MD-102 Q&As

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

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

https://www.pass4itsure.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

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

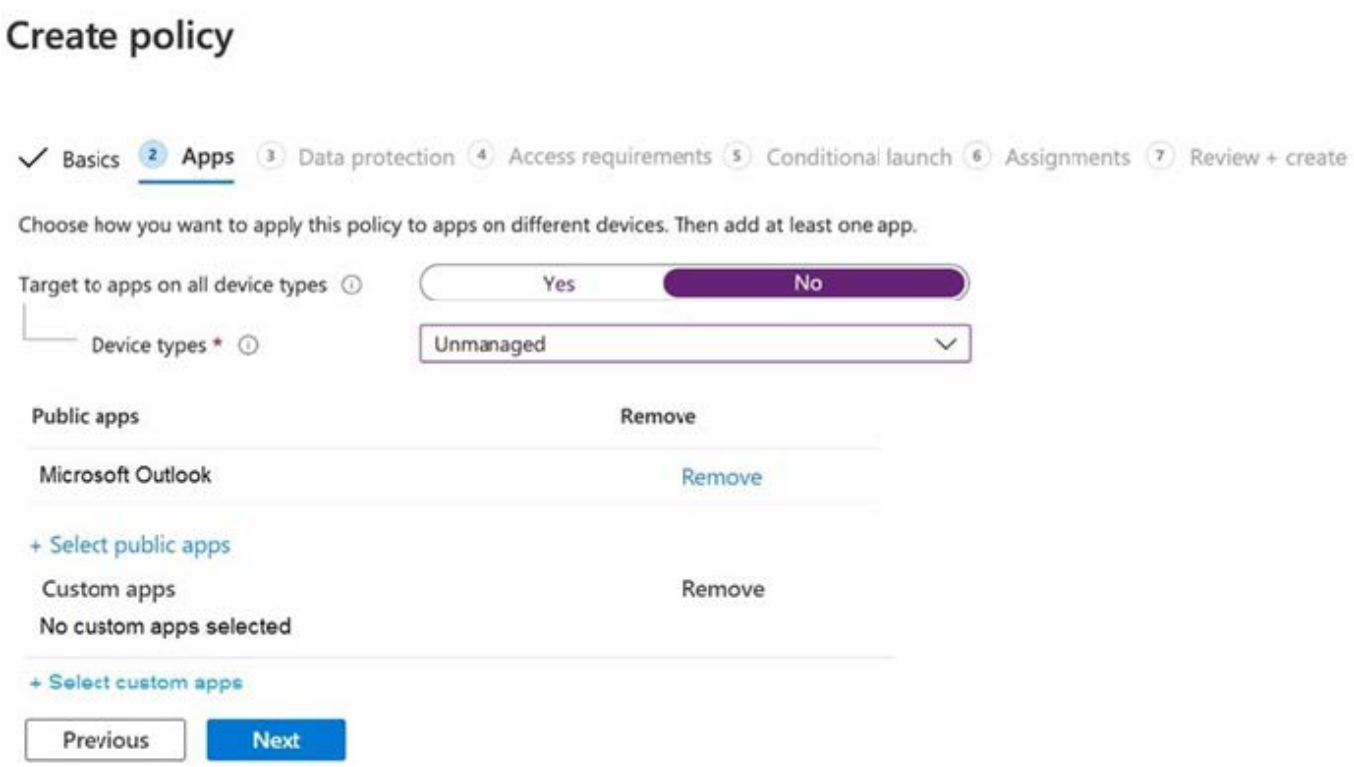
QUESTION 1

HOTSPOT

You have a Microsoft 365 subscription.

Users have iOS devices that are not enrolled in Microsoft Intune.

You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)



