

Microsoft

MS-101 Exam

Microsoft 365 Mobility and Security

**Questions & Answers
Demo**

Version: 38.0

Question: 1

HOTSPOT

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

You add Exchange Online as a cloud app.

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

NOTE: Each correct selection is worth one point.

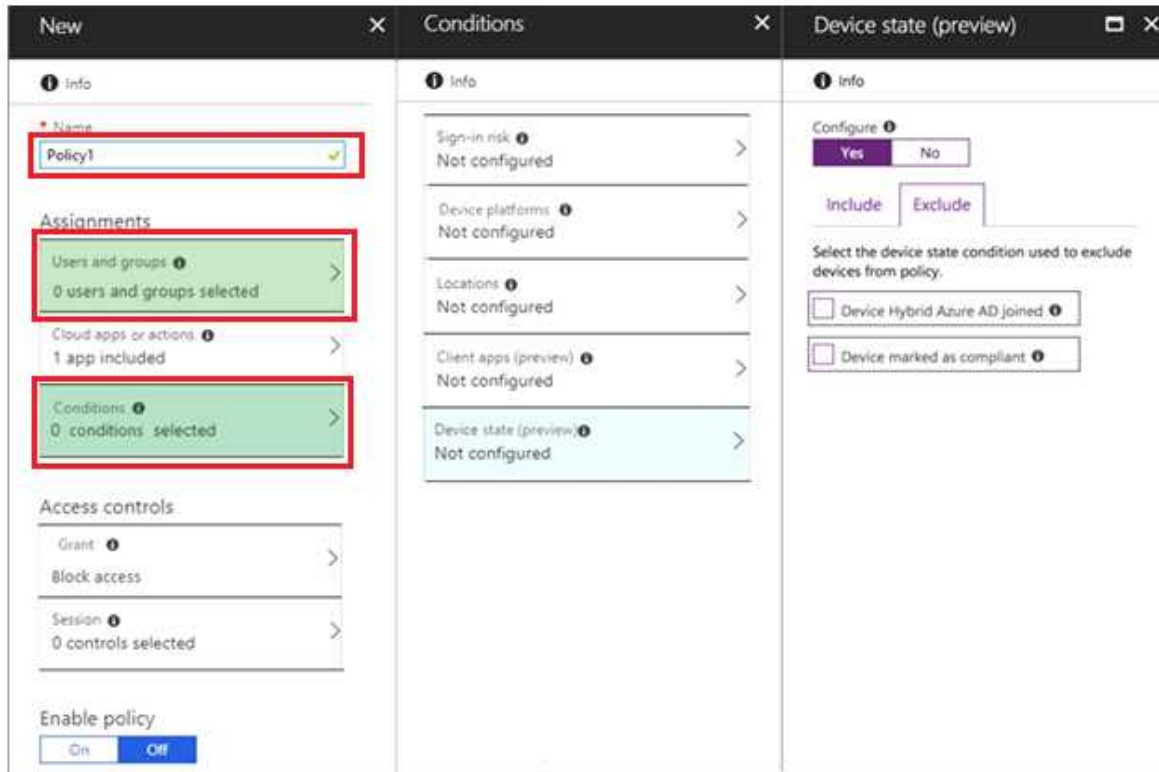
The screenshot displays the Microsoft Conditional Access configuration interface, divided into three main sections:

- New:** Shows the policy name 'Policy1' with a checkmark. Under 'Assignments', 'Cloud apps' shows '1 app included'. Under 'Access controls', 'Grant' is selected. At the bottom, the 'Enable policy' toggle is set to 'Off'.
- Conditions:** Lists several conditions that are currently 'Not configured': Sign-in risk, Device platforms, Locations, Client apps (preview), and Device state (preview). The 'Device state (preview)' condition is highlighted in light blue.
- Device state (preview):** Shows configuration options for the selected condition. The 'Configure' section has 'Yes' selected. The 'Include' and 'Exclude' buttons are visible. Below, there are two checkboxes for device state conditions: 'Device Hybrid Azure AD joined' and 'Device marked as compliant', both of which are currently unchecked.

Answer:

Explanation:

Suggested Answer:



Reference:
<https://docs.microsoft.com/en-us/intune/create-conditional-access-intune>

Question: 2

On which server should you install the Azure ATP sensor?

- A. Server 1
- B. Server 2
- C. Server 3
- D. Server 4
- E. Server 5

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning>

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

Question: 3

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: D

Explanation:

Question: 4

HOTSPOT

You need to meet the Intune requirements for the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

▼
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

▼
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Answer:

Explanation:

Settings to configure in Azure AD:

▼
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

▼
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Reference:

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

Question: 5

HOTSPOT

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

Answer:

Explanation:

Seattle:

▼
6 months
18 months
24 months
30 months
5 years

New York:

▼
6 months
18 months
24 months
30 months
5 years

<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

Reference:

<https://www.windowcentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10>