

Vendor: Microsoft

Exam Code: MS-500

Exam Name: Microsoft 365 Security Administration

➤ New Updated Questions from <u>Braindump2go</u> (Updated in <u>October/2021</u>)

Visit Braindump2go and Download Full Version MS-500 Exam Dumps

QUESTION 323

You have several Conditional Access policies that block noncompliant devices from connecting to services. You need to identify which devices are blocked by which policies. What should you use?

- A. the Setting compliance report in the Microsoft Endpoint Manager admin center
- B. Sign-ins in the Azure Active Directory admin center
- C. Activity log in the Cloud App Security portal
- D. Audit logs in the Azure Active Directory admin center

Answe/r: B Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access

QUESTION 324

You have a Microsoft 365 tenant.

You need to implement a policy to enforce the following requirements:

- If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint Online only from a web browser. The user must be prevented from downloading files or syncing files from SharePoint Online.
- If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files. What should you create?
- A. a conditional access policy in Azure AD that has Client apps conditions configured
- B. a conditional access policy in Azure AD that has Session controls configured
- C. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured
- D. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured

Answer: B Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

QUESTION 325

Hotspot Question

You have a Microsoft 365 E5 subscription.

You need to create a role-assignable group. The solution must ensure that you can nest the group.

How should you configure the group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

Group type:

Microsoft 365 only
Security only
Microsoft 365 or security

Membership type:

Assigned only
Dynamic User only
Assigned or Dynamic User

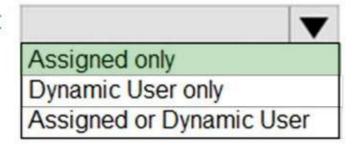
Answer:

Answer Area

Group type:

Microsoft 365 only
Security only
Microsoft 365 or security

Membership type:



Explanation:

Box 1: Security only

You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent



One Time!

group, saving you configuration time.

Box 2: Assigned only

The membership type for role-assignable groups must be Assigned and can't be an Azure AD dynamic group.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal

QUESTION 326

Hotspot Question

You create device groups in Microsoft Defender for Endpoint as shown in the following table.

Name	Rank	Membership rule		
Group1	1	Name Starts with Device		
Group2	2	Tag Equals Tag1		
Group3	3	Name Starts with Computer and OS is Windows 10		

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

Name	Operating system
Device1	Windows 10
Device2	MacOS
Computer3	Windows 10

After the devices are onboarded, you perform the following actions:

- Add a tag named Tag1 to Device1.
- Rename Computer3 as Device3.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 is in Group1.	0	0
Device2 is in Group2.	0	0
Device3 is in Group3.	0	0

Answer:



Answer Area

Statements	Yes	No
Device1 is in Group	1. 0	0
Device2 is in Group	2. 0	0
Device3 is in Group	3. O	0

Explanation:

Box 1: Yes

You can promote or demote the rank of a device group so that it's given higher or lower priority during matching. A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group. You can also edit and delete groups.

Box 2: No

The Group1 membership rule 'Name Start with Device' applies Device2.

No other rule applies.

Box 3: No

Compter3 rename to Device3 which will Apply to Group1.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups

QUESTION 327

You have a Microsoft 365 E5 subscription that contains 100 users. Each user has a computer that runs Windows 10 and either an Android mobile device or an iOS mobile device. All the devices are registered with Azure Active Directory (Azure AD).

You enable passwordless authentication for all the users.

You need to ensure that the users can sign in to the subscription by using passwordless authentication.

What should you instruct the users to do on their mobile device first?

- A. Install a device certificate.
- B. Install a user certificate.
- C. Install the Microsoft Authenticator app.
- D. Register for self-service password reset (SSPR).

Answer: C Explanation:

The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.

Note: Microsoft Authenticator App

You can allow your employee's phone to become a passwordless authentication method. You may already be using the Microsoft Authenticator App as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

One Time!

QUESTION 328

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

Name	Member of	Azure Multi-Factor Authentication (Azure MFA)
User1	Group1	None
User2	Group1	User authenticates by using a text message.
User3	Group1	User authenticates by using the Microsoft Authenticator app.
User4	Group1	User authenticates by using passwordless authentication.

You enable the authentication methods registration campaign and configure the Microsoft Authenticator method for Group1.

