Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

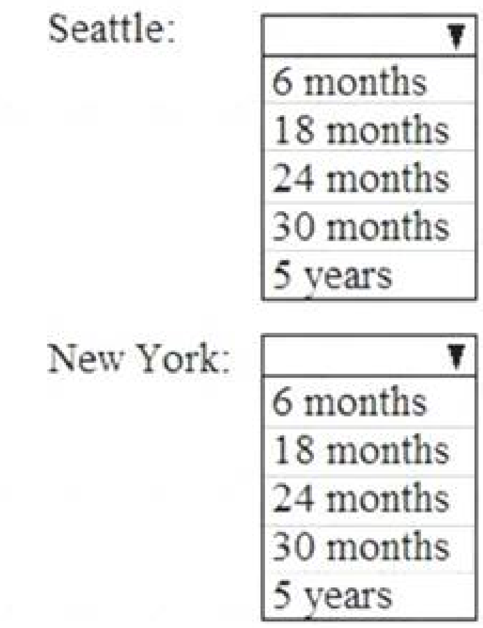
NEW QUESTION 1
- (Exam Topic 1)
You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator rote.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
C. From the Intune admin center, add User1 as a device enrollment manager.
D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

NEW QUESTION 2
- (Exam Topic 1)
As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Seattle:
- 6 months
- 18 months
- 24 months
- 30 months
- 5 years

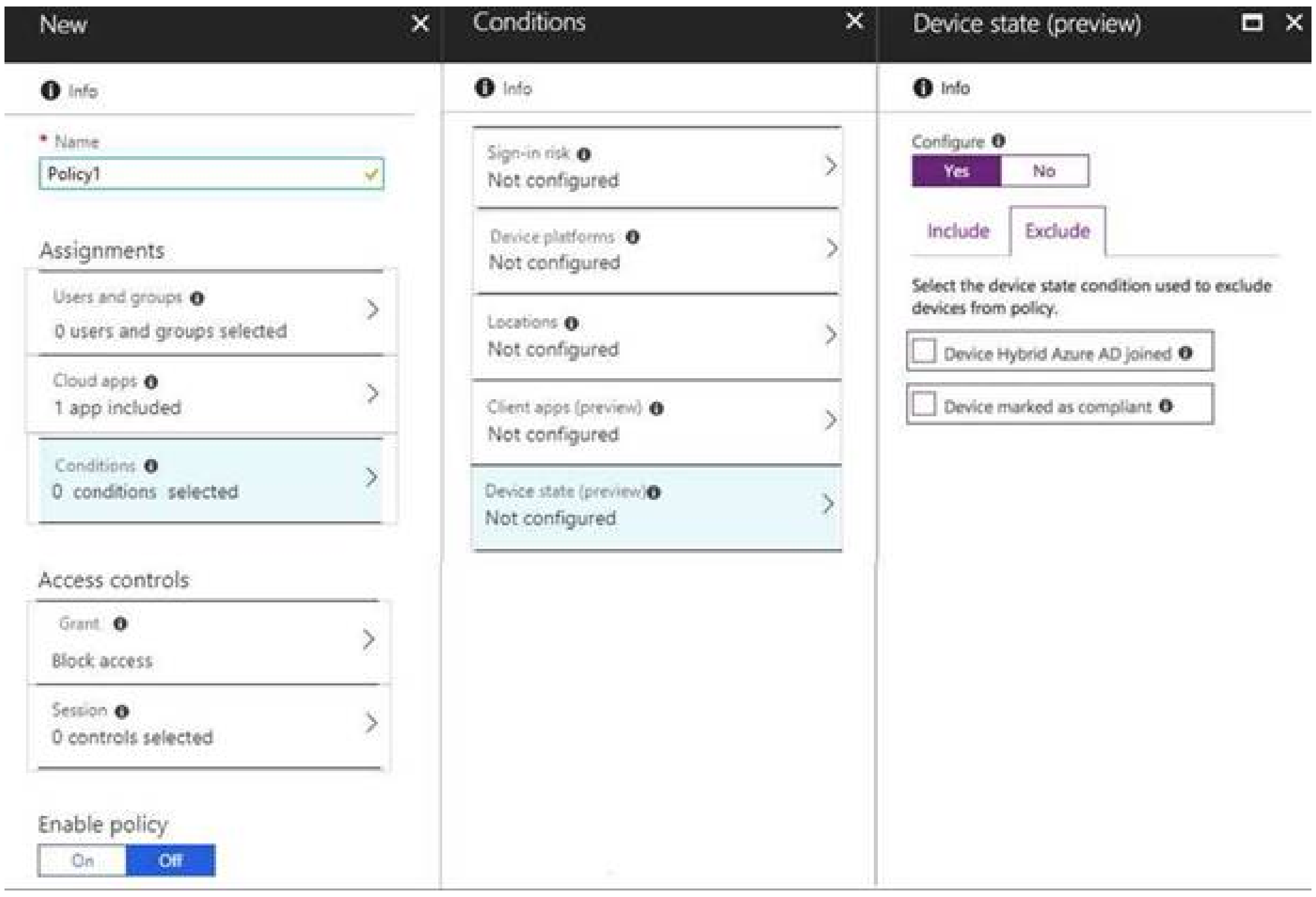
New York:
- 6 months
- 18 months
- 24 months
- 30 months
- 5 years

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date
References:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

NEW QUESTION 3
- (Exam Topic 1)
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

A. Mastered
B. Not Mastered

Answer: A

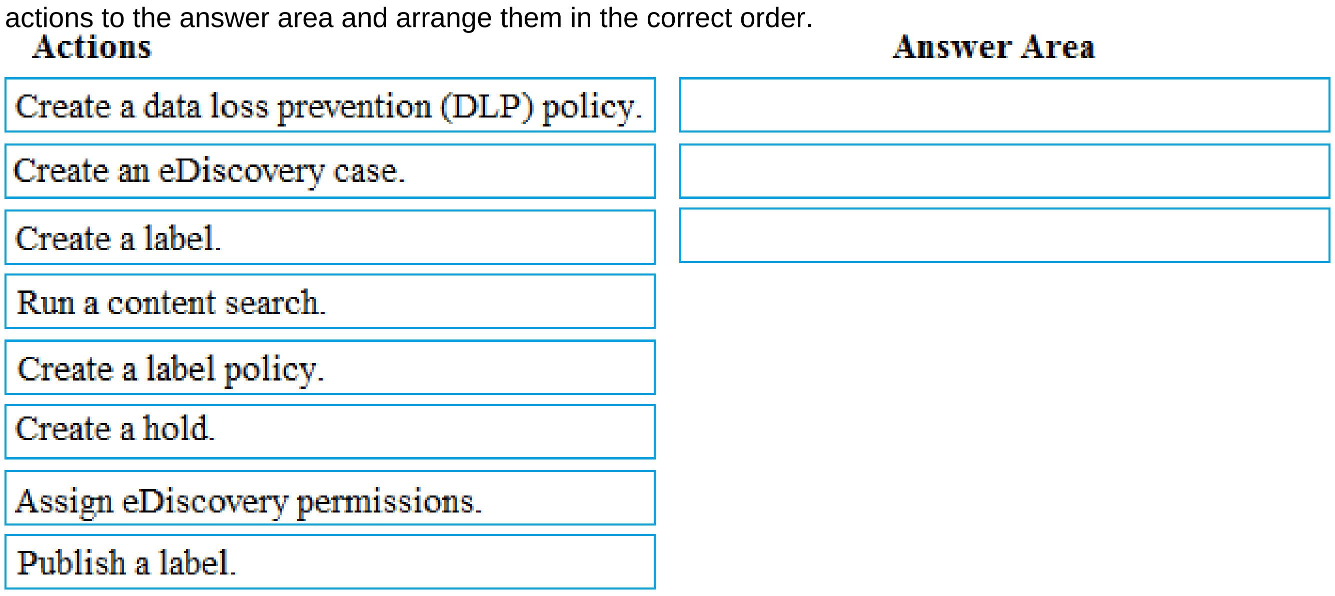
Explanation:
Suggested Answer
References:https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

NEW QUESTION 4
- (Exam Topic 1)
You need to meet the compliance requirements for the Windows 10 devices.
What should you create from the Intune admin center?

A. a device compliance policy
B. a device configuration profile
C. an application policy
D. an app configuration policy

Answer: C

NEW QUESTION 5
- (Exam Topic 2)
You need to meet the requirement for the legal department.
Which three actions should you perform in sequence from the Security & Compliance admin center? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Create a data loss prevention (DLP) policy.

Create an eDiscovery case.

Create a label.

Run a content search.

Create a label policy.

Create a hold.

Assign eDiscovery permissions.

Publish a label.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References: https://www.sherweb.com/blog/ediscovery-office-365/

NEW QUESTION 6
- (Exam Topic 2)
You need to protect the U.S. PII data to meet the technical requirements.
What should you create?

A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

Answer: A

NEW QUESTION 7
- (Exam Topic 2)
You need to meet the technical requirement for large-volume document retrieval. What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center
B. an alert policy from the Security & Compliance admin center
C. a file policy from Microsoft Cloud App Security
D. an activity policy from Microsoft Cloud App Security

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

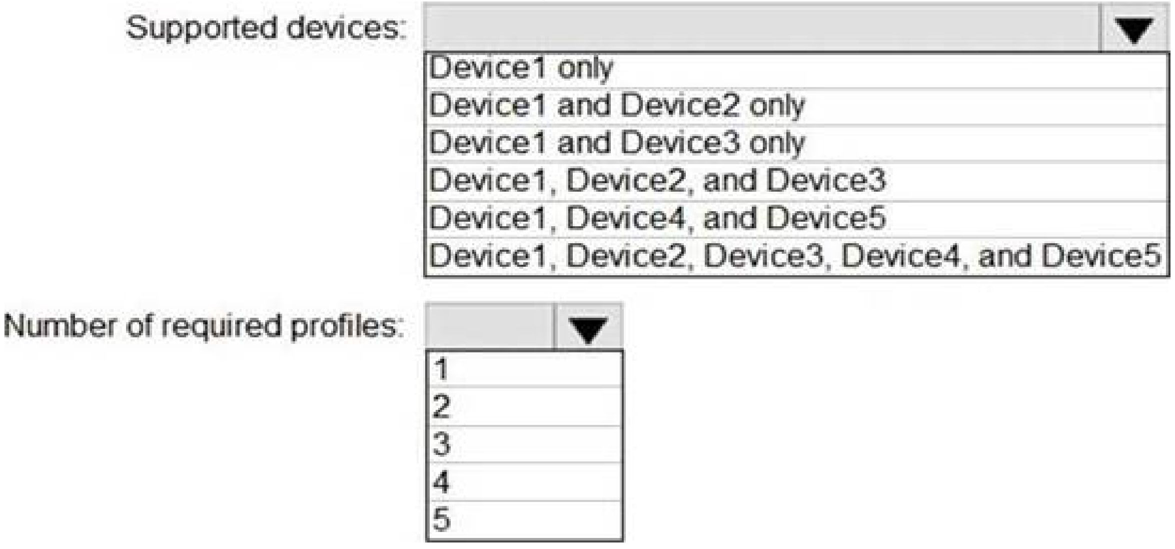
NEW QUESTION 8
- (Exam Topic 3)
You need to configure Office on the web to meet the technical requirements. What should you do?

A. Assign the Global reader role to User1.
B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
C. Configure an auto-labeling policy to apply the sensitivity labels.
D. Assign the Office apps admin role to User1.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o

NEW QUESTION 9
- (Exam Topic 3)
You plan to implement the endpoint protection device configuration profiles to support the planned changes. You need to identify which devices will be supported, and how many profiles you should implement.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Supported devices:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3
- Device1, Device4, and Device5
- Device1, Device2, Device3, Device4, and Device5

Number of required profiles:
- 1
- 2
- 3
- 4
- 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

NEW QUESTION 10
- (Exam Topic 4)
You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project. Which DNS record should you recommend?

A. host (A)
B. host information
C. text (TXT)
D. pointer (PTR)

Answer: A

Explanation:
When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers: Text (TXT)
Mail exchanger (MX)
incorrect answer options you may see on the exam include the following: alias (CNAME)
Host (A) host (AAA)
Pointer (PTR) Name Server (NS)
host information (HINFO) pointer (PTR)
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting

NEW QUESTION 10
- (Exam Topic 4)
You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

A. pass-through authentication
B. pass-through authentication and seamless SSO
C. password hash synchronization and seamless SSO
D. password hash synchronization

Answer: C

Explanation:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365. Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

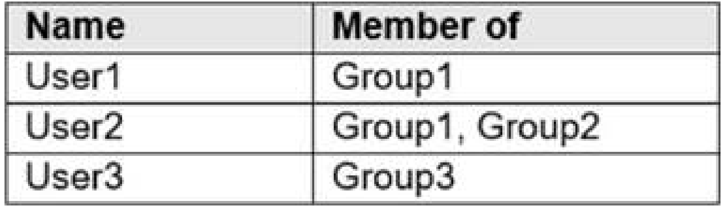
NEW QUESTION 13
- (Exam Topic 4)
Which role should you assign to User1?
Available Choices (select all choices that are correct)

A. Hygiene Management
B. Security Reader
C. Security Administrator
D. Records Management

Answer: B

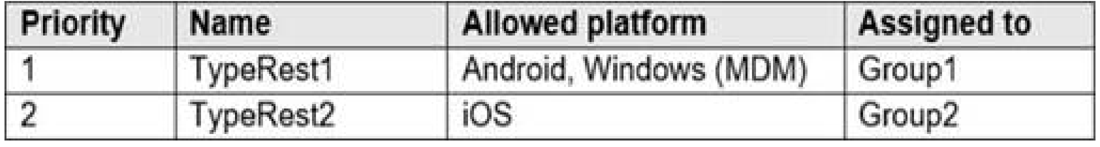
Explanation:
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

NEW QUESTION 17
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.



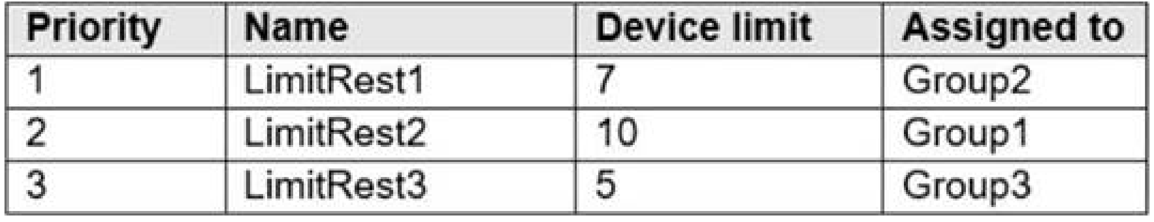
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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



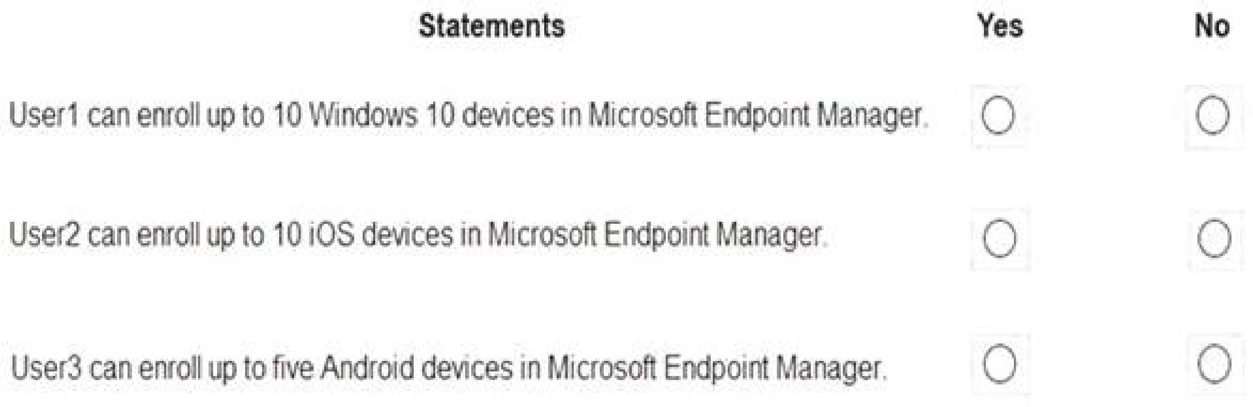
Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

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



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

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

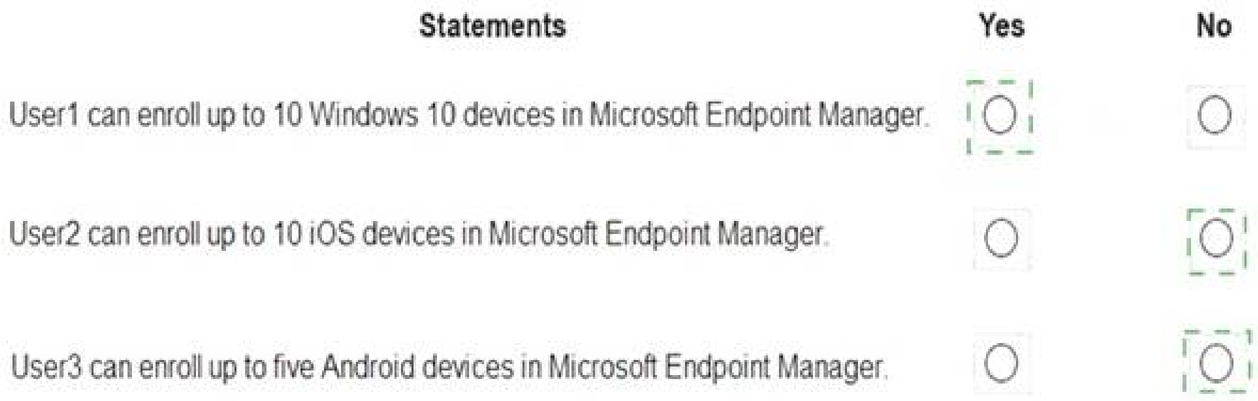


Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

NEW QUESTION 21
- (Exam Topic 5)
You have a new Microsoft 365 E5 tenant.
You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?

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

Answer: A

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

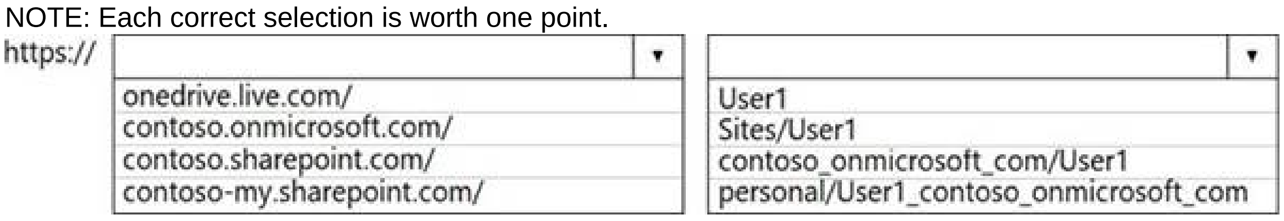
NEW QUESTION 23
- (Exam Topic 5)
Your network contains an Active Directory forest named contoso.local.
You purchase a Microsoft 365 subscription.
You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months. You need to prepare for the planned move to Microsoft 365.
What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

A. Purchase a third-party X.509 certificate.
B. Create an external forest trust.
C. Rename the Active Directory forest.
D. Purchase a custom domain name.

Answer: D

Explanation:
The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on-premise Active Directory if it's a routable domain name, for example, contoso.com.
If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.
Incorrect:
Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization

NEW QUESTION 25
- (Exam Topic 5)
You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
A user named User1 stores documents in Microsoft OneDrive.
You need to place the contents of User1's OneDrive account on an eDiscovery hold.
Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



https:// [▼]
onedrive.live.com/
contoso.onmicrosoft.com/
contoso.sharepoint.com/
contoso-my.sharepoint.com/

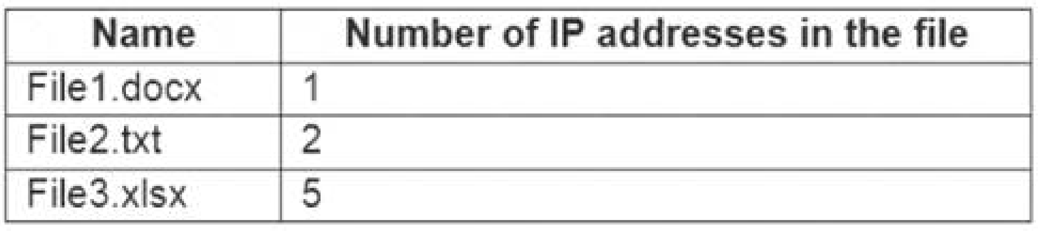
[▼]
User1
Sites/User1
contoso_onmicrosoft_com/User1
personal/User1_contoso_onmicrosoft_com

A. Mastered
B. Not Mastered

Answer: A

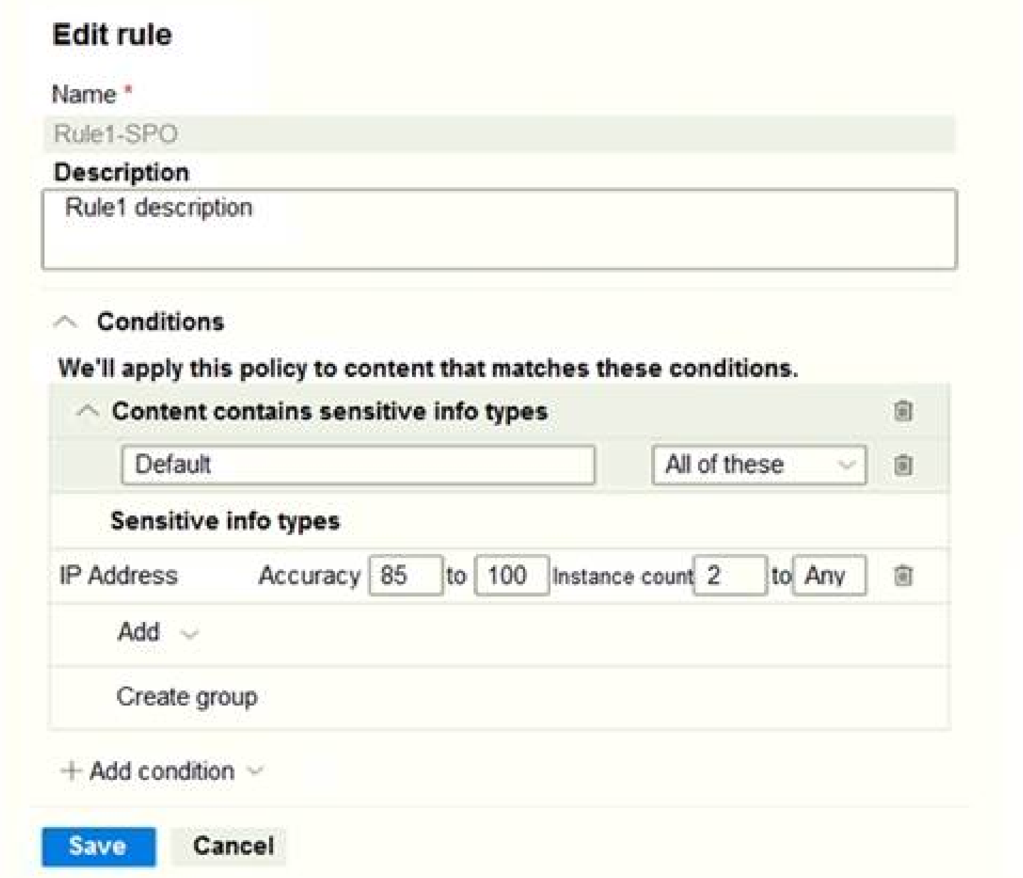
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds

NEW QUESTION 27
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.



Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:
- Name: AutoLabel1
- Label to auto-apply: Sensitivity1
- Rules for SharePoint Online sites: Rule1-SPO
- Choose locations where you want to apply the label: Site1 Rule1-SPO is configured as shown in the following exhibit.



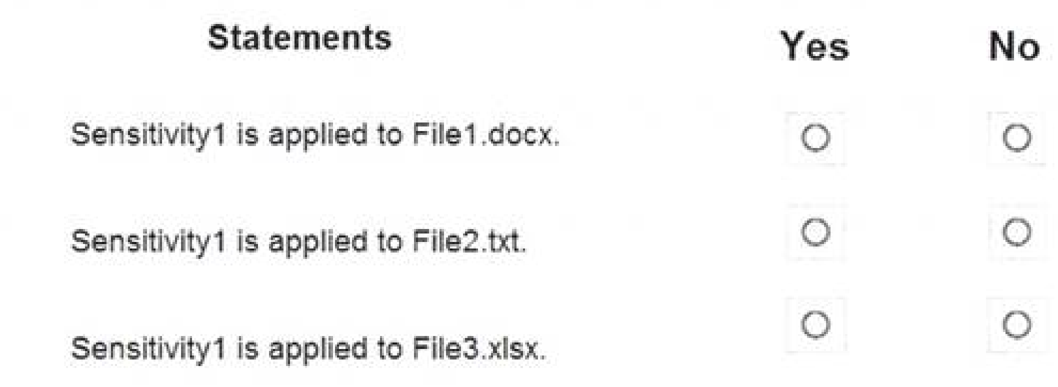
Edit rule

Name *
Rule1-SPO

Description
Rule1 description

Conditions
We'll apply this policy to content that matches these conditions.
Content contains sensitive info types
Default | All of these
Sensitive info types
IP Address Accuracy 85 to 100 Instance count 2 to Any

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



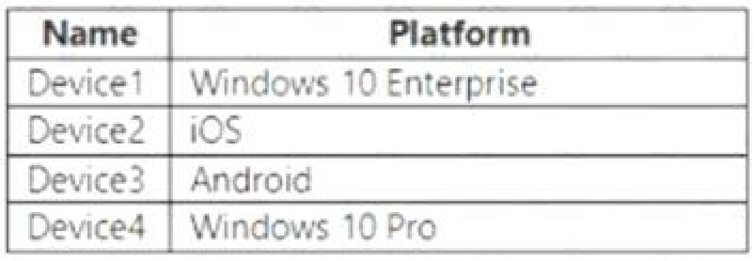
Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-w https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

NEW QUESTION 31
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.



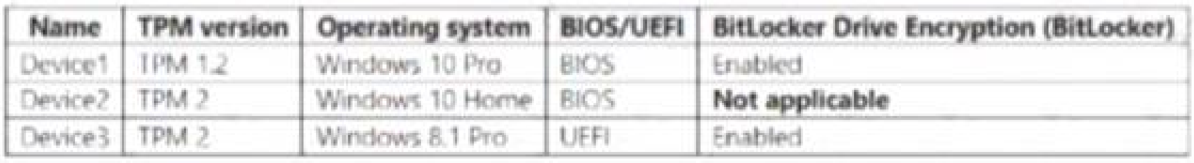
Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

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

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

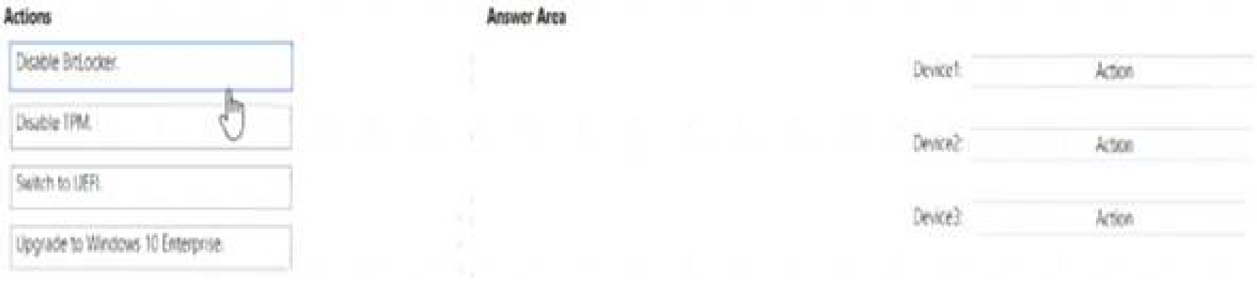
Answer: A

NEW QUESTION 36
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You have the devices shown in the following table.



Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	**Not applicable**
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD)
What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Actions

Disable BitLocker.
Disable TPM.
Switch to UEFI.
Upgrade to Windows 10 Enterprise.

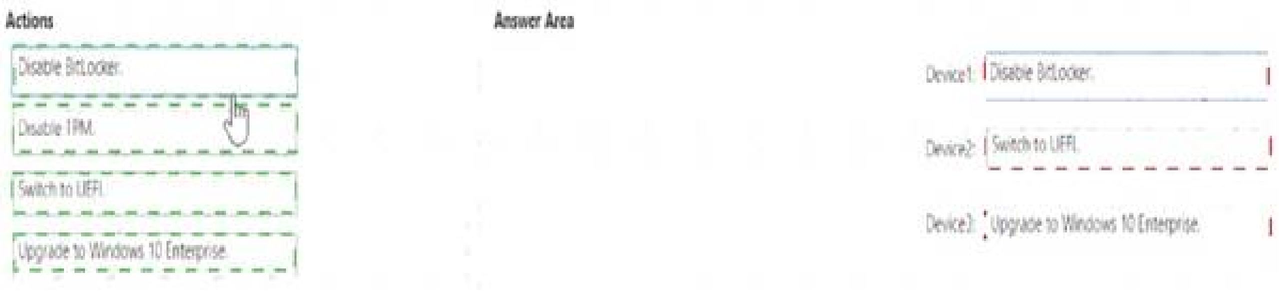
Answer Area

Device1: Action
Device2: Action
Device3: Action

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

- Disable BitLocker
- Disable TPM
- Switch to UEFI
- Upgrade to Windows 10 Enterprise

Answer Area

Device1: Disable BitLocker

Device2: Switch to UEFI

Device3: Upgrade to Windows 10 Enterprise

NEW QUESTION 41

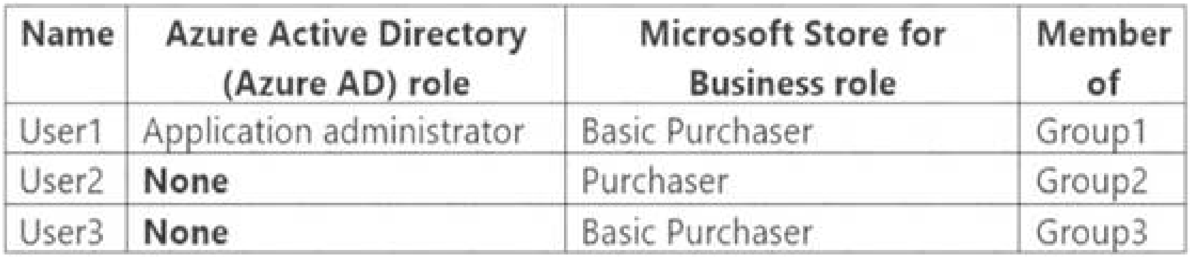
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes
B. no

Answer: B

NEW QUESTION 43

- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

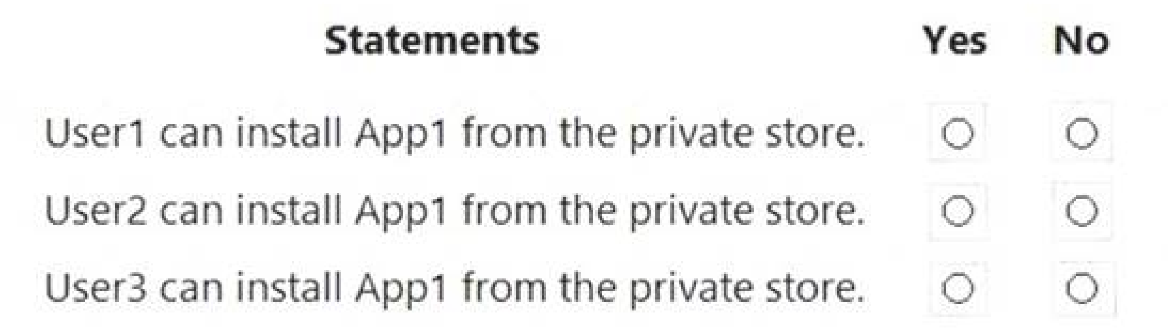


Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	None	Purchaser	Group2
User3	None	Basic Purchaser	Group3

You perform the following actions:

- Provision the private store in Microsoft Store for Business.
- Add an app named App1 to the private store.
- Set Private store availability for App1 to Specific groups, and then select Group3.

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



Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#priva

NEW QUESTION 45

- (Exam Topic 5)
You have a Microsoft 365 tenant.
Company policy requires that all Windows 10 devices meet the following minimum requirements:

- Require complex passwords.
- Require the encryption of data storage devices.
- Have Microsoft Defender Antivirus real-time protection enabled.

You need to prevent devices that do not meet the requirements from accessing resources in the tenant. Which two components should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a configuration policy
B. a compliance policy
C. a security baseline profile
D. a conditional access policy
E. a configuration profile

Answer: BD

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 50
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.
You plan to use Endpoint analytics to identify hardware issues.
You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

A. Configure the Endpoint analytics baseline regression threshold.
B. Create a configuration profile.
C. Create a Windows 10 Security Baseline profile
D. Create a compliance policy.

