MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You plan to create a script to automate user mailbox searches. The script will search the mailbox of a user named Allan Deyoung for messages that contain the word injunction.

You need to create the search that will be included in the script.

To complete this task, sign in to the Microsoft 365 admin center.

Correct Answer: See explanation below.

Step 1: Create a CSV file that contains information about the searches you want to run

The comma separated value (CSV) file that you create in this step contains a row for each user that want to search. You can search the user\\'s Exchange Online mailbox (which includes the archive mailbox, if it\\'s enabled) and their OneDrive for Business site. Or you can search just the mailbox or the OneDrive for Business site. You can also search any site in your SharePoint Online organization. The script that you run in Step 3 will create a separate search for each row in the CSV file.

1. Copy and paste the following text into a .txt file using NotePad. Save this file to a folder on your local computer. You\\'ll save the other scripts to this folder as well.

ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2000,12/31/2005 sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2006,12/31/2010
sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2011,3/21/2016 ,https://contoso.sharepoint.com/sites/contoso,,,3/21/2016 ,https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com,,1/1/2015, ,https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com,,1/1/2015,

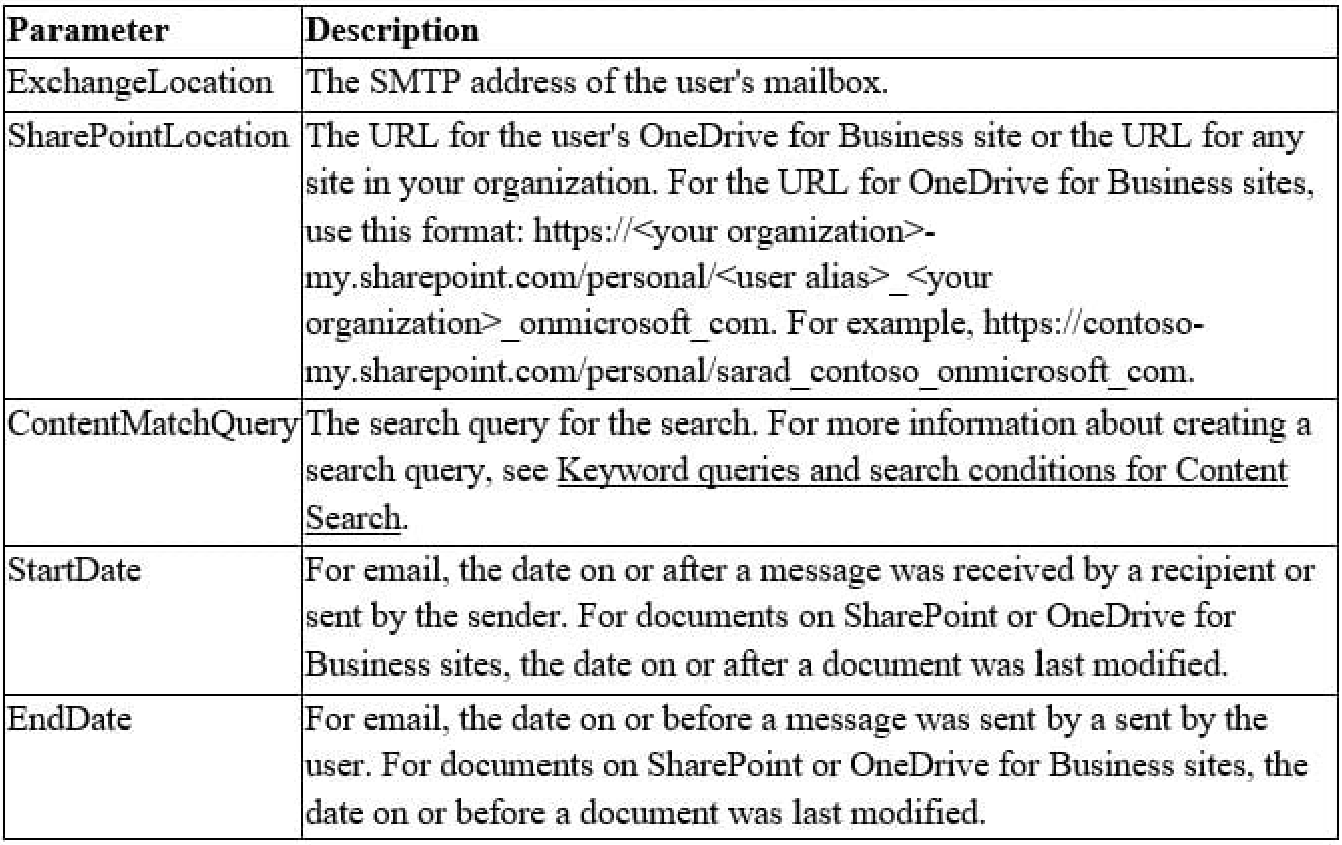
The first row, or header row, of the file lists the parameters that will be used by New-ComplianceSearch cmdlet to create a new Content Searches. Each parameter name is separated by a comma. Make sure there aren\\'t any spaces in the header row. Each row under the header row represents the parameter values for each search. Be sure to replace the placeholder data in the CSV file with your actual data.

2.

Open the .txt file in Excel, and then use the information in the following table to edit the file with information for each search.

3.

Save the Excel file as a CSV file to a folder on your local computer. The script that you create in Step 3 will use the information in this CSV file to create the searches.



Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see Keyword queries and search conditions for Content Search.
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-searches?view=o365-worldwide

Keyword queries and search conditions for Content Search https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365-worldwide

QUESTION 2

You have a Microsoft 365 E5 subscription

You need to use Microsoft Cloud App Security to identify documents stored in Microsoft SharePomt Online that contain proprietary information.

What should you create in Cloud App Security?

A. a data source and a file policy

B. a data source and an app discovery policy

C. an app connector and an app discovery policy

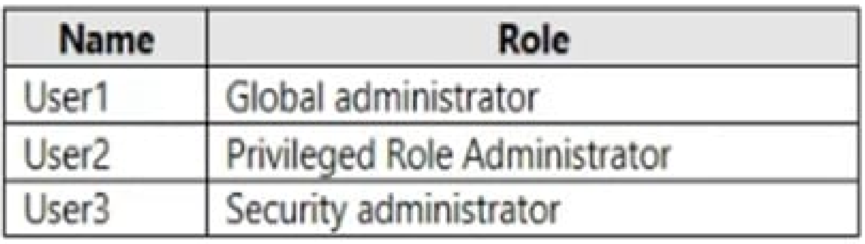
D. an app connector and a We policy

Correct Answer: B

QUESTION 3

HOTSPOT

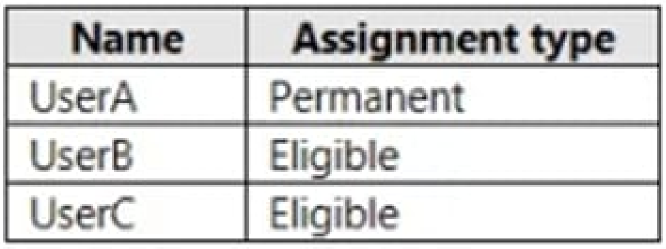
You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

You implement Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

From PIM, you review the Application Administrator role and discover the users shown in the following table.