Which users will be prompted to configure authentication during sign in?

- A. User1 only
- B. User2 only
- C. User2 and User3 only
- D. User1 and User2 only
- E. User2 and User3 only
- F. User1, User2, and User3 only

Answer: D Explanation:

You can nudge users to set up Microsoft Authenticator during sign-in. Users will go through their regular sign-in, perform multifactor authentication as usual, and then be prompted to set up Microsoft Authenticator. You can include or exclude users or groups to control who gets nudged to set up the app. This allows targeted campaigns to move users from less secure authentication methods to Microsoft Authenticator.

Incorrect:

Not C, Not E, Not F: Not User3 since the user must not have already set up Microsoft Authenticator for push notifications on their account.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-registration-campaign

QUESTION 329

Hotspot Question

You have a Microsoft 365 subscription that contains three users named User1, User2, and User3. You have the named locations shown in the following table.

Name	IP address range	Trusted	
NY	192.168.2.0/27	Yes	
DC	192.168.1.0/27	No	
LA	192.168.3.0/27	No	

You configure an Azure Multi-Factor Authentication (MFA) trusted IP address range of 192.168.1.0/27. You have the Conditional Access policies shown in the following table.

Name	Assignments: Users and groups	Assignments: Cloud apps or actions	Conditions: Locations	Access controls: Grant
CA1	All users	Microsoft Forms	All trusted locations	Grant access: Require multi-factor authentication
CAZ	All users	Microsoft Planner	NY	Block access

The users have the IP addresses shown in the following table.



One Time!

User	IP address
User1	192.168.1.16
User2	192.168.2.16
User3	192.168.3.16

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 will be prompted for Azure MFA when accessing Microsoft Forms.	0	0
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	0	0
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	0	0
Statements	Yes	No
User1 will be prompted for Azure MFA when accessing Microsoft Forms.	0	0
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	0	0
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	0	0

Explanation:

Box 1: Yes

Answer:

User 1 access through CA1 (forms) with Location:(included as nothing else is stated) trusted location = require MFA

Box 2: No

User2 has IP address 192.168.2.16, which is in NY named location. NY is trusted. However, CA2 blocks Microsoft Planner NY access.

Box 3: No

User3 is in LA. LA is not trusted.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies

QUESTION 330

Your network contains an on-premises Active Directory domain. The domain contains a domain controller named DC1. You have a Microsoft 365 E5 subscription.

You install the Microsoft Defender for Identity sensor on DC1.

You need to configure enhanced threat detection in Defender for Identity.

The solution must ensure that the following events are collected from DC1:

- 4726 User Account Deleted
- 4728 Member Added to Global Security Group
- 4776 Domain Controller Attempted to Validate Credentials for an Account (NTLM)

What should you do on DC1?

- A. Install the Azure Monitor agent.
- B. Install System Monitor (SYSMON).
- C. Configure the Windows Event Collector service.
- D. Configure the Advanced Audit Policy Configuration policy.

Answer: D Explanation:

Windows Event logs

MS-500 Exam Dumps MS-500 Exam Questions MS-500 PDF Dumps MS-500 VCE Dumps



One Time!

Defender for Identity detection relies on specific Windows Event logs that the sensor parses from your domain controllers. For the correct events to be audited and included in the Windows Event log, your domain controllers require accurate Advanced Audit Policy settings.

For the correct events to be audited and included in the Windows Event Log, your domain controllers require accurate Advanced Audit Policy settings.

Note: Relevant Windows Events

For Active Directory Federation Services (AD FS) events:

1202 - The Federation Service validated a new credential

1203 - The Federation Service failed to validate a new credential

4624 - An account was successfully logged on

4625 - An account failed to log on

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/prerequisites

https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection

QUESTION 331

You configure several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view Microsoft Defender for Office 365 reports in the Threat management dashboard.

Which role provides User1 with the required role permissions?

- A. Security reader
- B. Compliance administrator
- C. Information Protection administrator
- D. Exchange administrator

Answer: A Explanation:

In order to view and use the reports described in this article, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:

- Organization Management
- Security Administrator
- Security Reader
- Global Reader

Note:

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

- 1. Security Administrator
- 2. Security Reader

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

- Compliance administrator
- Exchange administrator

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo

QUESTION 332

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a Microsoft Office 365 connector.

