Microsoft

MS-101

Microsoft 365 Mobility and Security

QUESTION & ANSWERS

QUESTION 1

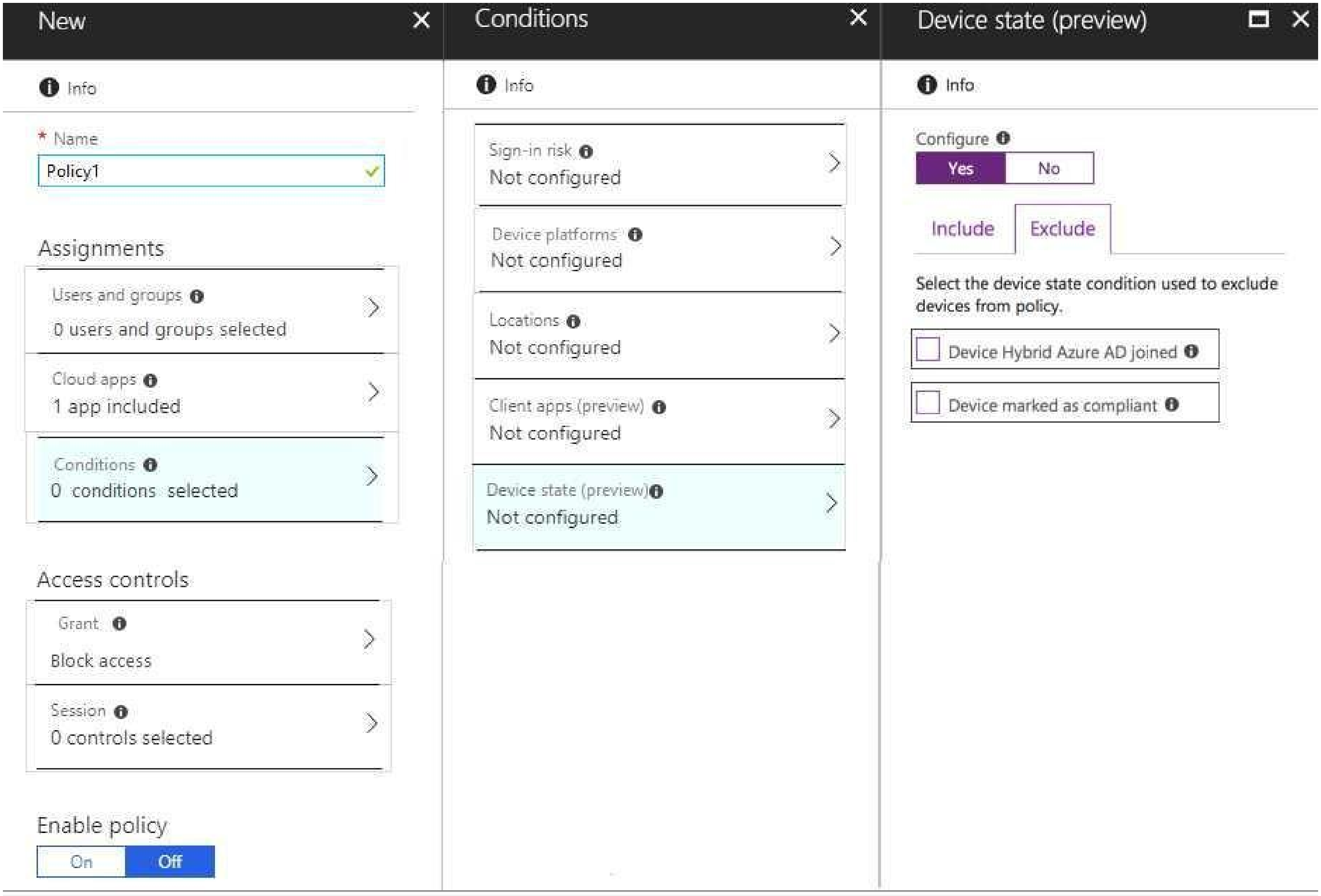
HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements.

You add Exchange Online as a cloud app.

Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



New

Info

* Name

Policy1

Assignments

Users and groups
0 users and groups selected

Cloud apps
1 app included

Conditions
0 conditions selected

Access controls

Grant
Block access

Session
0 controls selected

Enable policy

On [✓ Off]

Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (preview)
Not configured

Device state (preview)
Not configured

Device state (preview)

Info

Configure

[✓ Yes] No

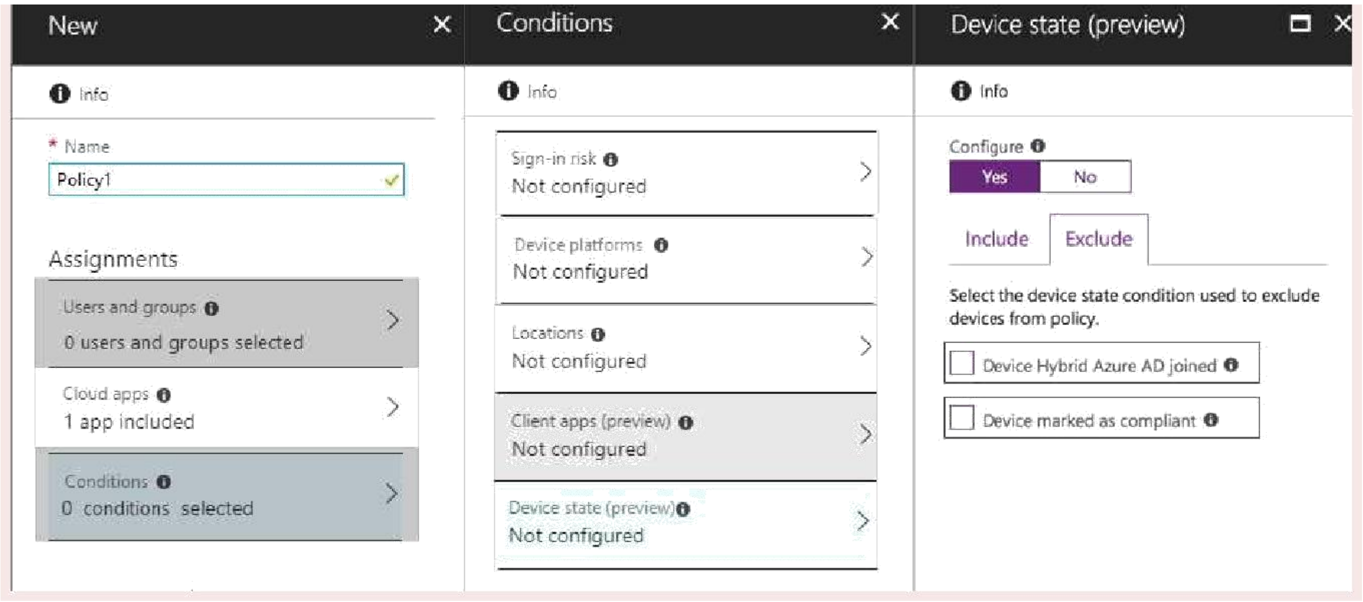
Include | Exclude

Select the device state condition used to exclude devices from policy.

□ Device Hybrid Azure AD joined

□ Device marked as compliant

Correct Answer:



New

Info

* Name

Policy1

Assignments

Users and groups
0 users and groups selected

Cloud apps
1 app included

Conditions
0 conditions selected

Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (preview)
Not configured

Device state (preview)
Not configured

Device state (preview)

Info

Configure
Yes | No

Include | Exclude

Select the device state condition used to exclude devices from policy.

