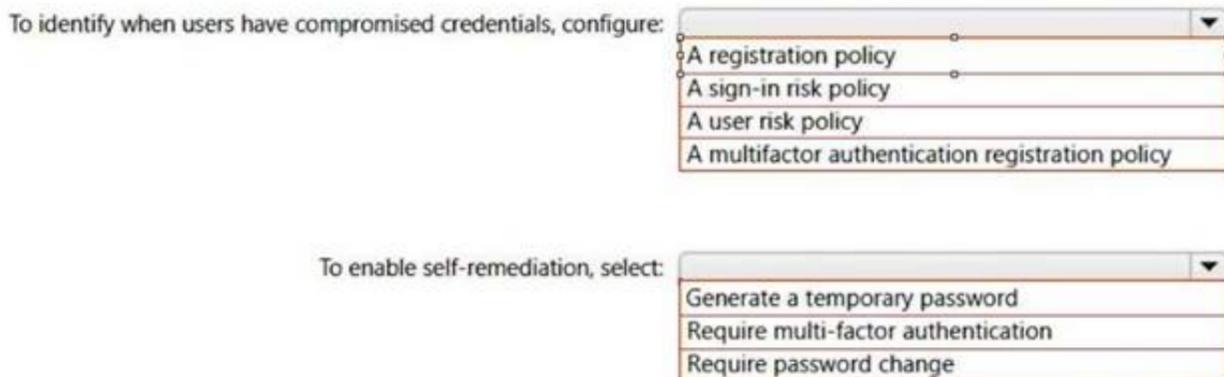
NEW QUESTION 5
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to implement identity protection. The solution must meet the following requirements:
? Identify when a user's credentials are compromised and shared on the dark web.
? Provide users that have compromised credentials with the ability to self-remediate.
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 identify when users have compromised credentials, configure:
- A registration policy
- A sign-in risk policy
- A user risk policy
- A multifactor authentication registration policy

To enable self-remediation, select:
- Generate a temporary password
- Require multi-factor authentication
- Require password change

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A user risk policy
Identify when a user's credentials are compromised and shared on the dark web.
User risk-based Conditional Access policy
Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:
Block access
Allow access but require a secure password change.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.
Box 2: Require password change
Provide users that have compromised credentials with the ability to self-remediate.
A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

NEW QUESTION 6
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 7
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

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

Answer: D

NEW QUESTION 8
- (Topic 6)
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 9
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the resources shown in the following table.

Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

A. Mailbox1 and Site1 only
B. Mailbox1, Account1, and Site1 only
C. Account1 and Site1 only
D. Mailbox1, Account1, Site1, and Channel1
E. Account1, Site1, and Channel1 only

Answer: E

Explanation:

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

NEW QUESTION 10
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: At a command prompt, you run the winver.exe command. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

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

NEW QUESTION 10
- (Topic 6)

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 Modem 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-authentication

NEW QUESTION 14
- (Topic 6)
Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset.
What should you do first?

A. From Compliance Manager, turn off automated testing.
B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

NEW QUESTION 19
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure a group naming policy.
Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Portal: The Microsoft 365 admin center
  The Microsoft 365 admin center
Group types: The Microsoft 365 Defender portal
  The Microsoft Entra admin center
  The Microsoft Purview compliance portal

Group types: Security only
  Microsoft 365 only
  Security only
  Security and mail-enabled security only
  Microsoft 365 and distribution only
  Microsoft 365, mail-enabled security, and distribution only
  Security, Microsoft 365, mail-enabled security, and distribution

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Portal: The Microsoft 365 admin center
  The Microsoft 365 admin center
Group types: The Microsoft 365 Defender portal
  The Microsoft Entra admin center
  The Microsoft Purview compliance portal

Group types: Security only
  Microsoft 365 only
  Security only
  Security and mail-enabled security only
  Microsoft 365 and distribution only
  Microsoft 365, mail-enabled security, and distribution only
  Security, Microsoft 365, mail-enabled security, and distribution

NEW QUESTION 21
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	Service Support Administrator
User3	Cloud Application Administrator
User4	None

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can
modify the setting. The solution must use the principle of least privilege.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft 365 setting:
- Office installation options
- Privileged access
- Release preferences

User:
- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

NEW QUESTION 25
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain. You deploy an Azure AD tenant.
Another administrator configures the domain to synchronize to Azure AD.
You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The question states that "all the user account synchronizations completed successfully". Therefore, the Azure AD credentials are configured correctly in Azure AD Connect. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync- configure-filtering

NEW QUESTION 30
- (Topic 6)
You have a Microsoft 365 E5 subscription.
On Monday, you create a new user named User1.
On Tuesday, User1 signs in for the first time and perform the following actions:
• Signs in to Microsoft Exchange Online from an anonymous IP address
• Signs in to Microsoft SharePoint Online from a device in New York City.
• Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections
Which types of sign-in risks will Azure AD Identity Protection detect for User1?

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

Answer: C

NEW QUESTION 31
- (Topic 6)
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)

SharePoint Content_Export   ✕

↓ Restart report   ↓ Download report   🗑 Delete

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

Items included from the search:
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

Close

Feedback

What will be excluded from the export?

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

Answer: B

Explanation:
Unrecognized file formats are excluded from the search.
Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide
https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search- report

NEW QUESTION 32
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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

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

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

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

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

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	⊙	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	⊙
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	⊙

NEW QUESTION 33
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goats. 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 SharePoint Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 35
HOTSPOT - (Topic 6)
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:

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

NEW QUESTION 40
- (Topic 6)
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-worldwide

NEW QUESTION 41
- (Topic 6)
You purchase a new computer that has Windows 10, version 2004 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 2004 and all the quality updates released since version 2004 only.
B. install the West feature update and the latest quality update only.
C. install all the feature updates released since version 2004 and the latest quality update only.
D. install the latest feature update and all the quality updates released since version 2004.

Answer: B

NEW QUESTION 45
- (Topic 6)
You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.
You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.
You need to identify which user can view security incidents from the Microsoft 365 Defender portal.
Which user should you identify?

A. User1
B. User2
C. User3
D. User4

Answer: A

NEW QUESTION 49
- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Anti-malware
B. Anti-phishing
C. Safe Attachments
D. Anti-spam
E. Safe Links

Answer: CE

NEW QUESTION 54
- (Topic 6)
You have a Microsoft 365 subscription.
You plan to use Adoption Score and need to ensure that it can obtain device and software metrics.
What should you do?

A. Enable Endpoint analytics.
B. Run the Microsoft 365 network connectivity test on each device.
C. Enable privileged access.
D. Configure Support integration.

Answer: A

NEW QUESTION 58
- (Topic 6)
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 61
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

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

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

A. Group1 only
B. Group2 only
C. Sitel only
D. Groupl and Group2 only
E. Group1, Group2, and Sitel

Answer: E

Explanation:
Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory
Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
When you configure a label policy, you can:
Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.
Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams- groups-sites
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365- worldwide

NEW QUESTION 65
- (Topic 6)
You have a Microsoft E5 subscription.
You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time.
What should you implement?

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

Answer: A

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

NEW QUESTION 67
HOTSPOT - (Topic 6)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.

You purchase a Windows 10 device named Device1.
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 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	⦿	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	⦿
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	⦿

NEW QUESTION 68
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 71
HOTSPOT - (Topic 6)
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.	◉	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	○	○

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

NEW QUESTION 74
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Endpoint Management admin center, you create a device configuration profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to create a trusted location and a conditional access policy.

NEW QUESTION 77
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

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

A user that is assigned the Global Administrator role as active **[answer choice]**.

▼
will lose the role after eight hours
can reactivate the role every eight hours
can reactivate the role every 15 days
will lose the role after 15 days

You can make the Global Administrator role available to activation requests **[answer choice]**.

▼
for up to eight hours
for up to three months
for up to 15 days
until the requests are revoked manually

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: will lose the role after eight hours
From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)
Box 2: for up to three months
We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 82
- (Topic 6)
You have a Microsoft 365 subscription that contains the alerts shown in the following table.

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

Which properties of the alerts can you modify?