Name	Assignment type
UserA	Permanent
UserB	Eligible
UserC	Eligible

The Application Administrator role is configured to use the following settings in PIM:

1.

Maximum activation duration: 1 hour

2.

Notifications: Disable

3.

Incident/Request ticket: Disable

4.

Multi-Factor Authentication: Disable

5.

Require approval: Enable

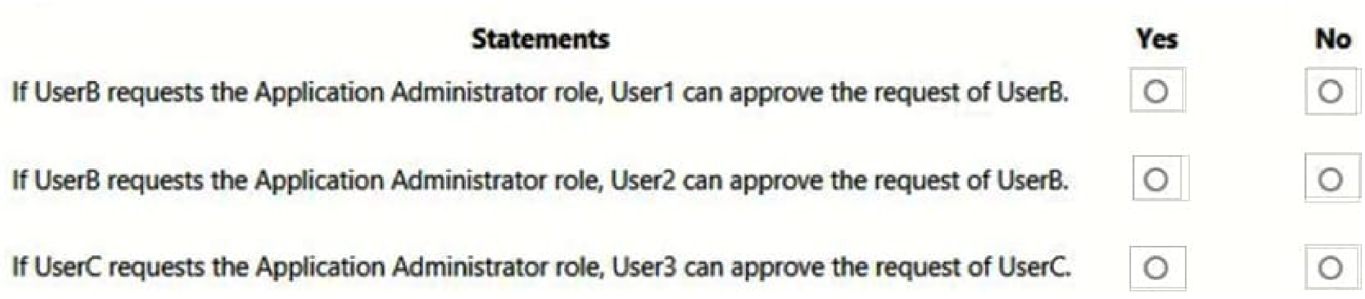
6.

Selected approver: No results

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

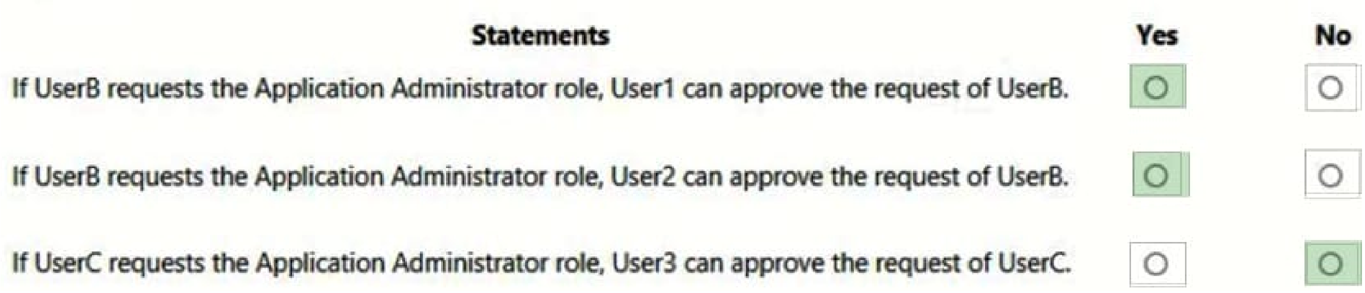
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	○	○
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	○	○
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	○	○

Correct Answer:



Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	[✓ ○]	○
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	[✓ ○]	○
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	○	[✓ ○]

QUESTION 4

You need to create Group2.

What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center

B. a mail-enabled security group in the Microsoft 365 admin center

C. a security group in the Microsoft 365 admin center

D. a distribution list in the Microsoft 365 admin center

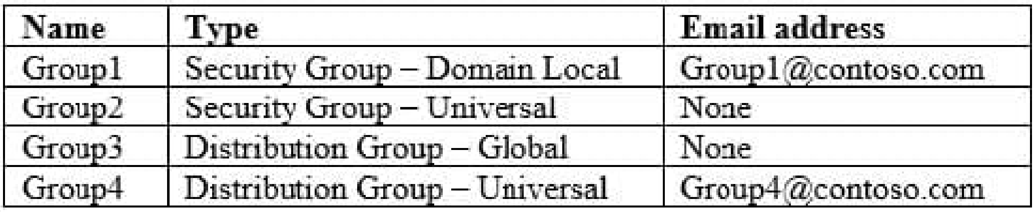
E. a security group in the Azure AD admin center

Correct Answer: CE

QUESTION 5

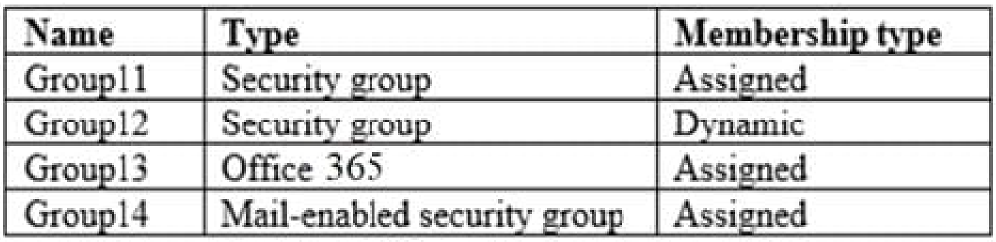
HOTSPOT

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 365	Assigned
Group14	Mail-enabled security group	Assigned

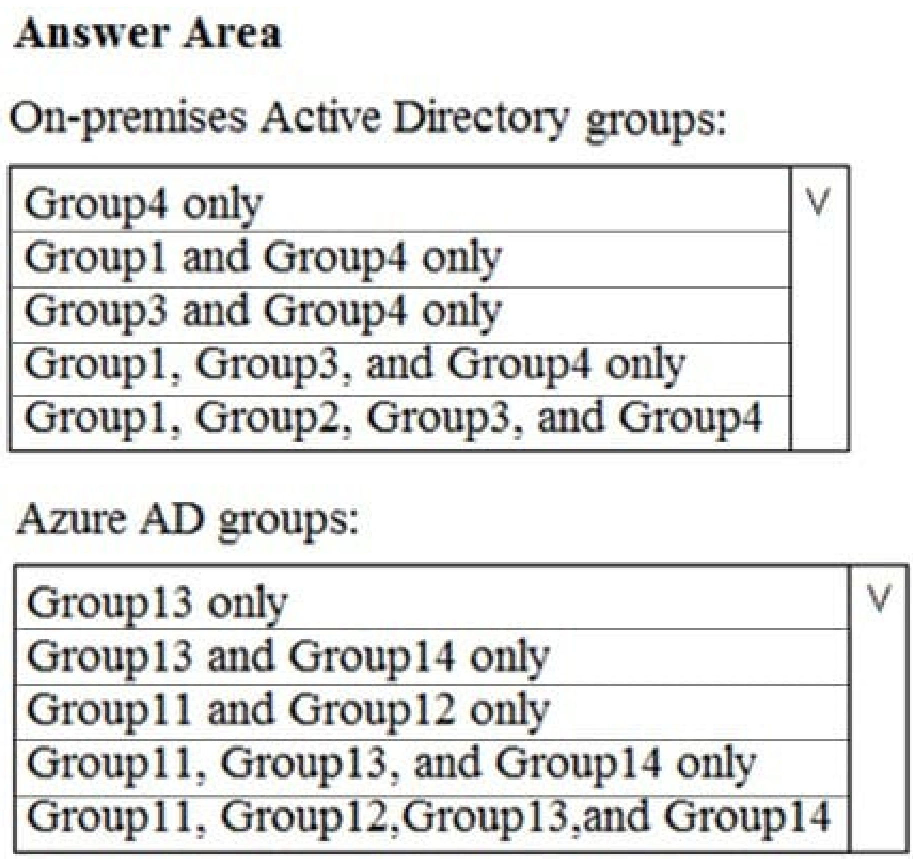
You create a sensitivity label named Label1.