□ Device Hybrid Azure AD joined

□ Device marked as compliant

QUESTION 2

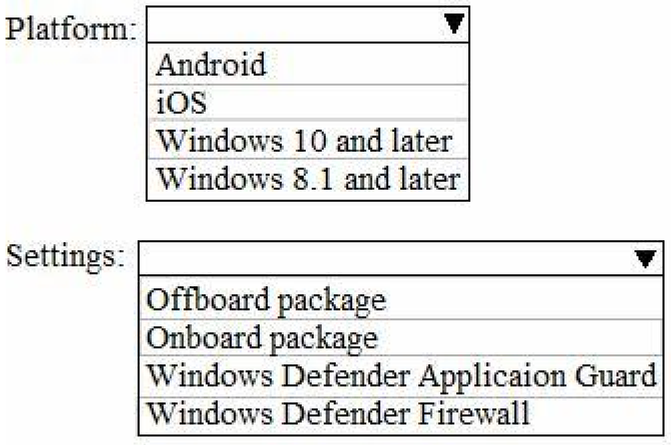
HOTSPOT

You have a Microsoft 365 subscription.

You need to implement Windows Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

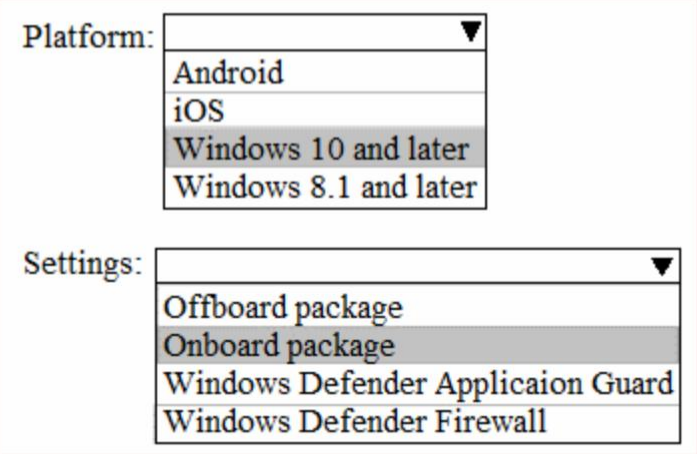
NOTE: Each correct selection is worth one point.



Platform: ▼
- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings: ▼
- Offboard package
- Onboard package
- Windows Defender Applicaion Guard
- Windows Defender Firewall

Correct Answer:



Platform:

Android
iOS
[✓ Windows 10 and later]
Windows 8.1 and later

Settings:

Offboard package
[✓ Onboard package]
Windows Defender Applicaion Guard
Windows Defender Firewall

Explanation/Reference:

References: https://docs.microsoft.com/en-us/intune/advanced-threat-protection

QUESTION 3

You have a Microsoft 365 subscription. You have a user named User1.
You need to ensure that User1 can place a hold on all mailbox content.
Which rote should you assign to User1?

A. e Discovery Manager from the Security & Compliance admin center
B. compliance management from the Exchange admin center
C. User management administrator from the Microsoft 365 admin center
D. Information Protection administrator from the Azure Active Directory admin center

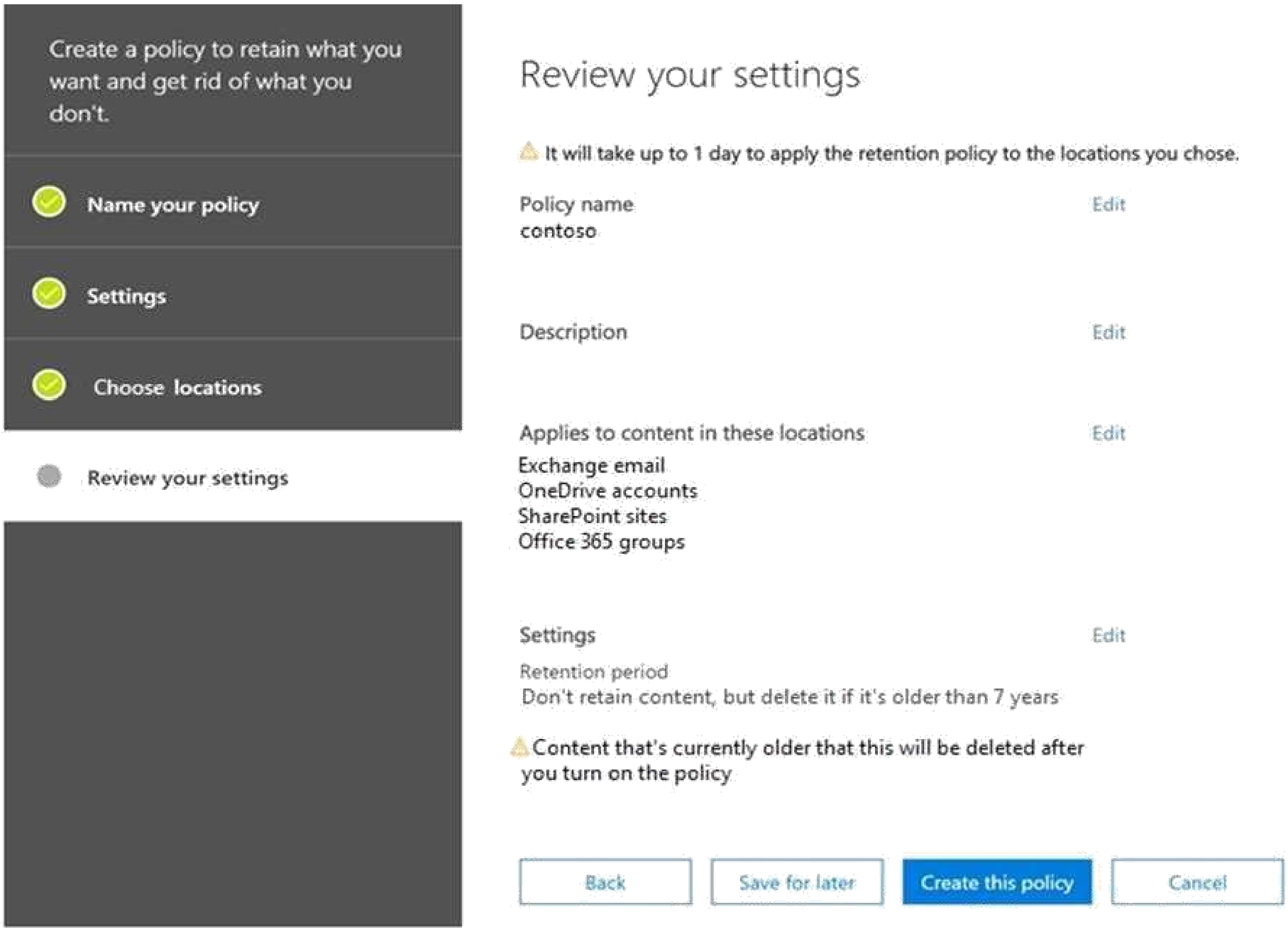
Correct Answer: A

Explanation/Reference:

References: https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-andcompliance-permissions?view=exchserver-2019

QUESTION 4

HOTSPOT
You have a Microsoft 365 tenant.
You plan to create a retention policy as shown in the following exhibit.



Create a policy to retain what you want and get rid of what you don't.

- ● Name your policy
- ● Settings
- ● Choose locations
- ○ Review your settings

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name — Edit
contoso

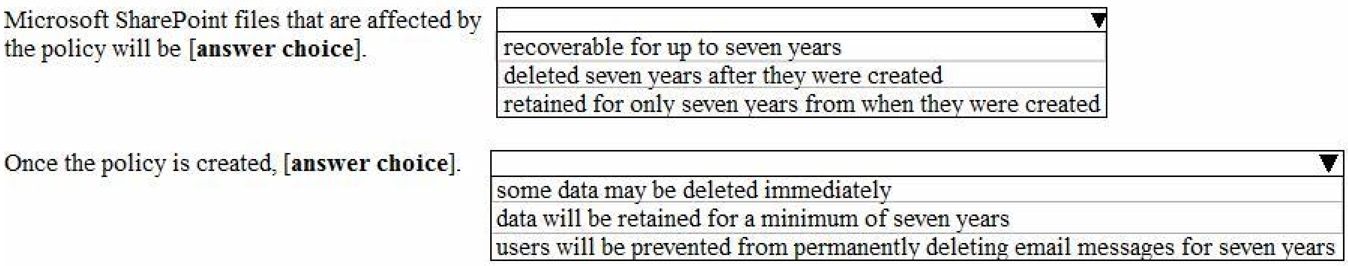
Description — Edit

Applies to content in these locations — Edit
Exchange email
OneDrive accounts
SharePoint sites
Office 365 groups

Settings — Edit
Retention period
Don't retain content, but delete it if it's older than 7 years

⚠Content that's currently older that this will be deleted after you turn on the policy

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.