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

Answer: B

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

NEW QUESTION 83
DRAG DROP - (Topic 6)
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	Answer Area	
An app configuration policy	Company-owned devices:	Solution
An app protection policy	Personal devices:	Solution
A compliance policy		
A configuration profile		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Solutions	Answer Area	
An app configuration policy	Company-owned devices:	A compliance policy
An app protection policy	Personal devices:	An app protection policy
A compliance policy		
A configuration profile		

NEW QUESTION 85
- (Topic 6)
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 87
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

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

User	Role
User1	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Add apps to the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Add apps to the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

NEW QUESTION 90
DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 subscription. Several users have iOS devices.
You plan to enroll the iOS devices in Microsoft Endpoint Manager.
You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.
From the Microsoft Endpoint Manager admin center, download a certificate signing request.
Upload an Apple MDM push certificate to Microsoft Endpoint Manager.
Create a certificate from the Apple Push Certificates Portal.
From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area

> (>)
> (<)
> (^)
> (v)

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.
From the Microsoft Endpoint Manager admin center, download a certificate signing request.
Upload an Apple MDM push certificate to Microsoft Endpoint Manager.
Create a certificate from the Apple Push Certificates Portal.
From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area

From the Microsoft Endpoint Manager admin center, download a certificate signing request.
Create a certificate from the Apple Push Certificates Portal.
Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

NEW QUESTION 95
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.
You need to identify the following information:
• The number of email messages quarantined by zero-hour auto purge (ZAP)
• The number of times users clicked a malicious link in an email message
Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

• • • • •

Answer Area

To identify the number of emails quarantined by ZAP: `Threat protection status ▾`
- Mailflow status report
- Spoof detections
- **Threat protection status**
- URL threat protection

To identify the number of times users clicked a malicious link in an email: `Mailflow status report ▾`
- **Mailflow status report**
- Spoof detections
- Threat protection status
- URL threat protection

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

To identify the number of emails quarantined by ZAP:	Threat protection status ▼	
	Mailflow status report	
	Spoof detections	
	Threat protection status	
	URL threat protection	

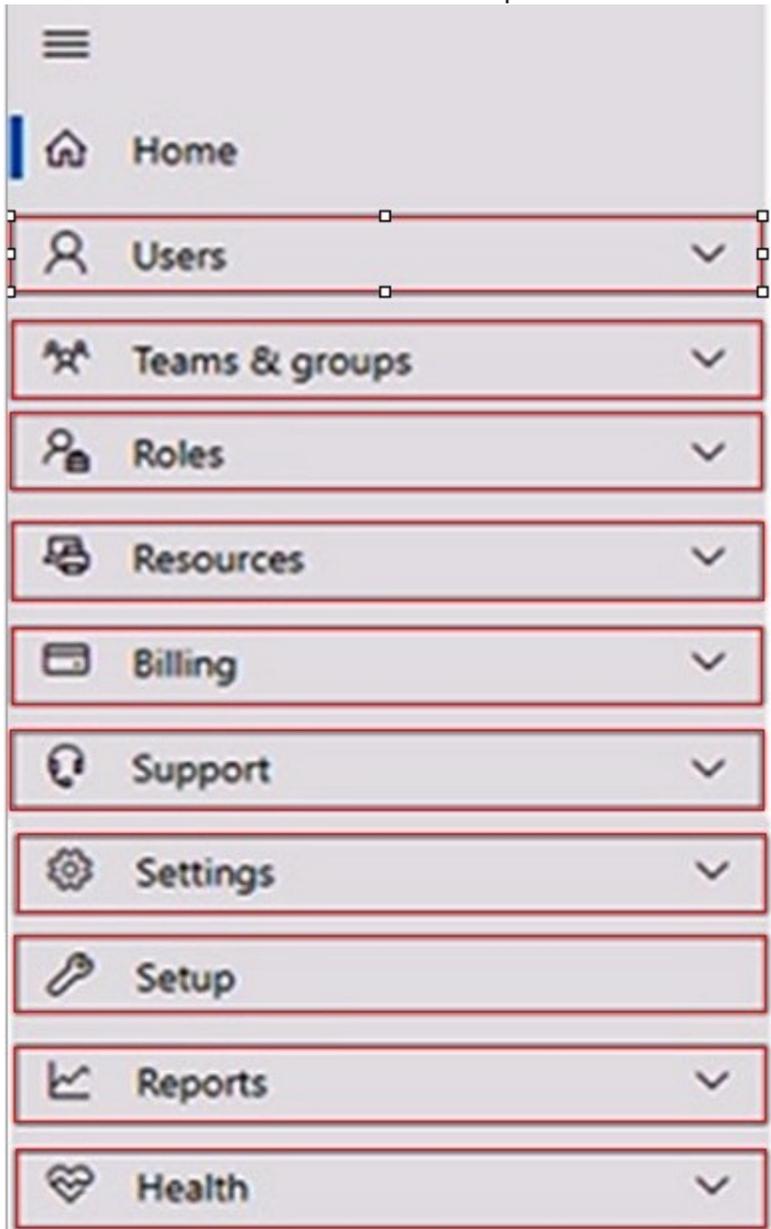|		
To identify the number of times users clicked a malicious link in an email:	Mailflow status report ▼	
	Mailflow status report	
	Spoof detections	
	Threat protection status	
	URL threat protection	

NEW QUESTION 99
HOTSPOT - (Topic 6)
HOTSPOT
Your company has a Microsoft 365 E5 subscription. You need to perform the following tasks:
View the Adoption Score of the company. Create a new service request to Microsoft.
Which two options should you use in the Microsoft 365 admin center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

☰

🏠 Home

👤 Users ⌄

👥 Teams & groups ⌄

🔑 Roles ⌄

🖥 Resources ⌄

💳 Billing ⌄

🎧 Support ⌄

⚙️ Settings ⌄

🔑 Setup

📈 Reports ⌄

💗 Health ⌄

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Reports
View the Adoption Score of the company.
How to enable Adoption Score To enable Adoption Score:
? Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score
? Select enable Adoption Score. It can take up to 24 hours for insights to become
available.
Box 2: Support
Create a new service request to Microsoft.
Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New
service request.

NEW QUESTION 100
HOTSPOT - (Topic 6)

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

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User1	Group1	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
User3	Group1, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.
From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

Microsoft Authenticator settings   ✕

ⓘ Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. Learn more

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more.

Enable and Target   Configure

Enable ⬤

Include   Exclude

Target ◯ All users ⦿ Select groups

Add groups

Name	Type	Registration	Authentication mode
Group1	Group	Optional ∨	Passwordless ∨ ✕

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 use number matching during sign-in.	◯	◯
User2 can use number matching during sign-in.	◯	◯
User3 can use number matching during sign-in.	◯	◯

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	◯	[◯]
User2 can use number matching during sign-in.	◯	[◯]
User3 can use number matching during sign-in.	◯	[◯]

NEW QUESTION 104
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. From Microsoft Defender for Endpoint you turn on the Allow or block file advanced feature. You need to block users from downloading a file named File1.exe.
What should you use?