You need to use a Fusion rule template to detect multistage attacks in which users sign in by using compromised credentials, and then delete multiple files from Microsoft OneDrive.

Based on the Fusion rule template, you create an active rule that has the default settings.

What should you do next?

- A. Add data connectors.
- B. Add a workbook.
- C. Add a playbook.
- D. Create a custom rule template.

Answer: B



One Time!

Explanation:

Create an automation rule Create a playbook Add actions to a playbook

Attach a playbook to an automation rule or an analytics rule to automate threat response https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 333

You have an Azure Sentinel workspace.

You need to manage incidents based on alerts generated by Microsoft Cloud App Security. What should you do first?

- A. From the Cloud App Security portal, configure security extensions.
- B. From the Cloud App Security portal, configure app connectors.
- C. From the Cloud App Security portal, configure log collectors.
- D. From the Microsoft 365 compliance center, add and configure a data connector.

Answer: A Explanation:

Integrating with Microsoft Sentinel

In the Defender for Cloud Apps portal, under the Settings cog, select Security extensions.

On the SIEM agents tab, select add (+), and then choose Microsoft Sentinel.

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

QUESTION 334

You have a Microsoft 365 E5 subscription.

You need to use Attack simulation training to launch a credential harvest simulation.

For which Microsoft 365 workloads can you create a payload?

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

Answer: D **Explanation:**

Create a payload, select a payload type.

On the Select type page, the only value that you can currently select is Email.

Incorrect:

Not A, Not B, Not C: Payloads cannot be created for Microsoft Exchange Online.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-payloads

QUESTION 335

You have a Microsoft 365 E5 subscription.

You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:

- web1.contoso.com
- web2.contoso.com

The solution must minimize administrative effort.

To what should you set the Service domains setting for Endpoint DLP?

- A. web1.contoso.com and web2.contoso.com
- B. contoso.com
- C. *.contoso.com
- D. web*.contoso.com



One Time!

Answer: A Explanation:

An * is a wildcard for example :

*.contoso.com wil include evrything befor .contoso.com and will be blocked

web*.contoso.com

web1wil be blocked

web2 wil be blocked

web3 wil be blocked

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about

QUESTION 336

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.

You need to ensure that users can only share files with users at specified partner companies. The solution must minimize administrative effort.

What should you do?

- A. Limit external sharing by domain.
- B. Set External sharing to New and existing guests.
- C. Allow only users in specific security groups to share externally.
- D. Set File and folder links to Specific people.

Answer: A Explanation:

Limiting domains

You can limit domains by allowing only the domains you specify or by allowing all domains except those you block. To limit domains at the organization level

- 1. Go to Sharing in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.
- 2. Under Advanced settings for external sharing, select the Limit external sharing by domain check box, and then select Add domains.
- 3. To create an allowlist (most restrictive), select Allow only specific domains; to block only the domains you specify, select Block specific domains.
- 4. List the domains (maximum of 3000) in the box provided, using the format domain.com.

5. Etc.

Reference:

https://docs.microsoft.com/en-us/sharepoint/restricted-domains-sharing

QUESTION 337

Hotspot Question

You have a Microsoft 365 E5 tenant that contains a published sensitivity label named Sensitivity1.

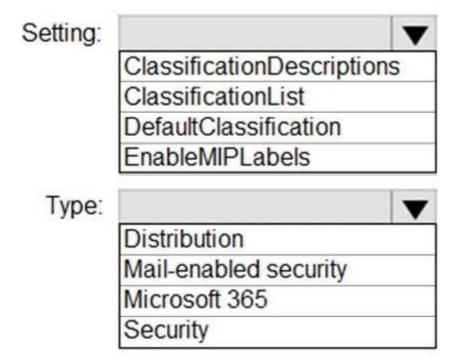
You plan to create an Azure Active Directory group named Group1 and assign Sensitivity1 to Group1.

How should you configure Group1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area



Answer:



Answer Area

ClassificationDescriptions
ClassificationList
DefaultClassification
EnableMIPLabels

Type:

Distribution
Mail-enabled security
Microsoft 365
Security

Explanation:

Box 1: EnableMIPLabels

The sensitivity label option is only displayed for groups when all the following conditions are met:

- * The feature is enabled, EnableMIPLabels is set to True in from the Azure AD PowerShell module.
- * The group is a Microsoft 365 group.
- * Etc.