Answer: B

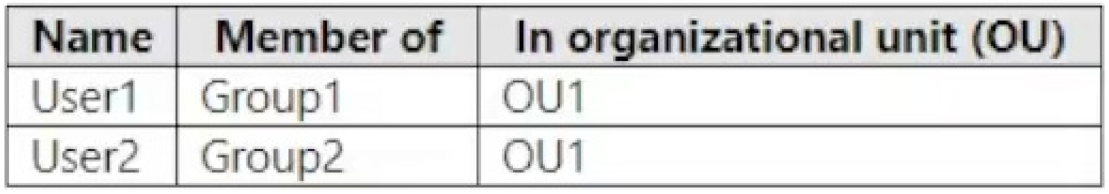
NEW QUESTION 53
- (Exam Topic 5)
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company’s current state of compliance.
What should you use?

A. eDiscovery
B. Information governance
C. Compliance Manager
D. Data Subject Requests (DSRs)

Answer: C

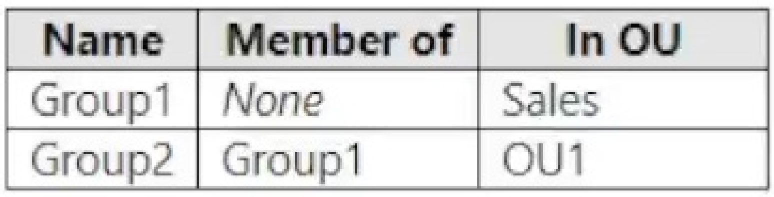
Explanation:
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

NEW QUESTION 58
- (Exam Topic 5)
HOTSPOT
Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription. The domain contains the users shown in the following table.



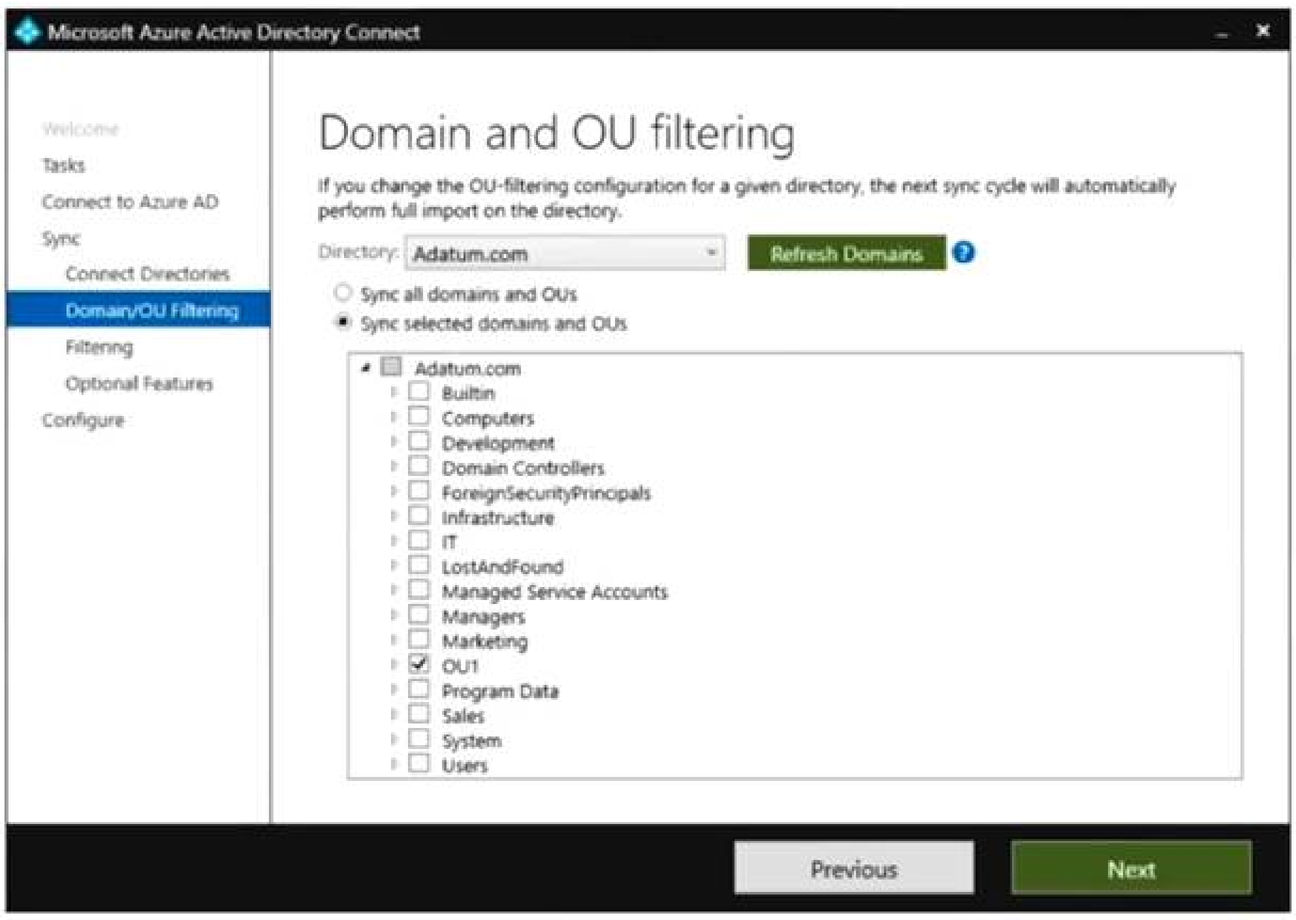
Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

The domain contains the groups shown in the following table.



Name	Member of	In OU
Group1	*None*	Sales
Group2	Group1	OU1

You are deploying Azure AD Connect.
You configure Domain and OU filtering as shown in the following exhibit.



Microsoft Azure Active Directory Connect

Domain and OU filtering

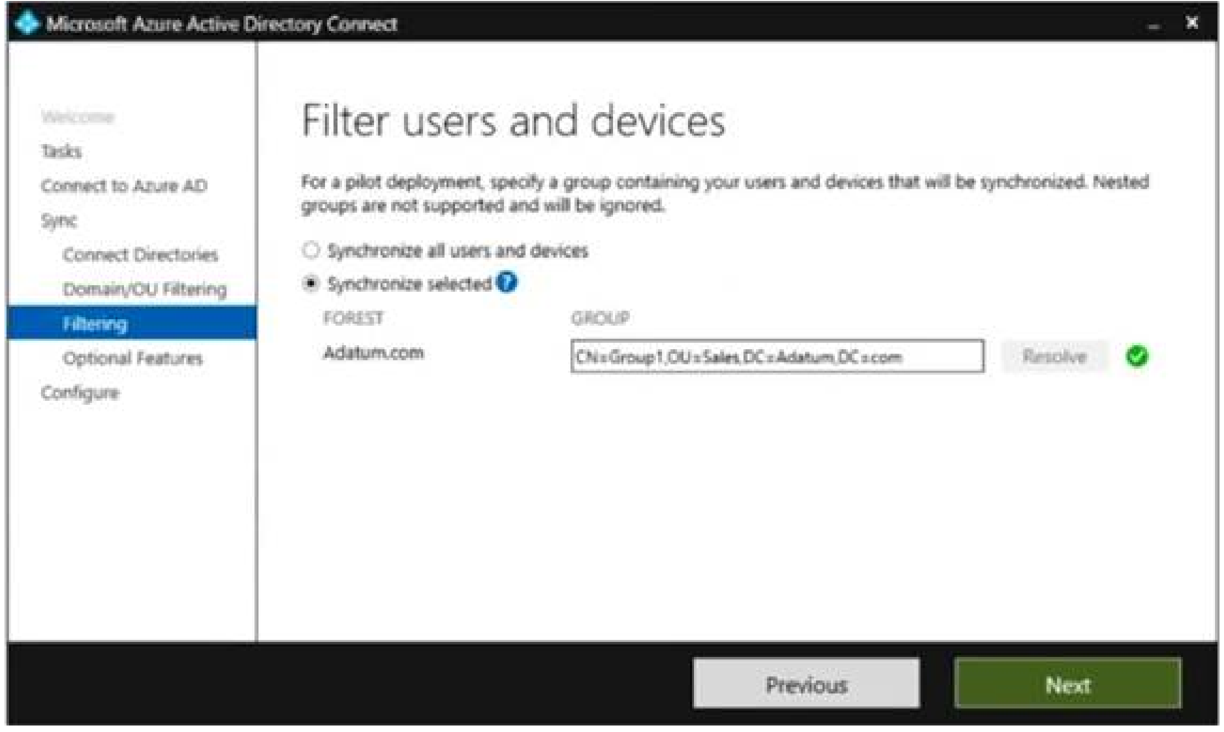
If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.

Directory: Adatum.com

○ Sync all domains and OUs
● Sync selected domains and OUs

- □ Adatum.com
  - □ Builtin
  - □ Computers
  - □ Development
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Infrastructure
  - □ IT
  - □ LostAndFound
  - □ Managed Service Accounts
  - □ Managers
  - □ Marketing
  - ☑ OU1
  - □ Program Data
  - □ Sales
  - □ System
  - □ Users

You configure Filter users and devices as shown in the following exhibit.



Microsoft Azure Active Directory Connect

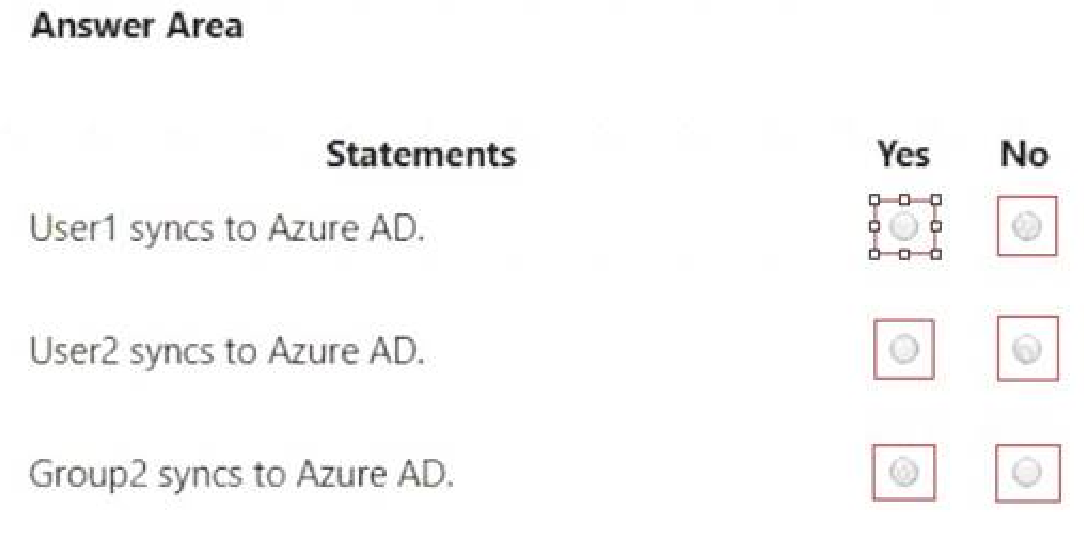
Filter users and devices

For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

○ Synchronize all users and devices
● Synchronize selected

FOREST	GROUP
Adatum.com	CN=Group1,OU=Sales,DC=Adatum,DC=com

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



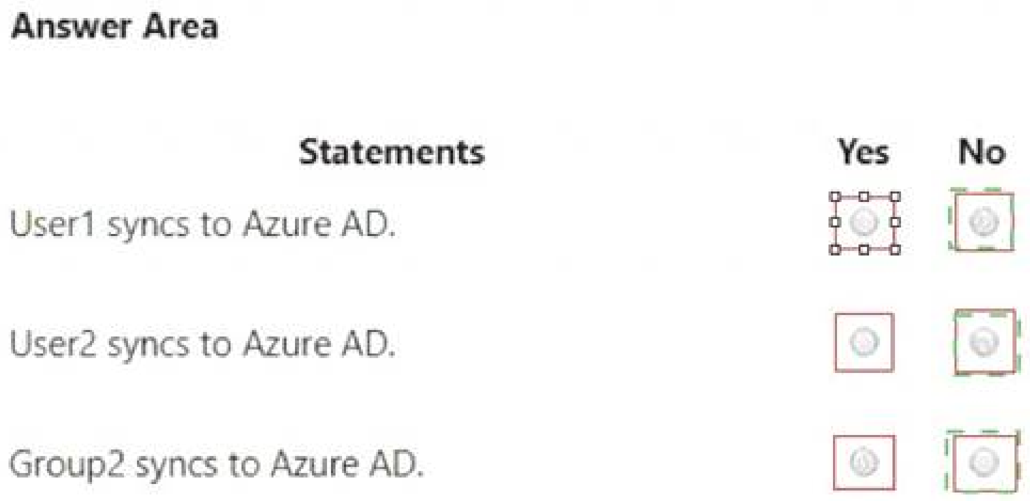
Answer Area

Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

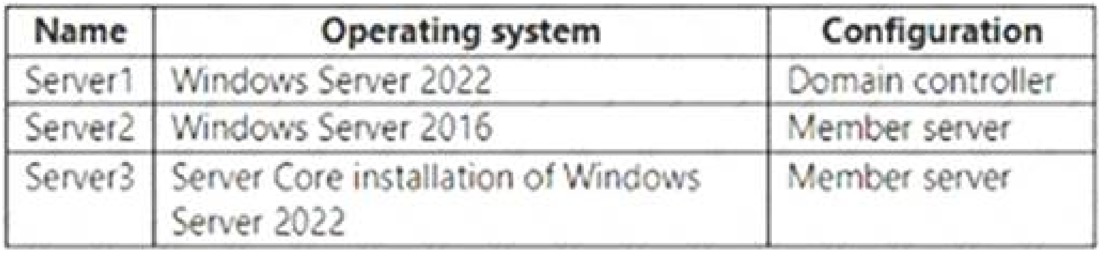
Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

NEW QUESTION 63

- (Exam Topic 5)

HOTSPOT

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.



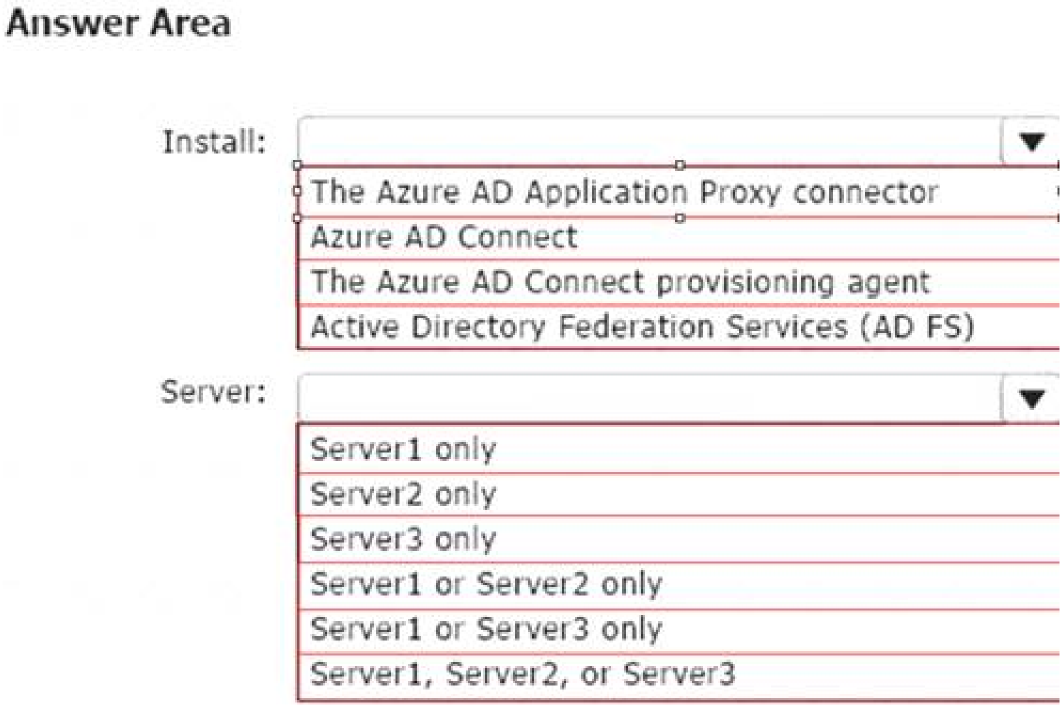
Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

Install: ▼
- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server: ▼
- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: The Azure AD Connect provisioning agent Install the Azure AD Connect provisioning agent

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a

light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

* An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites

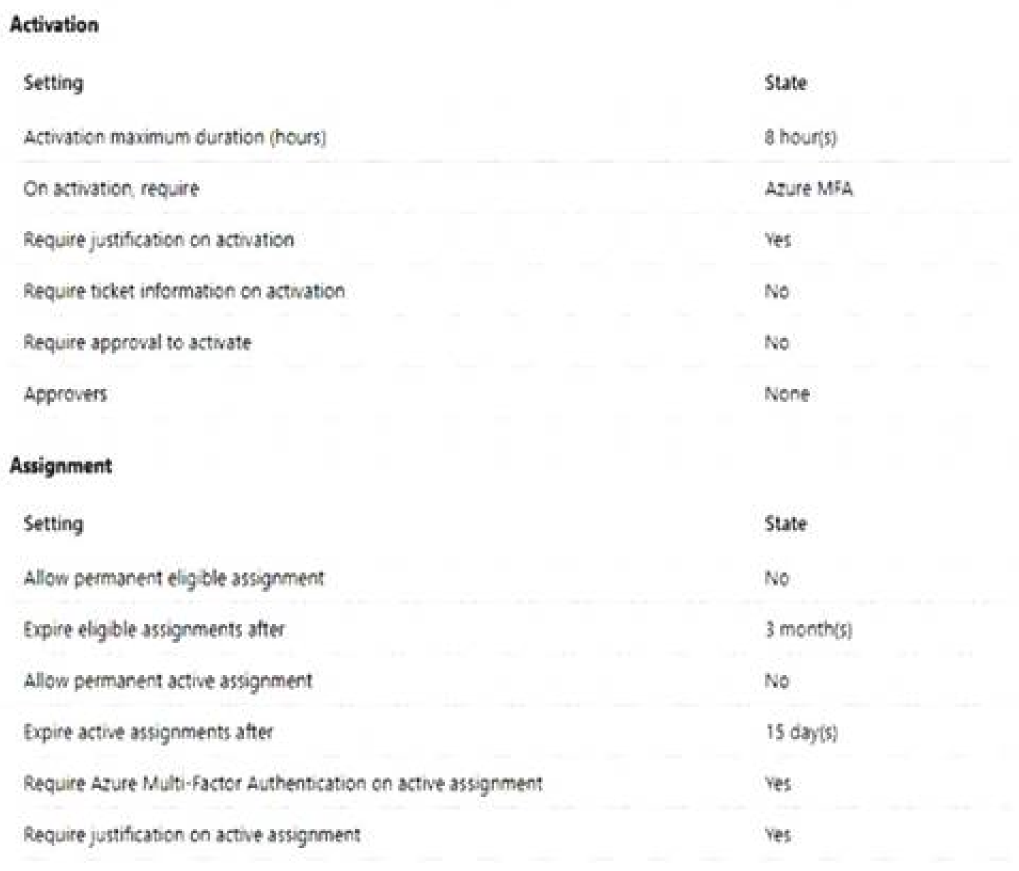
NEW QUESTION 66

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.



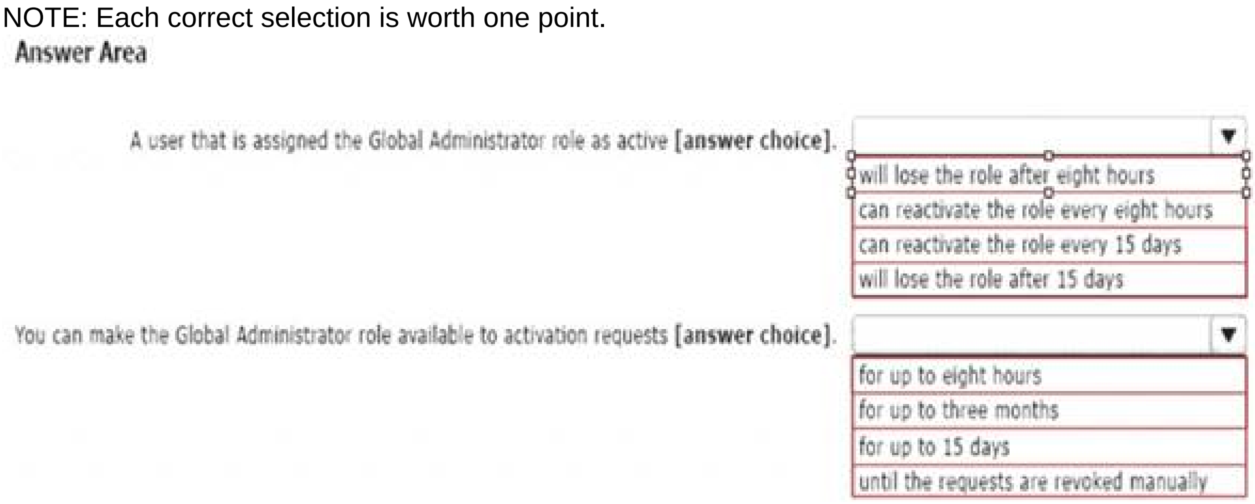
Activation

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

Assignment

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

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



Answer Area

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 70
- (Exam Topic 5)
Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.
Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com. You plan to install Azure AD Connect on a member server and implement pass-through authentication. You need to prepare the environment for the planned implementation of pass-through authentication. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

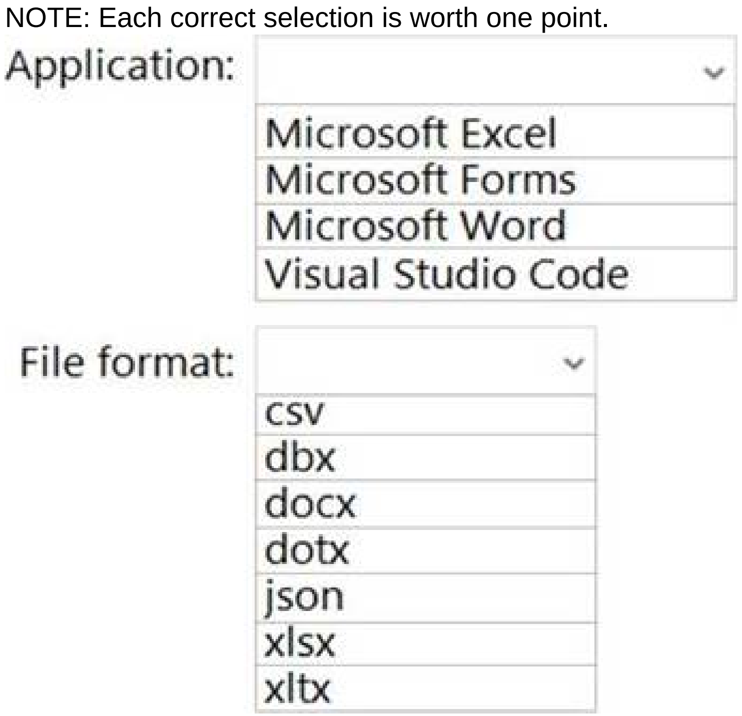
A. From a domain controller install an Authentication Agent
B. From the Microsoft Entra admin center, confiqure an authentication method.
C. From Active Director,' Domains and Trusts add a UPN suffix
D. Modify the email address attribute for each user account.
E. From the Microsoft Entra admin center,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

Answer: ABE

Explanation:
Deploy Azure AD Pass-through Authentication Step 1: Check the prerequisites
Ensure that the following prerequisites are in place. In the Entra admin center
* 1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.
(E) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.
(A) In your on-premises environment
* 1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.
* 2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the

version is supported.
* 3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.
* 4. Etc.
(B) Step 2: Enable the feature
Enable Pass-through Authentication through Azure AD Connect.
If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User
sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.
Incorrect:
Not C: From Active Directory Domains and Trusts, add a UPN suffix Not D. Modify the email address attribute for each user account.
Not F. Modify the User logon name for each user account. Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start

NEW QUESTION 72
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 tenant.
You need to create a custom Compliance Manager assessment template.
Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Application:
- Microsoft Excel
- Microsoft Forms
- Microsoft Word
- Visual Studio Code

File format:
- csv
- dbx
- docx
- dotx
- json
- xlsx
- xltx

A. Mastered
B. Not Mastered

Answer: A

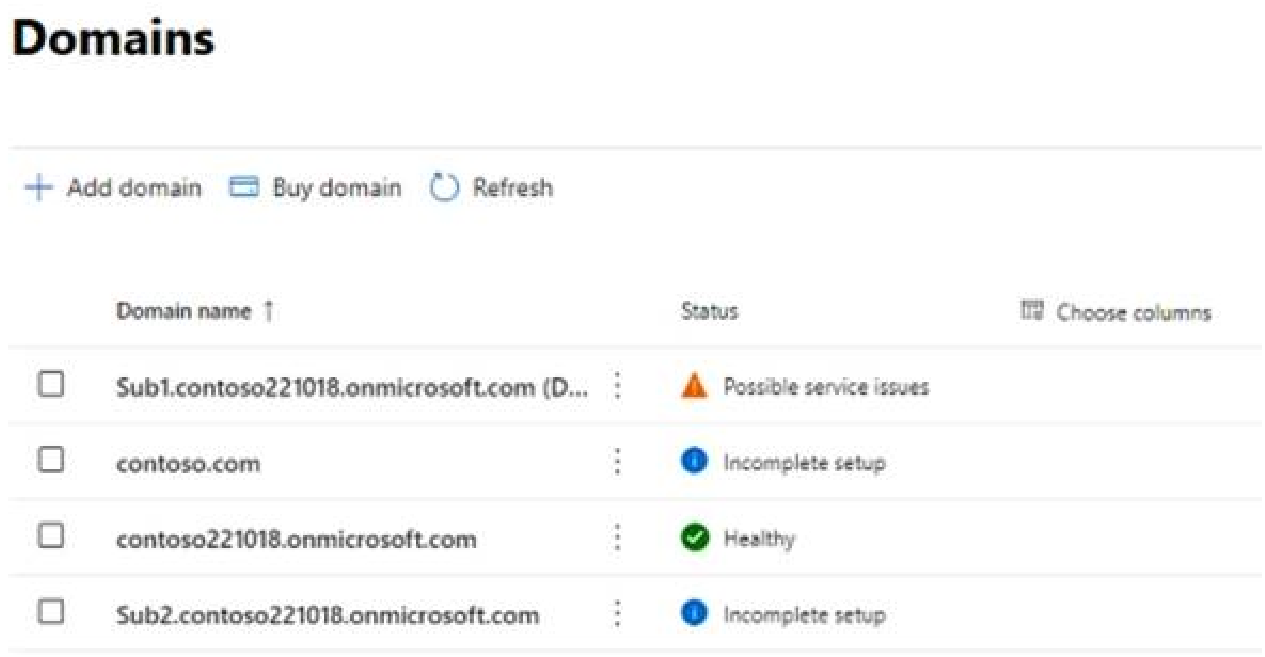
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-create?view=o365

NEW QUESTION 76
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select Update & Security to view the update history.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 81
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.



Domains

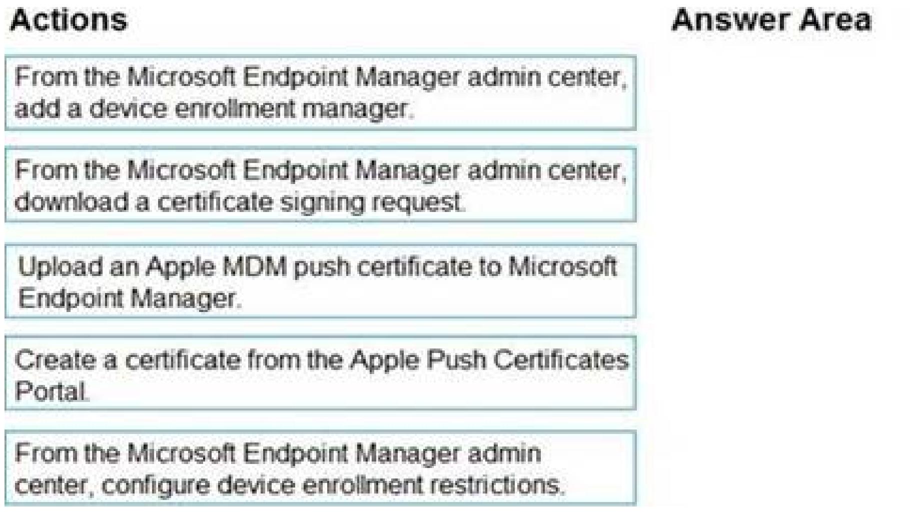
	Domain name ↑		Status
□	Sub1.contoso221018.onmicrosoft.com (D...	⋮	⚠ Possible service issues
□	contoso.com	⋮	● Incomplete setup
□	contoso221018.onmicrosoft.com	⋮	✓ Healthy
□	Sub2.contoso221018.onmicrosoft.com	⋮	● Incomplete setup

Which domain name suffixes can you use when you create users?

A. only Sub1.contoso221018.onmicrosoft.com
B. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com
C. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
D. all the domains in the subscription

Answer: B

NEW QUESTION 85
- (Exam Topic 5)
DRAG DROP
You have a Microsoft 365 E5 subscription. Several users have iOS devices.
You plan to enroll the iOS devices in Microsoft Endpoint Manager.
You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

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

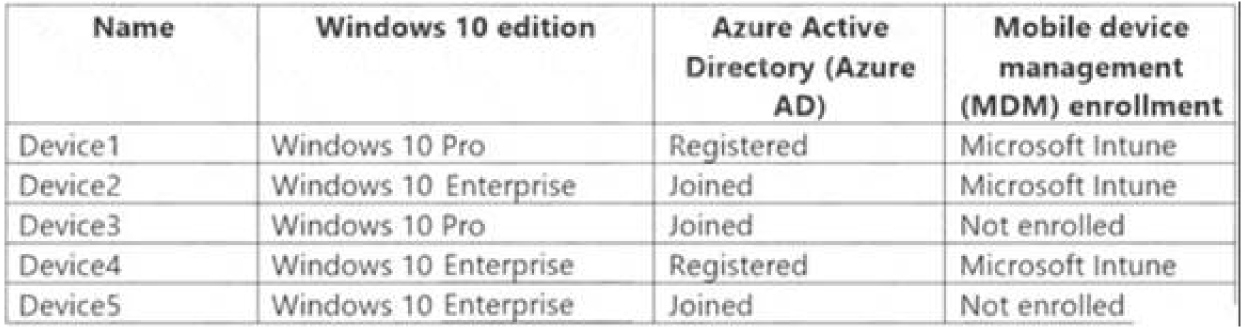
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

NEW QUESTION 90
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.



Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

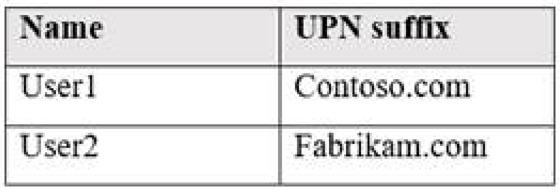
You add custom apps to the private store in Microsoft Store Business.
You plan to create a policy to show only the private store in Microsoft Store for Business. To which devices can the policy be applied?

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

D. Device2, Device3, and Device5 only
E. Device1, Device2, Device3, Device4, and Device5

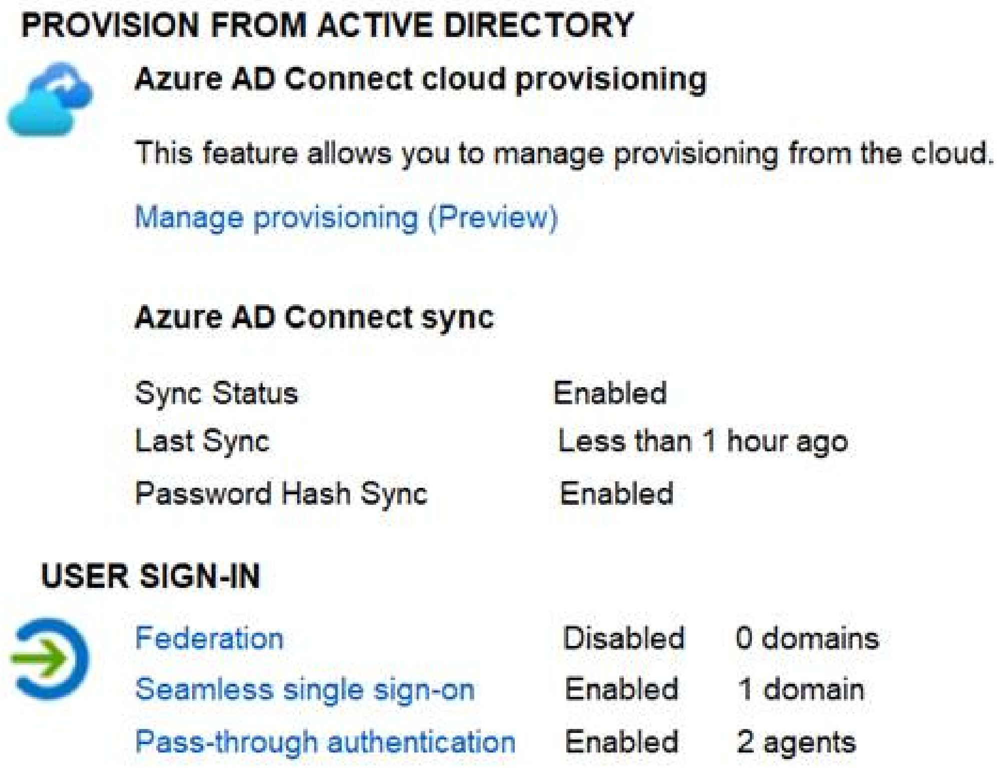
Answer: C

NEW QUESTION 95
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.



Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

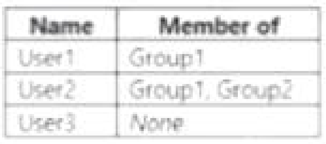
User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes
B. No

Answer: A

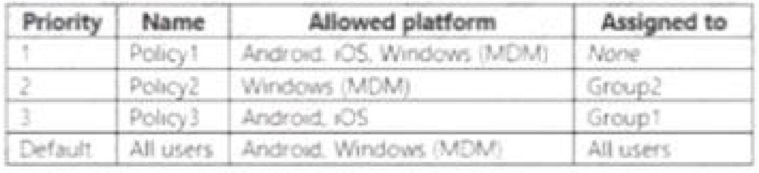
Explanation:
The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a
different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

NEW QUESTION 98
- (Exam Topic 5)
You have several devices enrolled in Microsoft Endpoint Manager.
You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

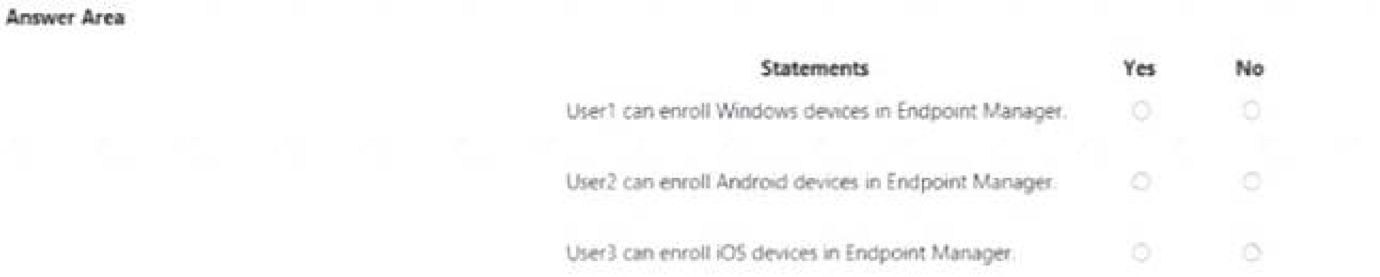


Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Endpoint Manager are configured as shown in the following table.



Priority	Name	Allowed platform	Assigned to
1	Policy1	Android. iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android. Windows (MDM)	All users



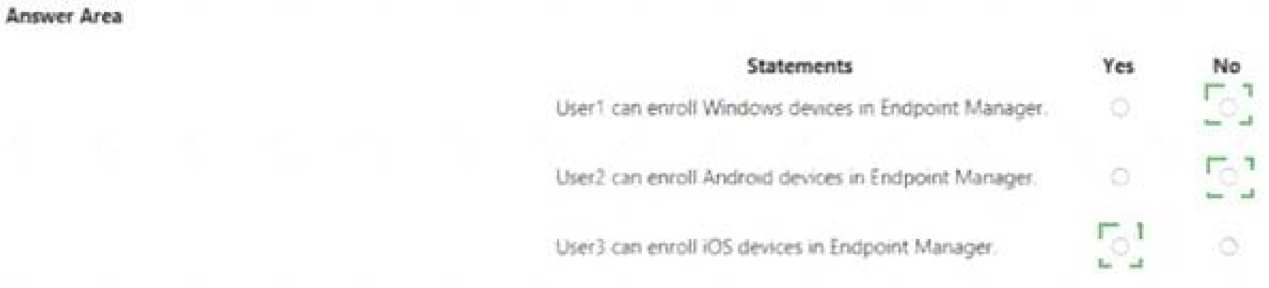
Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

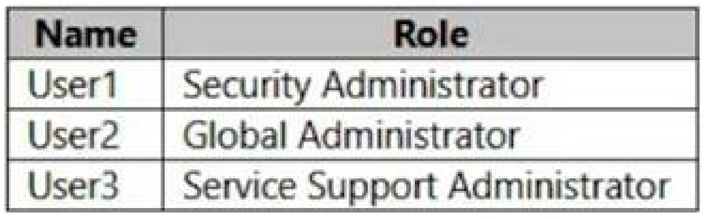
Explanation:



Answer Area

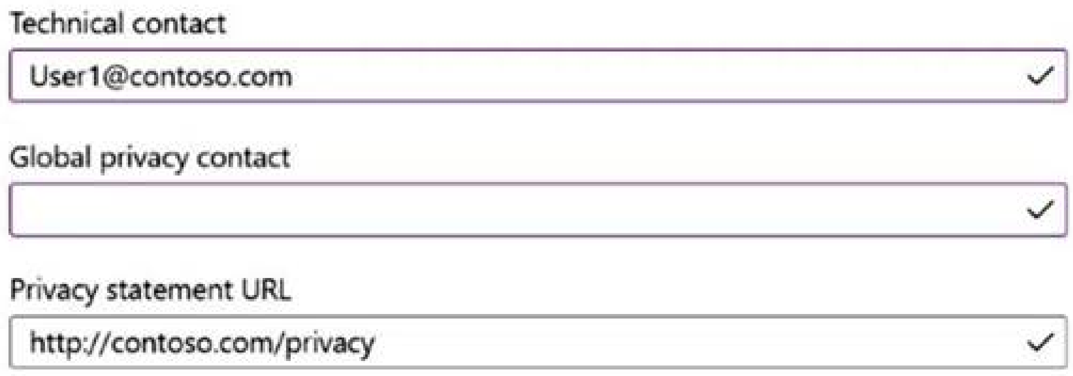
Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	[✓ ○]
User2 can enroll Android devices in Endpoint Manager.	○	[✓ ○]
User3 can enroll iOS devices in Endpoint Manager.	[✓ ○]	○

NEW QUESTION 103
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You have an Azure AD tenant that contains the users shown in the following table.



Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.



Technical contact
User1@contoso.com

Global privacy contact

Privacy statement URL
http://contoso.com/privacy

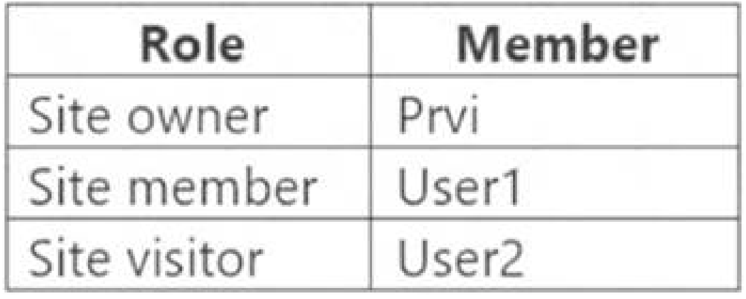
Which users will be contacted by Microsoft if the tenant experiences a data breach?

A. Used only
B. User2 only
C. User3 only
D. Used and User2 only
E. User2 and User3 only

Answer: B

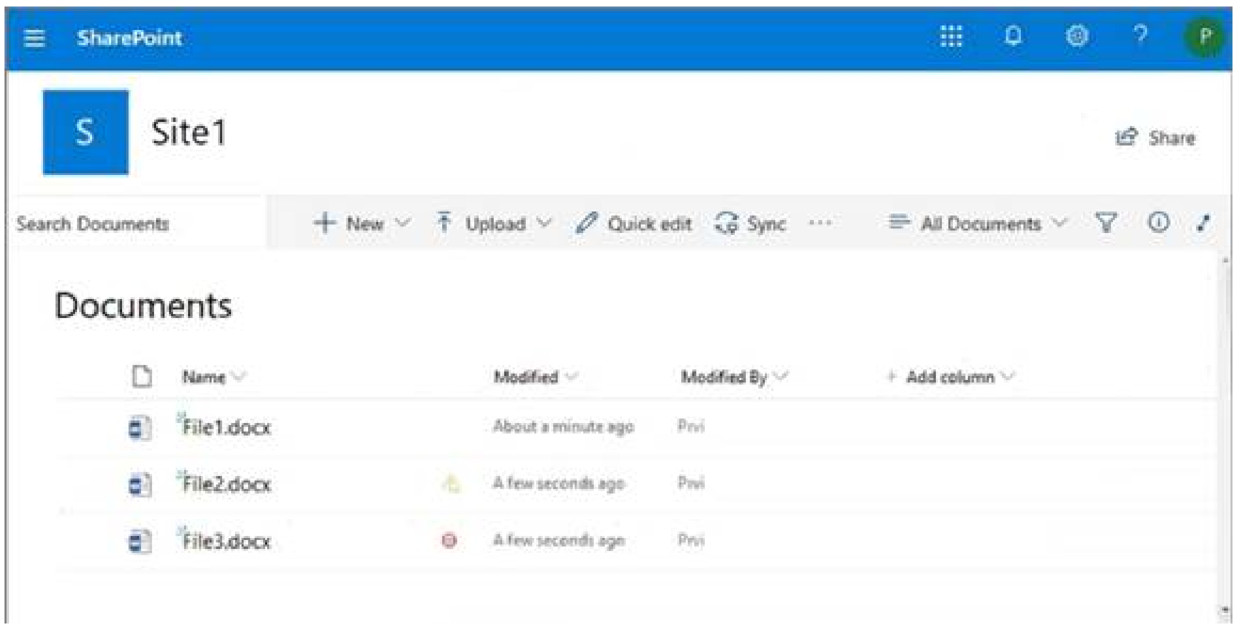
Explanation:
Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.
Reference:
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365

NEW QUESTION 107
- (Exam Topic 5)
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.



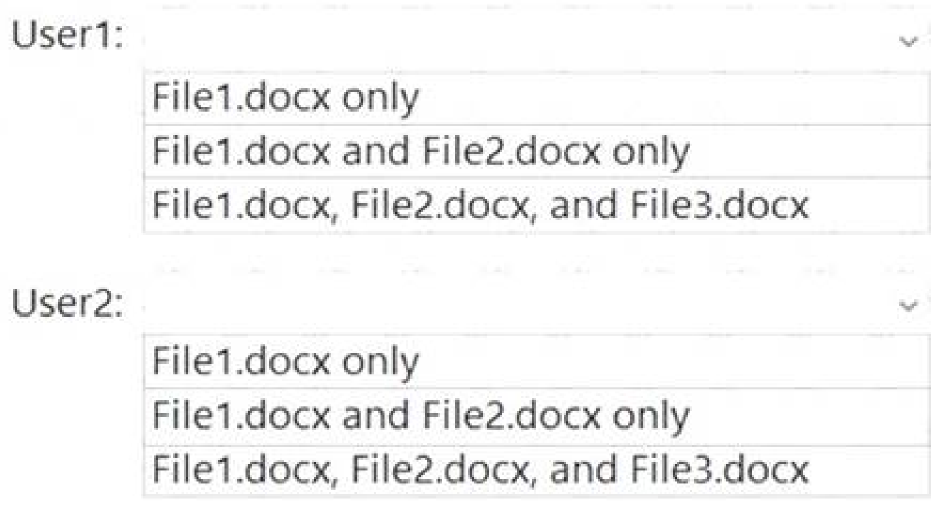
Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



Name	Modified	Modified By
File1.docx	About a minute ago	Prvi
File2.docx	A few seconds ago	Prvi
File3.docx	A few seconds ago	Prvi

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/ https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

NEW QUESTION 109
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwi

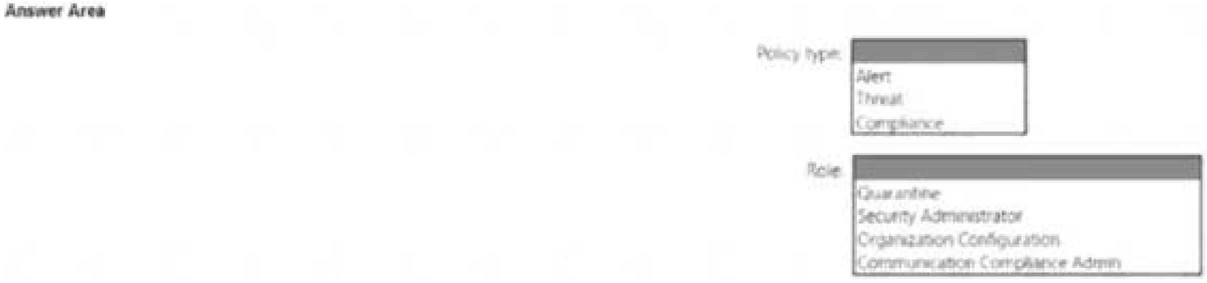
NEW QUESTION 113
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You plan to deploy 1.000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:
• Minimizes user interaction
• Minimizes administrative effort
• Automatically installs corporate apps What should you recommend?

A. Automated Device Enrollment (ADE)
B. bring your own device (BYOD) user and device enrollment
C. Apple Configurator enrollment

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

NEW QUESTION 118
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.
Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.


Answer Area

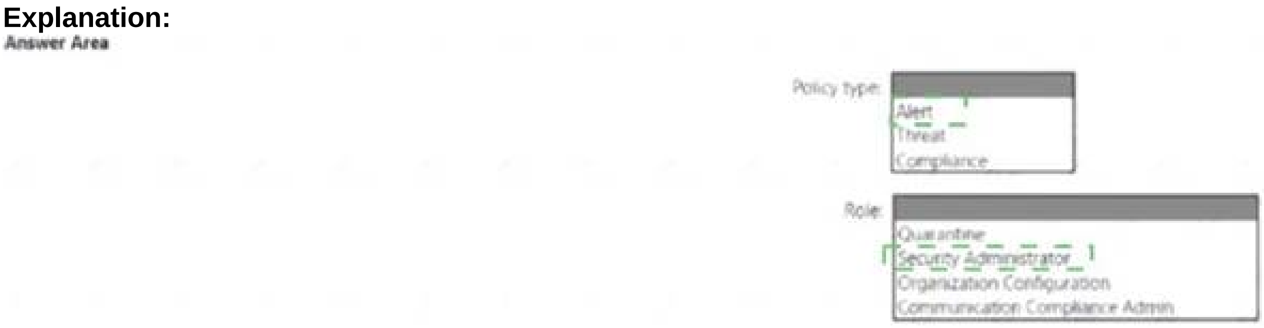
Policy type:
Alert
Threat
Compliance

Role:
Quarantine
Security Administrator
Organization Configuration
Communication Compliance Admin

A. Mastered
B. Not Mastered

Answer: A

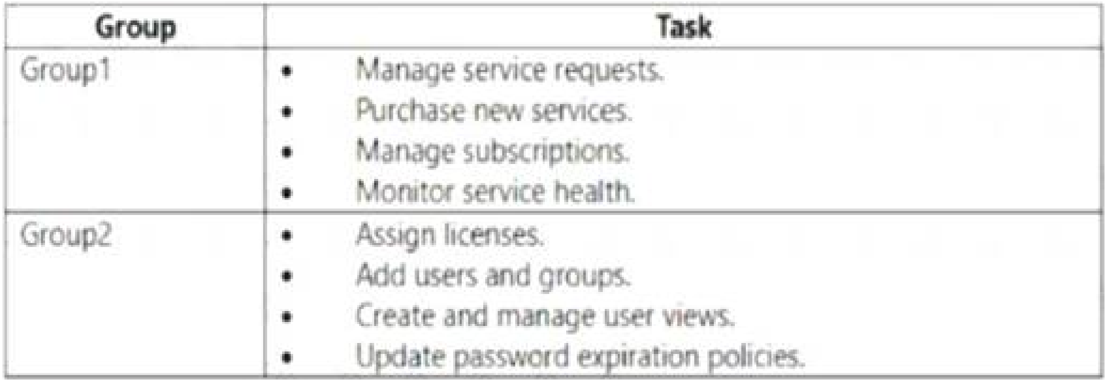
Explanation:


Answer Area

Policy type:
Alert
Threat
Compliance

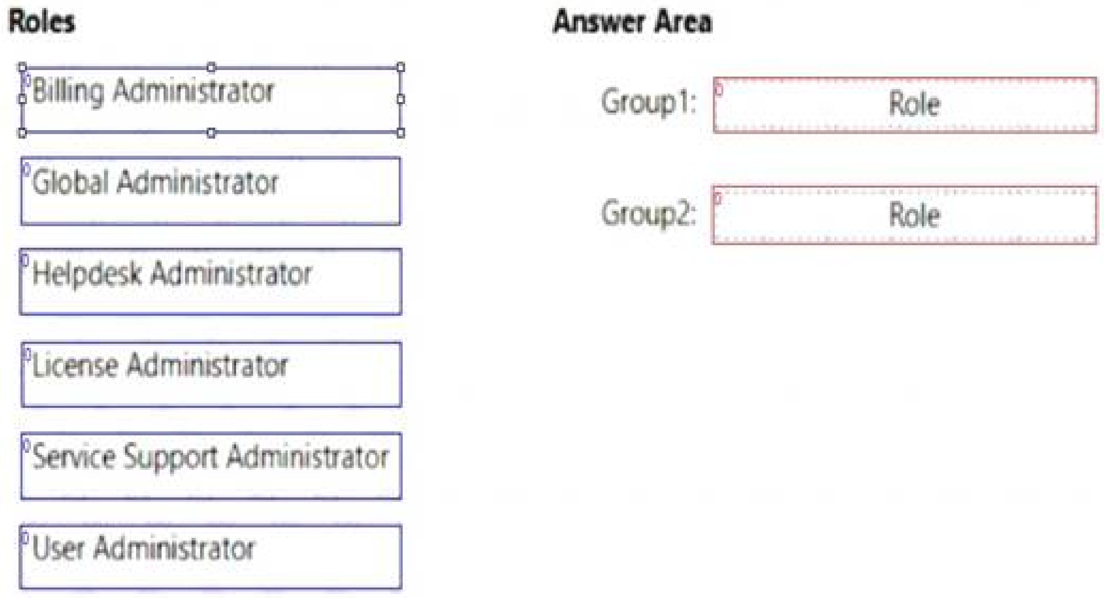
Role:
Quarantine
Security Administrator
Organization Configuration
Communication Compliance Admin

NEW QUESTION 121
- (Exam Topic 5)
DRAG DROP
You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2. You need to ensure that each group can perform the tasks shown in the following table.



Group	Task
Group1	• Manage service requests. • Purchase new services. • Manage subscriptions. • Monitor service health.
Group2	• Assign licenses. • Add users and groups. • Create and manage user views. • Update password expiration policies.

The solution must use the principle of least privilege.
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role 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.


Roles
Billing Administrator
Global Administrator
Helpdesk Administrator
License Administrator
Service Support Administrator
User Administrator

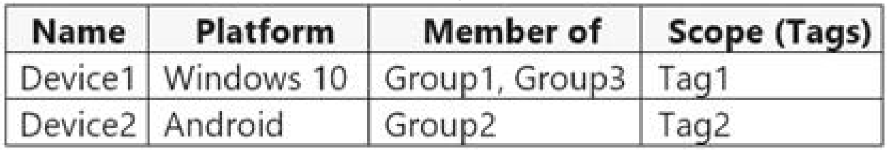
Answer Area
Group1: Role
Group2: Role

A. Mastered
B. Not Mastered

Answer: A

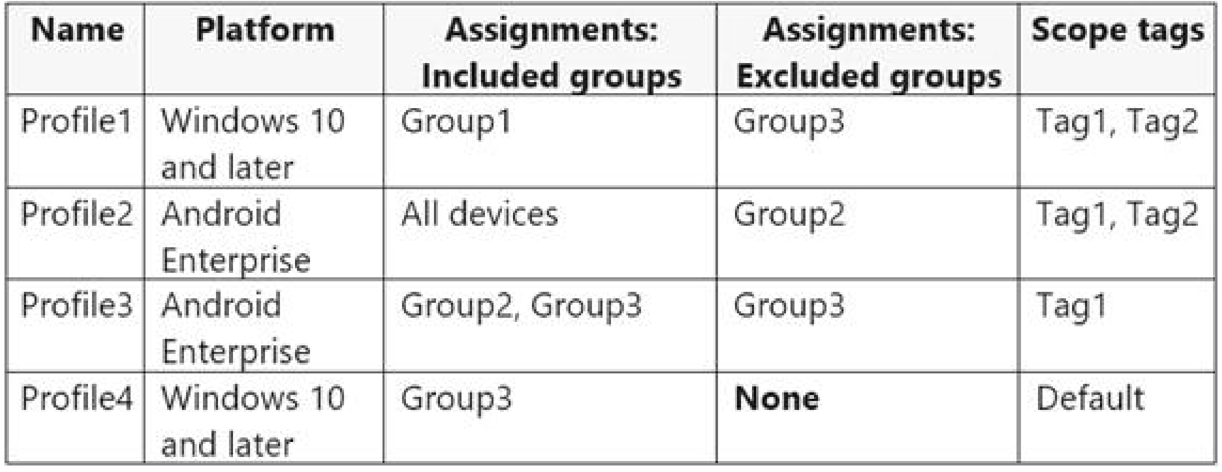
Explanation:
Box 1: Billing admin manage service request
Purchase new services Etc.
Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.
Box 2: User admin User admin
Assign the User admin role to users who need to do the following for all users:
- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles

NEW QUESTION 124
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table.



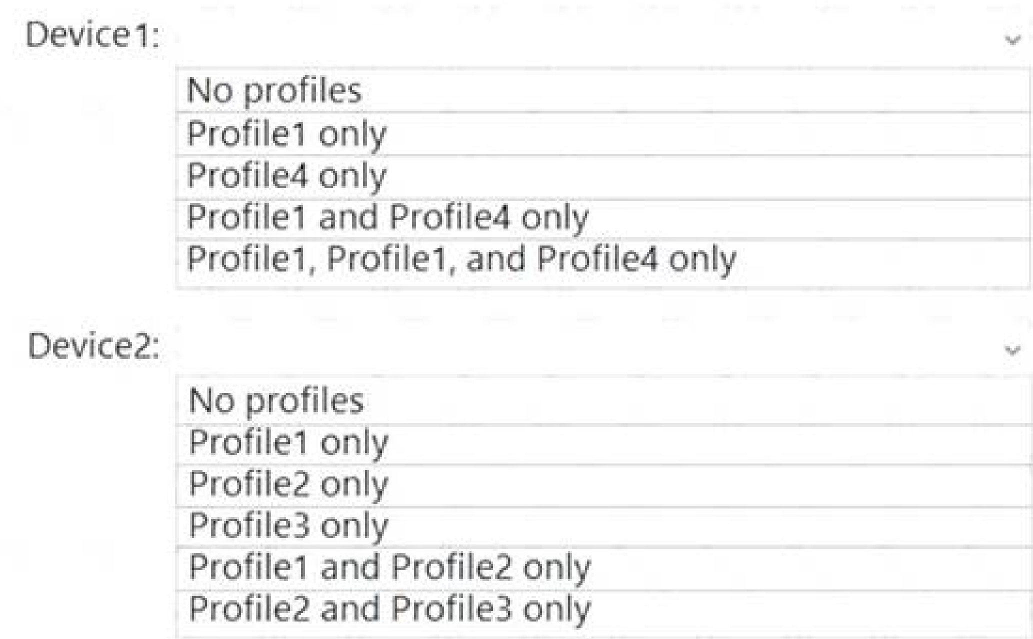
Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1, Group3	Tag1
Device2	Android	Group2	Tag2

You create the device configuration profiles shown in the following table.



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

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



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

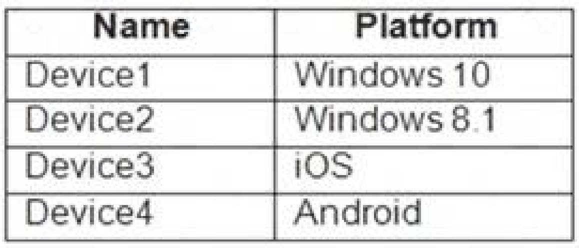
Device2:
- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

A. Mastered
B. Not Mastered

Answer: A

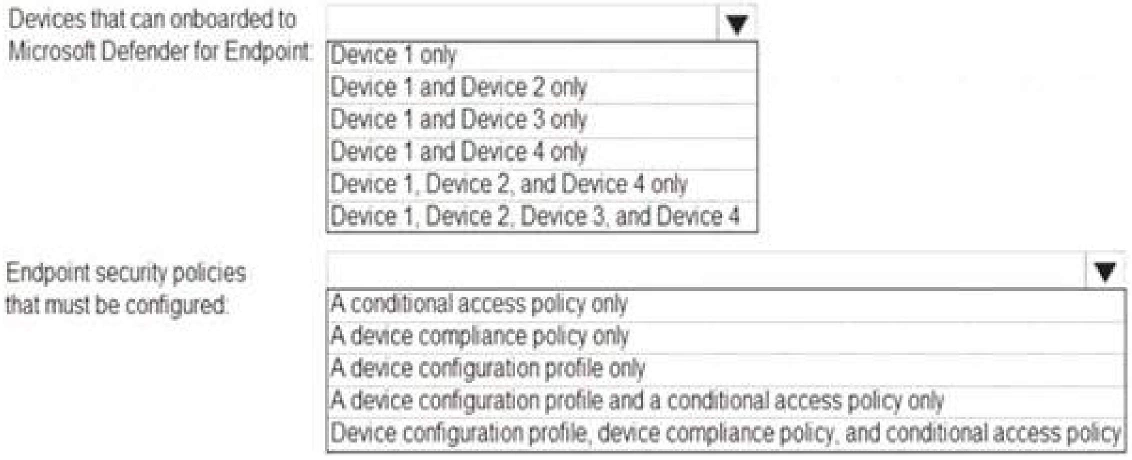
Explanation:
Graphical user interface, text, application, table Description automatically generated

NEW QUESTION 126
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint. You have devices enrolled in Microsoft Intune as shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.
You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Devices that can onboarded to Microsoft Defender for Endpoint:
- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

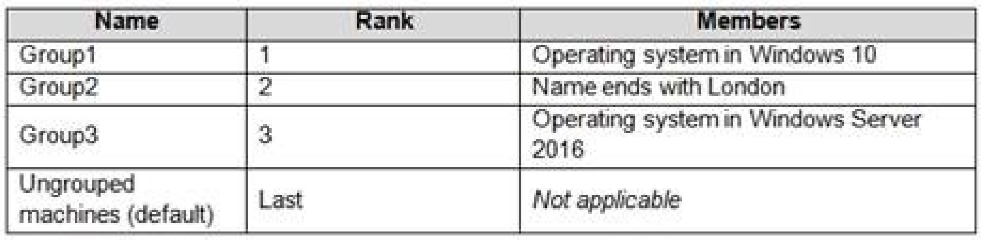
Endpoint security policies that must be configured:
- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

A. Mastered
B. Not Mastered

Answer: A

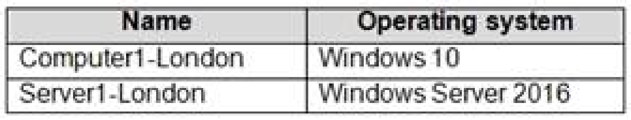
Explanation:
Text, table Description automatically generated with medium confidence
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?vie

NEW QUESTION 130
- (Exam Topic 5)
You use Microsoft Defender for Endpoint.
You have the Microsoft Defender for Endpoint device groups shown in the following table

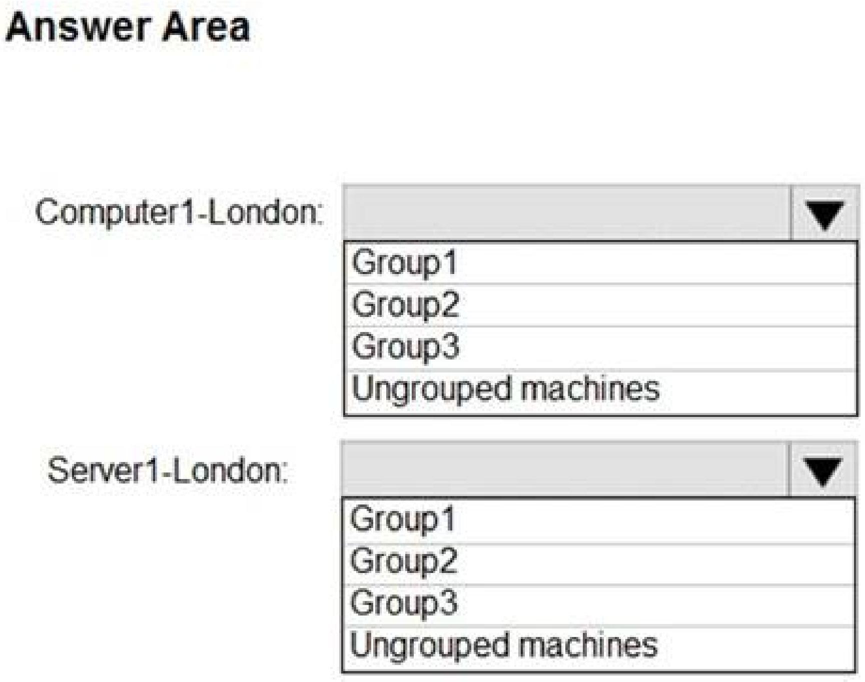


Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

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



Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016



Answer Area

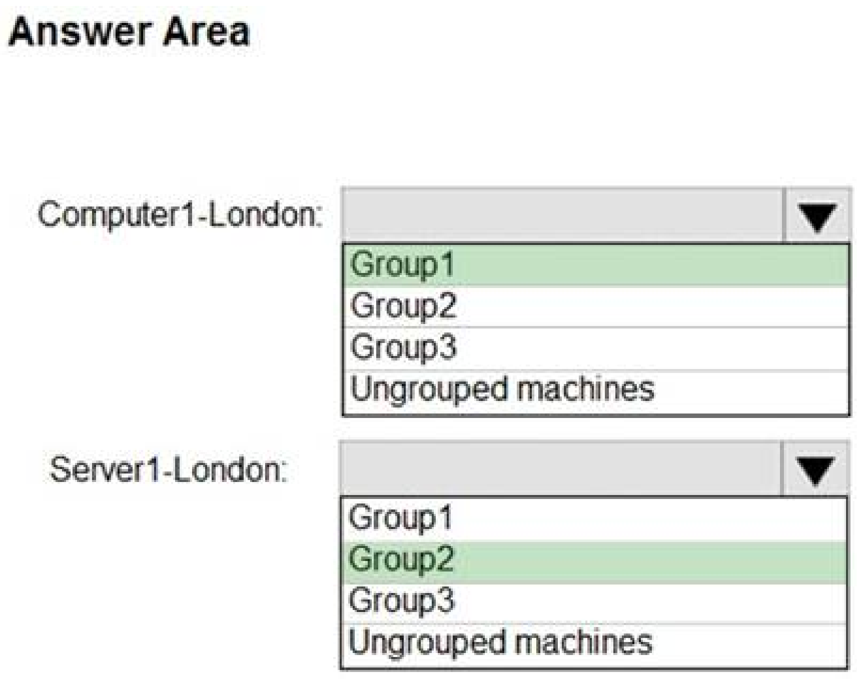
Computer1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

Server1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Computer1-London:

- Group1
- Group2
- Group3
- Ungrouped machines

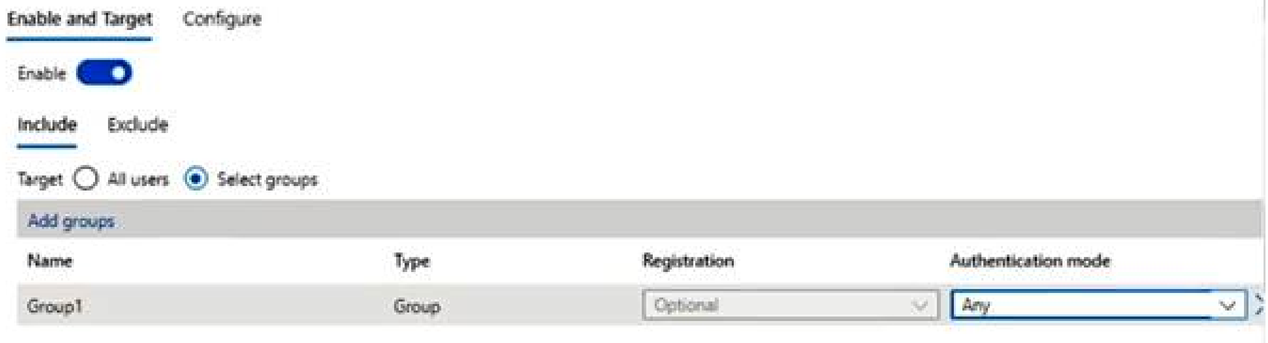
Server1-London:

- Group1
- Group2
- Group3
- Ungrouped machines

NEW QUESTION 131
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

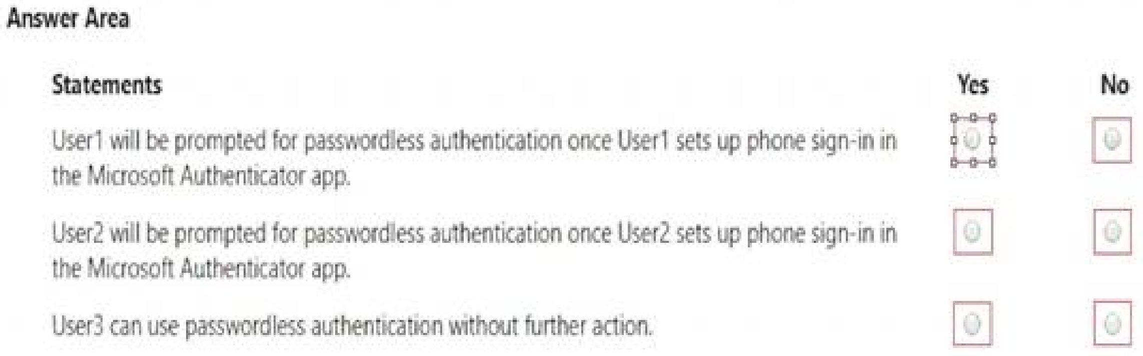
Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	*None*

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.



