

Microsoft.MD-102.vFeb-2024.by.Rina.114q

Number: MD-102
Passing Score: 800
Time Limit: 120
File Version: 14.2

Exam Code: MD-102

Exam Name: Endpoint Administrator



Case 01 - Contoso

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Network Environment

The network contains an on-premises Active domain named Contoso.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named Contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups

The Contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1



All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 lic

Enterprise State Roaming is enabled for Group1 and GroupA.

Group and Group have a Membership type of Assign

Devices

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	None
Device5	Yes	No	None

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder D:\Folder 1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

The Compliance policy settings are shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as Compliant Not Compliant

Enhanced jailbreak detection Enabled Disabled

Compliance status validity period (days)

The Automatic Enrolment settings have the following configurations:

- MDM user scope GroupA
- MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

- Name: Protection1
- Folder protection: Enable
- List of apps that have access to protected folders: CV\AppA.exe
- List of additional folders that need to be protected: D:\Folder1
- Assignments

Windows Autopilot Configuration



Create profile ...

Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments **4 Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No



Currently, there are no devices deployed by using Windows Autopilot

The Intune connector for Active Directory is installed on Server 1.

Planned Changes

Contoso plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
- Deploy a network boundary configuration profile that will have the following settings:
 - Name Boundary 1
 - Network boundary 192.168.1.0/24
 - Scope tags: Tag 1
 - Assignments;
 - included groups: Group 1, Group2
- Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
 - Name: Connection 1
 - Connection name: VPNI

- Connection type: L2TP
- Assignments:
 - Included groups: Group1, Group2, GroupA
 - Excluded groups: —
- Name: Connection
- Connection name: VPN2
- Connection type: IKEv2 i Assignments:
 - included groups: GroupA
 - Excluded groups: GroupB
- Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements

Contoso must meet the following technical requirements:

- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

QUESTION 1

HOTSPOT

User1 and User2 plan to use Sync your settings.

On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

Hot Area interface showing two dropdown menus for User1 and User2. Each dropdown menu contains the following options:

- No devices
- Device4 and Device5 only
- Device1, Device2 and Device3 only
- Device1, Device2, Device3, Device4, and Device5

Answer Area:



Section:

Explanation:

Reference:

<https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/>

QUESTION 2

You implement Boundary1 based on the planned changes.

Which devices have a network boundary of 192.168.1.0/24 applied?

- A. Device2 only
- B. Device3 only
- C. Device 1, Device2, and Device5 only
- D. Device 1, Device2, Device3, and Device4 only

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows>

QUESTION 3

Which devices are registered by using the Windows Autopilot deployment service?

- A. Device1 only
- B. Device3 only
- C. Device1 and Device3 only
- D. Device1, Device2, and Device3

Correct Answer: C

Section:

Explanation:

Scenario: Windows Autopilot Configuration

Assignments

Included groups: Group1

Excluded groups: Group2

Device1 is member of Group1.



Device2 is member of Group1 and member of Group2.
Device3 is member of Group1.
Group1 and Group2 have a Membership type of Assigned.
Exclusion takes precedence over inclusion in the following same group type scenarios.
Reference: <https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments>

QUESTION 4

You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.
To what should you grant the right to create the computer objects?

- A. Server2
- B. Server1
- C. GroupA
- D. DC1

Correct Answer: C

Section:

Explanation:

QUESTION 5

Which user can enroll Device6 in Intune?

- A. User4 and User2 only
- B. User4 and User 1 only
- C. User1, User2, User3, and User4
- D. User4. User Land User2 only

Correct Answer: C

Section:

QUESTION 6

HOTSPOT

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:

Answer Area	Statements	Yes	No
	If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	<input type="radio"/>	<input type="radio"/>
	If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<input type="radio"/>	<input type="radio"/>
	If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	<input type="radio"/>	<input type="radio"/>

Answer Area:



Answer Area	Statements	Yes	No
	If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	<input checked="" type="radio"/>	<input type="radio"/>
	If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<input type="radio"/>	<input checked="" type="radio"/>
	If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 7

Which users can purchase and assign App1?

- A. User3 only
- B. User1 and User3 only
- C. User1, User2, User3, and User4
- D. User1, User3, and User4 only
- E. User3 and User4 only

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business>

<https://docs.microsoft.com/en-us/microsoft-store/assign-apps-to-employees>



QUESTION 8

HOTSPOT

You implement the planned changes for Connection1 and Connection2

How many VPN connections will there be for User1 when the user signs in to Device1 and Device2?

To answer select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Hot Area:

Answer Area

Device1:

1
2
3
4
5

Device2:

1
2
3
4
5

Answer Area:

Answer Area

Device1:

1
2
3
4
5

Device2:

1
2
3
4
5

Vdumps

Section:

Explanation:

QUESTION 9

HOTSPOT

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

Device1 is marked as compliant.

Device4 is marked as compliant.

Device5 is marked as compliant.

Answer Area:

Statements	Yes	No
Device1 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device5 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 10

HOTSPOT

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
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

Case 02 - Azure DevOps

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements.

When you are ready to answer a question, click the Question button to return to the question.

Existing Environment

Current Business Model

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11:00 to 22:00. Litware has a Microsoft System Center 2012 R2 Configuration Manager deployment. During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Configuration Manager	Hybrid Azure AD-joined
Research	10	Configuration Manager	Hybrid Azure AD-joined
HR	8.1	Configuration Manager	Hybrid Azure AD-joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps is being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements

Business Goals

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements

Litware identifies the following device management requirements:

Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.

Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements

Litware identifies the following technical requirements for the planned deployment:

Re-provision the sales department computers by using Windows AutoPilot.

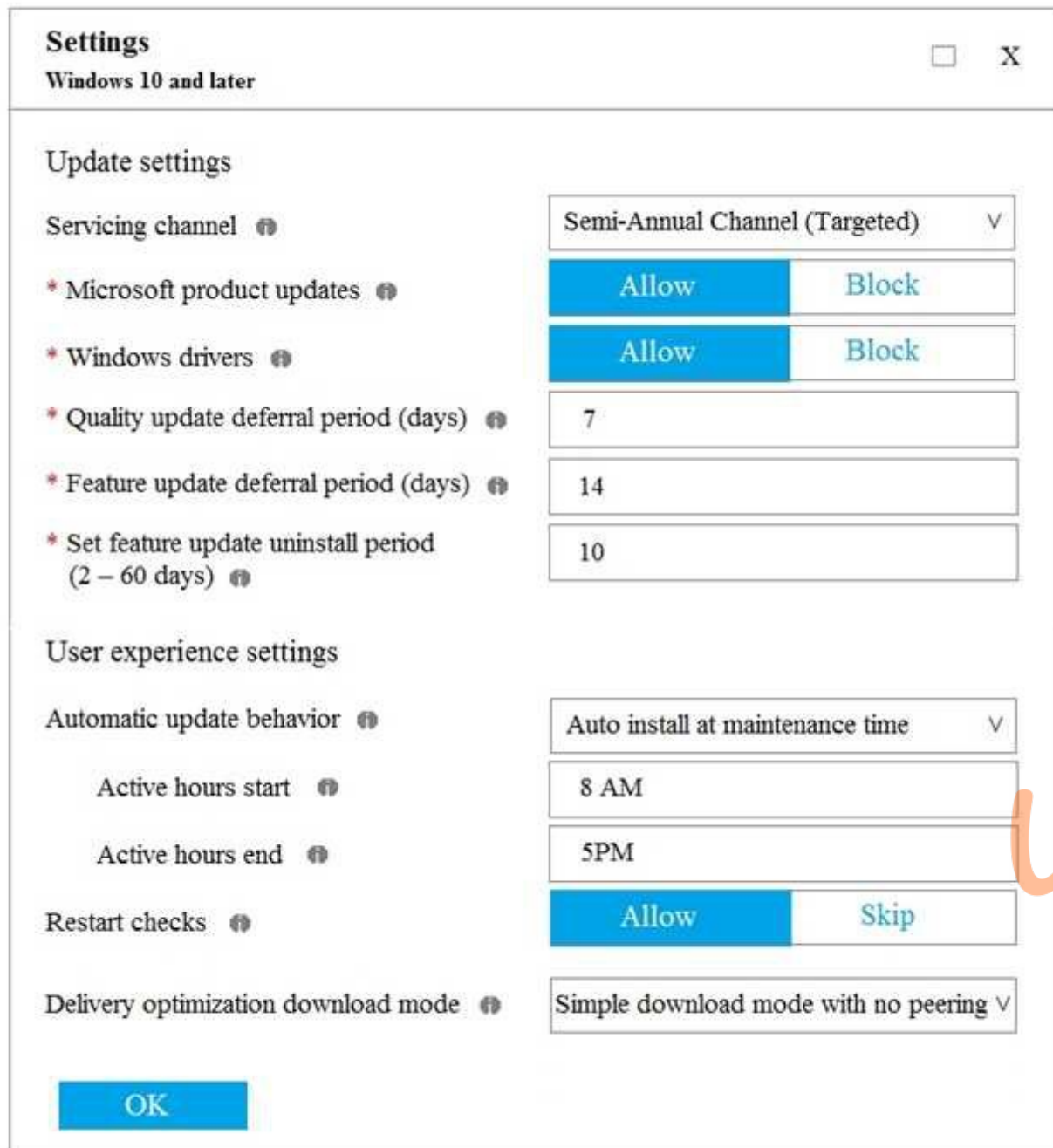
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.

Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits





QUESTION 1

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

Section:

Explanation:

Reference:

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

QUESTION 2

HOTSPOT

You need to recommend a solution to meet the device management requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

For the Research department employees:

<input type="checkbox"/>	An app configuration policy
<input type="checkbox"/>	An app protection policy
<input type="checkbox"/>	Azure information Protection
<input type="checkbox"/>	iOS app provisioning profiles

For the Sales department employees:

<input type="checkbox"/>	An app configuration policy
<input type="checkbox"/>	An app protection policy
<input type="checkbox"/>	Azure information Protection
<input type="checkbox"/>	iOS app provisioning profiles

Answer Area:

For the Research department employees:

<input checked="" type="checkbox"/>	An app configuration policy
<input type="checkbox"/>	An app protection policy
<input type="checkbox"/>	Azure information Protection
<input type="checkbox"/>	iOS app provisioning profiles

For the Sales department employees:

<input type="checkbox"/>	An app configuration policy
<input type="checkbox"/>	An app protection policy
<input checked="" type="checkbox"/>	Azure information Protection
<input type="checkbox"/>	iOS app provisioning profiles

Section:

Explanation:

Reference:

<https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md>

<https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-notforward-option-for-emails>

QUESTION 3

You need to capture the required information for the sales department computers to meet the technical requirements.

Which Windows PowerShell command should you run first?

- A. Install-Module WindowsAutoPilotIntune
- B. Install-Script Get-WindowsAutoPilotInfo

- C. Import-AutoPilotCSV
- D. Get-WindowsAutoPilotInfo

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices> "This topic describes how to convert Windows 7 or Windows 8.1 domain-joined computers to Windows 10 devices joined to either Azure Active Directory or Active Directory (Hybrid Azure AD Join) by using Windows Autopilot"

QUESTION 4

HOTSPOT

You need to meet the OOB requirements for Windows AutoPilot.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Overview

Getting started

Manage

Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Answer Area:



Overview

Getting started

Manage

Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings



Section:

Explanation:

Reference:

<https://blogs.msdn.microsoft.com/sgern/2018/10/11/intune-intune-and-autopilot-part-3-preparingyour-environment/>

<https://blogs.msdn.microsoft.com/sgern/2018/11/27/intune-intune-and-autopilot-part-4-enrollyour-first-device/>

QUESTION 5















HOTSPOT

You need to meet the technical requirements for Windows AutoPilot.

Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area















Manage	
	Users
	Groups
	Organizational relationships
	Roles and administrators
	Enterprise applications
	Devices
	App registrations
	Identity Governance
	Application proxy
	Licenses
	Azure AD Connect
	Custom domain names
	Mobility (MDM and MAM)
	Password reset

Answer Area:



Answer Area

Manage

 Users
 Groups
 Organizational relationships
 Roles and administrators
 Enterprise applications
 Devices
 App registrations
 Identity Governance
 Application proxy
 Licenses
 Azure AD Connect
 Custom domain names
 Mobility (MDM and MAM)
 Password reset



Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilotreset>

QUESTION 6

What should you upgrade before you can configure the environment to support co-management?

- A. the domain functional level
- B. Configuration Manager
- C. the domain controllers
- D. Windows Server Update Services (WSUS)

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/sccm/comange/tutorial-co-manage-clients>

QUESTION 7

You need to meet the device management requirements for the developers.
What should you implement?

- A. folder redirection
- B. Enterprise State Roaming
- C. home folders
- D. known folder redirection in Microsoft OneDrive

Correct Answer: B

Section:

Explanation:

Litware identifies the following device management requirements:

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.

Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roamingwindows-settings-reference>

QUESTION 8

HOTSPOT

You need to resolve the performance issues in the Los Angeles office.

How should you configure the update settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Change Delivery Optimization
download mode to:

<input type="checkbox"/>	Bypass mode
<input type="checkbox"/>	HTTP blended with internet peering
<input type="checkbox"/>	HTTP blended with peering behind same NAT
<input type="checkbox"/>	Simple download mode with no peering

Update Active Hours Start to:

<input type="checkbox"/>	10 AM
<input type="checkbox"/>	11 AM
<input type="checkbox"/>	10 PM
<input type="checkbox"/>	11 PM

Update Active Hours End to:

<input type="checkbox"/>	10 AM
<input type="checkbox"/>	11 AM
<input type="checkbox"/>	10 PM
<input type="checkbox"/>	11 PM

Answer Area:



Change Delivery Optimization
download mode to:

<input type="checkbox"/>	Bypass mode
<input type="checkbox"/>	HTTP blended with internet peering
<input checked="" type="checkbox"/>	HTTP blended with peering behind same NAT
<input type="checkbox"/>	Simple download mode with no peering

Update Active Hours Start to:

<input checked="" type="checkbox"/>	10 AM
<input type="checkbox"/>	11 AM
<input type="checkbox"/>	10 PM
<input type="checkbox"/>	11 PM

Update Active Hours End to:

<input type="checkbox"/>	10 AM
<input type="checkbox"/>	11 AM
<input type="checkbox"/>	10 PM
<input checked="" type="checkbox"/>	11 PM

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization>

<https://2pintsoftware.com/delivery-optimization-dl-mode/>

QUESTION 9

What should you configure to meet the technical requirements for the Azure AD-joined computers?

- A. Windows Hello for Business from the Microsoft Intune blade in the Azure portal.
- B. The Accounts options in an endpoint protection profile.
- C. The Password Policy settings in a Group Policy object (GPO).
- D. A password policy from the Microsoft Office 365 portal.

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hellomanage-inorganization>

Exam C

QUESTION 1

HOTSPOT

Your network contains an Active Directory domain. The domain contains 1,000 computers that run Windows 11.

You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:

- Prevent the sharing of clipboard contents.
- Ensure that users authenticate by using Network Level Authentication (NLA).

Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 2

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device1	64-bit version of Windows 10 Pro	Yes	No
Device2	32-bit version of Windows 10 Pro	No	Yes
Device3	64-bit version of Windows 10 Pro	No	Yes



You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11.

You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications.

Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Windows Autopilot: Device1 and Device3 only
None of the devices
Device1 only
Device1 and Device3 only
Device1, Device2, and Device3

In-place upgrade: Device1 and Device3 only
None of the devices
Device1 only
Device1 and Device3 only
Device1, Device2, and Device3

Answer Area:

Answer Area

Windows Autopilot: Device1 and Device3 only
None of the devices
Device1 only
Device1 and Device3 only
Device1, Device2, and Device3

In-place upgrade: Device1 and Device3 only
None of the devices
Device1 only
Device1 and Device3 only
Device1, Device2, and Device3

Section:

Explanation:

QUESTION 3

You have a Microsoft 365 tenant that contains the objects shown in the following table.

You are creating a compliance policy named Compliance1.

Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

- A. Group3 and Group4 only
- B. Group3, Group4, and Admin1 only
- C. Group1, Group2, and Group3 only
- D. Group1, Group2, Group3, and Group4 only
- E. Group1, Group2, Group3, Group4, and Admin1

Correct Answer: C

Section:

Explanation:

Reference:

<https://www.ravenswoodtechnology.com/microsoft-intune-compliance-notifications/>
<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

QUESTION 4

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1 @contoso.com.

You join a Windows 10 device named Client1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

net accounts
net localgroup
net user

Administrators /add "

AzureAD
CONTOSO
UPN

\user1@contoso.com"

Answer Area:

net accounts
net localgroup
net user

Administrators /add "

AzureAD
CONTOSO
UPN

\user1@contoso.com"

Section:

Explanation:

QUESTION 5

You have a Microsoft 365 subscription.

You need provide a user the ability to disable Security defaults and principle of least privilege.

Which role should you assign to the user?

- A. Global Administrator
- B. Conditional Access Administrator
- C. Security Administrator
- D. Intune Administrator

Correct Answer: B

Section:

Explanation:

To enable or disable security defaults in your directory, sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.

Note: Conditional Access Administrator

Users with this role have the ability to manage Azure Active Directory Conditional Access settings.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/conceptfundamentals-security-defaults>

QUESTION 6

DRAG DROP

You have 100 computers that run Windows 10.

You plan to deploy Windows 11 to the computers by performing a wipe and load installation.

You need to recommend a method to retain the user settings and the user data.

Which three actions should you recommend be performed 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
Configure known folder redirection in Microsoft OneDrive.	
Run scanstate.exe.	
Run loadstate.exe.	
Enable Enterprise State Roaming.	
Create a system image backup.	
Deploy Windows 11.	
Restore a system image backup.	

Correct Answer:

Actions	Answer Area
Configure known folder redirection in Microsoft OneDrive.	Create a system image backup.
Run scanstate.exe.	Deploy Windows 11.
Run loadstate.exe.	Restore a system image backup.
Enable Enterprise State Roaming.	

Section:

Explanation:

QUESTION 7

HOTSPOT

Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active Directory (Azure AD).

There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.

You plan to implement Microsoft Defender Exploit Guard.

You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Tool to use to configure the settings:

	▼
Security & Compliance in Microsoft 365	
Windows Security app	
Microsoft Endpoint Manager admin center	

Distribution method:

	▼
An Azure policy	
An Endpoint Protection configuration profile	
An Intune device compliance policy	
A device restrictions configuration profile	

Answer Area:

Tool to use to configure the settings:

	▼
Security & Compliance in Microsoft 365	
Windows Security app	
Microsoft Endpoint Manager admin center	

Distribution method:

	▼
An Azure policy	
An Endpoint Protection configuration profile	
An Intune device compliance policy	
A device restrictions configuration profile	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defenderatp/import-export-exploit-protection-emet-xml#manage-or-deploy-a-configuration>

<https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defenderatp/enable-exploit-protection>

QUESTION 8

Your company uses Microsoft Intune.

More than 500 Android and iOS devices are enrolled in the Intune tenant.

You plan to deploy new Intune policies. Different policies will apply depending on the version of Android or iOS installed on the device.

You need to ensure that the policies can target the devices based on their version of Android or iOS.

What should you configure first?

- A. groups that have dynamic membership rules in Azure AD
- B. Device categories in Intune
- C. Corporate device identifiers in Intune
- D. Device settings in Azure AD

Correct Answer: B

Section:

QUESTION 9

DRAG DROP

You have 500 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASLR) You need to configure a Windows 10 device that will be used to create a template file.

Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings.

Each protection area may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Protection areas

- Account protection
- App & browser control
- Device security
- Virus & threat protection

Answer Area

DEP:

Mandatory ASLR:

Correct Answer:

Protection areas

- Account protection
-
-
- Virus & threat protection

Answer Area

DEP:

Mandatory ASLR:

Section:

Explanation:

Exploit protection is a feature that helps protect against malware that uses exploits to infect devices and spread. Exploit protection consists of many mitigations that can be applied to either the operating system or individual apps1.

To configure a Windows 10 device that will be used to create a template file for Exploit protection, you need to configure the following protection areas on the device in the Windows Security app:

DEP: Device security. Data Execution Prevention (DEP) is a mitigation that prevents code from running in memory regions marked as non-executable. You can enable DEP system-wide or for specific apps in the Device security

section of the Windows Security app1.

Mandatory ASLR: App & browser control. Force randomization for images (Mandatory ASLR) is a mitigation that randomizes the location of executable images in memory, making it harder for attackers to predict where to inject code. You can enable Mandatory ASLR system-wide or for specific apps in the App & browser control section of the Windows Security app1.

QUESTION 10

You have an Azure AD tenant named contoso.com.

You have a workgroup computer named Computer1 that runs Windows 11.

You need to add Computer1 to contoso.com.

What should you use?

- A. dsreecmd.exe
- B. Computer Management
- C. netdom.exe
- D. the Settings app

Correct Answer: A

Section:

QUESTION 11

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage Windows 11 devices.

You need to implement passwordless authentication that requires users to use number matching Which authentication method should you use?

- A. Microsoft Authenticator
- B. voice calls
- C. FIDO2 security keys
- D. text messages

Correct Answer: A

Section:

QUESTION 12

You use a Microsoft Intune subscription to manage iOS devices.

You configure a device compliance policy that blocks jailbroken iOS devices.

You need to enable Enhanced jailbreak detection.

What should you configure?

- A. the Compliance policy settings
- B. the device compliance policy
- C. a network location
- D. a configuration profile

Correct Answer: D

Section:

QUESTION 13

DRAG DROP

You have a Microsoft 365 subscription that contains two users named User1 and User2. You need to ensure that the users can perform the following tasks:



- User1 must be able to create groups and manage users.
- User2 must be able to reset passwords for non-administrative users.

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Correct Answer:

Section:

Explanation:

Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the Microsoft 365 admin center. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers1.

To ensure that User1 can create groups and manage users, you should assign the User Administrator role to User1. This role allows User1 to create and manage all aspects of users and groups, including resetting passwords for non-administrative users1.

To ensure that User2 can reset passwords for non-administrative users, you should assign the Helpdesk Administrator role to User2. This role allows User2 to reset passwords, manage service requests, and monitor service health for non-administrative users1.

QUESTION 14

HOTSPOT

You have a Microsoft Intune subscription that has the following device compliance policy settings:

Mark devices with no compliance policy assigned as: Compliant Compliance status validity period (days): 14

On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:

Name: Policy1

Platform: Windows 10 and later

Require BitLocker: Require

Mark device noncompliant: 5 days after noncompliance

Scope (Tags): Tag1

Name: Policy2

Platform: Windows 10 and later

Firewall: Require

Mark device noncompliant: Immediately

Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

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
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>



Answer Area:

Statements	Yes	No
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On January 8, Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No

For the same reason as Box1.

Box 3: Yes

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.

The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

QUESTION 15

HOTSPOT

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have computers that run Windows 11 as shown in the following table.

Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

You create and assign the compliance policies shown in the following table.

Name	Configuration	Action for noncompliance	Assignment
Policy1	Require BitLocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Group1
Policy2	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group2

The next day, you review the compliance status of the computers.

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:

Answer Area

Statements	Yes	No
The compliance status of Computer1 is In grace period.	<input type="radio"/>	<input type="radio"/>
The compliance status of Computer2 is Compliant.	<input type="radio"/>	<input type="radio"/>
The compliance status of Computer3 is Not compliant.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
The compliance status of Computer1 is In grace period.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
The compliance status of Computer2 is Compliant.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
The compliance status of Computer3 is Not compliant.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Section:

Explanation:

QUESTION 16

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.

What should you configure?

- A. the Azure Monitor agent
- B. a device compliance policy
- C. a Conditional Access policy
- D. an Intune data collection policy

Correct Answer: D

Section:

QUESTION 17

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You use Windows Autopilot to deploy Windows 11 to devices.

A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.

You need to ensure that when a deployment fails, the deployment logs can be collected.

What should you configure?

- A. the automatic enrollment settings
- B. the Windows Autopilot deployment profile
- C. the enrollment status page (ESP) profile
- D. the device configuration profile

Correct Answer: B

Section:

QUESTION 18

You have a Microsoft 365 E5 subscription.



You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy. What should you select in the Microsoft Endpoint Manager admin center?

- A. Apps, and then App protection policies
- B. Apps, and then Monitor
- C. Devices, and then Monitor
- D. Reports, and the Device compliance

Correct Answer: A

Section:

Explanation:

App report: You can search by platform and app, and then this report will provide two different app protection statuses that you can select before generating the report. The statuses can be Protected or Unprotected.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-monitor>

QUESTION 19

HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Name	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
5	Group5	Name starts with COMP
Last	Ungrouped devices (default)	Not applicable

You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.



What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Computer1 will be a member of:

- Group3 only
- Group4 only
- Group5 only
- Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

- Group1 only
- Group2 only
- Group1 and Group2 only
- Group1, Group2, Group3, Group4, and Group5

Answer Area:

Answer Area

Computer1 will be a member of:

- Group3 only
- Group4 only
- Group5 only
- Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

- Group1 only
- Group2 only
- Group1 and Group2 only
- Group1, Group2, Group3, Group4, and Group5

Section:

Explanation:

QUESTION 20

HOTSPOT

You have a Microsoft 365 E5 subscription.

You create a new update rings policy named Policy1 as shown in the following exhibit.



Update ring settings [Edit](#)

Update settings

Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No

Set feature update uninstall period (2 - 60 days)

10

Servicing channel

General Availability channel

User experience settings

Automatic update behavior

Auto install at maintenance time

Active hours start

8 AM

Active hours end

5 PM

Restart checks

Allow

Option to pause Windows updates

Enable

Option to check for Windows updates

Enable

Change notification update level

Use the default Windows Update notifications

Use deadline settings

Allow

Deadline for feature updates

30

Deadline for quality updates

0

Grace period

0

Auto reboot before deadline

No



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point,

Answer:

Hot Area:

Answer Area

Updates that contain fixes and improvements to existing Windows functionality [answer choice].

- can be deferred for 30 days
- can be deferred indefinitely
- can be deferred for 30 days
- will be installed immediately

Updates that contain new Windows functionality will be installed within [answer choice] of release.

- 1 day
- 1 day
- 30 days
- 60 days

Answer Area:

Answer Area

Updates that contain fixes and improvements to existing Windows functionality [answer choice].

- can be deferred for 30 days
- can be deferred indefinitely
- can be deferred for 30 days
- will be installed immediately

Updates that contain new Windows functionality will be installed within [answer choice] of release.

- 1 day
- 1 day
- 30 days
- 60 days

Section:

Explanation:

*Updates that contain fixes and improvements to existing Windows functionality can be deferred for 30 days.

This is because the update rings policy named Policy1 has the "Quality updates deferral period (days)" setting set to 30. This means that quality updates, which include fixes and improvements to existing Windows functionality, can be deferred for up to 30 days from the date they are released by Microsoft. After 30 days, the devices will automatically install the quality updates. Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure>

*Updates that contain new Windows functionality will be installed within 60 days of release.

This is because the update rings policy named Policy1 has the "Feature updates deferral period (days)" setting set to 60. This means that feature updates, which include new Windows functionality, can be deferred for up to 60 days from the date they are released by Microsoft. After 60 days, the devices will automatically install the feature updates. Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure>

QUESTION 21

You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs. The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

- A. 1 only
- B. 2 and 3 only
- C. 1 and 3 only
- D. 1, 2, and 4 on
- E. 1, 2, 3, and 4

Correct Answer: E

Section:

Explanation:

All events from Windows event logs are collected in the Log Analytics workspace, regardless of the event level or source. Therefore, events 1, 2, 3, and 4 are all collected in the workspace. Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events>

QUESTION 22

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

- A. General
- B. Users and Accounts
- C. System security
- D. Device experience

Correct Answer: D

Section:

Explanation:

To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. Reference: <https://docs.microsoft.com/enus/mem/intune/configuration/device-restrictions-android-for-work#device-experience>

QUESTION 23

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.

You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.

What should you do?

- A. Onboard the macOS devices to the Microsoft Purview compliance portal.
- B. From the Microsoft Intune admin center, create a security baseline.
- C. Install Defender for Endpoint on the macOS devices.
- D. From the Microsoft Intune admin center, create a configuration profile.

Correct Answer: C

Section:

Explanation:

To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices. Reference: <https://docs.microsoft.com/en-us/windows/security/threatprotection/microsoft-defender-atp/mac-install-with-intune>



QUESTION 24

You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune. You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
- B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
- C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
- D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
- E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
- F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

Correct Answer: C, E

Section:

Explanation:

To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices. Reference: <https://docs.microsoft.com/enus/mem/intune/protect/endpoint-protection-windows-10>

QUESTION 25

You have an Azure AD group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile1 to Group1. You need to ensure that Profile1 applies to Device1 only. What should you modify in Profile1?

- A. Assignments
- B. Settings
- C. Scope (Tags)
- D. Applicability Rules

Correct Answer: D

Section:

Explanation:

To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1.

You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability rule that matches Device1's properties and excludes Device2's properties. Reference: <https://docs.microsoft.com/enus/mem/intune/configuration/device-profile-assign#applicability-rules>

QUESTION 26

DRAG DROP

You have a Microsoft 365 subscription that includes Microsoft Intune.

You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:

- Enforces compliance for Defender for Endpoint by using Conditional Access
- Prevents suspicious scripts from running on devices

What should you configure? To answer, drag the appropriate features to the correct requirements.

Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Features

- A device restriction policy
- A security baseline
- An attack surface reduction (ASR) rule
- An Intune connection

Answer Area

- Enforces compliance:
- Prevents suspicious scripts:

Correct Answer:

Features

- A device restriction policy
- A security baseline
-
-

Answer Area

- Enforces compliance: An Intune connection
- Prevents suspicious scripts: An attack surface reduction (ASR) rule



Section:

Explanation:

To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in

Defender for Endpoint. You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. Reference: <https://docs.microsoft.com/enus/windows/security/threat-protection/microsoft-defender-atp/conditional-access>

To prevent suspicious scripts from running on devices, you need to configure an attack surface reduction (ASR) rule in Intune. ASR rules are part of the endpoint protection settings that you can apply to devices by using device configuration profiles. You can use the ASR rule "Block Office applications from creating child processes" to prevent Office applications from launching child processes such as scripts or executables. Reference: <https://docs.microsoft.com/enus/mem/intune/protect/endpoint-protection-windows-10#attack-surface-reduction-asr-rules>

QUESTION 27

Your network contains an on-premises Active Directory domain and an Azure AD tenant.

The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

Which device configuration profile type template should you use?

- A. Administrative Templates
- B. Endpoint protection
- C. Device restrictions
- D. Custom

Correct Answer: A

Section:

Explanation:

To configure the settings shown in the table, you need to use the Administrative Templates device configuration profile type template. This template allows you to configure hundreds of settings that are also available in Group Policy. You can use this template to configure settings such as password policies, account lockout policies, and audit policies. Reference: <https://docs.microsoft.com/enus/mem/intune/configuration/administrative-templates-windows>

QUESTION 28

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.

Which three types of data can you collect from the computers by using Log Analytics? Each correct answer a complete solution.

NOTE: Each correct selection is worth one point.

- A. error events from the System log
- B. failure events from the Security log
- C. third-party application logs stored as text files
- D. the list of processes and their execution times
- E. the average processor utilization

Correct Answer: A, C, E

Section:

Explanation:

You can collect error events from the System log, third-party application logs stored as text files, and the average processor utilization from the computers by using Log Analytics. These are some of the types of data that you can collect by using data sources such as Windows event logs, custom logs, and performance counters. You cannot collect failure events from the Security log or the list of processes and their execution times by using Log Analytics. Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-overview>

QUESTION 29

You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

- A. an attack surface reduction (ASR) policy
- B. a security baseline
- C. an endpoint detection and response (EDR) policy
- D. an account protection policy
- E. an antivirus policy

Correct Answer: C

Section:

Explanation:

To onboard the devices to Microsoft Defender for Endpoint, you need to create an endpoint detection and response (EDR) policy in the Microsoft Intune admin center. This policy enables EDR capabilities on devices that are enrolled in Intune and allows you to configure various settings for EDR functionality. You can then assign the policy to groups of users or devices. Reference:



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

QUESTION 30

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in Intune.

Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

- A. From Platform Settings, set Android device administrator Personally Owned to Block.
- B. From Platform Settings, set Android Enterprise (work profile) to Allow.
- C. From Platform Settings, set Android device administrator Personally Owned to Allow
- D. From Platform Settings, set Android device administrator to Block.

Correct Answer: A, B

Section:

Explanation:

To ensure that only Android devices that use Android work profiles can enroll in Intune, you need to perform two configurations in the device enrollment restrictions. First, you need to set Android device administrator Personally Owned to Block. This prevents users from enrolling personal Android devices that use device administrator mode. Second, you need to set Android Enterprise (work profile) to Allow. This allows users to enroll corporate-owned or personal Android devices that use work profiles. Reference: <https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollmentrestrictions-set>

QUESTION 31

HOTSPOT

You have the device configuration profile shown in the following exhibit.



Kiosk

Windows 10 and later

Basics Configuration settings Assignments

Configure your devices to run in kiosk mode. Before you select a kiosk mode, review your app assignments in the Mobile Apps blade. Apps that you want to run in kiosk mode should be assigned to a Windows device. [Learn more about Windows kiosk mode.](#)

Select a kiosk mode *

User logon type *

Application type *

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. [Learn more about Microsoft Edge kiosk mode.](#)

Edge Kiosk URL *

Microsoft Edge kiosk mode type

Refresh browser after idle time

Specify Maintenance Window for App Restarts *

Maintenance Window Start Time

Maintenance Window Recurrence

 **Vdumps**

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Users [answer choice].

- cannot view the address bar in Microsoft Edge
- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com/

Windows 10 and later devices can have [answer choice].

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

Answer Area:

Answer Area

Users [answer choice].

- cannot view the address bar in Microsoft Edge
- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com/

Windows 10 and later devices can have [answer choice].

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

Section:

Explanation:

Users can only access URLs that start with https://contoso.com/

Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab the device configuration profile shown in the exhibit is a kiosk browser profile that configures

Microsoft Edge to run in kiosk mode. The profile has the following settings:

Kiosk mode: Enabled

Kiosk type: Multi-app

Allowed URLs: https://contoso.com/*

Address bar: Disabled

These settings mean that users can only access URLs that start with https://contoso.com/ and cannot view the address bar in Microsoft Edge. The kiosk type of Multi-app allows users to open multiple instances of Microsoft Edge, but each instance can only have a single tab. Therefore, users cannot access any URL, cannot view the address bar in Microsoft Edge, and can have multiple Microsoft Edge instances that each has a single tab. Reference: <https://docs.microsoft.com/enus/mem/intune/configuration/kiosk-settings#kiosk-browser-settings>

QUESTION 32

HOTSPOT

You have 100 Windows 10 devices enrolled in Microsoft Intune.

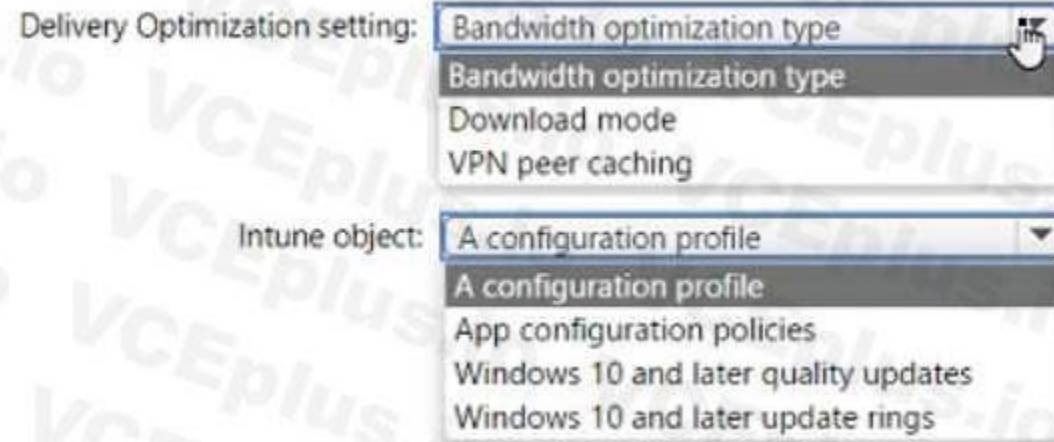
You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

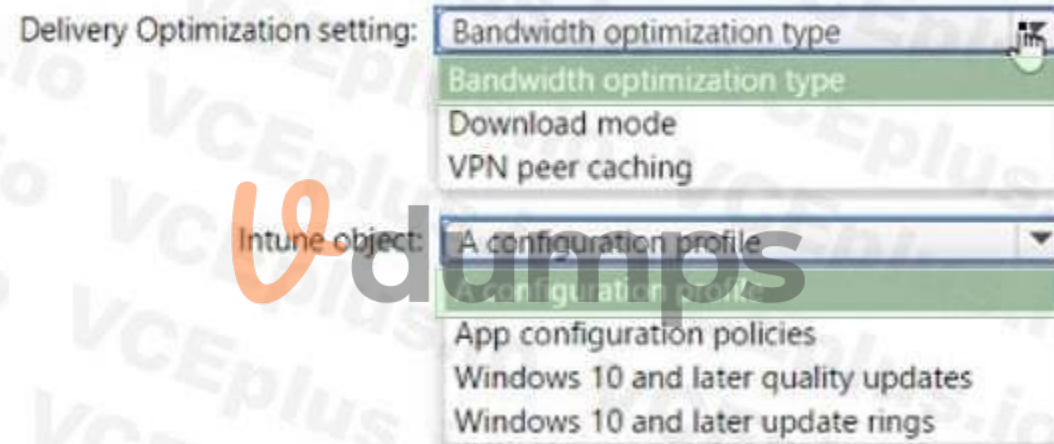
Hot Area:

Answer Area



Answer Area:

Answer Area



Section:

Explanation:

Delivery Optimization setting: B. Download mode Intune object: A configuration profile

To configure the devices to retrieve Windows updates from the internet and from other computers on a local network, you need to configure the Download mode setting in a Delivery Optimization device configuration profile. This setting specifies how the devices use Delivery Optimization to download updates. You can choose from several options, such as HTTP only, LAN only, or Group. For example, you can set the Download mode to Group and specify a group ID for the devices to share updates among themselves and with other devices that have the same group ID. You can also set the Download mode to Internet to allow the devices to download updates from Microsoft or other devices on the internet that use Delivery Optimization. Reference: <https://docs.microsoft.com/enus/mem/intune/configuration/delivery-optimization-windows>

QUESTION 33

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

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

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group1
Device3	iOS	Group2

From Intune, you create and send a custom notification named Notification1 to Group1.
 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
User1 receives Notification1 on Device1.	<input type="radio"/>	<input type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input type="radio"/>
User1 receives Notification1 on Device3.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
User1 receives Notification1 on Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User1 receives Notification1 on Device3.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications>

QUESTION 34

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

Section:**Explanation:**

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.

Sign in to the Microsoft Endpoint Manager admin center.

Select Reports > Intune Data warehouse > Data warehouse.

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

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

Open Power BI Desktop.

Choose File > Get Data. Select OData feed.

Choose Basic.

Type or paste the OData URL into the URL box.

Select OK.

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.

Select Organizational account.

Type your username and password.

Select Sign In.

Select Connect.

Select Load.

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

**QUESTION 35**

You have a Microsoft 365 E5 subscription and 25 Apple iPads.

You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method.

What should you do first?

- A. Upload a file that has the device identifiers for each iPad.
- B. Modify the enrollment restrictions.
- C. Configure an Apple MDM push certificate.
- D. Add your user account as a device enrollment manager (DEM).

Correct Answer: C**Section:****Explanation:**

Reference:

https://www.manageengine.com/mobile-devicemanagement/help/enrollment/mdm_creating_apns_certificate.html

Prerequisites for iOS enrollment Before you can enable iOS devices, complete the following steps:

Make sure your device is eligible for Apple device enrollment. Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority. Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS and macOS devices.

<https://docs.microsoft.com/en-gb/intune/enrollment/apple-mdm-push-certificate-get>

QUESTION 36

HOTSPOT

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD). The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements: The configuration must be managed from a central location. Internet traffic must be minimized. Costs must be minimized. How should you configure Windows Update? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Windows Update technology to use:

- | |
|--|
| Windows Server Update Services (WSUS) |
| Microsoft Endpoint Configuration Manager |
| Windows Update for Business |

Manage the configuration by using:

- | |
|--|
| A Group Policy object (GPO) |
| Microsoft Endpoint Configuration Manager |
| Microsoft Intune |

Manage the traffic by using:

- | |
|-----------------------|
| Delivery Optimization |
| BranchCache |
| Peer cache |

Answer Area:

Windows Update technology to use:

Windows Server Update Services (WSUS)
Microsoft Endpoint Configuration Manager
Windows Update for Business

Manage the configuration by using:

A Group Policy object (GPO)
Microsoft Endpoint Configuration Manager
Microsoft Intune

Manage the traffic by using:

Delivery Optimization
BranchCache
Peer cache

Section:

Explanation:

Box 1: Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.

Windows Server Update Services is a built-in server role that includes the following enhancements:

Can be added and removed by using the Server Manager

Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS

Etc.

Box 2: A Group Policy object

In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).

Box 3: BranchCache

BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them. BranchCache has two operating modes:

Distributed Cache mode and Hosted Cache mode.

Reference: <https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache>

<https://docs.microsoft.com/en-us/windows-server/administration/windows-server-updateservices/deploy/4-configure-group-policy-settings-for-automatic-updates>

QUESTION 37

You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices.

All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:

- Allow downloads from the internet and from other computers on the local network.
- Limit the percentage of used bandwidth to 50.

What should you use?

- A. a configuration profile
- B. a Windows Update for Business Group Policy setting
- C. a Microsoft Peer-to-Peer Networking Services Group Policy setting
- D. an Update ring for Windows 10 and later profile

Correct Answer: A

Section:

Explanation:

A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more.

A configuration profile is a template that contains one or more settings that you can apply to groups of devices. Reference:

Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn Delivery Optimization settings in Microsoft Intune

QUESTION 38

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Which groups can you add to Group4?

- A. Group2only
- B. Group1 and Group2 only
- C. Group2 and Group3 only
- D. Group1, Group2, and Group3

Correct Answer: C

Section:



QUESTION 39

DRAG DROP

You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:

- Requires BitLocker Drive Encryption (BitLocker) on each device
- Requires a minimum operating system version

Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point,

Select and Place:

Settings	Answer Area
Device Health	Requires BitLocker: <input type="text"/>
Device Properties	Requires a minimum operating system version: <input type="text"/>
Microsoft Defender for Endpoint	
System Security	

Correct Answer:

Settings

Device Health

Microsoft Defender for Endpoint

Answer Area

Requires BitLocker: System Security

Requires a minimum operating system version: Device Properties

Section:
Explanation:

QUESTION 40
 HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have the Windows 11 devices shown in the following table.

Name	Member of	BitLocker Drive Encryption (BitLocker)
Device1	Group1	Enabled
Device2	Group1, Group3	Disabled
Device3	Group1, Group2	Enabled

You deploy the device compliance policy shown in the exhibit. (Click the Exhibit tab.)



Basics [Edit](#)

Name Policy1

Description --

Platform Windows 10 and later

Profile type Windows 10/11 compliance policy

Compliance settings [Edit](#)

Device Health

Require BitLocker Require

Actions for noncompliance [Edit](#)

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Scope tags [Edit](#)

Default

Assignments [Edit](#)

Included groups

Group
Group1
Group3

Excluded groups

Group
Group2



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:

Answer Area

Statements

Device1 will have Policy1 assigned and will be marked as compliant.

Device2 will have Policy1 assigned and will be marked as compliant.

Device3 will have Policy1 assigned and will be marked as compliant.

Yes

No

Answer Area:

Answer Area

Statements

Device1 will have Policy1 assigned and will be marked as compliant.

Device2 will have Policy1 assigned and will be marked as compliant.

Device3 will have Policy1 assigned and will be marked as compliant.

Yes

No



Section:

Explanation:

QUESTION 41

DRAG DROP

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.

Which four 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

- Review the compliance dashboard for results.
- Create and assign a compliance policy that has System Security settings configured.
- Review the Conditional Access Insights and Reporting workbook for results.
- Create a PowerShell discovery script and a JSON file.
- Upload the PowerShell script to Intune.
- Upload the JSON file to Azure AD.
- Create and assign a custom compliance policy.



Answer Area



Correct Answer:

Actions

- Review the compliance dashboard for results.
- Create and assign a compliance policy that has System Security settings configured.
- Review the Conditional Access Insights and Reporting workbook for results.
-
-
-



Answer Area

- Create a PowerShell discovery script and a JSON file.
- Upload the PowerShell script to Intune.
- Upload the JSON file to Azure AD.
- Create and assign a custom compliance policy.



Section:

Explanation:

QUESTION 42

DRAG DROP

You have a computer that runs Windows 10 and contains two local users named User1 and User2.

You need to ensure that the users can perform the following actions:

- User 1 must be able to adjust the date and time.
- User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Groups

- Administrators
- Event Log Readers
- Performance Log Users
- Power Users
- System Managed Accounts Group

Correct Answer:

Groups

-
-
- Performance Log Users
- Power Users
- System Managed Accounts Group

Section:

Explanation:

QUESTION 43

HOTSPOT

You have an Azure AD tenant named contoso.com. You have the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

Which devices can be Azure AD joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



User1:

User2:

Answer Area



User1:

User2:



Answer Area

Azure AD joined:

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

Registered in contoso.com:

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

Answer Area:

Answer Area

Azure AD joined:

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

Registered in contoso.com:

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

Section:

Explanation:

QUESTION 44

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	None

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using user1@contoso.com.

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:

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 45

Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.

You enable Windows PowerShell remoting on the computers.

You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.

To which group should you add Admin1?

- A. Access Control Assistance Operators
- B. Remote Desktop Users
- C. Power Users
- D. Remote Management Users

Correct Answer: B

Section:

QUESTION 46

HOTSPOT

You have a Microsoft Intune subscription.

You are creating a Windows Autopilot deployment profile named Profile1 as shown in the following exhibit.

Create profile
Windows PC

Progress: 1 Basics, 2 **Out-of-box experience (OOBE)**, 3 Scope tags, 4 Assignments, 5 Review + create

Configure the out-of-box experience for your Autopilot devices

- * Deployment mode: User-Driven
- * Join to Azure AD as: Azure AD joined
- Microsoft Software License Terms: Hide
- Privacy settings: Hide
- The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. [Learn more](#)
- Hide change account options: Hide
- User account type: Standard
- Allow White Glove OOBE: No
- Apply device name template: No

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Hot Area:

Users who deploy a device by using Profile1
[answer choice].

	▼
are prevented from modifying any desktop settings	
can create additional local users on the device	
can modify the desktop settings for all device users	
can modify the desktop settings only for themselves	

Users can configure the [answer choice] during
the deployment.

	▼
computer name	
Cortana settings	
keyboard layout	

Answer Area:

Users who deploy a device by using Profile1
[answer choice].

	▼
are prevented from modifying any desktop settings	
can create additional local users on the device	
can modify the desktop settings for all device users	
can modify the desktop settings only for themselves	

Users can configure the [answer choice] during
the deployment.

	▼
computer name	
Cortana settings	
keyboard layout	

Section:

Explanation:

QUESTION 47

You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

- A. an app configuration policy
- B. a security baseline
- C. an app protection policy
- D. an iOS app provisioning profile

Correct Answer: C

Section:

Explanation:

An app protection policy is a set of rules that controls how data is accessed and handled by managed apps on mobile devices. App protection policies can prevent the printing of corporate data from managed apps on iOS devices by using the Restrict cut, copy, and paste with other apps setting. This setting can be configured to block printing from the iOS share menu. An app configuration policy is used to customize the behavior of a managed app, such as specifying a VPN profile or a web link. A security baseline is a collection of recommended security settings for Windows 10 devices that are managed by Intune. An iOS app provisioning profile is a file that contains information about the app's identity, entitlements, and distribution method.

QUESTION 48

You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

In the Microsoft Intune admin center, you are creating a Microsoft 365 Apps app named App1. To which objects can you assign App1?

- A. Group3 and Group4 only
- B. Admin1, Group3, and Group4 only
- C. Group1, Group3, and Group4 only
- D. Group1, Group2, Group3, and Group4 only
- E. Admin1, Group1, Group2, Group3, and Group4

Correct Answer: C

Section:

Explanation:

In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using device groups. In this scenario, the objects shown in the table are as follows:

Admin1 is an individual user account that belongs to the Global administrators role group.

Group1 is a user group that contains 100 users.

Group2 is a device group that contains 50 devices.

Group3 is a user group that contains 200 users.

Group4 is a device group that contains 150 devices.

Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment. Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

**QUESTION 49**

You have a Hyper-V host. The host contains virtual machines that run Windows 10 as shown in following table.

Name	Generation	Virtual TPM	Virtual processors	Memory
VM1	1	No	4	16 GB
VM2	2	Yes	2	4 GB
VM3	2	Yes	1	8 GB

Which virtual machines can be upgraded to Windows 11?

- A. VM1 only
- B. VM2 only
- C. VM2 and VM3 only
- D. VM1, VM2, and VM3

Correct Answer: C

Section:

Explanation:

Windows 11 has certain hardware requirements that must be met in order to upgrade from Windows 10. Some of these requirements are as follows:

A processor with at least 1 GHz clock speed and 2 cores.

A system firmware that supports UEFI and Secure Boot.

A Trusted Platform Module (TPM) version 2.0 or higher.

At least 4 GB of system memory (RAM).

At least 64 GB of storage space.

In this scenario, the virtual machines that run Windows 10 have the following specifications:

VM1 is a generation 1 virtual machine with no virtual TPM, 4 virtual processors, and 16 GB of memory.

VM2 is a generation 2 virtual machine with a virtual TPM, 2 virtual processors, and 4 GB of memory.

VM3 is a generation 2 virtual machine with a virtual TPM, 1 virtual processor, and 8 GB of memory.

VM1 cannot be upgraded to Windows 11 because it does not have a virtual TPM and it is not a generation 2 virtual machine. Generation 1 virtual machines do not support UEFI and Secure Boot, which are required for Windows 11. VM2 and VM3 can be upgraded to Windows 11 because they have a virtual TPM and they are generation 2 virtual machines. They also meet the minimum requirements for processor speed, cores, memory, and storage space.

QUESTION 50

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User1 uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1.

You need to identify what will occur when User1 next signs in to the devices.

What should you identify for each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

Device1: Will activate as Windows 11 Enterprise
 Will activate as Windows 11 Enterprise
 Will not upgrade to Windows 11 Enterprise
 Will perform a clean installation of Windows 11 Enterprise
 Will perform an in-place upgrade to Windows 11 Enterprise

Device2: Will not upgrade to Windows 11 Enterprise
 Will activate as Windows 11 Enterprise
 Will not upgrade to Windows 11 Enterprise
 Will perform a clean installation of Windows 11 Enterprise
 Will perform an in-place upgrade to Windows 11 Enterprise

Answer Area:

Answer Area

Device1:

- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Device2:

- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Section:

Explanation:

QUESTION 51

HOTSPOT

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share 1. You add Windows 10 images to Share 1 as shown in the following table.

Name	In WIM file	Description
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

 Vdumps

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

Answer Area:

Answer Area

Standard Client Task Sequence:  Image1, Image2, Image3, Image4, and Image5
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:  Image1, Image2, Image3, and Image4 only
Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Section:

Explanation:

QUESTION 52

RAG DROP

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to meet the following requirements during device provisioning:

* Display the progress of app and profile deployments.

* Join the devices to Azure AD.

What should you configure to meet each requirement? To answer drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Settings	Answer Area
CNAME Validation	Display the progress of app and profile deployments: <input type="text"/>
Co-management Settings	Join the devices to Azure AD: <input type="text"/>
Deployment Profiles	
Enrollment notifications	
Enrollment Status Page	

Correct Answer:

Settings	Answer Area
CNAME Validation	Display the progress of app and profile deployments: Enrollment Status Page
Co-management Settings	Join the devices to Azure AD: Deployment Profiles
Enrollment notifications	

Section:

Explanation:

QUESTION 53

Your company has a Remote Desktop Gateway (RD Gateway).

You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.

You need to configure a Remote Desktop connection to connect through the gateway.

Which setting should you configure?

- A. Connect from anywhere

- B. Server authentication
- C. Connection settings
- D. Local devices and resources

Correct Answer: A

Section:

Explanation:

To connect to a remote server through the RD Gateway, you need to configure the Connect from anywhere setting in the Remote Desktop Connection client. This setting allows you to specify the domain name and port of the RD Gateway server, as well as the authentication method. The other settings are not related to the RD Gateway connection. Reference: Configure Remote Desktop Connection Settings for Remote Desktop Gateway

QUESTION 54

DRAG DROP

Your network contains an Active Directory domain.

You install the Microsoft Deployment Toolkit (MDT) on a server.

You have a custom image of Windows 11.

You need to deploy the image to 100 devices by using MDT.

Which three actions should you perform in sequence? To answer, move answer area and arrange them in the correct order.

Select and Place:

Actions

- Enable multicast.
- Install Windows Deployment Services (WDS).
- Create a deployment share.
- Add the Windows 11 image.
- Create a task sequence.



Answer Area

Correct Answer:

Actions

- Enable multicast.
-
-
-
- Create a task sequence.



Answer Area

- Install Windows Deployment Services (WDS).
- Create a deployment share.
- Add the Windows 11 image.

Section:

Explanation:

Install Windows Deployment Services (WDS)

Create a deployment share.

Add the Windows 11 image.

QUESTION 55

You have the Microsoft Deployment Toolkit (MDT) installed.

You install and customize Windows 11 on a reference computer

You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.

Which command should you run before you capture the image?

- A. `dism`
- B. `wpeinit`
- C. `sysprep`
- D. `bcdedit`

Correct Answer: C

Section:

Explanation:

To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the `sysprep` command with the `/generalize` option. This option removes all unique system information from the Windows installation, such as the computer name, security identifier (SID), and driver cache. The other commands are not used for this purpose. Reference: Sysprep (Generalize) a Windows installation

QUESTION 56

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:

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

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

Section:

Explanation:

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
```

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/preparefor-windows-deployment-with-mdt>

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

QUESTION 57

DRAG DROP

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE_x64.iso image and connect to MDT1, the welcome screen appears as shown in the following exhibit.

You need to prevent the welcome screen from appearing when the computers connect to MDT1.



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
Modify the task sequence.	1
Replace the ISO image.	2
Modify the Bootstrap.ini file.	3
Modify the CustomSettings.ini file.	
Update the deployment share.	

Correct Answer:

Actions	Answer Area
Modify the task sequence.	1 Modify the Bootstrap.ini file.
Replace the ISO image.	2 Modify the CustomSettings.ini file.
	3 Update the deployment share.

Section:

Explanation:

Box 1: Modify the Bootstrap.ini file.

Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:

SkipBDDWelcome=YES

Box 2: Modify the CustomSettings.ini file.

SkipBDDWelcome

Indicates whether the Welcome to Windows Deployment wizard page is skipped.

For this property to function properly it must be configured in both CustomSettings.ini and

BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains

CustomSettings.ini) has been selected.

Box 3: Update the deployment share.

Reference: <https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages>

QUESTION 58

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. Personal
- B. Trusted Root Certification Authorities
- C. Client Authentication Issuers

Correct Answer: B

Section:

QUESTION 59

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	None
Device2	Windows 10	Joined	None
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured as shown in the following exhibit.



Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 1 Review + create

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	--



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

If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.

Yes

No

If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.

If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using

Answer Area:

Statements

If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.

Yes

No

If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.

If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using

Section:

Explanation:

Box 1: No

Device1 has no Mobile device Management (MDM) configured.

Note: Device1 is running Windows 8.1, and is registered, but not joined.

Device1 is in Group1.

Profile1 is assigned to Group1.

Box 2: No

Device2 has no Mobile device Management (MDM) configured.

Note: Device2 is running Windows 10, and is joined.

Device2 is in Group2.

Group2 is in Group1.

Profile1 is assigned to Group1.

Box 3: Yes

Device3 has Mobile device Management (MDM) configured.

Device3 is running Windows 10, and is joined

Device1 is in Group1.

Profile1 is assigned to Group1.

Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD,

Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations, policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.

Reference: <https://xo.xello.com.au/blog/windows-autopilot>

QUESTION 60

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 network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

QUESTION 61

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to manage Windows updates by using Intune.

You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.



User experience settings

Automatic update behavior ⓘ

Active hours start * ⓘ

Active hours end * ⓘ

Restart checks ⓘ Allow Skip

Option to pause Windows updates ⓘ Enable Disable

Option to check for Windows updates ⓘ Enable Disable

Change notification update level ⓘ

Use deadline settings ⓘ Allow Not configured

Deadline for feature updates ⓘ ✓

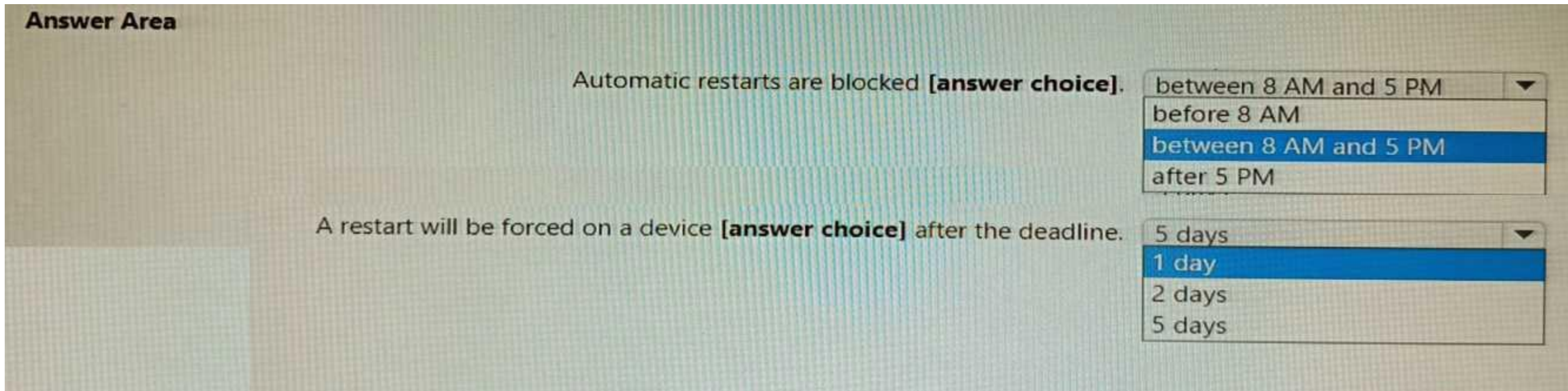
Deadline for quality updates ⓘ ✓

Grace period ⓘ ✓

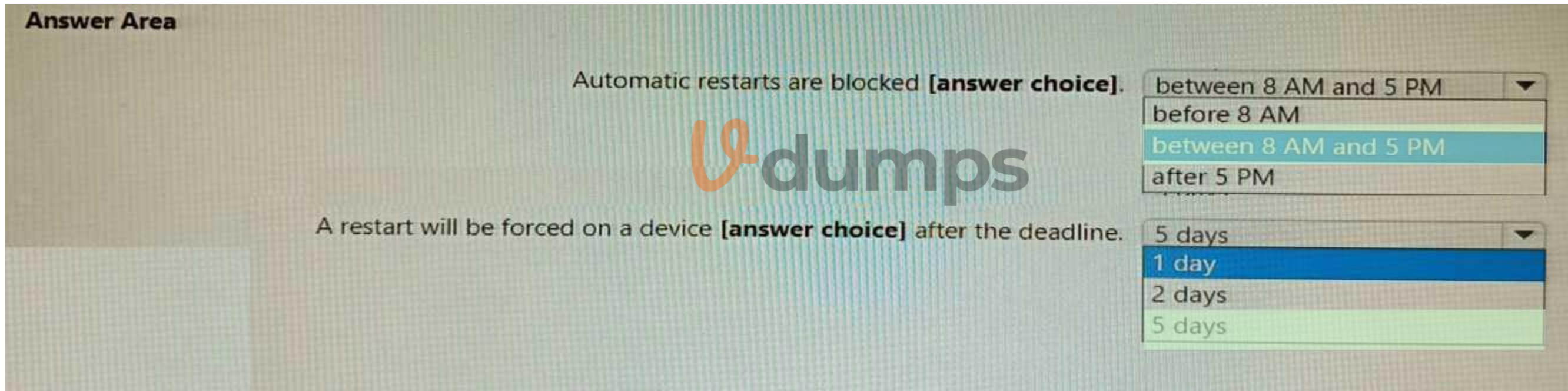
Auto reboot before deadline ⓘ Yes No

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 62

You have a Microsoft 365 tenant.

You have devices enrolled in Microsoft Intune.

You assign a conditional access policy named Policy1 to a group named Group1. Policy1 restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.

You need to identify which noncompliant devices attempt to access OneDrive for Business. What should you do?

- A. From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.
- B. From the Microsoft Intune admin center, review Device compliance report.
- C. From the Microsoft Intune admin center, review the Noncompliant devices report.
- D. From the Microsoft Intune admin center, review the Setting compliance report.

Correct Answer: C

Section:

QUESTION 63

HOTSPOT

You use Microsoft Endpoint Manager to manage Windows 10 devices.

You are designing a reporting solution that will provide reports on the following:

Compliance policy trends

Trends in device and user enrolment

App and operating system version breakdowns of mobile devices

You need to recommend a data source and a data visualization tool for the design.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Data source:

	▼
Audit logs in Azure Active Directory (Azure AD)	
Audit logs in Microsoft Intune	
Azure Synapse Analytics	
The Microsoft Intune Data Warehouse	

Data visualization tool:

	▼
Azure Data Studio	
Microsoft Power BI	
The Azure portal	

Answer Area:

Data source:

	▼
Audit logs in Azure Active Directory (Azure AD)	
Audit logs in Microsoft Intune	
Azure Synapse Analytics	
The Microsoft Intune Data Warehouse	

Data visualization tool:

	▼
Azure Data Studio	
Microsoft Power BI	
The Azure portal	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports>

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

QUESTION 64

Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10. You implement hybrid Azure AD and Microsoft Intune. You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort. What should you use?

- A. an Autodiscover address record
- B. a Group Policy object (GPO)
- C. an Autodiscover service connection point (SCP)
- D. a Windows Autopilot deployment profile

Correct Answer: D

Section:

QUESTION 65

HOTSPOT

You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group1, Group2

Windows 10 update rings are defined in Intune as shown in the following table.

Name	Quality deferral (days)	Assigned
Ring1	3	Yes
Ring2	10	Yes

You assign the update rings as shown in the following table.

Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Quality deferral on Computer1:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	

Quality deferral on Computer2:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	

Answer Area:

Quality deferral on Computer1:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	

Quality deferral on Computer2:

	▼
3 days	
7 days	
10 days	
13 days	
No effect	



Section:

Explanation:

Computer1 and Computer2 are members of Group1. Ring1 is applied to Group1.

Note: The term "Exclude" is misleading. It means that the ring is not applied to that group, rather than that group being blocked.

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-intune>

<https://allthingscloud.blog/configure-windows-update-business-using-microsoft-intune/>

QUESTION 66

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 configure an Intune device configuration profile to meet the following requirements:

Prevent Microsoft Office applications from launching child processes.

Block users from transferring files over FTP.

Which two settings should you configure in Endpoint protection? 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**

MD101 ✓

Description

Enter a description ✓

***Platform**

Windows 10 and later ✓

***Profile type**

Endpoint protection ✓

Settings >

Configure >

Scope (Tags)
0 scope(s) selected >

Endpoint protection
Windows 10 and later

Select a category to configure settings

- Windows Defender Application Gu...
11 settings available >
- Windows Defender Firewall
40 settings available >
- Windows Defender SmartScreen
2 settings available >
- Windows Encryption
37 settings available >
- Windows Defender Exploit Guard
20 settings available >
- Windows Defender Application Co...
2 settings available >
- Windows Defender Application Gua...
1 setting available >
- Windows Defender Security Center
14 settings available >
- Local device security options
46 settings available >
- Xbox services
5 settings available >

OK

Answer Area:

Answer Area

Create Profile

***Name**

MD101 ✓

Description

Enter a description ✓

***Platform**

Windows 10 and later ✓

***Profile type**

Endpoint protection ✓

Settings >

Configure >

Scope (Tags)
0 scope(s) selected >

Endpoint protection

Windows 10 and later

Select a category to configure settings

- Windows Defender Application Gu...
11 settings available >
- Windows Defender Firewall
40 settings available >
- Windows Defender SmartScreen
2 settings available >
- Windows Encryption
37 settings available >
- Windows Defender Exploit Guard
20 settings available >
- Windows Defender Application Co...
2 settings available >
- Windows Defender Application Gua...
1 setting available >
- Windows Defender Security Center
14 settings available >
- Local device security options
46 settings available >
- Xbox services
5 settings available >

OK

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

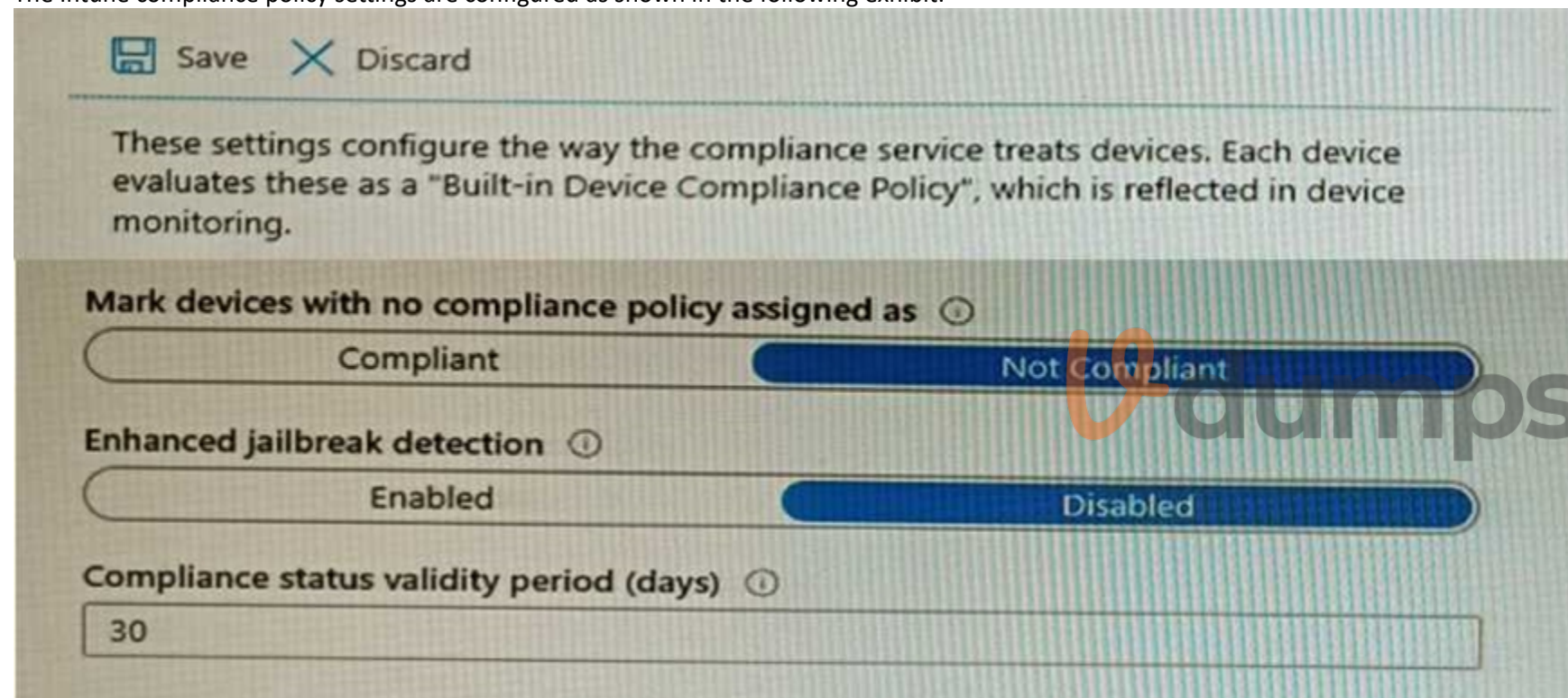
QUESTION 67

HOTSPOT

In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 and later	Require	Not applicable	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

The Intune compliance policy settings are configured as shown in the following exhibit.



On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	Group2

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
On June 4, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 6, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 9, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
On June 4, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On June 6, Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
On June 9, Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO.

Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until June 10th.

Source:

Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.

When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.

This action is supported on all platforms supported by Intune.

<https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance>

QUESTION 68

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices that run Windows 11.

User1 provides remote support for 75 devices in the marketing department.

You need to add User1 to the Remote Desktop Users group on each marketing department device.

What should you configure?

A. an app configuration policy

- B. a device compliance policy
- C. an account protection policy
- D. a device configuration profile

Correct Answer: D

Section:

QUESTION 69

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to deploy and manage Windows devices.

You have 100 devices from users that left your company.

You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

- A. Deploy a new configuration profile to the devices.
- B. Perform a Windows Autopilot reset on the devices.
- C. Perform an in-place upgrade on the devices.
- D. Perform a clean installation of Windows 11 on the devices.

Correct Answer: B

Section:

QUESTION 70

HOTSPOT

You create a Windows Autopilot deployment profile.

You need to configure the profile settings to meet the following requirements:

Automatically enroll new devices and provision system apps without requiring end-user authentication.

Include the hardware serial number in the computer name.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Create profile ...

Windows PC

✓ Basics **2 Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ ▼

Join to Azure AD as * ⓘ ▼

Microsoft Software License Terms ⓘ

i important information about hiding license terms

Privacy settings ⓘ

i The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. [Learn more](#)

Hide change account options ⓘ

User account type ⓘ

Allow White Glove OOBE ⓘ

Language (Region) ⓘ ▼

Automatically configure keyboard ⓘ

Apply device name template ⓘ

Answer Area:

Answer Area

Create profile ...

Windows PC

✓ Basics **2 Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ	User-Driven	▼
Join to Azure AD as * ⓘ	Azure AD joined	▼
Microsoft Software License Terms ⓘ	Show	Hide
i important information about hiding license terms		
Privacy settings ⓘ	Show	Hide
i The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more		
Hide change account options ⓘ	Show	Hide
User account type ⓘ	Administrator	Standard
Allow White Glove OOBE ⓘ	No	Yes
Language (Region) ⓘ	Operating system default	▼
Automatically configure keyboard ⓘ	No	Yes
Apply device name template ⓘ	No	Yes

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/autopilot/profiles>

QUESTION 71

You have a computer named Computer1 that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.

What should you do on Computer1?

- A. Turn on Reputation-based protection.
- B. Enable Network Level Authentication (NLA).
- C. Turn on Network Discovery.
- D. Configure the Remote Desktop Configuration service.

Correct Answer: B

Section:

QUESTION 72

You have a Hyper-V host that contains the virtual machines shown in the following table.

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

- A. VM1 only
- B. VM3only
- C. VM1 and VM2 only
- D. VM2 and VM3 only
- E. VM1, VM2, and VM3



Correct Answer: E

Section:

QUESTION 73

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have the devices shown in the following table.

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

- A. Device3 only
- B. Device2 and Device3 only

- C. Device 1 and Device2 only
- D. Device1, Device2, and Device3

Correct Answer: A

Section:

QUESTION 74

HOTSPOT

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

You add an Autopilot deployment profile as shown in the following exhibit.



Create profile

Windows PC

- ✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments **4** Review

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No

Language (Region)	Operating system default
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

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

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.

Hot Area:

Answer Area

Statements

	Yes	No
If you reset Device1, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If you reset Device2, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If you restart Device3, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>

Vdumps

Answer Area:

Answer Area

Statements

	Yes	No
If you reset Device1, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you reset Device2, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you restart Device3, the device will be deployed by using Autopilot.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 75

HOTSPOT

Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. Remote Desktop is enabled on Computer2. The domain contains the user accounts shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.

Name	Members
Group1	ADATUM\User2 ADATUM\User3
Group2	ADATUM\User2
Group3	ADATUM\User3
Administrators	ADATUM\Domain Admins ADATUM\User3
Remote Desktop Users	Group1

The relevant user rights assignments for Computer2 are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	Group3

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:

Answer Area		Yes	No
Statements			
User1 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>	
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>	
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>	

Answer Area:

Answer Area		
Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 76

You have two computers named Computer1 and Computer2 that run Windows 10. Computer2 has Remote Desktop enabled. From Computer1, you connect to Computer2 by using Remote Desktop Connection. You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session. What should you do?

- A. From Computer 2, configure the Remote Desktop settings.
- B. From Windows Defender Firewall on Computer 1, allow Remote Desktop.
- C. From Windows Defender Firewall on Computer 2, allow File and Printer Sharing.
- D. From Computer1, configure the Remote Desktop Connection settings.



Correct Answer: D

Section:

QUESTION 77

You have a Microsoft 365 subscription that uses Microsoft Intune. You have five new Windows 11 Pro devices. You need to prepare the devices for corporate use. The solution must meet the following requirements:

- Install Windows 11 Enterprise on each device.
- Install a Windows Installer (MSI) package named App1 on each device.
- Add a certificate named Certificate1 that is required by App1.
- Join each device to Azure AD.

Which three provisioning options can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. subscription activation
- B. a custom Windows image
- C. an in-place upgrade
- D. Windows Autopilot
- E. provisioning packages

Correct Answer: B, D, E

Section:

QUESTION 78

HOTSPOT

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

Name	Platform
Device1	Windows 10
Device2	macOS

In Microsoft Intune 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

Answer 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

Section:

Explanation:

QUESTION 79

HOTSPOT

Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.

The company purchases an Azure subscription.

You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.

What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Resource to create in Azure:

- An Azure event hub
- An Azure Log Analytics workspace
- An Azure SQL database
- An Azure Storage account

Configuration to perform on the computers:

- Configure the Event Collector service
- Create an event subscription
- Install the Microsoft Monitoring Agent

Answer Area:

Resource to create in Azure:

	▼
An Azure event hub	
An Azure Log Analytics workspace	
An Azure SQL database	
An Azure Storage account	

Configuration to perform on the computers:

	▼
Configure the Event Collector service	
Create an event subscription	
Install the Microsoft Monitoring Agent	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

QUESTION 80

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have an update ring named UpdateRing1 that contains the following settings:

- Automatic update behavior: Auto install and restart at a scheduled time
- Automatic behavior frequency: First week of the month
- Scheduled install day: Tuesday
- Scheduled install time: 3 AM

From the Microsoft Intune admin center, you select Uninstall for the feature updates of UpdateRing1.

When will devices start to remove the feature updates?

- A. when a user approves the uninstall
- B. as soon as the policy is received
- C. next Tuesday
- D. the first Tuesday of the next month

Correct Answer: C

Section:

QUESTION 81

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.

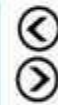
Select and Place:

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.

**Section:****Explanation:**

Reference:

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

QUESTION 82

Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer2 that run Windows 10.

You install Windows Admin Center on Computer1.

You need to manage Computer2 from Computer1 by using Windows Admin Center.

What should you do on Computer2?

- A. Update the TrustedHosts list
- B. Run the Enable-PSRemoting cmdlet
- C. Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.

D. Add an inbound Microsoft Defender Firewall rule.

Correct Answer: B

Section:

Explanation:

To manage a remote computer from Windows Admin Center, you need to enable PowerShell remoting on the remote computer. You can do this by running the Enable-PSRemoting cmdlet, which configures the WinRM service, creates a listener, and allows inbound firewall rules for PowerShell remoting. The other options are not sufficient or necessary for this task. Reference: Installation and configuration for Windows Remote Management

QUESTION 83

HOTSPOT

You have a hybrid Azure AD tenant.

You configure a Windows Autopilot deployment profile as shown in the following exhibit.

Create profile ...
Windows PC

Basics **2 Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode * ⓘ User-Driven

Join to Azure AD as * ⓘ Azure AD joined

Microsoft Software License Terms ⓘ Show Hide

Privacy settings ⓘ Show Hide

i The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.

Hide change account options ⓘ Show Hide

User account type ⓘ Administrator Standard

Allow pre-provisioned deployment ⓘ No Yes

Language (Region) ⓘ Operating system default

Automatically configure keyboard ⓘ No Yes

Apply device name template ⓘ No Yes

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To apply the profile to a new computer, you must first [answer choice].

- import a CSV file into Windows Autopilot
- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be [answer choice].

- joined to Active Directory and registered in Azure AD
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

Answer Area:

Answer Area

To apply the profile to a new computer, you must first [answer choice].

- import a CSV file into Windows Autopilot
- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be [answer choice].

- joined to Active Directory and registered in Azure AD
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

Section:

Explanation:

QUESTION 84

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You plan to create Windows 11 device builds for the marketing and research departments. The solution must meet the following requirements:

* Marketing department devices must support Windows Update for Business.

* Research department devices must have support for feature update versions for up to 36 months from release.

What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Hot Area:

Answer Area

Marketing:

Research:

Answer Area:

Answer Area

Marketing:

Research:

Section:

Explanation:

QUESTION 85

You have an Azure AD tenant named contoso.com.

You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

Name	Memory	TPM
Device1	16 GB	None
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

- A. Device2 only
- B. Device3 only
- C. Device2 and Devnce3 only
- D. Device 1, Device2, and Device3

Correct Answer: C

Section:

Explanation:

Windows Autopilot self-deploying mode requires devices that have a firmware-embedded activation key for Windows 10 Pro or Windows 11 Pro. This feature allows devices to automatically activate Windows Enterprise edition using the subscription license assigned to the user. Device1 does not have a firmware-embedded activation key, so it cannot use self-deploying mode. Device2 and Device3 have firmware-embedded activation keys for Windows 10 Pro, so they can use self-deploying mode. Reference: Windows Autopilot self-deploying mode (Public Preview), Deploy Windows Enterprise licenses

QUESTION 86

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains 100 client computers that run Windows 10.

Currently, your company does NOT have a deployment infrastructure.

The company purchases Windows 11 licenses through a volume licensing agreement.

You need to recommend how to upgrade the computers to Windows 11. The solution must minimize licensing costs.

What should you include in the recommendation?

- A. Microsoft Deployment Toolkit (MDT)
- B. Configuration Manager
- C. subscription activation
- D. Windows Autopilot

Correct Answer: A

Section:

QUESTION 87

You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.

You discover that Group Policy settings override the settings configured in Microsoft Intune policies.

You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings.

What should you do?

- A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
- B. From the Microsoft Intune admin center, create a custom device profile.
- C. From the Microsoft Intune admin center, create an Administrative Templates device profile.
- D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

Correct Answer: C

Section:

QUESTION 88

HOTSPOT

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.



Platform	Version
Android	8, 9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.

Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.

▼
Android enrollment
Apple enrollment
Corporate device identifiers
Device categories
Enrollment restrictions
Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment.

▼
Android enrollment
Apple enrollment
Corporate device identifiers
Device categories
Enrollment restrictions
Windows enrollment

Answer Area:

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

	▼
Android enrollment	
Apple enrollment	
Corporate device identifiers	
Device categories	
Enrollment restrictions	
Windows enrollment	

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

	▼
Android enrollment	
Apple enrollment	
Corporate device identifiers	
Device categories	
Enrollment restrictions	
Windows enrollment	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set>

<https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>



QUESTION 89

HOTSPOT

You have a Microsoft 365 ES subscription that uses Microsoft Intune. Devices are enrolled in Intune as shown in the following table.

Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

The devices are the members of groups as shown in the following table.

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

You create an IOS/iPadOS update profile as shown in the following exhibit.

Create profile ...

iOS/iPadOS

Basics Update policy settings Assignments Review + create

Summary

Basics

Name Profile1
Description --

Update policy settings

Update to install Install iOS/iPadOS Latest update
Schedule type Update outside of scheduled time
Time zone UTC±00
Time window

Start day	Start time	End day	End time
Monday	1 AM	Wednesday	1 PM
Friday	1 AM	Saturday	11 PM

Assignments

Included groups

Group	Group Members ⓘ
Group1	3 devices, 0 users

Excluded groups

Group	Group Members ⓘ
Group2	1 devices, 0 users

 Vdumps

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:

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 90

You have a Microsoft Intune deployment that contains the resources shown in the following table.

Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	Not applicable
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	Not applicable

You create a policy set named Set1 and add Comply1 to Set1.

Which additional resources can you add to Set1?

- A. Conf1 only
- B. Comply2 only
- C. Comply2 and Conf1 only
- D. CA1, Conf1, and Office 1 only
- E. Comply2, CA1, Conf1, and Office1

Correct Answer: B

Section:

QUESTION 91

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

- A. Microsoft Defender for Endpoint Power 81 app
- B. Microsoft Secure Score
- C. Endpoint Analytics
- D. Microsoft 365 Defender portal

Correct Answer: B

Section:

QUESTION 92

You have a Microsoft 365 subscription that has Windows 365 Enterprise licenses.

You plan to use a custom Windows 11 image as a template for Cloud PCs.

You have a Hyper-V virtual machine that runs Windows 11 and has the following configurations:

- * Name: VM1
- * Disk size: 64 GB
- * Disk format: VHDX
- * Disk type: Fixed size
- * Generation: Generation 2

You need to ensure that you can use VM1 as a source for the custom image. What should you do on VM1 first?

- A. Change the disk type to Dynamically expanding
- B. Change the disk format to the VHD
- C. Change the generation to Generation 1.
- D. Increase the disk size.

Correct Answer: B

Section:

QUESTION 93

DRAG DROP

Your on-premises network contains an Active Directory Domain Services (AD DS) domain.

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains five virtual machines and is NOT connected to the on-premises network.

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You purchase Windows 365 Enterprise licenses.

You need to deploy Cloud PC. The solution must meet the following requirements:

- * All users must be able to access their Cloud PC at any time without any restrictions.
- * The users must be able to connect to the virtual machines on VNet1.

How should you configure the provisioning policy for Windows 365? To answer, drag the appropriate options to the correct settings. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Select and Place:

Options

- Azure network connection
- Enterprise
- Frontline
- Microsoft Entra Hybrid Join
- Microsoft Entra Join
- Microsoft hosted network

Answer Area

Join type:

Network:

License type:

Correct Answer:

Options

-
-
- Frontline
-
- Microsoft Entra Join
- Microsoft hosted network

Answer Area

Join type: Microsoft Entra Hybrid Join

Network: Azure network connection

License type: Enterprise



Section:

Explanation:

QUESTION 94

DRAG DROP

Your company has a Microsoft 365 E5 tenant.

All the devices of the company are enrolled in Microsoft Intune.

You need to create advanced reports by using custom queries and visualizations from raw Microsoft Intune data.

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.

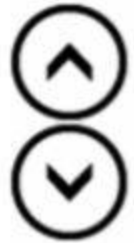
Select and Place:

Actions

- Install Microsoft Power BI Desktop.
- Create a Microsoft SharePoint Online site.
- Add a certificate connector to Microsoft Intune.
- Purchase an Azure subscription.
- Create a Log Analytics workspace.
- Add diagnostic settings.



Answer Area



Correct Answer:

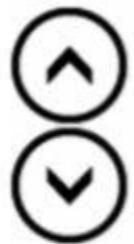
Actions

- Install Microsoft Power BI Desktop.
- Create a Microsoft SharePoint Online site.
- Add a certificate connector to Microsoft Intune.
-
-
-



Answer Area

- Purchase an Azure subscription.
- Create a Log Analytics workspace.
- Add diagnostic settings.



Section:

Explanation:

- Purchase an Azure subscription.
- Create a Log Analytics workspace.
- Add diagnostic settings.

QUESTION 95

You manage 1,000 computers that run Windows 10. All the computers are enrolled in Microsoft Intune. You manage the servicing channel settings of the computers by using Intune. You need to review the servicing status of a computer. What should you do?

- A. From Software updates, view the Per update ring deployment state.
- B. From Software updates, view the audit logs.
- C. From Device configuration - Profiles, view the device status.
- D. From Device compliance, view the device compliance.

Correct Answer: A
Section:

