MS-102Q&As

Microsoft 365 Certified: Enterprise Administrator Expert

Pass Microsoft MS-102 Exam with 100% Guarantee

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

https://www.pass2lead.com/ms-102.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

Correct Answer: B

QUESTION 2

HOTSPOT

You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

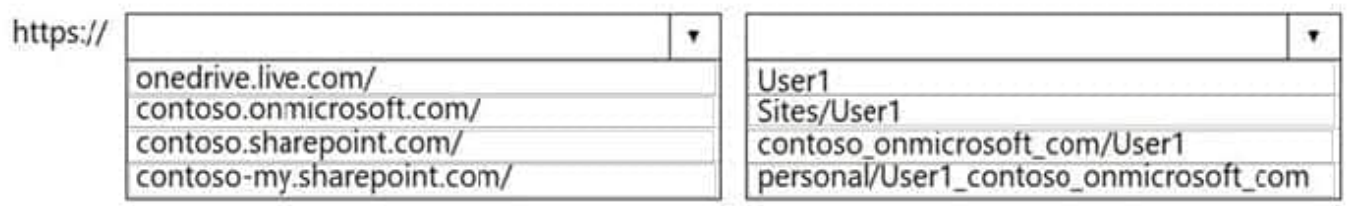
A user named User1 stores documents in Microsoft OneDrive.

You need to place the contents of User1\\'s OneDrive account on an eDiscovery hold.

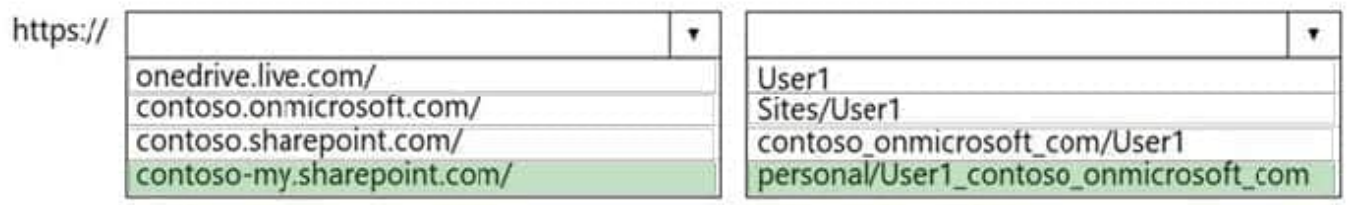
Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



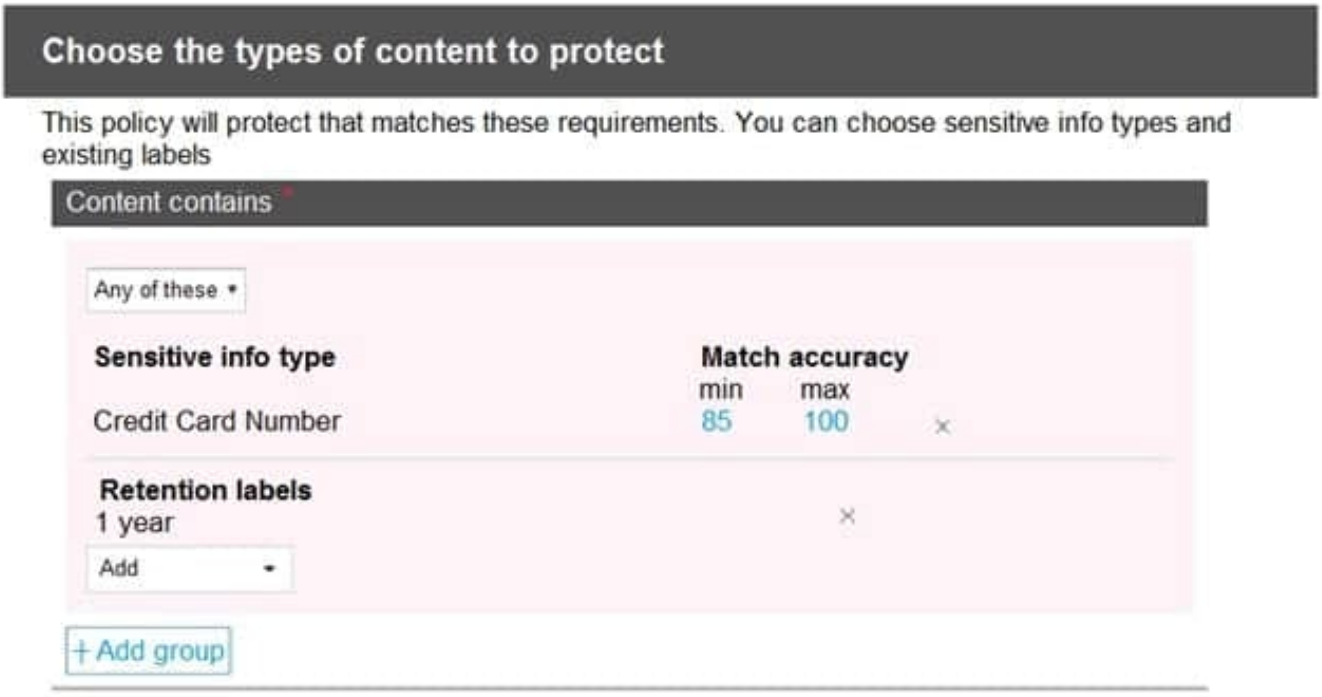
Correct Answer:



QUESTION 3

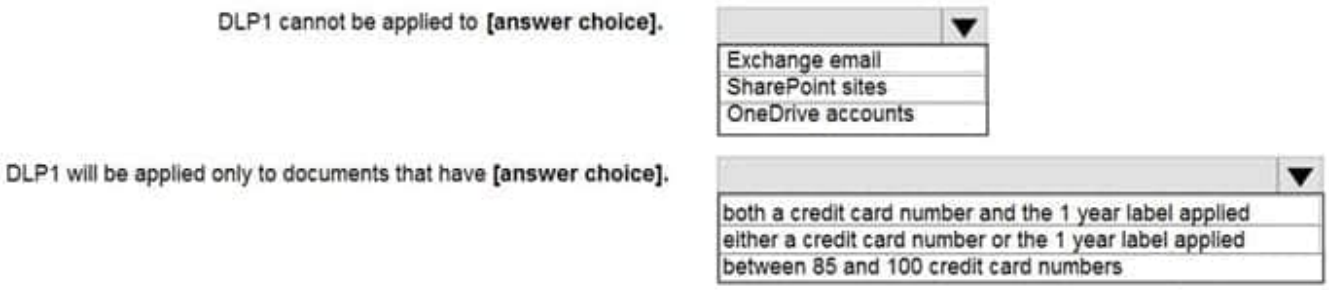
HOTSPOT

You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

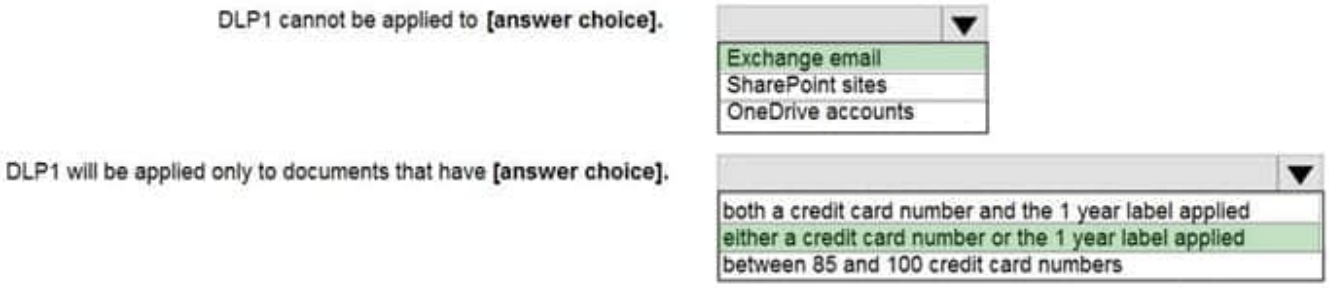


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 4

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 365 admin center, you assign SecAdmin1 the Exchange Administrator role.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

You need to assign the Security Administrator role. Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp

QUESTION 5

DRAG DROP

Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

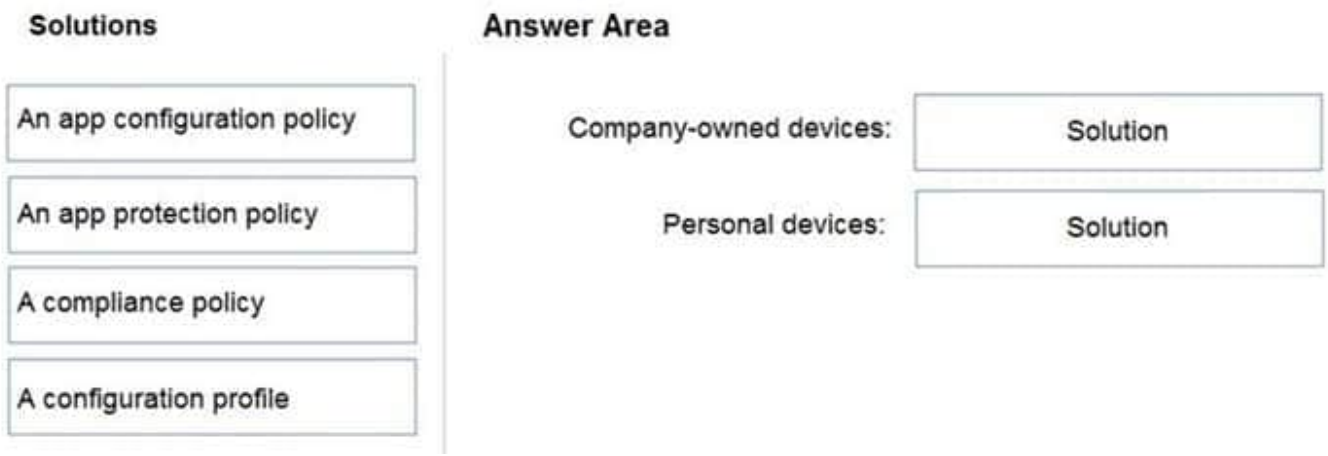
You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between

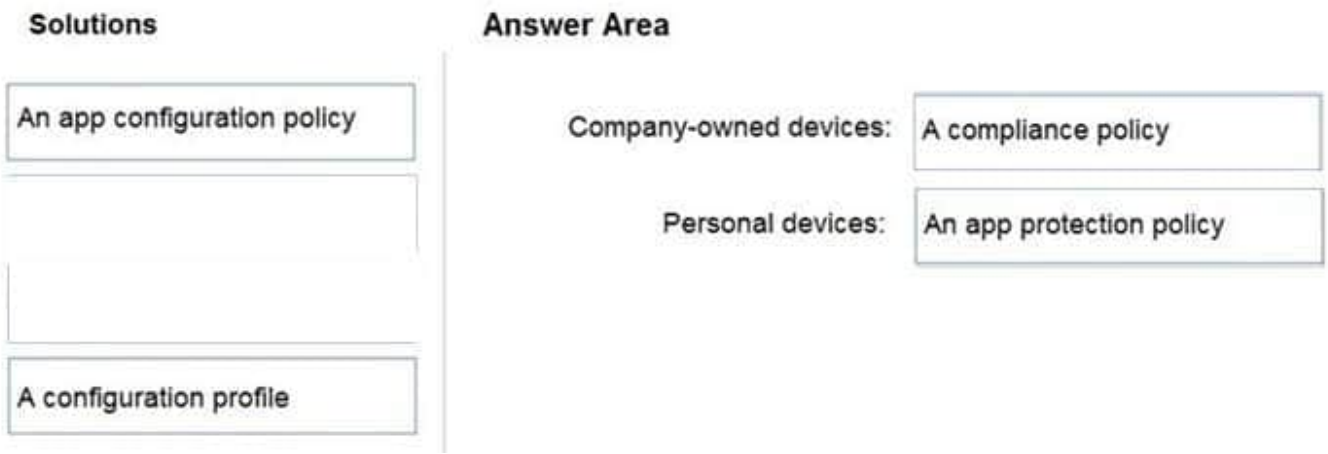
panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



QUESTION 6

HOTSPOT

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Not configured	15	Yes

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

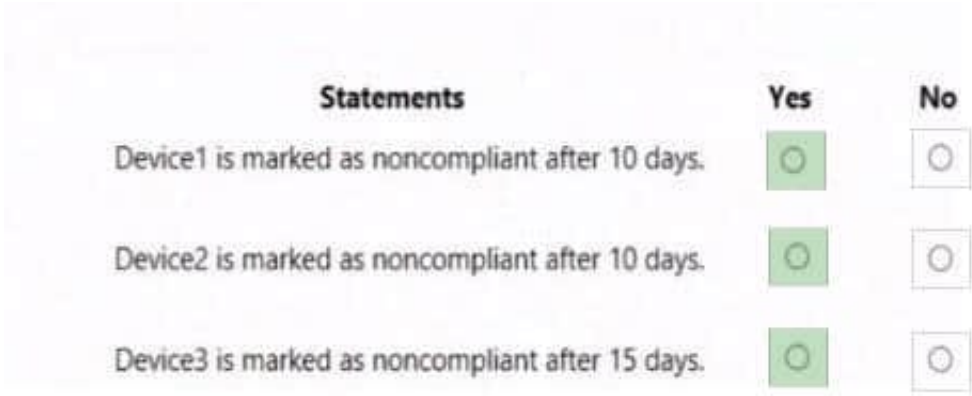
Name	Assigned to
Policy2	Group2
Policy3	Group3

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

Hot Area:

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

Correct Answer:



Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

QUESTION 7

You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.

Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. advanced hunting

B. security reports

C. digital certificate assessment

D. device discovery

E. attack surface reduction (ASR)

Correct Answer: BE

B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting The Microsoft 365 Defender portal (https://security.microsoft.com) provides easy access to information about detected threats and actions to address those threats.

The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created. The Incidents and alerts section lists any incidents that were created as a result of

triggered alerts. Alerts and incidents are generated as threats are detected across devices. The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the

Action center on the History tab.

The Reports section includes reports that show threats detected and their status.

E: What can you expect from Microsoft Defender for Endpoint P1?

Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:

Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks. (E) Attack surface reduction capabilities that harden the device, prevent zero days,

and offer granular control over access and behaviors on the endpoint. Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.

The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL backing	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
APIs, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts**		✓

**Includes Targeted Attack Notifications (TAN) and Experts On Demand (EOD). Customers must apply for TAN. EOD is available for purchase as an add-on.

Incorrect:

Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender- endpoint-plan-1

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft- defender-for-endpoint-plan-1-now-included-in-m365-e3/ba-p/3060639

QUESTION 8

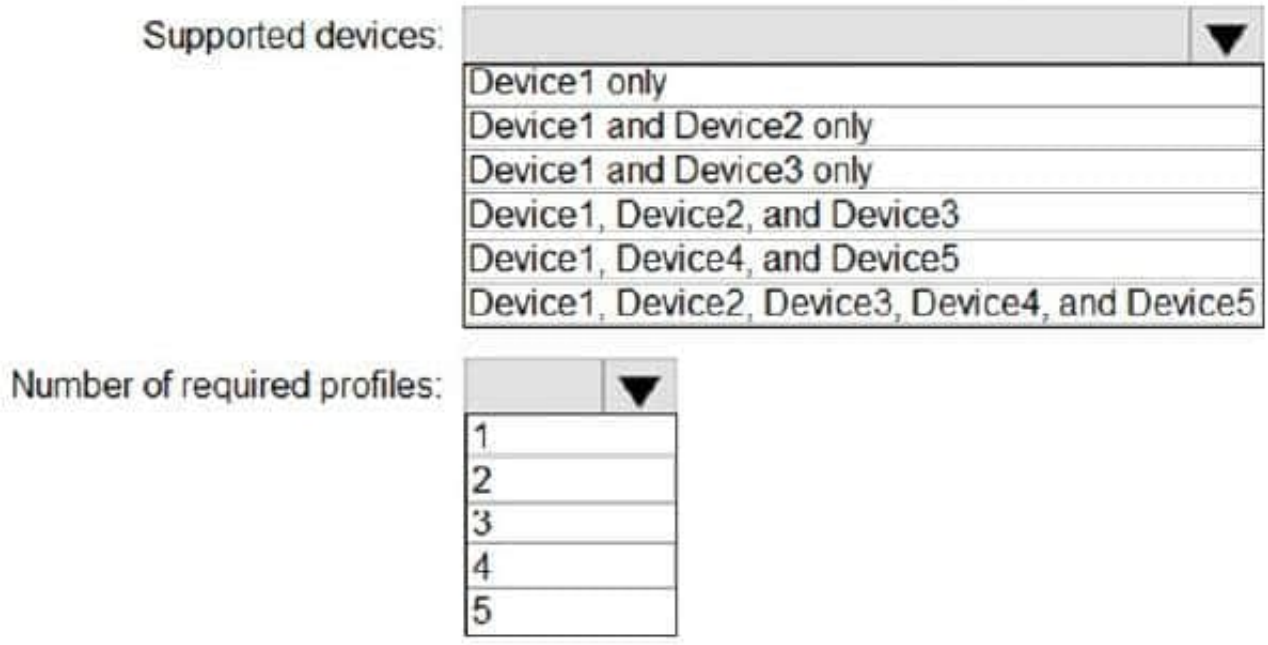
You plan to implement the endpoint protection device configuration profiles to support the planned changes.

You need to identify which devices will be supported, and how many profiles you should implement.

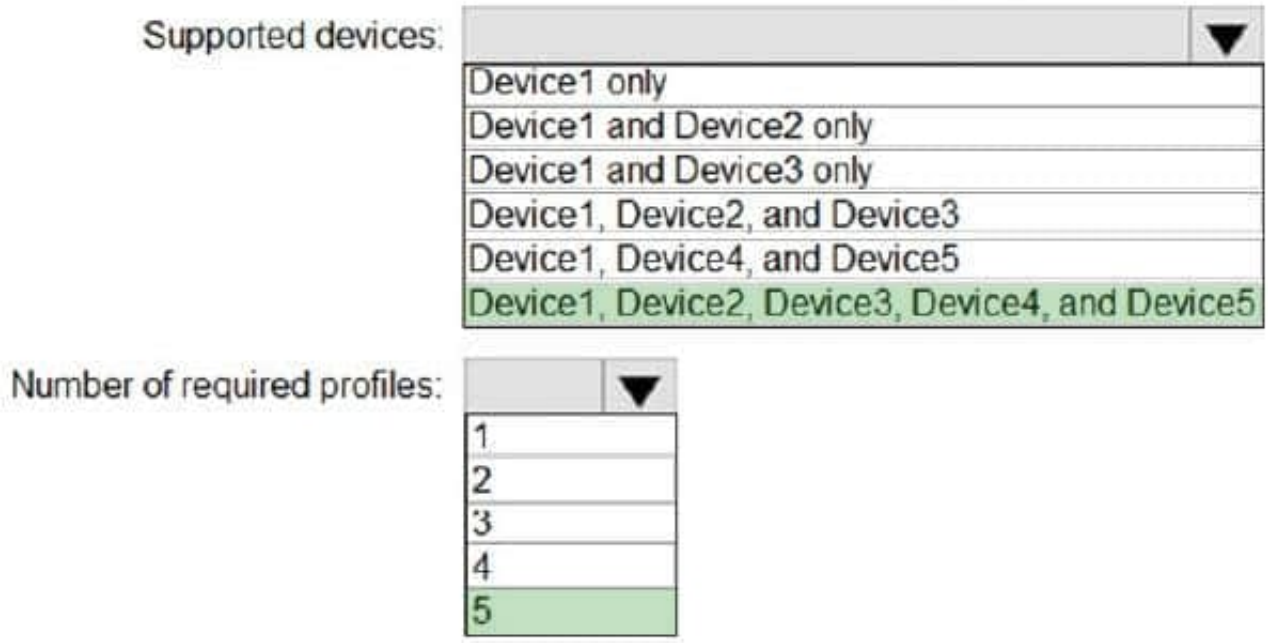
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 9

HOTSPOT

You have a Microsoft 365 E5 subscription.

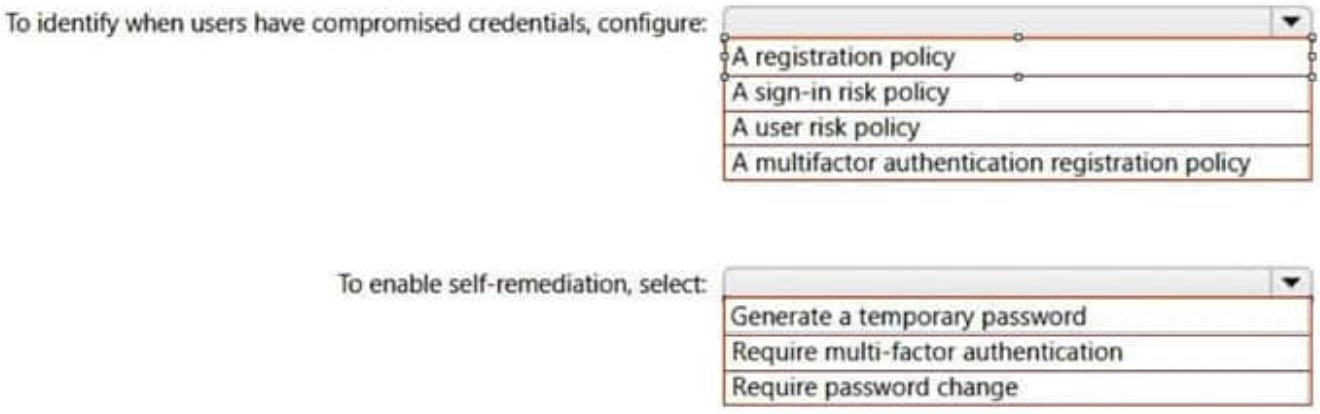
You need to implement identity protection. The solution must meet the following requirements:

Identify when a user\\'s credentials are compromised and shared on the dark web. Provide users that have compromised credentials with the ability to self-remediate.

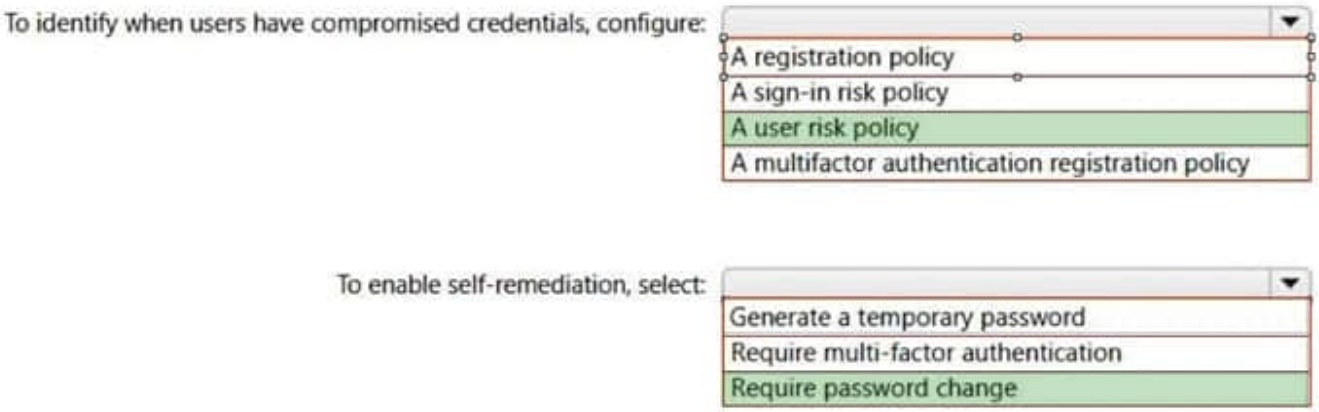
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 10

HOTSPOT

You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

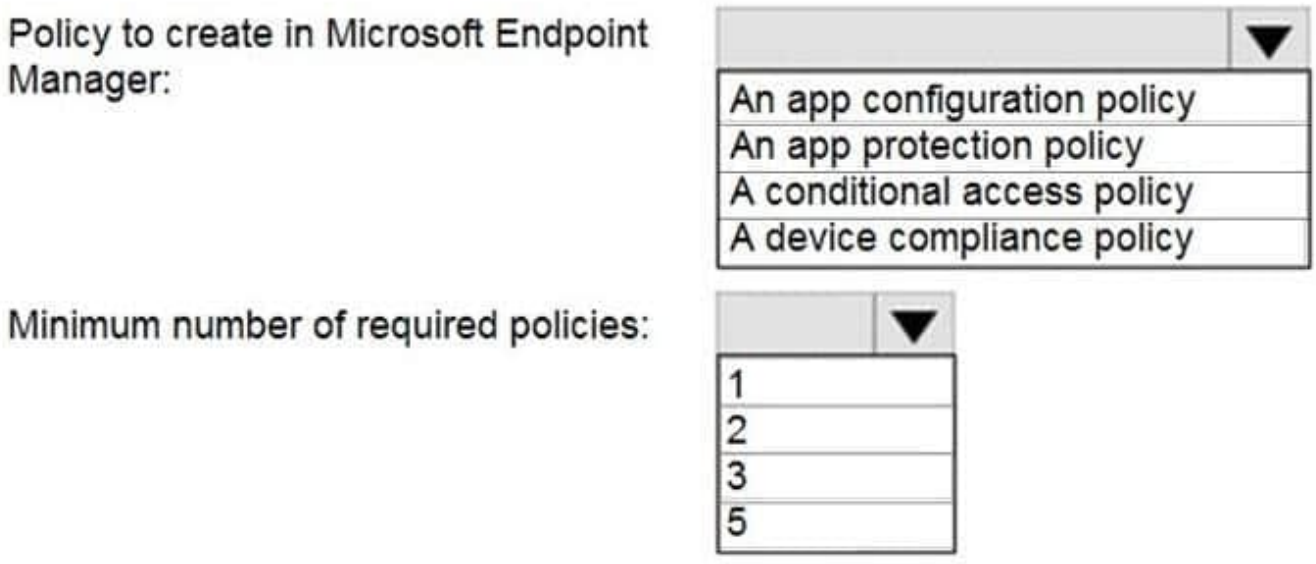
All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

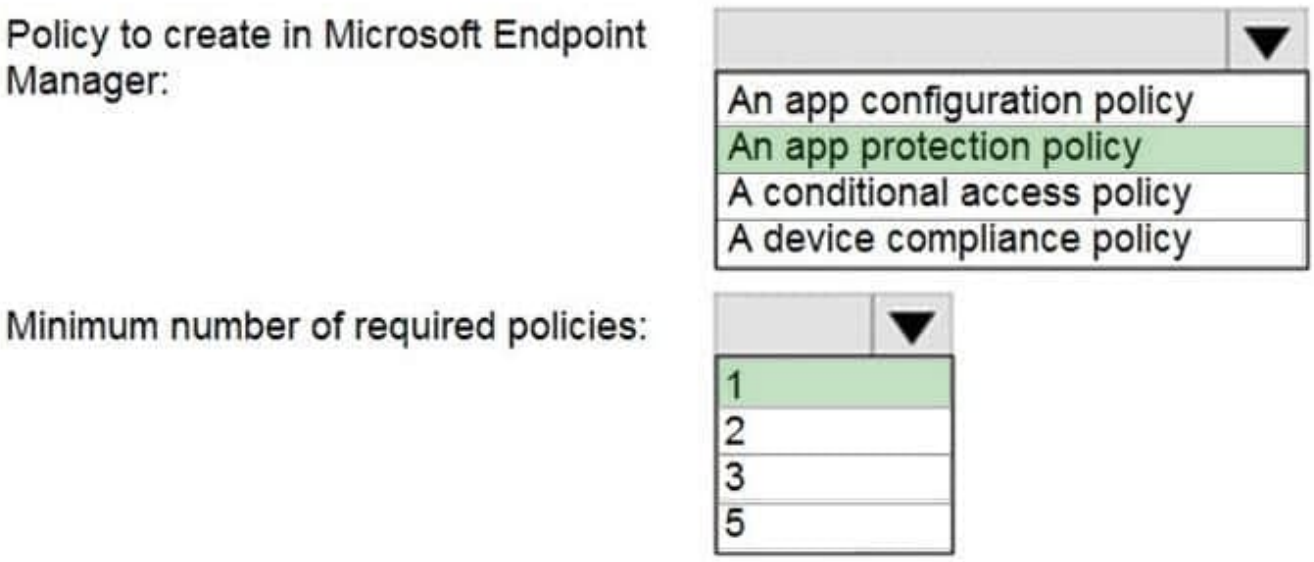
Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 11

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

Correct Answer: A

QUESTION 12

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)

Correct Answer: A

https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dnsrecords-at-any-dns-hosting-provider

QUESTION 13

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data.

What should you do in the Microsoft 365 compliance center?

A. Create a Data Subject Request (DSR)

B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data

C. Create an assessment based on the EU GDPR assessment template

D. Create an assessment based on the Data Protection Baseline assessment template

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan

QUESTION 14

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

Correct Answer: D

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

QUESTION 15

You have a Microsoft 365 E5 tenant that contains a user named User1.

You plan to implement insider risk management.

You need to ensure that User1 can perform the following tasks:

Review alerts.

Manage cases.

Create notice templates.

Review user emails by using Content explorer.

The solution must use the principle of least privilege.

To which role group should you add User1?

A. Insider Risk Management

B. Insider Risk Management Analysts

C. Insider Risk Management Investigators

D. Insider Risk Management Admin

Correct Answer: C

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management- configure?view=o365-worldwide