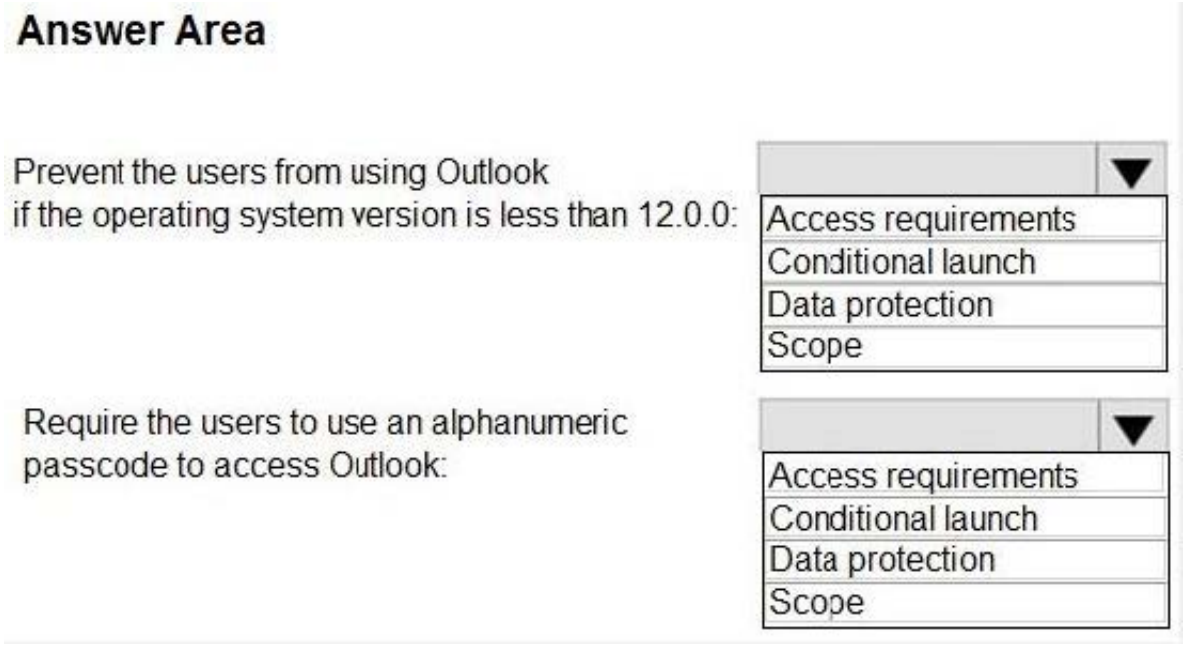
You need to configure the policy to meet the following requirements:

Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.

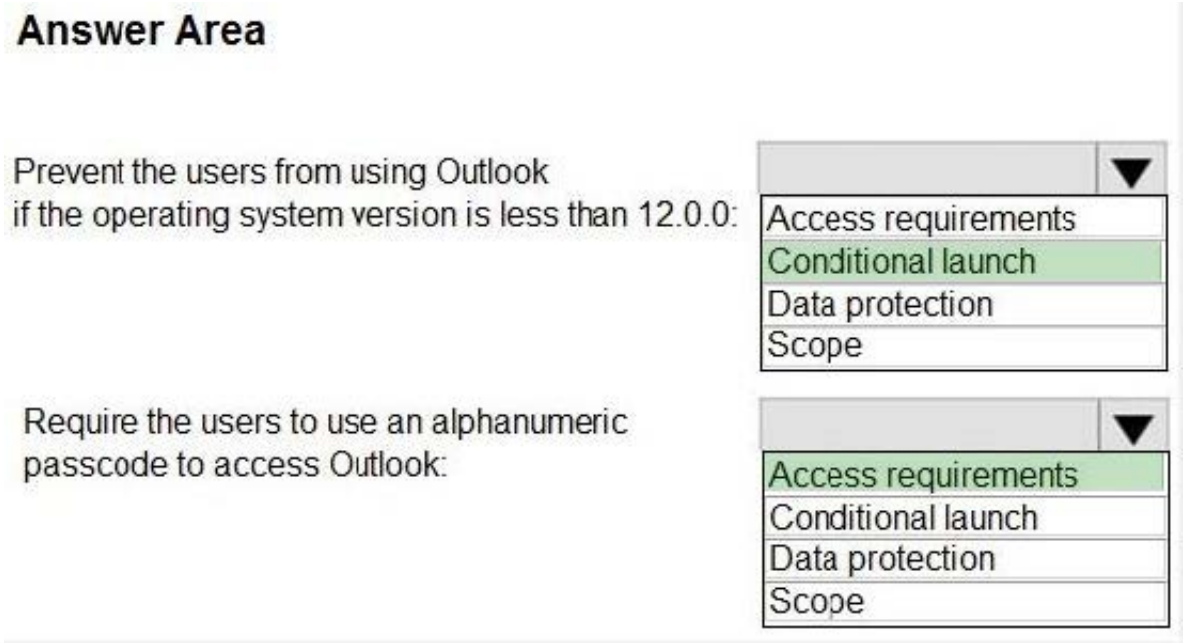
Require the users to use an alphanumeric passcode to access the Outlook app.

What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Conditional launch

Configure conditional launch settings to set sign-in security requirements for your access protection policy.

By default, several settings are provided with pre-configured values and actions. You can delete some of these, like the Min OS version. You can also select additional settings from the Select one dropdown.

Note: There are three categories of policy settings: Data relocation, Access requirements, and Conditional launch.

Box 2. Access requirements

Access requirements include:

PIN for access: Select Require to require a PIN to use this app. The user is prompted to set up this PIN the first time they run the app in a work or school context. The PIN is applied when working either online or offline.

You can configure the PIN strength using the settings available under the PIN for access section.

Reference:

https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios

QUESTION 2

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

Name	Member of
Device1	Group1
Device2	Group1
Device3	Group1

The devices are managed by using Microsoft Intune.

