

**100%** Money Back  
**Guarantee**

**Vendor:**Microsoft

**Exam Code:**MD-101

**Exam Name:**Managing Modern Desktops

**Version:**Demo

**QUESTION 1**

**HOTSPOT**

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share1.

You add Windows 10 images to Share1 as shown in the following table.

<b>Name</b>	<b>In WIM file</b>	<b>Description</b>
Image1	Install1.wim	Default Windows 10 Pro image from the Windows 10 installation media
Image2	Install1.wim	Default Windows 10 Enterprise image from the Windows 10 installation media
Image3	Install2.wim	Default Windows 10 Pro for Workstations image from the Windows 10 installation media
Image4	Custom1.wim	Custom Windows 10 Enterprise image without any additional applications
Image5	Custom2.wim	Custom Windows 10 Enterprise image that includes custom applications

Which images can be used in the Standard Client Task Sequence, and which images can be used in the Standard Client Upgrade Task Sequence? NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Standard Client Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Correct Answer:

## Answer Area

Standard Client Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Box 1: Image1, Image2, Image3, Image4, and Image5.

All images.

Standard Client Task Sequence Standard Client task sequence. The most frequently used task sequence. Used for creating reference images and for deploying clients in production.

Box 2: Image1, Image2, Image3, and Image4 only.

Exclude image5 with applications.

Standard Client Upgrade Task Sequence

Standard Client Upgrade task sequence. A simple task sequence template used to perform an in-place upgrade from Windows 7, Windows 8, or Windows 8.1 directly to Windows 10, automatically preserving existing data, settings,

applications, and drivers.

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit>

---

## QUESTION 2

What should you use to meet the technical requirements for Azure DevOps?

- A. An app protection policy
- B. Windows Information Protection (WIP)
- C. Conditional access
- D. A device configuration profile

Correct Answer: C

Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

Reference:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access?view=azure-devops>

---

## QUESTION 3

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft Intune.

You are creating a device configuration profile for the workstations. You have been informed that a custom image should be displayed on the sign-in screen.

Which of the following is a Device restriction setting that should be configured?

- A. Locked screen experience
- B. Personalization
- C. Display
- D. General

Correct Answer: B

Wallpaper image, or Desktop background picture, URL is set under Personalization.

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

---

## QUESTION 4

HOTSPOT

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You need to create Endpoint security policies to meet the following requirements:

1.

Hide the Firewall and network protection area in the Windows Security app.

2.

Disable the provisioning of Windows Hello for Business on the devices.









Which two policy types should you use? To answer, select the policies in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

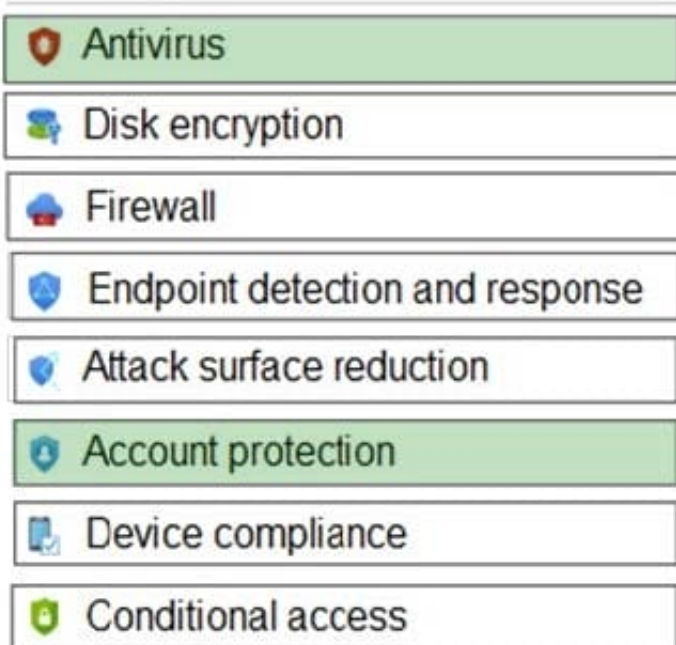
### Manage

 Antivirus
 Disk encryption
 Firewall
 Endpoint detection and response
 Attack surface reduction
 Account protection
 Device compliance
 Conditional access

Correct Answer:

## Answer Area

### Manage



In the Antivirus policy settings, you can hide the Firewall and network protection area in the Windows Security app.

Windows Hello for Business settings are configured in Identity protection.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings>

<https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings>

---

### QUESTION 5

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 configure automatic mobile device management (MDM) enrollment. From the Device Management admin center, you create and assign a device restrictions profile.

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.

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

---

## QUESTION 6

You use Windows Admin Center to remotely administer computers that run Windows 10.

When connecting to Windows Admin Center, you receive the message shown in the following exhibit.

### This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

 [Go to your Start page](#)

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG\_FLAGS\_INVALID\_CA

[Go on to the webpage](#) (Not recommended)

You need to prevent the message from appearing when you connect to Windows Admin Center. To which certificate store should you import the certificate?

A. Client Authentication Issuers



B. Trusted Root Certification Authorities

C. Personal

Correct Answer: B

The domain members should have trusted root certificate stored.

Reference:

<https://social.technet.microsoft.com/Forums/en-US/6b3abb8e-007e-4047-bd30-2946b9c3aaba/windows-admin-center-three-questions-login-and-certs?forum=ws2016>

---

### QUESTION 7

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 redirect Windows known folders to Microsoft OneDrive for Business.

Which folder will be included in the redirection?

A. Saved Games

B. Documents

C. Music

D. Downloads

E. Favorites

F. AppData

G. Videos

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/onedrive/redirect-known-folders>

---

### QUESTION 8

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 during a maintenance window.

Solution: In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 3 ?Auto download and notify for Install, and then enter a time.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: 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.

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

---

## QUESTION 9

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 have a Microsoft 365 subscription.

You have 20 computers that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD).

You plan to replace the computers with new computers that run Windows 10. The new computers will be joined to Azure AD.

You need to ensure that the desktop background, the favorites, and the browsing history are available on the new computers.

Solution: You configure Enterprise State Roaming.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable>

---

## QUESTION 10

You have a Microsoft 365 subscription. The subscription contains 500 computers that run Windows 11 and are enrolled in Microsoft Endpoint Manager. You need to manage the deployment of monthly security updates. The solution must meet the following requirements:

1.

Updates must be deployed to a group of test computers for quality assurance.

2.

Updates must be deployed automatically 15 days after the quality assurance testing. What should you create in the Microsoft Endpoint Manager admin center?

A. a security baseline

B. a device configuration profile

C. an update ring

D. a feature update policy

Correct Answer: C

---

#### QUESTION 11

Your on-premises network contains an Active Directory domain named contoso.com. You perform the following actions:

1.

Purchase a new Microsoft 365 subscription.

2.

Create a new user named User1.

3.

Assign User1 the Security Administrator role.

You need to ensure that User1 can enable Conditional Access policies.

What should User1 do first?

A. Register for Azure Multi-Factor Authentication (MFA).

B. Request the Conditional Access Administrator role.

C. Disable Security defaults.

D. Implement Azure AD Connect.

Correct Answer: C

Microsoft provides security defaults that ensure a basic level of security enabled in tenants that don't have Azure AD Premium. With Conditional Access, you can create policies that provide the same protection as security defaults, but

with

granularity. Conditional Access and security defaults aren't meant to be combined as creating Conditional Access policies will prevent you from enabling security defaults.

Incorrect:

Not B:

Not required. Global administrator, security administrator, or Conditional Access administrator is enough.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>

---

## QUESTION 12

Your network contains an Active Directory domain named contoso.com. The domain contains computers that run Windows 10 and are joined to the domain.

The domain is synced to Microsoft Azure Active Directory (Azure AD).

You create an Azure Log Analytics workspace and deploy the Device Health solution.

You need to enroll the computers in Windows Analytics.

Which Group Policy setting should you configure?

- A. Specify intranet Microsoft update service location
- B. Allow Telemetry
- C. Configure the Commercial ID
- D. Connected User Experiences and Telemetry

Correct Answer: C

Microsoft uses a unique commercial ID to map information from user computers to your Azure workspace. Copy your commercial ID key from any of the Windows Analytics solutions you have added to your Windows Portal, and then deploy it to user computers.

References: <https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-get-started>