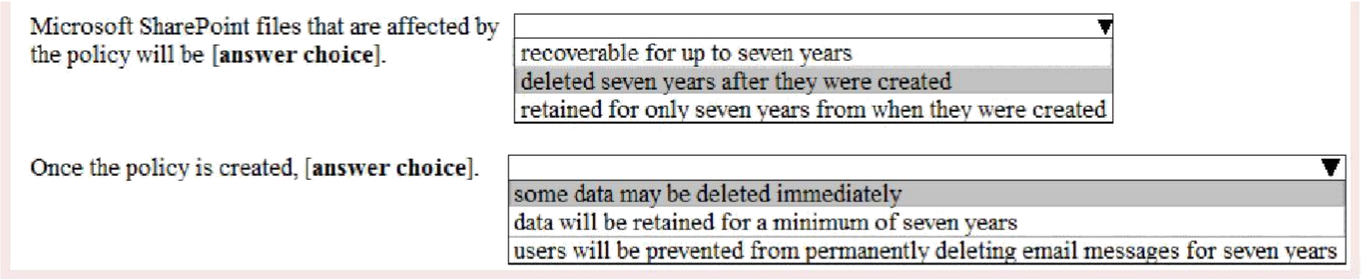
Microsoft SharePoint files that are affected by the policy will be [**answer choice**].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [**answer choice**].

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Correct Answer:



Microsoft SharePoint files that are affected by the policy will be [**answer choice**]. ▼
- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [**answer choice**]. ▼
- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

QUESTION 5

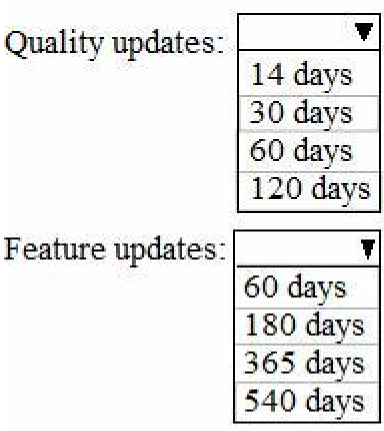
HOTSPOT

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

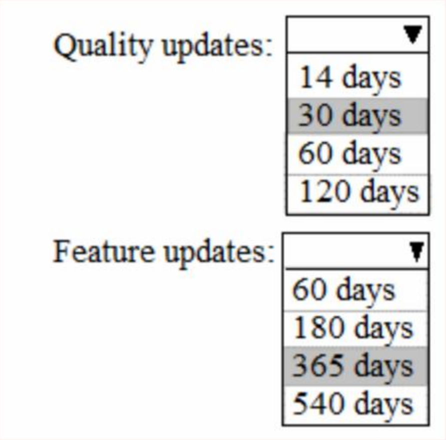
NOTE: Each correct selection is worth one point.



Quality updates: ▼
- 14 days
- 30 days
- 60 days
- 120 days

Feature updates: ▼
- 60 days
- 180 days
- 365 days
- 540 days

Correct Answer:



Quality updates: ▼

14 days
[✓ 30 days]
60 days
120 days

Feature updates: ▼

60 days
180 days
[✓ 365 days]
540 days

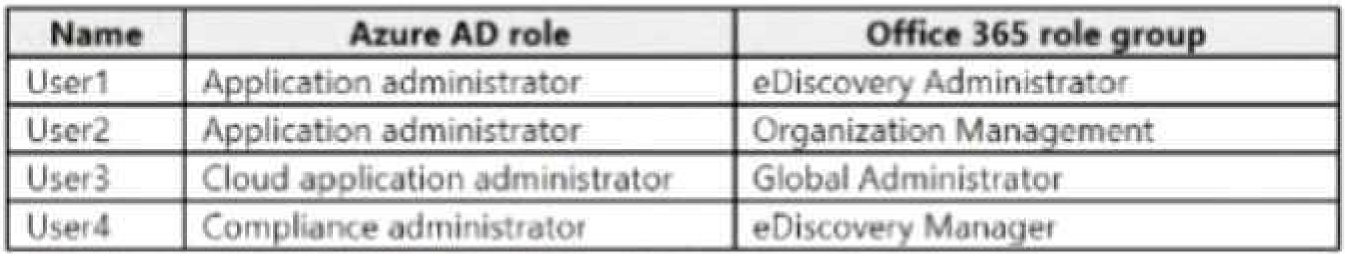
Explanation/Reference:

References: https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

QUESTION 6

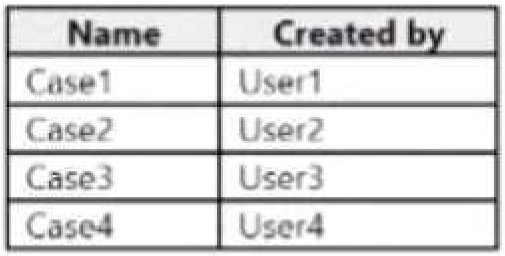
HOTSPOT

You have a Microsoft 365 tenet named Contoso.com. the tenant contains the users shown in the following



Name	Azure AD role	Office 365 role group
User1	Application administrator	eDiscovery Administrator
User2	Application administrator	Organization Management
User3	Cloud application administrator	Global Administrator
User4	Compliance administrator	eDiscovery Manager

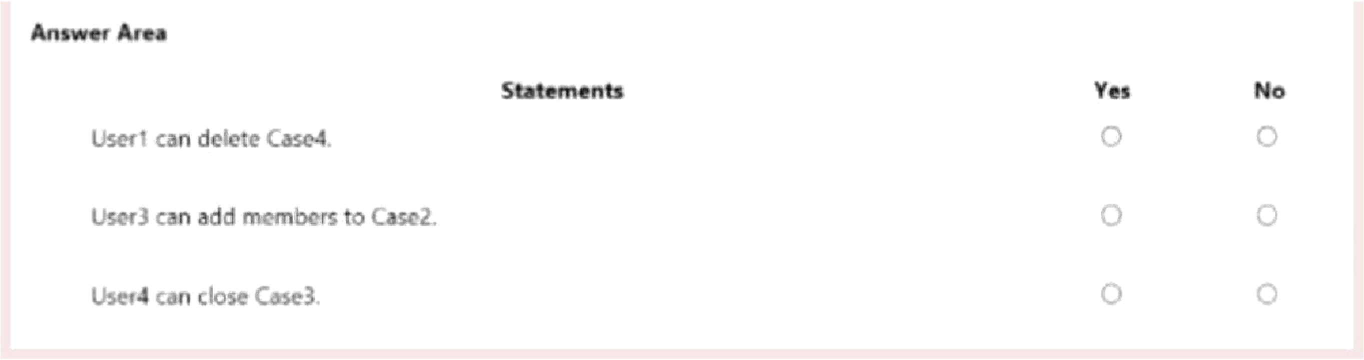
You have an eDiscovery case shown in the follow table.



Name	Created by
Case1	User1
Case2	User2
Case3	User3
Case4	User4

For each of the following statements select yes of the statements is true. Otherwise, select NO. NOTE: each correct selection is worth one point.

Correct Answer:



Answer Area

Statements	Yes	No
User1 can delete Case4.	○	○
User3 can add members to Case2.	○	○
User4 can close Case3.	○	○

QUESTION 7

You have a Microsoft 365 tenant.
All users are assigned the Enterprise Mobility + Security license.
You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD),the
device is enrolled in Microsoft Intune automatically.
What should you configure?

A. Enrollment restrictions from the Intune admin center
B. device enrollment managers from the Intune admin center
C. MAM User scope from the Azure Active Directory admin center D.
MDM User scope from the Azure Active Directory admin center

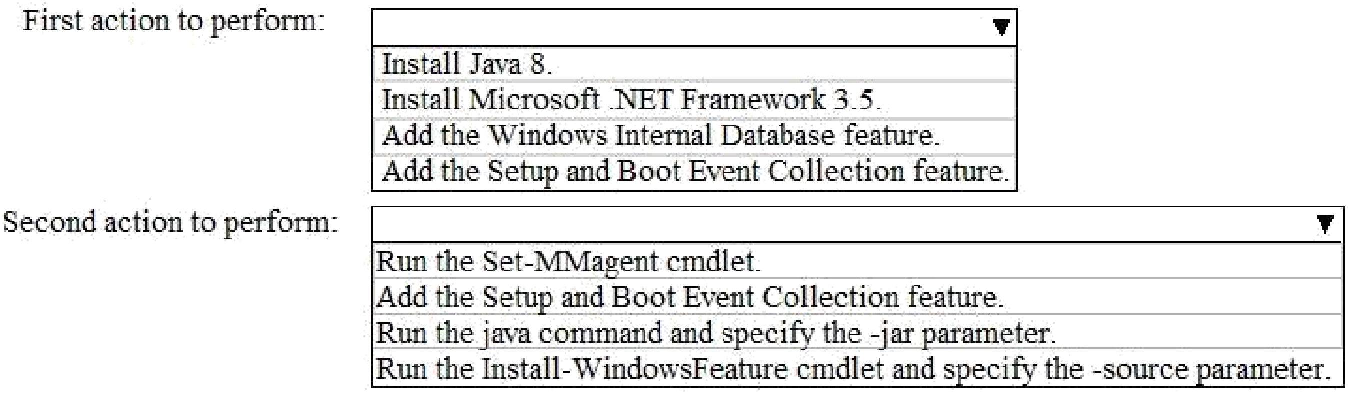
Correct Answer: D

Explanation/Reference:

References: https://docs.microsoft.com/en-us/intune/windows-enroll

QUESTION 8

HOTSPOT
Your company uses Microsoft Cloud App Security.
You plan to integrate Cloud App Security and security information and event management (SIEM).
You need to deploy a SIEM agent on a server that runs Windows Server 2016.
What should you do? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



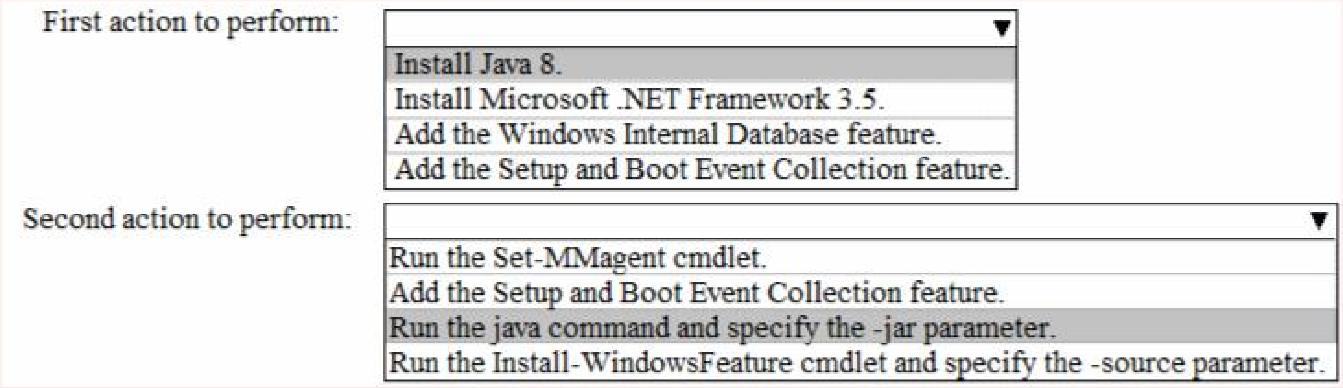
First action to perform:

- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Correct Answer:



First action to perform:

- [✓ Install Java 8.]
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

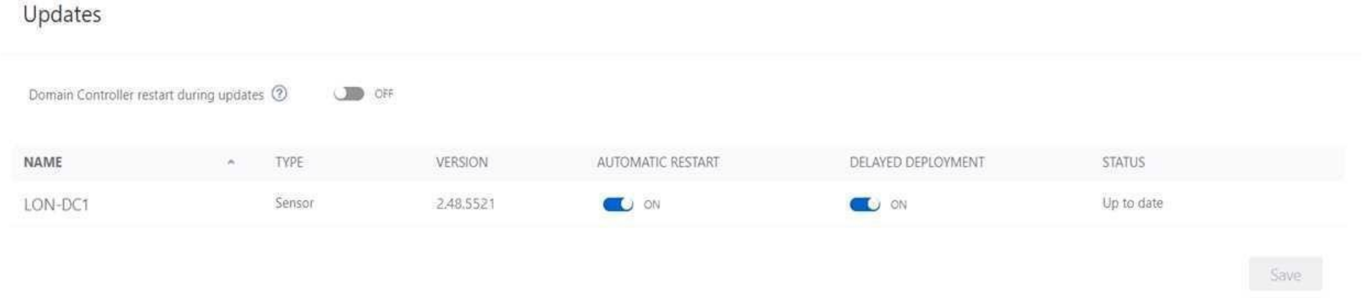
- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- [✓ Run the java command and specify the -jar parameter.]
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Explanation/Reference:

References: https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-withoffice-365-cas

QUESTION 9

You implement Microsoft Azure Advanced Threat Protection (Azure ATP).
You have an Azure ATP sensor configured as shown in the following exhibit.



Updates

Domain Controller restart during updates ⓘ OFF

NAME	TYPE	VERSION	AUTOMATIC RESTART	DELAYED DEPLOYMENT	STATUS
LON-DC1	Sensor	2.48.5521	ON	ON	Up to date

How long after the Azure ATP cloud service is updated will the sensor update?

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

Correct Answer: E

Explanation/Reference:

References: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new

QUESTION 10

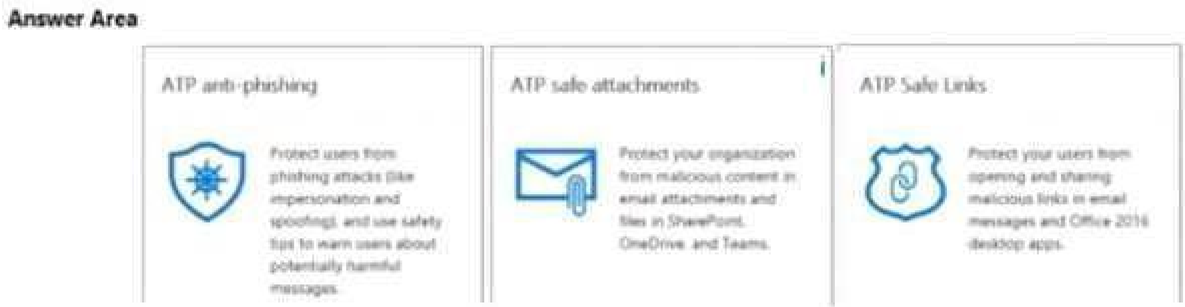
HOTSPOT

Your company has a Microsoft 365 subscription.

You need to configure Microsoft 365 to meet the following requirements:

- Malware found in email attachments must be quarantined for 20 days.
- The email address of senders to your company must be verified.

Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

ATP anti-phishing

Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.

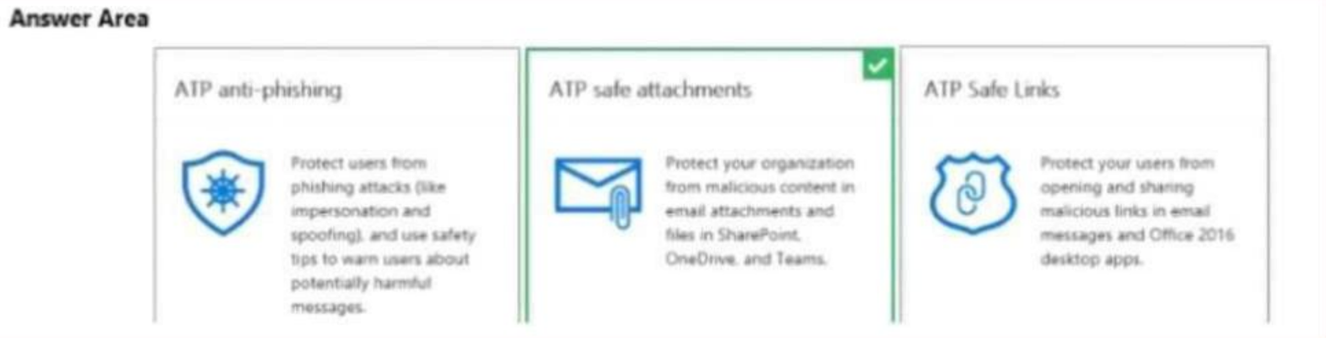
ATP safe attachments

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP Safe Links

Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.

Correct Answer:



Answer Area

ATP anti-phishing

Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.

ATP safe attachments ✓

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP Safe Links

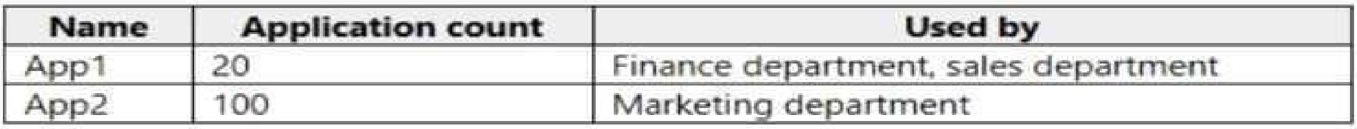
Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.

QUESTION 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.



Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the importance status of App2 to Low install count.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A

Explanation/Reference:

If an app is installed on less than 2% of the targeted devices, it's marked Low install count. Two percent is the default value. You can adjust the threshold in the readiness settings from 0% to 10%. Desktop Analytics automatically marks these apps as Ready to upgrade. Reference:

https://docs.microsoft.com/en-us/configmgr/desktop-analytics/about-deployment-plans

QUESTION 12

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices. You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices. You need to recommend a Windows 10 deployment method. What should you recommend?

A. a provisiong package
B. an in place upgrade
C. wipe and load refresh
D. Windows Autopilot

Correct Answer: A

Explanation/Reference:

References: https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

QUESTION 13

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices. Your company uses the following types of devices:

•Windows 10
•Windows 8.1
•Android
• iOS
Which devices can be managed by using co-management?

A. Windows 10 and Windows 8.1 only
B. Windows 10, Android, and iOS only
C. Windows 10 only
D. Windows 10, Windows 8.1, Android, and iOS

Correct Answer: D

Explanation/Reference:

References: https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-managementsolution#bkmk_intune

QUESTION 14

Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.
What should you do from the Security & Compliance admin center?

A. Create a data toss prevention (DLP) policy that has a Content is shared condition.
B. Modify the default safe links policy.
C. Create a data loss prevention (DLP) policy that has a Content contains condition.
D. Create a new safe links policy.

Correct Answer: D

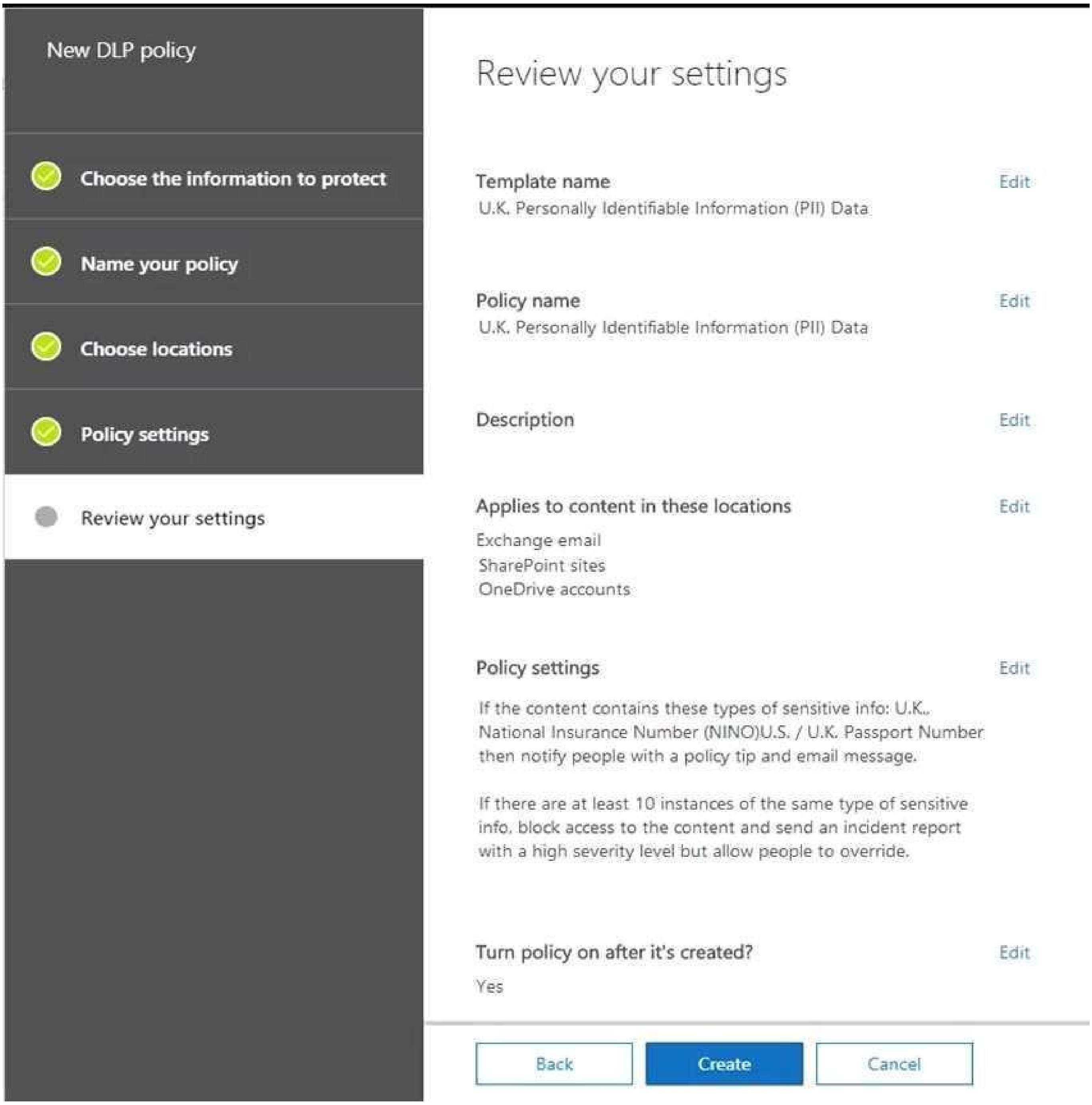
Explanation/Reference:

References: https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-linkspolicies#policies-that-apply-to-specific-email-recipients

QUESTION 15

HOTSPOT
Your company is based in the United Kingdom (UK).
Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company.
The policy is configured as shown in the following exhibit.



