



# MD-101<sup>Q&As</sup>

Managing Modern Desktops

**Pass Microsoft MD-101 Exam with 100% Guarantee**

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

<https://www.geekcert.com/md-101.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 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:

#### Answer Area

The screenshot shows the Microsoft Conditional Access policy configuration interface. It consists of three main panes: 'New', 'Conditions', and 'Device state (preview)'.  
1. **New** pane: Shows the policy name 'PolicyA'. Under 'Assignments', 'Users and groups' has 0 selected, 'Cloud apps' has 1 app included, and 'Conditions' has 0 selected. Under 'Access controls', 'Grant' is set to 'Block access' and 'Session' has 0 controls selected. At the bottom, the 'Enable policy' toggle is set to 'On'.  
2. **Conditions** pane: Lists several conditions, all currently 'Not configured'. The 'Device state (preview)' condition is highlighted in blue.  
3. **Device state (preview)** pane: Shows a 'Configure' section with 'Yes' selected. Below it are 'Include' and 'Exclude' buttons. A note states: 'Select the device state condition used to exclude devices from policy.' Two checkboxes are visible: 'Device Hybrid Azure AD joined' and 'Device marked as compliant', both of which are currently unchecked.

Correct Answer:



## Answer Area

The screenshot displays the Microsoft Conditional Access configuration interface. It is divided into three main sections: 'New', 'Conditions', and 'Device state (preview)'.  
 - **New:** Shows a policy named 'PolicyA'. Under 'Assignments', 'Users and groups' is selected with '0 users and groups selected'. Under 'Access controls', 'Block access' is selected.  
 - **Conditions:** Lists several conditions, with 'Device state (preview)' selected.  
 - **Device state (preview):** Shows configuration options for the selected condition. The 'Include' button is active, and the 'Device marked as compliant' checkbox is checked, indicating that compliant devices will be excluded from the policy.

The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access



We therefore need to exclude compliant devices.

From the scenario:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.

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 2

### HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to perform the following tasks for User1:

1.

Set the Usage location to Canada.

2.

Configure the Phone and Email authentication contact info for self-service password reset (SSPR).

Which two settings should you configure in the Azure Active Directory admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



## Answer Area

### Manage











-  Profile
-  Custom security attributes  
(Preview)
-  Assigned roles
-  Administrative units
-  Groups
-  Applications
-  Licenses
-  Devices
-  Azure role assignments
-  Authentication methods

Correct Answer:



## Answer Area

### Manage

 Profile
 Custom security attributes (Preview)
 Assigned roles
 Administrative units
 Groups
 Applications
 Licenses
 Devices
 Azure role assignments
 Authentication methods

### QUESTION 3

#### HOTSPOT

You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard.

You need to create a deployment share on Server1.

What should you do on Server1, and what are the minimum components you should add to the MDT deployment





share?

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

Hot Area:

### Answer Area

On Server1:

Import the Deployment Image Servicing and Management (DISM) PowerShell module.
Import the WindowsAutopilotIntune Windows PowerShell module.
Install the Windows Assessment and Deployment Kit (Windows ADK).
Install the Windows Deployment Services server role.

Add to the MDT deployment share:

Windows 10 image and package only
Windows 10 image and task sequence only
Windows 10 image only
Windows 10 image, task sequence, and package

Correct Answer:

### Answer Area

On Server1:

Import the Deployment Image Servicing and Management (DISM) PowerShell module.
Import the WindowsAutopilotIntune Windows PowerShell module.
Install the Windows Assessment and Deployment Kit (Windows ADK).
Install the Windows Deployment Services server role.

Add to the MDT deployment share:

Windows 10 image and package only
Windows 10 image and task sequence only
Windows 10 image only
Windows 10 image, task sequence, and package

Box 1: Install the Windows Deployment Services role.



Install and initialize Windows Deployment Services (WDS)

On the server:

Open an elevated Windows PowerShell prompt and enter the following command:

```
Install-WindowsFeature -Name WDS -IncludeManagementTools
```

```
WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall"
```

```
WDSUTIL /Set-Server /AnswerClients:All
```

Incorrect:

\* Install the Windows Assessment and Deployment Kit (Windows ADK) MDT installation required the ADK, but MDT is already installed.

Box 2: Windows 10 image and task sequence only

Create the reference image task sequence

In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment-with-mdt>

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-image>

---

#### QUESTION 4

You have computers that run Windows 8.1 or Windows 10. All the computers are enrolled in Microsoft Intune, Endpoint Configuration Manager, and Desktop Analytics. Co-management is enabled for your environment.

You plan to upgrade the Windows 8.1 computers to Windows 10.

You need to identify which Windows 8.1 computers do NOT have supported Windows 10 drivers.

What should you use?

- A. the General Hardware Inventory report in Configuration Manager
- B. the List of devices in a specific device category report in Configuration Manager
- C. Deployment plans in Desktop Analytics
- D. the Device compliance report in Intune

Correct Answer: C

Desktop Analytics collects and analyzes device, application, and driver data in your organization. Based on this analysis and your input, you can use the service to create deployment plans for Windows 10. Deployment plans have the following features:

\*





Drivers:

See the list of drivers included with this deployment plan. Set the Upgrade decision, review Microsoft's recommendation, and see compatibility risk factors.

\*

etc.

Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans>

### QUESTION 5





#### DRAG DROP

Your company uses Microsoft Intune. You have a Microsoft Store for Business account.

You need to ensure that you can deploy Microsoft Store for Business apps by using Intune.

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.

Select and Place:

Actions		Answer Area
<b>From Intune, enable Microsoft Store for Business.</b>		
<b>From Microsoft Store for Business, assign apps to people.</b>		
<b>From Intune, sync Microsoft Store for Business.</b>		
<b>From Intune, create an app configuration policy.</b>		
<b>From Microsoft Store for Business, add a management tool.</b>		

Correct Answer:



**Actions**

From Intune, enable Microsoft Store for Business.

From Intune, create an app configuration policy.

**Answer Area**

From Microsoft Store for Business, add a management tool.



From Microsoft Store for Business, assign apps to people.



From Intune, sync Microsoft Store for Business.

References: [https://blogs.msdn.microsoft.com/teju\\_shyamsundar/2016/05/29/integrate-windows-store-for-business-with-microsoft-intune/](https://blogs.msdn.microsoft.com/teju_shyamsundar/2016/05/29/integrate-windows-store-for-business-with-microsoft-intune/)

[MD-101 VCE Dumps](#)

[MD-101 Study Guide](#)

[MD-101 Braindumps](#)