A. an indicator
B. a suppression rule
C. a device configuration profile

Answer: A

NEW QUESTION 108
HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.
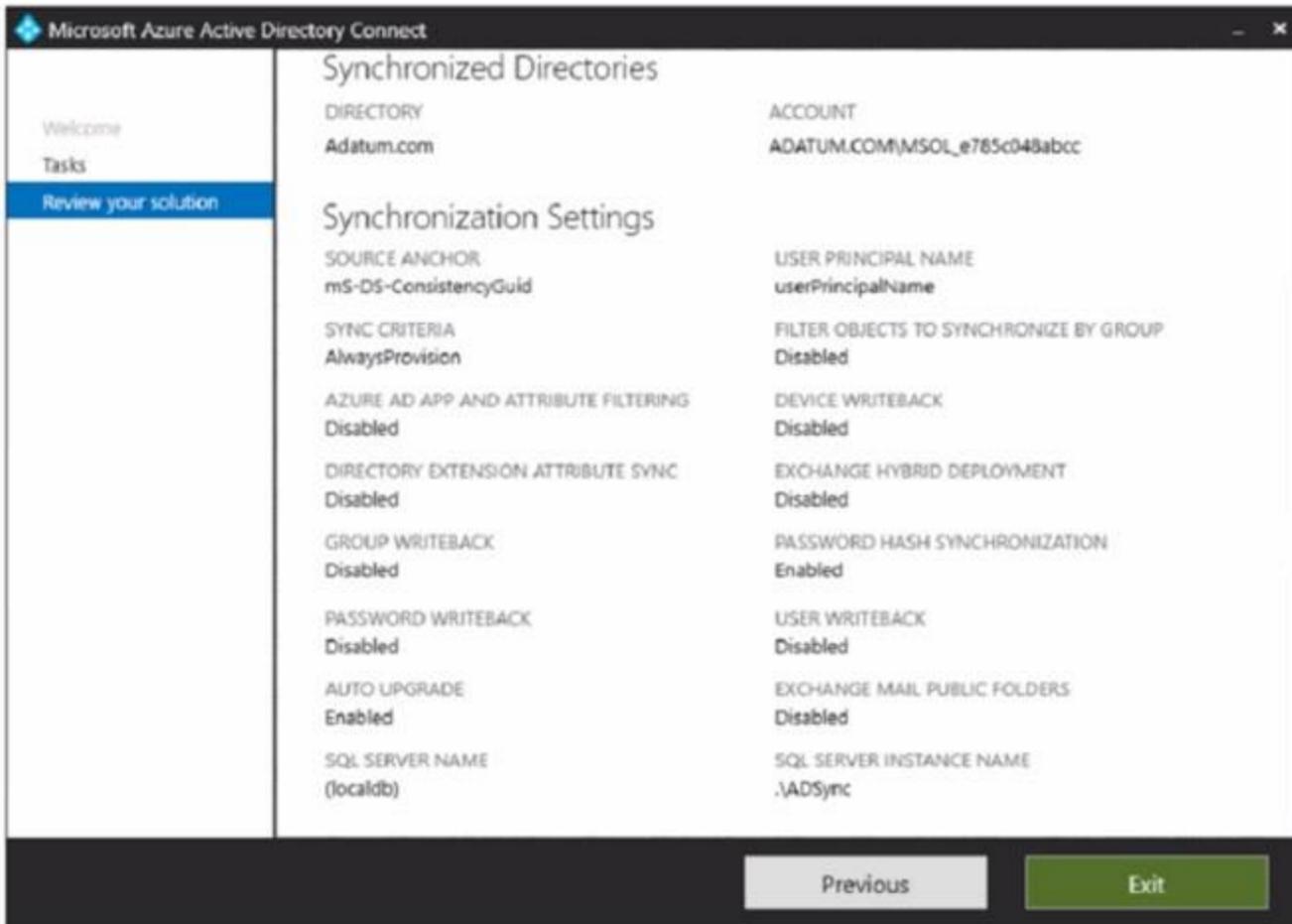
An on-premises Active Directory user account named Allan You is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan @>ddatum.onmicrosoft.com.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 113
HOTSPOT - (Topic 6)
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:

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

NEW QUESTION 116
- (Topic 6)
Your network contains three Active Directory forests. There are forests trust relationships between the forests.
You create an Azure AD tenant.
You plan to sync the on-premises Active Directory to Azure AD.
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.
What should you include in the recommendation?

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

Answer: A

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

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

NEW QUESTION 121
- (Topic 6)
You have a Microsoft 365 E5 subscription.
From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.
What is the longest time range that can be included in the report?

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

Answer: C

Explanation:
View email security reports in the Microsoft 365 Defender portal
The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email- security

NEW QUESTION 125
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Reports Reader
User2	Exchange Administrator
User3	User Experience Success Manager

Which users can review the Adoption Score in the Microsoft 365 admin center?

A. User! only
B. User2onry
C. User1 and User2 only
D. User! and User3 only
E. User1, User2. and User3

Answer: E

NEW QUESTION 129
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.
You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.
On Thursday, you review the results of the app deployments.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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
Word is installed on Device1.		
App3 is displayed in the Company Portal.	○	○
Excel is installed on Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Word is installed on Device1.		
App3 is displayed in the Company Portal.		○
Excel is installed on Device1.		○

NEW QUESTION 134
- (Topic 6)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.
You plan to use a configuration profile to assign the Delivery Optimization settings. Which devices will support the settings?

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

Answer: A

NEW QUESTION 135
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	None

You create an administrative unit named AU1 that contains the members shown in the following exhibit.

AU1

Members   Role assignments

Add users and groups, or select and remove them. The administrators assigned to this unit will
manage these users and groups. Adding groups doesn't add users to the unit, it lets the assigned
admins manage group settings.

☐ Add users   ☒ Add groups   ⤒ Upload users   ···   ▽ Filter   🔍 Search this list   ☰

	Members	Email address	Last sign-in	Member type
☐	User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User
☐	User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User

General   Assigned   Permissions

You can assign this role to users and groups. and select users and groups to remove
or manage them.

Learn more about assigning admin roles

☐ Add users   ☒ Add groups

	Admin name	Last sign-in	Scope ⓘ
☐	Admin name	Last sign-in	Scope ⓘ
☐	**Group1**	Unavailable for groups	Organization
☐	**Group2**	Unavailable for groups	AU1

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 reset the password of User3.	○	○
User2 can reset the password of User3.	○	○
User2 can reset the password of User1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	○	▢
User2 can reset the password of User3.	○	▢
User2 can reset the password of User1.	○	▢

NEW QUESTION 139
DRAG DROP - (Topic 6)
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, of 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 143
- (Topic 6)
You have a Microsoft 365 subscription.
You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples
Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages
Which two components should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a trainable classifier
B. a sensitive info type
C. an insider risk policy
D. an adaptive policy scope
E. a data loss prevention (DLP) policy

Answer: AE

Explanation:
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.
Where you can use classifiers
Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.
Data loss prevention
E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

NEW QUESTION 148
- (Topic 6)
You need to notify the manager of the human resources department when a user in the department shares a file or folder from the 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: D

NEW QUESTION 153
HOTSPOT - (Topic 6)
HOTSPOT
Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

