



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.passapply.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

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.

You need to ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window.

Solution: In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 4-Auto download and schedule the install, and then enter a time.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/sccm/sum/deploy-use/automatically-deploy-software-updates>

QUESTION 2

HOTSPOT

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to set a custom image as the wallpaper and sign-in screen.

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

* Name

MD_101

Description

Enter a description...

* Platform

Windows 10 and later

* Profile type

Device restrictions

Settings

Configure

Scope (Tags)

0 scope(s) selected

Device restrictions

Windows 10 and later

Select a category to configure settings.

App Store ⓘ

13 settings available

Cellular and connectivity ⓘ

15 settings available

Cloud and Storage ⓘ

4 settings available

Cloud Printer ⓘ

6 settings available

Control Panel and Settings ⓘ

16 settings available

Display ⓘ

2 settings available

General ⓘ

24 settings available

Locked Screen Experience ⓘ

6 settings available

Messaging ⓘ

3 settings available

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

OK



Correct Answer:



Answer Area

Create profile

* Name

MD_101

Description

Enter a description...

* Platform

Windows 10 and later

* Profile type

Device restrictions

Settings

Configure

Scope (Tags)

0 scope(s) selected

Device restrictions

Windows 10 and later

Select a category to configure settings.

App Store ⓘ

13 settings available

Cellular and connectivity ⓘ

15 settings available

Cloud and Storage ⓘ

4 settings available

Cloud Printer ⓘ

6 settings available

Control Panel and Settings ⓘ

16 settings available

Display ⓘ

2 settings available

General ⓘ

24 settings available

Locked Screen Experience ⓘ

6 settings available

Messaging ⓘ

3 settings available

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

OK



Sign-in screen, or Locked screen, image is set under Locked screen experience Wallpaper image, or Desktop background picture, URL is set under Personalization. References:

<https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10>

QUESTION 3

HOTSPOT

Name	Platform
Device1	Windows 10
Device2	macOS

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

In Endpoint security, you need to configure a disk encryption policy for each device.

Which encryption type should you use for each device, and which role-based access control (RBAC) role in Intune should you use to manage the encryption keys?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Device1:

	▼
FileVault	
Cryptsetup	
Encrypting File System (EFS)	
BitLocker Drive Encryption (BitLocker)	

Device2:

	▼
FileVault	
Cryptsetup	
Encrypting File System (EFS)	
BitLocker Drive Encryption (BitLocker)	

RBAC role:

	▼
Help Desk Operator	
Application Manager	
Intune Role Administrator	
Policy and Profile Manager	

Correct Answer:



Answer Area

Device1:

	▼
FileVault	
Cryptsetup	
Encrypting File System (EFS)	
BitLocker Drive Encryption (BitLocker)	

Device2:

	▼
FileVault	
Cryptsetup	
Encrypting File System (EFS)	
BitLocker Drive Encryption (BitLocker)	

RBAC role:

	▼
Help Desk Operator	
Application Manager	
Intune Role Administrator	
Policy and Profile Manager	

QUESTION 4

Your company standardizes on Windows 10 Enterprise for all users.

Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.

You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Microsoft Azure Active Directory (Azure AD), and install several Microsoft Store apps. The solution must meet the following

requirements:

1.



Ensure that any applications installed by the users are retained.

2.

Minimize user intervention.

What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Microsoft Deployment ToolKit (MDT)
- B. Windows Deployment Services (WDS)
- C. a Windows Configuration Designer provisioning package
- D. Windows AutoPilot

Correct Answer: C

You use Windows Configuration Designer to create a provisioning package (.ppkg) that contains customization settings. You can apply the provisioning package to a device running Windows 10. Incorrect Answers:

A: Microsoft Deployment Toolkit (MDT) allows you to automate the deployment of Windows operating systems in your organization. It is not used to upgrade to Windows 10 Enterprise.

B: Windows Deployment Services (WDS) is the revised version of Remote Installation Services (RIS). WDS enables the deployment of Windows operating systems. You can use it to set up new computers using network-based installations. It is not used to upgrade to Windows 10 Enterprise.

D: Windows Autopilot is a user-driven mode designed to minimize intervention of the IT administrator.

References: <https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-edition-upgrades>
<https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-create-package>

QUESTION 5

You use Microsoft Intune and Intune Data Warehouse.

You need to create a device inventory report that includes the data stored in the data warehouse.

What should you use to create the report?

- A. the Azure portal app
- B. Endpoint analytics
- C. the Company Portal app
- D. Microsoft Power BI

Correct Answer: D

You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:



Devices

Enrollment -

App protection policy

Compliance policy

Device configuration profiles

Software updates

Device inventory logs Note: Load the data in Power BI using the OData link With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

Select Reports > Intune Data warehouse > Data warehouse.

3.

Retrieve the custom feed URL from the reporting blade, for example:

4.

<https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api-version=v1.0>

5.

Open Power BI Desktop.

6.

Choose File > Get Data. Select OData feed.

7.

Choose Basic.

8.

Type or paste the OData URL into the URL box.

9.

Select OK.

10.If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.

11.Select Organizational account.



12.Type your username and password.

13.Select Sign In.

14.Select Connect.

15.Select Load.

Reference: <https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi>

QUESTION 6

HOTSPOT

You have the devices shown in the following table.

Name	Operating system
Device1	Windows 10 Enterprise
Device2	Windows 8.1 Pro
Device3	Android 9.03
Device4	iOS

You plan to implement Desktop Analytics.

You need to identify which devices support the following:

1.

Compatibility insights

2.

App usage insights

Which devices should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Compatibility insights:

Device1 only
Device1 and Device2 only
Device3 and Device4 only
Device1, Device2, Device3, and Device4

App usage insights:

Device1 only
Device1 and Device2 only
Device3 and Device4 only
Device1, Device2, Device3, and Device4

Correct Answer:

Answer Area

Compatibility insights:

Device1 only
Device1 and Device2 only
Device3 and Device4 only
Device1, Device2, Device3, and Device4

App usage insights:

Device1 only
Device1 and Device2 only
Device3 and Device4 only
Device1, Device2, Device3, and Device4

Box 1: Device1 and Device2 only You can use the Compatibility Administrator Tool on the following operating systems:
Windows 10 Windows 8.1 Windows 8 Windows 7

Windows Server 2012 Windows Server 2008 R2 Box 2: Device1, Device2, Device3, and Device4

Application Insights adds support for iOS and Android apps.

Reference:



<https://docs.microsoft.com/en-us/windows/deployment/planning/using-the-compatibility-administrator-tool> <https://azure.microsoft.com/en-us/updates/application-insights-adds-support-for-ios-and-android-apps-improved-java-app-support-and-fine-time-selection/>

QUESTION 7

HOTSPOT

You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

You are deploying Microsoft 365 apps.


You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Endpoint Manager admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)



App Information [Edit](#)

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https://products.office.com/en-us/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/en-US/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	...
Logo	
Architecture	Teams, Word
Update channel	64-bit
Remove other versions	Current Channel
Version to install	Yes
Use shared computer activation	Latest
Accept the Microsoft Software License	No
Teams on behalf of users	No
Install background service for Microsoft	No
Search in Bing	
Apps to be installed as part of the suite	1 language(s) selected

Assignments [Edit](#)

Group mode	Group
<input checked="" type="checkbox"/> Required	
<input type="checkbox"/> Included	Group1

Available for enrolled devices

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
LT1 will have Microsoft Office 365 installed	<input type="radio"/>	<input type="radio"/>
LT2 will have Microsoft Office 365 installed	<input type="radio"/>	<input type="radio"/>
LT3 will have Microsoft Office 365 installed	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
LT1 will have Microsoft Office 365 installed	<input checked="" type="radio"/>	<input type="radio"/>
LT2 will have Microsoft Office 365 installed	<input type="radio"/>	<input checked="" type="radio"/>
LT3 will have Microsoft Office 365 installed	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes Policy applies to Group1.

Box 2: No Policy does not apply to Group2.

Box 3: No The policy will not apply for MacOS.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365>

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy>

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add>

QUESTION 8

All of your company's devices are managed via Microsoft Intune.



conditional access is used to prevent devices that are not compliant with company security policies, from accessing Microsoft 365 services.

You need to access Device compliance to view the non-compliant devices.

Where should you access Device compliance from?

- A. System Center Configuration Manager
- B. Windows Defender Security Center.
- C. The Intune admin center.
- D. The Azure Active Directory admin center.

Correct Answer: C

Open the Intune Device compliance dashboard:

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

Select Devices > Overview > Compliance status tab. Important: Devices must be enrolled into Intune to receive device compliance policies. Note 1: Intune Admin portal URL, Microsoft Endpoint Manager admin center: <https://endpoint.microsoft.com> Microsoft Intune, which is a part of Microsoft Endpoint Manager, provides the cloud infrastructure, the cloud-based mobile device management (MDM), cloud-based mobile application management (MAM), and cloud-based PC management for your organization. Note 2: Compliance reports help you review device compliance and troubleshoot compliance-related issues in your organization. Using these reports, you can view information on: The overall compliance states of devices The compliance status for an individual setting The compliance status for an individual policy Drill down into individual devices to view specific settings and policies that affect the device

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor>
<https://docs.microsoft.com/en-us/mem/intune/fundamentals/account-sign-up>

QUESTION 9

HOTSPOT

Your company has 1,000 Windows 10 devices that are enrolled in Windows Analytics.

You need to view the following information:

1.

The number of devices that are vulnerable to Spectre and Meltdown vulnerabilities

2.

The number of devices that have Windows Defender real-time protection turned off

Which Windows Analytics solutions should you use? To answer, select the appropriate options in the answer area.



NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The number of devices that are vulnerable to Spectre and Meltdown vulnerabilities:

	▼
Device Health	
Update Compliance	
Upgrade Readiness	

The number of devices that have Windows Defender real-time protection turned off:

	▼
Device Health	
Update Compliance	
Upgrade Readiness	

Correct Answer:

Answer Area

The number of devices that are vulnerable to Spectre and Meltdown vulnerabilities:

	▼
Device Health	
Update Compliance	
Upgrade Readiness	

The number of devices that have Windows Defender real-time protection turned off:

	▼
Device Health	
Update Compliance	
Upgrade Readiness	

Box 1: Device Health Driver health -

App health (outside of a deployment plan) Frequently crashing devices or driver-induced crashes Windows sign-in



health Windows Information Protection Support for Windows Server Box 2: Device Health

Incorrect:

* Update Compliance

Support for Windows Update for Business Delivery Optimization insights Support for Windows 10 long-term servicing channel (LTSC)

Windows Insider reports Windows Defender status

* Upgrade Readiness Internet Explorer Site Discovery data Microsoft 365 Apps add-in insights (now available in Configuration Manager)

Feedback Hub insights

Reference: <https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/faq>

QUESTION 10

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 company has an Azure Active Directory (Azure AD) tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Azure Active Directory admin center, you modify the User settings and the Device settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead, from the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Device Management admin center, you configure the Windows Hello for Business enrollment options.

Reference: <https://docs.microsoft.com/en-us/intune/protect/windows-hello>



QUESTION 11

You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft intune. You create an app configuration policy that contains the following settings:

1.

Device enrollment type: Managed devices

2.

Profile Type: All Profile Types

3.

Platform: Android Enterprise

Which two types of apps can be associated with the policy?

Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Android Enterprise system app

B. Android store app

C. Web link

D. Managed Google Play store app

E. Built-in Android app

Correct Answer: AD

QUESTION 12

Your network contains an Active Directory domain. The domain contains computers that run Windows 8.1 and the users shown in the following table.

Name	Domain group membership	Local group membership
User1	Domain Users, Domain Admins	Administrators
User2	Domain Users, Remote Management Users	Users
User3	Domain Users	Administrators
User4	Domain Users	Remote Management Users

You plan to use the Microsoft Assessment and Planning (MAP) Toolkit to collect inventory data. The MAP Toolkit has the following configurations:

1.

Inventory scenario: Windows computers



2.

Discovery method: Use Active Directory Domain Services (AD DS)

You need to identify which user to use for the MAP Toolkit inventory discovery. The solution must use principle of least privilege.

What should you identify?

- A. User3
- B. User1
- C. User4
- D. User2

Correct Answer: A

Discovery method: Use Active Directory Domain Services (AD DS)

Credentials required " The wizard requires a domain account that is to be used to query AD DS. At a minimum, this account should be a member of the Domain

Users group in the domain. For each computer to be included in the WMI inventory process, the wizard also requires an account that is a member of the local

Administrators group on that computer.

Reference:

<https://social.technet.microsoft.com/wiki/contents/articles/17808.map-toolkit-choose-a-discovery-method.aspx>

QUESTION 13

DRAG DROP

You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).

You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

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

- Obtain the root certificate.
- From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.
- From the Enterprise CA, configure certificate managers.
- From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.
- From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.

Answer Area



Correct Answer:

Actions

-
-
- From the Enterprise CA, configure certificate managers.
-
- From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.

Answer Area



- Obtain the root certificate.
- From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.
- From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.

Step 1: Obtain the root certificate.

Export the root certificate from the Enterprise CA.

To authenticate a device with VPN, WiFi, or other resources, a device needs a root or intermediate CA certificate.

Step 2: From the Microsoft Endpoint Manager admin center, create a trusted certificate profile

Create a trusted certificate profile

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.



Select and go to Devices > Configuration profiles > Create profile.

3.

Enter the following properties:

Platform:

Profile: Select Trusted certificate. Or, select Templates > Trusted certificate.

Select Create.

4.

Etc.

Step 3: From the Microsoft Endpoint Manager admin center, create a PKCS certificate profile

Create a PKCS certificate profile

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

Select and go to Devices > Configuration profiles > Create profile.

3.

Enter the following properties:

Platform:

Profile: Select PKCS certificate. Or, select Templates > PKCS certificate.

Select Create.

4.

Etc.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure>

QUESTION 14

You are currently making use of the Antimalware Assessment solution in Microsoft Azure Log Analytics.

You have accessed the Protection Status dashboard and find that there is a device that has no real time protection.

Which of the following could be a reason for this occurring?

A. Windows Defender has been disabled.

B. You need to install the Azure Diagnostic extension.



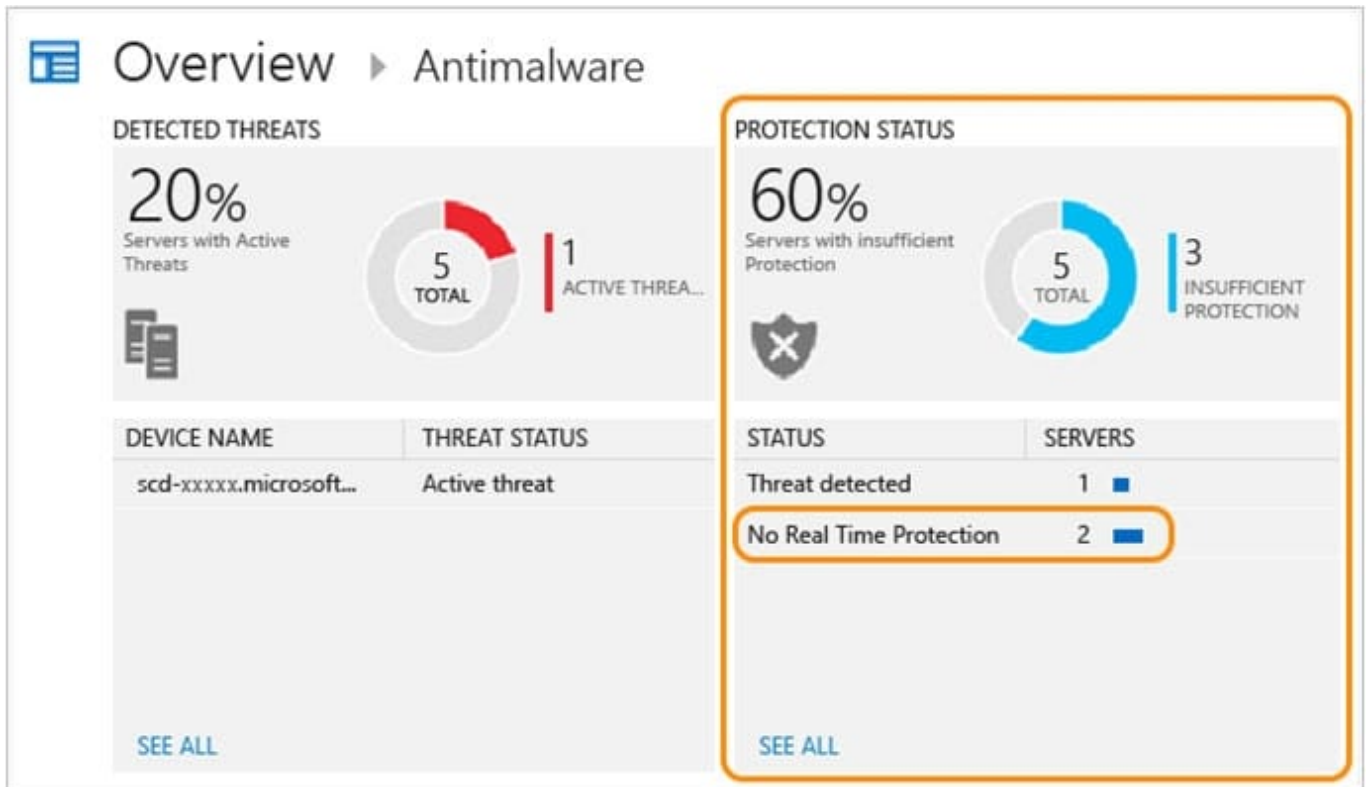
C. Windows Defender Credential Guard is incorrectly configured.

D. Windows Defender System Guard is incorrectly configured.

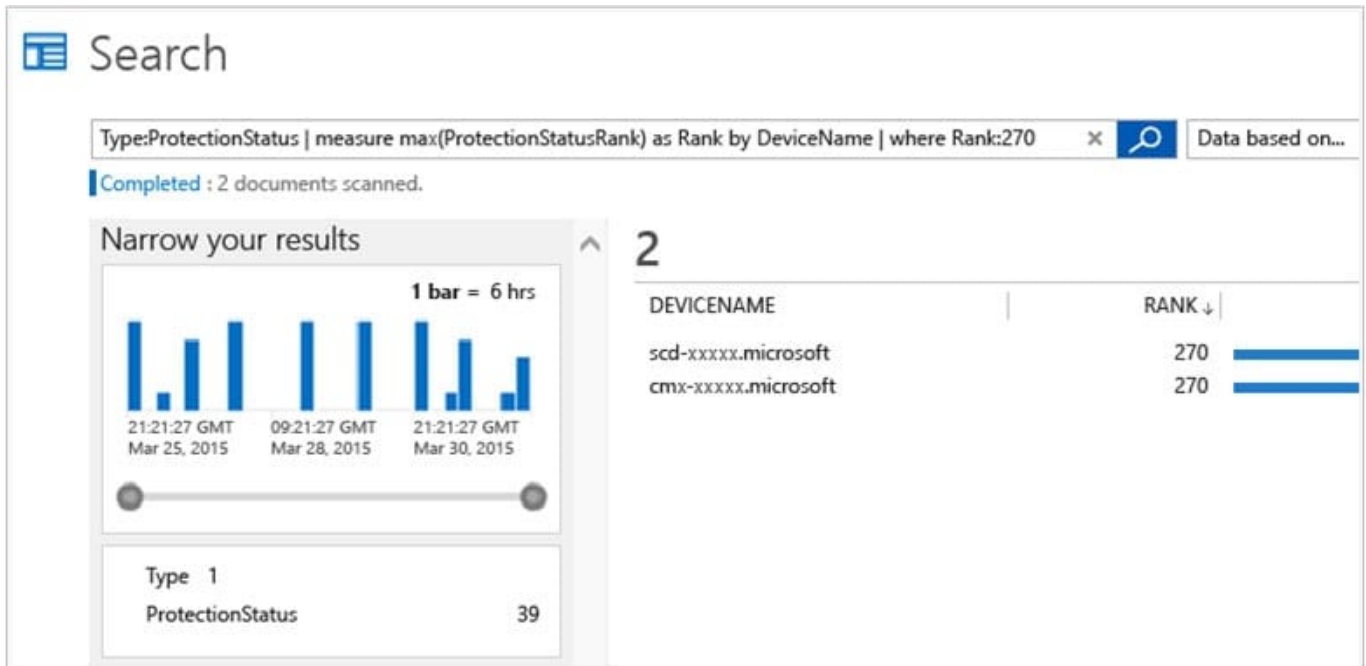
Correct Answer: A

Microsoft Defender Antivirus is usually the primary antivirus/antimalware product on your device. To review protection status

1. On the Antimalware dashboard, you will review the Protection Status blade and click no real time protection.



2. Search shows a list of servers without protection.



3. At this point you now know what servers do not have realtime protection.

Computers that do not have System Center Endpoint Protection installed (or if SCEP is not detected) will be reported as no real time protection.

Reference: <https://docs.microsoft.com/ga-ie/azure/security-center/security-center-install-endpoint-protection>

QUESTION 15

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 company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft Intune subscription.

Contoso.com contains a user named user1@contoso.com.

You have a computer named Computer1 that runs Windows 8.1.

You need to perform an in-place upgrade of Computer1 to Windows 10.

Solution: You start Computer1 from the Windows 10 installation media and use the Install option.

Does this meet the goal?

A. Yes



B. No

Correct Answer: B

Instead: From Windows 8.1, you run setup.exe from the Windows 10 installation media. How To Upgrade To Windows 10 Using ISO File

1. Open your existing Windows edition and locate the ISO file. Now right click on this file and Mount, restart the machine. After rebooting, open File Explorer and locate the DVD drive, you'll find that the ISO file is already mounted to it with a temporary drive letter (as you can see in below shown window, where D: is temporary drive letter). Open this drive and click on the setup.exe file.

Reference: <https://www.kapilarya.com/how-to-upgrade-to-windows-10-using-iso-file>

[MD-101 VCE Dumps](#)

[MD-101 Study Guide](#)

[MD-101 Exam Questions](#)