Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator

NEW QUESTION 1
An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.

What should you do to meet the security requirements?

A. Change the Assignment Type for Admin2 to Permanent
B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
D. Change the Assignment Type for Admin1 to Eligible

Answer: D

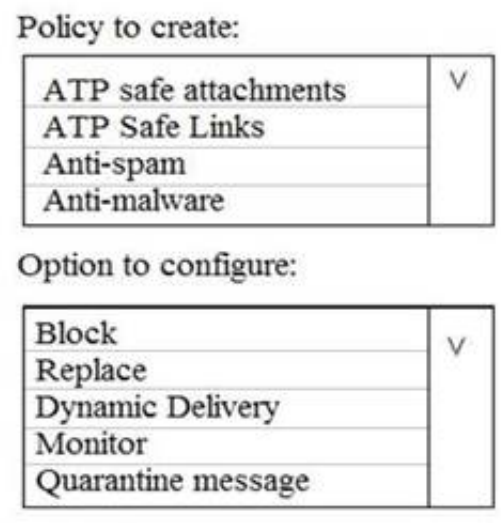
NEW QUESTION 2
You need to recommend a solution for the user administrators that meets the security requirements for auditing.
Which blade should you recommend using from the Azure Active Directory admin center?

A. Sign-ins
B. Azure AD Identity Protection
C. Authentication methods
D. Access review

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

NEW QUESTION 3
HOTSPOT
You need to recommend an email malware solution that meets the security requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Policy to create:

ATP safe attachments
ATP Safe Links
Anti-spam
Anti-malware

Option to configure:

Block
Replace
Dynamic Delivery
Monitor
Quarantine message

NEW QUESTION 4
HOTSPOT
You install Azure ATP sensors on domain controllers.
You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.
You need to meet the security requirements for Azure ATP reporting.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Policy to edit:

Default Domain Controllers Policy
Default Domain Policy
A local policy on one domain controller

Audit setting to configure:

Audit User Account Management
Audit Computer Account Management
Audit Other Account Management Events
Audit Security Group Management

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy

NEW QUESTION 5
You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.
What should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
A. Create an access review.
B. Assign the Global administrator role to User1.
C. Assign the Guest inviter role to User1.
D. Modify the External collaboration settings in the Azure Active Directory admin center.

Answer: AC

NEW QUESTION 6
You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

A. Synchronization Service Manager
B. Azure AD Connect wizard
C. Synchronization Rules Editor
D. IdFix

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization
Case Study: 2 Litware, Inc Overview
Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in
a branch office in San Francisco.
Existing Environment
Internal Network Infrastructure
The network contains a single domain forest. The forest functional level is Windows Server 2016. Users are subject to sign-in hour restrictions as defined in Active

Directory.
The network has the IP address range shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).
The following operating systems are used on the network:
•Windows Server 2016
•Windows 10 Enterprise
•Windows 8.1 Enterprise
The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.
Cloud Infrastructure
Litware recently purchased Microsoft 365 subscription licenses for all users.
Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.
You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes
Litware plans to implement the following changes: Migrate the email system to Microsoft Exchange Online Implement Azure AD Privileged Identity Management
Security Requirements
Litware identities the following security requirements:
•Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
•Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
•Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
•Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
•Implement a permanent eligible assignment of the Compliance administrator role for User1
•Integrate Windows Defender and Windows Defender ATP on domain-joined servers
•Prevent access to Azure resources for the guest user accounts by default
•Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts. You identify the following requirements for testing MFA.
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location Any disruption of legitimate authentication attempts must be minimized
General Requirements
Litware want to minimize the deployment of additional servers and services in the Active Directory forest.

NEW QUESTION 7
Which IP address space should you include in the MFA configuration?

A. 131.107.83.0/28
B. 192.168.16.0/20
C. 172.16.0.0/24
D. 192.168.0.0/20

Answer: B

NEW QUESTION 8
You need to implement Windows Defender ATP to meet the security requirements. What should you do?

A. Configure port mirroring
B. Create the ForceDefenderPassiveMode registry setting
C. Download and install the Microsoft Monitoring Agent
D. Run WindowsDefenderATPOnboardingScript.cmd

Answer: C

Explanation:
Case Study: 3 Contoso, Ltd Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, and New York.
The company has the offices shown in the following table.

Location	Employees	Laptops	Desktops computers	Mobile devices
Montreal	2, 500	2, 800	300	3, 100
Seattle	1, 000	1, 100	200	1, 500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.
Existing Environment Infrastructure
The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.
The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.
Each client computer has a single volume.
Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.
Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department. The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	User.city-contains “SEA”
ADGroup2	Office 365	User.city-match “Sea”

Customer Lockbox is enabled in Microsoft 365. Microsoft Intune Configuration
The devices enrolled in Intune are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	Not applicable	GroupA
Device6	Windows 10	Enabled	None