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

The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.
You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)
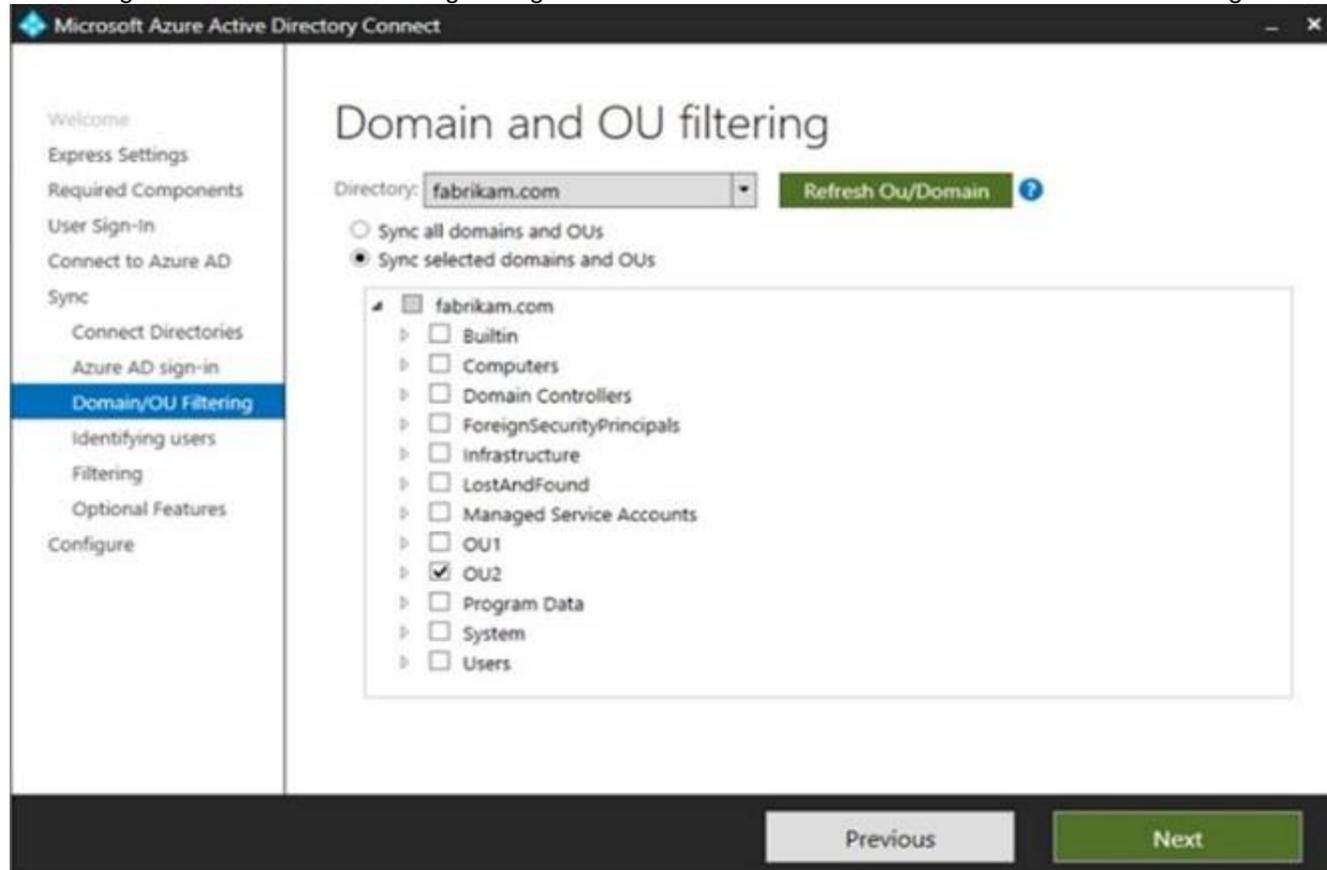
You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)
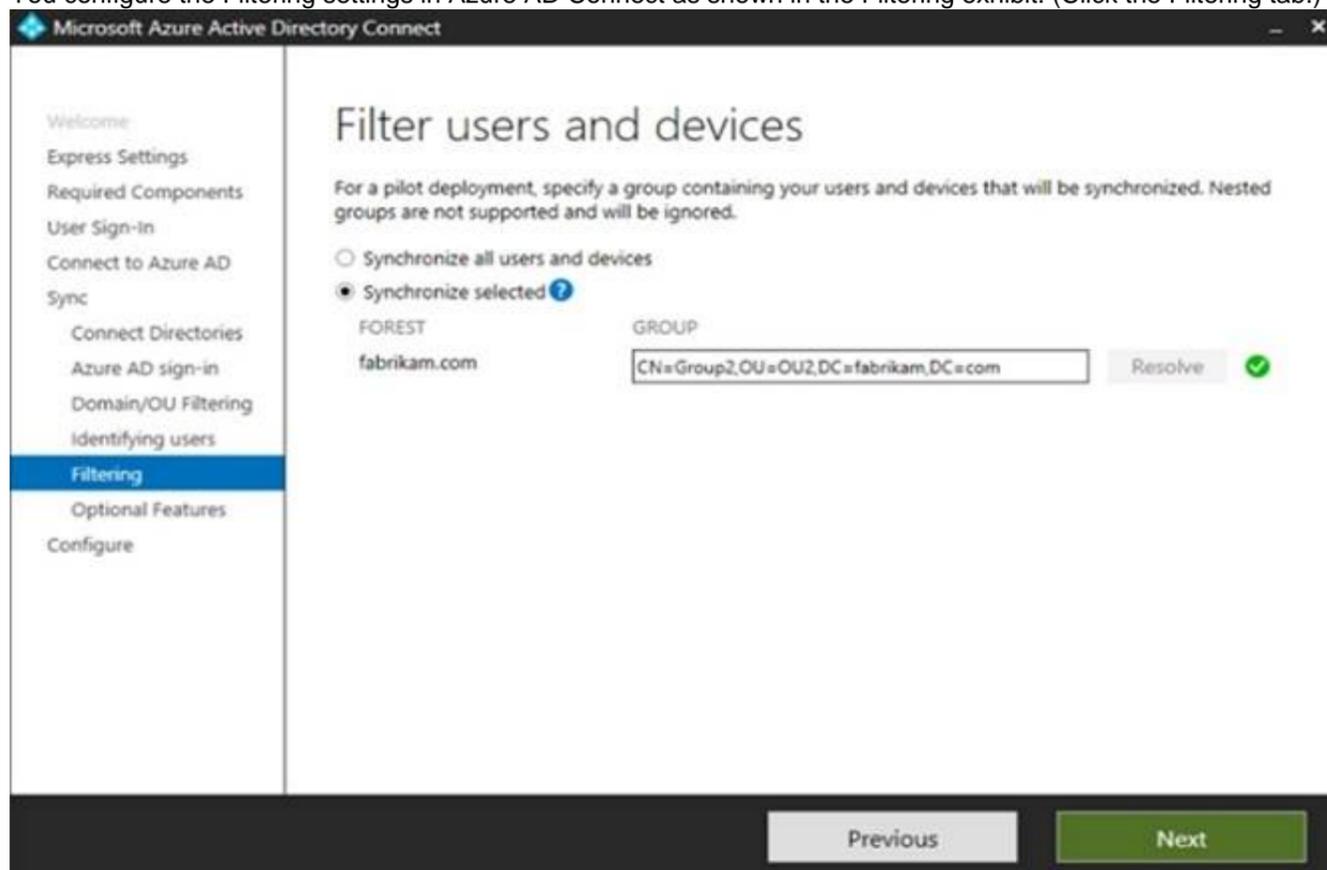
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User2 will synchronize to Azure AD.	⊙	◯
Group2 will synchronize to Azure AD.	◯	◯
User3 will synchronize to Azure AD.	◯	◯

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.
User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD.
Box 2: Yes
Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.
Box 3: Yes
User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD.

NEW QUESTION 154
HOTSPOT - (Topic 6)
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	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	⊙	◯
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.

NEW QUESTION 159
- (Topic 6)
You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

A. a device configuration policy
B. a device compliance policy
C. a conditional access policy
D. an endpoint detection and response policy

Answer: B

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

NEW QUESTION 160
- (Topic 6)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Platform	Count
Windows 10	50
Android	50
Linux	50

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

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

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

NEW QUESTION 163
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

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

The tenant has a conditional access policy that has the following configurations: Name: Policy1
Assignments:
- Users and groups: Group1

- Cloud aps or actions: All cloud apps
? Access controls:
? Grant, require multi-factor authentication
? Enable policy: Report-only
You set Enabled Security defaults to Yes for the tenant.
For each of the following settings select Yes, if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:
? Conditional Access policies can be enabled in report-only mode.
? During sign-in, policies in report-only mode are evaluated but not enforced.
? Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
? Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

NEW QUESTION 166
- (Topic 6)
Your company has on-premises servers and an Azure AD tenant.
Several months ago, the Azure AD Connect Hearth agent was installed on all the servers. You review the health status of all the servers regularly.
Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.
You suspect that another administrator removed Server1 from the list. You need to ensure that you can view the health status of Server1.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. From Azure Cloud shell, run the Connect-Azure AD cmdlet.
B. From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)
C. From Server1, change the Azure AD Connect Health Services Startup type to Automatic
D. From Windows PowerShell, run the Rejister-ArureADConnectHealthsyncAgent cmdlet.
E. From Server1, reinstall the Azure AD Connect Health agent

Answer: DE

NEW QUESTION 171
HOTSPOT - (Topic 6)
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
? uk.co.certification.simulator.questionpool.PList@184e72e0
? MAM user scope: Some
? uk.co.certification.simulator.questionpool.PList@184e7360 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	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	[○]	○
User1 can enroll Device2 in Intune by using automatic enrollment	[○]	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	[○]

NEW QUESTION 172
DRAG DROP - (Topic 6)
You have a Microsoft 365 subscription.
You need to meet the following requirements:
• Report a Microsoft 365 service issue.
• Request help on how to add a new user to an Azure AD tenant.
What should you use in the Microsoft 365 admin center? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Features

| Message center |
| New service request |
| Product feedback |
| Service health |

Answer Area

To report issues regarding a Microsoft 365 service: [_____]

To request help on how to add a new user to the tenant: [_____]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Features

| Message center |
| New service request |
| Product feedback |
| Service health |

Answer Area

To report issues regarding a Microsoft 365 service: [New service request]

To request help on how to add a new user to the tenant: [Message center]

NEW QUESTION 173
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain 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 175
- (Topic 6)
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-1-now-included-in-m365-e3/ba-p/3060639

NEW QUESTION 177
HOTSPOT - (Topic 6)
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:
- Add and configure the Diagnostics settings for the Azure Activity Log.
- Add and configure an Azure Log Analytics workspace.
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers:
- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

In Azure: ▼
Add and configure the Diagnostics settings for the Azure Activity Log.
Add and configure an Azure Log Analytics workspace.
Add an Azure Storage account and Azure Cognitive Search
Add an Azure Storage account and a file share.

On the computers: ▼
Create an event subscription.
Modify the membership of the Event Log Readers group.
Enroll in Microsoft Endpoint Manager.
Install the Microsoft Monitoring Agent.