You need to publish Label1.

To which groups can you publish Label1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

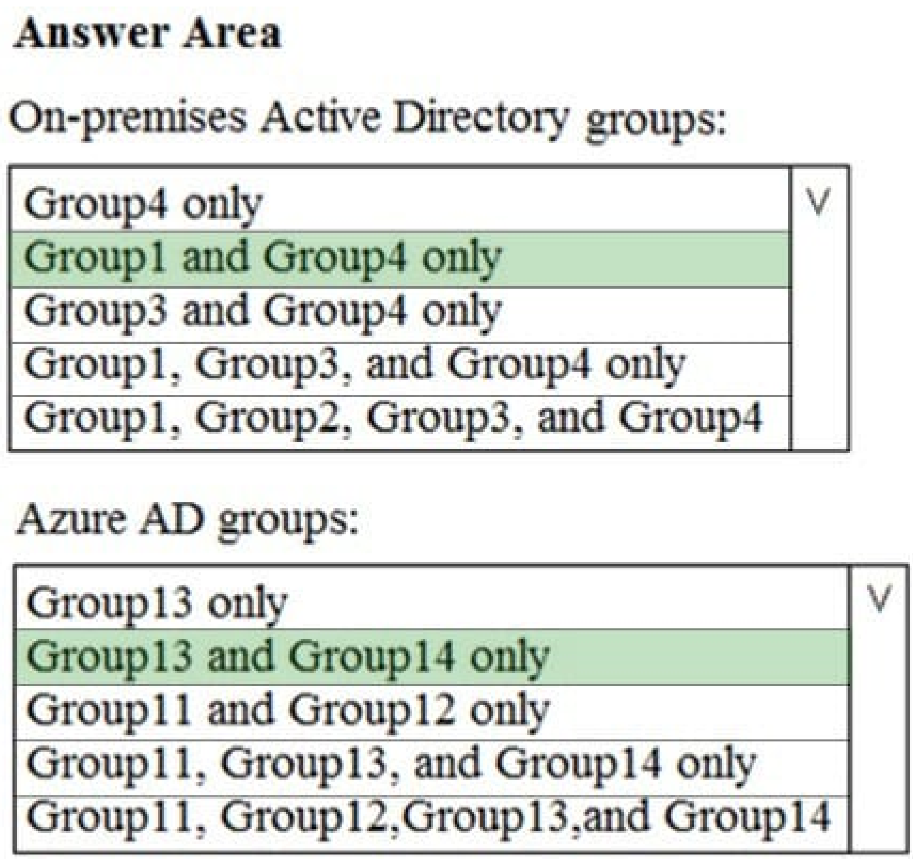
On-premises Active Directory groups:

- 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

Correct Answer:



Answer Area

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

The groups must be mail-enabled.

Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.

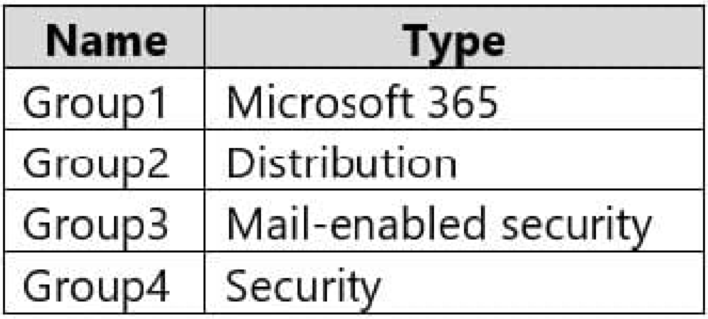
Reference:

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

QUESTION 6

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1 and the groups shown in the following table.



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

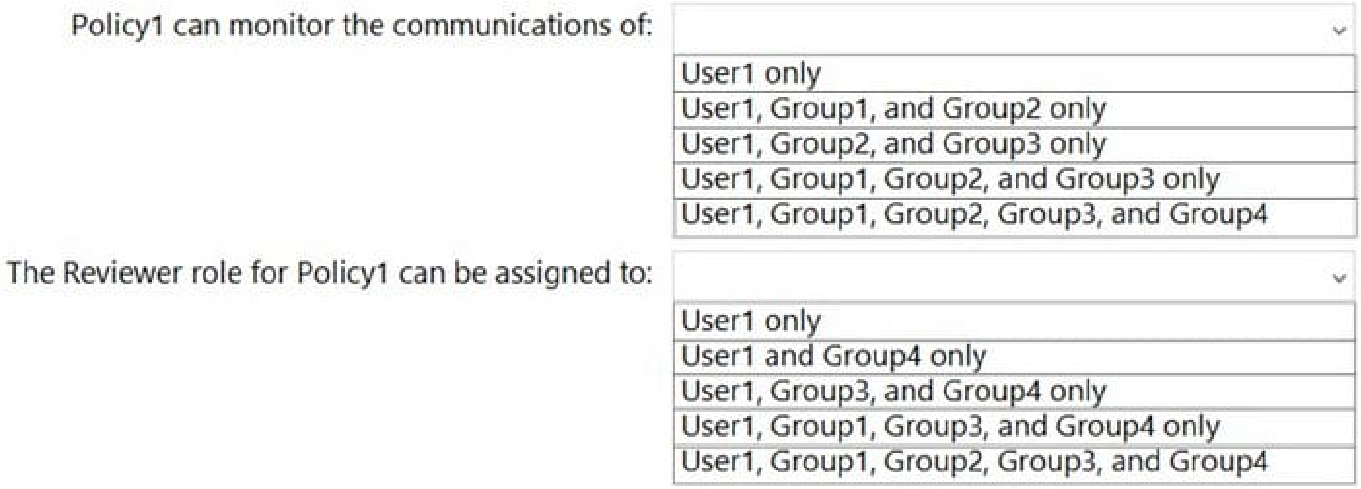
You plan to create a communication compliance policy named Policy1.

You need to identify whose communications can be monitored by Policy1, and who can be assigned the Reviewer role for Policy1.

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

NOTE: Each correct selection is worth one point.