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

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

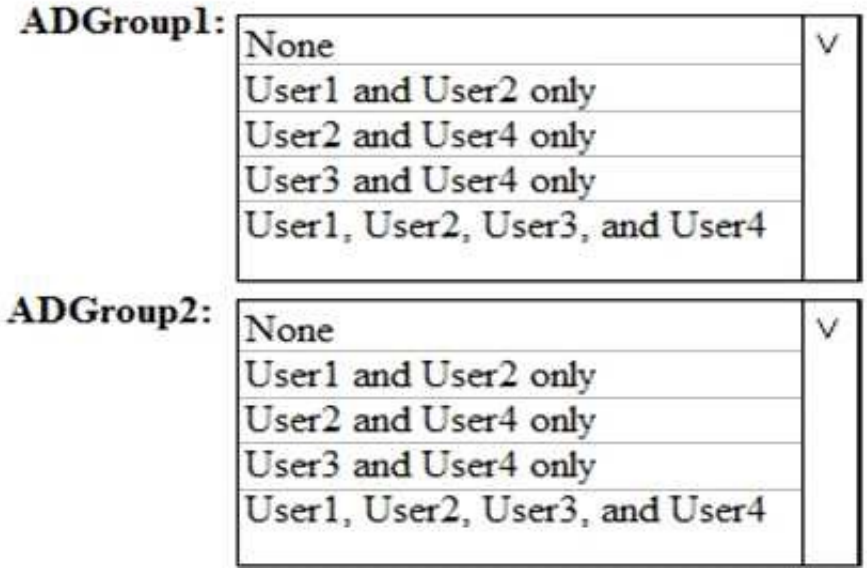
The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

The Mark devices with no compliance policy assigned as setting is set to Compliant.
Requirements
Technical Requirements
Contoso identifies the following technical requirements:
•Use the principle of least privilege
•Enable User1 to assign the Reports reader role to users

•Ensure that User6 approves Customer Lockbox requests as quickly as possible
•Ensure that User9 can implement Azure AD Privileged Identity Management

NEW QUESTION 9
HOTSPOT
Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

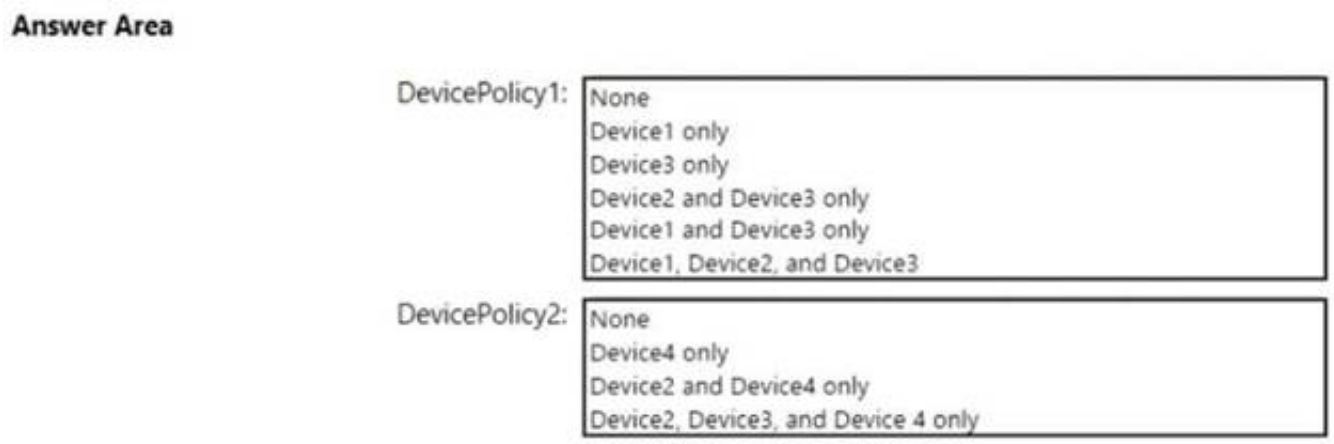
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

NEW QUESTION 10
What should User6 use to meet the technical requirements?

A. Supervision in the Security & Compliance admin center
B. Service requests in the Microsoft 365 admin center
C. Security & privacy in the Microsoft 365 admin center
D. Data subject requests in the Security & Compliance admin center

Answer: B

NEW QUESTION 10
HOTSPOT
Which policies apply to which devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

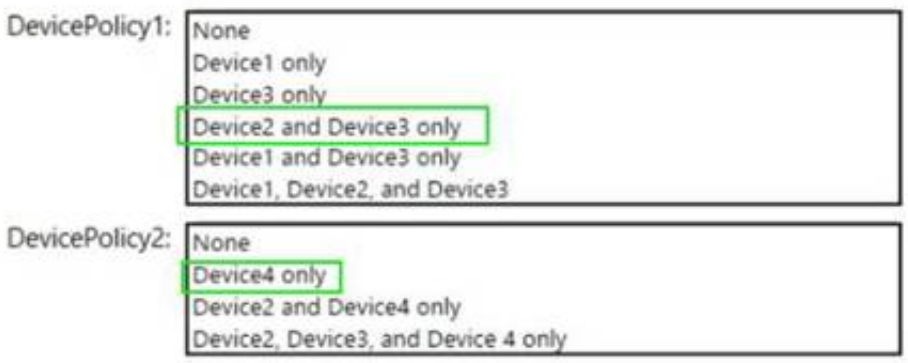


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 13
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 that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports. The Compliance Manager Reader role is not assigned to any users.
You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.
Solution: You recommend assigning the Compliance Manager Reader role to User5. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 17
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:
•Source Anchor: objectGUID
•Password Hash Synchronization: Disabled
•Password writeback: Disabled
•Directory extension attribute sync: Disabled
•Azure AD app and attribute filtering: Disabled
•Exchange hybrid deployment: Disabled
•User writeback: Disabled
You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Azure AD app and attribute filtering settings.
Does that meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 18
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:
•Source Anchor: objectGUID
•Password Hash Synchronization: Disabled
•Password writeback: Disabled
•Directory extension attribute sync: Disabled
•Azure AD app and attribute filtering: Disabled
•Exchange hybrid deployment: Disabled
•User writeback: Disabled
You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Password Hash Synchronization settings.
Does that meet the goal?