New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

✓ Policy settings

● Review your settings

Review your settings

Template name — Edit
U.K. Personally Identifiable Information (PII) Data

Policy name — Edit
U.K. Personally Identifiable Information (PII) Data

Description — Edit

Applies to content in these locations — Edit
Exchange email
SharePoint sites
OneDrive accounts

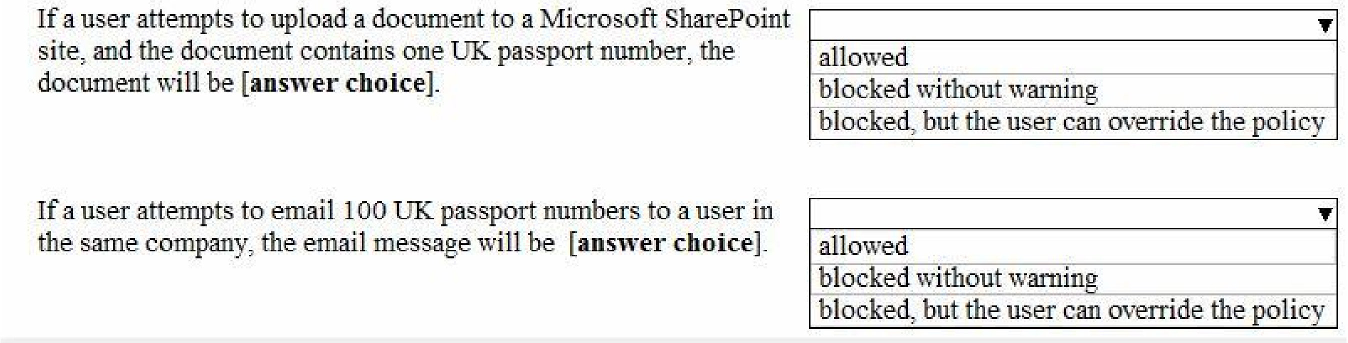
Policy settings — Edit

If the content contains these types of sensitive info: U.K.. National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.

If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created? — Edit
Yes

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



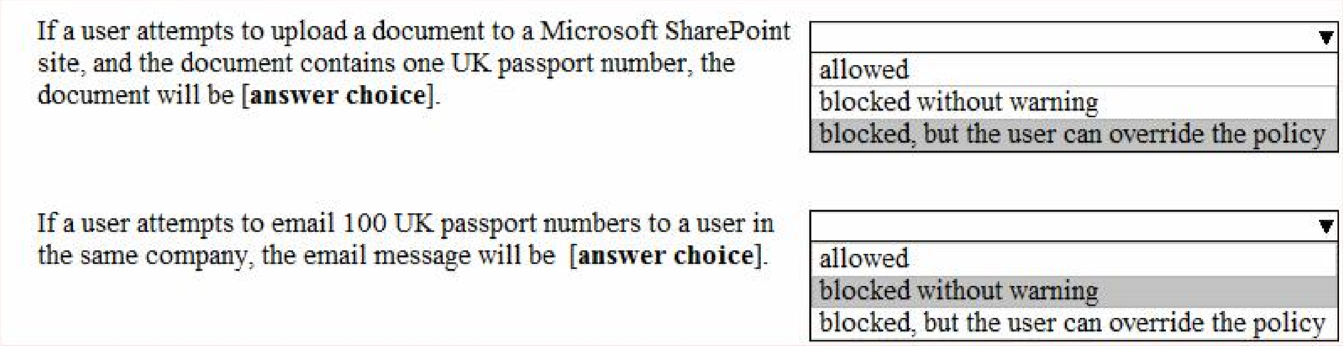
If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [**answer choice**].

- allowed
- blocked without warning
- blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [**answer choice**].

- allowed
- blocked without warning
- blocked, but the user can override the policy

Correct Answer:



If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [**answer choice**].

- allowed
- blocked without warning
- [✓ blocked, but the user can override the policy]

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [**answer choice**].

- allowed
- [✓ blocked without warning]
- blocked, but the user can override the policy

Explanation/Reference:

References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 16

Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender
Advanced Threat Protection (ATP).
You need to view which Windows Defender ATP alert events have a high severity and occurred during the last seven days.
What should you use in Windows Defender ATP?

A. the threat intelligence API
B. Automated investigations
C. Threat analytics
D. Advanced hunting

Correct Answer: B

Explanation/Reference:

References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defenderatp/investigate-alertswindowsdefender-advanced-threat-protection
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defenderatp/automatedinvestigationswindows-defender-advanced-threat-protection

QUESTION 17

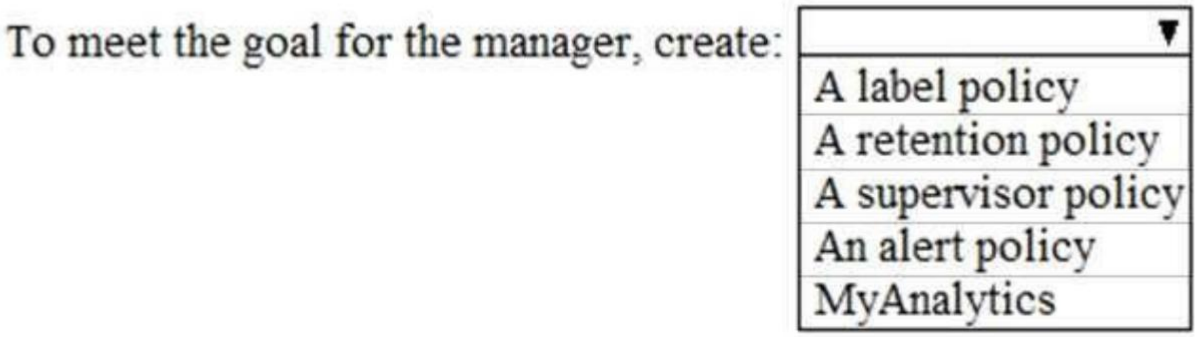
HOTSPOT
You have a Microsoft 365 subscription.
You have a group named Support. Users in the Support group frequently send email messages to

external users.

The manager of the Support group wants to randomly review messages that contain attachments. You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

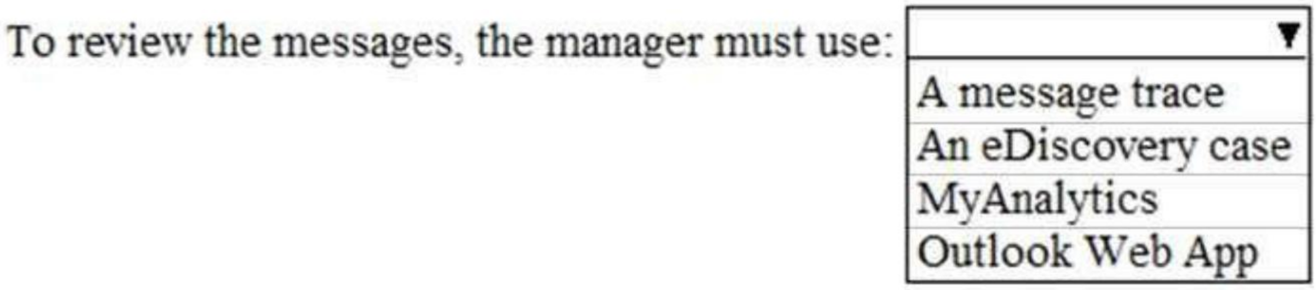
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