Name	Type	Registration	Authentication mode
Group1	Group	Optional	Any

Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.
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 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.	○	○
User3 can use passwordless authentication without further action.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
User1 is member of Group1.
User1 has MFA registered method of Microsoft Authenticater app (push notification)
The Microsoft Authenticator authentication method policy is configured for Group1, registration is optional, authentication method is any.
Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.
This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.
Box 2: No
User2 is member of Group2.
The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2. Box 3: No
User3 is member of Group1.
User3 has no MFA method registered.
User3 must choose an authentication method.
Note: Enable passwordless phone sign-in authentication methods
Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they'd like to use.

Reference:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phon

NEW QUESTION 135

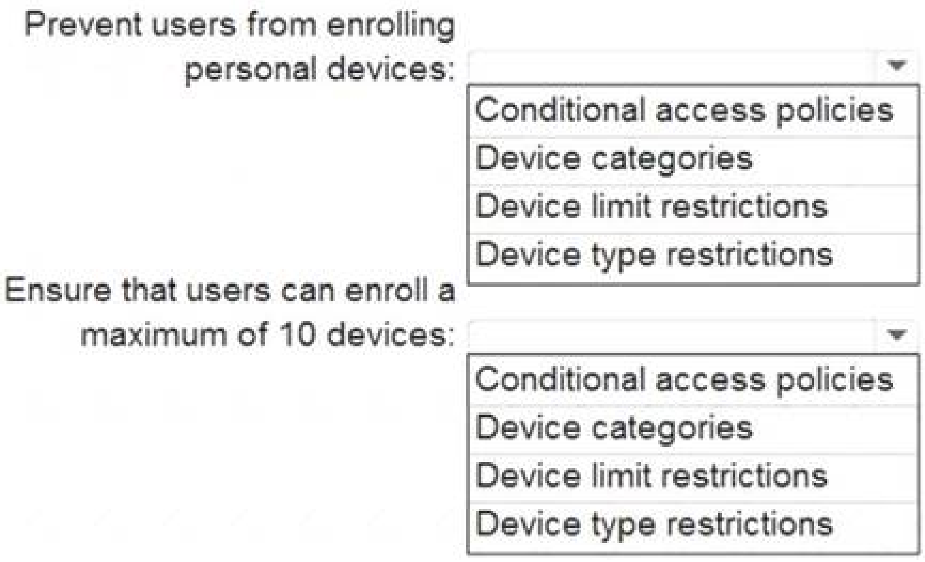
- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to configure Intune to meet the following requirements:

- Prevent users from enrolling personal devices.
- Ensure that users can enroll a maximum of 10 devices.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Prevent users from enrolling personal devices:

Conditional access policies
Device categories
Device limit restrictions
Device type restrictions

Ensure that users can enroll a maximum of 10 devices:

Conditional access policies
Device categories
Device limit restrictions
Device type restrictions

A. Mastered
B. Not Mastered

Answer: A

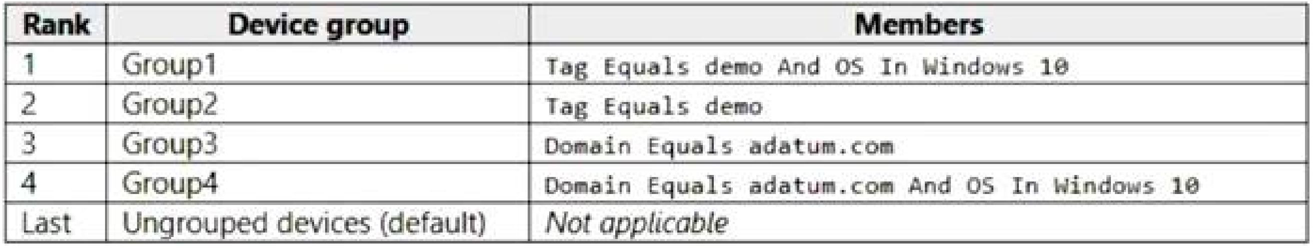
Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#blocking-personal-window

NEW QUESTION 137

- (Exam Topic 5)

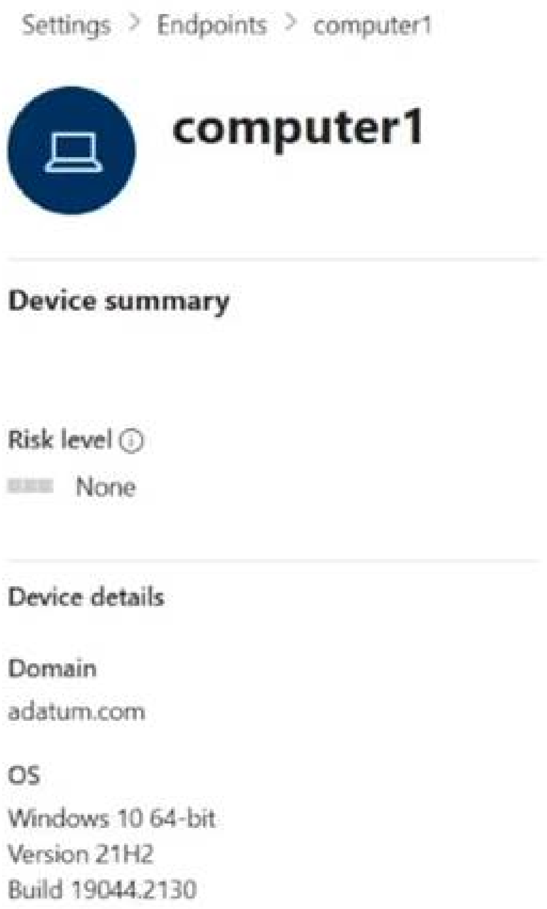
HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.



Rank	Device group	Members
1	Group1	`Tag Equals demo And OS In Windows 10`
2	Group2	`Tag Equals demo`
3	Group3	`Domain Equals adatum.com`
4	Group4	`Domain Equals adatum.com And OS In Windows 10`
Last	Ungrouped devices (default)	*Not applicable*

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.



Settings > Endpoints > computer1

computer1

Device summary

Risk level
None

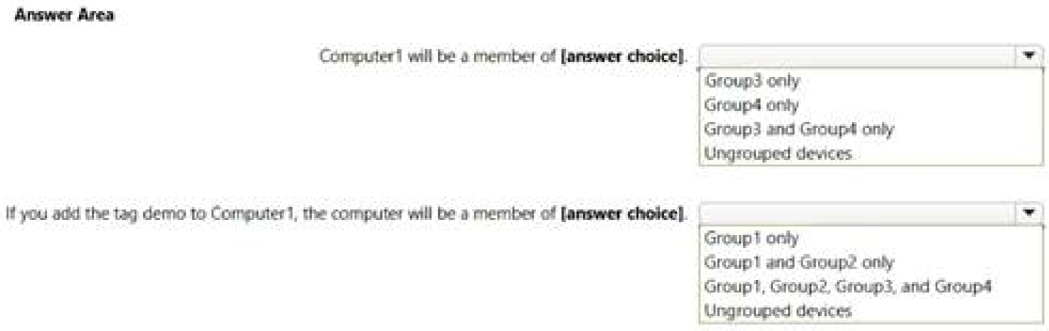
Device details

Domain
adatum.com

OS
Windows 10 64-bit
Version 21H2
Build 19044.2130

Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.



Answer Area

Computer1 will be a member of **[answer choice]**.

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Group3 and Group4 only Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION 141
- (Exam Topic 5)
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager. You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

A. an app configuration policy
B. an app
C. a device configuration profile
D. a device compliance policy

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

NEW QUESTION 146
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
Conditional Access is configured to block high-risk sign-ins for all users.
All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month.
You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention. What should you configure?

A. an exclusion group
B. the MFA registration policy
C. named locations
D. self-service password reset (SSPR)

Answer: D

Explanation:
Self-remediation with self-service password reset
If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate

NEW QUESTION 147
- (Exam Topic 5)
You are reviewing alerts in the Microsoft 365 Defender portal.
How long are the alerts retained in the portal?

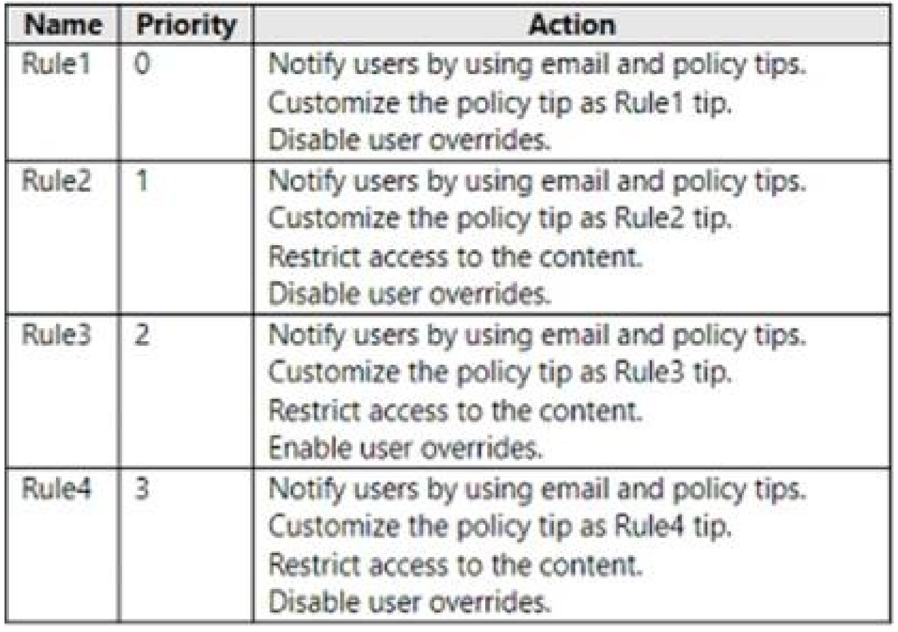
A. 30 days
B. 60 days
C. 3 months
D. 6 months
E. 12 months

Answer: C

Explanation:
Data retention information for Microsoft Defender for Office 365
By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.
Defender for Office 365 Plan 1
* Alert metadata details (Microsoft Defender for Office alerts) 90 days.
Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the

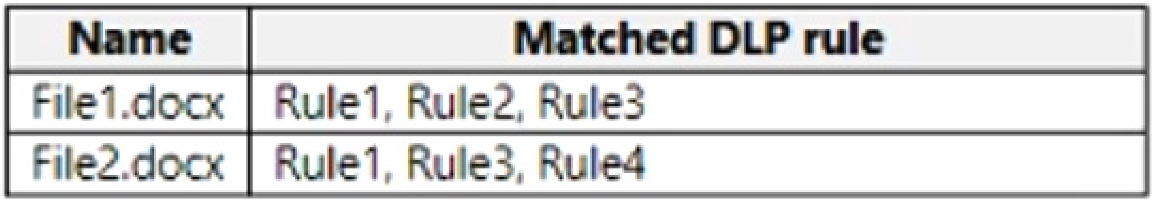
top of the list so you can see it first.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention

NEW QUESTION 149
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.



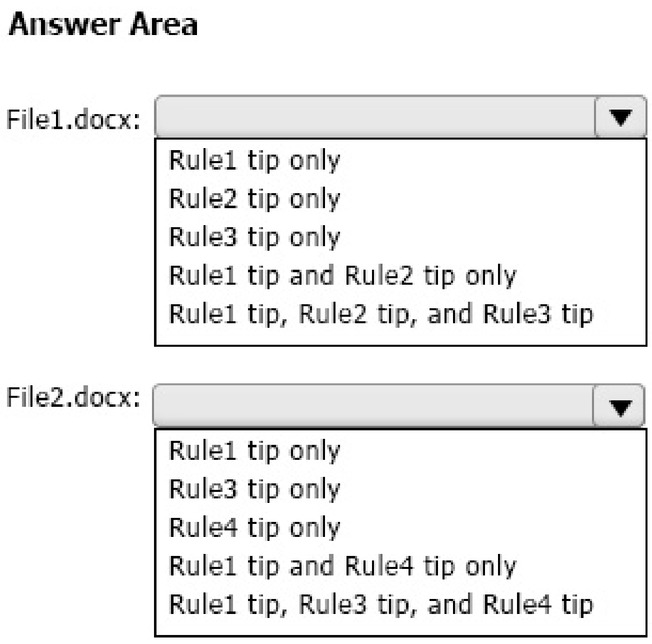
Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.



Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

File1.docx:
- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:
- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

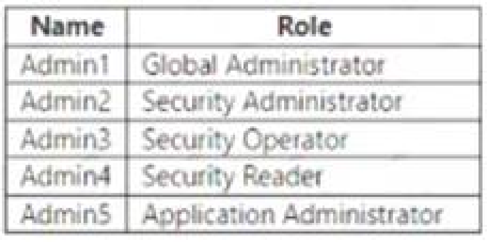
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Rule1 tip only
File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.
Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.
Box 2: Rule1 tip only
Note: User Override support
The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).
It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched. Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips

NEW QUESTION 154
- (Exam Topic 5)

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

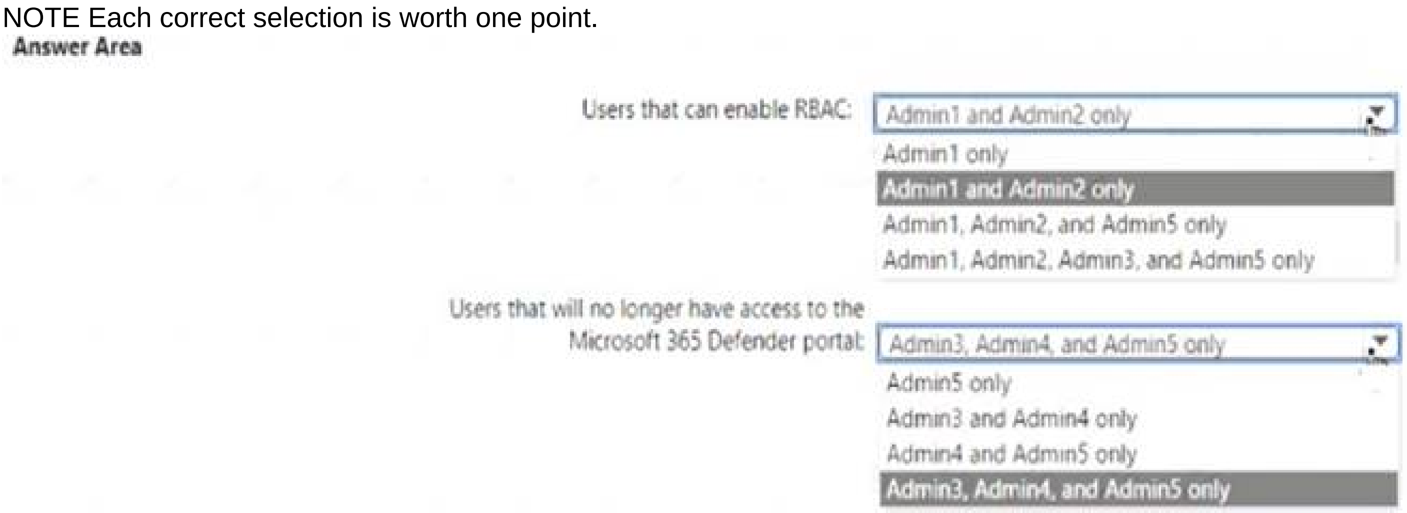


Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You ate implementing Microsoft Defender for Endpoint

You need to enable role-based access control (RBAQ to restrict access to the Microsoft 365 Defender portal. Which users can enable RBAC, and winch users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.



Answer Area

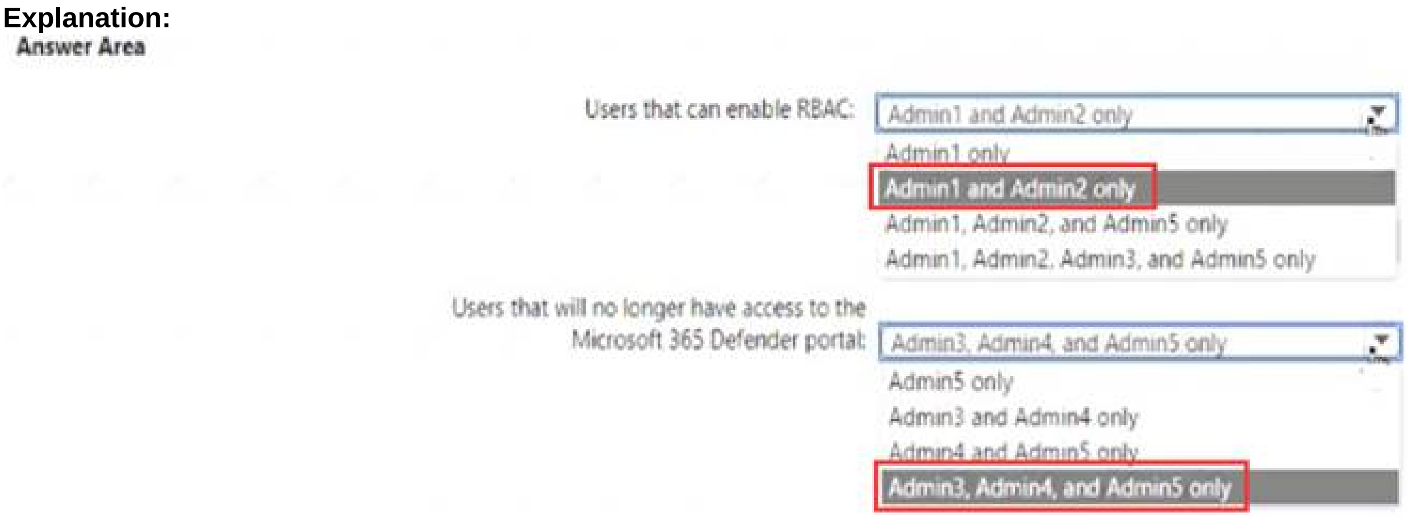
Users that can enable RBAC: Admin1 and Admin2 only
- Admin1 only
- Admin1 and Admin2 only
- Admin1, Admin2, and Admin5 only
- Admin1, Admin2, Admin3, and Admin5 only

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

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

NEW QUESTION 157

- (Exam Topic 5)

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

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

A. 20 hours
B. 12 hours
C. 7 hours
D. 48 hours

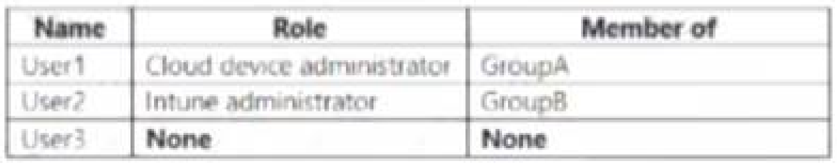
Answer: B

NEW QUESTION 160

- (Exam Topic 5)

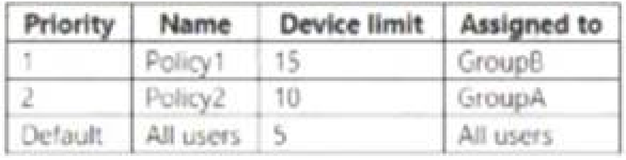
You have several devices enrolled in Microsoft Endpoint Manager

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown In the following table.



Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

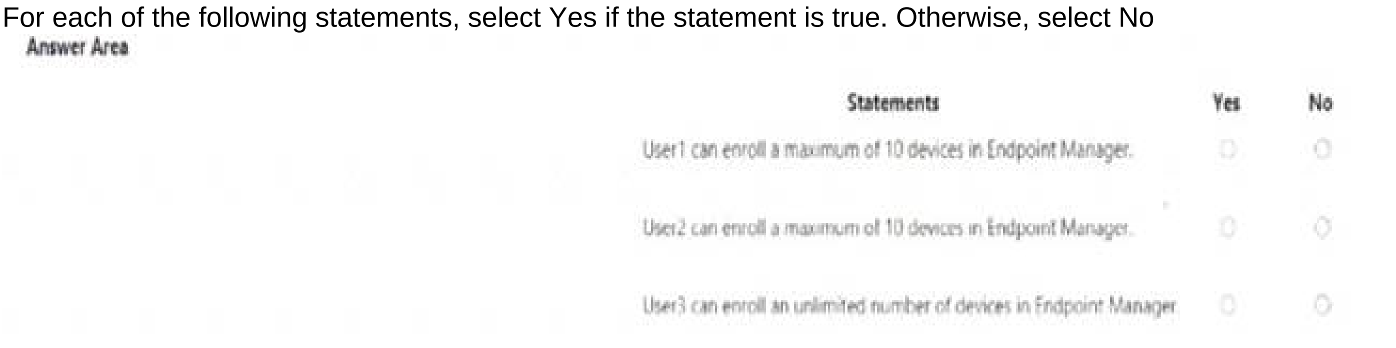
The device limit restrictions in Endpoint manager are configured as shown in the following table.



Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All users

You add user as a device enrollment manager in Endpoint manager

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



Answer Area

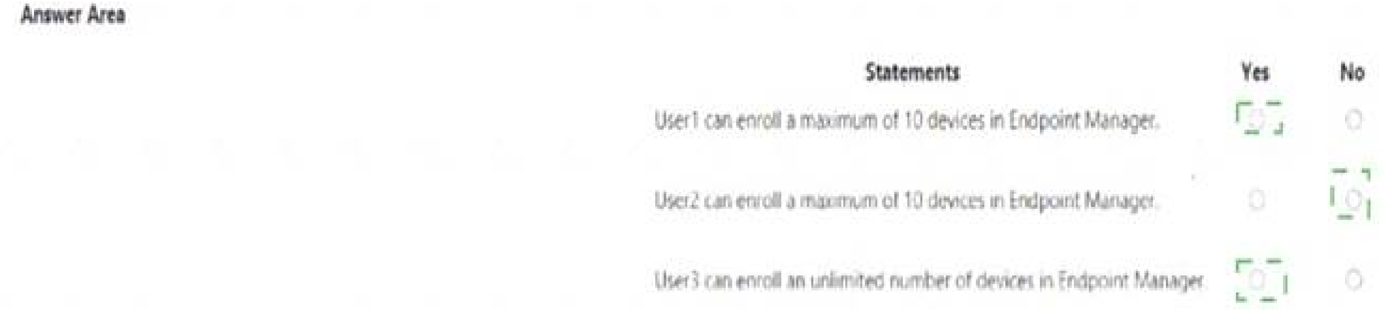
Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager	○	○

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	[✓ ○]	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	[✓ ○]
User3 can enroll an unlimited number of devices in Endpoint Manager	[✓ ○]	○

NEW QUESTION 161

- (Exam Topic 5)

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

- Microsoft 365 Apps for enterprise
- Office for the web
- Office 2016
- Office 2019

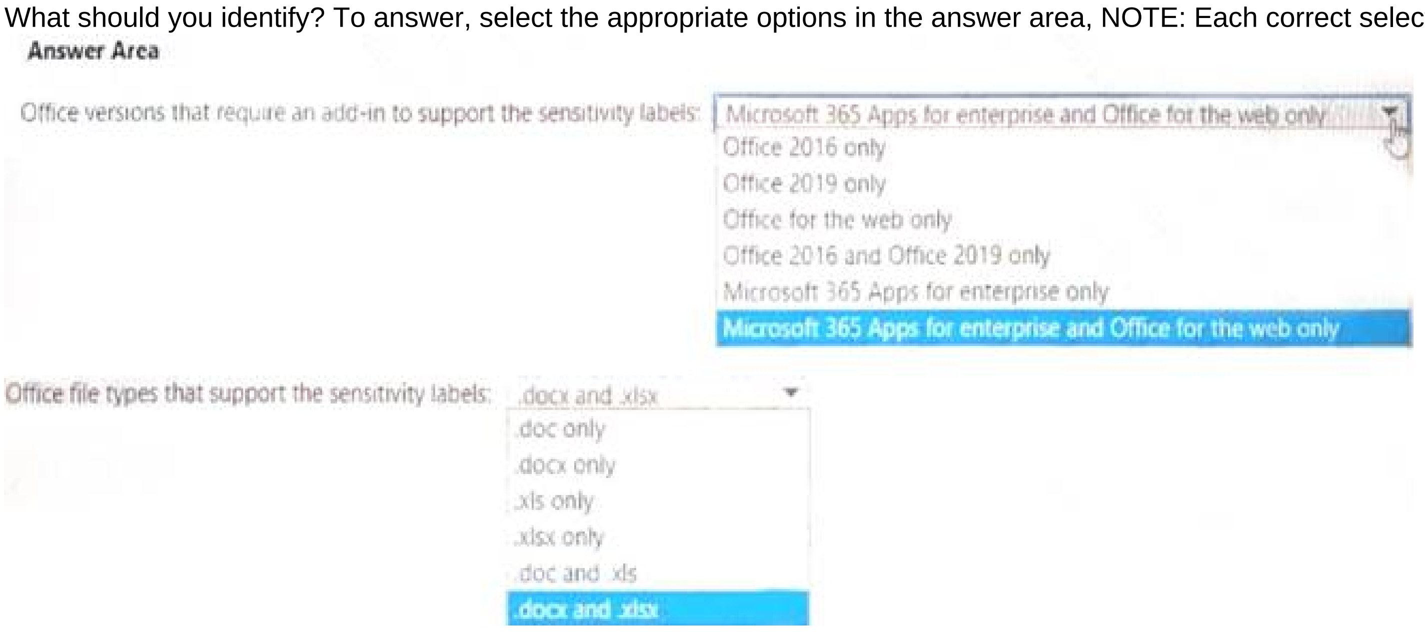
The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- xls

You plan to use sensitivity labels. You need to identify the following:

- Which versions of Office require an add-in to support the sensitivity labels.
- Which file types support the sensitivity labels.

What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.



Answer Area

Office versions that require an add-in to support the sensitivity labels: Microsoft 365 Apps for enterprise and Office for the web only

Office 2016 only
Office 2019 only
Office for the web only
Office 2016 and Office 2019 only
Microsoft 365 Apps for enterprise only
Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels: .docx and .xlsx

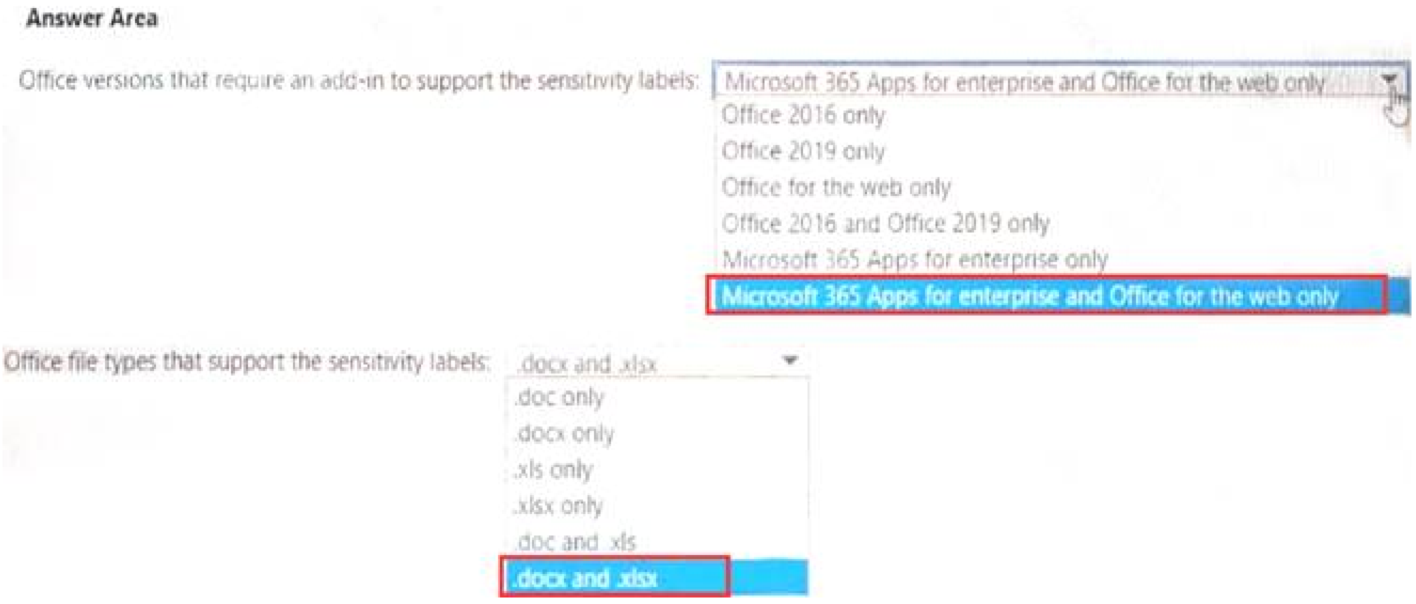
.doc only
.docx only
.xls only
.xlsx only
.doc and .xls
.docx and .xlsx

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Answer Area

Office versions that require an add-in to support the sensitivity labels: Microsoft 365 Apps for enterprise and Office for the web only

Office 2016 only
Office 2019 only
Office for the web only
Office 2016 and Office 2019 only
Microsoft 365 Apps for enterprise only
Microsoft 365 Apps for enterprise and Office for the web only

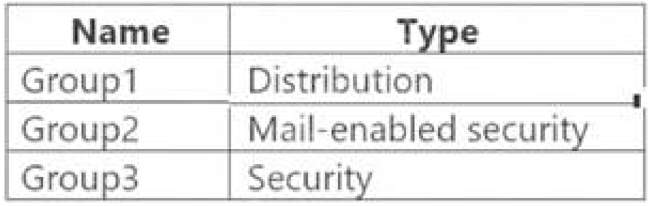
Office file types that support the sensitivity labels: .docx and .xlsx

.doc only
.docx only
.xls only
.xlsx only
.doc and .xls
.docx and .xlsx

NEW QUESTION 166

- (Exam Topic 5)

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



Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile. To which groups can you assign to the profile?

A. Group3 only
B. Group1 and Group3 only
C. Group2 and Group3 only
D. Group1. Group2. and Group3

Answer: A

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

NEW QUESTION 168

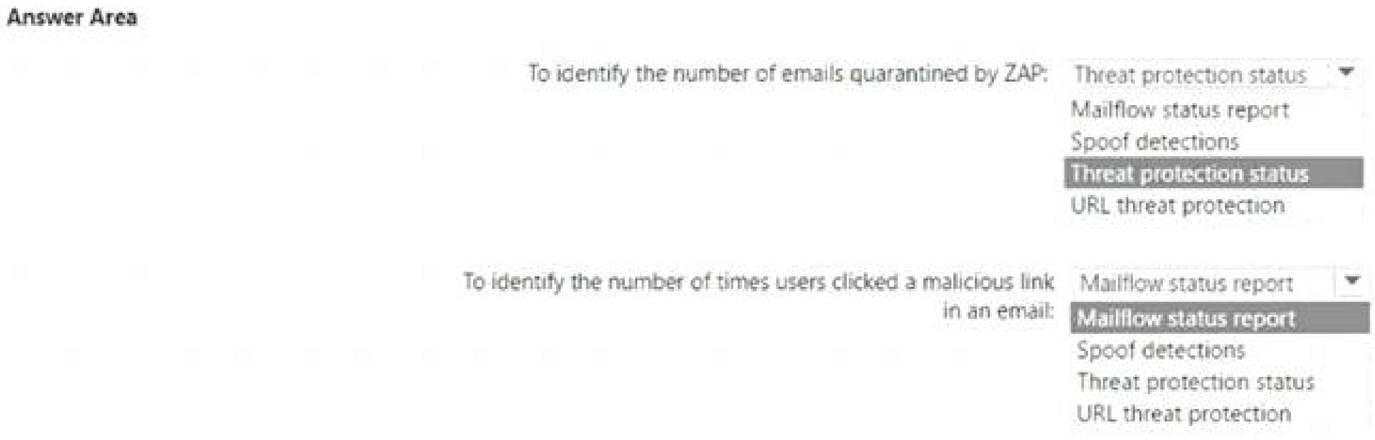
- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.