A. Yes
B. No

Answer: A

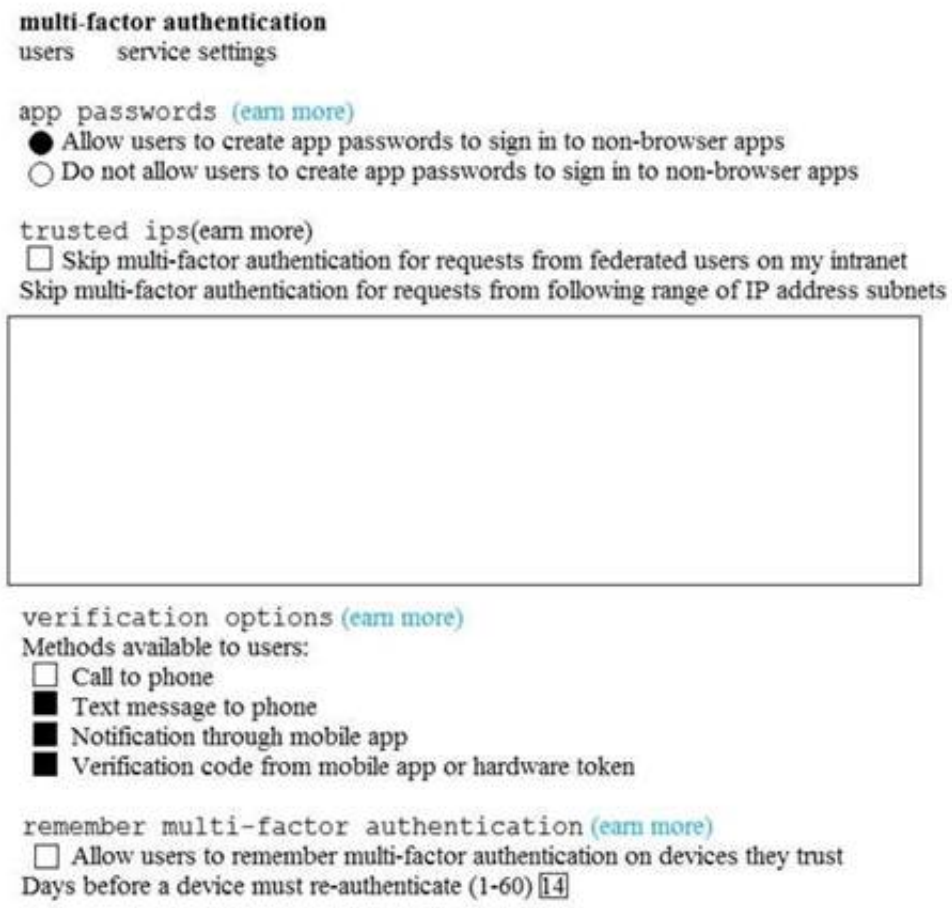
Explanation:
References:
https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

NEW QUESTION 21
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:
•Source Anchor: objectGUID
•Password Hash Synchronization: Disabled
•Password writeback: Disabled
•Directory extension attribute sync: Disabled
•Azure AD app and attribute filtering: Disabled
•Exchange hybrid deployment: Disabled
•User writeback: Disabled
You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.
Solution: You modify the Source Anchor settings.
Does that meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 25
HOTSPOT
You have a Microsoft 365 subscription that uses a default domain name of contoso.com.
The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Clock the Exhibit tab.)



In contoso.com, you create the users shown in the following table.

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

User1:

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

User2:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

User1:

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

User2:

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

NEW QUESTION 27
You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.
You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on- premises network.
What should you do first?

A. From the Azure Active Directory admin center, create a new certificate
B. Enable Application Proxy in Azure AD
C. From Active Directory Administrative Center, create a Dynamic Access Control policy
D. From the Azure Active Directory admin center, configure authentication methods

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn- connectivitywindows10

NEW QUESTION 31
You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you create a new user. You plan to assign the Reports reader role to the user.
You need to see the permissions of the Reports reader role. Which admin center should you use?

A. Azure Active Directory
B. Cloud App Security
C. Security & Compliance
D. Microsoft 365

Answer: A

NEW QUESTION 33
Your company has a Microsoft 365 subscription.
The company forbids users to enroll personal devices in mobile device management (MDM). Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.
The users must be prevented from backing up the app's data to iCloud. What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
B. an app protection policy in Microsoft Intune
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
D. a device compliance policy in Microsoft Intune

Answer: B

NEW QUESTION 35
You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription. You need to allow a user named User1 to view ATP reports in the Threat management dashboard. Which role provides User1with the required role permissions?