Box 2: Microsoft 365

Incorrect:

* Not ClassificationList:

Classic classifications are the old classifications you set up by defining values for the ClassificationList setting in Azure AD PowerShell. When this feature is enabled, those classifications will not be applied to groups.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels

QUESTION 338

Hotspot Question

You have a Microsoft E5 subscription that contains two users named User1 and User2.

You have a Microsoft SharePoint site named Site1. Site1 stores files that contain IP addresses as shown in the following table.

Name	Number of IP addresses
File1.txt	3
File2.docx	1

User1 is assigned the SharePoint admin role for Site1. User2 is a member of Site1. You create the data loss prevention (DLP) policy shown in the following exhibit.

Edit

One Time!

Review your settings

Template name	Edit
Custom policy	
Policy name	Edit
Policy1	
Description	Edit
Applies to content in these locations	Edit
SharePoint sites	
Policy settings	Edit
If the content contains these types of sensitive info: IP Address	
If there are at least 2 instances of the same type of sensitive info block access to the content.	
Turn policy on after it's created?	Edit
Yes	
Back Create Cancel	

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

Answer Area

Statements	Yes	No
User1 can view the contents of File1.txt.	0	0
User2 can view the contents of File1.txt.	0	0
User2 can view the contents of File2.docx	c. O	0

Answer:



Answer Area

Statements	Yes	No
User1 can view the contents of File1.txt.	0	0
User2 can view the contents of File1.txt.	0	0
User2 can view the contents of File2.docx.	0	0

Explanation:

Box 1: Yes

Note: Key tasks of the SharePoint admin

Here are some of the key tasks users can do when they are assigned to the SharePoint admin role:

- Create sites
- Delete sites
- Manage sharing settings at the organization level
- Add and remove site admins
- Manage site storage limits

Box 2: No

File1.text contains 3 IP addresses.

Box 3: Yes

File2.docx contains only 1 IP address.

QUESTION 339

Hotspot Question

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and a sensitivity label named Label1.

The external sharing settings for Site1 are configured as shown in the Site1 exhibit. (Click the Site1 tab.)



Sharing

The sharing settings available for this site depend on your organization-level settings. Learn more about the external sharing settings

External sharing
Site content can be shared with:
O Anyone Users can share files and folders using links that don't require sign-in.
New and existing guests Guests must sign in or provide a verification code.
Only guests already in your organization's directory.
Only people in your organization No external sharing allowed.
The external sharing settings for Label1 are configured as shown in the Label1 exhibit. (Click the Label1 tab. Define external sharing and conditional access settings
Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.
Control external sharing from labeled SharePoint sites When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.
Content can be shared with Anyone Users can share files and folders using links that don't require sign-in.
○ New and existing guests ○ Guests must sign in or provide a verification code.
Orly guests O Only guests in your organization's directory.
Only people in your organization No external sharing allowed.
Use Azure AD Conditional Access to protect labeled SharePoint sites
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.
Label 1 is applied to Site1. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



One Time!

	Statements	Yes	No
	Internal users can share documents on Site1 with external users.	0	0
	External users require an invitation to access Site1.	0	0
	Only users on managed devices can access Site1.	0	0
nswer:			
	Statements	Yes	No
	Statements Internal users can share documents on Site1 with external users.	Yes	No
		Yes	No

Explanation:

Box 1: Yes

The Sensitive label setting of Label1 in the second exhibit 2overrides the setting in exhibit 1.

Box 2: No Box 3: No

QUESTION 340

Drag and Drop Question

Your company has two departments named department1 and department2 and a Microsoft 365 E5 subscription.

You need to prevent communication between the users in department1 and the users in department2.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value 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.

New-InformationSerrierPolicy		-Name "Department1" -UserGroupFilter "Department -eq 'department1'"
New-OrganizationSegment	***	
Set-InformationBarrierPolicy		-Name "Departmentiand2" -AssignedSegment "Department1"
	-SegmentsBlocked "De	portment2" -State Active
Set-OrganizationSegment		
Values	Answer Area	
	New-OrganizationSegment	-Name "Department1" -UserGroupFilter "Department -eq 'department1'"
	222	
	New-InformationSarrierPolicy	-Name "Departmentiand2" -AssignedSegment "Department1"
Set-InformationBarrierPolicy	-SegmentsBlocked "De	portment2" -State Active

Explanation:

Answer:

Box 1: New-OrganizationSegment

Use the New-OrganizationSegment cmdlet to create organization segments for use with information barrier policies in the Microsoft Purview compliance portal.

Organization Segments are not in effect until you apply information barrier policies.

Syntax:

New-OrganizationSegment -

[-Name] <String>

-UserGroupFilter <String>

[-Confirm]

[-Whatlf]



One Time!

[<CommonParameters>]

Box 2: New-InformationBarrierPolicy

To define your first blocking policy, use the New-InformationBarrierPolicy cmdlet with the SegmentsBlocked parameter. Reference:

https://docs.microsoft.com/en-us/powershell/module/exchange/new-organizationsegment https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies

QUESTION 341

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

Name	Type	Location
Mail1	Email message	Microsoft Exchange Online
File1.docx	File	Microsoft SharePoint Online
File2.xlsx	File	Microsoft OneDrive

You have a retention label configured as shown in the following exhibit.

Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

•	Retain items for a specific period
	Labeled items will be retained for the period you choose. Retention period
	5 years ~
	Start the retention period based on
	When items were created
	+ Create new event type
	During the retention period
	Retain items even if users delete Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. Learn more
	Mark items as a record
	At the end of the retention period
	Delete items automatically We'll delete items from where they're currently stored.
	Trigger a disposition review
	On nothing Items will be left in place. You'll have to manually delete them if you want them gone.

You publish the retention label and set the scope as shown in the following exhibit.

Choose locations

We'll publish the labels to the locations you choose.

All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.
 Let me choose specific locations.

You apply the label to the resources.

Which items can you delete?

- A. Mail1 only
- B. File1.docx and File2.xlsx only
- C. Mail1 and File1.docx only
- D. Mail1 and File2.xlsx only
- E. Mail1, File1.docx, and File2.xlsx

Answer: E



One Time!

Explanation:

All the items can be deleted according to the settings.

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#how-retention-settings-work-with-content-in-place

QUESTION 342

You have a Microsoft 365 E5 subscription.

You plan to implement retention policies for Microsoft Teams.

Which item types can be retained?

- A. voice memos from the Teams mobile client
- B. code snippets
- C. embedded images

Answer: C Explanation:

Code snippets, recorded voice memos from the Teams mobile client, thumbnails, announcement images, and reactions from others in the form of emoticons aren't retained when you use retention policies for Teams.

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

QUESTION 343

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

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

The DLP rules are configured as shown in the following table.

Rule	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	On	Tip 1	Enabled
Rule2	On	Tip 2	Disabled
Rule3	On	Tip 3	Enabled
Rule4	On	Tip 4	Disabled

All the policies are assigned to Site1.

You need to ensure that if a user uploads a document to Site1 that matches all the rules, the user will be shown the Tip 2 policy tip.

What should you do?

- A. Enable additional processing of the policies if there is a match for Rule1.
- B. Prevent additional processing of the policies if there is a match for Rule2.
- C. Change the priority of DLP2 to 3.
- D. Change the priority of DLP2 to 0.

Answer: D Explanation:

The rule with priority 0 is processed first.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference

QUESTION 344

MS-500 Exam Dumps MS-500 Exam Questions MS-500 PDF Dumps MS-500 VCE Dumps



One Time!

Hotspot Question

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

Name	Team membership
User1	Team1, Team2
User2	Team2

You have the retention policies shown in the following table.

Name	Location	Included	Retain items for	Start retention period	At the end of retention period
Policy1	y1 Microsoft Teams channel All teams 7 messages	7 years	When items are created	Delete items automatically	
	Microsoft Teams chats	User1		27.50.176325	2.4400000000000000000000000000000000000
Policy2	Microsoft Teams channel messages	Team1	5 years	When items are created	Delete items automatically
	Microsoft Teams chats	User2		A Particular Section 1	0.000.000000000000000000000000000000000

The users perform the actions shown in the following table.

User	Location	Action
User1	Team1 channel	Edits a message
User2	Private 1:1 chat with User1	Sends a message to User1
User1	Team2 channel	Deletes a message

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
0	0
0	0
0	0
Yes	No
0	0
0	0
	O O Yes

Explanation:

Box 1: No

It will be retained for seven years.

Both Policy1 and Policy2 apply.

If there is a conflict in how long to retain the same content, it is retained in the secured location for the longest retention period.

Note: If you configure a Teams retention policy to retain chats or channel messages, users

Box 2: No

MS-500 Exam Dumps MS-500 Exam Questions MS-500 PDF Dumps MS-500 VCE Dumps



One Time!

User2 creates the message in chat. Policy2 applies. The message will be retained for 5 years.

Box 3: Yes

After a retention policy is configured for chat and channel messages, a timer job from the Exchange service periodically evaluates items in the hidden mailbox folder where these Teams messages are stored. The timer job typically takes 1-7 days to run. When these items have expired their retention period, they are moved to the SubstrateHolds folderx€"another hidden folder that's in every user or group mailbox to store "soft-deleted" items before they're permanently deleted.

Messages remain in the SubstrateHolds folder for at least 1 day, and then if they're eligible for deletion, the timer job permanently deletes them the next time it runs.

Reference:

https://docs.microsoft.com/en-us/microsoftteams/retention-policies

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-teams

QUESTION 345

Your company has a Microsoft 365 E5 subscription that uses Microsoft Defender for identity.

You plan to create a detection exclusion in Microsoft Defender for Identity.

What should you use to create the detection exclusion?

- A. Microsoft Defender for Identity portal
- B. Microsoft 365 Compliance center
- C. Microsoft Defender for Cloud Apps portal
- D. Microsoft 365 Defender portal

Answer: D Explanation:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-identity/exclusions?view=o365-worldwide#how-to-add-detection-exclusions

QUESTION 346

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

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

You plan to implement privileged access in Microsoft 365.

Which groups can you specify as the default approval group?

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

Answer: C

QUESTION 347

You have an Azure Sentinel workspace.

You need to manage incidents based on alerts generated by Microsoft Defender for Cloud Apps. What should you do first?

- A. From the Microsoft Defender for Cloud Apps portal, configure security extensions.
- B. From the Microsoft Defender for Cloud Apps portal, configure app connectors.
- C. From the Microsoft Defender for Cloud Apps portal, configure log collectors.
- D. From the Microsoft 365 Compliance admin center, add and configure a data connector.



One Time!

Answer: A Explanation:

Integrating with Microsoft Sentinel:

In the Defender for Cloud Apps portal, under the Settings cog, select Security extensions.

https://learn.microsoft.com/en-us/defender-cloud-apps/siem-sentinel

QUESTION 348

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 on-premises network contains a server that runs Windows Server 2019, computers that run Windows 10, macOS, or Linux, and a firewall that utilizes syslog.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. All the computers are onboarded to Microsoft Defender for Endpoint.

You are implementing Microsoft Defender for Cloud Apps.

You need to discover which cloud apps are accessed from the computers.

Solution: You install a Microsoft Defender for Identity sensor on the server.

Does this meet the goal?

A. Yes

B No

Answer: A Explanation:

https://docs.microsoft.com/en-us/defender-cloud-apps/mdi-integration

QUESTION 349

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 on-premises network contains a server that runs Windows Server 2019, computers that run Windows 10, macOS, or Linux, and a firewall that utilizes syslog.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. All the computers are onboarded to Microsoft Defender for Endpoint.

You are implementing Microsoft Defender for Cloud Apps.

You need to discover which cloud apps are accessed from the computers.

Solution: You install a Microsoft Defender for Cloud Apps log collector and collect logs from the firewall.

Does this meet the goal?

A. Yes

B. No

Answer: B

QUESTION 350

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 on-premises network contains a server that runs Windows Server 2019, computers that run Windows 10, macOS, or Linux, and a firewall that utilizes syslog.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. All the computers are onboarded to Microsoft Defender for Endpoint.

MS-500 Exam Dumps MS-500 Exam Questions MS-500 PDF Dumps MS-500 VCE Dumps



One Time!

You are implementing Microsoft Defender for Cloud Apps.

You need to discover which cloud apps are accessed from the computers.

Solution: You install an Azure Arc agent on the workstations.

Does this meet the goal?

A. Yes B. No

Answer: B

QUESTION 351

Hotspot Question

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

Name	Microsoft 365 role	Role group
Admin1	Global Administrator	None
Admin2	Compliance admin	None
User3	User	Compliance Manager Contributors
User4	User	Compliance Manager Administrators
User5	User	None

You create an assessment named Assessment1 as shown in the following exhibit.

Assessment1

Status Created
oin progress 1/15/2021

Generate report

Overview Controls Your improvement actions Microsoft actions

Review details about this assessment and understand your progress toward completion.

49% Assessment progress

1083/2169

Your points achieved (i)

0/1066

Microsoft managed points achieved (i)

1083/1083

Which users can update the title of Assessment1, and which users can add User5 to the Compliance Manager Readers role group? To answer, select the appropriate options in the answer area.

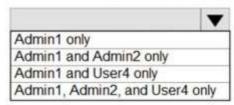
NOTE: Each correct selection is worth one point.

Answer Area



User4 only
Admin2 and User4 only
Admin1, Admin2, and User4 only
Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Reader role group:



Answer:

Answer Area

Can update the Assessment1 title:

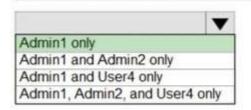
User4 only

Admin2 and User4 only

Admin1, Admin2, and User4 only

Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Reader role group:



Explanation:

Box 1: Admin 1, Admin 2, User 4

"Compliance Administrator" Azure AD role can also edit data same as "Compliance Manager Assessor". https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#set-user-permissions-and-assign-roles

Box 2: Only Admin 1

https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center-permissions?view=o365-worldwide

QUESTION 352

Hotspot Question

You have a Microsoft 365 E5 subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains three groups named Group1, Group2, and Group3 and the users shown in the following table.



Name	Member of	
User1	Group1	
User2	Group2	
User3	Group1, Group2	

You create a new access package as shown in the following exhibit.

New access packa	ge	Ü	
Basics Resource roles *R	equests Requestor inform	nation *Lifecycle Review	r + Create
Summary of access package co	onfiguration		
Basics			
Name	Package1		
Description	Package1 descrip	tion	
Catalog name	General		
Resource roles			
Resource	Туре	Sub Type	Role
Group1	Group and Team	Security Group	Member
Group3	Group and Team	Security Group	Member
Site1	SharePoint Site	SharePoint Online Site	Site1 Members
Requests			
Users who can request access	For users in your	directory(Group2)	
Require approval	No		
Enabled	Yes		
Requestor information			
Questions			
Question	Answer format	Required	
Lifecycle			
Access package assignments	expire After 10 days		
Require access reviews	No		

You assign Package1 on June 1, 2021, by using die following configurations:

- Select users: User1, User2, User3
- Select policy: Initial policy
- Assignment starts: June 1, 2021
- Assignment ends: July 1, 2021

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

NOTE: Each correct selection is worth one point.

MS-500 Exam Dumps MS-500 Exam Questions MS-500 PDF Dumps MS-500 VCE Dumps



One Time!

	Statements	Yes	No
	On June 5, 2021, User1 can access Package1.	0	0
	On June 15, 2021, User2 can access Package1.	0	0
	On June 5, 2021, User1, User2, and User3 are members of Group3.	0	0
inswer:	Statements	Yes	No
	On June 5, 2021, User1 can access Package1.	0	0
	On June 5, 2021, User1 can access Package1. On June 15, 2021, User2 can access Package1.	0	0

Explanation:

Box 1: Yes Box 2: No

Lifecycle, Access package assignments expires: After 10 days

Box 3: Yes

The access package resource roles includes: Group3 Member

Note: Entitlement management introduces to Azure AD the concept of an access package. An access package is a bundle of all the resources with the access a user needs to work on a project or perform their task. Access packages are used to govern access for your internal employees, and also users outside your organization.

Here are the types of resources you can manage user's access to, with entitlement management:

- Membership of Azure AD security groups
- Membership of Microsoft 365 Groups and Teams
- Assignment to Azure AD enterprise applications, including SaaS applications and custom-integrated applications that support federation/single sign-on and/or provisioning
- Membership of SharePoint Online sites

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview

QUESTION 353

Hotspot Question

You have a Microsoft 365 subscription that contains 100 users.

