MD-101^{Q&As}

MD-101^{Q&As}

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

HOTSPOT

You have 100 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to configure the following device restrictions:

1.

Block users from browsing to suspicious websites.

2.

Scan all scripts loaded into Microsoft Edge.

Which two settings should you configure in Device restrictions? To answer, select the appropriate settings in the answer area.
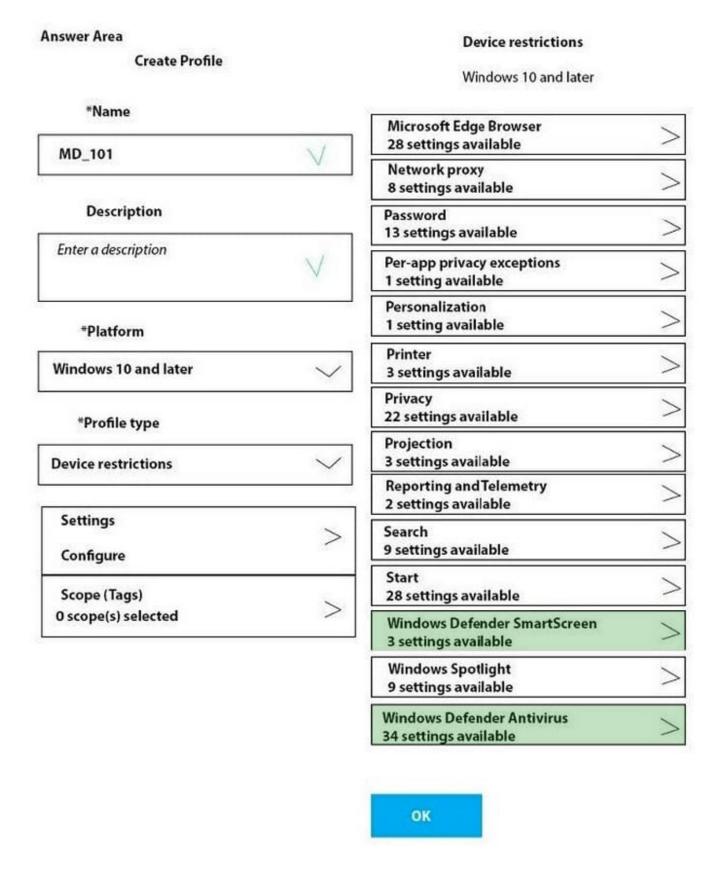
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create Profile

Device restrictions

Windows 10 and later

*Name

MD_101 ✓

Description

Enter a description ✓

*Platform

Windows 10 and later ⌄

*Profile type

Device restrictions ⌄

Settings

Configure >

Scope (Tags)
0 scope(s) selected >

Microsoft Edge Browser
28 settings available >

Network proxy
8 settings available >

Password
13 settings available >

Per-app privacy exceptions
1 setting available >

Personalization
1 setting available >

Printer
3 settings available >

Privacy
22 settings available >

Projection
3 settings available >

Reporting and Telemetry
2 settings available >

Search
9 settings available >

Start
28 settings available >

Windows Defender SmartScreen
3 settings available >

Windows Spotlight
9 settings available >

Windows Defender Antivirus
34 settings available >

OK

Correct Answer:

Answer Area

Create Profile

Device restrictions

Windows 10 and later

*Name

| MD_101 | ✓ |

Description

| Enter a description | ✓ |

*Platform

| Windows 10 and later | ⌄ |

*Profile type

| Device restrictions | ⌄ |

| Settings

Configure | > |

| Scope (Tags)

0 scope(s) selected | > |

| Microsoft Edge Browser
28 settings available | > |
| Network proxy
8 settings available | > |
| Password
13 settings available | > |
| Per-app privacy exceptions
1 setting available | > |
| Personalization
1 setting available | > |
| Printer
3 settings available | > |
| Privacy
22 settings available | > |
| Projection
3 settings available | > |
| Reporting and Telemetry
2 settings available | > |
| Search
9 settings available | > |
| Start
28 settings available | > |
| Windows Defender SmartScreen
3 settings available | > |
| Windows Spotlight
9 settings available | > |
| Windows Defender Antivirus
34 settings available | > |

OK

Box 1: Windows Defender SmartScreen

Block users from browsing to suspicious websites.

Microsoft Defender SmartScreen protects against phishing or malware websites and applications, and the downloading of potentially malicious files.

Microsoft Defender SmartScreen determines whether a site is potentially malicious

Box 2: Windows Defender Antivirus

Scan all scripts loaded into Microsoft Edge.

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-smartscreen/windows-defender-smartscreen-overview

QUESTION 2

DRAG DROP

Your company has a computer named Computer1 that runs Windows 10.

Computer1 was used by a user who left the company.

You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows AutoPilot.

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

Upload the file by using Microsoft Intune.
Generate a CSV file that contains the computer information.
Upload the file by running `azcopy.exe`.
Generate a JSON file that contains the computer information.
Reset the computer.

Answer Area

Correct Answer:

Actions	Answer Area
	Generate a CSV file that contains the computer information.
	Upload the file by using Microsoft Intune.
Upload the file by running `azcopy.exe`.	Reset the computer.
Generate a JSON file that contains the computer information.	

Step 1: Generate a CSV file that contains the computer information

You can perform Windows Autopilot device registration within your organization by manually collecting the hardware identity of devices (hardware hashes) and uploading this information in a comma-separated-values (CSV) file.

Step 2: Upload the file by using Microsoft Intune

By default, Intune only applies this profile to Windows Autopilot devices. Yes, to convert all targeted, non-auto pilot devices to Autopilot so that they can receive the profile the next time they perform a factory reset.

Step 3: Reset the computer Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

Removes personal files, apps, and settings.

Reapplies a device\\'s original settings.

Sets the region, language, and keyboard to the original values.

Maintains the device\\'s identity connection to Azure AD.

Maintains the device\\'s management connection to Intune.

Reference:

https://docs.microsoft.com/en-us/intune/enrollment-autopilot

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

QUESTION 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.

Computer1 has apps that are compatible with Windows 10.

You need to perform a Windows 10 in-place upgrade on Computer1.

Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment share. You create a task sequence, and then you run the MDT deployment wizard on Computer1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

Your network contains an Active Directory named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10.

Folder Redirection is configured for a domain user named User1. The AppData\Roaming folder and the Desktop folder are redirected to a network share.

User1 signs in to Computer1 and performs the following tasks:

1.

Configures screen saver to start after five minutes of inactivity

2.

Modifies the default save location for Microsoft Word

3.

Creates a file named File1.docx on the desktop

4.

Modifies the desktop background

What will be retained when User1 signs in to Computer2?

A. File1.docx and the desktop background only

B. File1.docx, the screen saver settings, the desktop background, and the default save location for Word

C. File1.docx only

D. File1.docx, the desktop background, and the default save location for Word only

Correct Answer: A

Answer is A for sure!

Desktop background is saved in:

"C:\Users\\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper".

Your user profile stores your individual settings under Windows. It is used to re-create your preferred system environment when you log on. This includes everything from your wallpaper and desktop, to your email settings and network

connections. A roaming profile is stored on a central server which can be accessed from all domain computers. This allows you to have the same environment settings on every machine to which you log on. Your roaming profile is copied to a

machine when you log on, and the synchronized back to the server when you log off.

On KAPLAN exam - The only difference is that in their question there was not a Desktop background change. In their official explanation they say that the document in the desktop folder surely is retained. The other settings like screen saver,

default save location for Word, and map a network drive (their option instead of our desktop background) are NOT retained. They explained that the Appdata\Roaming folder stores default templates, some configuration files (like desktop

background, and support data. To redirect everything you would have to use a roaming user profile, not Folder Redirection.

So for this scenario the final answer is A. the file and desktop background.

[MD-101 PDF Dumps](#)   [MD-101 VCE Dumps](#)   [MD-101 Braindumps](#)