You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the device security settings match the settings specified in the policy.

You discover that devices that are not members of Group1 are shown as Compliant.

You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not compliant.

What should you do from the Microsoft Intune admin center?

A. From Device compliance, configure the Compliance policy settings.

B. From Endpoint security, configure the Conditional access settings.

C. From Tenant administration, modify the Diagnostic settings.

D. From Policy1, modify the actions for noncompliance.

Correct Answer: A

There are two parts to compliance policies in Intune:

Compliance policy settings - Tenant-wide settings that are like a built-in compliance policy that every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that haven\\'t received any device compliance policies are compliant or noncompliant.

Device compliance policy - Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.

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

QUESTION 3

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.

Which three types of data can you collect from the computers by using Log Analytics? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. failure events from the Security log

B. the list of processes and their execution times

C. the average processor utilization

D. error events from the System log

E. third-party application logs stored as text files

Correct Answer: CDE

E: The Custom Logs data source for the Log Analytics agent in Azure Monitor allows you to collect events from text files on both Windows and Linux computers. Many applications log information to text files instead of standard logging services, such as Windows Event log or Syslog. After the data is collected, you can either parse it into individual fields in your queries or extract it during collection to individual fields.

D: Collect Windows event log data sources with Log Analytics agent Windows event logs are one of the most common data sources for Log Analytics agents on Windows virtual machines because many applications write to the Windows event log. You can collect events from standard logs, such as System and Application, and any custom logs created by applications you need to monitor.

C: Summary of data sources The following table lists the agent data sources that are currently available with the Log Analytics agent. Each agent data source links to an article that provides information for that data source. It also provides information on their method and frequency of collection.

*

Performance counters Performance counters in Windows and Linux provide insight into the performance of hardware components, operating systems, and applications. Azure Monitor can collect performance counters from Log Analytics agents at frequent intervals for near real time analysis. Azure Monitor can also aggregate performance data for longer-term analysis and reporting.

*

Etc.

Log queries with performance records The following table provides different examples of log queries that retrieve performance records. Example, CPU utilization across all computers Query: Perf | where ObjectName == "Processor" and CounterName == "% Processor Time" and InstanceName == "_Total" | summarize AVGCPU = avg(CounterValue) by Computer Average

B: The following table lists the objects and counters that you can specify in the configuration file. More counters are available for certain applications.

*

Processor, % Processor Time

*

Processor, % User Time

*

Etc.

Incorrect:

Not A: Not from the Security log.

Important

You can\\'t configure collection of security events from the workspace by using the Log Analytics agent. You must use Microsoft Defender for Cloud or Microsoft Sentinel to collect security events. The Azure Monitor agent can also be used to

collect security events.

Reference: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-custom-logs
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-performance-counters

QUESTION 4

HOTSPOT

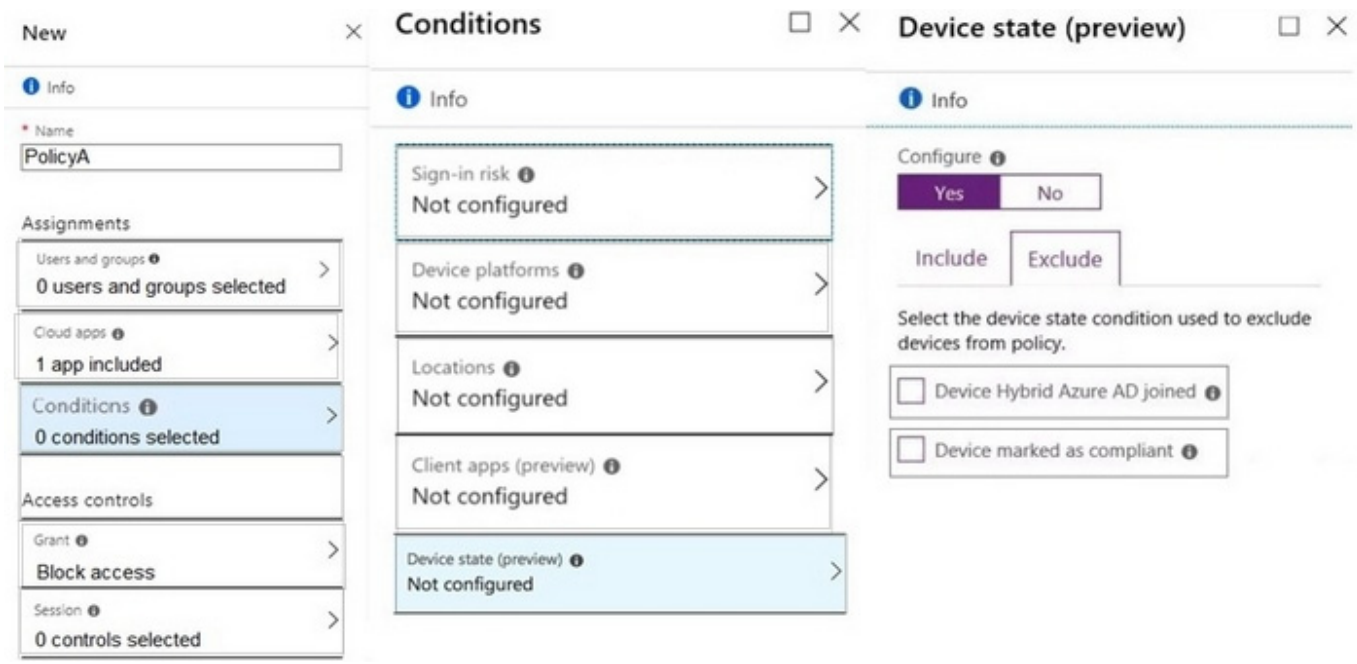
You need a new conditional access policy that has an assignment for Office 365 Exchange Online.