The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy. You need to identify the following information:

- The number of email messages quarantined by zero-hour auto purge (ZAP)
- The number of times users clicked a malicious link in an email message

Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

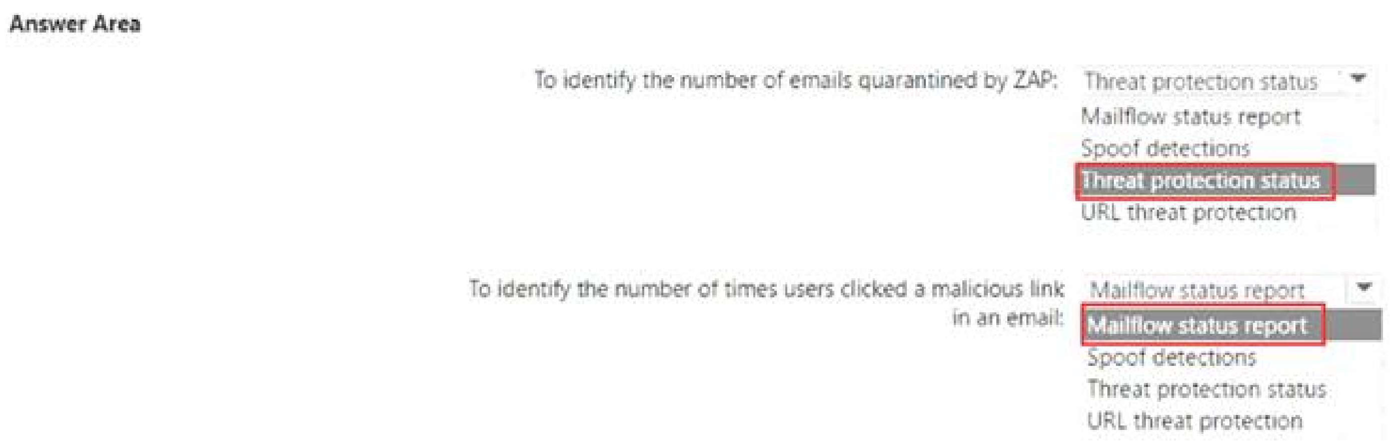
To identify the number of emails quarantined by ZAP: Threat protection status

To identify the number of times users clicked a malicious link in an email: Mailflow status report

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

To identify the number of emails quarantined by ZAP: Threat protection status

To identify the number of times users clicked a malicious link in an email: Mailflow status report

NEW QUESTION 169
- (Exam Topic 5)
Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours. You plan to sync contoso.com to an Azure AD tenant.
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?

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

Answer: A

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

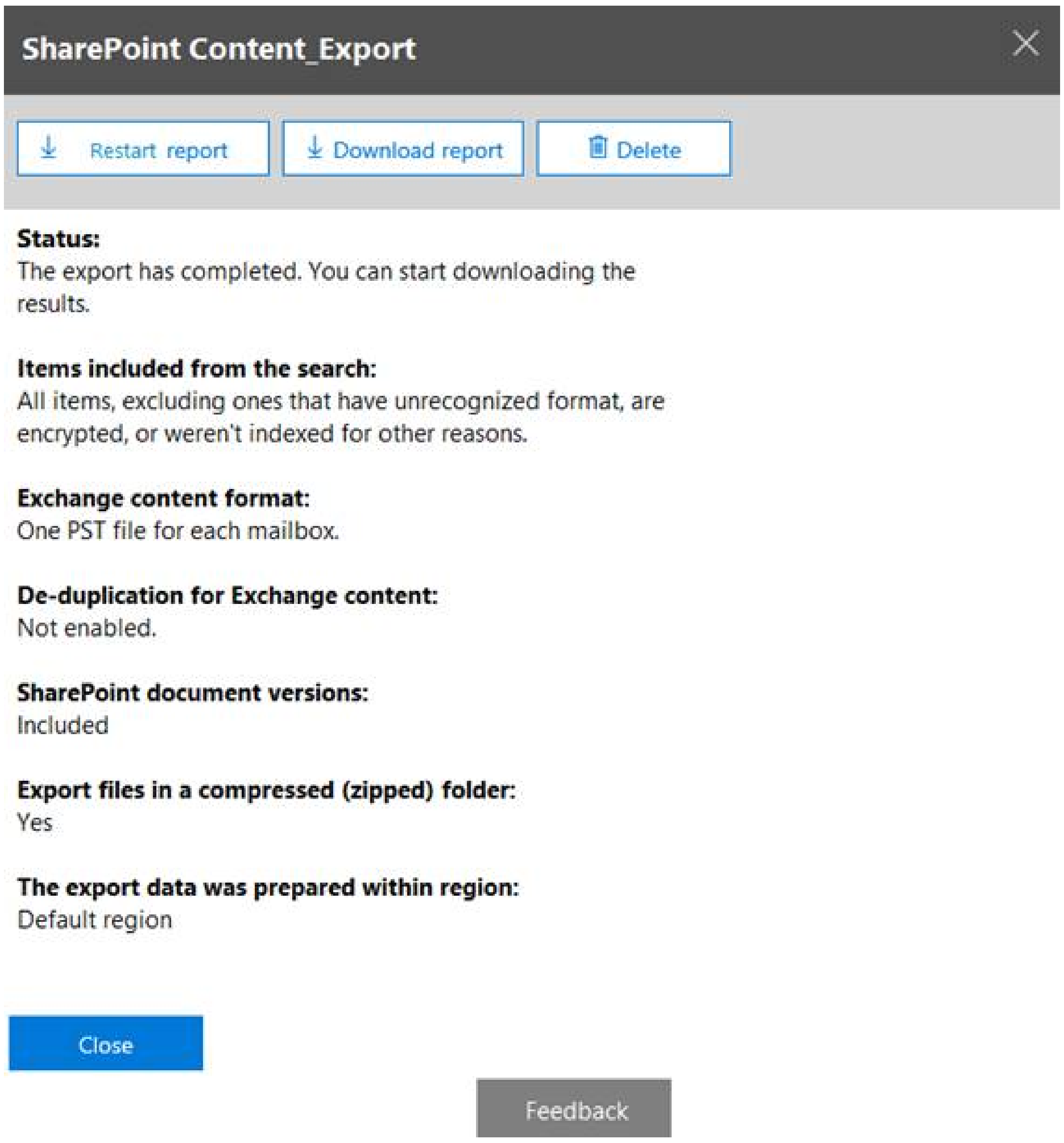
NEW QUESTION 173
- (Exam Topic 5)
Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company’s compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset. What should you do first?

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

Answer: D

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

NEW QUESTION 175
- (Exam Topic 5)
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



SharePoint Content_Export

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

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

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

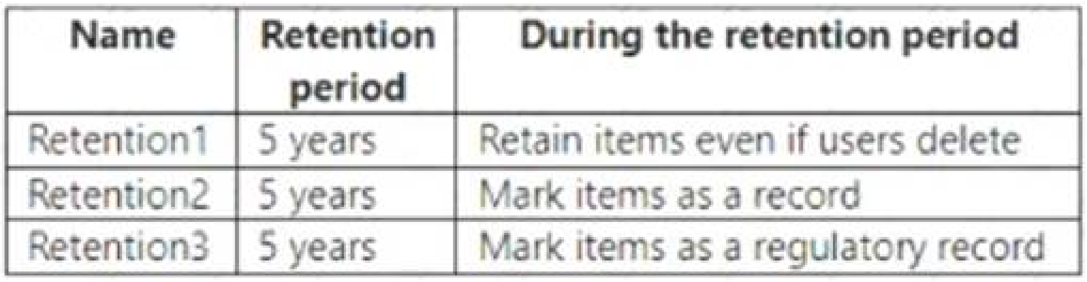
What will be excluded from the export?

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

Answer: B

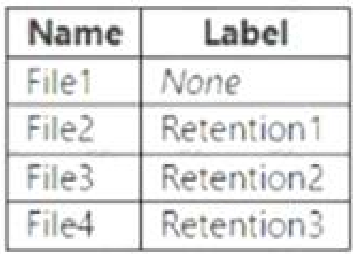
Explanation:
Unrecognized file formats are excluded from the search.
Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o3 https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

NEW QUESTION 176
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.



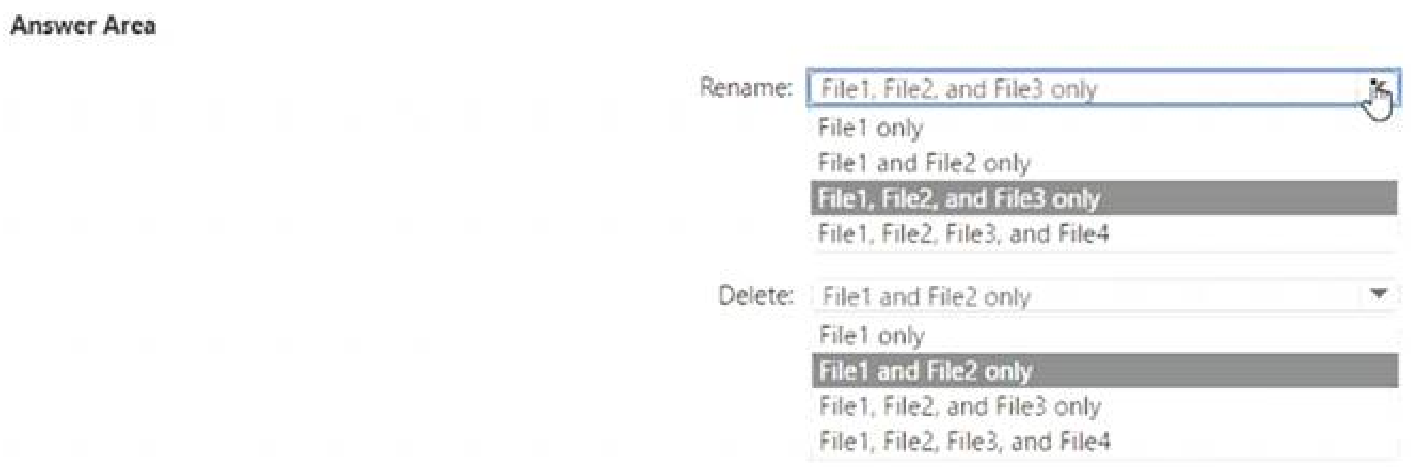
Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record

Site1 contains the files shown in the following table.



Name	Label
File1	*None*
File2	Retention1
File3	Retention2
File4	Retention3

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

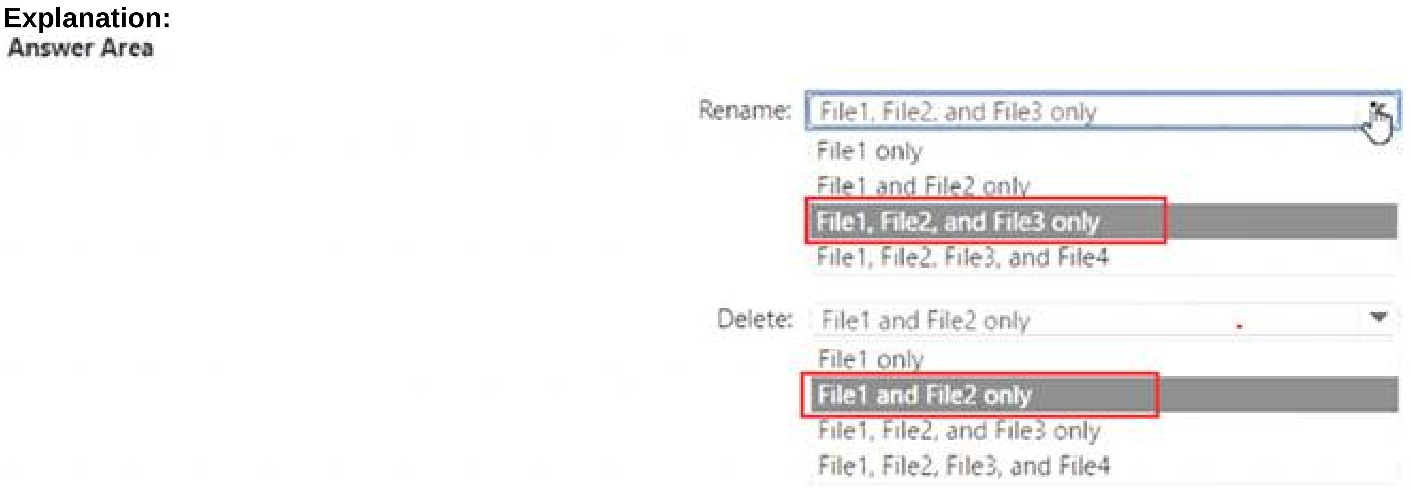
Rename: File1, File2, and File3 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

Delete: File1 and File2 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Rename: File1, File2, and File3 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

Delete: File1 and File2 only
- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

NEW QUESTION 179
- (Exam Topic 5)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

A. Ubuntu Linux
B. macOS
C. iOS
D. Android

Answer: B

Explanation:
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices Note:
There are several versions of this question in the exam. The question has two possible correct answers:
- Windows 10
- macOS

Other incorrect answer options you may see on the exam include the following:
- Android Enterprise
- Windows 8.1 Reference:

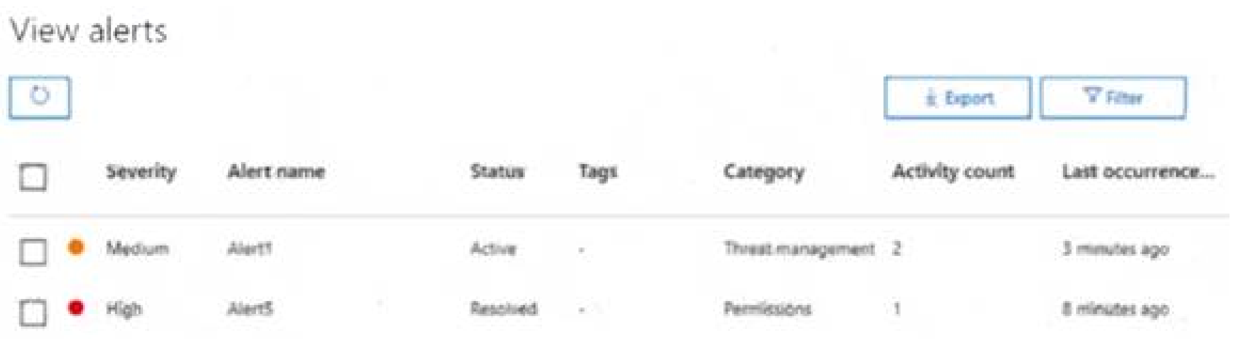
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

NEW QUESTION 184
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
Al users have Mac computers. ATI the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.
You need to configure Microsoft Defender for Endpoint on the computers. What should you create from the Endpoint Management admin center?

A. a Microsoft Defender for Endpoint baseline profile
B. an update policy for iOS
C. a device configuration profile
D. a mobile device management (MDM) security baseline profile

Answer: D

NEW QUESTION 186
- (Exam Topic 5)
You have a Microsoft 365 ES tenant.
You have the alerts shown in the following exhibit.

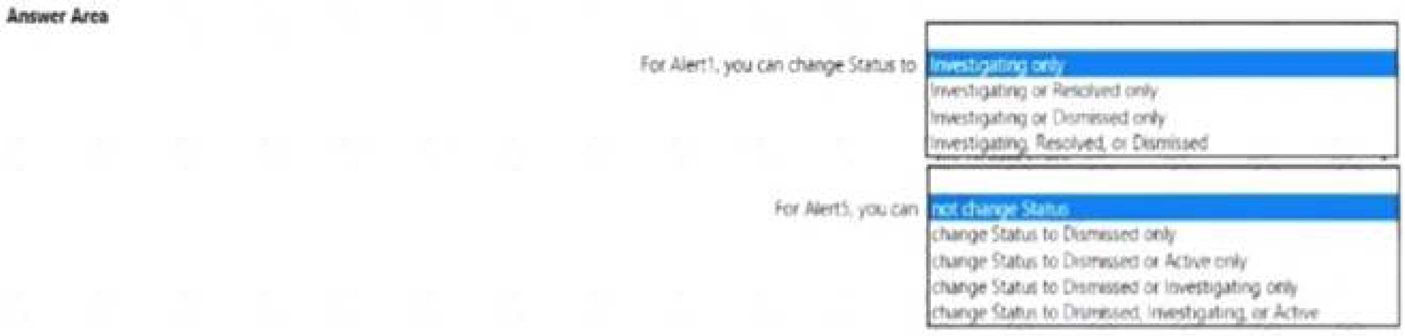


View alerts

□	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
□	● Medium	Alert1	Active	-	Threat management	2	3 minutes ago
□	● High	Alert5	Resolved	-	Permissions	1	8 minutes ago

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

NOTE: Each correct selection is worth one point.



Answer Area

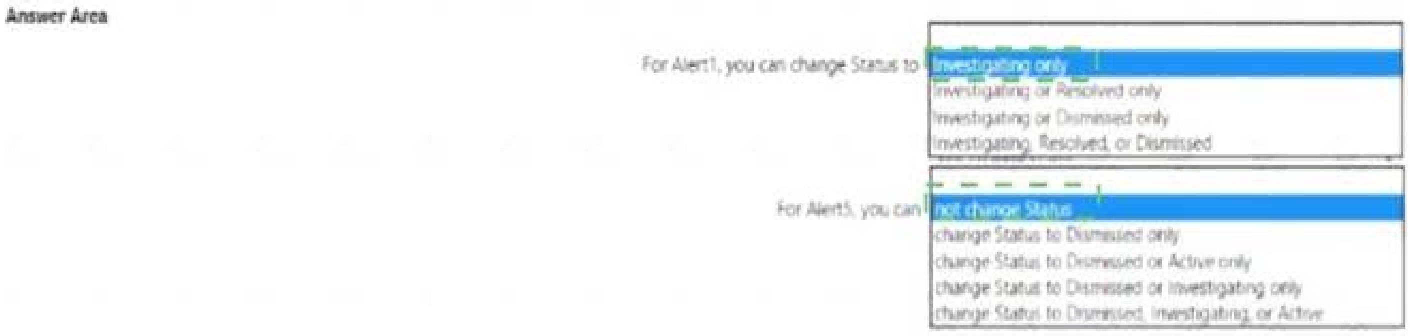
For Alert1, you can change Status to
- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can
- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

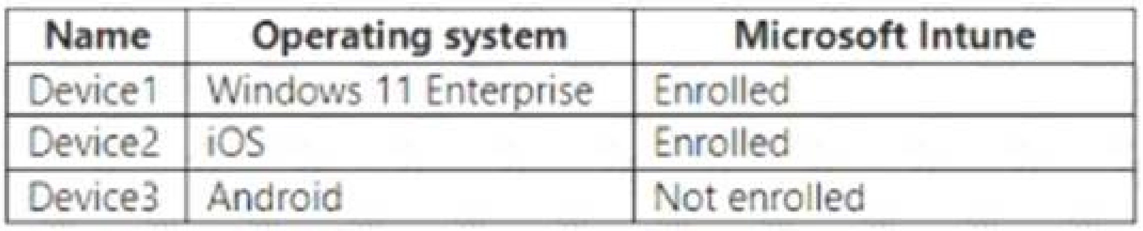
For Alert1, you can change Status to
- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can
- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

NEW QUESTION 190

- (Exam Topic 5)

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



Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

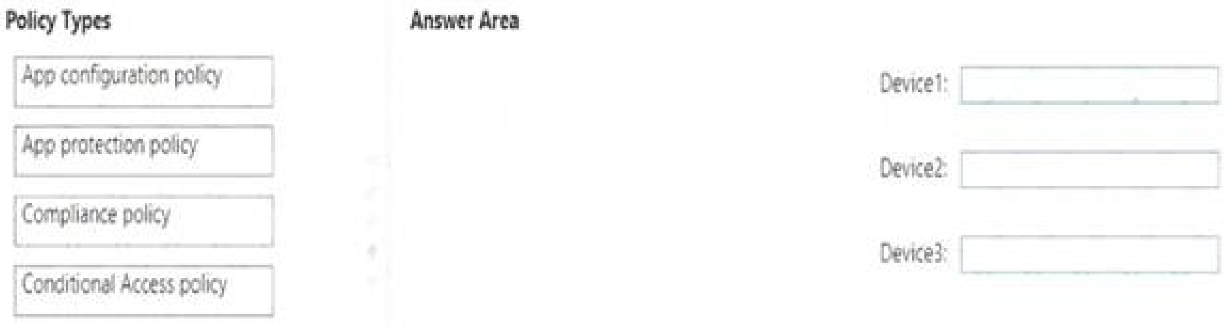
You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

- Word files created by using Windows devices must be encrypted automatically.
- If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
- For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of polio/ should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Policy Types

- App configuration policy
- App protection policy
- Compliance policy
- Conditional Access policy

Answer Area

Device1:

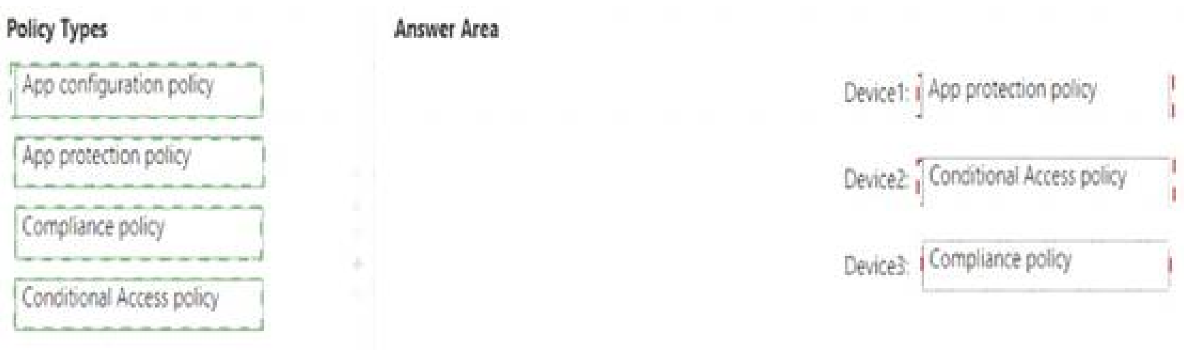
Device2:

Device3:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Policy Types

- App configuration policy
- App protection policy
- Compliance policy
- Conditional Access policy

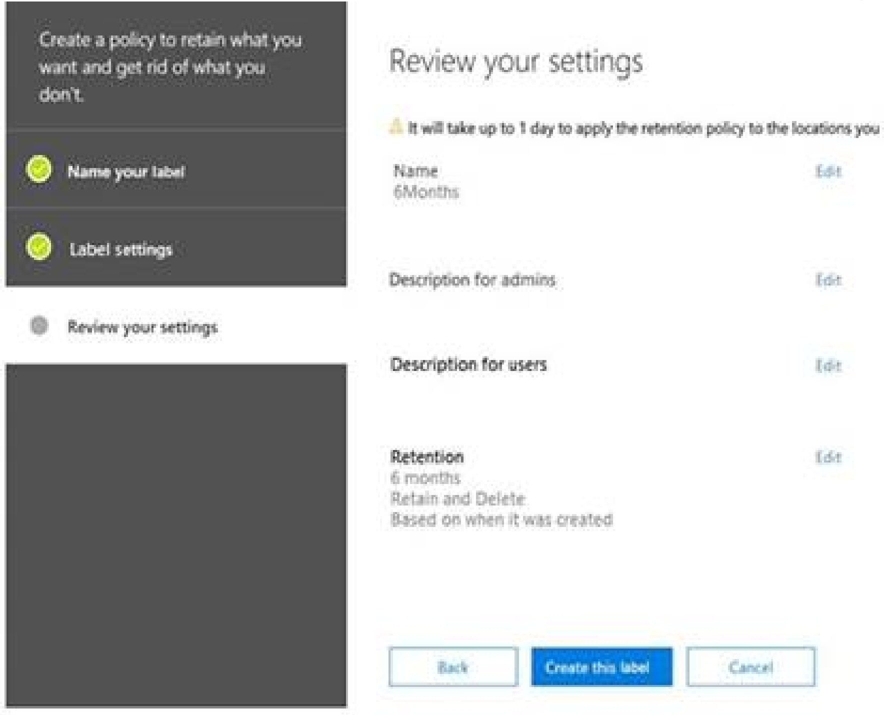
Answer Area

Device1: App protection policy

Device2: Conditional Access policy

Device3: Compliance policy

NEW QUESTION 193
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 tenant.
You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)



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

- Name your label
- Label settings
- Review your settings

Review your settings

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

Name
6Months
Edit

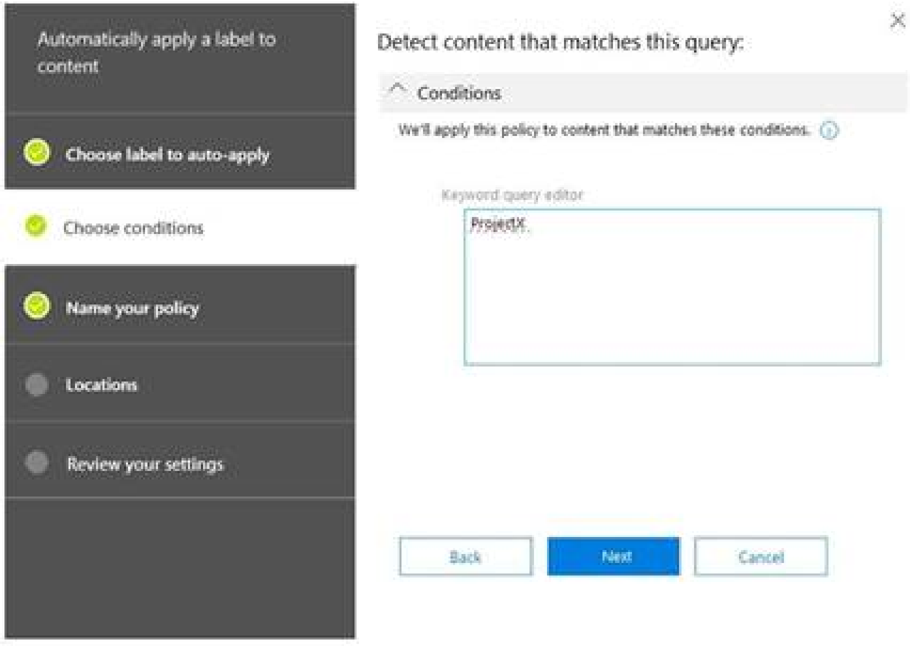
Description for admins
Edit

Description for users
Edit

Retention
6 months
Retain and Delete
Based on when it was created
Edit

Back | Create this label | Cancel

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)



Automatically apply a label to content

- Choose label to auto-apply
- Choose conditions
- Name your policy
- Locations
- Review your settings

Detect content that matches this query:

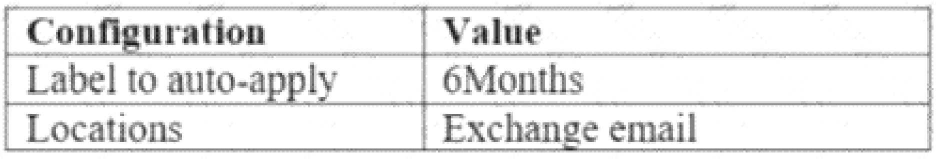
Conditions

We'll apply this policy to content that matches these conditions.

Keyword query editor
ProjectX

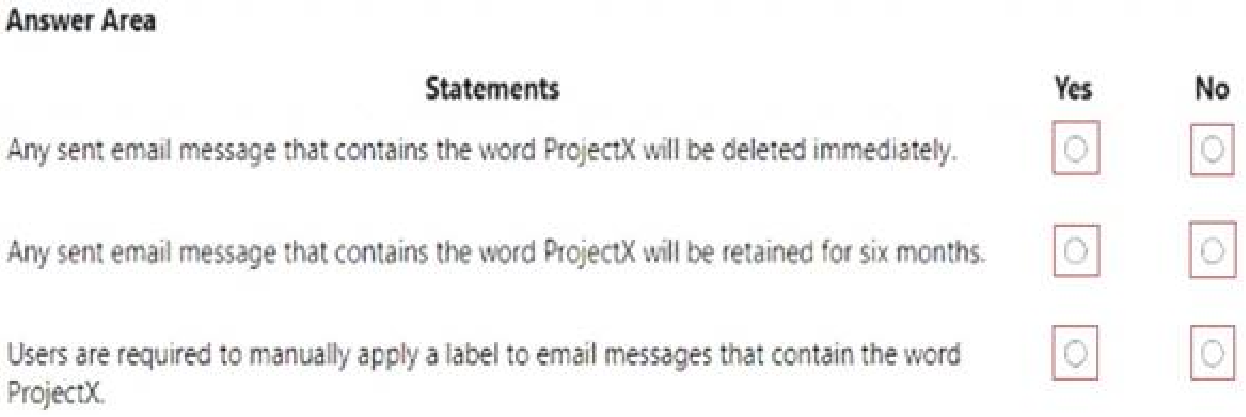
Back | Next | Cancel

The label policy is configured as shown in the following table.



Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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
Any sent email message that contains the word ProjectX will be deleted immediately.	○	○
Any sent email message that contains the word ProjectX will be retained for six months.	○	○
Users are required to manually apply a label to email messages that contain the word ProjectX.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
Box 2: Yes
Box 3: No Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

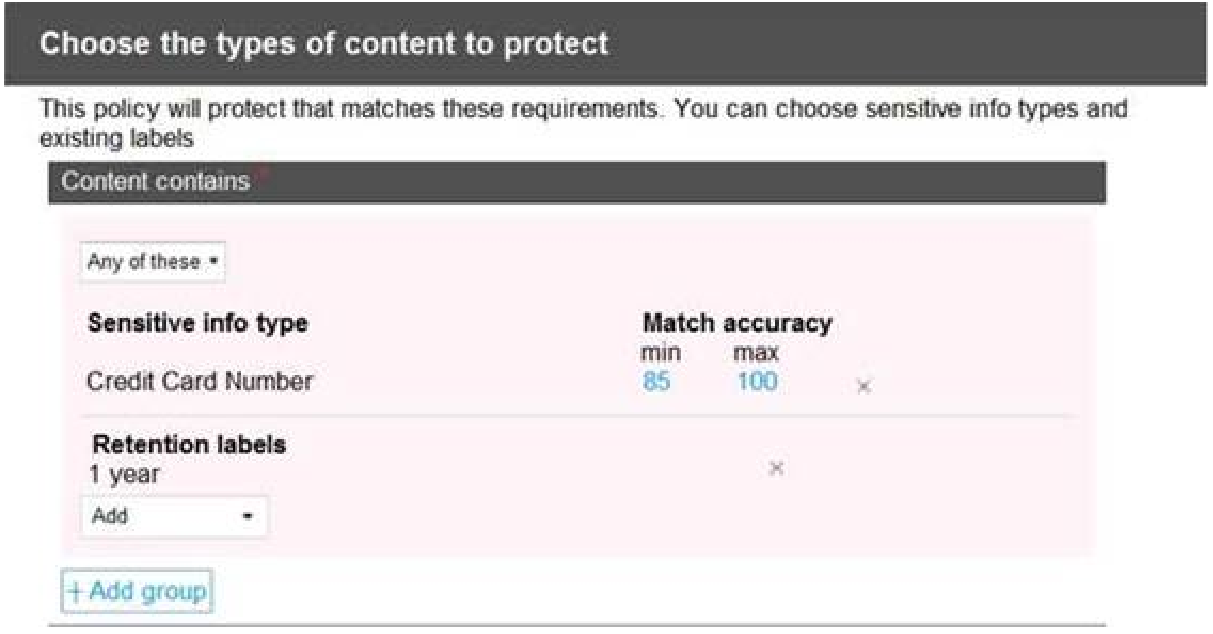
NEW QUESTION 198
- (Exam Topic 5)
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector. Where can you store data from the LinkedIn connector?

A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide

NEW QUESTION 201
- (Exam Topic 5)
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.



Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

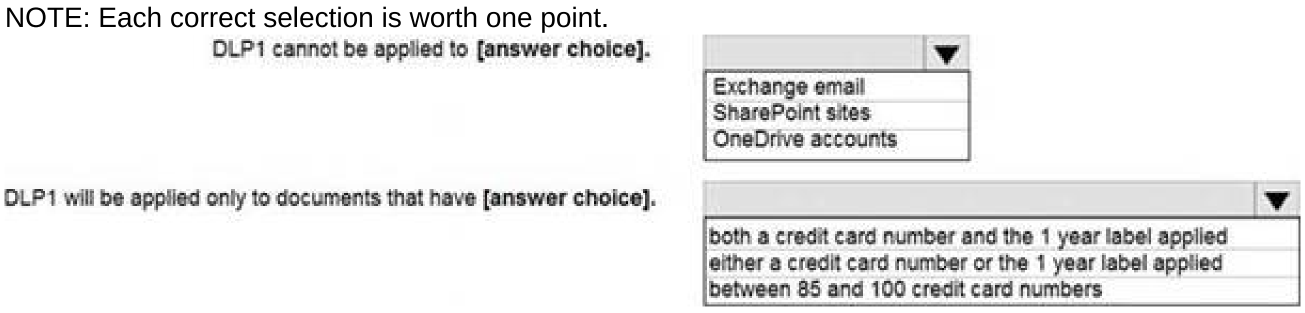
Content contains

Any of these

Sensitive info type	Match accuracy min	Match accuracy max
Credit Card Number	85	100

Retention labels
1 year

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.



DLP1 cannot be applied to [answer choice].
- Exchange email
- SharePoint sites
- OneDrive accounts

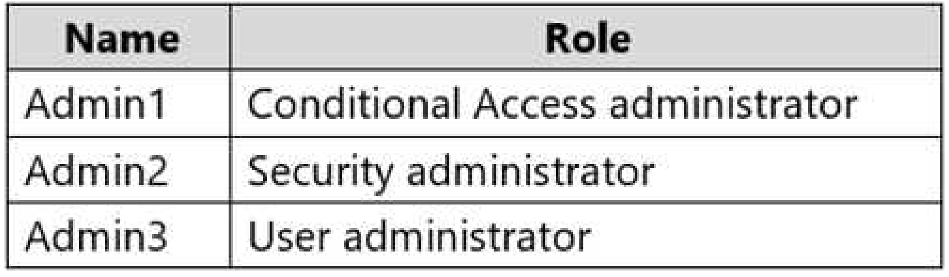
DLP1 will be applied only to documents that have [answer choice].
- both a credit card number and the 1 year label applied
- either a credit card number or the 1 year label applied
- between 85 and 100 credit card numbers

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwid

NEW QUESTION 202
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

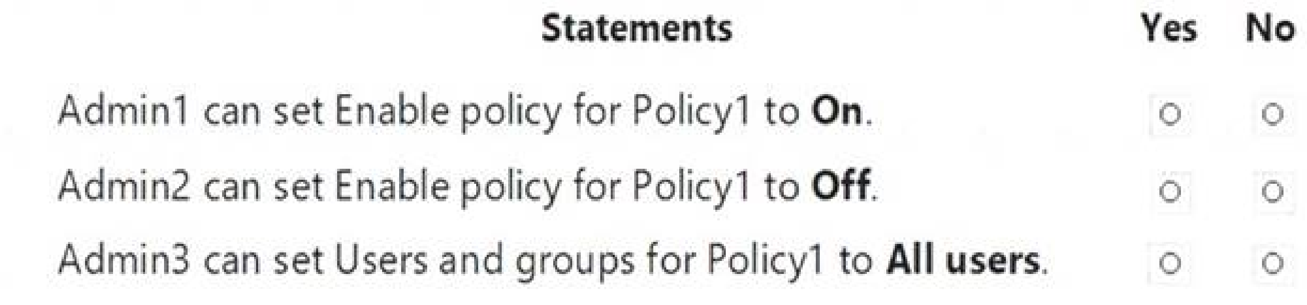


Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations: Name: Policy1
Assignments:
- Users and groups: Group1
- Cloud aps or actions: All cloud apps

- Access controls:
- Grant, require multi-factor authentication
- Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.
For each of the following settings select Yes, if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



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

A. Mastered
B. Not Mastered

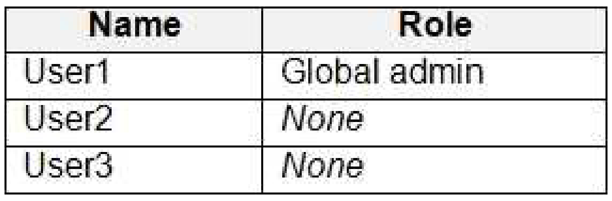
Answer: A

Explanation:
Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

- Conditional Access policies can be enabled in report-only mode.
- During sign-in, policies in report-only mode are evaluated but not enforced.
- Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

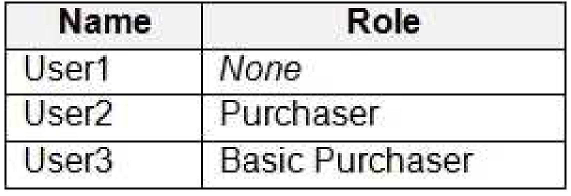
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-on

NEW QUESTION 205
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



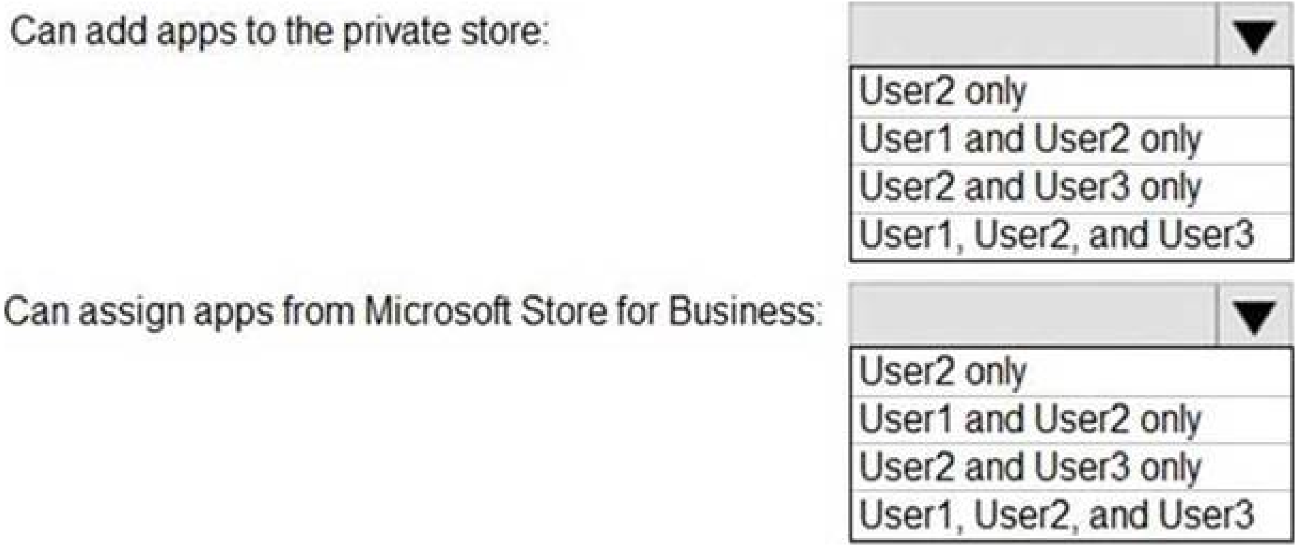
Name	Role
User1	Global admin
User2	*None*
User3	*None*

You provision the private store in Microsoft Store for Business.
You assign Microsoft Store for Business roles to the users as shown in the following table.



Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

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



Can add apps to the private store:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

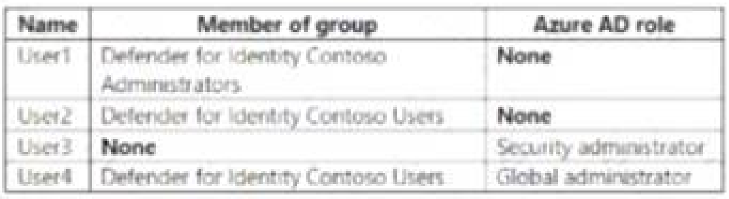
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-rol

NEW QUESTION 206
- (Exam Topic 5)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.



Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User1 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

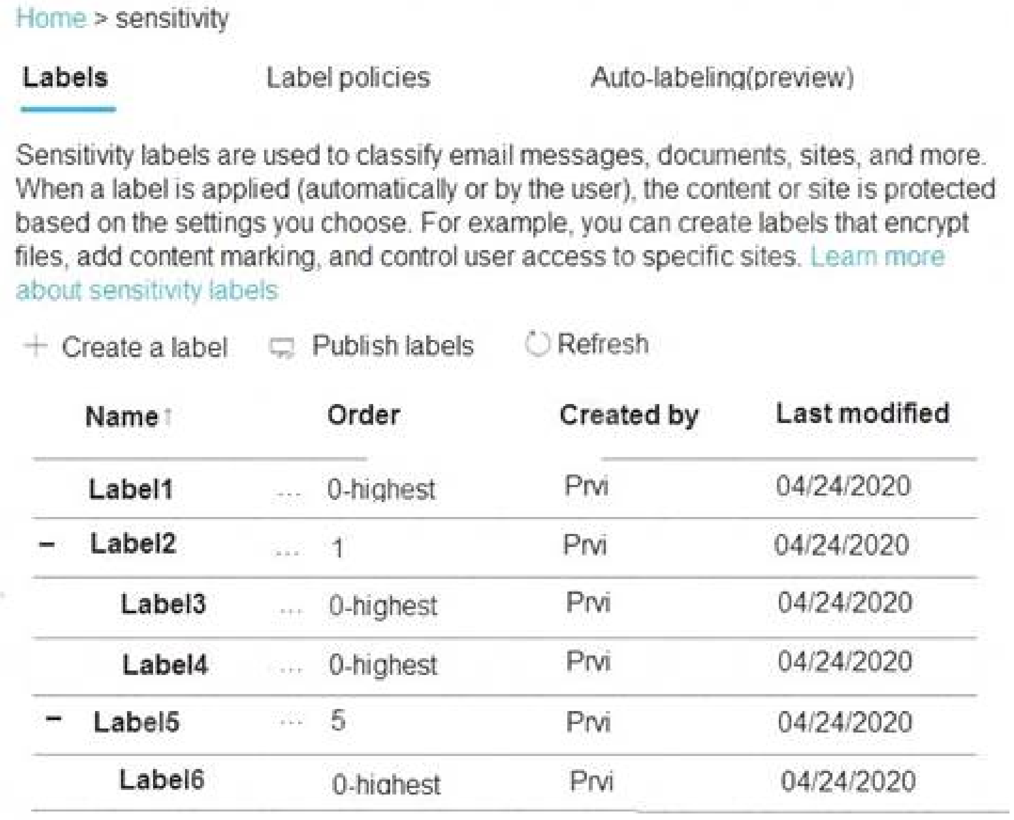
NEW QUESTION 208
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list. You need to remove User1 from the Restricted entities list. What should you use?

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

Answer: D

Explanation:
Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft 365 Defender portal
In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review
> Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-user

NEW QUESTION 210
- (Exam Topic 5)
You have the sensitivity labels shown in the following exhibit.



Home > sensitivity

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

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

Which labels can users apply to content?

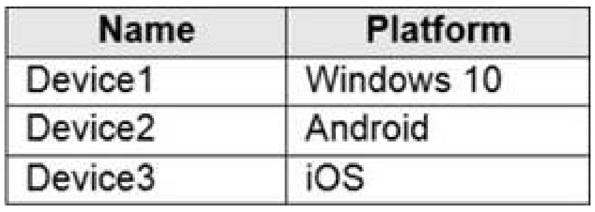
A. Label3, Label4, and Label6 only
B. Label1, Label2. Label3. Label4. Label5. and Label6
C. Label1, Label2, and Label5 only
D. Label1, Label3, Label4, and Label6 only

Answer: D

Explanation:

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

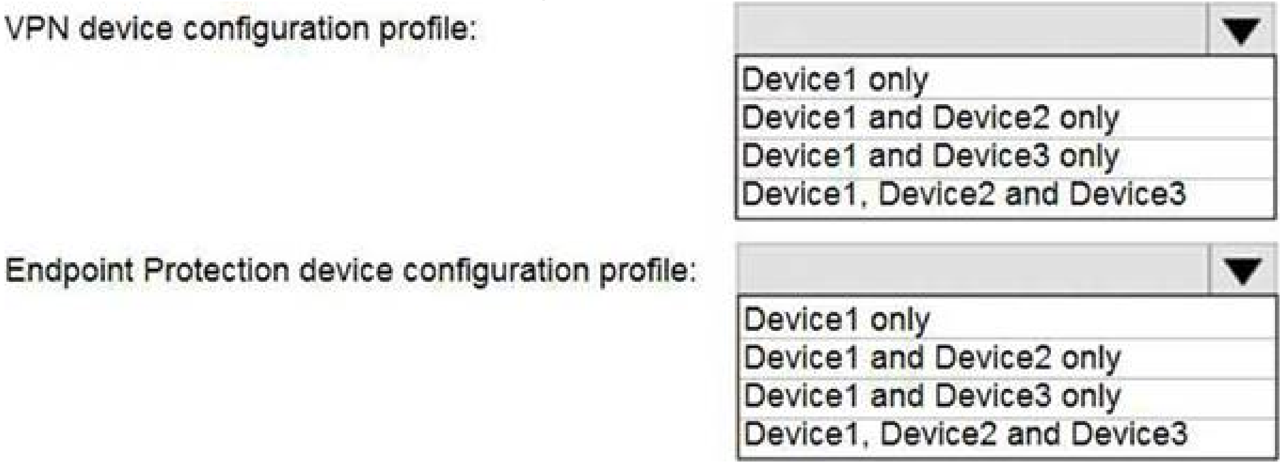
NEW QUESTION 211
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:
- Deploy a VPN connection by using a VPN device configuration profile.
- Configure security settings by using an Endpoint Protection device configuration profile. You support the management tasks.

What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



VPN device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:
- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos

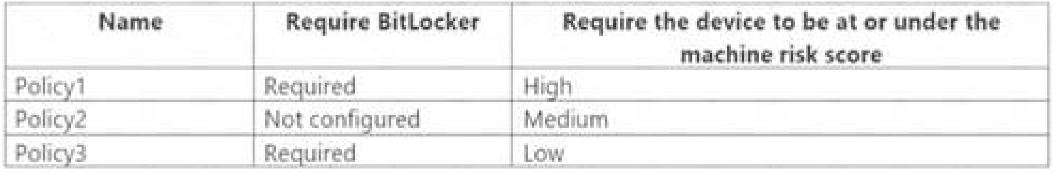
NEW QUESTION 214
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

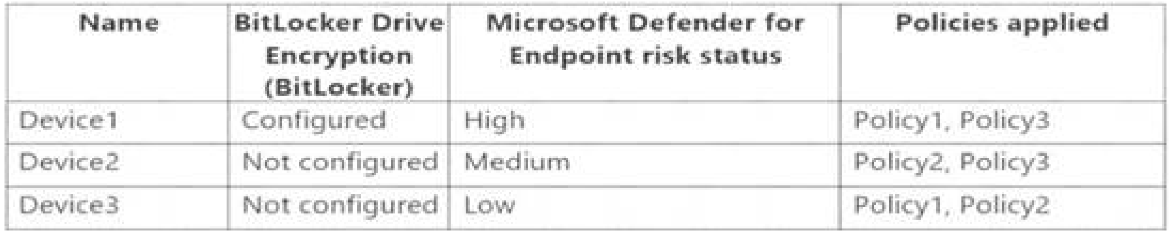
Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

NEW QUESTION 216
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains the compliance policies shown in the following table.



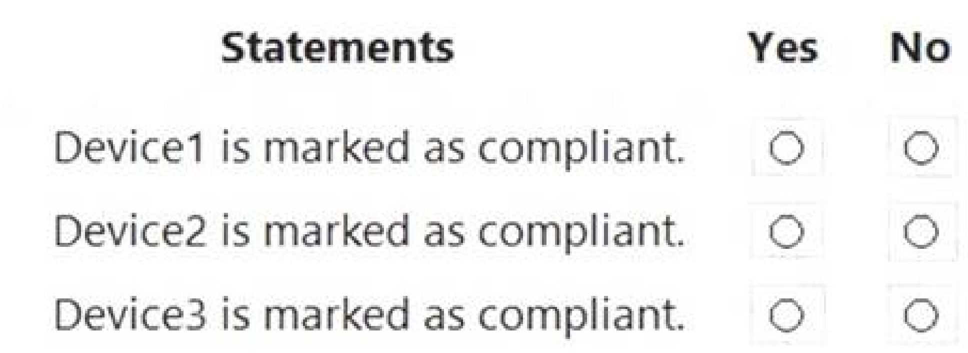
Name	Require BitLocker	Require the device to be at or under the machine risk score
Policy1	Required	High
Policy2	Not configured	Medium
Policy3	Required	Low

The tenant contains the devices shown in the following table.



Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Device1	Configured	High	Policy1, Policy3
Device2	Not configured	Medium	Policy2, Policy3
Device3	Not configured	Low	Policy1, Policy2

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



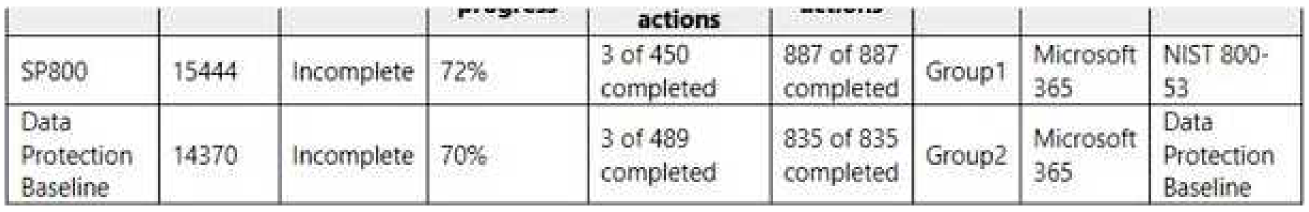
Statements	Yes	No
Device1 is marked as compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

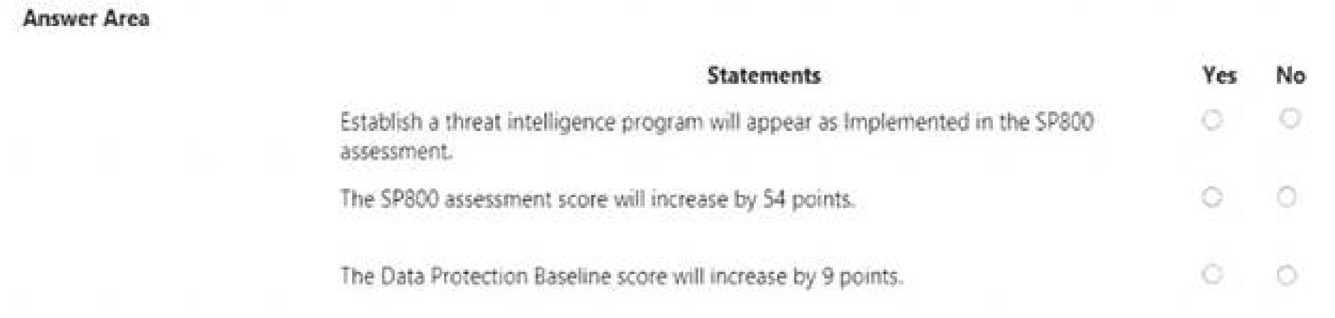
Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 220
- (Exam Topic 5)
HOTSPOT



			progress	actions	actions			
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.



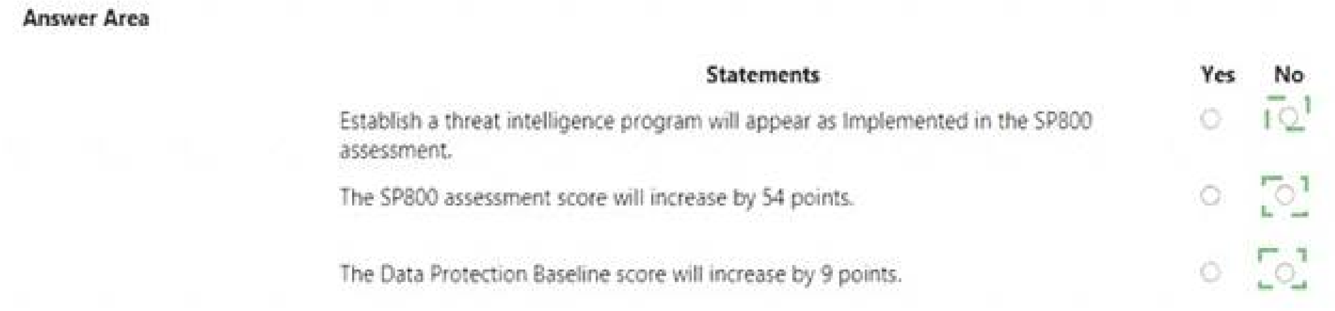
Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

A. Mastered
B. Not Mastered

Answer: A

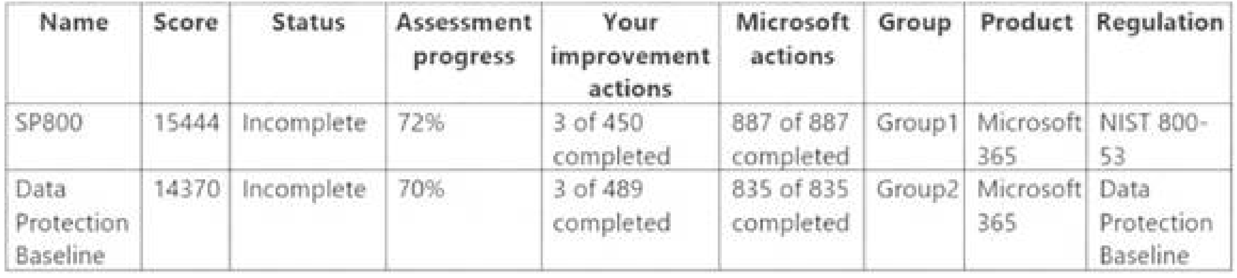
Explanation:



Answer Area

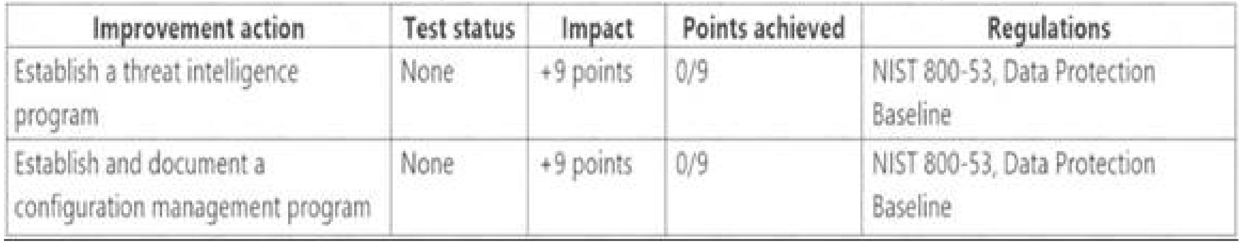
Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	[✓ ○]
The SP800 assessment score will increase by 54 points.	○	[✓ ○]
The Data Protection Baseline score will increase by 9 points.	○	[✓ ○]

NEW QUESTION 224
- (Exam Topic 5)
You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).
The tenant has two Compliance Manager assessments as shown in the following table.



Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.



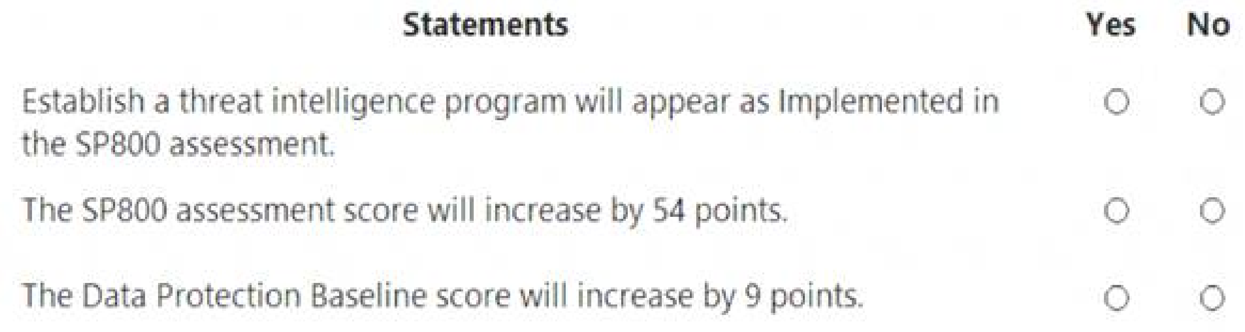
Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:
- For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence

program to Implemented.

- Enable multi-factor authentication (MFA) for all users.

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
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365-worl https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwid

NEW QUESTION 229
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune. What should you create?

A. scope tags
B. device configuration profiles
C. device categories
D. device compliance policies

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

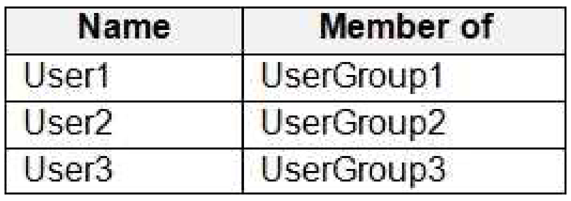
NEW QUESTION 232
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Service Administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B

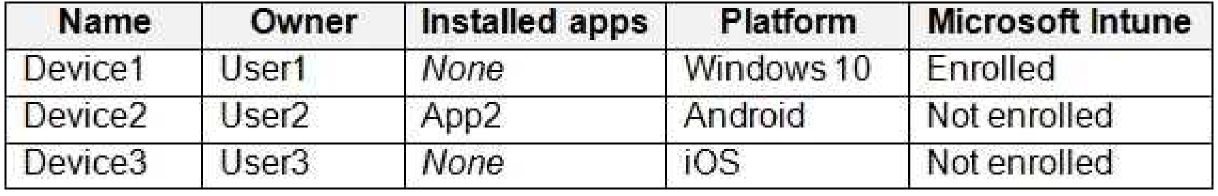
Explanation:
You need to assign the Security Administrator role. Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwi

NEW QUESTION 236
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



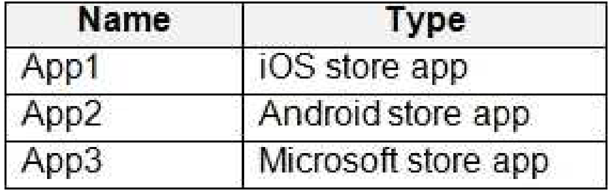
Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.



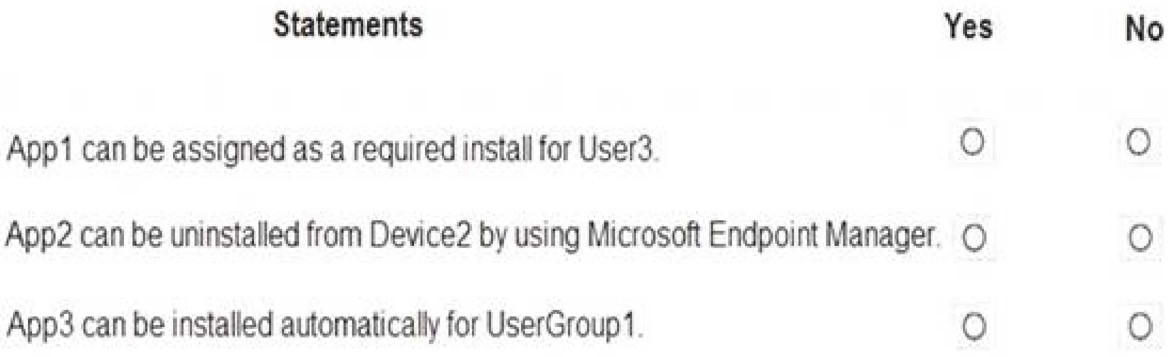
Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	*None*	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	*None*	iOS	Not enrolled

You have the apps shown in the following table.



Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.
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
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy

NEW QUESTION 239
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

A. Yes
B. No

Answer: A

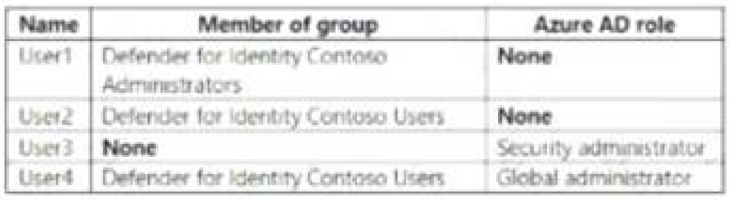
Explanation:
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628be

NEW QUESTION 242
- (Exam Topic 5)
You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft SharePoint Online site. What should you do?

A. From the SharePoint Online site, create an alert.
B. From the SharePoint Online admin center, modify the sharing settings.
C. From the Microsoft 365 Defender portal, create an alert policy.
D. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.

Answer: C

NEW QUESTION 246
- (Exam Topic 5)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.



Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User4 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 247
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft Purview policies to meet the following requirements:
Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII).
Report on shared documents that contain PII. What should you create?

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

Answer: A

Explanation:
Demonstrate data protection
Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.
There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.
In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

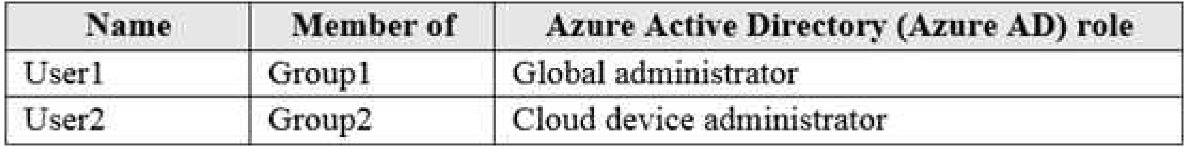
- From the Security & Compliance tab of your browser, click Home.
- Click Data loss prevention > Policy.
- Click + Create a policy.
- In Start with a template or create a custom policy, click Custom > Custom policy > Next.
- In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy

b. Description: Protect the personally identifiable information of European citizens

- Etc. Reference:

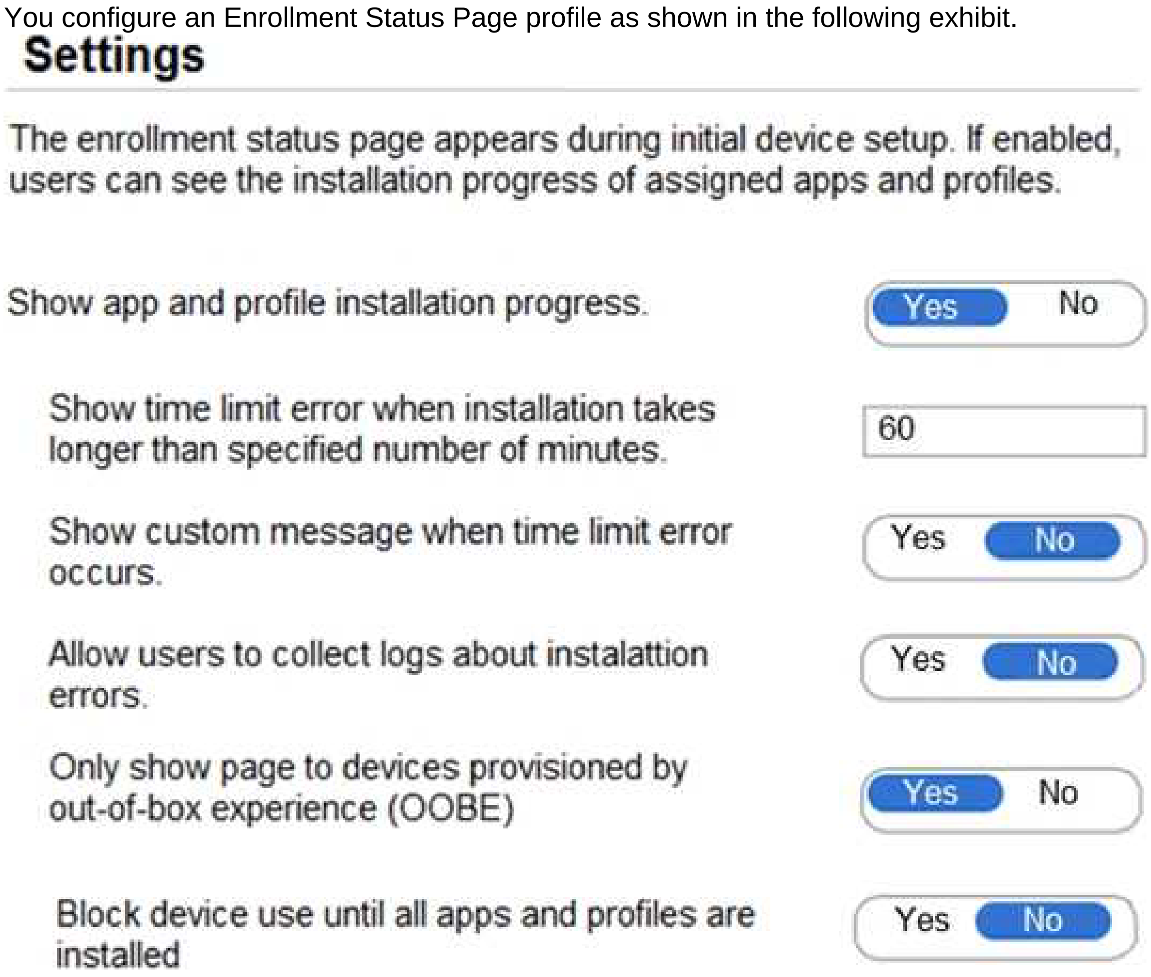
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-t

NEW QUESTION 251
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.



Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress. [✓ Yes] No

Show time limit error when installation takes longer than specified number of minutes. 60

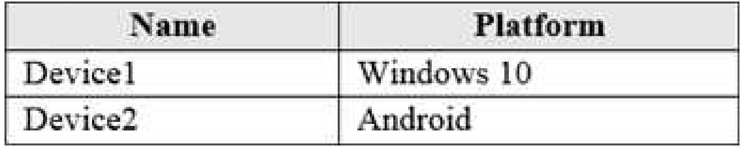
Show custom message when time limit error occurs. Yes [✓ No]

Allow users to collect logs about instalattion errors. Yes [✓ No]

Only show page to devices provisioned by out-of-box experience (OOBE) [✓ Yes] No

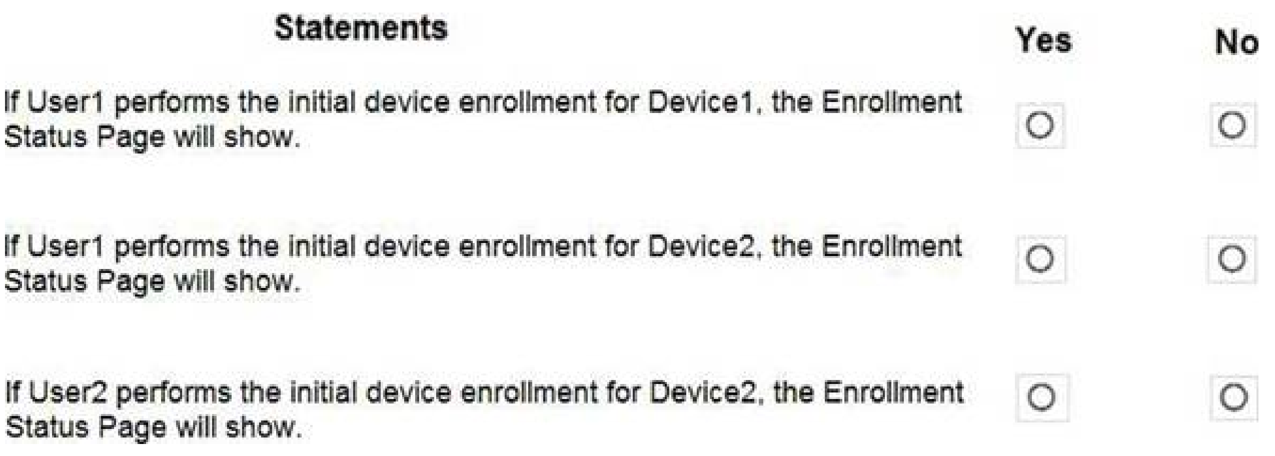
Block device use until all apps and profiles are installed Yes [✓ No]

You assign the policy to Group1.
You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

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



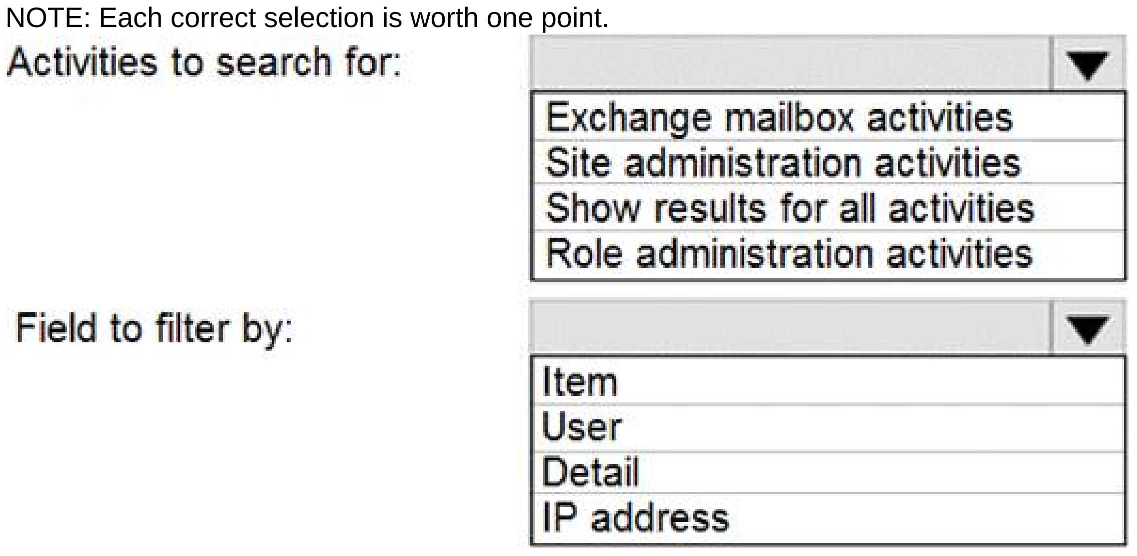
Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

NEW QUESTION 255
- (Exam Topic 5)
You have a Microsoft 365 subscription.
Your network uses an IP address space of 51.40.15.0/24.
An Exchange Online administrator recently created a role named Role1 from a computer on the network. You need to identify the name of the administrator by using an audit log search.
For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Activities to search for:

- Exchange mailbox activities
- Site administration activities
- Show results for all activities
- Role administration activities

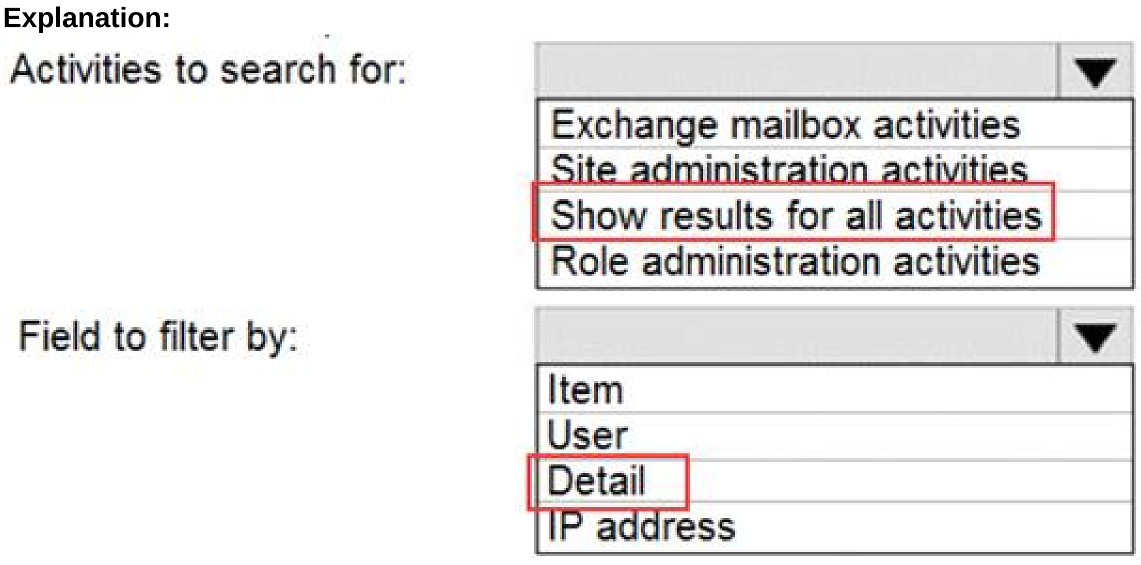
Field to filter by:

- Item
- User
- Detail
- IP address

A. Mastered
B. Not Mastered

Answer: A

Explanation:



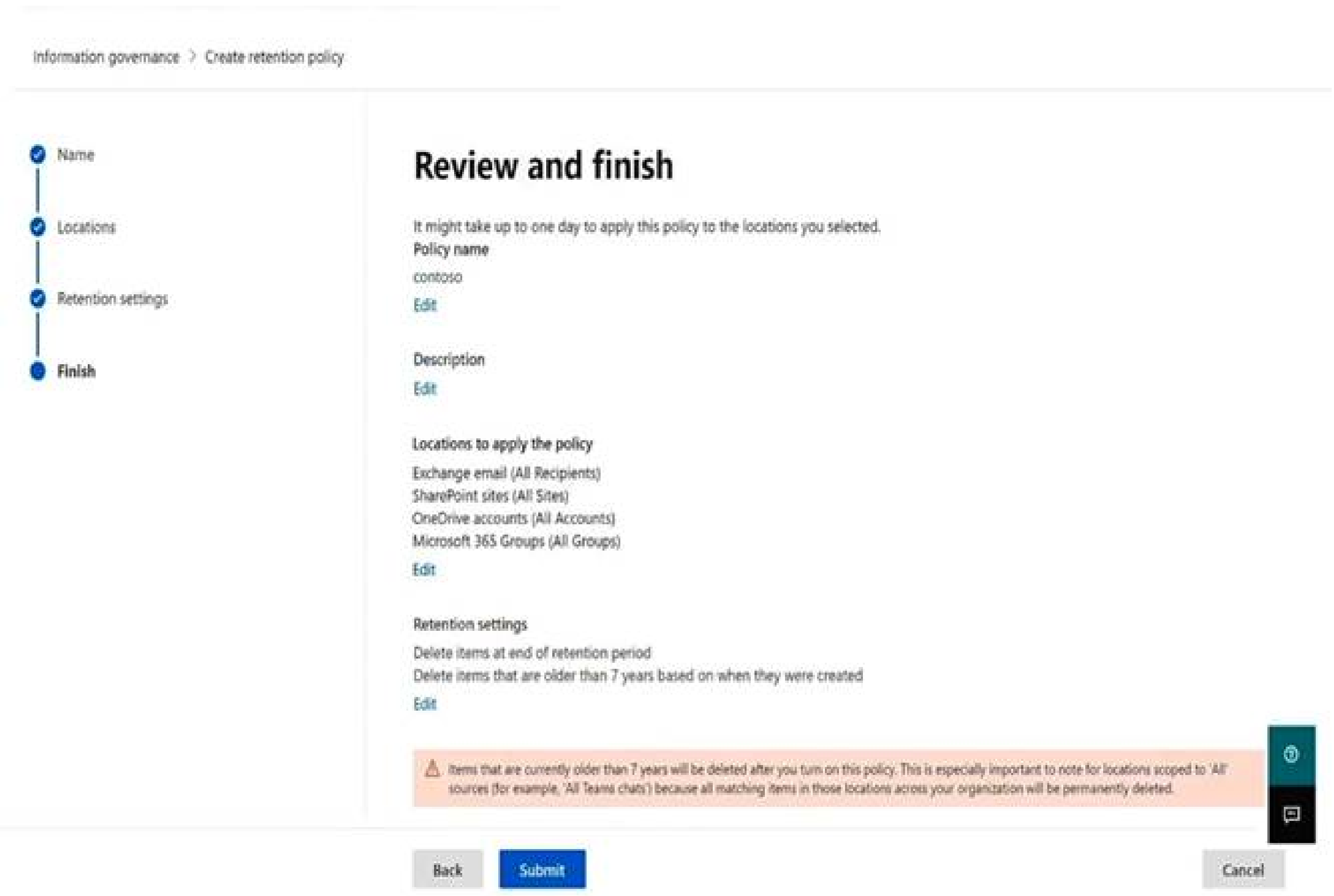
Activities to search for:

- Exchange mailbox activities
- Site administration activities
- [✓ Show results for all activities]
- Role administration activities

Field to filter by:

- Item
- User
- [✓ Detail]
- IP address

NEW QUESTION 258
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 tenant.
You plan to create a retention policy as shown in the following exhibit.



Information governance > Create retention policy

Review and finish

It might take up to one day to apply this policy to the locations you selected.

Policy name
contoso
Edit

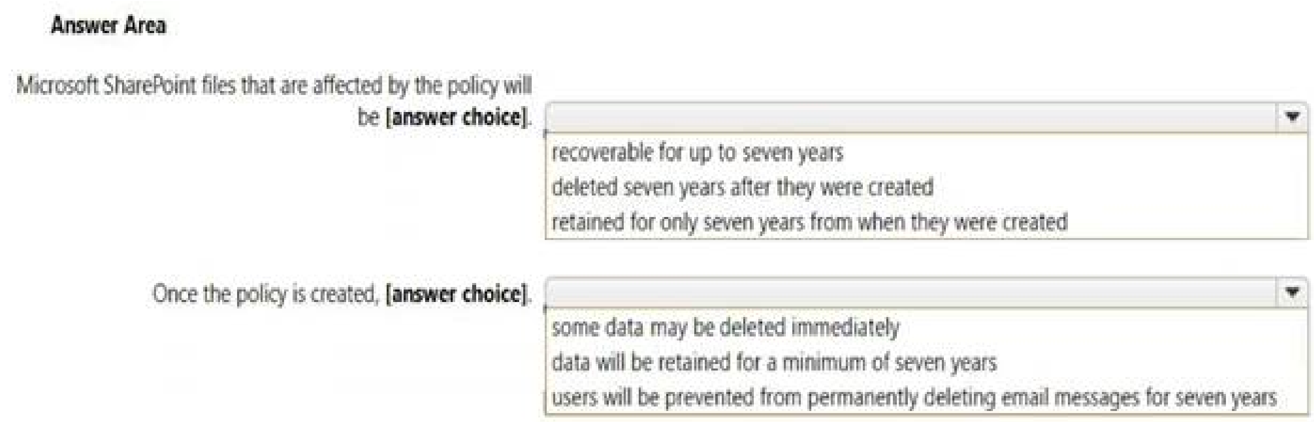
Description
Edit

Locations to apply the policy
Exchange email (All Recipients)
SharePoint sites (All Sites)
OneDrive accounts (All Accounts)
Microsoft 365 Groups (All Groups)
Edit

Retention settings
Delete items at end of retention period
Delete items that are older than 7 years based on when they were created
Edit

⚠ Items that are currently older than 7 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted.

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



Answer Area

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]**.

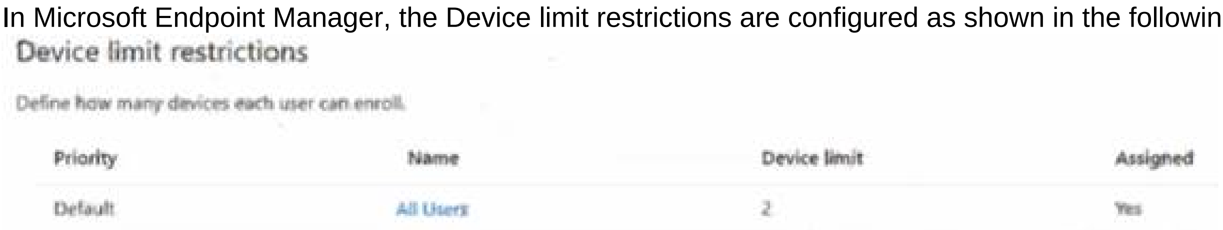
some data may be deleted immediately
data will be retained for a minimum of seven years
users will be prevented from permanently deleting email messages for seven years

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Deleted seven years after they were created. From the exhibit:
The retention policy applies to SharePoint sites.
Delete items that are older than 7 years based on when they were created. Box 2: data will retained for a minimum of seven years
The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.
Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).
For example, if all documents in a SharePoint site should be retained for 5 years, it's more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5 years and others retained for 10 years, a retention policy wouldn't be able to do this. When you need to specify retention settings at the item level, use retention labels.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION 263
- (Exam Topic 5)
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

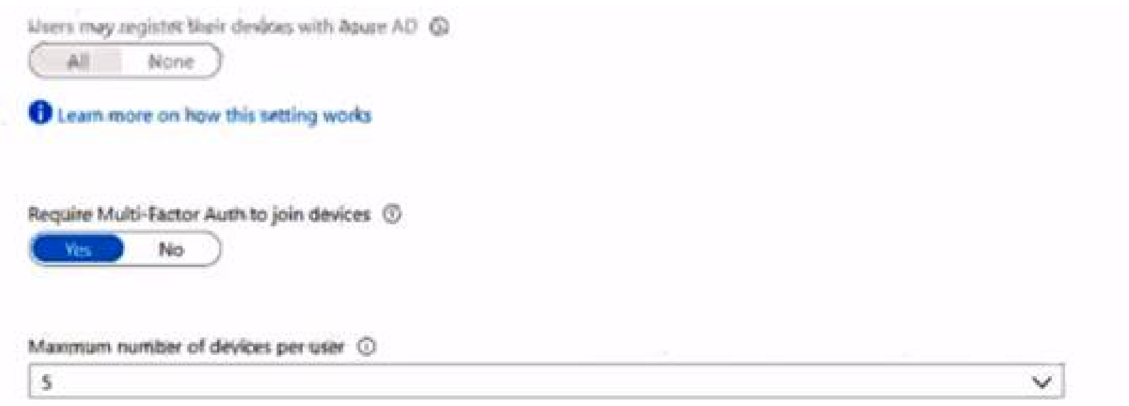


Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.



Users may register their devices with Azure AD ⓘ

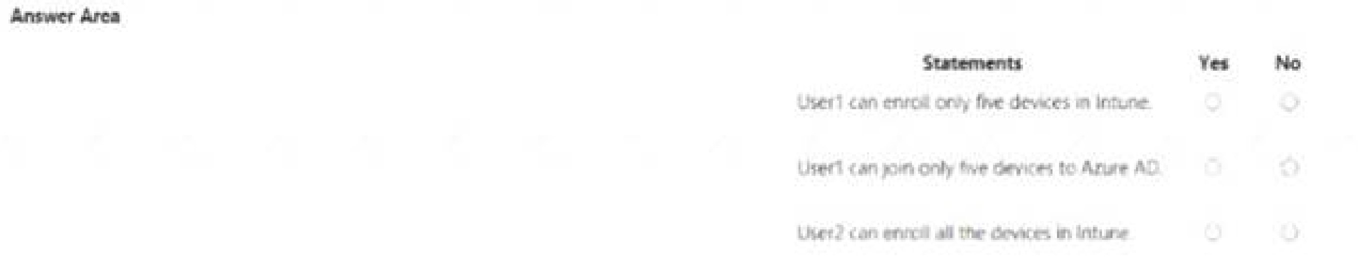
ⓘ Learn more on how this setting works

Require Multi-Factor Auth to join devices ⓘ

Maximum number of devices per user ⓘ

5

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM). For each of the following statement, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



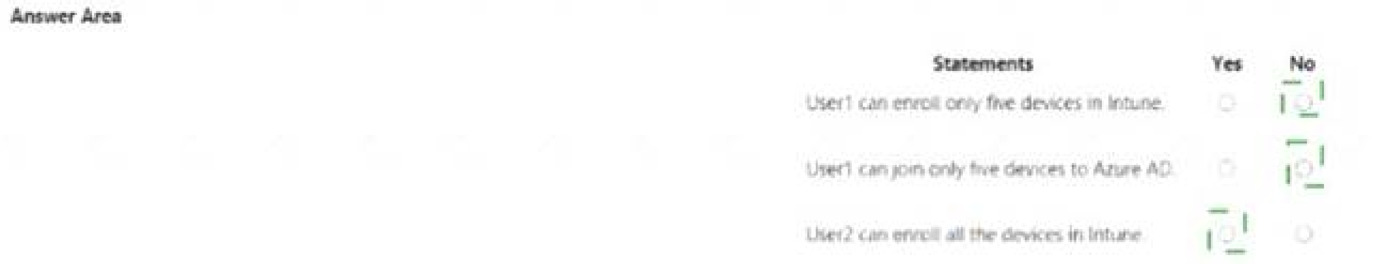
Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	○	○
User1 can join only five devices to Azure AD.	○	○
User2 can enroll all the devices in Intune	○	○

A. Mastered
B. Not Mastered

Answer: A

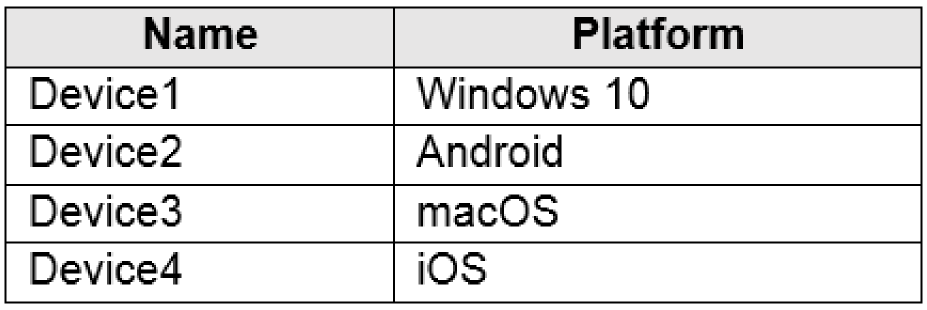
Explanation:



Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	○	[✓ ○]
User1 can join only five devices to Azure AD.	○	[✓ ○]
User2 can enroll all the devices in Intune	[✓ ○]	○

NEW QUESTION 267
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager. To which devices can you deploy Microsoft 365 Apps for enterprise?

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

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

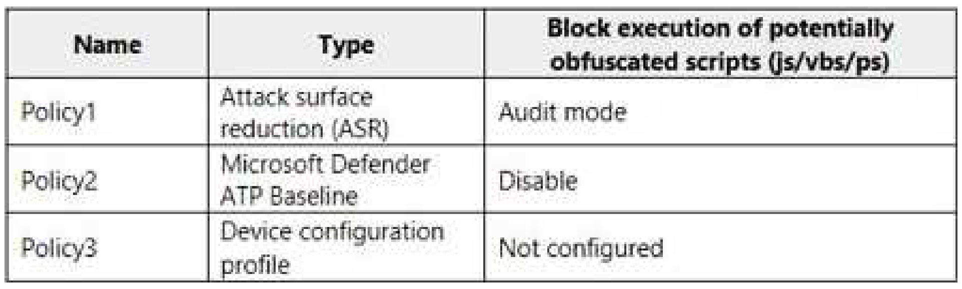
NEW QUESTION 271
- (Exam Topic 5)
You have an Azure AD tenant.
You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD. You purchase a Microsoft 365 E3 subscription.
You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.
What should you do?

A. From the Microsoft Endpoinf Manager admin center, create a Windows Autopilot deployment profile.Assign the profile to all the computer
B. Instruct users to restart their computer and perform a network restart.
C. Enroll the computers in Microsoft Intun
D. Create a configuration profile by using the Edition upgrade and mode switch templat
E. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer.
F. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online sit
G. Instruct users to run the provisioning package from SharePoint Online.

H. From the Azure Active Directory admin center, create a security group that has dynamic device membershi
I. Assign licenses to the group and instruct users to sign in to their computer.

Answer: B

NEW QUESTION 276
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

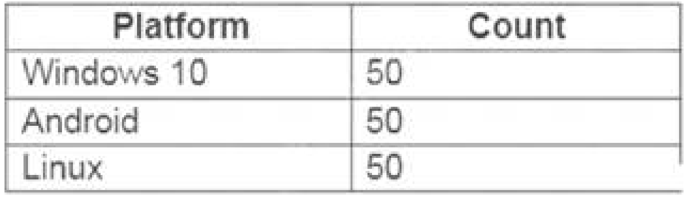


Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

A. only the settings of Policy1
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Answer: C

NEW QUESTION 277
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.



Platform	Count
Windows 10	50
Android	50
Linux	50

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

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

Answer: B

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

NEW QUESTION 281
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Endpoint Management admin center, you create a device configuration profile. Does this meet the goal?

A. Yes
B. No

Answer: B

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

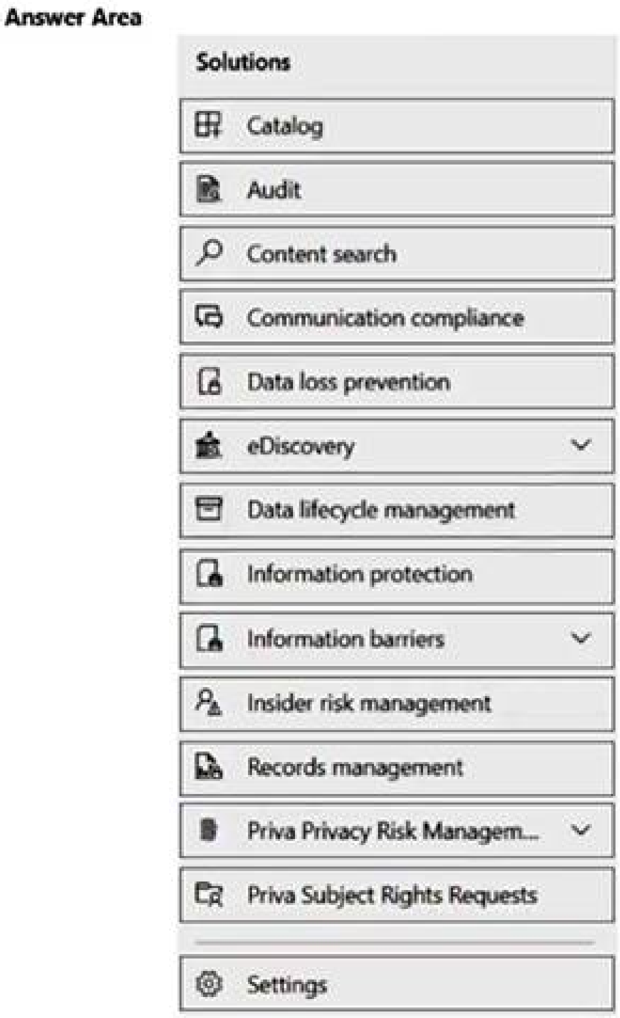
NEW QUESTION 282
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You need to create Conditional Access policies to meet the following requirements:
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must be blocked from signing in from outside the United States and Canada.
Only users in the R&D department must be blocked from signing in from both Android and iOS devices. Only users in the finance department must be able to sign in to an Azure AD enterprise application named
App1. All other users must be blocked from signing in to App1.
What is the minimum number of Conditional Access policies you should create?

A. 3
B. 4
C. 5
D. 6
E. 7
F. 8

Answer: B

Explanation:
* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.
One Policy.
* Only users in the R&D department must be blocked from signing in from both Android and iOS devices. One Policy.
* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network. One policy
* All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android One Policy
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

NEW QUESTION 286
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription. You need to meet the following requirements:
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Information protection
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection
All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is
select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.
To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels: In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information
Protection -> Microsoft Information Protection.
Note: Encryption of data at rest
Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.
BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology.

Box 2: Settings
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring

NEW QUESTION 288
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.
You need to export the existing template.
Which file format should you use for the exported template?

A. CSV
B. XLSX
C. JSON
D. XML

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldw

NEW QUESTION 290
- (Exam Topic 5) You have a Microsoft 365 E5 tenant. You configure sensitivity labels.
Users report that the Sensitivity button is unavailability in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.
You need to ensure that the users can apply the sensitivity labels when they use Word for the web. What should you do?

A. Copy policies from Azure information Protection to the Microsoft 365 Compliance center
B. Publish the sensitivity labels.
C. Create an auto-labeling policy
D. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.

Answer: B

NEW QUESTION 294
- (Exam Topic 5)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

A. Yes
B. No

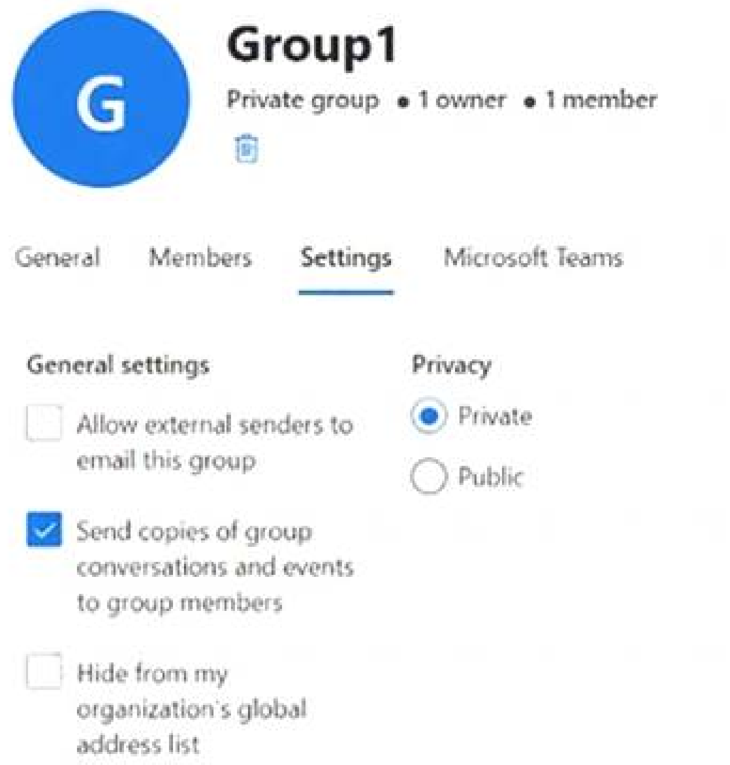
Answer: A

NEW QUESTION 297
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

A. From Policy in the Azure portal, select Compliance, and then assign a pokey
B. From Compliance Manager, create an assessment
C. From the Microsoft J6i compliance center, create an audit retention policy.
D. From the Microsoft 365 admin center enable the Productivity Score.

Answer: B

NEW QUESTION 302
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



Group1

Private group • 1 owner • 1 member

General settings

□ Allow external senders to email this group

☑ Send copies of group conversations and events to group members

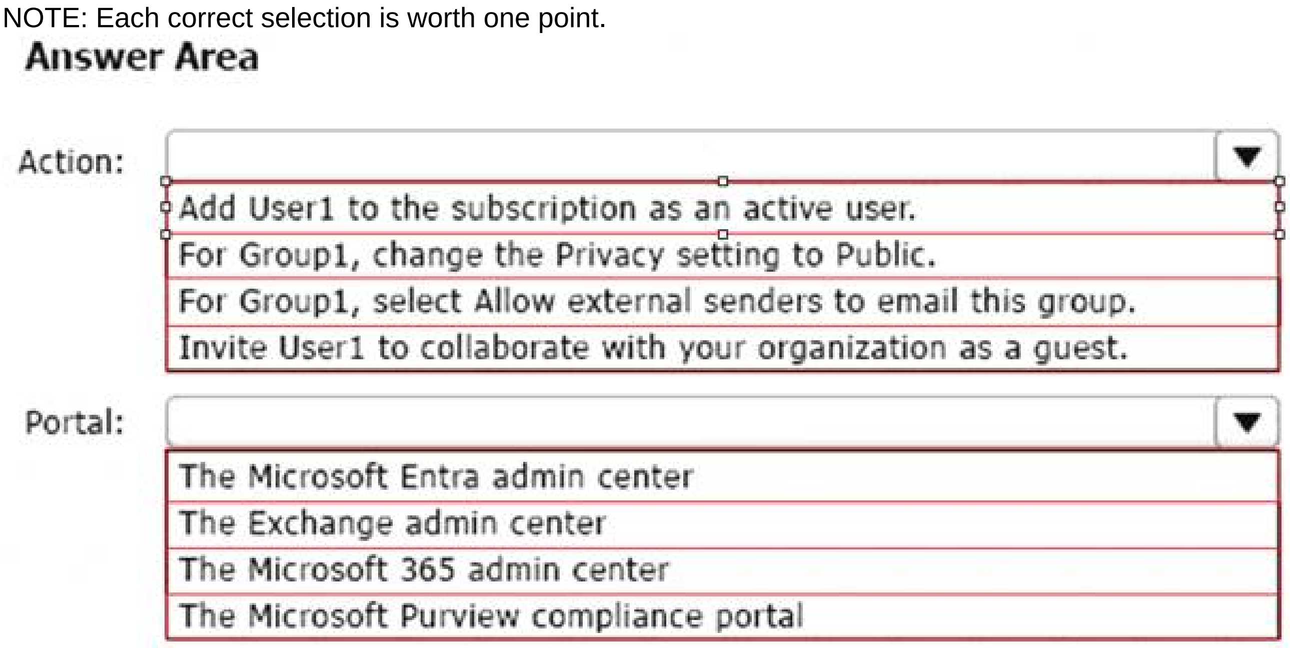
□ Hide from my organization's global address list

Privacy

● Private

○ Public

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



Answer Area

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

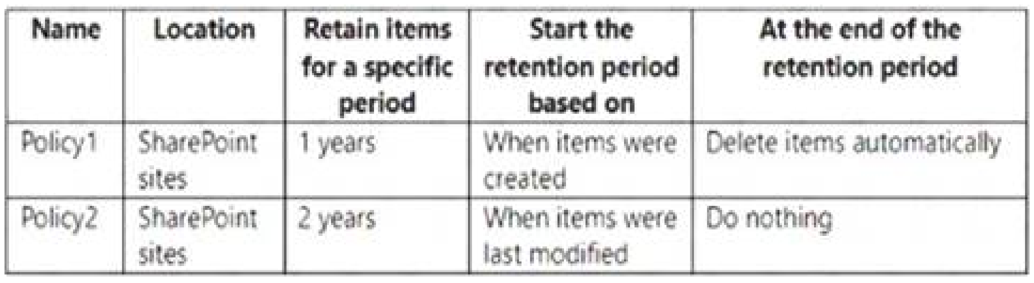
Portal:
- The Microsoft Entra admin center
- The Exchange admin center
- The Microsoft 365 admin center
- The Microsoft Purview compliance portal

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Invite User1 to collaborate with your organization as a guest.
To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps. Navigate with your Web browser to https://admin.microsoft.com.
On the left pane, click on “Users”, then click “Guest Users”.
On the “Guest Users” page, to create a new guest user, click on either the “Add a guest user” link on the top of the page or click on “Go to Azure Active Directory to add guest users” link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.com.
On the “New user” page in the Microsoft Azure portal, you must choose to either “Create user” or “Invite user”. If you choose the “Create user” option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the “Invite user” option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the “Invite user” option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Azure AD with family of identity and access products
Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.
Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).
Reference:
https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-ac

NEW QUESTION 305
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You have the retention policies shown in the following table.



Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

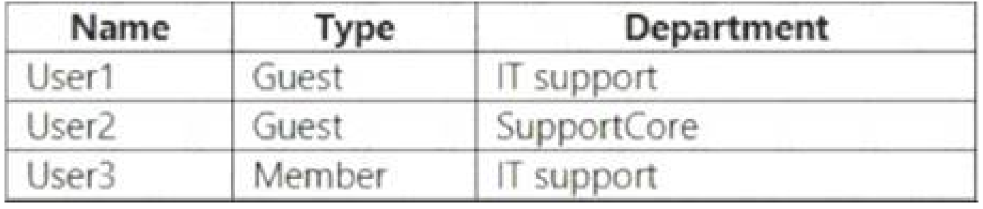
Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx. File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.
When will File1.docx be deleted automatically?

A. January 1,2023
B. January 1,2024
C. January 31, 2023
D. January 31, 2024
E. never

Answer: D

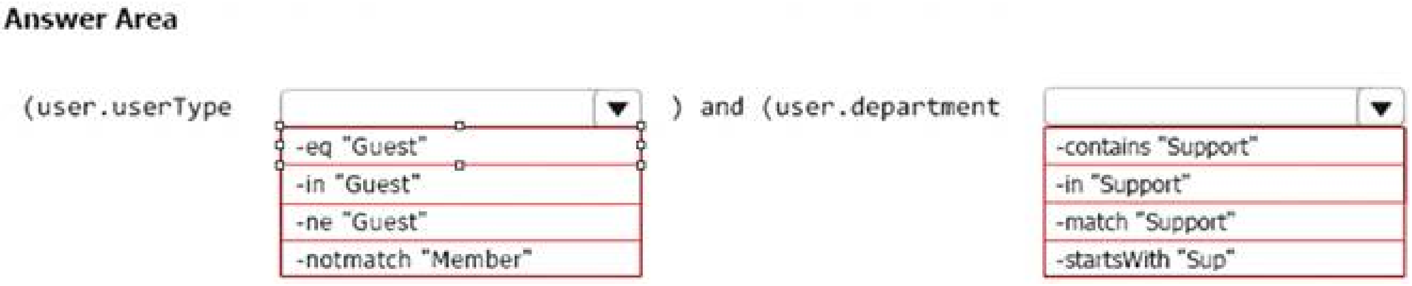
Explanation:
for the four different principles:
* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
* 2. Etc. Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

NEW QUESTION 308
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

(user.userType [▼]) and (user.department [▼]

-eq "Guest"
-in "Guest"
-ne "Guest"
-notmatch "Member"

-contains "Support"
-in "Support"
-match "Support"
-startsWith "Sup"

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: -eq "Guest"
Dynamic membership rules for groups in Azure Active Directory Supported expression operators
The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.
* Equals
-eq
* Contains
-contains
* Etc.
Box 2: -contains "Support" Incorrect:
* -in
If you want to compare the value of a user attribute against multiple values, you can use the -in or -notIn operators.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

NEW QUESTION 312
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy. You need to prevent the users from bypassing the DLP policy.
What should you configure?

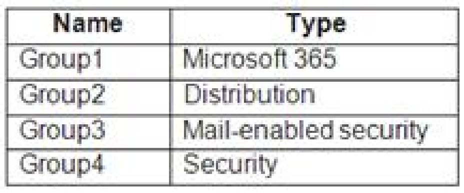
A. actions

B. incident reports
C. exceptions
D. user overrides

Answer: D

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

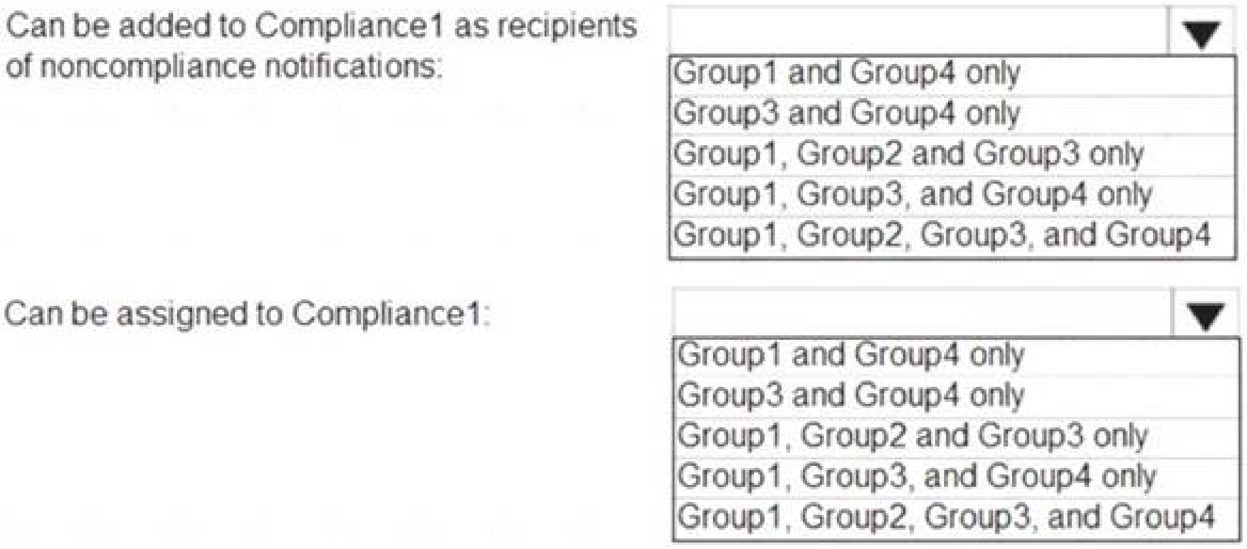
NEW QUESTION 316
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains the groups shown in the following table.



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

You plan to create a compliance policy named Compliance1.
You need to identify the groups that meet the following requirements:
- Can be added to Compliance1 as recipients of noncompliance notifications
- Can be assigned to Compliance1

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



Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

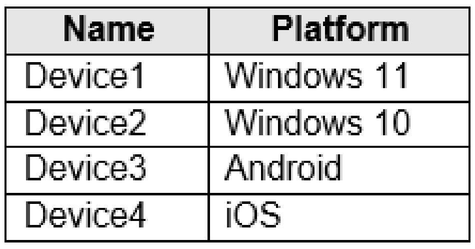
- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

A. Mastered
B. Not Mastered

Answer: A

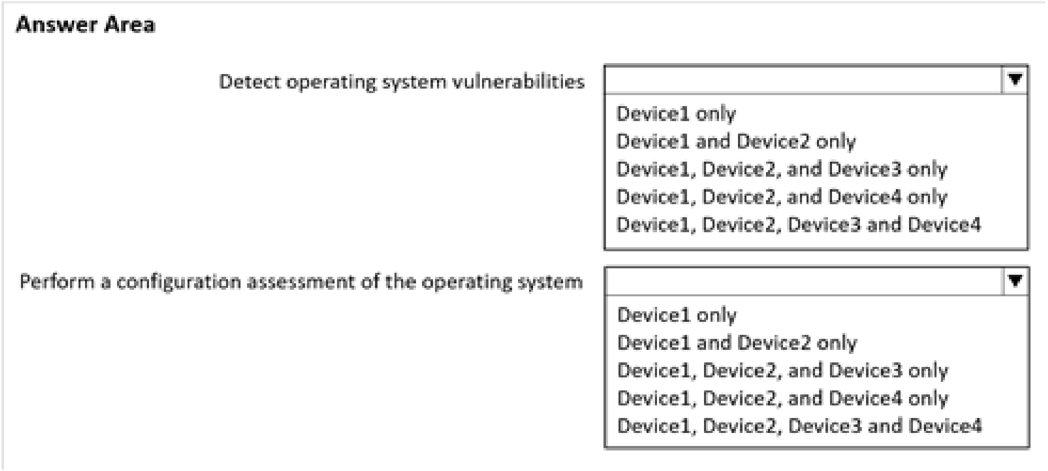
Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated
Reference:
https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manage

NEW QUESTION 321
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.



Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

All the devices are onboarded To Microsoft Defender for Endpoint
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:
• Detect operating system vulnerabilities.



Answer Area

Detect operating system vulnerabilities

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

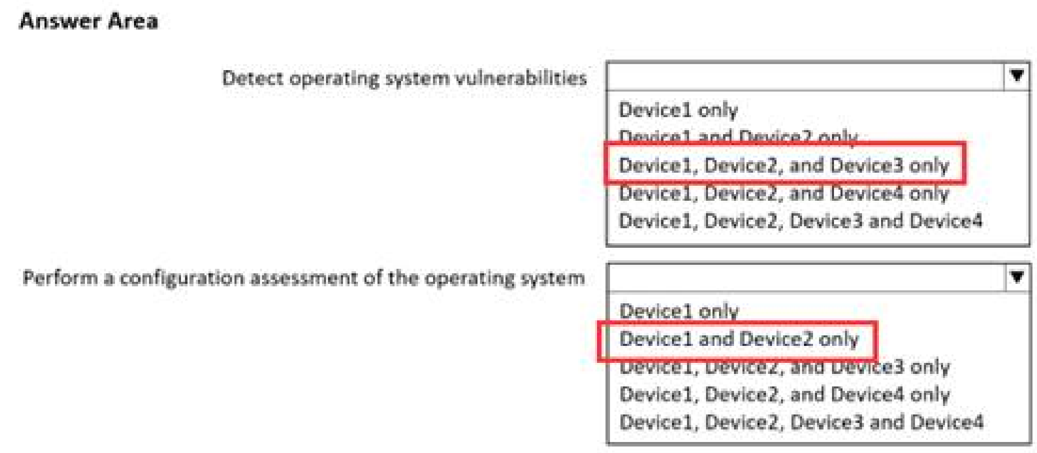
Perform a configuration assessment of the operating system

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Detect operating system vulnerabilities

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

Perform a configuration assessment of the operating system

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

NEW QUESTION 325
- (Exam Topic 5)
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

A. Android
B. CentOS Linux
C. iOS
D. Window 10

Answer: D

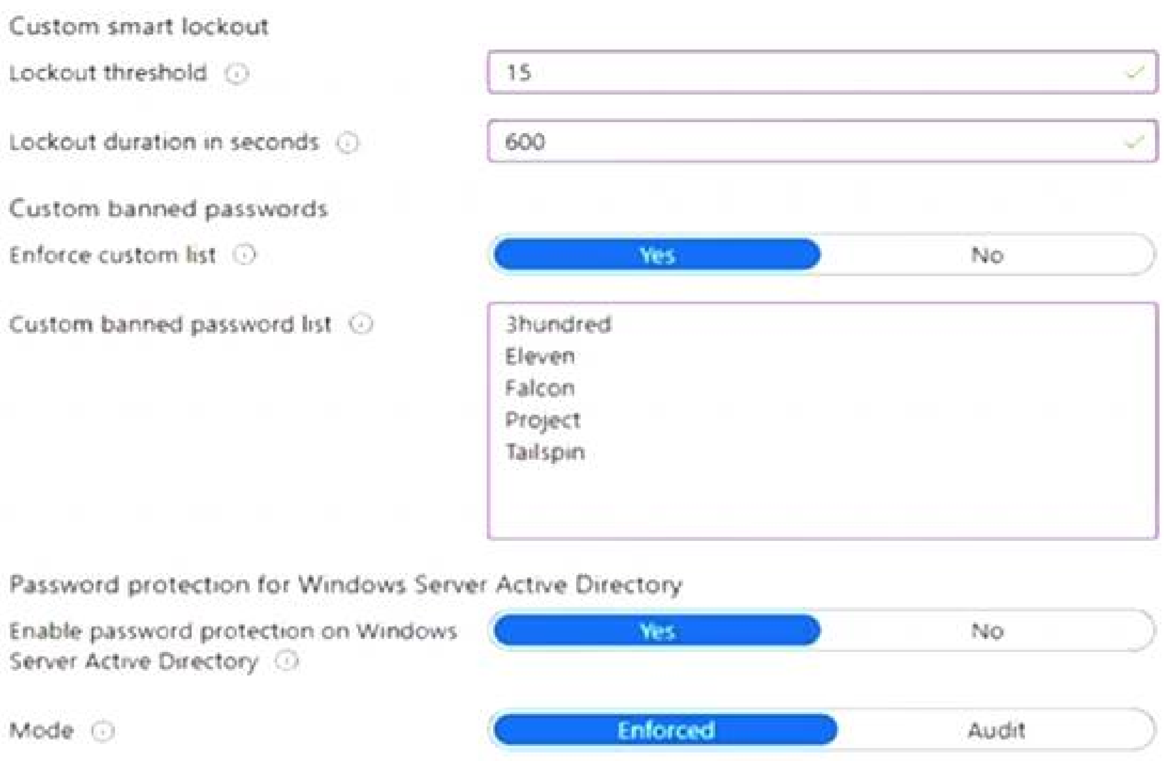
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

NEW QUESTION 326
- (Exam Topic 5)
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 domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings. You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 331
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a user named User1. Azure AD Password Protection is configured as shown in the following exhibit.



Custom smart lockout

Lockout threshold: 15

Lockout duration in seconds: 600

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:
3hundred
Eleven
Falcon
Project
Tailspin

Password protection for Windows Server Active Directory

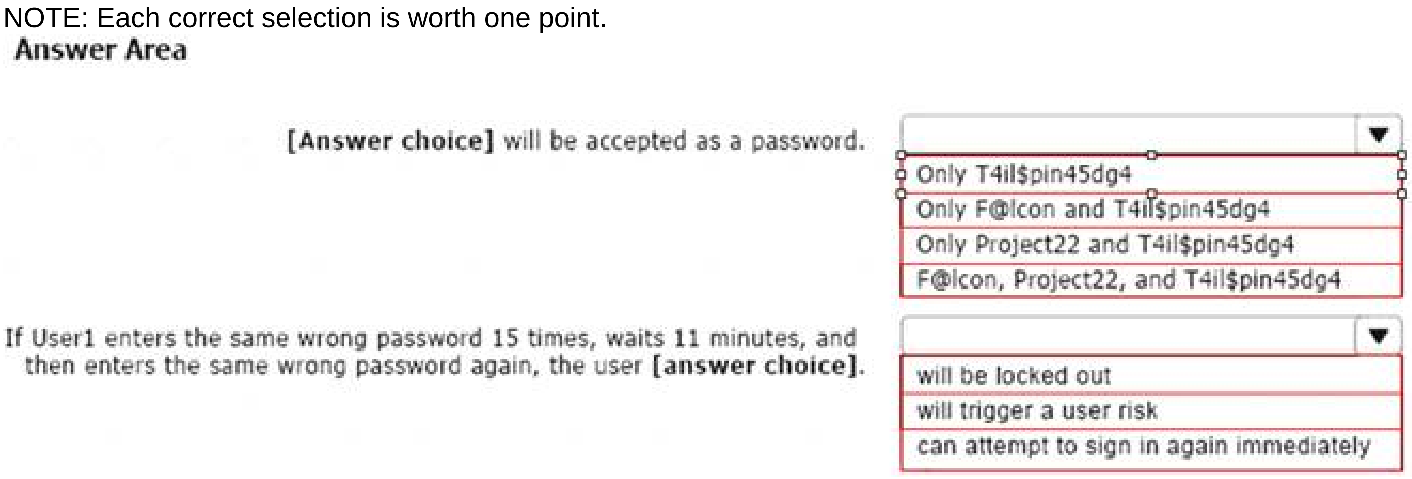
Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: [✓ Enforced] Audit

User1 attempts to update their password to the following passwords:

- F@lcon
- Project22
- T4il$pin45dg4

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



Answer Area

[Answer choice] will be accepted as a password.

- Only T4il$pin45dg4
- Only F@lcon and T4il$pin45dg4
- Only Project22 and T4il$pin45dg4
- F@lcon, Project22, and T4il$pin45dg4

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

- will be locked out
- will trigger a user risk
- can attempt to sign in again immediately

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Only T4il$pin45dg4
Box 2: can attempt to sign in immediately Note: Manage Azure AD smart lockout values
Based on your organizational requirements, you can customize the Azure AD smart lockout values. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.
To check or modify the smart lockout values for your organization, complete the following steps:

- Sign in to the Entra portal.
- Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.
- Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.
- The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.
- Set the Lockout duration in seconds, to the length in seconds of each lockout.
- The default is 60 seconds (one minute).

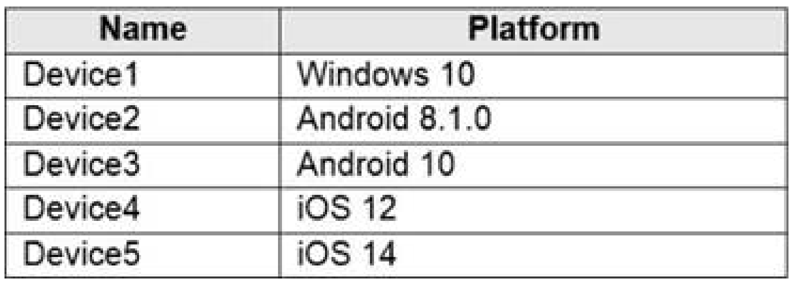
If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

NEW QUESTION 332
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to be notified when a single user downloads more than 50 files during any 60-second period. What should you configure?

A. a session policy
B. a file policy
C. an activity policy
D. an anomaly detection policy

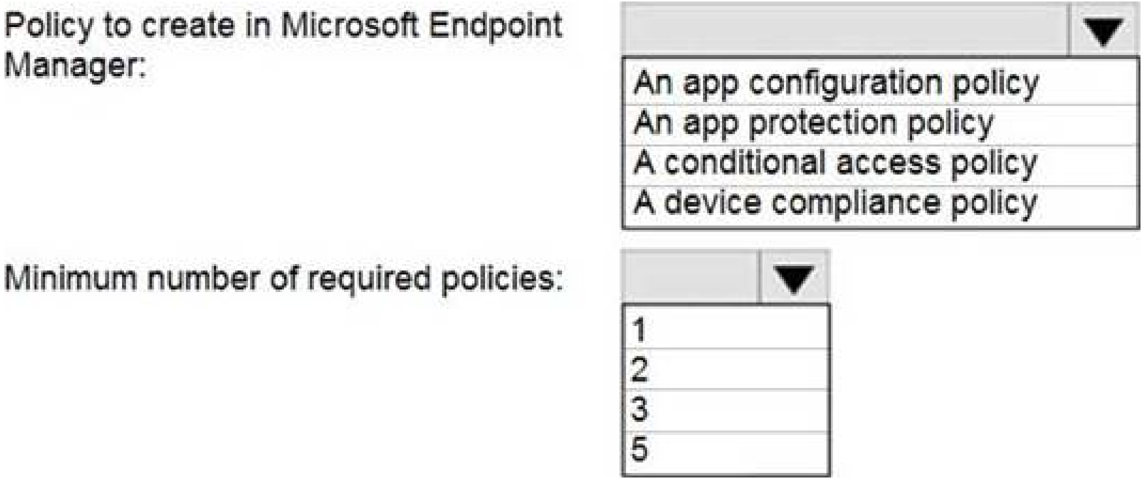
Answer: D

NEW QUESTION 333
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Policy to create in Microsoft Endpoint Manager:

- An app configuration policy
- An app protection policy
- A conditional access policy
- A device compliance policy

Minimum number of required policies:

- 1
- 2
- 3
- 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application, table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

NEW QUESTION 336
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a data loss prevention (DLP) policy
B. a sensitivity label policy
C. a Microsoft Cloud App Security file policy
D. a communication compliance policy
E. a retention label policy

Answer: AD

NEW QUESTION 338
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.
Company policy requires that the devices have the following configurations:

- Require complex passwords.
- Require the encryption of removable data storage devices.
- Have Microsoft Defender Antivirus real-time protection enabled.

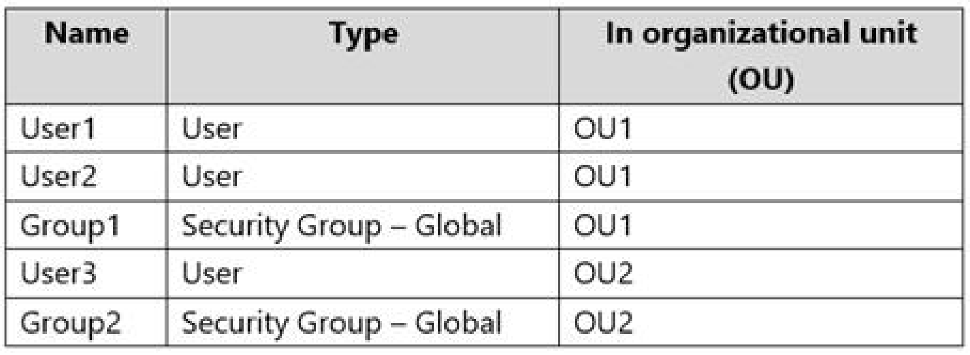
You need to configure the devices to meet the requirements. What should you use?

A. an app configuration policy
B. a compliance policyC a security baseline profile D a conditional access policy

Answer: B

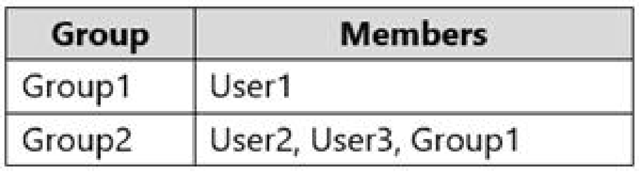
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

NEW QUESTION 340
- (Exam Topic 5)
HOTSPOT
Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.



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

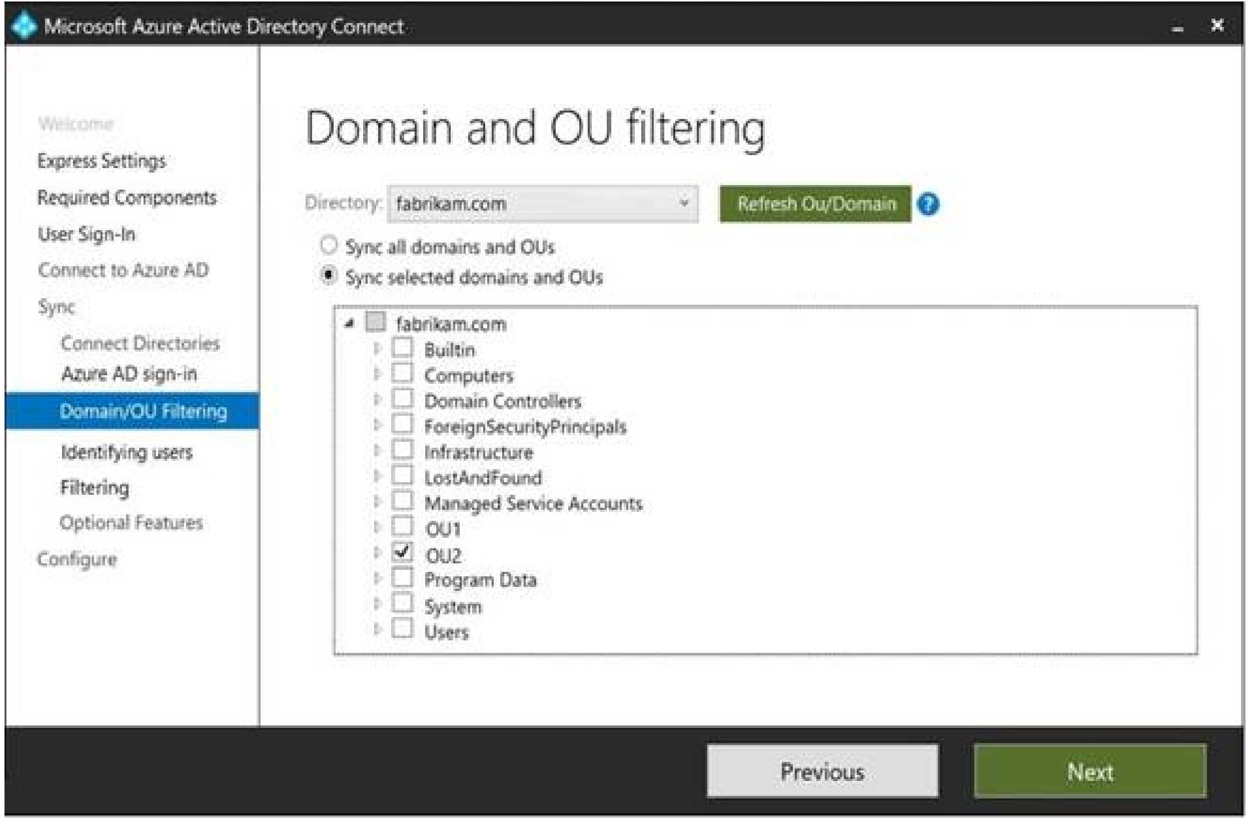
The groups have the members shown in the following table.



Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.

You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



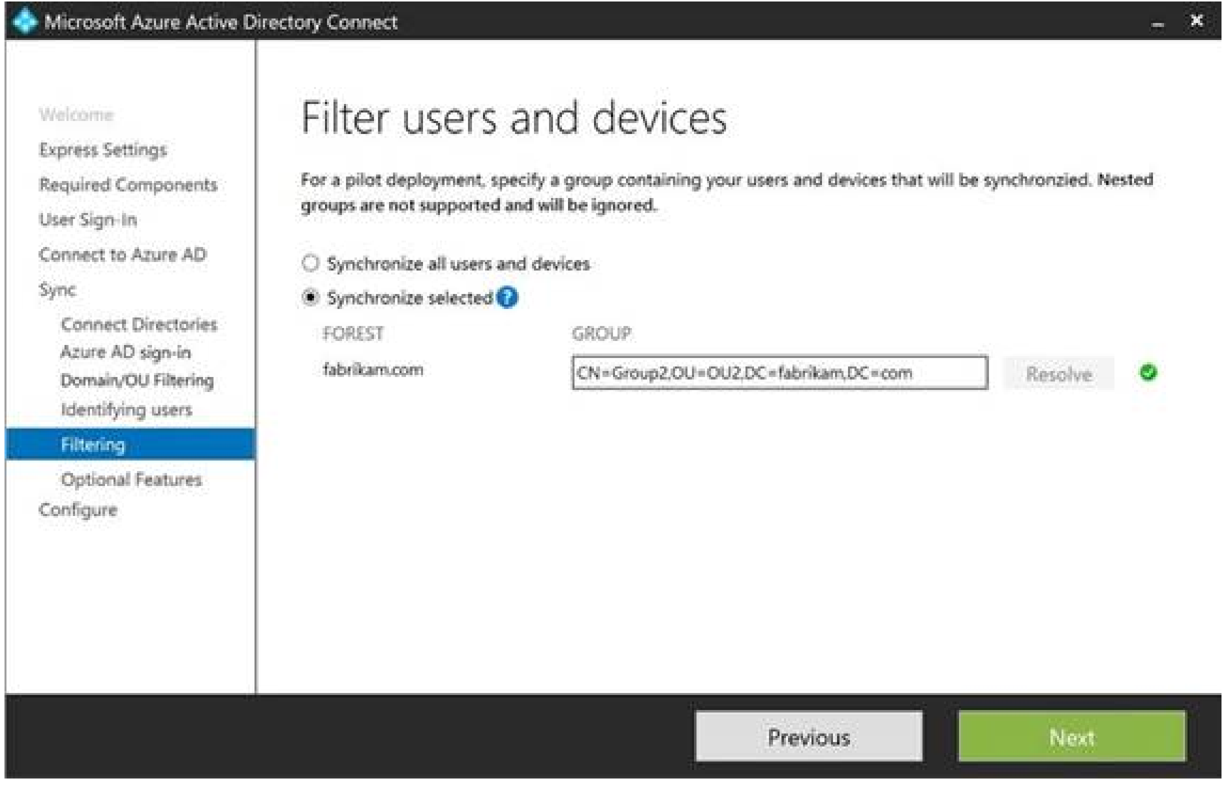
Domain and OU filtering

Directory: fabrikam.com

○ Sync all domains and OUs
● Sync selected domains and OUs

- □ fabrikam.com
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Infrastructure
  - □ LostAndFound
  - □ Managed Service Accounts
  - □ OU1
  - ☑ OU2
  - □ Program Data
  - □ System
  - □ Users

You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



Filter users and devices

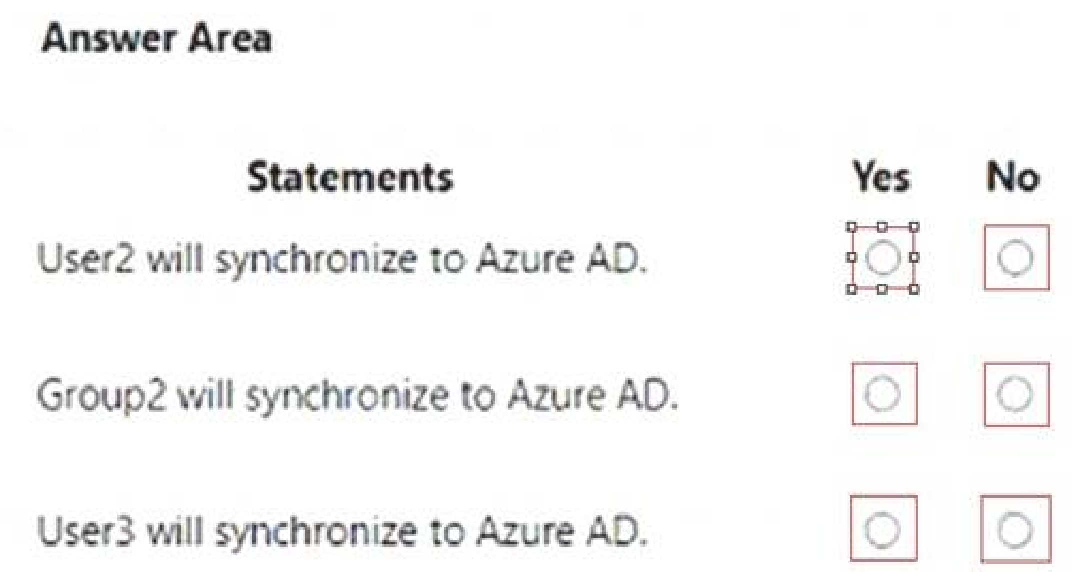
For a pilot deployment, specify a group containing your users and devices that will be synchronzied. Nested groups are not supported and will be ignored.

○ Synchronize all users and devices
● Synchronize selected

FOREST	GROUP
fabrikam.com	CN=Group2,OU=OU2,DC=fabrikam,DC=com

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

NOTE: Each correct selection is worth one point.



Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.
User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD. Box 2: Yes
Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.
Box 3: Yes
User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#group-b

NEW QUESTION 344
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You discover that some external users accessed center for a Microsoft SharePoint site. You modify the sharePoint sharing policy to prevent sharing, outside your organization.
You need to be notified if the SharePoint sharing policy is modified in the future.
Solution: From the Security $ Compliance admin center you create a threat management policy. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 349
- (Exam Topic 5)
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?

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

Answer: D

Explanation:
Use the Microsoft 365 Defender portal to create Safe Links policies
In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies
& Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use https://security.microsoft.com/safelinksv2.
* 1. On the Safe Links page, select Create to start the new Safe Links policy wizard.
* 2. On the Name your policy page, configure the following settings: Name: Enter a unique, descriptive name for the policy. Description: Enter an optional description for the policy.
* 3. When you're finished on the Name your policy page, select Next.
* 4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):
Users: The specified mailboxes, mail users, or mail contacts.
*-> Groups:
Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).
The specified Microsoft 365 Groups.
Domains: All recipients in the specified accepted domains in your organization. Etc.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure

NEW QUESTION 354
- (Exam Topic 5)

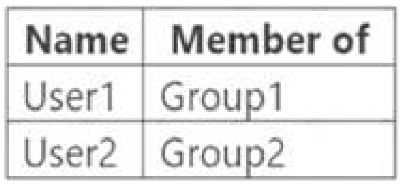
You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

A. Microsoft Store for Business
B. Apple Business Manager
C. Apple iTunes Store
D. Apple Configurator

Answer: B

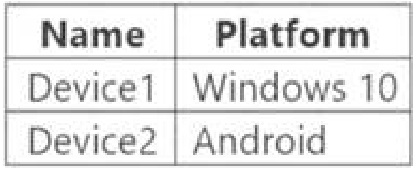
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

NEW QUESTION 359
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group2

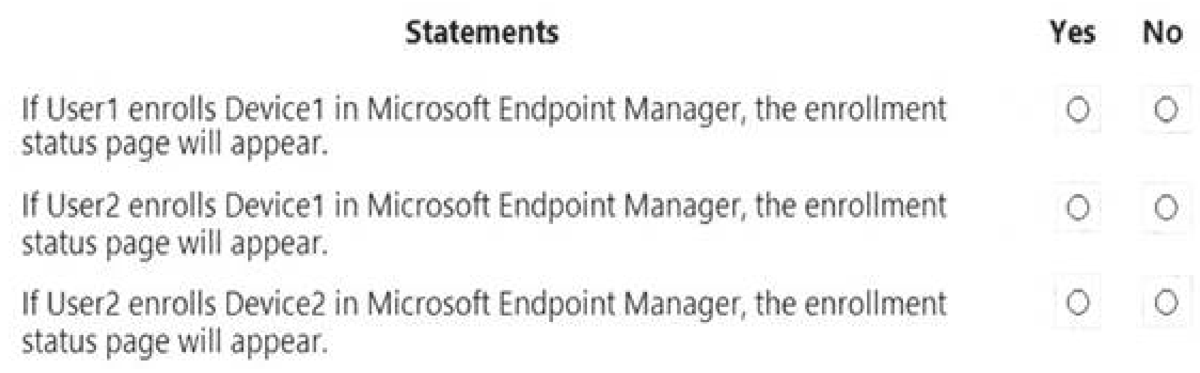
You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:
> Show app and profile configuration progress: Yes
> Allow users to collect logs about installation errors: Yes
> Assignments: Group2

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



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

NEW QUESTION 363
......