To meet the goal for the manager, create: ▼

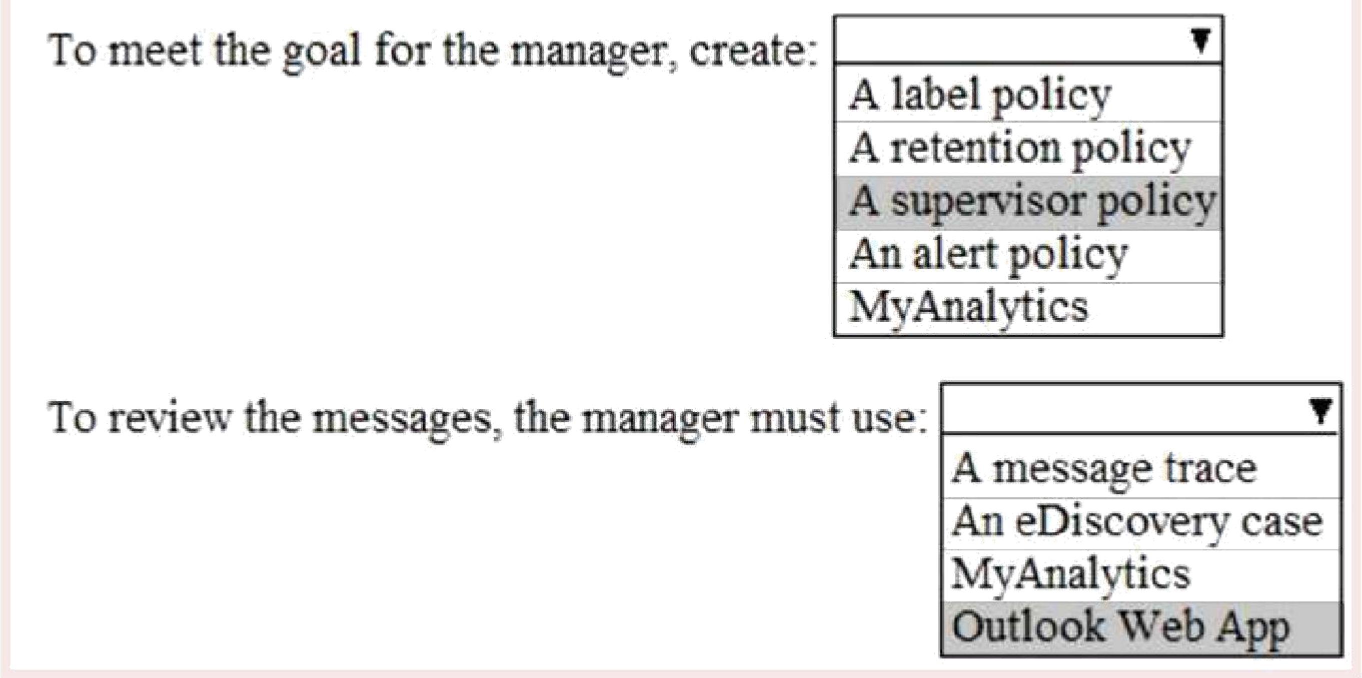
- A label policy
- A retention policy
- A supervisor policy
- An alert policy
- MyAnalytics



To review the messages, the manager must use: ▼

- A message trace
- An eDiscovery case
- MyAnalytics
- Outlook Web App

Correct Answer:



To meet the goal for the manager, create: ▼

- A label policy
- A retention policy
- [✓ A supervisor policy]
- An alert policy
- MyAnalytics

To review the messages, the manager must use: ▼

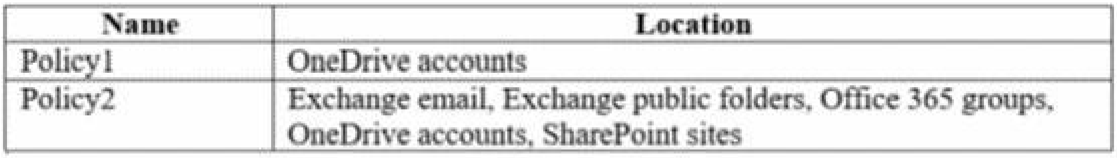
- A message trace
- An eDiscovery case
- MyAnalytics
- [✓ Outlook Web App]

Explanation/Reference:

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

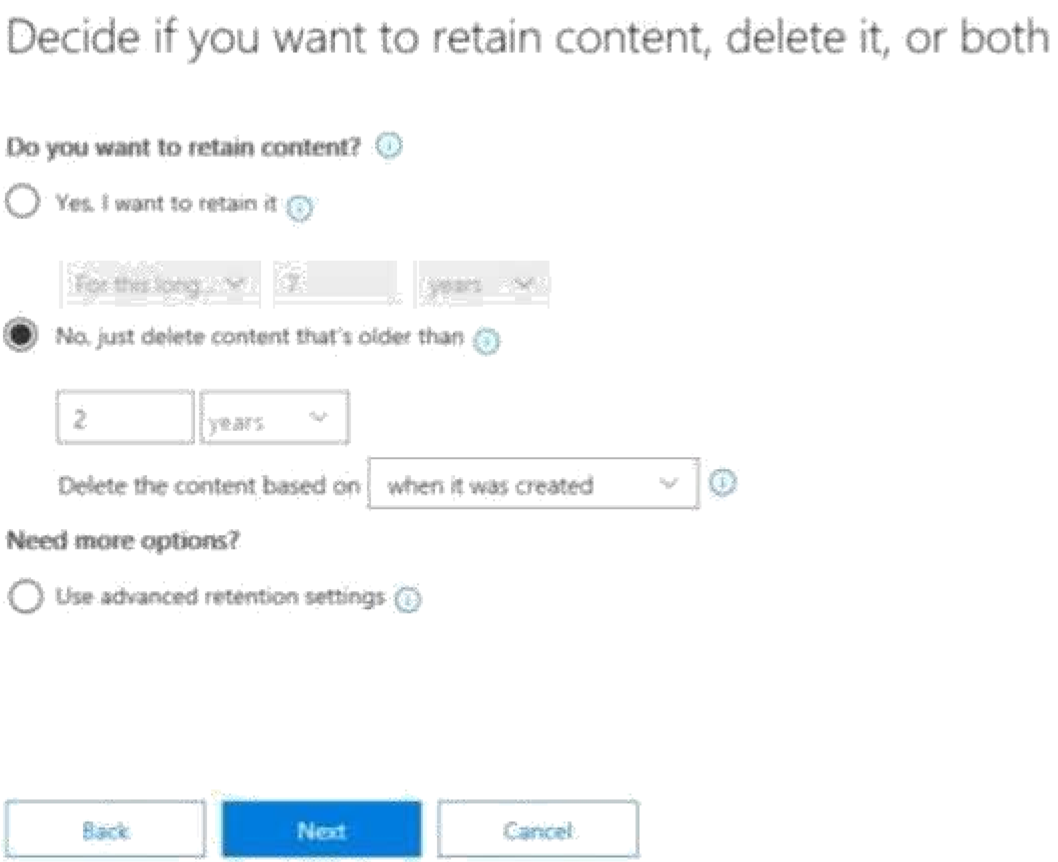
QUESTION 18

HOTSPOT
You have retention policies in Microsoft 365 as shown in the following table.



Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 is configured as shown in the Policy1 exhibit. (Click the Policy1 tab.)



Decide if you want to retain content, delete it, or both

Do you want to retain content?

○ Yes, I want to retain it

For this long... | 7 | years

● No, just delete content that's older than

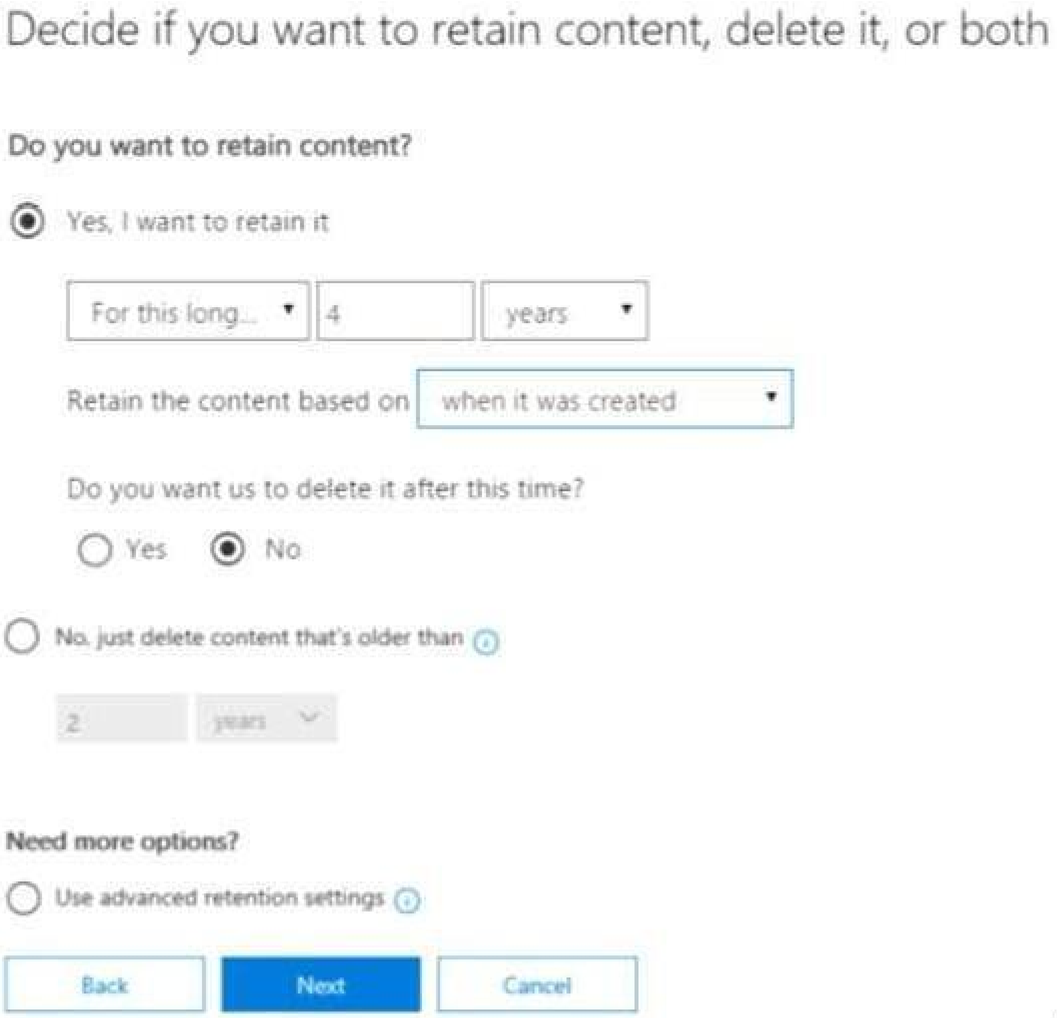
2 | years

Delete the content based on | when it was created

Need more options?

○ Use advanced retention settings

Policy2 is configured as shown in the Policy2 exhibit. (Click the Policy2 tab.)



Decide if you want to retain content, delete it, or both

Do you want to retain content?

● Yes, I want to retain it

For this long... | 4 | years

Retain the content based on | when it was created

Do you want us to delete it after this time?

○ Yes ● No

○ No, just delete content that's older than

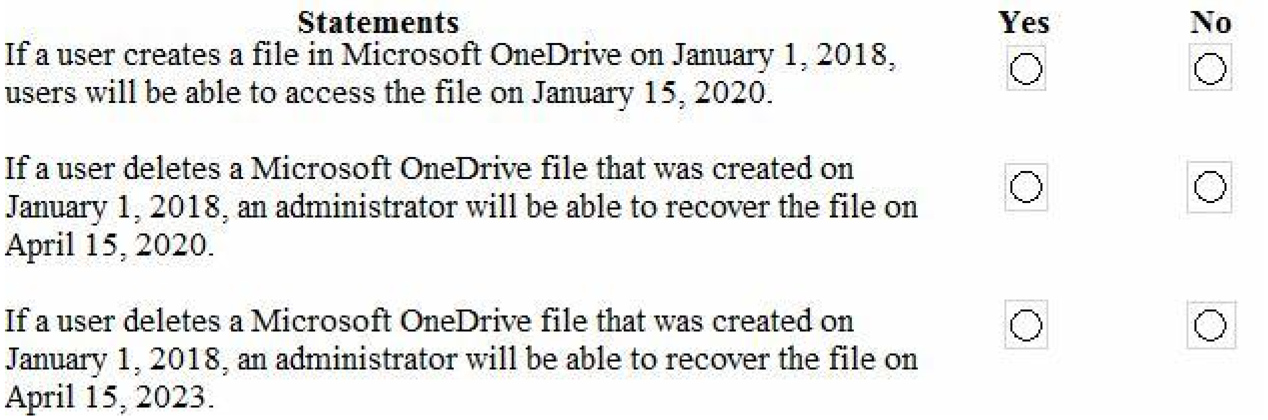
2 | years

Need more options?

○ Use advanced retention settings

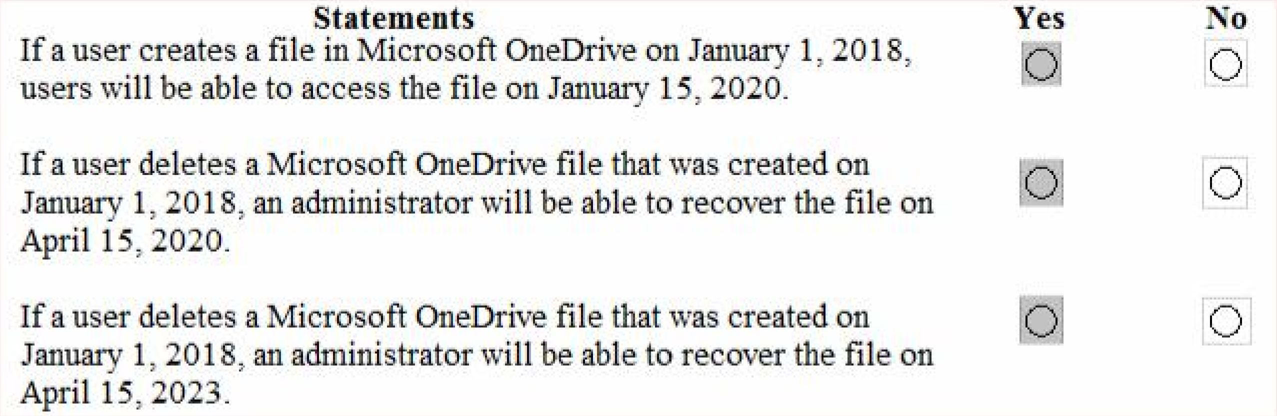
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

Correct Answer:



Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	●	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	●	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	●	○

Explanation/Reference:

References: https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principlesof-retention-or-what-takes-precedence

QUESTION 19

You have a Microsoft 365 E5 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
D18912E1457D5D1DDCBD40AB3BF70D5D
From Microsoft Defender ATP, you turn on the Allow or block file advanced feature.
You need to block users from downloading a file named File1.exe.
What should you use?

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

Correct Answer: B

Explanation/Reference:

Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defenderatp/respond-filealerts#allow-or-block-file

QUESTION 20

You have two conditional access policies named Policy1 and Policy2.
Policy1 has the following settings:

- Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected
- Access controls:
- Grant: Grant access
- Session: 0 controls selected
- Enable policy: On
- Policy2 has the following settings:
- Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected
- Access controls:
- Grant: Block access
- Session: 0 controls selected
- Enable policy: On

You need to ensure that User1 can access Microsoft Exchange Online only from devices that are marked as compliant.
What should you do?

A. Modify the Grant settings of Policy2.
B. Disable Policy2.
C. Modify the Conditions settings of Policy2.
D. Modify the Grant settings of Policy1.

Correct Answer: C