

# MS-101 Demo

---

**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.

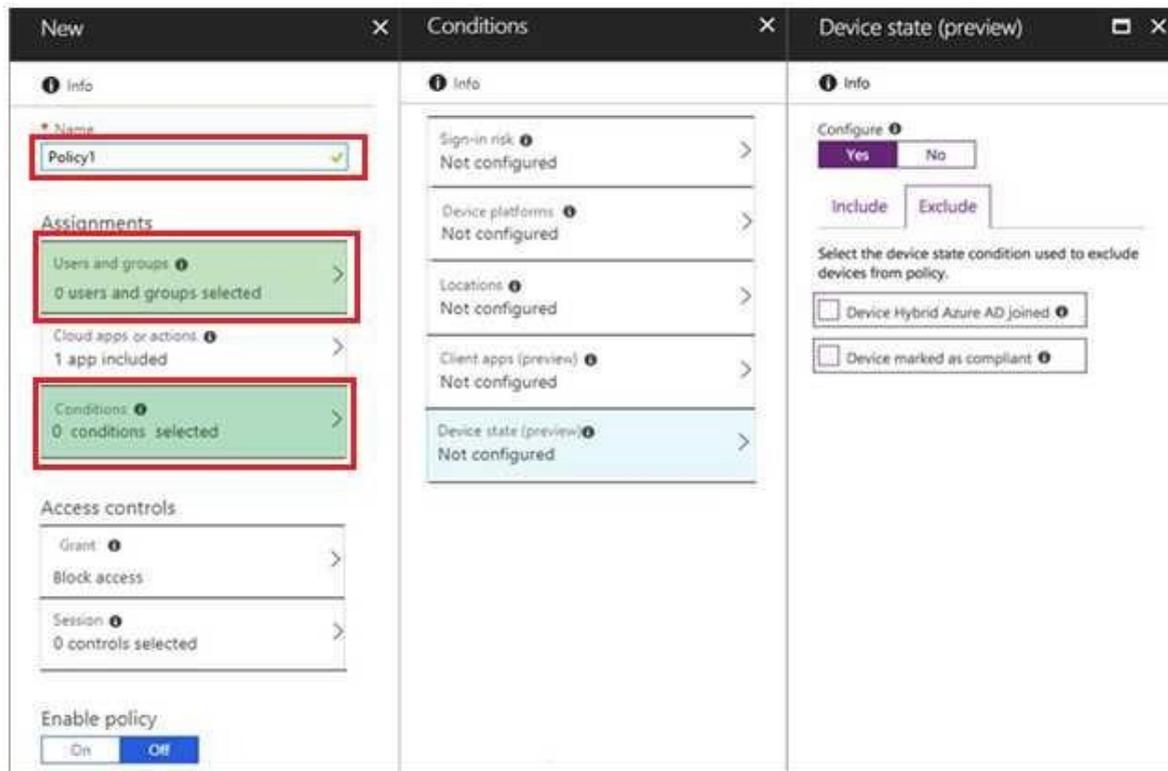
The screenshot displays three panes from the Microsoft Intune console:

- New:** Shows the policy name 'Policy1' and assignment options for 'Users and groups' (0 selected), 'Cloud apps' (1 included), and 'Conditions' (0 selected). It also includes 'Access controls' for 'Grant' (Block access) and 'Session' (0 controls selected), and an 'Enable policy' toggle set to 'Off'.
- Conditions:** Lists configuration options: 'Sign-in risk' (Not configured), 'Device platforms' (Not configured), 'Locations' (Not configured), 'Client apps (preview)' (Not configured), and 'Device state (preview)' (Not configured).
- Device state (preview):** Features a 'Configure' toggle set to 'Yes', 'Include' and 'Exclude' buttons, and a section to 'Select the device state condition used to exclude devices from policy' with checkboxes for 'Device Hybrid Azure AD joined' and 'Device marked as compliant'.

**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: C**

---

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	

Explanation:

---

**Answer:**

---

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>