Hot Area:



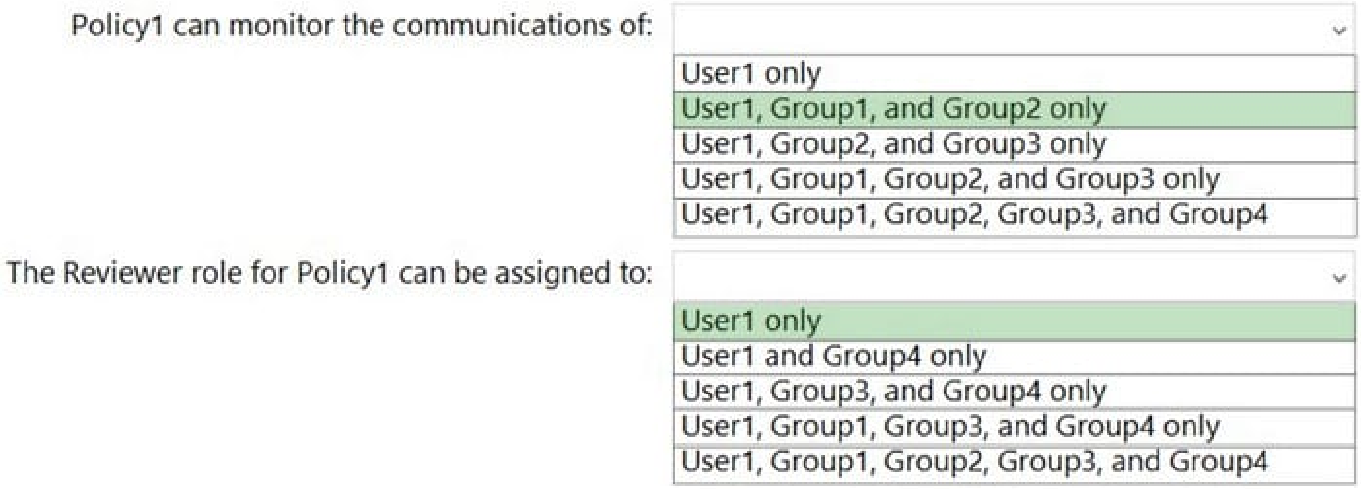
Policy1 can monitor the communications of:

- User1 only
- User1, Group1, and Group2 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

The Reviewer role for Policy1 can be assigned to:

- User1 only
- User1 and Group4 only
- User1, Group3, and Group4 only
- User1, Group1, Group3, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Correct Answer:



Policy1 can monitor the communications of:

- User1 only
- [✓ User1, Group1, and Group2 only]
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

The Reviewer role for Policy1 can be assigned to:

- [✓ User1 only]
- User1 and Group4 only
- User1, Group3, and Group4 only
- User1, Group1, Group3, and Group4 only
- User1, Group1, Group2, Group3, and Group4

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

QUESTION 7

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create?

A. ATP anti-phishing

B. DKIM

C. Anti-spam

D. Anti-malware

Correct Answer: C

"The default value is 15 days in the default anti-spam policy and in new anti-spam policies that you create in PowerShell. The default value is 30 days in new anti-spam policies that you create in the Microsoft 365 Defender portal.A valid value is from 1 to 30 days."

References: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-policies-configure?view=o365-worldwide

QUESTION 8

Your company has a main office and a Microsoft 365 subscription.

You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.

What should you include in the configuration?

A. a user risk policy

B. a sign-in risk policy

C. a named location in Azure Active Directory (Azure AD)

D. an Azure MFA Server

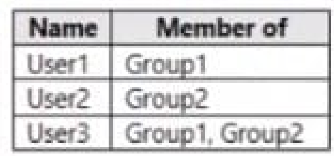
Correct Answer: C

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

QUESTION 9

HOTSPOT

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 Group!, Group2. and Group3 and the users shown in the following table.

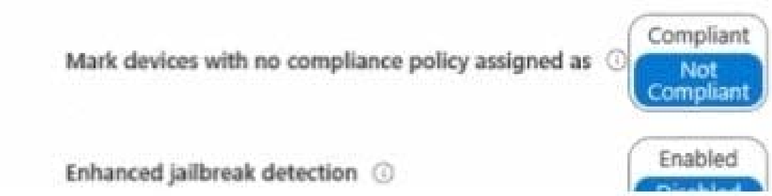


Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

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

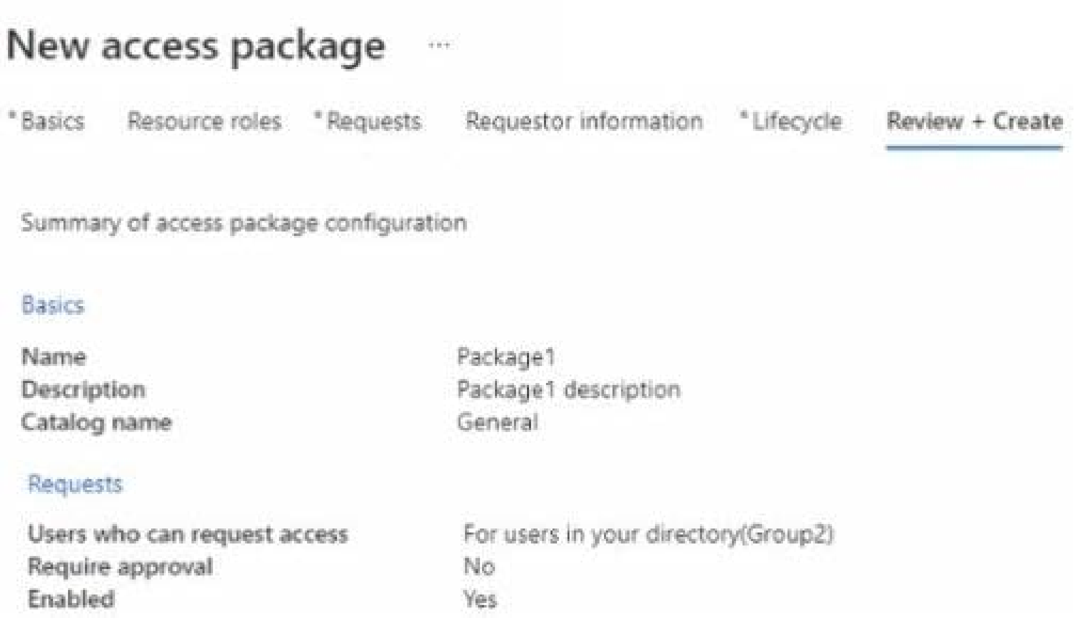
You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager. The Compliance policy settings are configured as shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.



Mark devices with no compliance policy assigned as ⓘ Compliant | **Not Compliant**

Enhanced jailbreak detection ⓘ Enabled



New access package ···

*Basics | Resource roles | *Requests | Requestor information | *Lifecycle | **Review + Create**