A. Security reader
B. Message center reader
C. Compliance administrator
D. Information Protection administrator

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-areneeded-to-view-the-atp-reports

NEW QUESTION 38
You have a Microsoft 365 Enterprise E5 subscription.
You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You plan to use Microsoft Office 365 Attack simulator.
What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA)
B. Configure Advanced Threat Protection (ATP)
C. Create a Conditional Access App Control policy for accessing Office 365
D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

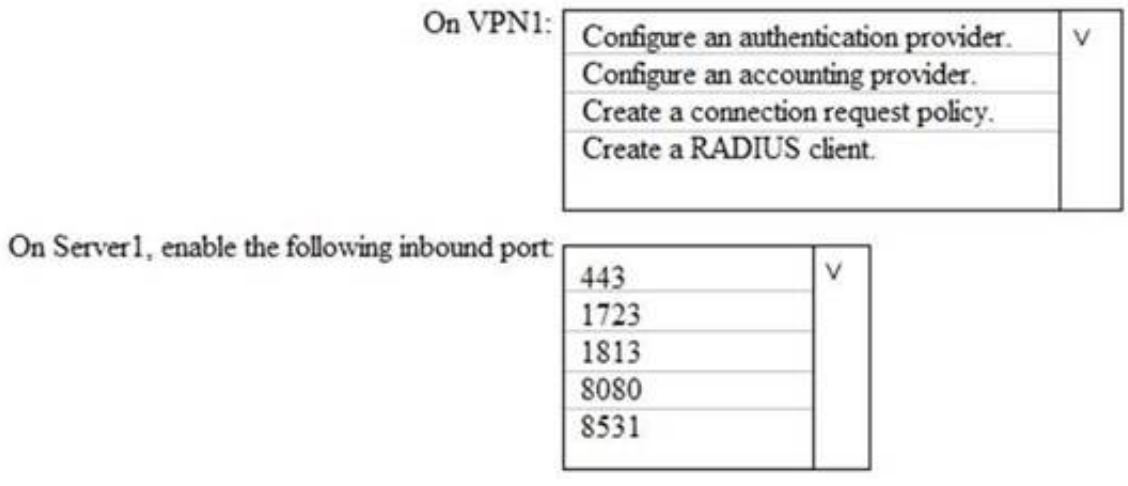
NEW QUESTION 42
You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.
Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.
You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.
The email address that you intend to spoof belongs to the Executive group members. What should you do first?

A. From Azure ATP admin center, configure the primary workspace settings
B. From the Microsoft Azure portal, configure the user risk settings in Azure AD Identity Protection
C. Enable MFA for the Research group members
D. Migrate the Executive group members to Exchange Online

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

NEW QUESTION 43
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed. You have a Microsoft Azure subscription.
You are deploying Azure Advanced Threat Protection (ATP)
You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.
You need to integrate the VPN and Azure ATP.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn

NEW QUESTION 45
HOTSPOT
You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.
You create an app protection policy named ProtectionPolicy1 that has the following settings:
•Protected apps: App1
•Exempt apps: App2
•Windows Information Protection mode: Block
You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1. 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

	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	○
From Device2, User1 can copy data from App1 to App2.	○	○
From Device2, User1 can copy data from App1 to App3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	○
From Device2, User1 can copy data from App1 to App2.	○	○
From Device2, User1 can copy data from App1 to App3.	○	○

NEW QUESTION 46
Your company uses Microsoft Azure Advanced Threat Protection (ATP).
You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1. How long after the Azure ATP cloud service is updated will Sensor1 be updated?

A. 7 days
B. 24 hours
C. 1 hour
D. 48 hours
E. 12 hours

Answer: B

Explanation:
Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

NEW QUESTION 47
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.
You add CompanyConfidential to a global policy.
A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them. Solution: You modify the content expiration settings of the label. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 52
HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1. You need to apply Policy1.
To which groups can you apply Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On-premises Active Directory groups:

Group4 only ∨
Group1 and Group4 only
Group3 and Group4 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

Azure AD groups:

Group13 only ∨
Group13 and Group14 only
Group11 and Group12 only
Group11, Group13, and Group14 only
Group11, Group12,Group13,and Group14 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/prepare

NEW QUESTION 57
HOTSPOT
You have the Microsoft conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.

Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

You have the Azure Information Protection policies shown in the following table.

Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

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

Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

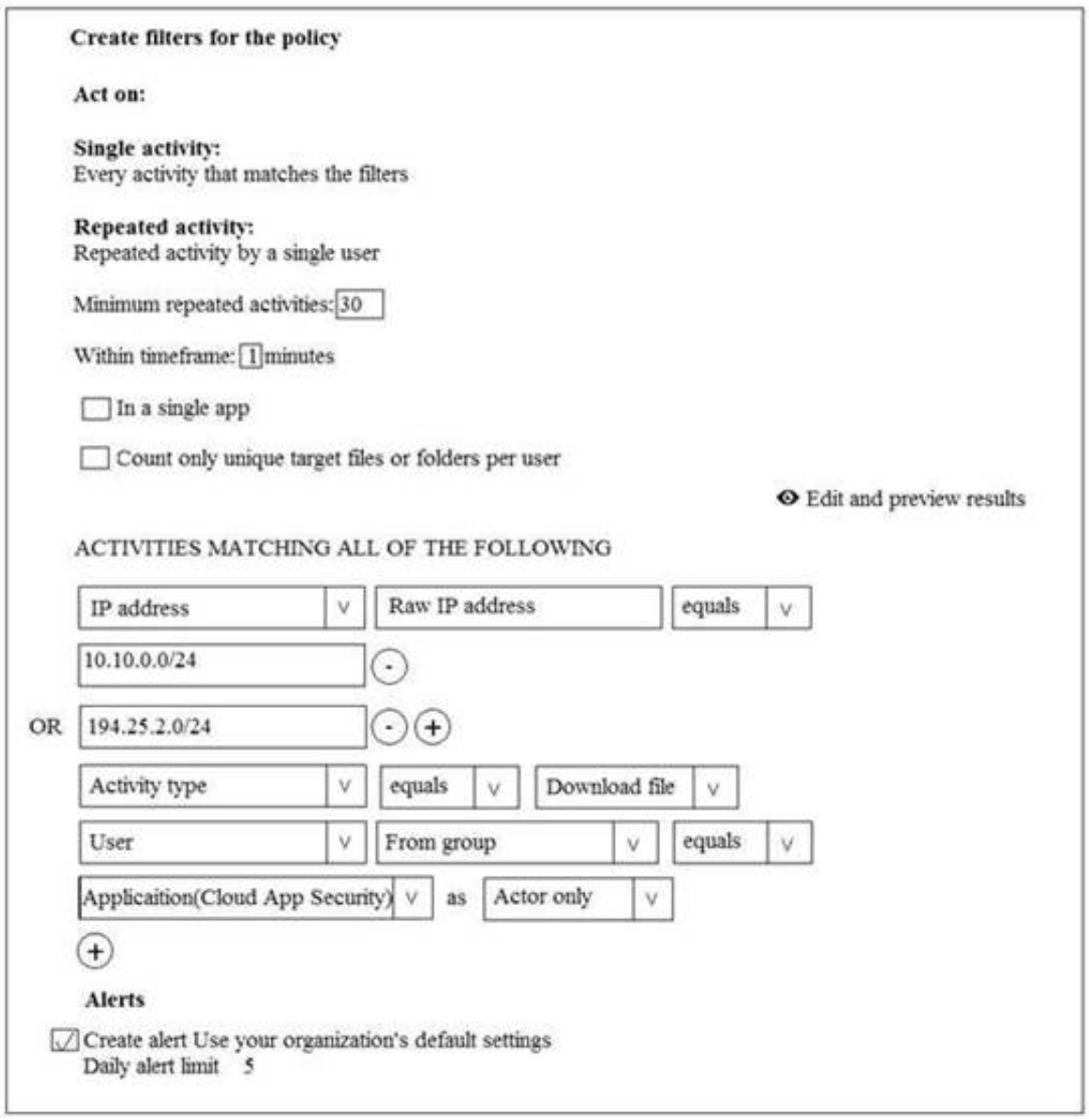
NEW QUESTION 59
HOTSPOT
Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com.
The company has the offices shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

The tenant contains the users shown in the following table.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

You create the Microsoft Cloud App Security policy shown in the following exhibit.



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

Statements	Yes	No
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	○	○
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	○	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	○	○
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	○	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	○

NEW QUESTION 61
You have a Microsoft 365 subscription.
Some users access Microsoft SharePoint Online from unmanaged devices.
You need to prevent the users from downloading, printing, and synching files. What should you do?

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

Answer: B

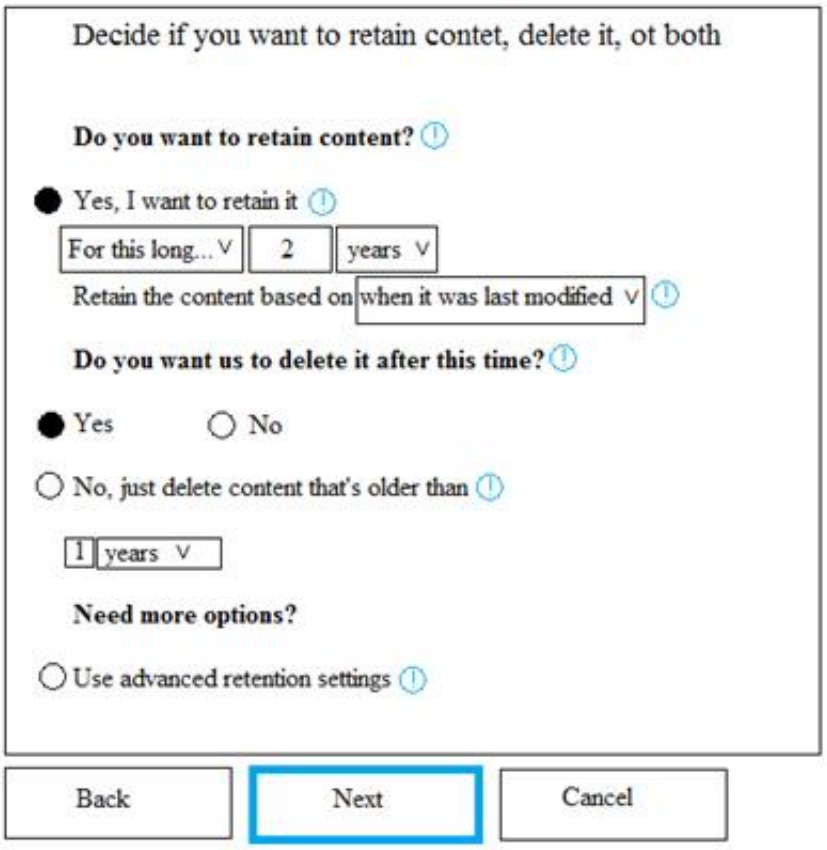
NEW QUESTION 62
You have a Microsoft 365 subscription.
You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.
Which type of site collection should you create first?

A. Records Center
B. Compliance Policy Center
C. eDiscovery Center
D. Enterprise Search Center
E. Document Center

Answer: C

Explanation:
Reference:
https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bbb944-448d-b83d-8fec4abcc24c

NEW QUESTION 66
HOTSPOT
You have a Microsoft 365 subscription.
You are creating a retention policy named Retention1 as shown in the following exhibit.



You apply Retention1 to SharePoint sites and OneDrive accounts.
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.

If a user creates a file in a Microsoft SharePoint library on January 1,2019, and modifies the file every six months, the file will be **[answer choice]**.

- retained
- deleted on Jauary 1,2021
- deleted on July 1,2021

If a user creates a file in Microsoft OneDrive on January 1,2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

- cannot recover the file
- can recover the file until Jauary 1,2020
- can recover the file until March 1,2020
- can recover the file until May 1,2020

A. Mastered
B. Not Mastered

Answer: A

Explanation:

If a user creates a file in a Microsoft SharePoint library on January 1,2019, and modifies the file every six months, the file will be **[answer choice]**.

retained
deleted on Jauary 1,2021
deleted on July 1,2021

If a user creates a file in Microsoft OneDrive on January 1,2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice].**

cannot recover the file
can recover the file until Jauary 1,2020
can recover the file until March 1,2020
can recover the file until May 1,2020

NEW QUESTION 70
HOTSPOT
You view Compliance Manager as shown in the following exhibit.

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

To increase the GDPR Compliance Score for Microsoft Office 365, you must **[answer choice].**

assign action items
review actions
perform an assessment
create a service request with Microsoft

The current GDPR Compliance Score **[answer choice].**

proves that the organization is non-compliant
proves that the organization is compliant
shows that actions are required to evaluate compliance

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud

NEW QUESTION 72
You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.
You need to ensure that the users can use the new label to protect their email. What should you do?

A. Modify the priority order of label policies
B. Wait six hours and ask the users to try again
C. Create a label policy
D. Create a new sensitive information type

Answer: B

NEW QUESTION 76
You have a Microsoft 365 subscription.
Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.
You need to ensure that the labels will be available for manual assignment as soon as possible. What should you do?

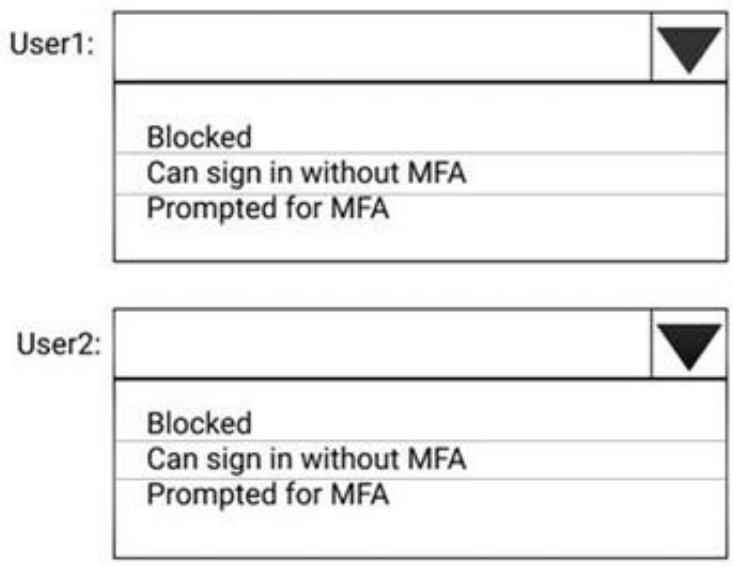
A. From the Security & Compliance admin center, create a label policy
B. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning
C. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Answer: C

NEW QUESTION 81
HOTSPOT
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

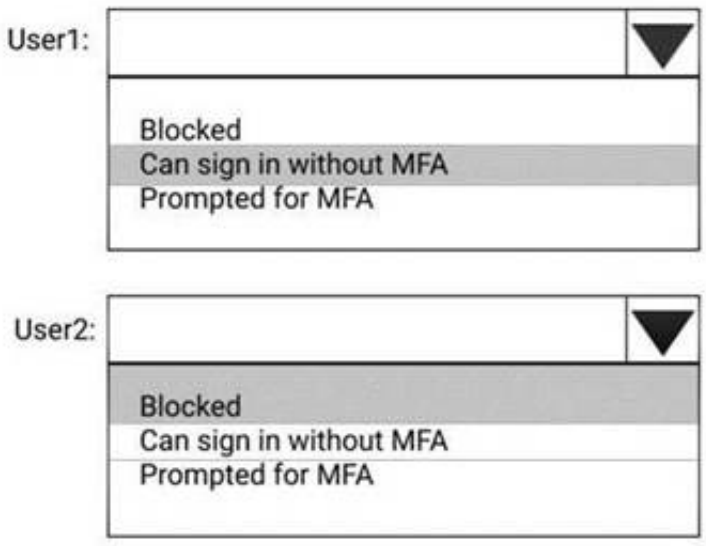
You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
•Assignments: Include Group1, Exclude Group2
•Conditions: Sign in risk of Low and above
•Access: Allow access, Require password multi-factor authentication You need to identify how the policy affects User1 and User2.
What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 84
Your network contains an on-premises Active Directory domain. The domain contains servers that run
Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

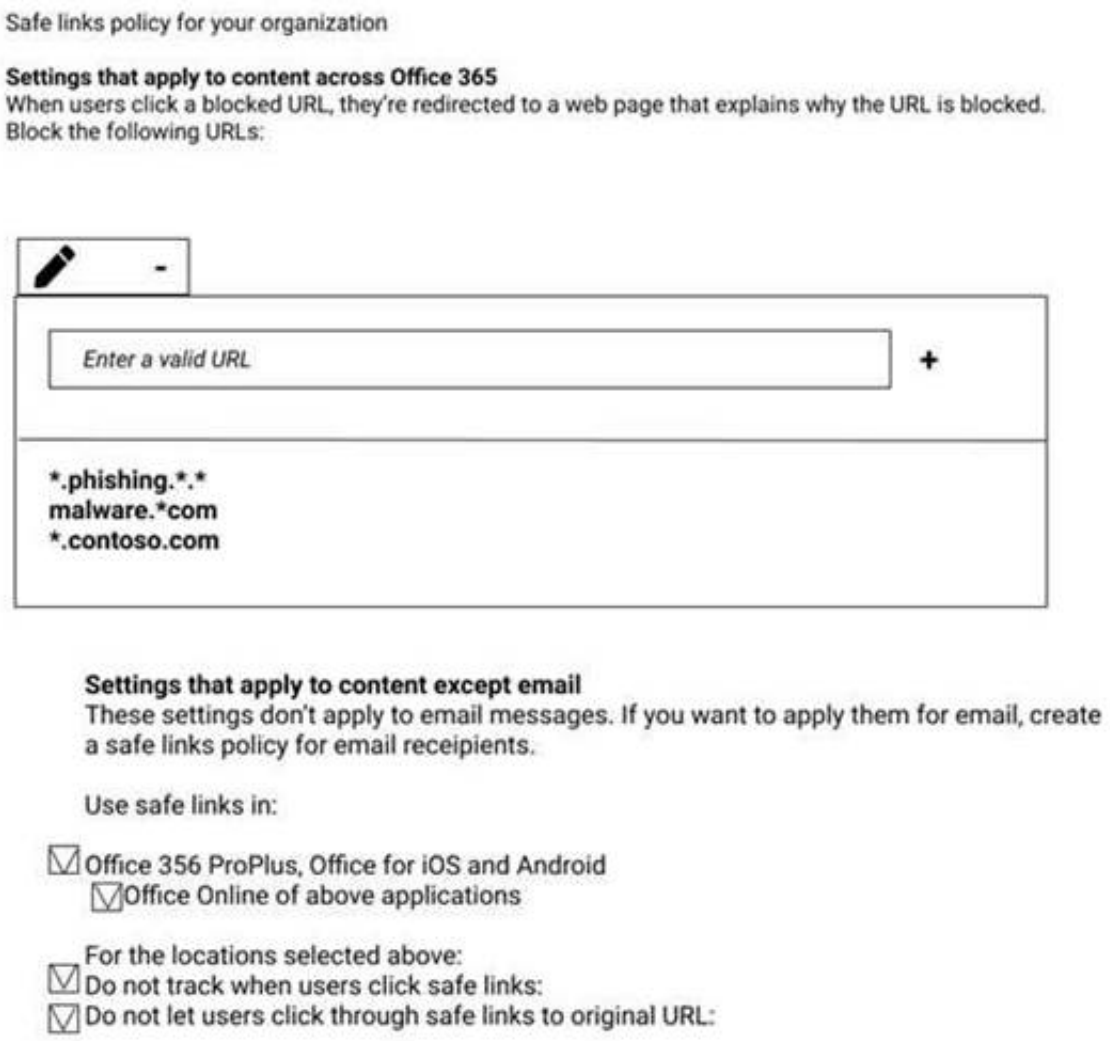
A. Configure auditing in the Office 365 Security & Compliance center.
B. Turn off Delayed updates for the Azure ATP sensors.
C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
D. Integrate SIEM and Azure ATP.

Answer: C

Explanation:
References:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

NEW QUESTION 89
You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com. You create a safe links policy, as shown in the following exhibit.



Which URL can a user safely access from Microsoft Word Online?

A. fabrikam.phishing.fabrikam.com
B. malware.fabrikam.com
C. fabrikam.contoso.com
D. www.malware.fabrikam.com

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list- wtih-atp

NEW QUESTION 94
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 questions 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 have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-AuditConfig -Workload Exchange command.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps

NEW QUESTION 96
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 questions 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 have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled $true-AdminAuditLogCmdlets *Mailbox* command. Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/setadminauditlogconfig?view=exchange-ps

NEW QUESTION 98
You have a Microsoft 365 subscription.
You need to be notified by email whenever an administrator starts an eDiscovery search. What should you do from the Security & Compliance admin center?

A. From Search & investigation, create a guided search.
B. From Events, create an event.
C. From Alerts, create an alert policy.
D. From Search & Investigation, create an eDiscovery case.

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

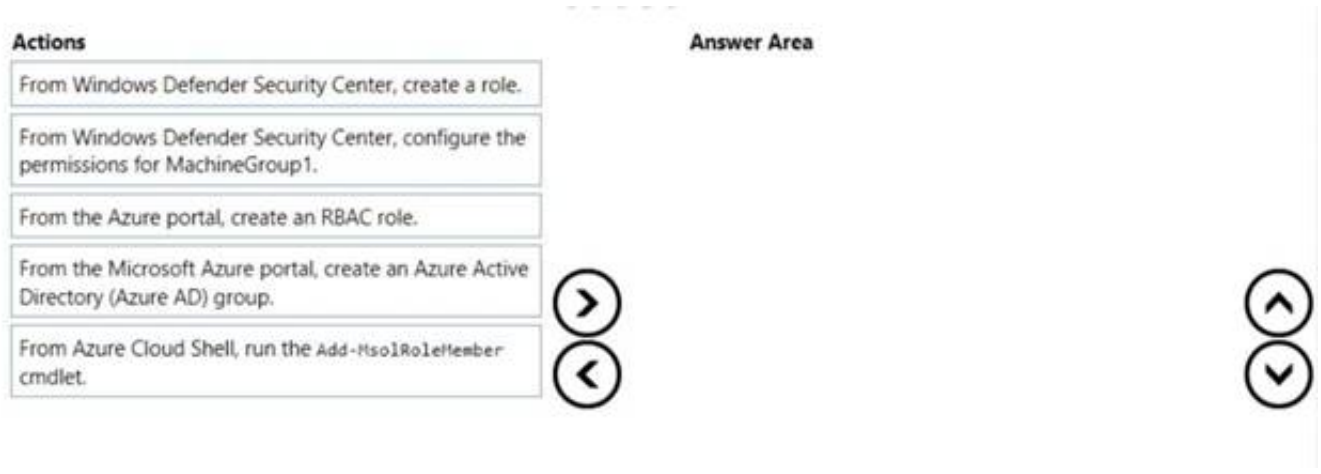
NEW QUESTION 101
Several users in your Microsoft 365 subscription report that they received an email message without the attachment. You need to review the attachments that were removed from the messages. Which two tools can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. the Exchange admin center
B. the Azure ATP admin center
C. Microsoft Azure Security Center
D. the Security & Compliance admin center
E. Outlook on the web

Answer: AD

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages- and-files

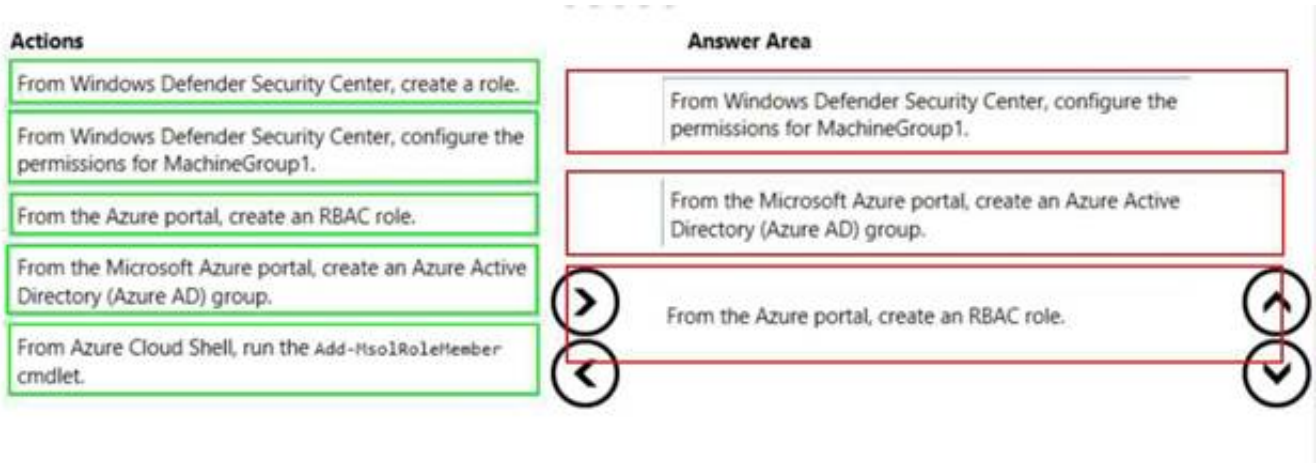
NEW QUESTION 104
DRAG DROP
You have a Microsoft 365 E5 subscription.
All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP).
You create a Windows Defender machine group named MachineGroupl.
You need to enable delegation for the security settings of the computers in MachineGroupl.
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 107
Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

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

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

NEW QUESTION 109
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

MS-500 Practice Exam Features:

* MS-500 Questions and Answers Updated Frequently

* MS-500 Practice Questions Verified by Expert Senior Certified Staff

* MS-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MS-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year