NEW QUESTION 179
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to use a mailbox named Mailbox1 to analyze malicious email messages. You need to configure Microsoft Defender for Office 365 to meet the following requirements:
• Ensure that incoming email is NOT filtered for Mailbox1.
• Detect impersonation and spoofing attacks on all other mailboxes in the subscription. Which two settings should you configure? To answer, select the appropriate settings in the
answer area.

Answer Area

Policies

🛡	Anti-phishing
📧	Anti-spam
🐛	Anti-malware
📎	Safe Attachments
🔗	Safe Links

Rules

⊖	Tenant Allow/Block Lists
🔍	Email authentication settings
🔍	DKIM
⊕	Advanced delivery
🔽	Enhanced filtering
🔄	Quarantine policies

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments. This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.
? Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

NEW QUESTION 181
- (Topic 6)
You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

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

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform.
Which two tasks should you identify? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Delete User2 and User4 only.
B. Reset the password of User4 only

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

Answer: AE

Explanation:
Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).
Only on users who are non-admins or in any of the following limited admin roles:
• Directory Readers
• Guest Inviter
• Helpdesk Administrator
• Message Center Reader
• Reports Reader
• User Administrator Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles

NEW QUESTION 183
- (Topic 6)
You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.
You need to prevent the users from bypassing the DLP policy. What should you configure?

A. actions
B. incident reports
C. exceptions
D. user overrides

Answer: D

Explanation:
A DLP policy can be configured to allow users to override a policy tip and report a false positive.
You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention- policies

NEW QUESTION 184
- (Topic 6)
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center. Which Microsoft service source will appear on the Incidents page of the Microsoft 365
security center?

A. Microsoft Cloud App Security
B. Azure Sentinel
C. Azure Web Application Firewall
D. Azure Defender

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- alerts?view=o365-worldwide

NEW QUESTION 188
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours.
You plan to sync contoso.com to an Azure AD tenant.
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?

A. pass-through authentication
B. conditional access policies
C. password synchronization
D. Azure AD Identity Protection policies

Answer: A

Explanation:
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

NEW QUESTION 191

- (Topic 6)
You enable the Azure AD Identity Protection weekly digest email. You create the users shown in the following table.

Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

Which users will receive the weekly digest email automatically?

A. Admin2, Admin3, and Admin4 only
B. Admin1, Admin2, Admin3, and Admin4
C. Admin2 and Admin3 only
D. Admin3 only
E. Admin1 and Admin3 only

Answer: E

Explanation:
By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or
Security Administrators will automatically be added to the recipients list.

NEW QUESTION 192
HOTSPOT - (Topic 6)
Your company has a Microsoft 365 tenant
You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)
The device type restriction are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restriction are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restriction-priority
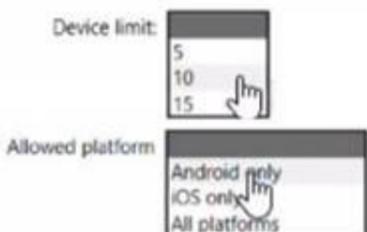
NEW QUESTION 197
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From 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 201
HOTSPOT - (Topic 6)
Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Device group	Member
1	Group1	Name starts with Comp
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped devices (default)	Not applicable

You onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer! and Computed members? To answer, select the appropriate options in The answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1: Group1 only
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Computer2: Group1 only
- Group1 only
- Group3 only
- Group1 and Group3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1: Group1 only
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped devices

Computer2: Group1 only
- Group1 only
- Group3 only
- Group1 and Group3

NEW QUESTION 206
- (Topic 6)
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 Exchanqe Online and SharePoint Online only
D. Microsoft Teams and SharePoint Online only
E. Microsoft Teams, Exchanqe 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 211
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You ate implementing Microsoft Defender for Endpoint
You need to enable role-based access control (RBAQ to restrict access to the Microsoft 365 Defender portal.
Which users can enable RBAC, and winch users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point.

Answer Area

Users that can enable RBAC: | Admin1 and Admin2 only ▼
Admin1 only
Admin1 and Admin2 only
Admin1, Admin2, and Admin5 only
Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal: | Admin3, Admin4, and Admin5 only ▼
Admin5 only
Admin3 and Admin4 only
Admin4 and Admin5 only
Admin3, Admin4, and Admin5 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Users that can enable RBAC: | Admin1 and Admin2 only ▼
Admin1 only
Admin1 and Admin2 only
Admin1, Admin2, and Admin5 only
Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal: | Admin3, Admin4, and Admin5 only ▼
Admin5 only
Admin3 and Admin4 only
Admin4 and Admin5 only
Admin3, Admin4, and Admin5 only

NEW QUESTION 216
HOTSPOT - (Topic 6)
HOTSPOT
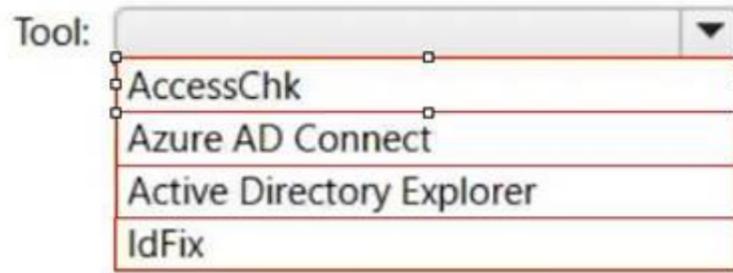Your network contains an on-premises Active Directory domain. You have a Microsoft 365 E5 subscription.
You plan to implement directory synchronization.
You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.
What should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Tool:
AccessChk
Azure AD Connect
Active Directory Explorer
IdFix

Required group membership:
Domain Admins
Domain Users
Server Operators
Enterprise Admins

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: IdFix
Query and fix invalid object attributes with the IdFix tool
Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.
The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Window's Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.
Incorrect:
* AccessChk
Box 2: Enterprise Admins
IdFix permissions requirements
The user account that you use to run IdFix must have read and write access to the AD DS domain.
If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.
* Enterprise Admins
The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.
Incorrect:
* Domain Admins
Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.
* Server Operator
Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.
* Domain Users - too few permissions
The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

NEW QUESTION 218
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

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 221
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

You need to enable user access to the partner company's portal. Which Microsoft Defender for Endpoint setting should you modify?

A. Alert notifications
B. Alert suppression
C. Custom detections
D. Advanced hunting
E. Indicators

Answer: E

Explanation:
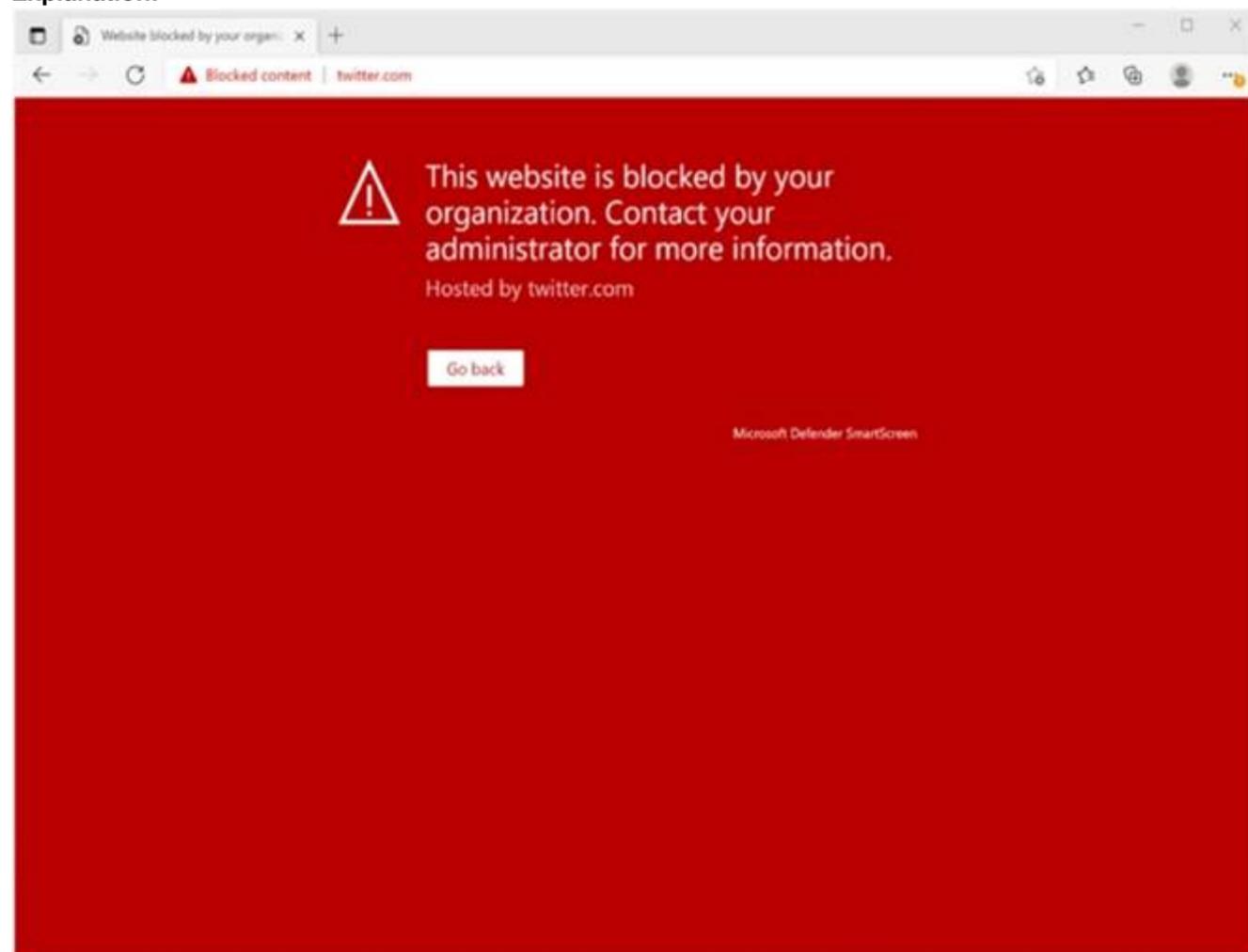
This Website Is Blocked By Your Organization
Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.
Reference: https://jadexstrategic.com/web-protection/