Microsoft Secure Score for the subscription is shown in the following exhibit.



One Time!

Microsoft Secure Score

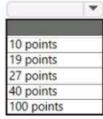
Score last calculated 11/05; 1:00 AM

Overvi	ew Improvement actions History Metrics & trends		
Actions y	ou can take to improve your Microsoft Secure Score. Score updates m	ay take up to	24 hours.
± Exp	ort 32 items 🔎 Search	√ Filter	\equiv Group by \vee
Applied t	ilters:		
Rank ①	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+7.75%	0/10
2	Ensure all users can complete multi-factor authentication for	+6.98%	0/9
3	Enable policy to block legacy authentication	+6.2%	0/8
4	Turn on sign-in risk policy	+5.43%	0/7
5	Turn on user risk policy	+5.43%	0/7
6	Install Azure ATP Sensor on all Domain Controllers	+3.1%	0/4
7	Do not allow users to grant consent to unmanaged applicatio	+3.1%	0/4
8	Set automated notifications for new OAuth applications conn	+3.1%	0/4
9	Use Cloud App Security to detect anomalous behavior	+2.33%	0/3
10	Set automated notifications for new and trending cloud appli	+2.33%	0/3

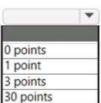
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic

NOTE: Each correct selection is worth one point.

If you set Enable Security defaults to Yes in Azure Active Directory (Azure AD), Microsoft Secure Score will increase by [answer choice].



If you enable multi-factor authentication (MFA) for 30 users, Microsoft Secure Score will increase by [answer choice].



Answer:

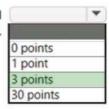


One Time!

If you set Enable Security defaults to **Yes** in Azure Active Directory (Azure AD), Microsoft Secure Score will increase by **[answer choice]**.



If you enable multi-factor authentication (MFA) for 30 users, Microsoft Secure Score will increase by [answer choice].



Explanation:

Box 1: 27 points

- Security defaults

Microsoft Secure Score has updated improvement actions to support security defaults in Azure Active Directory, which make it easier to help protect your organization with pre-configured security settings for common attacks. If you turn on security defaults, you'll be awarded full points for the following improvement actions:

- Ensure all users can complete multi-factor authentication for secure access (9 points)
- Require MFA for administrative roles (10 points)
- Enable policy to block legacy authentication (7 points)

Box 2: 3 points

Some improvement actions only give points when fully completed. Some give partial points if they're completed for some devices or users.

In this case: 30/100 * 10 = 3 points

Note: How improvement actions are scored

Each improvement action is worth 10 points or less, and most are scored in a binary fashion. If you implement the improvement action, like create a new policy or turn on a specific setting, you get 100% of the points. For other improvement actions, points are given as a percentage of the total configuration.

For example, an improvement action states you get 10 points by protecting all your users with multi-factor authentication. You only have 50 of 100 total users protected, so you'd get a partial score of 5 points (50 protected / 100 total * 10 max pts = 5 pts).

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score

QUESTION 354

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 on-premises network contains a server that runs Windows Server 2019, computers that run Windows 10, macOS, or Linux, and a firewall that utilizes syslog.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. All the computers are onboarded to Microsoft Defender for Endpoint.

You are implementing Microsoft Defender for Cloud Apps.

You need to discover which cloud apps are accessed from the computers.

Solution: You enable Defender for Endpoint and Defender for Cloud Apps integration.

Does this meet the goal?

A. Yes B. No

Answer: A Explanation:



One Time!

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-cloud-app-security-config?view=o365-worldwide

QUESTION 355

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Office 365 enabled. You need to review the zero-hour auto purge (ZAP) configuration for the subscription. Which two threat policies should you review? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Safe attachments Built-in protection (Microsoft)
- B. Anti-malware (Default) Default
- C. Safe links Built-in protection (Microsoft)
- D. Anti-spam outbound policy (Default)
- E. Office365 AntiPhish Default (Default)
- F. Anti-spam inbound policy (Default)

Answer: BF Explanation:

ZAP for malware is enabled by default in anti-malware policies.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#zero-hour-auto-purge-zap-for-malware

By default, ZAP for phishing is enabled in anti-spam policies[...]

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#zero-hour-auto-purge-zap-for-phishing