You need to configure the policy to meet the technical requirements for Group4.

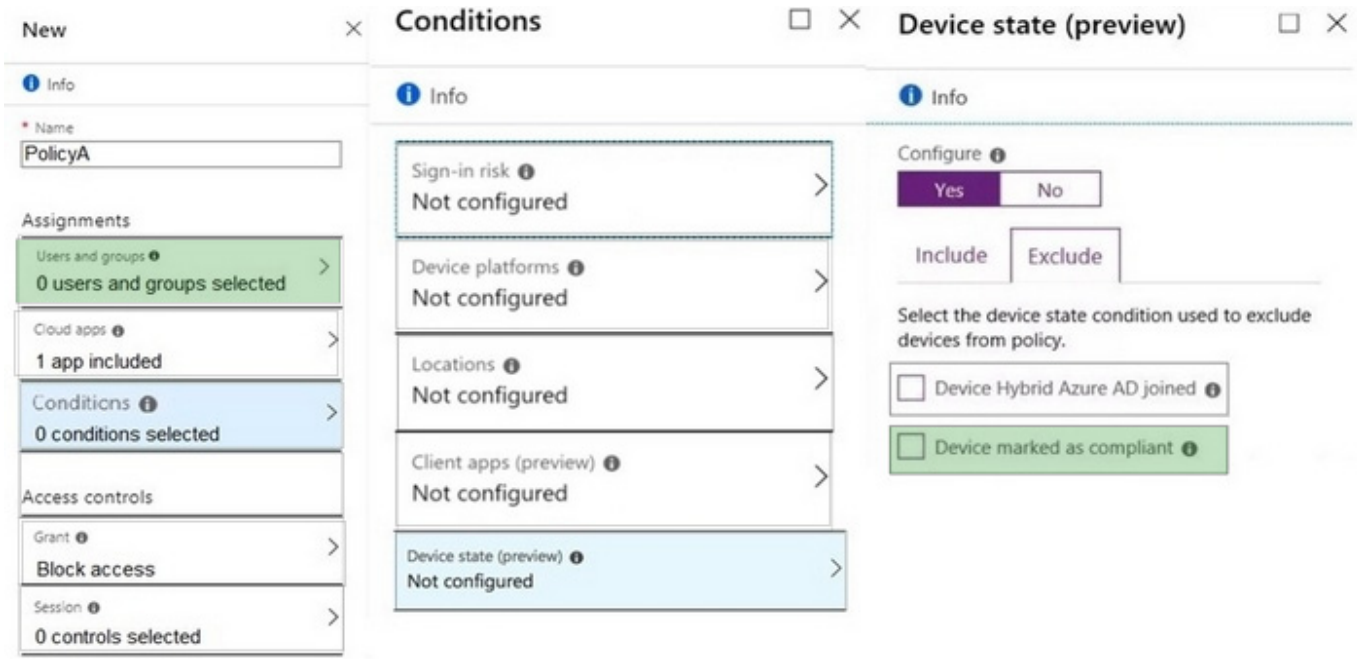
Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions https://docs.microsoft.com/en-us/intune/device-compliance-get-started

QUESTION 5

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

1.

Ensure that you can manage the personal devices by using Microsoft Intune.

2.

Ensure that users can access company data seamlessly from their personal devices.

3.

Ensure that users can only sign in to their personal devices by using their personal account. What should you use to add the devices to Azure AD?

A. Azure AD registered

B. hybrid Azure AD join

C. Azure AD joined

Correct Answer: A

Azure AD registered devices are personal devices that are associated with Azure AD. This allows users to access company data from their personal devices without having to join the devices to the company\\'s domain. Additionally, Azure AD registered devices can be managed by Microsoft Intune.