NEW QUESTION 223
HOTSPOT - (Topic 6)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)
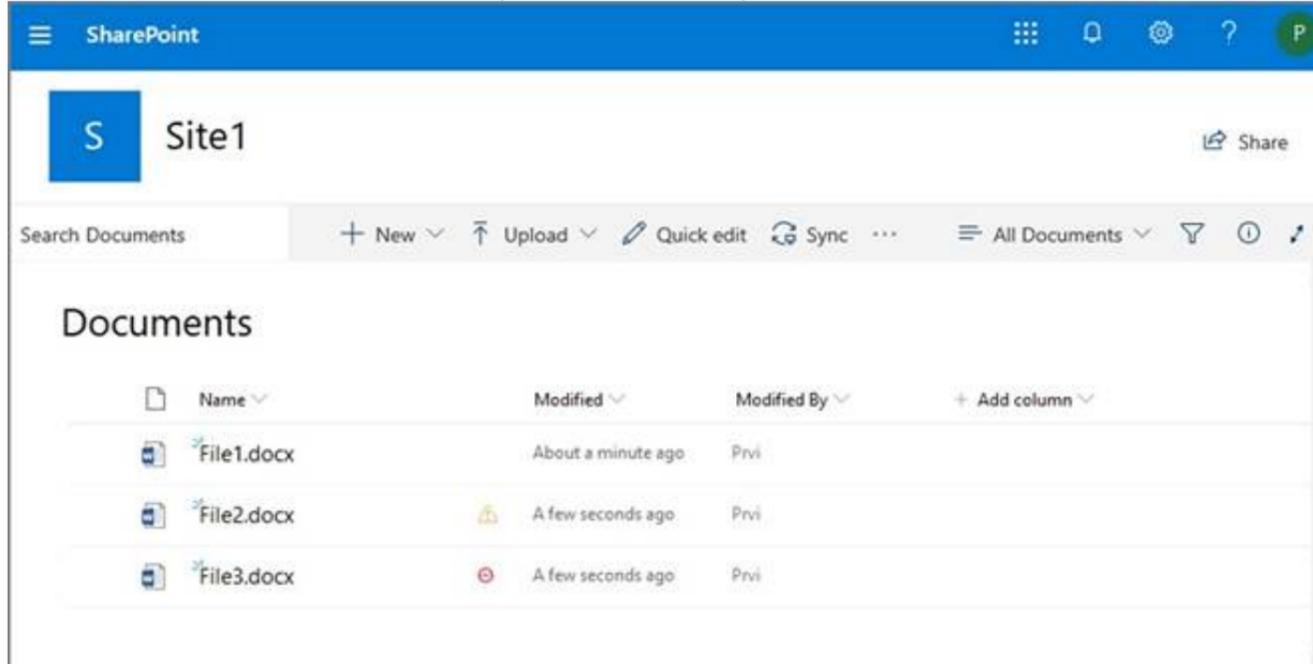
Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

A. Mastered
B. Not Mastered

Answer: A

Explanation:

User1:
- File1.docx only
- File1.docx and File2.docx only
- **File1.docx, File2.docx, and File3.docx**

User2:
- **File1.docx only**
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

NEW QUESTION 226
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.
All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).
You plan to create a user named Admin1 that will perform following tasks:
• View BitLocker recovery keys.

• Configure the usage location for the users in contoso.com.
You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.
NOTE: Each correct selection is worth one point

Answer Area

Devices

☐ Cloud Device Administrator ⓘ

☐ Desktop Analytics Administrator ⓘ

☐ Intune Administrator ⓘ

☐ Printer Administrator ⓘ

☐ Printer Technician ⓘ

☐ Windows 365 Administrator ⓘ

Global

☐ Global Administrator ⓘ

Identity

☐ Application Administrator ⓘ

☐ Application Developer ⓘ

☐ Authentication Administrator ⓘ

☐ Cloud Application Administrator ⓘ

☐ Conditional Access Administrator ⓘ

☐ Domain Name Administrator ⓘ

☐ External Identity Provider Administrator ⓘ

☐ Guest Inviter ⓘ

☐ Helpdesk Administrator ⓘ

☐ Hybrid Identity Administrator ⓘ

☐ License Administrator ⓘ

☐ Password Administrator ⓘ

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

NEW QUESTION 231
DRAG DROP - (Topic 6)
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:

NEW QUESTION 235
- (Topic 6)
You have a Microsoft 365 subscription that uses Security & Compliance retention policies.
You implement a preservation lock on a retention policy that is assigned to all executive users.
Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point?

A. Add locations to the policy
B. Reduce the duration of policy
C. Remove locations from the policy
D. Extend the duration of the policy
E. Disable the policy

Answer: AB

NEW QUESTION 240
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it As a result these questions will not appear in the review screen.
Your network contains an Active Directory forest. You deploy Microsoft 365.
You plan to implement directory synchronization.
You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:
• Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
• User passwords must be 10 characters or more.
Solution: implement password hash synchronization and configure password protection in the Azure AD tenant.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 244
HOTSPOT - (Topic 6)
You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.
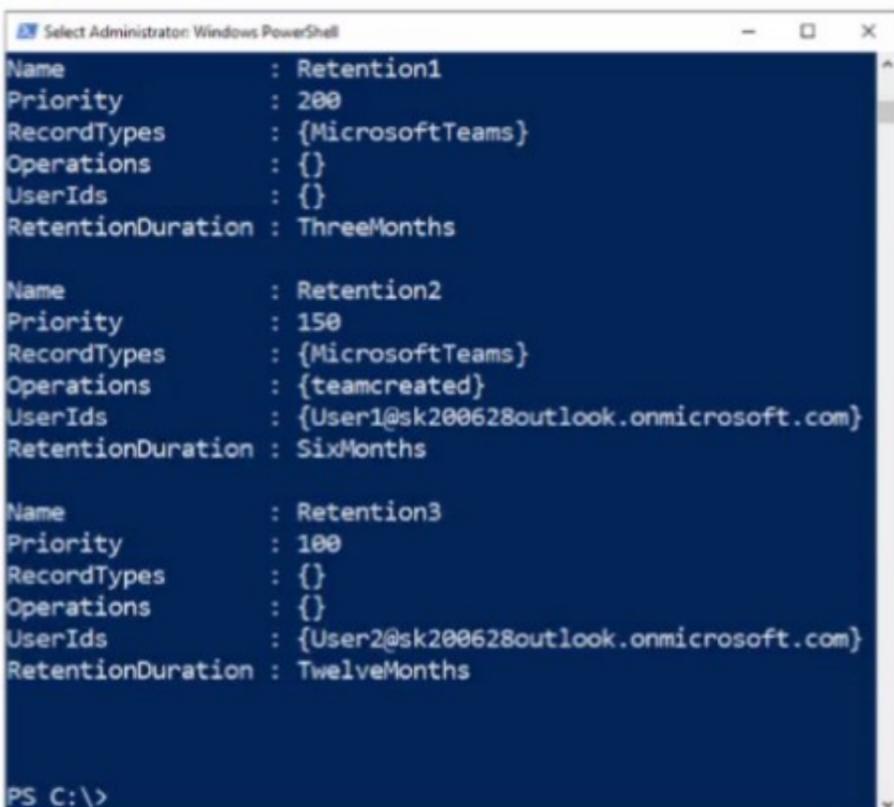
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic NOTE Each correct selection is worth one point.

Answer Area

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

| not retained |
| retained for 90 days |
| retained for six months |
| retained for one year |

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

| not retained |
| retained for 90 days |
| retained for six months |
| retained for one year |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

| not retained |
| retained for 90 days |
| retained for six months |
| retained for one year |

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

| not retained |
| retained for 90 days |
| retained for six months |
| retained for one year |

NEW QUESTION 246
DRAG DROP - (Topic 6)
Your company purchases a cloud app named App1.
You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

| Deploy Azure Active Directory (Azure AD) Application Proxy. |
| From the Cloud App Security admin center, add an app connector. |
| Sign in to App1. |
| Create a conditional access policy. |
| From the Azure Active Directory admin center, configure the Diagnostic settings. |
| From the Azure Active Directory admin center, add an app registration for App1. |

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.

Answer Area

- From the Cloud App Security admin center, add an app connector.
- Create a conditional access policy.
- Sign in to App1.
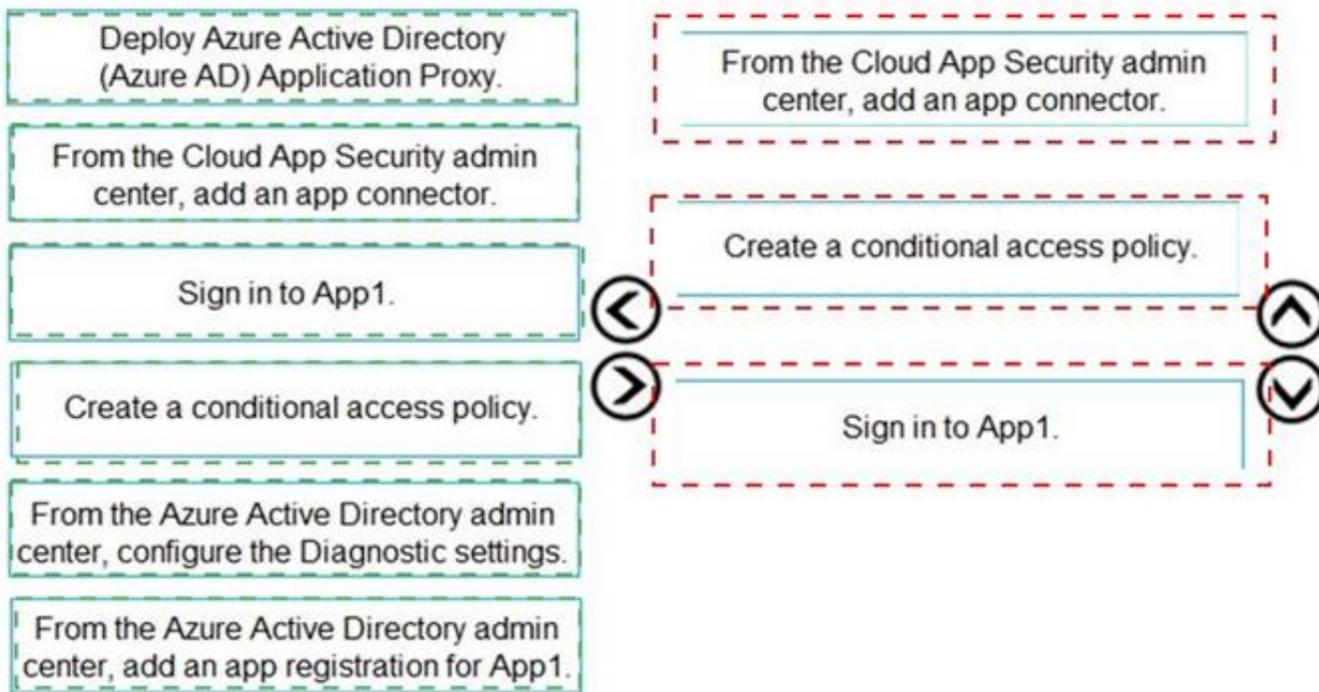
NEW QUESTION 250
- (Topic 6)
You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is 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 255
- (Topic 6)
You have a Microsoft 365 E5 subscription.
Users have the devices shown in the following table.

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

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

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

Answer: C

Explanation:
You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

NEW QUESTION 256
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Endpoint security.

You need to create a group and assign the Endpoint Security Manager role to the group. Which type of group can you use?

A. Microsoft 365 only
B. security only
C. mail-enabled security and security only
D. mail-enabled security, Microsoft 365, and security only
E. distribution, mail-enabled security, Microsoft 365, and security

Answer: D

NEW QUESTION 259
HOTSPOT - (Topic 6)
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: Microsoft Endpoint Manager ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2: A local script ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Device1: Microsoft Endpoint Manager ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

Device2: A local script ▼
A local script
Group Policy
Microsoft Endpoint Manager
An app from the Google Play store
Integration with Microsoft Defender for Cloud

NEW QUESTION 262
- (Topic 6)
You have the sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels   Label policies   Auto-labeling(preview)

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

+ Create a label   🖵 Publish labels   ↻ Refresh

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

Which labels can users apply to content?

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

Answer: D

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

NEW QUESTION 265
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed. Solution: From Device Manager, you view the computer properties. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 270
- (Topic 6)
You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.
To which users can User! send documents that contain PII?

A. User2only
B. User2and User3only
C. User2, User3, and User4 only
D. User2, User3, User4, and User5

Answer: B

NEW QUESTION 273
- (Topic 6)
You have a Microsoft 365 subscription.
You need to receive a notification each time a user in the service desk department grants Full Access permissions for a user mailbox.
What should you configure?

A. a data loss prevention (DLP) policy
B. an alert policy
C. an audit search
D. an insider risk management policy

Answer: B

NEW QUESTION 277
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:
• Create a sensitive info type named SIT1 based on a regular expression.
• Add a watermark to all new documents that are matched by SIT1.
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Purview

- Home
- Compliance Manager
- Data classification
- Data connectors
- Reports

Solutions

- Catalog
- App governance
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery ⌄
- Data lifecycle management ⌄
- Information protection
- Information barriers ⌄
- Insider risk management
- Records management
- Privacy risk management ⌄
- Subject rights requests

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft Purview

☰

🏠 Home

🏆 Compliance Manager

🛇 Data classification

🎛 Data connectors

📈 Reports

Solutions

⊞ Catalog

⊞ App governance

📄 Audit

🔍 Content search

🗨 Communication compliance

🔒 Data loss prevention

🏛 eDiscovery ⌄

🗄 Data lifecycle management ⌄

🔒 Information protection

🔒 Information barriers ⌄

👤 Insider risk management

📊 Records management

🖐 Privacy risk management ⌄

🗂 Subject rights requests

NEW QUESTION 279
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange 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 280
FILL IN THE BLANK - (Topic 6)
You have a Microsoft 365 tenant.
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

| Save the audit logs to: | [dropdown] |

| Azure Active Directory admin center blade to use to view the saved audit logs: | [dropdown] |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

| Save the audit logs to: | Azure Log Analytics |

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

NEW QUESTION 284
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to configure Microsoft Defender for Office 365 to meet the following requirements:
• A user's email sending patterns must be used to minimize false positives for spoof protection.
• Documents uploaded to Microsoft Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365.
What should you configure for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:	Domains to protect
	Domains to protect
	Mailbox intelligence
	Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:	Global settings for safe attachments
	Global settings for safe attachments
	The Safe Attachments policy settings
	The Safe Links policy settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:	Domains to protect
	Domains to protect
	Mailbox intelligence
	Users to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:	Global settings for safe attachments
	Global settings for safe attachments
	The Safe Attachments policy settings
	The Safe Links policy settings

NEW QUESTION 285
- (Topic 6)
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. Used only1
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 289
- (Topic 6)
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 290
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table.
You create the device configuration profiles shown in the following table.

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

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Device1:
- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device2:
- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Device1:

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

Device2:

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

NEW QUESTION 291
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain 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 assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION 294
HOTSPOT - (Topic 6)
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
? Only show page to devices provisioned by out-of-box experience (OOBE): No
? 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.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[○]
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	[○]	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[○]

NEW QUESTION 296
DRAG DROP - (Topic 6)
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

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

The email will be blocked, and the user will receive the policy tip: Message contains sensitive 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.

Answer Area

When the user sends an email that contains financial data and health records: Result

When the user sends an email that contains only financial data: Result

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.

NEW QUESTION 300
- (Topic 6)
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 305
- (Topic 6)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select Update & Security to view the update history. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 306
HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:
? Assignments: All users
? Controls: Require Azure AD multifactor authentication registration
? Enforce Policy: On
? On August 3, you create two users named User1 and User2.
Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:
▼
August 6
August 17
August 19
September 3
September 5

User2:
▼
August 8
August 17
August 19
August 21
September 7

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: August 19
Note: Security defaults will trigger a 14 day grace period for registration after a user's first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.
Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period. Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi- Factor Authentication, then the user must be able to pass that MFA request.
Box 2: August 21

NEW QUESTION 311
HOTSPOT - (Topic 6)
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-do-date	**Require**	Not configured
Real-time protection ⓘ	**Require**	Not configured

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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-do-date ⓘ	Require	Not configured
Real-time protection ⓘ	Require	Not configured

NEW QUESTION 313
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.
Which conditions can you use in the DLP rules of the policy?

A. sensitive info types
B. content search queries
C. keywords
D. sensitivity labels

Answer: C

Explanation:
Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:
Specific types of sensitive information.
Specific keywords that match a query you create.
Pattern matches for a trainable classifier.
Note: Retention policies can be applied to the following locations: Exchange mailboxes
SharePoint classic and communication sites OneDrive accounts
Microsoft 365 Group mailboxes & sites Skype for Business
Exchange public folders
Teams channel messages (standard channels and shared channels) Teams chats
Teams private channel messages Yammer community messages Yammer user messages
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions

NEW QUESTION 314
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to create the data loss prevention (DLP) policies shown in the following table.

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

You need to create DLP rules for each policy.
Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Sender is condition:
```
DLP1 only                    ▼
DLP1 only
DLP2 only
DLP3 only
DLP2 and DLP3 only
DLP1, DLP2, and DLP3
```

File extension is condition:
```
DLP1, DLP2, and DLP3         ▼
DLP1 only
DLP2 only
DLP3 only
DLP2 and DLP3 only
DLP1, DLP2, and DLP3
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Sender is condition:
```
DLP1 only                    ▼
DLP1 only
DLP2 only
DLP3 only
DLP2 and DLP3 only
DLP1, DLP2, and DLP3
```

File extension is condition:
```
DLP1, DLP2, and DLP3         ▼
DLP1 only
DLP2 only
DLP3 only
DLP2 and DLP3 only
DLP1, DLP2, and DLP3
```

NEW QUESTION 319
HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.

Group1

Private group ● 1 owner ● 1 member

General   Members   **Settings**   Microsoft Teams

General settings

☐ Allow external senders to email this group

☑ Send copies of group conversations and events to group members

☐ Hide from my organization's global address list

Privacy

◉ Private

○ Public

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

Answer Area

Action: ▼

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

Portal: ▼

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Invite User1 to collaborate with your organization as a guest.
To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps.
Navigate with your Web browser to https://admin.microsoft.com. On the left pane, click on "Users", then click "Guest Users".
On the "Guest Users" page, to create a new guest user, click on either the "Add a guest user" link on the top of the page or click on "Go to Azure Active Directory to add guest users" link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.com.
On the "New user" page in the Microsoft Azure portal, you must choose to either "Create user" or "Invite user". If you choose the "Create user" option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the "Invite user" option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the "Invite user" option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Azure AD with family of identity and access products
Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.

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

NEW QUESTION 324
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.
The subscription has the following two anti-spam policies:
• Name: AntiSpam1
• Priority: 0
• Induce these users, groups and domains o Users: User3
o Groups: Group!
• Exclude these users, groups and domains o Groups: Group2
• Message limits
o Set a daily message limit 100
• Name: AntiSpam2
• Priority: 1
• Include these users, groups and domains o Users: User! o Groups: Group2
• Exclude these users, groups and domains o Users: User3
• Message limits
o Set a daily message limit 50
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	○	○
User2 can send a maximum of 50 email messages per day.	○	○
User3 can send a maximum of 100 email messages per day.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	○	⊡
User2 can send a maximum of 50 email messages per day.	⊡	○
User3 can send a maximum of 100 email messages per day.	⊡	○

NEW QUESTION 328
- (Topic 6)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You need to access service health alerts from a mobile phone.
What should you use?

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

Answer: B

NEW QUESTION 329
- (Topic 6)
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 334
- (Topic 6)
You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?

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

Answer: A

Explanation:
Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.
Note: Permissions alert policies
Example: Elevation of Exchange admin privilege
Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies

NEW QUESTION 338
- (Topic 6)
Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.
Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com.
You plan to install Azure AD Connect on a member server and implement pass-through authentication.
You need to prepare the environment for the planned implementation of pass-through authentication.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: ABE

Explanation:
Deploy Azure AD Pass-through Authentication Step 1: Check the prerequisites
Ensure that the following prerequisites are in place. In the Entra admin center
* 1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.
(E) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.
(A) In your on-premises environment
* 1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.
* 2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is supported.
* 3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.
* 4. Etc.
(B) Step 2: Enable the feature
Enable Pass-through Authentication through Azure AD Connect.
If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.
Incorrect:
Not C: From Active Directory Domains and Trusts, add a UPN suffix Not D. Modify the email address attribute for each user account. Not F. Modify the User logon name for each user account.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta- quick-start

NEW QUESTION 343
- (Topic 6)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview policies to meet the following requirements: Identify documents that are stored in Microsoft Teams and SharePoint that

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

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

Answer: A

Explanation:
Demonstrate data protection
Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.
There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.
? From the Security & Compliance tab of your browser, click Home.
? Click Data loss prevention > Policy.
? Click + Create a policy.
? In Start with a template or create a custom policy, click Custom > Custom policy > Next.
? In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy b. Description: Protect the personally identifiable information of European citizens
? Etc.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment

NEW QUESTION 346
- (Topic 6)
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
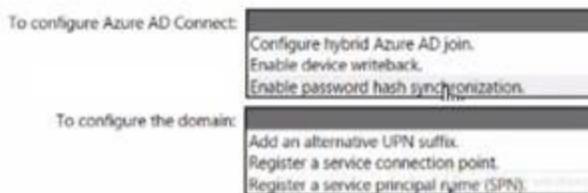What can you configure as the minimum number of days before a device a removed automatically?

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

Answer: D

NEW QUESTION 350
HOTSPOT - (Topic 6)
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.
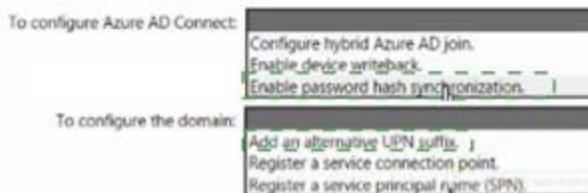
Answer Area

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 351
HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription. You need to meet the following requirements:
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label. Which two settings should you use in the Microsoft Purview compliance

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

Answer Area

Solutions
⊞ Catalog
🗎 Audit
🔍 Content search
🗩 Communication compliance
🗎 Data loss prevention
🏛 eDiscovery ⌄
🗄 Data lifecycle management
🗎 Information protection
🗎 Information barriers ⌄
👤 Insider risk management
🗎 Records management
🗎 Priva Privacy Risk Managem... ⌄
🗎 Priva Subject Rights Requests
⚙ Settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Information protection
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection
All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files
without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.
To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels:
In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.
Note: Encryption of data at rest
Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.
BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology. Box 2: Settings
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

NEW QUESTION 354
......

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