Summary of access package configuration

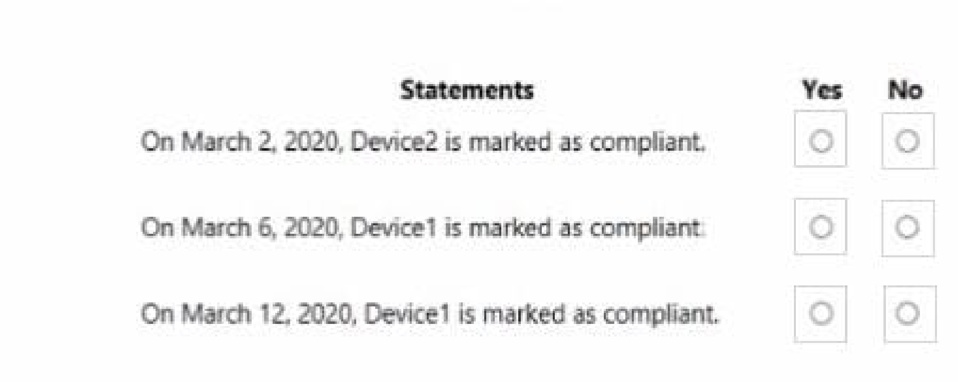
Basics

Name	Package1
Description	Package1 description
Catalog name	General

Requests

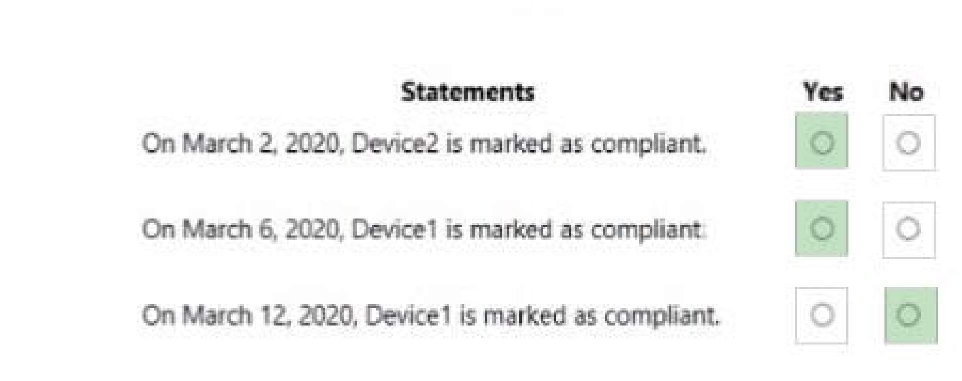
Users who can request access	For users in your directory(Group2)
Require approval	No
Enabled	Yes

Hot Area:



Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Correct Answer:



Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	[✓ ○]	○
On March 6, 2020, Device1 is marked as compliant.	[✓ ○]	○
On March 12, 2020, Device1 is marked as compliant.	○	[✓ ○]

QUESTION 10

You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Intune.

You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.

Which type of device configuration profile should you use?

A. Endpoint protection

B. Device restrictions

C. Identity protection

D. Windows Defender ATP

Correct Answer: A

References: https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

QUESTION 11

SIMULATION

You need to implement a solution to manage when users select links in documents or email messages from Microsoft Office 365 ProPlus applications or Android devices. The solution must meet the following requirements:

1.

Block access to a domain named fabrikam.com

2.

Store information when the users select links to fabrikam.com

To complete this task, sign in to the Microsoft 365 portal.

Correct Answer: See explanation below.

You need to configure a Safe Links policy.

1.

Go to the Office 365 Security and Compliance admin center.

2.

Navigate to Threat Management > Policy > Safe Links.

3.

In the Policies that apply to the entire organization section, select Default, and then click the Edit icon.

4.

In the Block the following URLs section, type in *.fabrikam.com. This meets the first requirement in the question.

5.

In the Settings that apply to content except email section, untick the checkbox labelled Do not track when users click safe links. This meets the second requirement in the question.

6.

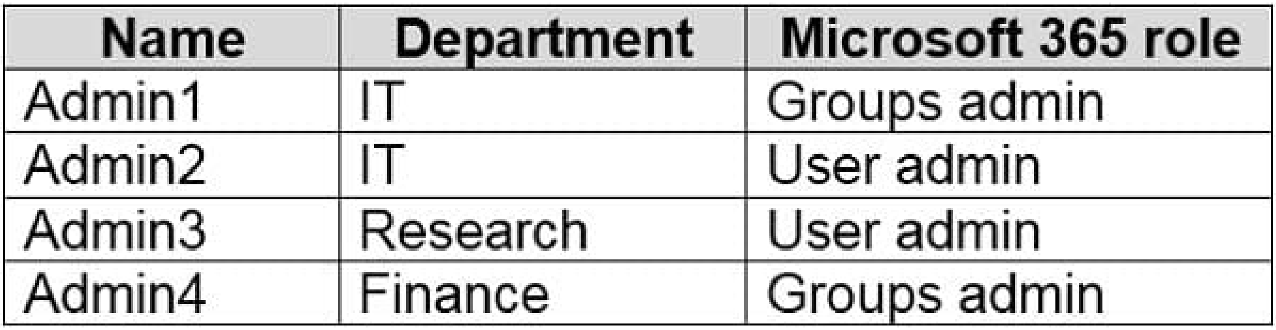
Click Save to save the changes.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-linkspolicies?view=o365-worldwide

QUESTION 12

HOTSPOT

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

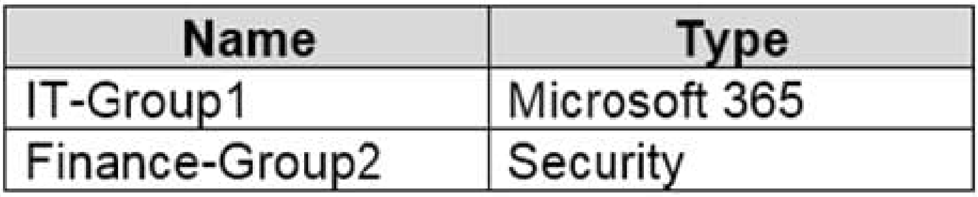


Name	Department	Microsoft 365 role
Admin1	IT	Groups admin
Admin2	IT	User admin
Admin3	Research	User admin
Admin4	Finance	Groups admin

For contoso.com, you create a group naming policy that has the following configuration.

-

You plan to create the groups shown in the following table.

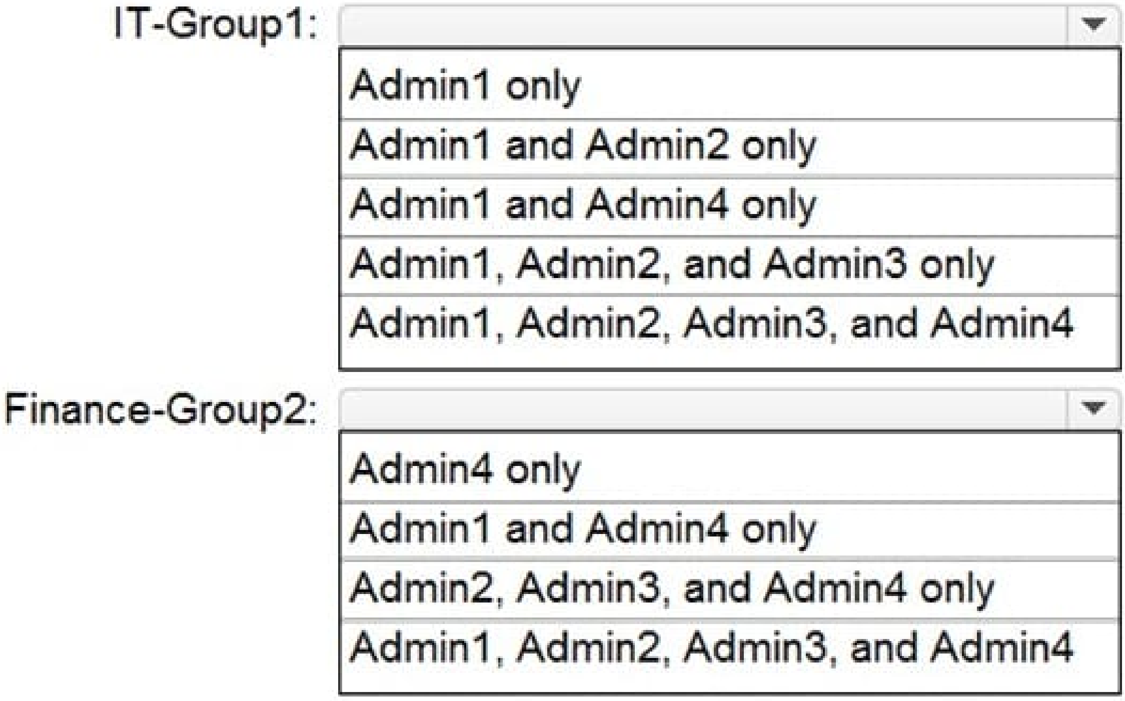


Name	Type
IT-Group1	Microsoft 365
Finance-Group2	Security

Which users can be used to create each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



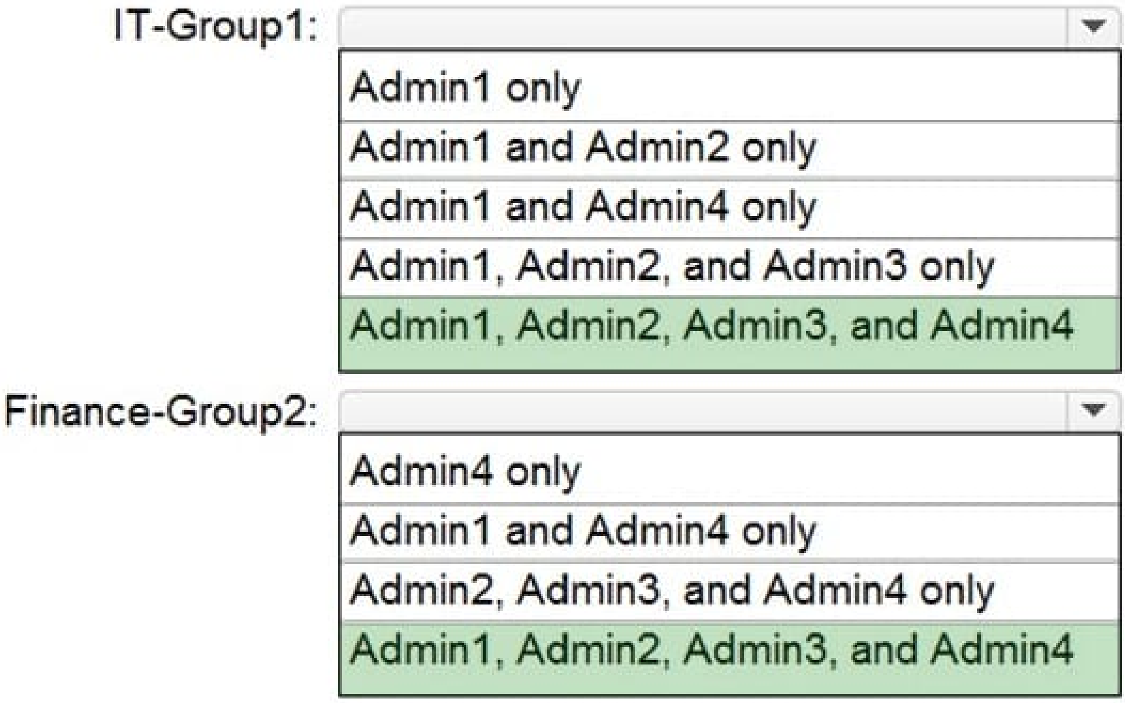
IT-Group1:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin4 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Finance-Group2:

- Admin4 only
- Admin1 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Correct Answer:



IT-Group1:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin4 only
- Admin1, Admin2, and Admin3 only
- [✓ Admin1, Admin2, Admin3, and Admin4]

Finance-Group2:

- Admin4 only
- Admin1 and Admin4 only
- Admin2, Admin3, and Admin4 only
- [✓ Admin1, Admin2, Admin3, and Admin4]

Reference:

https://office365itpros.com/2020/01/22/using-groups-admin-role/

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

QUESTION 13

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security and Compliance admin center, you create a label that designates personal data.

You need to auto-apply the new label to all the content in Site1.

What should you do first?

A. From PowerShell, run Set-ManagedContentSettings.

B. From PowerShell, run Set-ComplianceTag.

C. From the Security and Compliance admin center, create a Data Subject Request (DSR).

D. Remove Azure Information Protection from the Site1 files.

Correct Answer: D

References: https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in-office-365

QUESTION 14

DRAG DROP

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

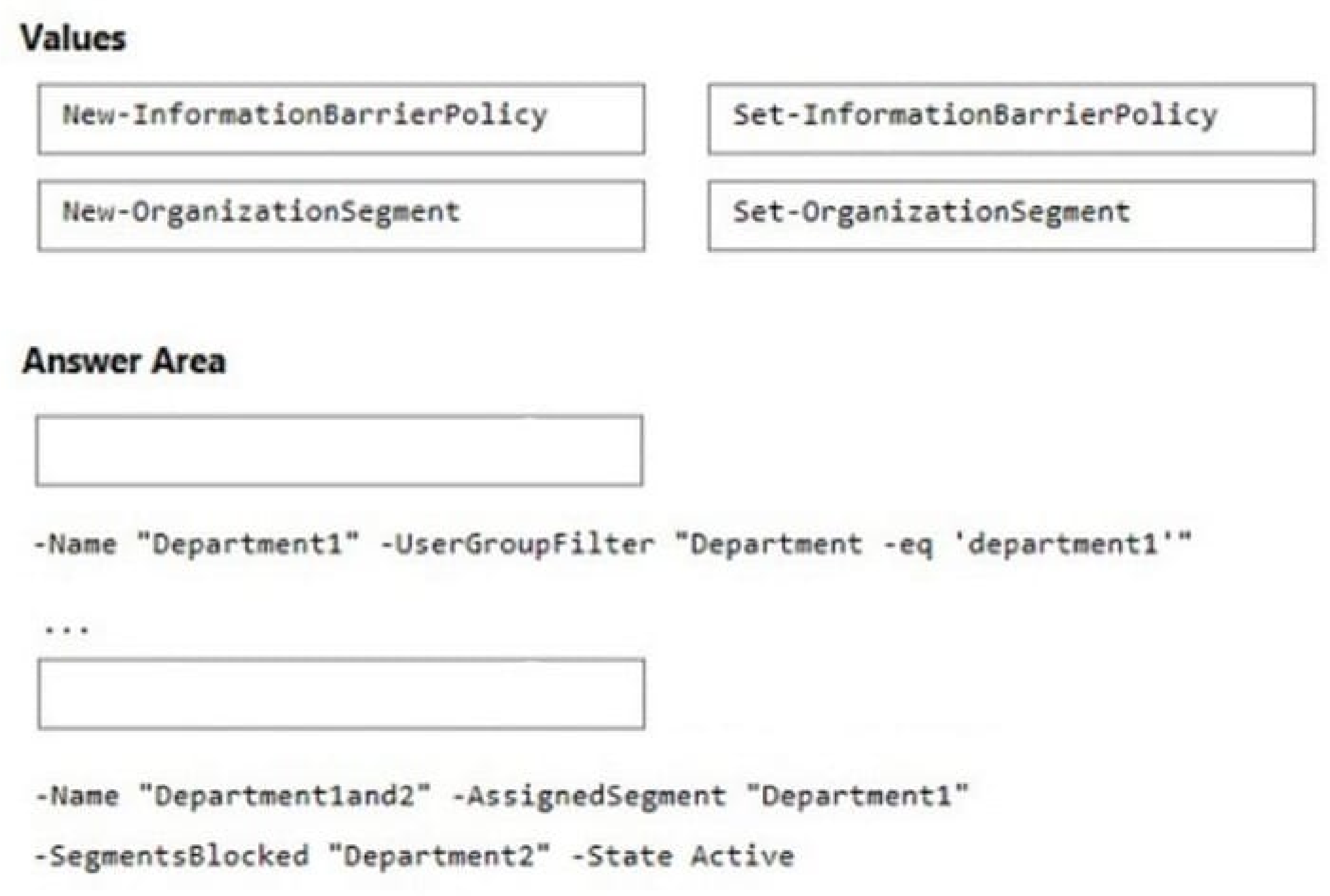
You need to prevent communication between the users in department1 and the users in department2.

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.

Select and Place:



Values

New-InformationBarrierPolicy

Set-InformationBarrierPolicy

New-OrganizationSegment

Set-OrganizationSegment

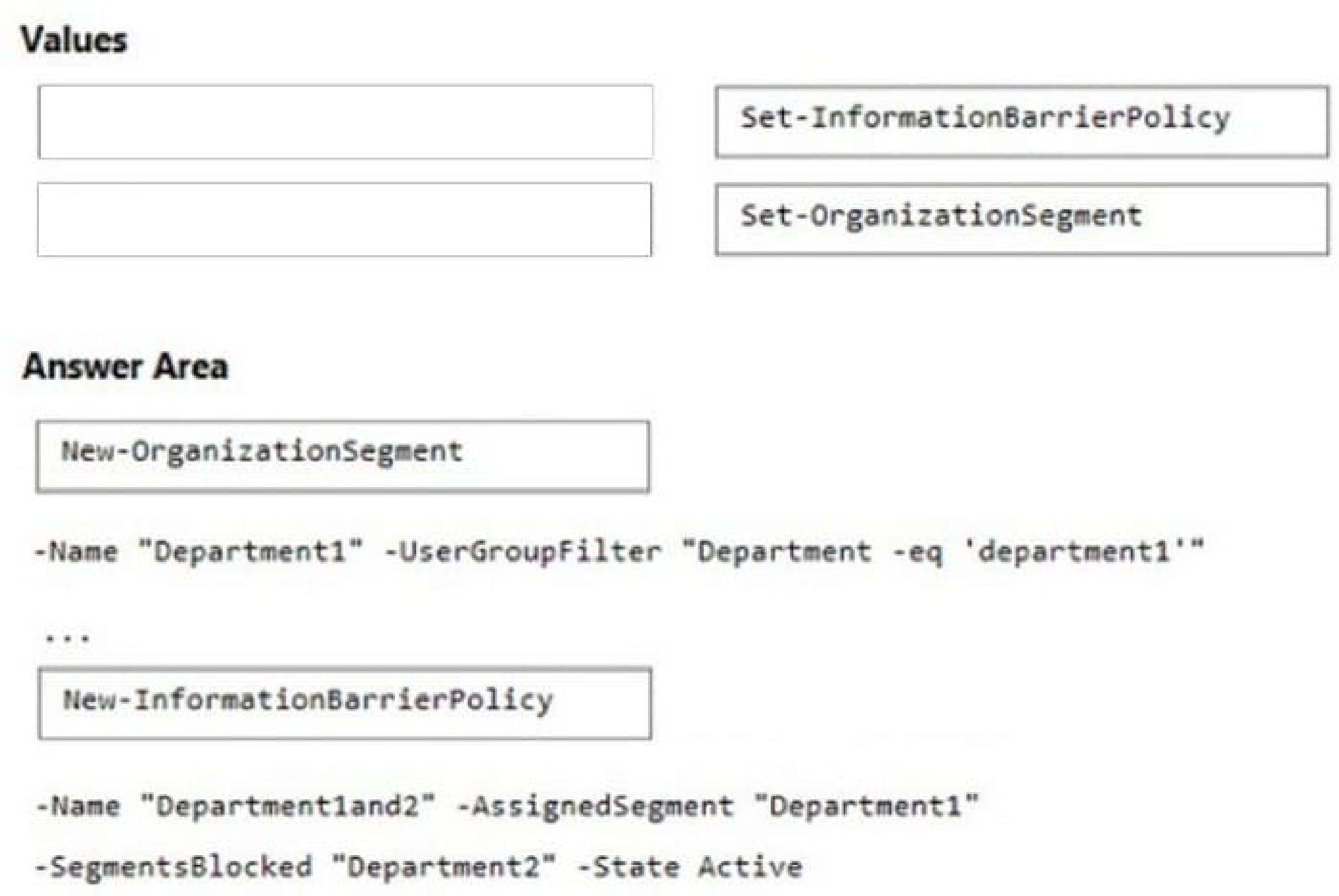
Answer Area

```
-Name "Department1" -UserGroupFilter "Department -eq 'department1'"

...

-Name "Department1and2" -AssignedSegment "Department1"
-SegmentsBlocked "Department2" -State Active
```

Correct Answer:



Values

Set-InformationBarrierPolicy

Set-OrganizationSegment

Answer Area

New-OrganizationSegment

```
-Name "Department1" -UserGroupFilter "Department -eq 'department1'"

...
```

New-InformationBarrierPolicy

```
-Name "Department1and2" -AssignedSegment "Department1"

-SegmentsBlocked "Department2" -State Active
```

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]

-UserGroupFilter

[-Confirm]

[-WhatIf]

[]

Box 2: New-InformationBarrierPolicy

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

Reference:

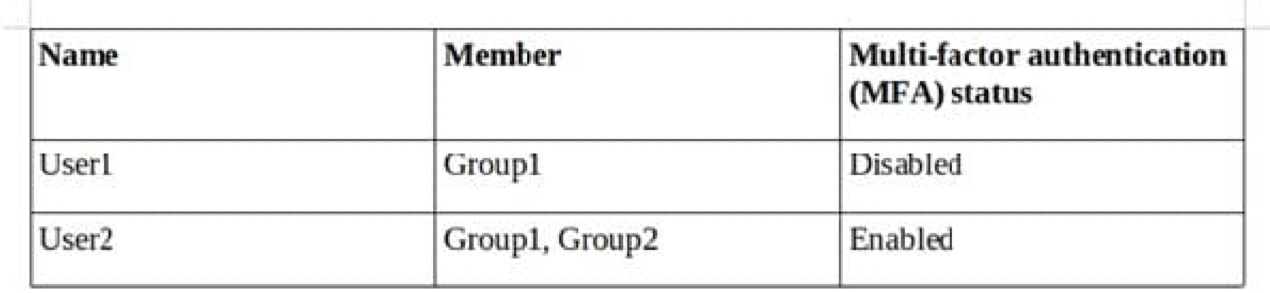
https://docs.microsoft.com/en-us/powershell/module/exchange/new-organizationsegment

https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies

QUESTION 15

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	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

1.

Assignments: Include Group1, Exclude Group2

2.

Conditions: Sign in risk of Low and above

3.

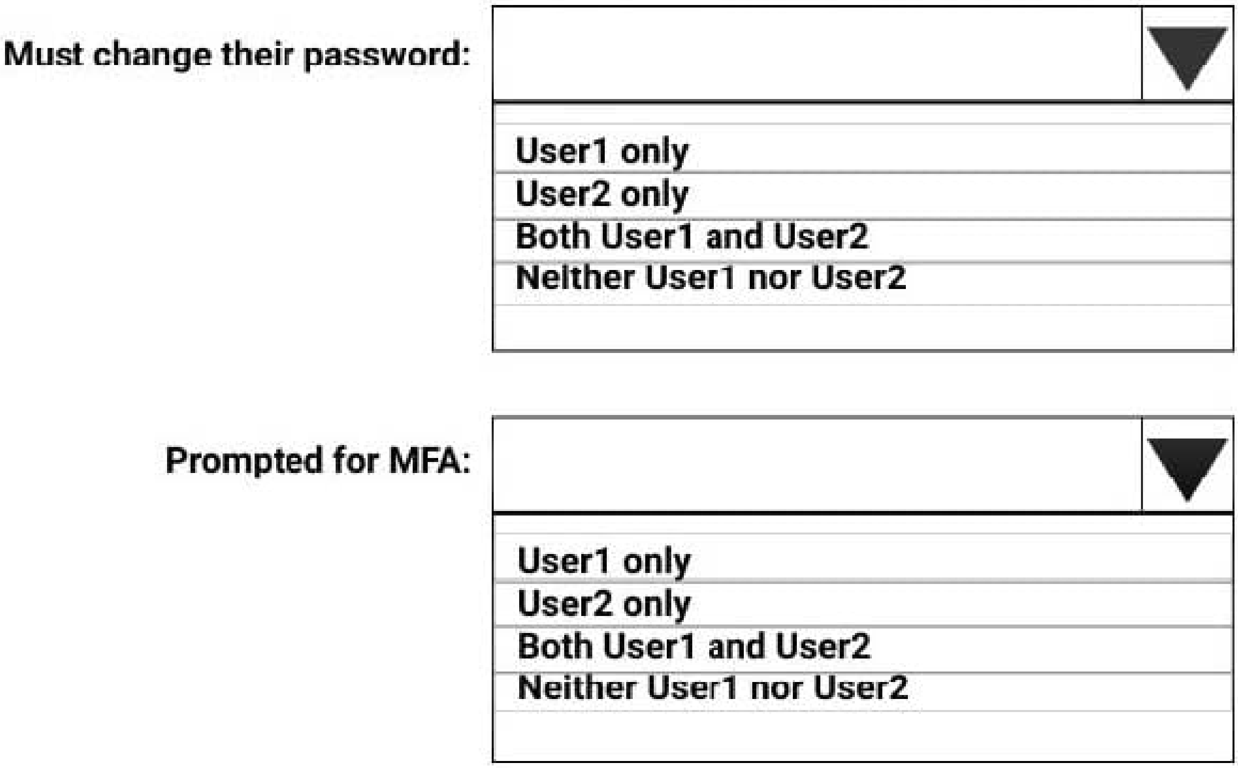
Access: Allow access, Require password change

You need to identify how the policy affects User1 and User2.

What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



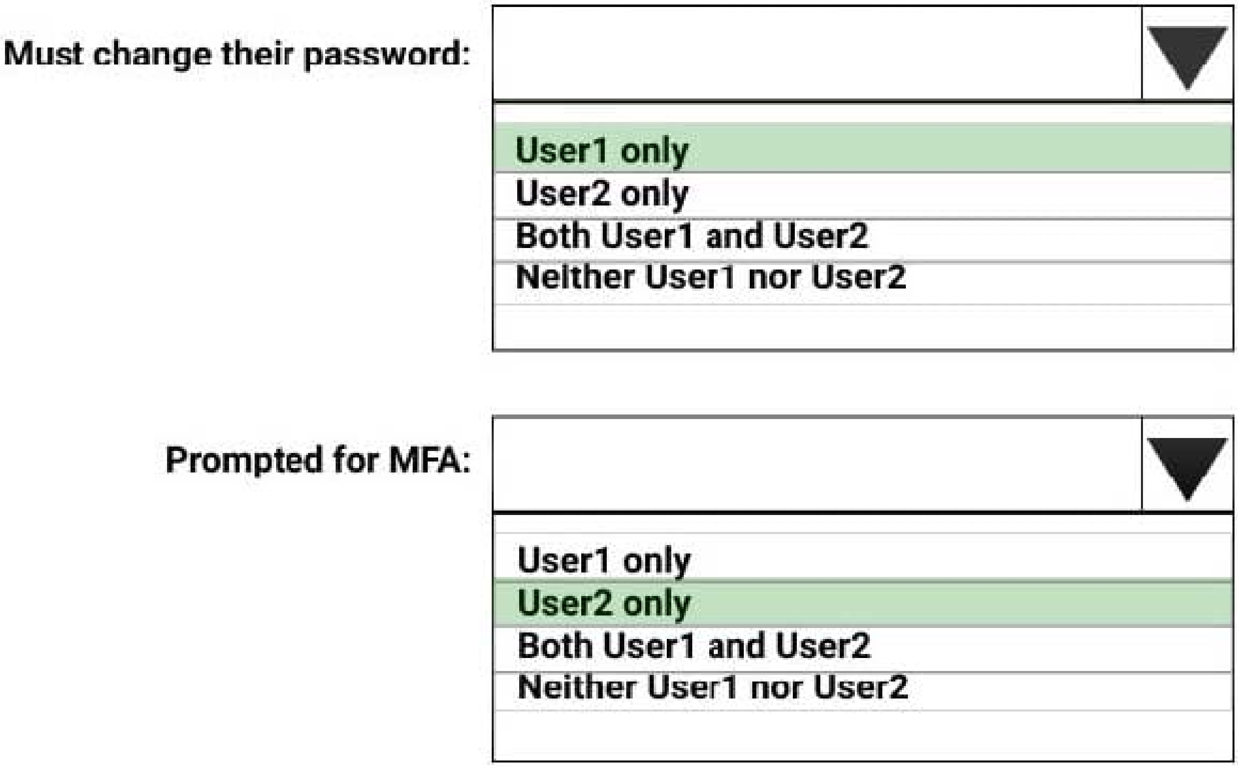
Must change their password:

User1 only
User2 only
Both User1 and User2
Neither User1 nor User2

Prompted for MFA:

User1 only
User2 only
Both User1 and User2
Neither User1 nor User2

Correct Answer:



Must change their password:

[✓ User1 only]
User2 only
Both User1 and User2
Neither User1 nor User2

Prompted for MFA:

User1 only
[✓ User2 only]
Both User1 and User2
Neither User1 nor User2

Box 1: User1 only

The Azure AD Identity Protection user risk policy is excluded from Group2. Exclusion overrides inclusion. Therefore, the policy will not affect User2. Thus, only

User 1 needs to change the Password.

Box 2: User2 only

MFA will be triggered for User 2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies