

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 license.

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 **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

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

User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.

Yes No

User2 can remove D:\Folder1 from the list of protected folders on Device2.

User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.

Section:

Explanation:

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

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
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:

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="checkbox"/>	<input type="checkbox"/>
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
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="checkbox"/>	<input checked="" type="checkbox"/>

Section:

Explanation:

QUESTION 5

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 6

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

Section:

Explanation:

QUESTION 7

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

User1:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

User2:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

Answer Area:

Answer Area

User1:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

User2:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

Section:

Explanation:

Reference:

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

QUESTION 8

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 9

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 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
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

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:

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

The screenshot shows the Windows Settings application for Windows 10 and later. The window title is "Settings" with a close button (X) and a maximize button (square). The subtitle is "Windows 10 and later".

Update settings

- Servicing channel: Semi-Annual Channel (Targeted) (dropdown menu)
- * Microsoft product updates: Allow (selected), Block
- * Windows drivers: Allow (selected), Block
- * Quality update deferral period (days): 7
- * Feature update deferral period (days): 14
- * Set feature update uninstall period (2 – 60 days): 10

User experience settings

- Automatic update behavior: Auto install at maintenance time (dropdown menu)
- Active hours start: 8 AM
- Active hours end: 5PM
- Restart checks: Allow (selected), Skip
- Delivery optimization download mode: Simple download mode with no peering (dropdown menu)

At the bottom left, there is a blue "OK" button.

QUESTION 1

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 2

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>

QUESTION 3

HOTSPOT

You need to meet the OOBE 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:

The logo for 'Vdumps' features a stylized orange 'V' followed by the word 'dumps' in a grey, lowercase, sans-serif font.

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 4

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 5

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 6

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 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 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

Answer Area:

For the Research department employees:

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

For the Sales department employees:

<input checked="" type="checkbox"/>
An app configuration policy
An app protection policy
Azure information Protection
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 7

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 8

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 9

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>

Exam C

QUESTION 1

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 2

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 Computer1?



- 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 3

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

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

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

Deployment mode *	<input type="text" value="User-Driven"/>
Join to Azure AD as *	<input type="text" value="Azure AD joined"/>
Microsoft Software License Terms	<input type="radio"/> Show <input checked="" type="radio"/> Hide
Privacy settings	<input type="radio"/> Show <input checked="" type="radio"/> 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	<input type="radio"/> Show <input checked="" type="radio"/> Hide
User account type	<input type="radio"/> Administrator <input checked="" type="radio"/> Standard
Allow pre-provisioned deployment	<input checked="" type="radio"/> No <input type="radio"/> Yes
Language (Region)	<input type="text" value="Operating system default"/>
Automatically configure keyboard	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply device name template	<input checked="" type="radio"/> No <input type="radio"/> 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 4

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 5

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

- 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.



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 6

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 anions:

- 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

Answer Area



User1:

User2:

Correct Answer:

Groups

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

Answer Area



User1:

User2:



Section:

Explanation:

QUESTION 7

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 8

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 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"/>

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 9

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 10

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 11

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 12

DRAG DROP

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

You import a Windows 11 image to DS1.

You have an executable installer for an application named App1.

You need to ensure that App1 will be installed for all the task sequences that deploy the image.

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

- Modify a Windows 11 operating system setting.
- Modify a selection profile.
- Add App1 to DS1.
- Identify the GUID of App1.
- Modify CustomSettings.ini.

Answer Area

1

2

3

vdumps

Correct Answer:

Actions

- Modify a Windows 11 operating system setting.
- Modify a selection profile.
-
-
-

Answer Area

1 Add App1 to DS1.

2 Identify the GUID of App1.

3 Modify CustomSettings.ini.

Section:

Explanation:

MDT is a tool that allows you to automate the deployment of Windows operating systems and applications. To install an application for all the task sequences that deploy a Windows 11 image, you need to perform the following three actions in sequence:

Add App1 to DS1. You can use the Deployment Workbench to import the executable installer of App1 to a folder in your deployment share. This will create an application entry with a unique GUID that identifies App1. Identify the GUID of App1. You can find the GUID of App1 by opening the application properties in the Deployment Workbench and looking at the Application GUID field. You can copy the GUID to use it later. Modify CustomSettings.ini. You can edit the CustomSettings.ini file in your deployment share to specify which applications to install for each task sequence. You can use the Applications property to list the GUIDs of the applications you want to install, separated by commas. For example, if you want to install App1 and another application with GUID {1234-5678-90AB-CDEF}, you can use this line: Applications={GUID of App1},{1234-5678-90AB-CDEF}

These are the three actions you need to perform to ensure that App1 will be installed for all the task sequences that deploy the Windows 11 image from DS1. I hope this helps you.

If you want to learn more about MDT and how to deploy applications with it, you can check out these resources:

Get started with the Microsoft Deployment Toolkit (MDT) (Windows 10) How to deploy applications with the Microsoft Deployment Toolkit

QUESTION 13

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

The screenshot shows a hot spot question interface with two dropdown menus. The first dropdown is labeled "Azure AD joined:" and the second is labeled "Registered in contoso.com:". Both dropdowns have a list of options, with the first option in each dropdown selected and highlighted in grey. The options for "Azure AD joined:" are: Device1 and Device2 only, Device1 only, Device1 and Device2 only, Device1 and Device3 only, Device1, Device2, and Device3 only, and Device1, Device2, Device3, and Device4. The options for "Registered in contoso.com:" are: Device1 and Device2 only, Device1 and Device2 only, Device2 and Device3 only, Device3 and Device4 only, Device2, Device3, and Device4 only, and Device1, Device2, Device3, and Device4.

Answer Area:

Answer Area



Section:

Explanation:

QUESTION 14

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.

Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.

Admin2@contoso.com can install software on Computer1.

Answer Area:

Answer Area

Statements

Yes

No

User1@contoso.com is a member of the local Administrators group on Computer1.

Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.

Admin2@contoso.com can install software on Computer1.



Section:

Explanation:

QUESTION 15

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 16

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

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

* Join to Azure AD as

Microsoft Software License Terms Hide

Important information about hiding license terms

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 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:

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 17

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 18

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.	<div style="display: flex; flex-direction: column; align-items: center;"> > < </div>	1	<div style="display: flex; flex-direction: column; align-items: center;"> > < </div>
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.	<div style="display: flex; flex-direction: column; align-items: center;"> > < </div>	1	Modify the Bootstrap.ini file.	<div style="display: flex; flex-direction: column; align-items: center;"> > < </div>
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 19

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 20

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 21

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 22

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 23

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
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.



Answer Area



Correct Answer:

Actions
Configure known folder redirection in Microsoft OneDrive.
Run scanstate.exe.
Run loadstate.exe.
Enable Enterprise State Roaming.



Answer Area

Create a system image backup.
Deploy Windows 11.
Restore a system image backup.



Section:

Explanation:

QUESTION 24

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 25

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You have a device named Device1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Deploy the Remote Help app to Device1.
- B. Assign the Help Desk Operator role to User1.
- C. Assign the Intune Administrator role to User1.
- D. Assign a Microsoft 365 E5 license to User1.
- E. Rerun device onboarding on Device1.
- F. Assign the Remote Help add-on license to User1.

Correct Answer: A, B, F

Section:

QUESTION 26

You have a Windows 11 capable device named Device1 that runs the 64-bit version of Windows 10

Enterprise and has Microsoft Office 2019 installed. You have the Windows 11 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

Which images can be used to perform an in-place upgrade of Device1?

- A. image1 only
- B. Image2only
- C. Image1 and Image2

Correct Answer: B

Section:

QUESTION 27



HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant by using Azure AD Connect.

You use Microsoft Intune and Configuration Manager to manage devices.

You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:

- Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.
- Devices for The sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to The homes of the sales department users.
- Administrative effort must be minimized.

Which deployment method should you recommend 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

The screenshot shows a hot spot question interface with two dropdown menus. The first dropdown is labeled 'Sales:' and has 'Windows Autopilot with automatic registration' selected. The second dropdown is labeled 'Marketing:' and has 'Configuration Manager' selected. A large watermark 'VCEplus.io' is visible across the image.

Answer Area:

Answer Area

This screenshot is identical to the one above, but the selected options are highlighted in green to indicate they are the correct answers: 'Windows Autopilot with automatic registration' for Sales and 'Configuration Manager' for Marketing. A large watermark 'VCEplus.io' is visible across the image.

Section:

Explanation:

QUESTION 28

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.

You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.

What should you do first?

- A. Import an OS package.
- B. Create a selection profile.
- C. Add a Gather task to the task sequence.
- D. Add a Validate task to the task sequence.

Correct Answer: B

Section:

QUESTION 29

You have an on-premises server named Server1 that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

- A. Multipath I/O (MPIO)
- B. Multipoint Connector
- C. Windows Deployment Services (WDS)
- D. Windows Server Update Services (WSUS)

Correct Answer: C

Section:

QUESTION 30

Your company standardizes on Windows 10 Enterprise for all users.

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

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

- Ensure that any applications installed by the users are retained.
- Minimize user intervention.

What is the best recommendation to achieve the goal?

More than one answer choice may achieve the goal.

Select the BEST answer.

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

Correct Answer: A

Section:

QUESTION 31

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

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

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

Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings.

Does this meet the goal?

- A. Yes

B. No

Correct Answer: B

Section:

QUESTION 32

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

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

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

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 33

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

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

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

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 34

HOTSPOT

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



Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Enabled

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

You have a Conditional Access policy named CAPolicy1 that has the following settings:

- Assignments
 - o Users or workload identities: User 1. User1
 - o Cloud apps or actions: Office 365 Exchange Online

o Conditions: Device platforms: Windows, iOS

- Access controls

o Grant Require multi-factor authentication

You have a Conditional Access policy named CAPolicy2 that has the following settings:

Assignments

o Users or workload identities: Used, User2

o Cloud apps or actions: Office 365 Exch

o Conditions

- Device platforms: Android, iOS

- Filter for devices

- Device matching the rule: Exclude filtered devices from policy

- Rule syntax: device.displayName- contains "1"

- Access controls

- Grant Block access

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

Hot Area:

Answer Area

Statements	Yes	No
If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	<input type="radio"/>	<input type="radio"/>
If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 35

HOTSPOT

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.

How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Device1:

- Every 15 minutes for one hour, and then every eight hours
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Device2:

- Every 15 minutes for one hour, and then every eight hours
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Answer Area:

Device1:

- Every 15 minutes for one hour, and then every eight hours
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Device2:

- Every 15 minutes for one hour, and then every eight hours
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Section:

Explanation:

Box 1: Every three minutes for 15 minutes, then every 15 minutes for two hours, and then around every eight hours

If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:

Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Platform	Frequency
iOS/iPadOS	Every 15 minutes for 1 hour, and then around every 8 hours
macOS	Every 15 minutes for 1 hour, and then around every 8 hours
Android	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 10/11 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 8.1	Every 5 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Box 2: Every 15 minutes for one hour, and then every eight hours
 iOS/iPadOS: Every 15 minutes for 1 hour, and then around every 8 hours
 Reference: <https://docs.microsoft.com/en-us/mem/intune/configuration/device-profiletroubleshoot>

QUESTION 36

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. From the Microsoft Endpoint Manager admin center, create a configuration profile.
- B. From the Microsoft Endpoint Manager admin center, create a security baseline.
- C. Onboard the macOS devices to the Microsoft 365 compliance center.
- D. Install Defender for Endpoint on the macOS devices.



Correct Answer: D

Section:

Explanation:

Just install, and use Defender for Endpoint on Mac.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoftdefender-endpoint-mac>

QUESTION 37

HOTSPOT

You have the on-premises servers shown in the following table.

Name	Description
DC1	Domain controller that runs Windows Server 2022
Server1	Standalone server that runs Windows Server 2022
Server2	Member server that runs Windows Server 2022 and has the Remote Access role installed
Server3	Member server that runs Windows Server 2019
Server4	Red Hat Enterprise Linux (RHEL) 8.4 server

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.

You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.

To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

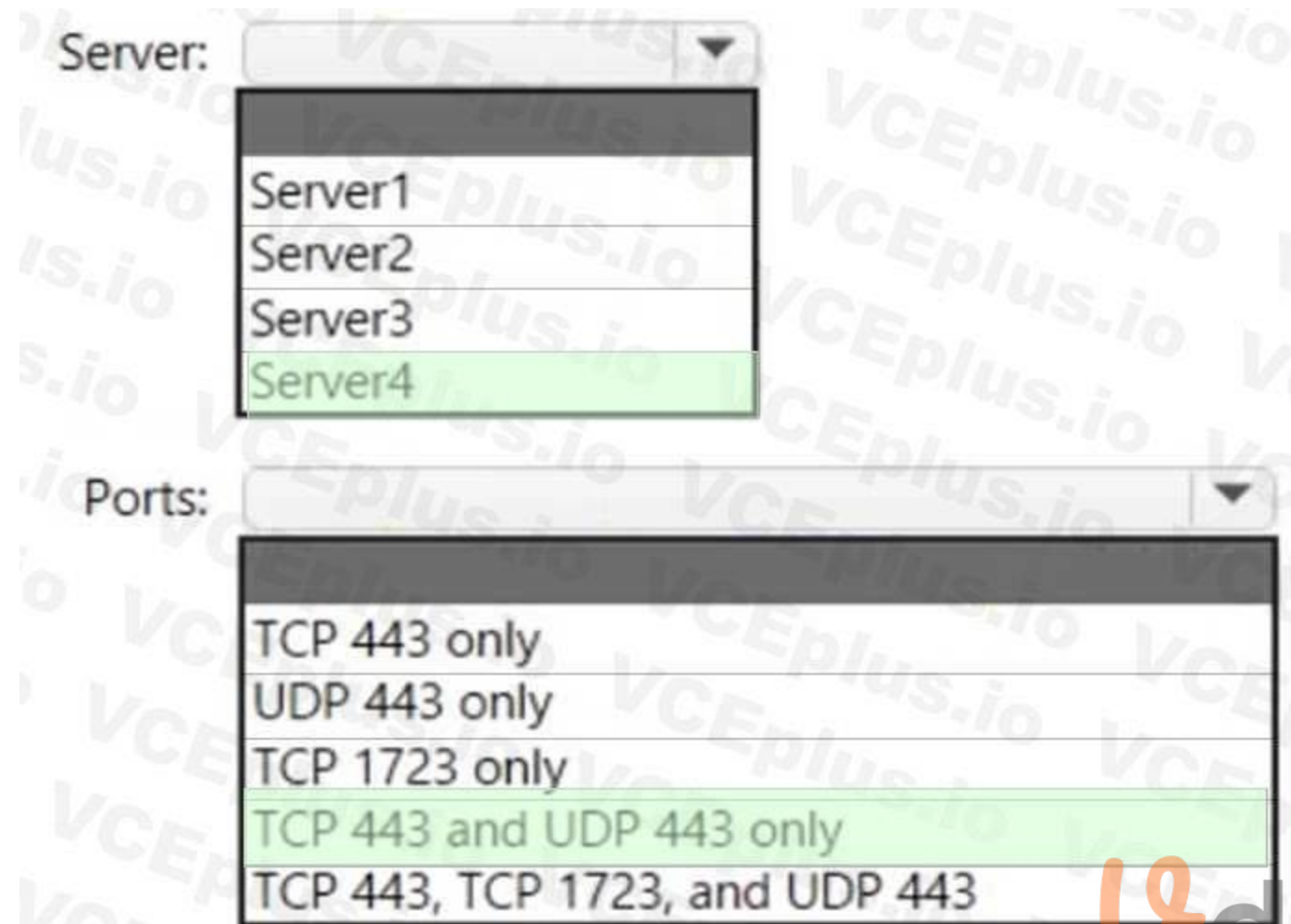
Hot Area:

Server:

Ports:

Answer Area:





Section:

Explanation:

Box 1: Server4

Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.

Box 2: TCP 443 and UDP 443 only

Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.

By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Saerver Configuration – Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.

Incorrect:

TCP 1723 is not used.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-overview>

QUESTION 38

HOTSPOT

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

MDM user scope: Group1

MAM user scope: 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

User1 can enroll Device1 in Intune by using automatic enrollment.

Yes

No

User1 can enroll Device2 in Intune by using automatic enrollment.

User2 can enroll Device1 in Intune by using automatic enrollment.

Answer Area:

Statements

User1 can enroll Device1 in Intune by using automatic enrollment.

Yes

No

User1 can enroll Device2 in Intune by using automatic enrollment.

User2 can enroll Device1 in Intune by using automatic enrollment.

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll>

<https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/>

QUESTION 39

Your company has devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

In Microsoft Endpoint Manager, you define the company's network as a location named Location1. Which devices can use network location-based compliance policies?

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

Correct Answer: E

Section:

Explanation:

Intune supported operating systems

Intune supports devices running the following operating systems (OS):

iOS

Android

Windows

macOS

Note: View the device compliance settings for the different device platforms:

Android device administrator

Android Enterprise

iOS

macOS

Windows Holographic for Business

Windows 8.1 and later

Windows 10/11

Reference: <https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devicesbrowsers>

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

QUESTION 40

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 41

HOTSPOT

You have a Microsoft 365 tenant and an internal certification authority (CA).

You need to use Microsoft Intune to deploy the root CA certificate to managed devices.

Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Policy type:

- App configuration policy
- App protection policy
- Compliance policy
- Configuration profile

Profile:

- Imported public key pair (PKCS) certificate
- Public key pair (PKCS) certificate
- Simple Certificate Enrollment Protocol (SCEP) certificate
- Trusted certificate

Answer Area:



Policy type:

App configuration policy
App protection policy
Compliance policy
Configuration profile

Profile:

Imported public key pair (PKCS) certificate
Public key pair (PKCS) certificate
Simple Certificate Enrollment Protocol (SCEP) certificate
Trusted certificate

Section:

Explanation:

Box 1: Configuration profile

Create a trusted certificate profile.

Box 2: Trusted certificate

When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices.

Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.

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

QUESTION 42

You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.

You plan to integrate Intune with Microsoft Defender for Endpoint.

You need to establish a service-to-service connection between Intune and Defender for Endpoint.

Which settings should you configure in the Microsoft Endpoint Manager admin center?

- A. Connectors and tokens
- B. Premium add-ons
- C. Microsoft Tunnel Gateway
- D. Tenant enrollment

Correct Answer: A

Section:

Explanation:

Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure

Right Now.

As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.
Reference: <https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/>

QUESTION 43

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.
You plan to use Endpoint analytics.
You need to create baseline metrics.
What should you do first?

- A. Create an Azure Monitor workbook.
- B. Onboard 10 devices to Endpoint analytics.
- C. Create a Log Analytics workspace.
- D. Modify the Baseline regression threshold.

Correct Answer: B

Section:

Explanation:

Onboarding from the Endpoint analytics portal is required for Intune managed devices.
Reference: <https://docs.microsoft.com/en-us/mem/analytics/enroll-intune>

QUESTION 44

DRAG DROP

You have a Microsoft 365 subscription that contains the devices shown in the following table.



Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. 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

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

- Device1: Setting
- Device2: Setting
- Device3: Setting

Correct Answer:

Settings

-
-
-
- Require Secure Boot to be enabled on the device.

Answer Area

- Device1: Require BitLocker.
- Device2: Prevent jailbroken devices from having corporate access.
- Device3: Prevent rooted devices from having corporate access.

Section:

Explanation:

Box 1:

Device Compliance settings for Windows 10/11 in Intune

There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.

Note: Windows Health Attestation Service evaluation rules

Require BitLocker:

Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user data. It also helps confirm that a computer isn't tampered with, even if it's left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.

Box 2: Prevent jailbroken devices from having corporate access

Device Compliance settings for iOS/iPadOS in Intune

There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.

Device Health

Jailbroken devices

Supported for iOS 8.0 and later

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Block - Mark rooted (jailbroken) devices as not compliant.

Box 3: Prevent rooted devices from having corporate access.

Device compliance settings for Android Enterprise in Intune

There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.

Device Health - for Personally-Owned Work Profile

Rooted devices

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Block - Mark rooted devices as not compliant.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-createtime>

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work>

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios>

QUESTION 45

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to perform the following tasks for User1:

Set the Usage location to Canada.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:



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

Answer Area:





Section:

Explanation:

QUESTION 46

You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune. You need to review the startup processes and how often each device restarts. What should you use?

- A. Endpoint analytics
- B. Intune Data Warehouse
- C. Azure Monitor
- D. Device Management

Correct Answer: B

Section:

QUESTION 47

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
Admin1	Application admin
Admin2	Cloud application admin
Admin3	Office apps admin
Admin4	Security admin

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization.
Which users can download the Office customization file from the admin center?

- A. Admin1, Admin2, Admin3. and Admin4
- B. Admin1, Admin2, and Admin3 only
- C. Admin3 only
- D. Admin3 and Admin4 only
- E. Admin1 and Admin3 only

Correct Answer: B

Section:

Explanation:

* Admin1

An application admin has full access to enterprise applications, applications registrations, and application proxy settings.

* Admin2

Mark your app as publisher verified.

In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.

* Admin3

Office Apps admin - Assign the Office Apps admin role to users who need to do the following:

- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health

Reference:

Office Apps admin - Assign the Office Apps admin role to users who need to do the following

<https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified>

QUESTION 48

HOTSPOT

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.



Create policy

- Basics
- Apps**
- Data protection
- Access requirements

Choose how you want to apply this policy to apps on different devices. Then add at least one app.

Target to apps on all device types Yes No

Device types *

Target policy to

i We'll continue to add managed apps to your policy as they become available in Intune. [View a list of apps that will be targeted](#)

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:

To apply Policy1 to an Android device, you must **[answer choice]**.

- install the Company Portal app on the device
- install the Microsoft Authenticator app on the device
- onboard the device to Microsoft Defender for Endpoint
- onboard the device to the Microsoft 365 compliance center

When Policy1 is assigned, the policy will apply to **[answer choice]**.

- users only
- devices only
- users and devices

Answer Area:

To apply Policy1 to an Android device, you must [answer choice].

- install the Company Portal app on the device
- install the Microsoft Authenticator app on the device
- onboard the device to Microsoft Defender for Endpoint
- onboard the device to the Microsoft 365 compliance center

When Policy1 is assigned, the policy will apply to [answer choice].

- users only
- devices only
- users and devices

Section:

Explanation:

Box 1: Install the Intune Company Portal app on the device

On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.

Box 2: Devices only

For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.

Reference: <https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#appprotection-policies-for-iosipados-and-android-apps>

QUESTION 49

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>

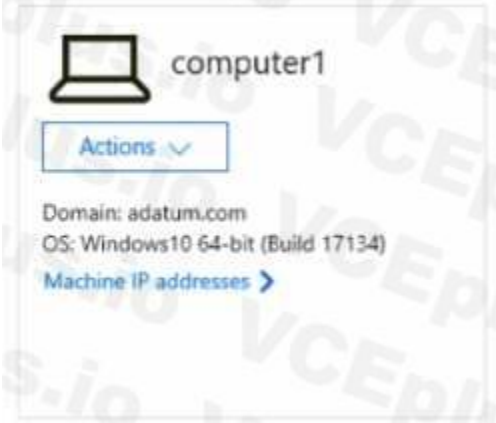
QUESTION 50

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 51

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 52

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 ⓘ ✓

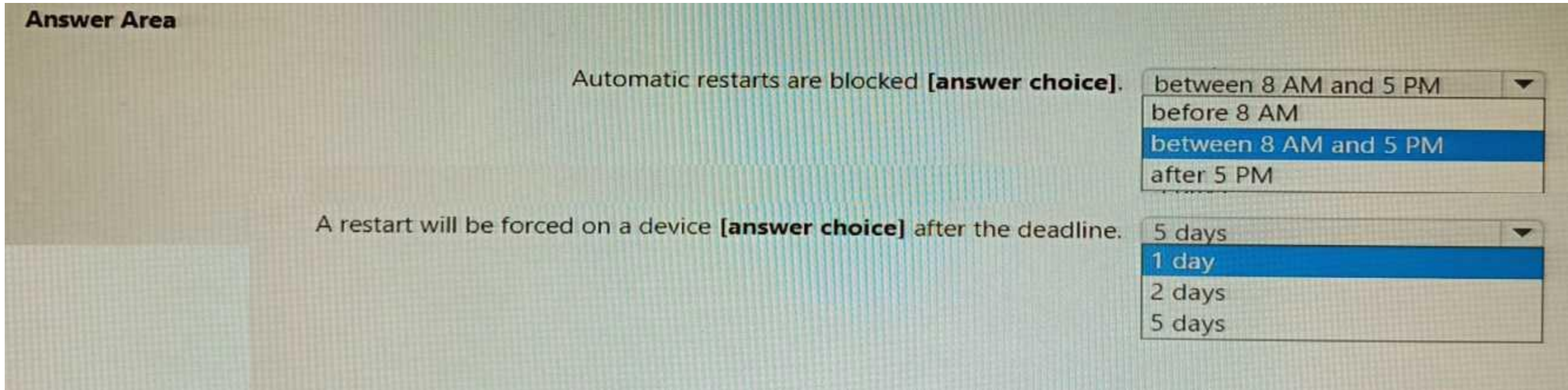
Deadline for quality updates ⓘ ✓

Grace period ⓘ ✓

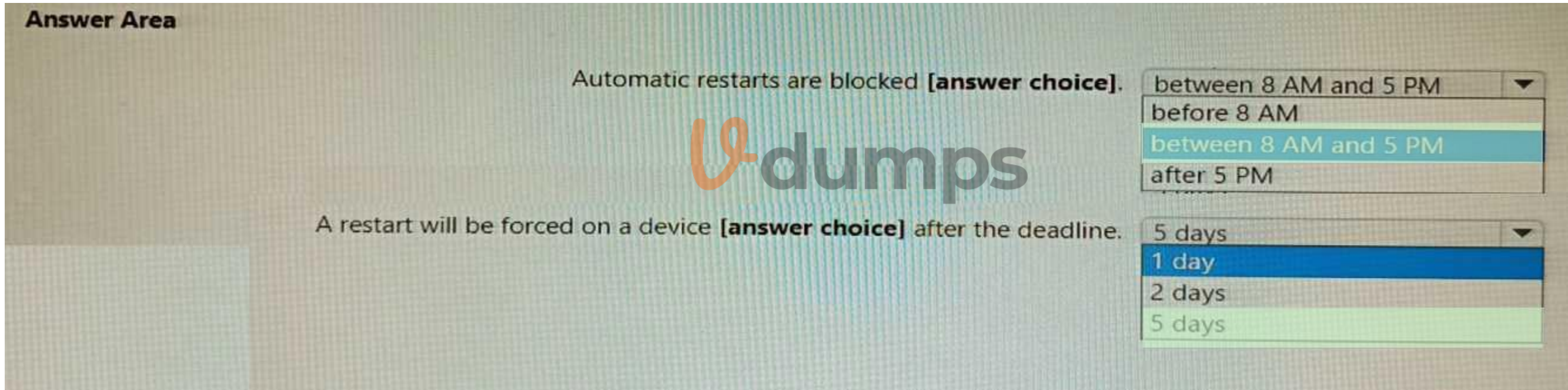
Auto reboot before deadline ⓘ Yes No

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 53

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 54

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 55

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 56

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 57

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 58

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 59

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 60

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>

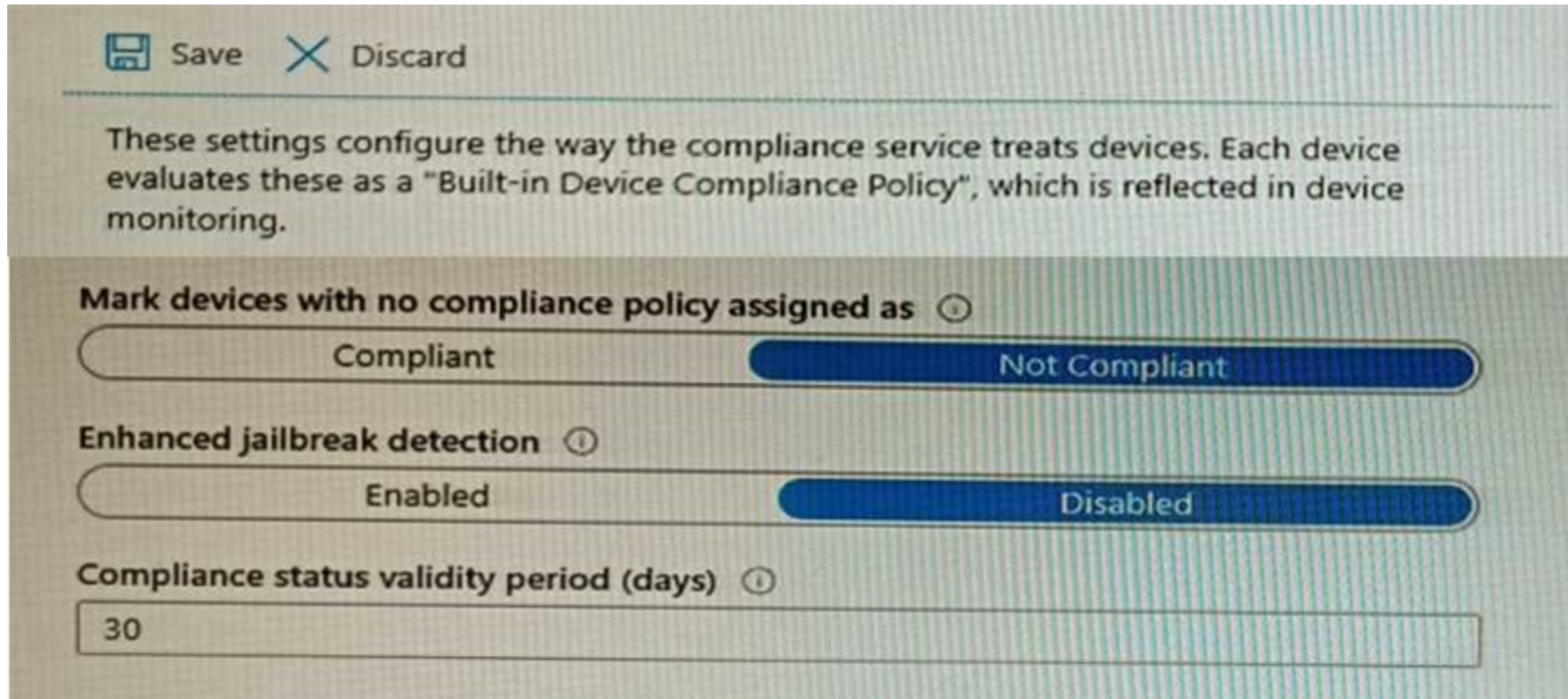
QUESTION 61

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	<i>Not applicable</i>	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:

Answer 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:

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 62

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 63

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 64

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 65

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 device, 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 66

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 67

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 68

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 69

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 70

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 71

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 72

HOTSPOT

You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.

MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

You use Distributed File System (DFS) Replication to replicate images in a share named Production.

You configure the following settings in the Bootstrap.ini file.




```
[Settings]
Priority=DefaultGateway, Default
```

```
[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London
```

```
[NewYork]
DeployRoot=\\MDT1\Production$
```

```
[NewYork]
DeployRoot=\\MDT1\Production$
```

```
[London]
DeployRoot=\\MDT2\Production$
KeyboardLocale=en-gb
```

```
[Default]
DeployRoot=\\MDT3\Production$
KeyboardLocale=en-us
```



You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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
TB1 will download the image from MDT3.	<input type="radio"/>	<input type="radio"/>
DT1 will have a KeyboardLocale of en-gb.	<input type="radio"/>	<input type="radio"/>
LT1 will download the image from MDT1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
TB1 will download the image from MDT3.	<input type="radio"/>	<input checked="" type="radio"/>
DT1 will have a KeyboardLocale of en-gb.	<input checked="" type="radio"/>	<input type="radio"/>
LT1 will download the image from MDT1.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 73

HOTSPOT

You have the devices shown in the following table.

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Seryer1 during the migration.

Which command should you run on 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: ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
Device2: LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
          LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
          ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
Device2: LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
          LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretkey"
          LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
          LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
          ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
```

Answer Area:

Answer Area

```
Device1: ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
Device2: LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
          LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
          ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
Device2: LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
          LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretkey"
          LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
          LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretkey"
          ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
          ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"
```

Section:

Explanation:

QUESTION 74

You have a Microsoft 365 subscription.
You plan to use Windows Autopilot to provision 25 Windows 11 devices.
You need to configure the Out-of-box experience (OOBE) settings.
What should you create in the Microsoft Intune admin center?

- A. an enrollment status page (ESP)
- B. a deployment profile
- C. a compliance policy
- D. a PowerShell script
- E. a configuration profile

Correct Answer: B

Section:

QUESTION 75

You have an Azure AD tenant that contains the devices shown in the following table.
You purchase Windows 11 Enterprise E5 licenses.

Name	App type
App1	Android store app
App2	Android line-of-business app
App3	Managed Google Play app

Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, Device3, and Device4

Correct Answer: B

Section:

QUESTION 76

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You add apps to Intune as shown in the following table.
You need to create an app configuration policy named Policy1 for the Android Enterprise platform.
Which apps can you manage by using Policy1?

- A. App2 only
- B. App3 only
- C. App1 and App3 only
- D. App2 and App3 only
- E. App1, App2, and App3

Correct Answer: D

Section:



QUESTION 77

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the users shown in the following table.

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1.

All the users use Microsoft Excel.

From the Microsoft Endpoint Manager admin center, you create the policies shown in the following table.

Name	Type	Priority	Assigned to	Default file format for Excel
Policy1	Policies for Office apps	0	Group1	OpenDocument Spreadsheet (*.ods)
Policy2	Policies for Office apps	1	Group2	Excel Binary Workbook (*.xlsb)

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



When User1 saves a new spreadsheet, the .ods format is used.

When User2 saves a new spreadsheet, the .xlsb format is used.

When User3 saves a new spreadsheet, the .xlsx format is used.

Answer Area:

Statements

Yes

No

When User1 saves a new spreadsheet, the .ods format is used.

When User2 saves a new spreadsheet, the .xlsb format is used.

When User3 saves a new spreadsheet, the .xlsx format is used.

Section:

Explanation:

Box 1: No User1 is member of Group1 and Group2.

Policy1 with priority 0 is assigned to Group1: default file format for Excel is.ods.

Policy2 with priority 1 is assigned to Group2: default file format for Excel is.xlsb.

Note: Key points to remember about policy order Policies are assigned an order of priority.

Devices receive the first applied policy only.

You can change the order of priority for policies.

Default policies are given the lowest order of priority.

Box 2: Yes User2 is member of Group2.

Group2 and Group3 are members of Group1.

Box 3: No User3 is member of Group3.

Group2 and Group3 are members of Group1.

Reference: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdbpolicy-order>



QUESTION 78

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

- Device enrollment type: Managed devices
- Profile Type: All Profile Types
- Platform: Android Enterprise

Which two types of apps can be associated with the policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Built-in Android app
- B. Managed Google Play store app
- C. Web link
- D. Android Enterprise system app
- E. Android store app

Correct Answer: B, D

Section:

QUESTION 79

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to ensure that you can deploy apps to Android Enterprise devices.

What should you do first?

- A. Create a configuration profile.
- B. Add a certificate connector.
- C. Configure the Partner device management settings.
- D. Link your managed Google Play account to Intune.

Correct Answer: D

Section:

QUESTION 80

You have a Microsoft 365 subscription.

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

To which devices can you deploy apps by using Intune?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, and Device3 only
- E. Device1, Device2, Device3, and Device4

Correct Answer: E

Section:

QUESTION 81

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices.

From the Microsoft Intune admin center, you add a Microsoft Store app.

Which two App information types are visible in the Company Portal?

NOTE: Each correct selection is worth one point.

- A. Privacy URL
- B. Information URL
- C. Developer
- D. Owner

Correct Answer: A, B

Section:

Explanation:

QUESTION 82

HOTSPOT

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to set a custom image as the wallpaper and sign-in screen.

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

NOTE: Each correct selection is worth one point.



Hot Area:



Answer Area

Device restrictions

Windows 10 and later

- ✓ Basics
- 2 Configuration settings**
- 3 Assignments
- 4 Applicability Rules
- 5 Review + create

✓ App Store

✓ Cellular and connectivity

✓ Cloud and Storage

✓ Cloud Printer

✓ Control Panel and Settings

✓ Display

✓ General

✓ Locked Screen Experience ✓

✓ Messaging

✓ Microsoft Edge Browser

✓ Network proxy

✓ Password

✓ Per-app privacy exceptions

✓ Personalization ✓

✓ Printer

✓ Privacy

✓ Projection

Previous

Next



Answer Area:



Answer Area

Device restrictions

Windows 10 and later

- ✓ Basics
- 2 Configuration settings**
- 3 Assignments
- 4 Applicability Rules
- 5 Review + create

✓ App Store

✓ Cellular and connectivity

✓ Cloud and Storage

✓ Cloud Printer

✓ Control Panel and Settings

✓ Display

✓ General

✓ Locked Screen Experience ✓

✓ Messaging

✓ Microsoft Edge Browser

✓ Network proxy

✓ Password

✓ Per-app privacy exceptions

✓ Personalization ✓

✓ Printer

✓ Privacy

✓ Projection

Previous

Next



Section:

Explanation:

QUESTION 83

You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to upgrade the computers to Windows 11 Enterprise. What should you configure in Intune?

- A. a device compliance policy
- B. a device cleanup rule
- C. a device enrollment policy
- D. a device configuration profile

Correct Answer: D

Section:

QUESTION 84

You have computers that run Windows 10 and are managed by using Microsoft Intune.

Users store their files in a folder named D:\Folder1.

You need to ensure that only a trusted list of applications is granted write access to D:\Folder1.

What should you configure in the device configuration profile?

- A. Microsoft Defender Exploit Guard
- B. Microsoft Defender Application Guard
- C. Microsoft Defender SmartScreen
- D. Microsoft Defender Application Control

Correct Answer: A

Section:

QUESTION 85

HOTSPOT

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

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

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

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









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

NOTE: Each correct selection is worth one point.

Hot Area:











Manage

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

Answer Area:

Manage

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

Section:

Explanation:

In the Antivirus policy settings, you can hide the Firewall and network protection area in the Windows Security app. Windows Hello for Business settings are configured in Identity protection.

Reference:

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

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

QUESTION 86

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune. Currently, Windows updates are downloaded without using Delivery Optimization. You need to configure the computers to use Delivery Optimization. What should you create in Intune?

A. a device compliance policy



- B. a Windows 10 update ring
- C. a device configuration profile
- D. an app protection policy

Correct Answer: C

Section:

QUESTION 87

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

You use Microsoft Intune to manage devices.

Auto-enrollment in Intune is configured.

You have 100 Windows 11 devices in a workgroup.

You need to connect the devices to the corporate wireless network and enroll 100 new Windows devices in Intune.

What should you use?

- A. a provisioning package
- B. a Group Policy Object (GPO)
- C. mobile device management (MDM) automatic enrollment
- D. a device configuration policy

Correct Answer: C

Section:

QUESTION 88

HOTSPOT

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
 LON-CL2	Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	Yes
 LON-CL4	Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Identified by Intune as a personal device:

▼
LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

▼
LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Answer Area:

Identified by Intune as a personal device:

▼
LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

▼
LON-CL2 only
LON-CL4 only
Both LON-CL2 and LON-CL4
Neither LON-CL2 or LON-CL4

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join>

<https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register>

QUESTION 89

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

You use Microsoft Intune to manage devices. All devices are in the same time zone.

You create an update rings policy and assign the policy to all Windows devices.

On the November 1, you pause the update rings policy.

All devices remain online.

Without further modification to the policy, on which date will the devices next attempt to update?

A. December 1

- B. December 6
- C. November 15
- D. November 22

Correct Answer: C

Section:

QUESTION 90

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

All devices have Microsoft Edge installed.

From the Microsoft Intune admin center, you create a Microsoft

You need to apply Edge1 to all the supported devices.

To which devices should you apply Edge1?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

Correct Answer: E

Section:

QUESTION 91

You have following types of devices enrolled in Microsoft Intune:

- Windows 10
- Android
- iOS For which types of devices can you create VPN profiles in Microsoft Intune admin center?

- A. Windows 10 only
- B. Windows 10 and Android only
- C. Windows 10 and iOS only
- D. Android and iOS only
- E. Windows 10, Android, and iOS

Correct Answer: E

Section:

QUESTION 92

You are creating a device configuration profile in Microsoft Intune

You need to configure specific OMA-URI settings in the profile.

Which profile type template should you use?

- A. Device restrictions (Windows 10 Team)
- B. Identity protection
- C. Custom
- D. Device restrictions



Correct Answer: C

Section:

QUESTION 93

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 94

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 no 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:

Roles

- Global Administrator
- Helpdesk Administrator
- Security Administrator
- User Administrator

Answer Area

User1:

User2:

Correct Answer:

Roles

- Global Administrator
- Helpdesk Administrator
- Security Administrator
- User Administrator

Answer AreaUser1: User2: **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 95**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 96

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 97

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 98

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 99

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 100

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:	<ul style="list-style-type: none">Will activate as Windows 11 EnterpriseWill activate as Windows 11 EnterpriseWill not upgrade to Windows 11 EnterpriseWill perform a clean installation of Windows 11 EnterpriseWill perform an in-place upgrade to Windows 11 Enterprise
Device2:	<ul style="list-style-type: none">Will not upgrade to Windows 11 EnterpriseWill activate as Windows 11 EnterpriseWill not upgrade to Windows 11 EnterpriseWill perform a clean installation of Windows 11 EnterpriseWill perform an in-place upgrade to Windows 11 Enterprise

Answer Area:

Answer Area

Device1:	<ul style="list-style-type: none">Will activate as Windows 11 EnterpriseWill activate as Windows 11 EnterpriseWill not upgrade to Windows 11 EnterpriseWill perform a clean installation of Windows 11 EnterpriseWill perform an in-place upgrade to Windows 11 Enterprise
Device2:	<ul style="list-style-type: none">Will not upgrade to Windows 11 EnterpriseWill activate as Windows 11 EnterpriseWill not upgrade to Windows 11 EnterpriseWill perform a clean installation of Windows 11 EnterpriseWill perform an in-place upgrade to Windows 11 Enterprise

Section:

Explanation:

QUESTION 101

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

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 102

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

CNAME Validation

Co-management Settings

Deployment Profiles

Enrollment notifications

Enrollment Status Page

Answer Area

Display the progress of app and profile deployments:

Join the devices to Azure AD:

Correct Answer:

Settings

CNAME Validation

Co-management Settings

Enrollment notifications

Answer Area

Display the progress of app and profile deployments:

Join the devices to Azure AD:

Section:

Explanation:

QUESTION 103

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 104

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.



Correct Answer:

Actions

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



Answer Area

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 105

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:
Windows 11 Enterprise
Windows 11 Pro
Windows 11 Pro for Workstations

Research:
Windows 11 Enterprise
Windows 11 Pro
Windows 11 Pro for Workstations

Answer Area:

Answer Area

Marketing:
Windows 11 Enterprise
Windows 11 Pro
Windows 11 Pro for Workstations

Research:
Windows 11 Enterprise
Windows 11 Pro
Windows 11 Pro for Workstations

Section:

Explanation:

QUESTION 106

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 Device3 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 107

HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft 365 subscription

You plan to use Windows Autopilot to deploy new Windows devices.

You plan to create a deployment profile.

You need to ensure that The deployment meets the following requirements:

- * Devices must be joined to AD DS regardless of their current working location.
- * Users in the marketing department must have a line-of-business (LOB) app installed during the deployment.

The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Devices must be joined to AD DS regardless of their current working location:

- Install the Intune connector for Active Directory.
- Deploy Always On VPN.
- Install the Intune connector for Active Directory.**
- Modify the Autopilot deployment profile.
- Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

- Modify the Autopilot deployment profile.
- Modify the Autopilot deployment profile.**
- Create a Microsoft Intune app deployment.
- Create a device configuration profile in Intune.

Answer Area:
Answer Area

Devices must be joined to AD DS regardless of their current working location:

- Install the Intune connector for Active Directory.
- Deploy Always On VPN.
- Install the Intune connector for Active Directory.**
- Modify the Autopilot deployment profile.
- Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

- Modify the Autopilot deployment profile.
- Modify the Autopilot deployment profile.**
- Create a Microsoft Intune app deployment.
- Create a device configuration profile in Intune.

Section:
Explanation:

QUESTION 108

HOTSPOT

You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.

Intune has the device compliance policies shown in the following table.

Name	Platform	Setting	Applied to
Compliance1	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	Group3

The Compliance policy settings are configured as shown in the exhibit. (Click the Exhibit tab.) You create the following Conditional Access policy:

- * Name: Policy1
- * Assignments
 - o Users and groups: User1
 - o Cloud apps or actions: Office 365 SharePoint Online
- * Access controls
 - o Grant Require device to be marked as compliant
- * Enable policy: On

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

User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.

Yes

No

User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.

User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.

Answer Area:

Answer Area

Statements

User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.

Yes

No

User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.

User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.

Section:

Explanation:

QUESTION 109

You have an Azure AD tenant named contoso.com.

You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.

What should you configure?

- A. Windows Autopilot
- B. provisioning packages for Windows
- C. Security defaults in Azure AD
- D. Device settings in Azure AD

Correct Answer: D

Section:

Explanation:

To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users. By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected1.

The other options are not relevant for this scenario because:

Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune. It does not control the local administrator role of the users who join the devices². Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users³.

Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role⁴.

QUESTION 110

You have an Azure subscription.

You have an on-premises Windows 11 device named Device 1.

You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription.

To what should you associate DCR1 ?

- A. Azure Network Watcher
- B. Device1
- C. a Log Analytics workspace
- D. a Monitored Object

Correct Answer: B

Section:

Explanation:

To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it. A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs¹. To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules². You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription³.

The other options are not correct for this scenario because:

Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources. It is not related to data collection rules or Azure Monitor⁴.

A Log Analytics workspace is a destination where you can send the data collected by a data collection rule. It is not an entity that you can associate a DCR with⁵.

A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules.

QUESTION 111

You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.

You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Enroll the devices in Microsoft Intune by using the Intune Company Portal.
- B. Create a compliance policy.
- C. Enroll the devices in Microsoft Intune by using Apple Business Manager.
- D. Create an iOS app provisioning profile.
- E. Create a device configuration profile.

Correct Answer: C, E

Section:

Explanation:

To deploy a specific iOS update to the unmanaged iPad devices, you need to perform the following actions:

Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to

create device groups and assign roles and permissions¹².

Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices³⁴. The other options are not correct for this scenario because:

Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune. However, this method requires user interaction and consent, and does not enroll the devices as supervised devices⁵.

Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings. However, a compliance policy does not deploy or manage software updates on the devices⁶.

Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune. However, an iOS app provisioning profile does not affect the software updates on the devices⁷.

QUESTION 112

HOTSPOT

You have a Microsoft 365 subscription.

You plan to enable Microsoft Intune enrollment for the following types of devices:

- * Existing Windows 11 devices managed by using Configuration Manager
- * Personal iOS devices

The solution must minimize user disruption.

Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Windows 11 devices managed by using Configuration Manager:

Windows Autopilot
Co-management
User enrollment
Windows Autopilot

Personal iOS devices:

Automated Device Enrollment (ADE)
Apple Configurator
Automated Device Enrollment (ADE)
User enrollment

Answer Area:

Answer Area



Section:

Explanation:

QUESTION 113

You have a Windows 10 device named Device1 that is joined to Active Directory and enrolled in Microsoft Intune. Device1 is managed by using Group Policy and Intune. You need to ensure that the Intune settings override the Group Policy settings. What should you configure?

- A. a device configuration profile
- B. a device compliance policy
- C. an MDM Security Baseline profile
- D. a Group Policy Object (GPO)

Correct Answer: A

Section:

Explanation:

A device configuration profile is a collection of settings that can be applied to devices enrolled in Microsoft Intune. You can use device configuration profiles to manage Windows 10 devices that are joined to Active Directory and enrolled in Intune. To ensure that the Intune settings override the Group Policy settings, you need to enable the policy CSP setting called MDMWinsOverGP in the device configuration profile. This setting will give precedence to the MDM policy over any conflicting Group Policy settings. Reference: [Use policy CSP settings to create custom device configuration profiles]

QUESTION 114

HOTSPOT

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

* MDM user scope: Group1

* MAM user scope: 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

	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>



Answer Area:

Answer Area

Statements

	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 115

HOTSPOT

You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.)

Create profile

Block Office applications from injecting code into other processes ⓘ

Disable



Block Office applications from creating executable content ⓘ

Audit mode



Block all Office applications from creating child processes ⓘ

Audit mode



Block Win32 API calls from Office macro ⓘ

Disable



Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ

Disable



Edit profile

^ Attack Surface Reduction Rules

Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ

Audit mode ▼

Block Adobe Reader from creating child processes ⓘ

Audit mode ▼

Block Office applications from injecting code into other processes ⓘ

Audit mode ▼

Block Office applications from creating executable content ⓘ

Audit mode ▼

You plan to deploy both profiles to devices enrolled in Microsoft Intune. You need to identify how the following settings will be configured on the devices:

- * Block Office applications from creating executable content
- * Block Win32 API calls from Office macro

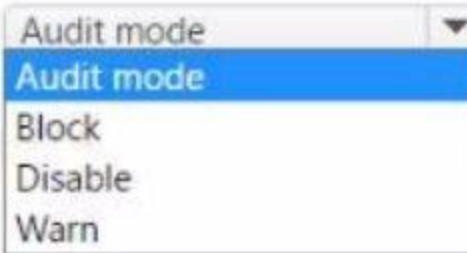
Currently, the settings are disabled locally on each device.

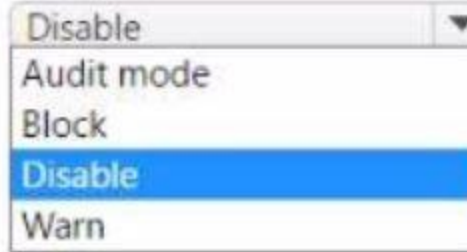
What are the effective settings on the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

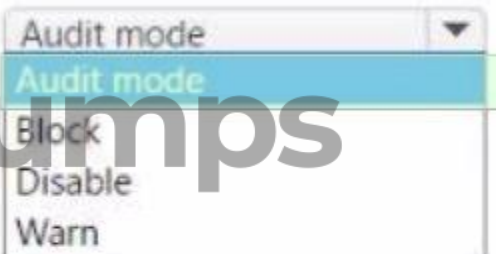
Answer Area

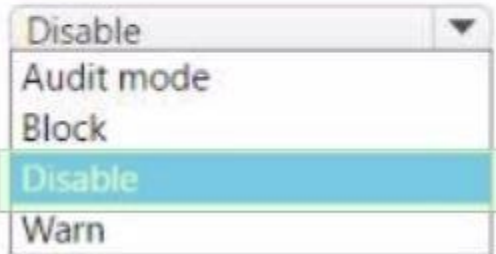
Block Office applications from creating executable content: 

Block Win32 API calls from Office macro: 

Answer Area:

Answer Area

Block Office applications from creating executable content: 

Block Win32 API calls from Office macro: 

Section:

Explanation:

QUESTION 116

DRAG DROP

You have an on-premises Active Directory domain that syncs to Azure AD tenant.

The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune. The Microsoft Office settings on the computers are configured by using a Group Policy Object (GPO).

You need to migrate the GPO to Intune.

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

Select and Place:

Actions

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.
- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.



Answer Area

-
-
-
-



Correct Answer:

Actions

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.
-
-
-



Answer Area

- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.



Section:

Explanation:

Create a configuration profile.
Configure the Administrative Templates settings.
Assign the profile.

QUESTION 117

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You need to configure an update ring that meets the following requirements:

* Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.

* The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.

* Devices must restart automatically three days after an update is installed.

How should you configure the update ring? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

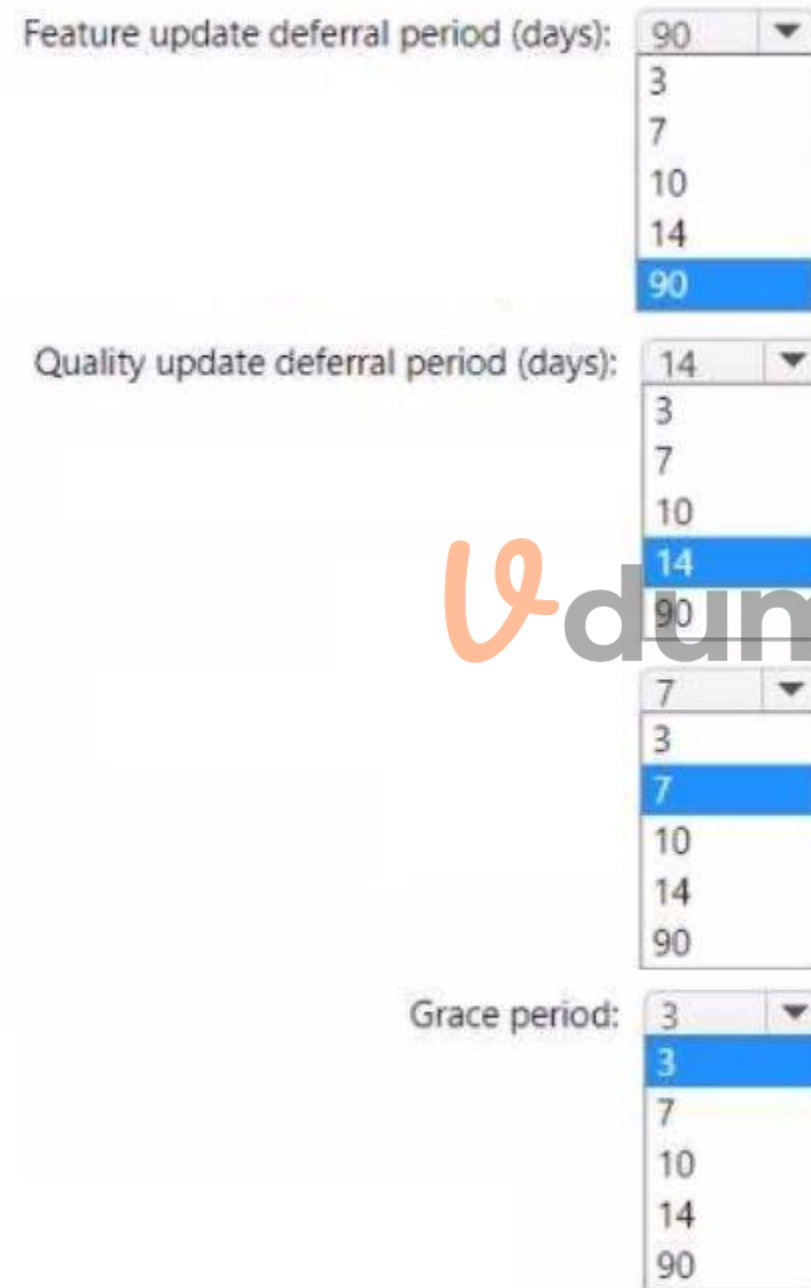
Hot Area:

Answer Area

Feature update deferral period (days): 90

Quality update deferral period (days): 14

Grace period: 3



Answer Area:

Answer Area

Feature update deferral period (days): 90 ▼

- 3
- 7
- 10
- 14
- 90

Quality update deferral period (days): 14 ▼

- 3
- 7
- 10
- 14
- 90

7 ▼

- 3
- 7
- 10
- 14
- 90

Grace period: 3 ▼

- 3
- 7
- 10
- 14
- 90

Section:

Explanation:

QUESTION 118

You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

- A. 30 days
- B. 60 days
- C. 90 days
- D. 365 days

Correct Answer: B

Section:

Explanation:

The Device compliance trends report shows the number of devices that are compliant, noncompliant, and not evaluated over time. The report displays trend data for the last 60 days by default, but you can change the time range to view data for the last 7, 14, or 30 days as well. The report does not show data for more than 60 days. Reference: [Device compliance trends report]

QUESTION 119

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune. You plan to manage Microsoft Defender Antivirus on the computers. You need to prevent users from disabling Microsoft Defender Antivirus. What should you do?

- A. From the Microsoft Intune admin center, create a security baseline.
- B. From the Microsoft 365 Defender portal, enable tamper protection.
- C. From the Microsoft Intune admin center, create an account protection policy.
- D. From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.

Correct Answer: B

Section:

Explanation:

Tamper protection is a feature of Microsoft Defender Antivirus that prevents users or malicious software from disabling or modifying the antivirus settings. Tamper protection can be enabled from the Microsoft 365 Defender portal for devices that are Azure AD joined and enrolled in Microsoft Intune. This will prevent users from turning off Microsoft Defender Antivirus or changing its configuration through Windows Security, PowerShell, Registry, or Group Policy. Reference: [Enable tamper protection]

QUESTION 120

HOTSPOT

You have 1,000 computers that run Windows 10 and are members of an Active Directory domain. You need to capture the event logs from the computers to Azure. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

Azure service to provision:

- Log Analytics
- An Azure Storage account
- Azure Cosmos DB
- Azure SQL Database
- Log Analytics**

Action to perform on the computers:

- Install the Azure Monitor Agent
- Create a collector-initiated subscription**
- Install the Azure Monitor Agent
- Enroll in Microsoft Intune
- Register to Azure AD

Answer Area:

Answer Area

Azure service to provision:

- Log Analytics
- An Azure Storage account
- Azure Cosmos DB
- Azure SQL Database
- Log Analytics

Action to perform on the computers:

- Install the Azure Monitor Agent
- Create a collector-initiated subscription
- Install the Azure Monitor Agent
- Enroll in Microsoft Intune
- Register to Azure AD

Section:

Explanation:

QUESTION 121

You have 200 computers that run Windows 10 and are joined to an Active Directory domain. You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Enable the Allow Remote Shell access setting.
- B. Enable the Allow remote server management through WinRM setting.
- C. Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.
- D. Enable the Windows Defender Firewall: Allow inbound Remote Desktop exceptions setting.
- E. Set the Startup Type of the Remote Registry service to Automatic
- F. Enable the Windows Defender Firewall: Allow inbound remote administration exception setting.

Correct Answer: B, C, F

Section:

Explanation:

To enable WinRM on domain computers using Group Policy, you need to perform the following actions:

Enable the Allow remote server management through WinRM setting under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service. This setting allows you to specify the IP address ranges that can connect to the WinRM service.

Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic under Computer Configuration > Preferences > Control Panel Settings > Services. This setting ensures that the WinRM service starts automatically on the computers.

Enable the Windows Defender Firewall: Allow inbound remote administration exception setting under Computer Configuration > Policies > Security Settings > Windows Firewall and Advanced Security > Windows Firewall and Advanced Security > Inbound Rules. This setting creates a firewall rule that allows incoming TCP connections on port 5985 for WinRM. Reference: How to Enable WinRM via Group Policy, Installation and configuration for Windows Remote Management

QUESTION 122

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices. You purchase a Microsoft 365 E5 subscription. You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.

Which upgrade method should you use?

- A. Windows Autopilot
- B. a Microsoft Deployment Toolkit (MDT) lite-touch deployment
- C. Subscription Activation
- D. an in-place upgrade by using Windows installation media

Correct Answer: C

Section:

Explanation:

Subscription Activation is a feature that allows you to upgrade from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise without needing a product key or reinstallation. You just need to assign a subscription license (such as Microsoft 365 E5) to the user in Azure AD, and then sign in to the device with that user account. The device will automatically activate Windows Enterprise edition using the firmware-embedded activation key for Windows Pro edition. This method minimizes administrative effort and simplifies the upgrade process. Reference: Windows subscription activation, Deploy Windows Enterprise licenses

QUESTION 123

HOTSPOT

You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.

Name	Platform	IP address
Device1	Windows	192.168.10.35
Device2	Android	10.10.10.40
Device3	Android	192.168.10.10

The devices are members of a group named Group1.

In Intune, you create a device compliance location that has the following configurations:

* Name: Network1

* IPv4 range: 192.168.0.0/16

In Intune, you create a device compliance policy for the Android platform. The policy has the following configurations:

* Name: Policy1

* Device health: Rooted devices: Block

* Locations: Location: Network1

* Mark device noncompliant: Immediately

* Assigned: Group1

The Intune device compliance policy has the following configurations:

* Mark devices with no compliance policy assigned as: Compliant

* Enhanced jailbreak detection: Enabled

* Compliance status validity period (days): 20

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
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>



Section:

Explanation:

QUESTION 124

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

- * Ensure that you can manage the personal devices by using Microsoft Intune.
- * Ensure that users can access company data seamlessly from their personal devices.
- * Ensure that users can only sign in to their personal devices by using their personal account

What should you use to add the devices to Azure AD?

- A. Azure AD registered
- B. hybrid Azure AD join
- C. AD joined

Correct Answer: A

Section:

Explanation:

To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization's resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.

The other options are not suitable for this scenario because:

Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories².

AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources³.

QUESTION 125

HOTSPOT

You have a Microsoft 365 subscription.

All computers are enrolled in Microsoft Intune.

You have business requirements for securing your Windows 11 environment as shown in the following table.

Requirement	Detail
Requirement1	Ensure that Microsoft Exchange Online can be accessed from known locations only.
Requirement2	Lock a device that has a high Microsoft Defender for Endpoint risk score.

What should you implement to meet each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Requirement1:

Requirement2:

Answer Area:

Answer Area

Requirement1:
A conditional access policy
A device compliance policy
A device configuration profile

Requirement2:
A device compliance policy
A conditional access policy
A device configuration profile

Section:

Explanation:

QUESTION 126

HOTSPOT

You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to assign roles in Intune to meet the following requirements:

* The members of Group1 must manage Intune roles and assignments.

* The members of Group2 must assign existing apps and policies to users and devices.

The solution must follow the principle of least privilege.

Which role should you assign to each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Group1:
Help Desk Operator
Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

Group2:
Help Desk Operator
Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

Answer Area:

Answer Area

Group1: ▼
 Help Desk Operator
 Intune Role Administrator
 Intune Service Administrator
 Policy and Profile Manager

Group2: ▼
 Help Desk Operator
 Intune Role Administrator
 Intune Service Administrator
 Policy and Profile Manager

Section:

Explanation:

QUESTION 127

HOTSPOT

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

Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	<i>Not applicable</i>	Group3



Intune includes the device compliance policies shown in the following table.

Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	<i>Not applicable</i>

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group1
Policy2	Group1, Group2
Policy3	Group3
Policy4	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

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 128

HOTSPOT

You have an 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 11 device named Client1 to contoso.com.

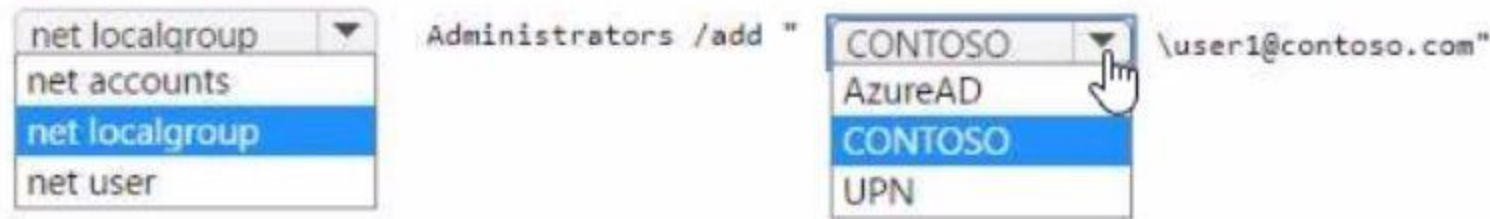
You need to add User1 to the local Administrators group of Client1.

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

NOTE: Each correct selection is worth one point.

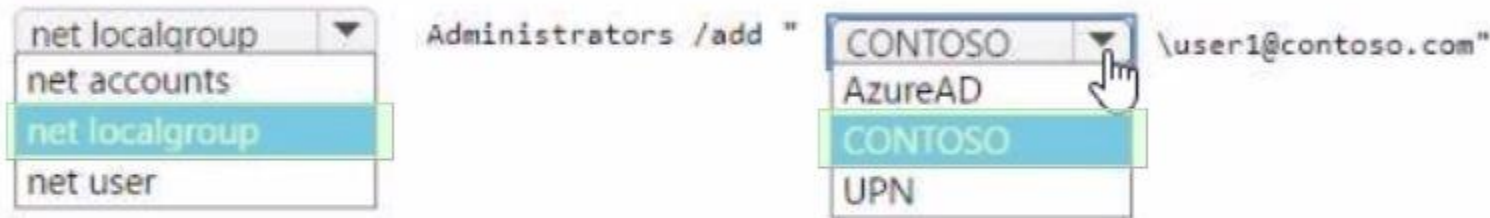
Hot Area:

Answer Area



Answer Area:

Answer Area



Section:

Explanation:

QUESTION 129

You have a computer named Computer5 that has Windows 10 installed.

You create a Windows PowerShell script named config.ps1.

You need to ensure that config.ps1 runs after feature updates are installed on Computer5.

Which file should you modify on Computer5?

- A. LiteTouch.wsf
- B. SetupConfig.ini
- C. Unattendb*
- D. Unattend.xml

Correct Answer: B

Section:

Explanation:

SetupConfig.ini is a file that can be used to customize the behavior of Windows Setup during feature updates. You can use this file to specify commands or scripts that run before or after the installation process. To run a PowerShell script after a feature update, you can use the PostOOBE parameter in SetupConfig.ini and specify the path to the script file. Reference:[SetupConfig.ini reference]

QUESTION 130

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices. You need to create Intune configuration profiles to perform the following actions on the devices:

- * Deploy a custom Start layout.
- * Rename the local Administrator account.

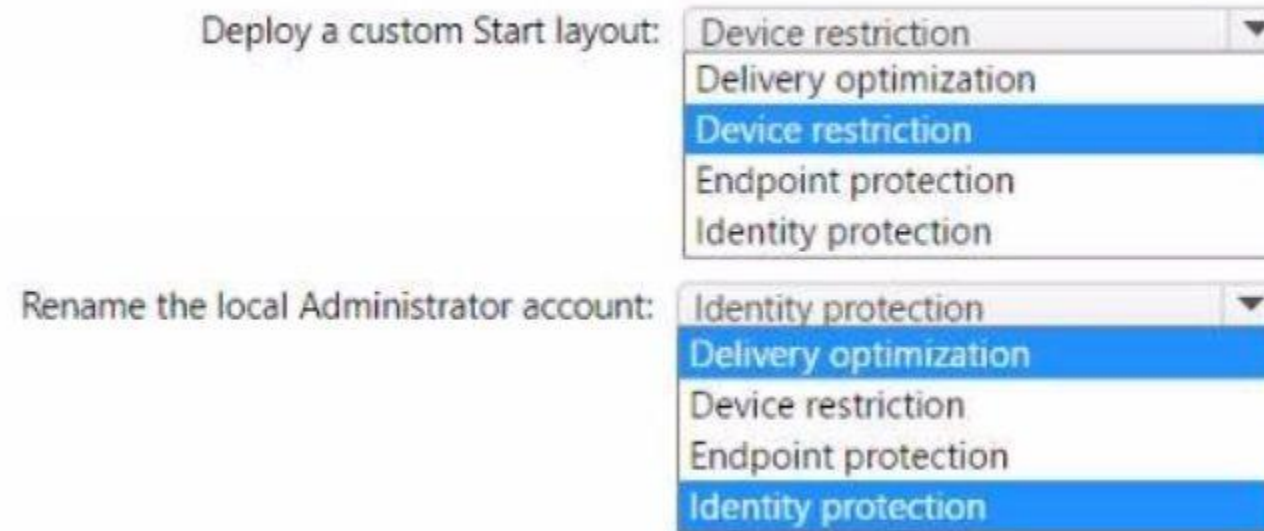
Which profile type template should you use for each action? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Deploy a custom Start layout:

Rename the local Administrator account:

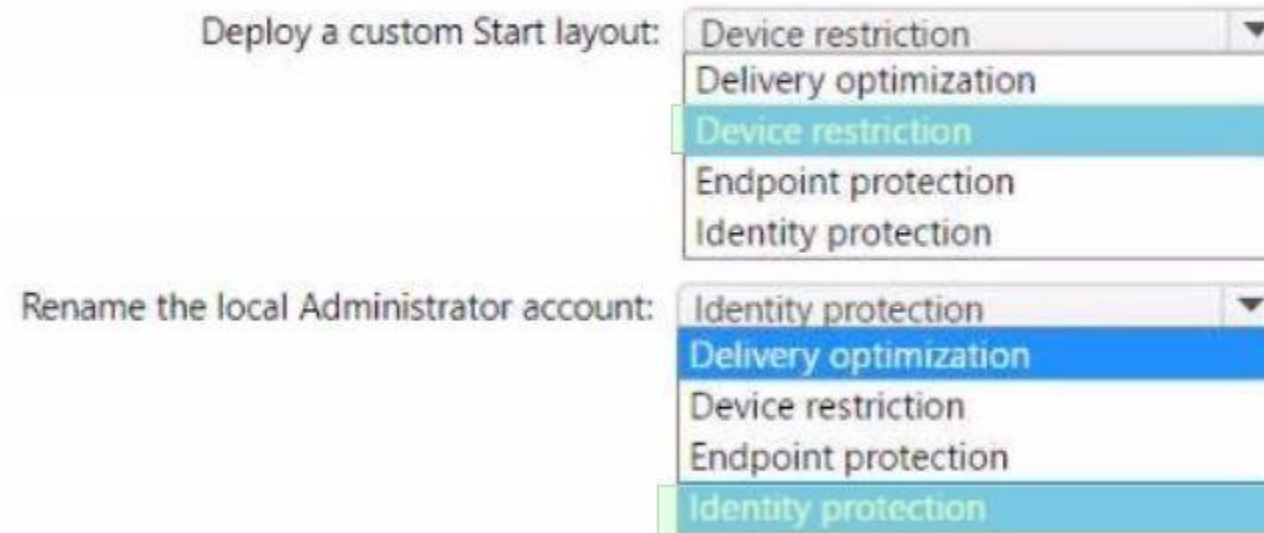


Answer Area:

Answer Area

Deploy a custom Start layout:

Rename the local Administrator account:



Section:

Explanation:

QUESTION 131

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 132

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 133

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 134**

You have a Microsoft Intune subscription associated to an Azure AD tenant named contoso.com.

Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com.

You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment process. The solution must minimize the number of changes. Which DNS records do you need?

- A. three CNAME records
- B. one CNAME record only
- C. three TXT records
- D. one TXT record only

Correct Answer: A**Section:****QUESTION 135****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.

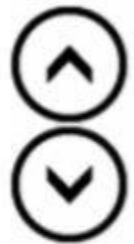
Select and Place:

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:

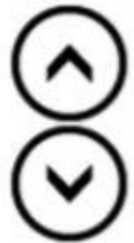
Actions

- 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 136

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You configure Intune to send log data to Log Analytics. You need to review events involving devices that fail to enroll in Intune. What should you monitor?

- A. operational logs
- B. audit logs
- C. the Intune Device log

D. device compliance organizational logs

Correct Answer: C

Section:

QUESTION 137

You have a Microsoft 365 subscription.

You use Microsoft Intune to manage Windows 11 devices.

You need to implement Windows Local Administrator Password Solution (Windows LAPS).

What should you configure?

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

Correct Answer: C

Section:

QUESTION 138

You have a Microsoft 365 subscription that includes Microsoft Intune.

You create a new Android app protection policy named Policy1 that prevents screen captures in all Microsoft apps. You discover that an unmanaged email client installed on Android devices can still capture screens. You need to ensure that users can only use Microsoft apps to access email. What should you do?

- A. Create a Conditional Access policy.
- B. Create a compliance policy.
- C. Modify the Data protection settings of Policy1.
- D. Modify the assignments of Policy1.

Correct Answer: D

Section:

