

Microsoft.MD-102.vNov-2024.by.Tino.140q

Number: MD-102
Passing Score: 800
Time Limit: 120
File Version: 22.0

Exam Code: MD-102

Exam Name: Endpoint Administrator



Group Exam 1

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.

Vdumps

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

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

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

Problem Statements

Litware identifies the following issues on the network:

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

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

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

Requirements

Business Goals

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

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

Device Management Requirements

Litware identifies the following device management requirements:

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

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

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

Technical Requirements

Litware identifies the following technical requirements for the planned deployment:

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

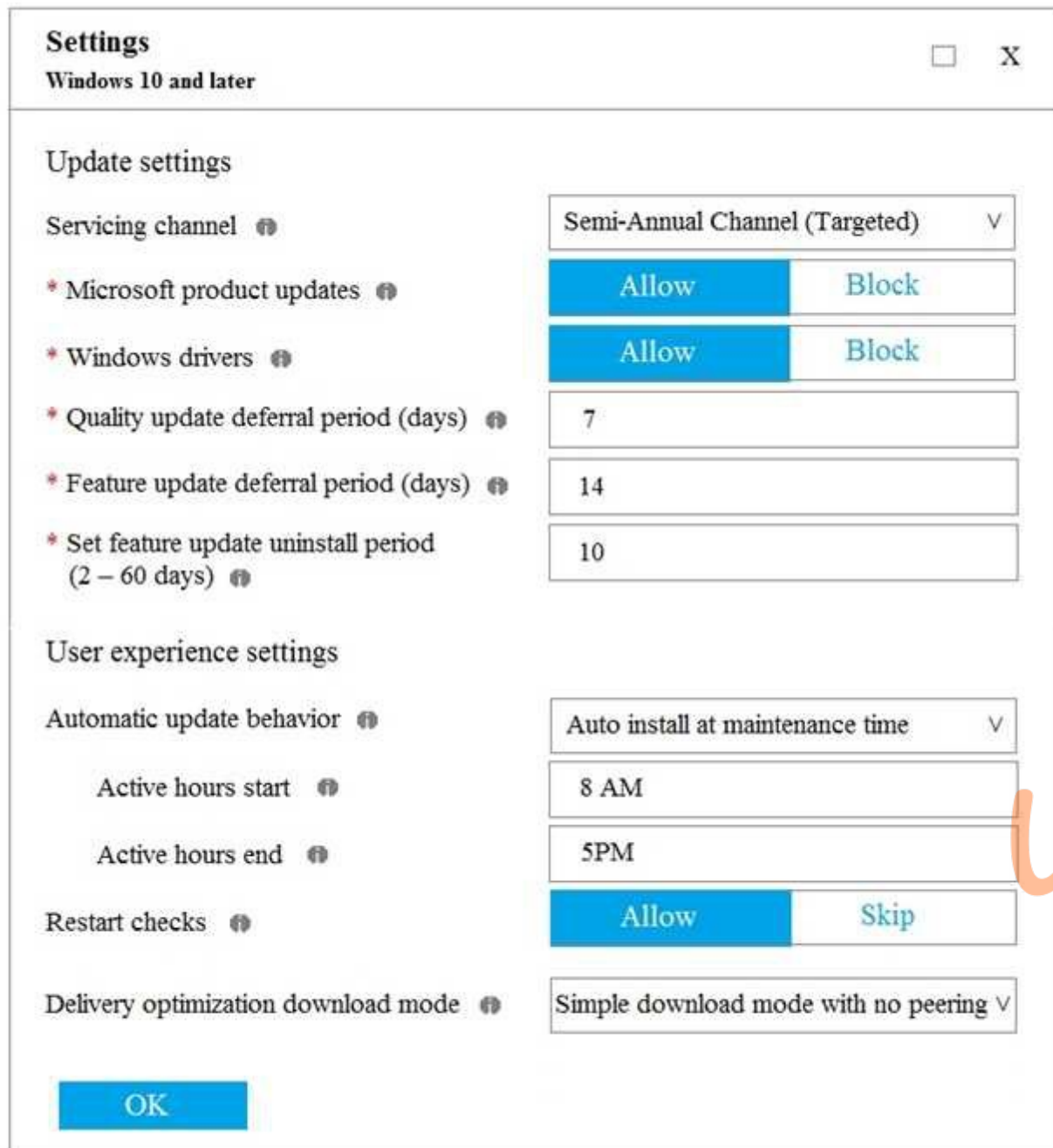
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

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

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

Exhibits





QUESTION 1

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 2

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:

Bypass mode
HTTP blended with internet peering
HTTP blended with peering behind same NAT
Simple download mode with no peering

Update Active Hours Start to:

10 AM
11 AM
10 PM
11 PM

Update Active Hours End to:

10 AM
11 AM
10 PM
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 3

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 4

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:

Overview

Getting started

Manage

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

Answer Area:



Overview

Getting started

Manage

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

Section:

Explanation:

Reference:

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

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

QUESTION 5

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

For the Sales department employees:

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

Answer Area:

For the Research department employees:

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

For the Sales department employees:

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

Section:

Explanation:

Reference:

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

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

QUESTION 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 A

QUESTION 1

HOTSPOT

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

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

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

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

Hot Area:

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



Answer Area:



Section:

Explanation:

QUESTION 2

HOTSPOT

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

Answer Area:

Answer Area

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

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

Section:

Explanation:

QUESTION 3

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 4

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

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

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

Correct Answer: D

Section:

Explanation:

The correct answer is D because app configuration policies can be applied to managed devices and managed apps¹. Managed devices are enrolled and managed by Intune, while managed apps are integrated with Intune App SDK or wrapped using the Intune Wrapping Tool¹. Device2, Device3, and Device4 are either enrolled in Intune or have managed apps installed, so they can receive app configuration policies². Device1 is not enrolled in any MDM solution and does not have any managed apps installed, so it cannot receive app configuration policies². Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Policy sets - Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets>

QUESTION 5

HOTSPOT

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

Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

All devices contain an app named App1 and are enrolled in Microsoft Intune.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which type of policy and how many policies should you create in Intune? 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 the 'Policy type' dropdown menu with the following options: App protection policy (selected), App configuration policy, App protection policy, Conditional access policy, and Device compliance policy. The 'Minimum number of policies' dropdown menu has the following options: 1 (selected), 2, 3, 4, and 5.

Answer Area:

Answer Area

Policy type:

App protection policy
App configuration policy
Conditional access policy
Device compliance policy

Minimum number of policies:

1
2
3
4
5

Section:

Explanation:

Policy type: App protection policy

Minimum number of policies: 1

Comprehensive Explanation of Correct Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices¹. One of the settings you can configure is

Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps². You only need one policy to apply this setting to all devices that have App1 installed¹. Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policiesoverview> 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protectionpolicies/troubleshoot-cut-copy-paste>

QUESTION 6

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

You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps.

You need to ensure that App1 is installed before App2 on every device.

What should you configure?

- A. the App1 deployment configurations
- B. a dynamic device group
- C. a detection rule
- D. the App2 deployment configurations

Correct Answer: D

Section:

Explanation:

The correct answer is D because you can configure the dependencies for a Win32 app in the deployment configurations¹. Dependencies are other Win32 apps that must be installed before your Win32 app can be installed¹.

You can add Win32 app dependencies only after your Win32 app has been added and uploaded to Intune². In this case, you need to configure the App2 deployment configurations to add App1 as a dependency². Reference:

1: Microsoft Intune Win32 App Dependencies - MEndpointMgr <https://msendpointmgr.com/2019/06/03/new-intune-featurewin32-app-dependencies/> 2: Add and assign Win32 apps to Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add>

QUESTION 7

You have a Microsoft Intune subscription.

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

Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage App1?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Correct Answer: B

Section:

Explanation:

The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices¹. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices¹. The settings are assigned to user groups and applied when the app runs¹. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune¹. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings².

Reference: 1: App configuration policies for Microsoft Intune | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios>

QUESTION 8

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

You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.

Which extension should you select for the app package file?

- A. .intunemac
- B. apk
- C. jpa
- D. .appx

Correct Answer: C

Section:

Explanation:

iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.

Reference:

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

QUESTION 9

You have a Microsoft 365 E5 subscription that contains a user named User1 and a web app named

App1.

App1 must only accept modern authentication requests.

You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:

- Assignments
- Users or workload identities: User1
- Cloud apps or actions: App1
- Access controls
- Grant: Block access

You need to block only legacy authentication requests to App1. Which condition should you add to CAPolicy1?

- A. Filter for devices
- B. Device platforms
- C. User risk
- D. Sign-in risk
- E. Client apps

Correct Answer: E

Section:

Explanation:

you can use the client apps condition to block legacy authentication requests to App1. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access². Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos². To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols¹³.

Reference: 1: Conditional Access: Block legacy authentication | Microsoft Learn <https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacyauthentication> 2: What is legacy authentication? | Microsoft Learn <https://learn.microsoft.com/enus/mem/identity-protection/conditional-access/legacy-authentication> 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn <https://learn.microsoft.com/enus/mem/identity-protection/conditional-access/client-apps-condition>

QUESTION 10

HOTSPOT

You have a Microsoft 365 subscription.

All users have Microsoft 365 apps deployed.

You need to configure Microsoft 365 apps to meet the following requirements:

- Enable the automatic installation of WebView2 Runtime.
- Prevent users from submitting feedback.

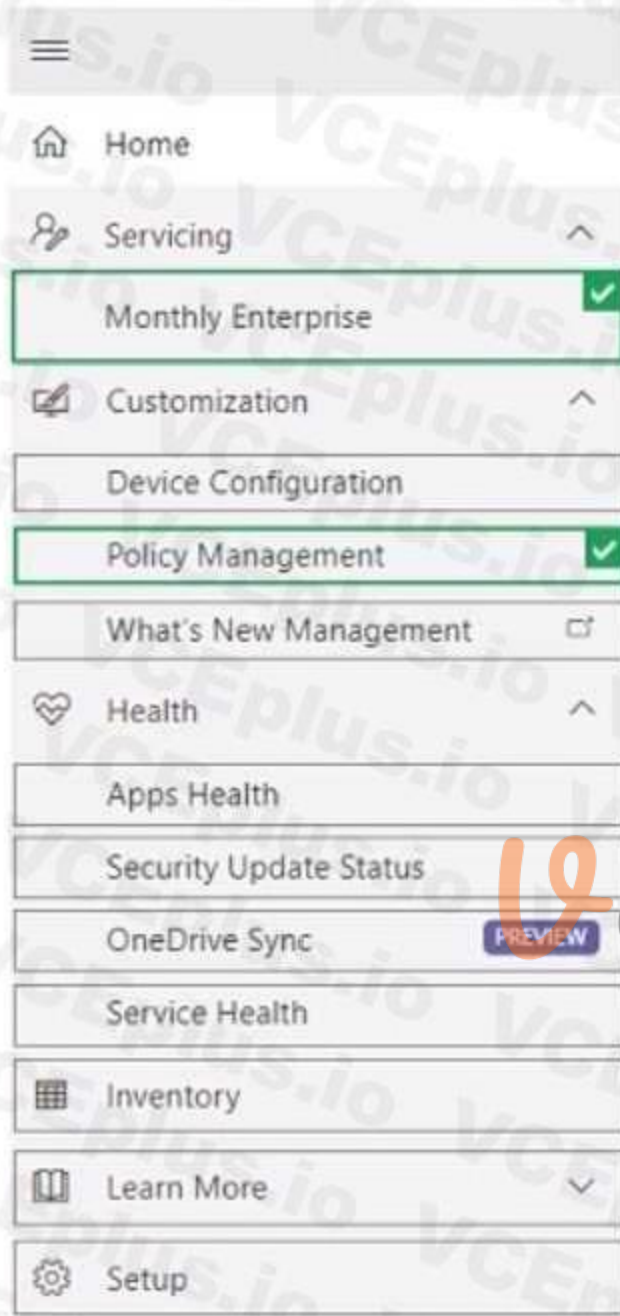
Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



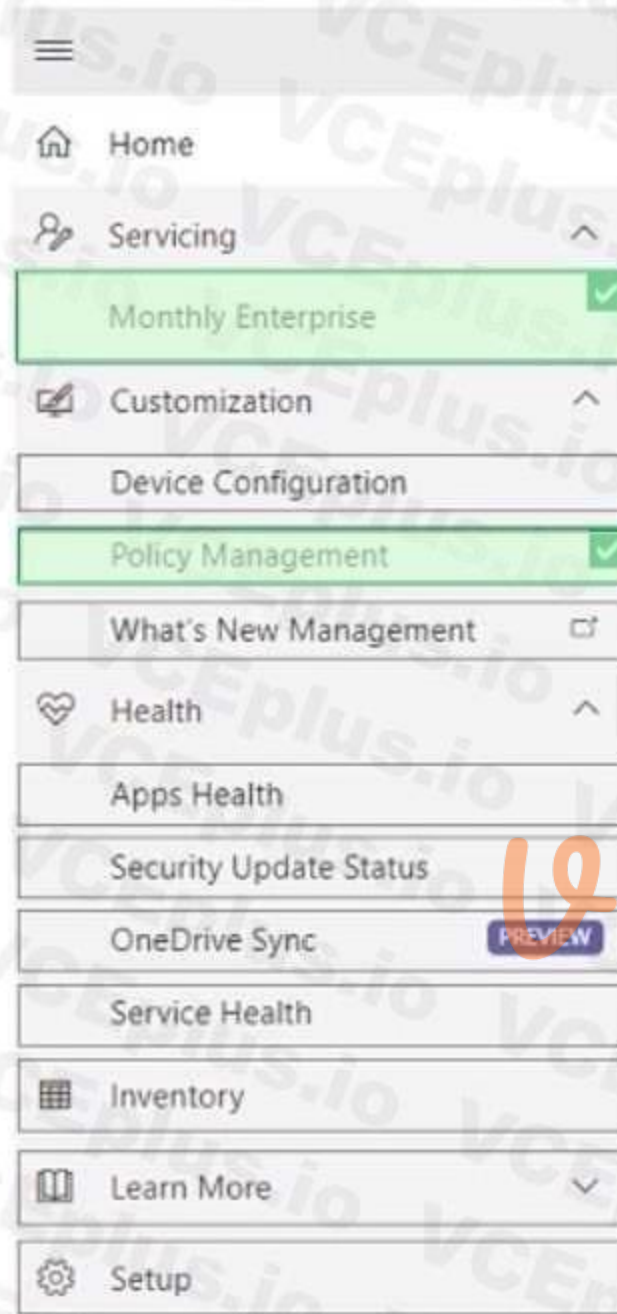
Answer Area



19 dumps

Answer Area:

Answer Area



Vdumps

Section:

Explanation:

QUESTION 11

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM).

You need to deploy the Microsoft 365 Apps for enterprise suite to all the computers.

What should you do?

- A. From the Microsoft Intune admin center, create a Windows 10 device profile.
- B. From Azure AD, add an app registration.
- C. From Azure AD, add an enterprise application.
- D. From the Microsoft Intune admin center, add an app.

Correct Answer: D

Section:

Explanation:

To deploy Microsoft 365 Apps for enterprise to Windows 10 devices that are enrolled in Intune, you need to add an app of type "Windows 10 app (Win32)" in the Microsoft Intune admin center and configure the app settings. You can then assign the app to groups of users or devices. Reference: <https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management>

QUESTION 12

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

You use Microsoft Intune to manage devices.

You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30 days.

You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained.

What should you use?

- A. a Delete action
- B. a Retire action
- C. a Fresh Start action
- D. an Autopilot Reset action

Correct Answer: B

Section:

Explanation:

A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are offline for more than 30 days. Reference:

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

QUESTION 13

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

You need to review the startup times and restart frequencies of the devices. What should you use?

- A. Azure Monitor
- B. Intune Data Warehouse
- C. Microsoft Defender for Endpoint
- D. Endpoint analytics

Correct Answer: D

Section:

Explanation:

Endpoint analytics is a feature of Microsoft Intune that provides insights into the performance and health of devices. You can use endpoint analytics to review the startup times and restart frequencies of the devices, as well as other metrics such as sign-in times, battery life, app reliability, and software inventory. Reference: <https://docs.microsoft.com/en-us/mem/analytics/overview>

QUESTION 14

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

Update ring settings [Edit](#)

Update settings

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

Set feature update uninstall period (2 - 60 days)

10

Servicing channel

General Availability channel

User experience settings

Automatic update behavior

Auto install at maintenance time

Active hours start

8 AM

Active hours end

5 PM

Restart checks

Allow

Option to pause Windows updates

Enable

Option to check for Windows updates

Enable

Change notification update level

Use the default Windows Update notifications

Use deadline settings

Allow

Deadline for feature updates

30

Deadline for quality updates

0

Grace period

0

Auto reboot before deadline

No



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

Answer:

Hot Area:

Answer Area

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

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

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

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

Answer Area:

Answer Area

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

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

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

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

Section:

Explanation:

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

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

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

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

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

QUESTION 15

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

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

Which events are collected in the Log Analytics workspace?

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

Correct Answer: E

Section:

Explanation:

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

QUESTION 16

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

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

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

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 17

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

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

What should you do?

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

Correct Answer: C

Section:

Explanation:

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



QUESTION 18

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

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

Correct Answer: C, E

Section:

Explanation:

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

QUESTION 19

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

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

Correct Answer: D

Section:

Explanation:

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

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

QUESTION 20

DRAG DROP

You have a Microsoft 365 subscription that includes Microsoft Intune.

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

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

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Features

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

Answer Area

- Enforces compliance:
- Prevents suspicious scripts:

Correct Answer:

Features

- A device restriction policy
- A security baseline
-
-

Answer Area

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



Section:

Explanation:

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

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

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

QUESTION 21

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

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

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

Which device configuration profile type template should you use?

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 22

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: A, C, E

Section:

Explanation:

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

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

QUESTION 23

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

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

Correct Answer: C

Section:

Explanation:

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



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

QUESTION 24

Your company uses Microsoft Intune to manage devices.

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

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

NOTE Each correct selection is worth one point.

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

Correct Answer: A, B

Section:

Explanation:

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

QUESTION 25

HOTSPOT

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



Kiosk

Windows 10 and later

Basics Configuration settings Assignments

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

Select a kiosk mode *

User logon type *

Application type *

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

Edge Kiosk URL *

Microsoft Edge kiosk mode type

Refresh browser after idle time

Specify Maintenance Window for App Restarts *

Maintenance Window Start Time

Maintenance Window Recurrence

 **Vdumps**

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

Hot Area:

Answer Area

Users [answer choice].

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

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

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

Answer Area:

Answer Area

Users [answer choice].

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

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

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

Section:

Explanation:

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

Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab. The device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:

Kiosk mode: Enabled

Kiosk type: Multi-app

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

Address bar: Disabled

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

QUESTION 26

HOTSPOT

You have 100 Windows 10 devices enrolled in Microsoft Intune.

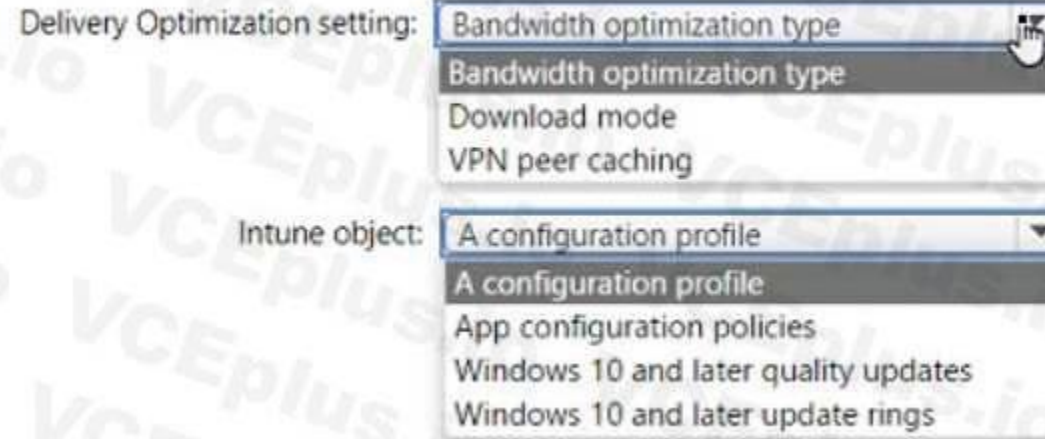
You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

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

NOTE: Each correct selection is worth one point.

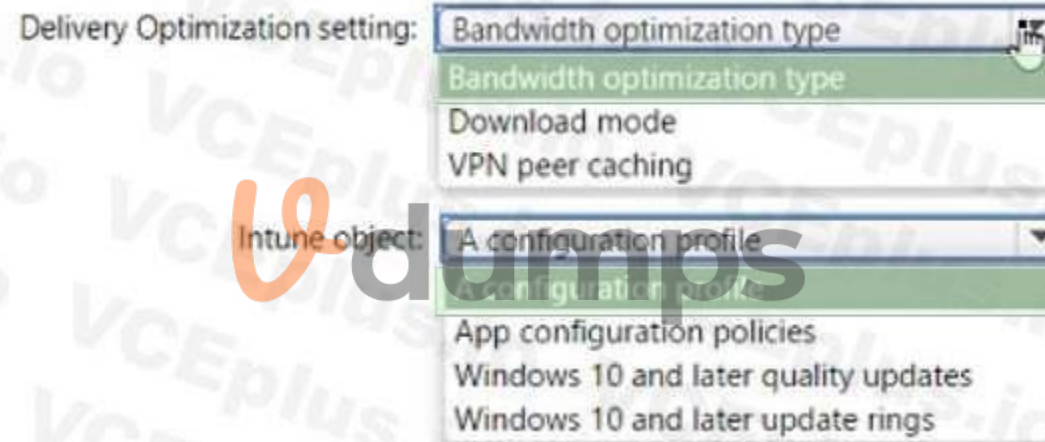
Hot Area:

Answer Area



Answer Area:

Answer Area



Section:

Explanation:

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

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

QUESTION 27

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2

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

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

From Intune, you create and send a custom notification named Notification1 to Group1.
 For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

Hot Area:

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

Answer Area:

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

Section:

Explanation:

Reference:

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

QUESTION 28

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 29**

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

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

What should you do first?

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

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

Reference:

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

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

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

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

QUESTION 30

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

Correct Answer:

Groups

Performance Log Users
Power Users
System Managed Accounts Group

Section:

Explanation:

QUESTION 31

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?

Answer Area

User1:

User2:

- A. December 1
- B. December 6
- C. November 15
- D. November 22

Correct Answer: C

Section:

QUESTION 32

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 33

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 34

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 35

You have a Microsoft 365 E5 subscription and 100 computers that run Windows 10.

You need to deploy Microsoft Office Professional Plus 2019 to the computers by using Microsoft Office Deployment Tool (ODT).

What should you use to create a customization file for ODT?

- A. the Microsoft 365 admin center
- B. the Microsoft Intune admin center
- C. the Microsoft Purview compliance portal
- D. the Microsoft 365 Apps admin center

Correct Answer: D

Section:

QUESTION 36

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

Azure AD joined:

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

Registered in contoso.com:

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

Answer Area:

Answer Area

Azure AD joined:

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

Registered in contoso.com:

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

Section:

Explanation:

QUESTION 37

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 38

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 39

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 40

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 41

DRAG DROP

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

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

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





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

Select and Place:

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

Correct Answer:

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

Section:

Explanation:

Box 1: Modify the Bootstrap.ini file.

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

SkipBDDWelcome=YES

Box 2: Modify the CustomSettings.ini file.

SkipBDDWelcome

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

For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.

Box 3: Update the deployment share.

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

QUESTION 42

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 43

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 44

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 45

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 46

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 47

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.

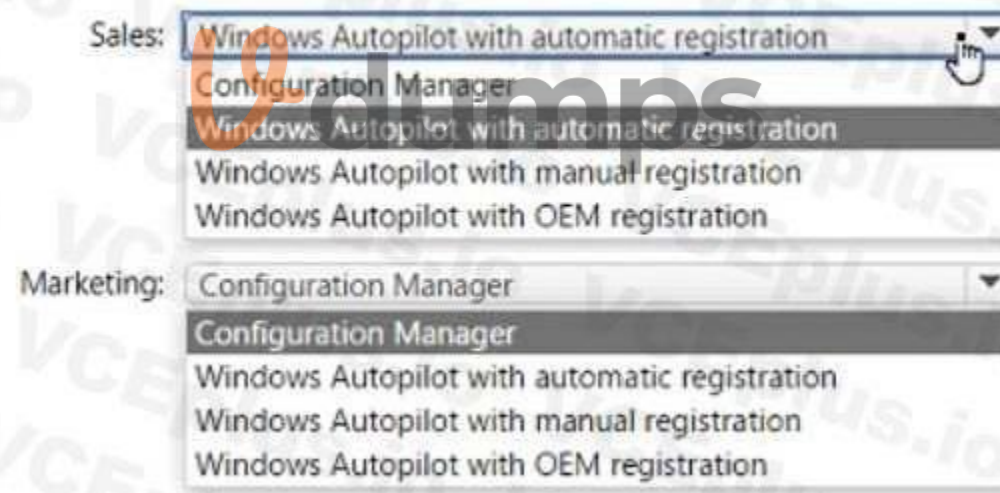
You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:

- 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



Answer Area:

Answer Area



Section:

Explanation:

QUESTION 48

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 49

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 50

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 51

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 52

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 53

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 54

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: User1, 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

If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.

Yes

No

If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.

User2 can access Microsoft Exchange Online from Device2.

Answer Area:

Answer Area

Statements

If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.

Yes

No

If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.

User2 can access Microsoft Exchange Online from Device2.

Section:

Explanation:

QUESTION 55

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 56

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 57

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:



Server:

Ports:

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 58

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 59

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 60

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 61

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 62

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

Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange

Online from iOS devices. You assign CAPolicy1 to Group1.

You discover that User1 can still connect to Exchange Online from an iOS device.

You need to ensure that CAPolicy1 is enforced.

What should you do?

A. Configure a new terms of use (TOU).

B. Assign CAPolicy1 to Group2.

- C. Enable CAPolicy1
- D. Add a condition in CAPolicy1 to filter for devices.

Correct Answer: B

Section:

Explanation:

Common signals that Conditional Access can take in to account when making a policy decision include the following signals:

* User or group membership

Policies can be targeted to specific users and groups giving administrators fine-grained control over access.

* Device

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Use filters for devices to target policies to specific devices like privileged access workstations.

* Etc.

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

QUESTION 63

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 64

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 65

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 ⓘ

ⓘ [important information about hiding license terms](#)

Privacy settings ⓘ

ⓘ 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 66

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 67

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 68

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 69

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 70

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 71

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 72

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 73

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:

The screenshot shows the 'Select and Place' interface in MDT. On the left, under the 'Actions' header, there is a list of five actions: 'Modify a Windows 11 operating system setting.', 'Modify a selection profile.', 'Add App1 to DS1.', 'Identify the GUID of App1.', and 'Modify CustomSettings.ini.'. To the right of this list are two circular arrows, one pointing right and one pointing left. In the center, there are three numbered boxes (1, 2, 3) for ordering. On the right, under the 'Answer Area' header, there is an empty list with two circular arrows, one pointing up and one pointing down. A watermark 'Vdumps' is visible in the center of the interface.

Correct Answer:

The screenshot shows the 'Select and Place' interface with the correct answer. The 'Actions' list on the left is the same as in the previous screenshot. The 'Answer Area' on the right now contains three actions in the following order: 'Add App1 to DS1.', 'Identify the GUID of App1.', and 'Modify CustomSettings.ini.'. The numbered boxes (1, 2, 3) are still present, corresponding to the order in the answer area.

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 74

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 75

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"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /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"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /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 76

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 77

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 78

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 79

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 80

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 81

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 82

You have a Microsoft 365 subscription and use Microsoft Intune Suite. The subscription contains devices enrolled in Intune as shown in the following table.

Name	Platform	Join type
Device1	Windows 10	Microsoft Entra joined
Device2	Windows 11	Microsoft Entra registered
Device3	iOS	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

Which devices support Device query?

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

Correct Answer: C

Section:

QUESTION 83

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 84

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 85

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 86

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 87

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 88

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 89

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 90

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 91

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 92

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune. You plan to use Intune to deploy an application named App1 that contains multiple installation files. What should you do first?

- A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.
- B. Create an Android application package (APK).
- C. Upload the contents of App1 to Intune.
- D. Install the Microsoft Deployment Toolkit (MDT).

Correct Answer: A

Section:

QUESTION 93

HOTSPOT

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

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

You are deploying Microsoft 365 apps.

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

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

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



App Information [Edit](#)

Name Microsoft 365 Apps for Windows 10
Description Microsoft 365 Apps for Windows 10

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



Assignments [Edit](#)

Group mode **Group**

∨ **Required**

⊕ **Included** **Group1**

Available for enrolled devices

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

NOTE: Each correct selection is worth one point.

Hot Area:

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

Answer Area:

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



Section:

Explanation:

Reference:

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

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

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

QUESTION 94

HOTSPOT

You have a Microsoft 365 subscription.

Users have iOS devices that are not enrolled in Microsoft 365 Device Management.

You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)

Dashboard > Client apps - App protection policies > Create policy > Settings

Create policy

* Name
Policy1 ✓

Description

* Platform
iOS ▾

Target to all app types ⓘ
 Yes No

* App types ⓘ
Apps on unmanaged devices ▾

Apps >
1 app selected

Settings >
Review configured settings

Settings

Data protection >
Default settings configured

Access requirements >
Default settings configured

Conditional launch >
Default settings configured

Scope (Tags) >
0 scope(s) selected



You need to configure the policy to meet the following requirements:

Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.

Require the users to use an alphanumeric passcode to access the Outlook app.

What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Prevent the users from using Outlook if the operating system version is less than 12.0.0:

	▼
Access requirements	
Conditional launch	
Data protection	
Scope	

Require the users to use an alphanumeric passcode to access Outlook:

	▼
Access requirements	
Conditional launch	
Data protection	
Scope	

Answer Area:

Prevent the users from using Outlook if the operating system version is less than 12.0.0:

	▼
Access requirements	
Conditional launch	
Data protection	
Scope	

Require the users to use an alphanumeric passcode to access Outlook:

	▼
Access requirements	
Conditional launch	
Data protection	
Scope	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios>

QUESTION 95

HOTSPOT

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

You have the apps shown in the following exhibit.

Apps | All apps

Search (Ctrl+ /)

+ Add Refresh Filter Export Columns

- Overview
- All apps
- Monitor
- By platform
 - Windows
 - iOS/iPadOS
 - macOS
 - Android
- Policy
 - App protection policies
 - App configuration policies

Search by name or publisher

Name	Type	Assigned
App1	Android line-of-business app	Yes
App2	iOS line-of-business app	Yes
App3	iOS line-of-business app	No
Excel	Android store app	Yes
Excel	iOS store app	Yes
Managed Home Screen	Managed Google Play store app	Yes
Microsoft Authenticator	Managed Google Play store app	No
OneDrive	Android store app	No
OneDrive	iOS store app	No

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

NOTE: Each correct selection is worth one point.

Hot Area:

You can create configuration policies for [answer choice] iOS-supported apps.

- 1
- 2
- 3
- 4
- 5

You can create configuration policies for [answer choice] Android-supported apps.

- 1
- 2
- 3
- 4
- 5

Answer Area:

You can create configuration policies for [answer choice] iOS-supported apps.

- 1
- 2
- 3
- 4
- 5

You can create configuration policies for [answer choice] Android-supported apps.

- 1
- 2
- 3
- 4
- 5

Section:

Explanation:

QUESTION 96

You have a Microsoft 365 subscription. All devices run Windows 10.

You need to prevent users from enrolling the devices in the Windows Insider Program.

What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

- A. a device restrictions device configuration profile
- B. an app configuration policy
- C. a Windows 10 and later security baseline
- D. a custom device configuration profile
- E. a Windows 10 and later update ring

Correct Answer: A, E

Section:

QUESTION 97

You install a feature update on a computer that runs Windows 10.

How many days do you have to roll back the update?

- A. 5
- B. 10
- C. 14
- D. 30

Correct Answer: B

Section:

QUESTION 98

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.

You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup.

You need to ensure that you can use Log Analytics to query events from Computer1.

What should you do on Computer1?

- A. Join Azure AD.



- B. Configure Windows Defender Firewall
- C. Create an event subscription.
- D. Install the Azure Monitor Agent.

Correct Answer: D

Section:

QUESTION 99

HOTSPOT

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

Name	Platform
Device1	Windows 10
Device2	macOS

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

Which encryption type should you use for each device, and which role-based access control (RBAC) role in Intune should you use to manage the encryption keys? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device1:

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

Device2:

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

RBAC role:

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

Answer Area:

Answer Area

Device1:	<ul style="list-style-type: none">FileVaultCryptsetupEncrypting File System (EFS)BitLocker Drive Encryption (BitLocker)
Device2:	<ul style="list-style-type: none">FileVaultCryptsetupEncrypting File System (EFS)BitLocker Drive Encryption (BitLocker)
RBAC role:	<ul style="list-style-type: none">Help Desk OperatorApplication ManagerIntune Role AdministratorPolicy and Profile Manager

Section:

Explanation:

QUESTION 100

HOTSPOT

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

The company purchases an Azure subscription.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Resource to create in Azure:

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

Configuration to perform on the computers:

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

Answer Area:

Resource to create in Azure:

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

Configuration to perform on the computers:

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

Section:

Explanation:

Reference:

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

QUESTION 101

You have a Microsoft 365 subscription that includes Microsoft Intune.

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

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

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

When will devices start to remove the feature updates?

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

Correct Answer: C

Section:

QUESTION 102

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

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

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

What should you do?

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

Correct Answer: C



Section:

QUESTION 103

HOTSPOT

You have a Microsoft 365 subscription.

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

Platform	Version
Android	8, 9
iOS	11, 12

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

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

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

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

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

Answer Area:

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

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

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

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

Section:

Explanation:

Reference:

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

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

QUESTION 104

HOTSPOT

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

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

You plan to implement Microsoft Defender Exploit Guard.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:



Tool to use to configure the settings:

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

Distribution method:

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

Answer Area:

Tool to use to configure the settings:

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

Distribution method:

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

Section:

Explanation:

Reference:

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

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

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

QUESTION 105

Your company uses Microsoft Intune.

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

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

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

What should you configure first?

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

Correct Answer: B

Section:

QUESTION 106

DRAG DROP

You have 500 Windows 10 devices enrolled in Microsoft Intune.

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

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

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

Protection areas

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

Answer Area

DEP:

Mandatory ASLR:

Correct Answer:

Protection areas

- Account protection
-
-
- Virus & threat protection

Answer Area

DEP:

Mandatory ASLR:

Section:

Explanation:

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

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

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

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

QUESTION 107

You have an Azure AD tenant named contoso.com.

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



You need to add Computer1 to contoso.com.
What should you use?

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

Correct Answer: A
Section:

QUESTION 108

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage Windows 11 devices.
You need to implement passwordless authentication that requires users to use number matching Which authentication method should you use?

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

Correct Answer: A
Section:

QUESTION 109

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 110

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 Area

User1: User Administrator

User2: Helpdesk Administrator



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 111

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 checked="" type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input checked="" type="radio"/>	<input 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 112

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 113

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 114

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 115

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 116

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 117

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).

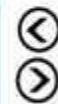
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

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 118**

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 119

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, andGroup4

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 theGlobal administratorsrole 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 120

You have the Windows 10 devices shown in the following table.



Name	Operating system	Edition
Device1	64-bit version of Windows 10	Home
Device2	32-bit version of Windows 10	Pro
Device3	64-bit version of Windows 10	Enterprise
Device4	64-bit version of Windows 10	Pro

You plan to upgrade the devices to Windows 11 Enterprise.

On which devices can you perform a direct in-place upgrade to Windows 11 Enterprise?

- A. Device3 only
- B. Device 3 and Device 4 only
- C. Device2. Device3. and Devtce4 only
- D. Device1. Device3, and Devtce4 only
- E. Device1, Device2. Device3. and Devke4 only

Correct Answer: B

Section:

Explanation:

<https://learn.microsoft.com/en-us/windows/deployment/upgrade/windows-upgrade-paths> <https://learn.microsoft.com/en-us/windows/deployment/upgrade/windows-edition-upgrades>

QUESTION 121

You have a Microsoft Deployment Toolkit (MDT) deployment shore.

You plan to deploy Windows 11 by using the Standard Client Task Sequence template.

You need to modify the task sequence to perform the following actions:

* Format disks to support Unified Extensible Firmware Interface (UEFI).

* Create a recovery partition.

Which phase of the Task sequence should you modify?

- A. Preinstall
- B. Install
- C. Initialization
- D. Post Install

Correct Answer: A

Section:

QUESTION 122

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have 500 corporate-owned Android devices enrolled as fully managed devices.

You need to prepare an app named App1 for deployment to the devices.

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

NOTE: Each correct selection is worth one point,

- A. From the Intune Company Portal, download Appl.
- B. Create an OEMConfig profile.
- C. From the Managed Google Play Store, approve App1.
- D. Sync App1 with Intune.

Correct Answer: C, D

Section:

Explanation:

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work>



QUESTION 123

You are implementing Microsoft Intune Suite.

You enroll devices in Intune as shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

The performance of which devices can be analyzed by using Endpoint analytics?

- 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: B

Section:

Explanation:

https://learn.microsoft.com/en-us/mem/analytics/overview#bkmk_prereq

QUESTION 124

You have a Microsoft 365 subscription that includes Microsoft Intune. The subscription contains corporate-owned, fully managed Android Enterprise devices. You plan to deploy a configuration profile that will have a device restrictions profile type named Profile1. Profile1 will assign maintenance windows for system updates. What should you configure from the Configuration settings for Profile1?

- A. Device experience
- B. General
- C. Connectivity
- D. Power Settings Explanation

Correct Answer: A

Section:

QUESTION 125

HOTSPOT

You have a Microsoft 365 subscription.

You have 25 Microsoft Surface Hub devices that you plan to manage by using Microsoft Intune.

You need to configure the devices to meet the following requirements:

- * Enable Windows Hello for Business.
- * Configure Microsoft Defender SmartScreen to block users from running unverified files.

Which profile type template should you use 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

The screenshot shows two dropdown menus. The first is labeled 'Windows Hello for Business:' and has a list of options: 'Identity protection', 'Device restrictions', 'Device restrictions (Windows 10 Team)', 'Endpoint protection', 'Identity protection', and 'Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)'. The second dropdown is labeled 'Microsoft Defender SmartScreen:' and has a list of options: 'Endpoint protection', 'Windows health monitoring', 'Device restrictions (Windows 10 Team)', 'Endpoint protection', 'Identity protection', and 'Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)'. A watermark 'Vdumps' is visible in the background.

Answer Area:

Answer Area

Windows Hello for Business: Identity protection
Device restrictions
Device restrictions (Windows 10 Team)
Endpoint protection
Identity protection
Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Microsoft Defender SmartScreen: Endpoint protection
Windows health monitoring
Device restrictions (Windows 10 Team)
Endpoint protection
Identity protection
Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Section:

Explanation:

QUESTION 126

HOTSPOT

You have a Microsoft 365 E5 subscription and use Microsoft Intune Suite. You manage the following types of devices;

- * Windows 11
- * Android
- * iOS

You need to implement Microsoft Tunnel for Mobile Application Management (MAM) to provide the devices with access to on-premises company apps. What should you deploy first, and which device types can use Tunnel for MAM? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Deploy: Microsoft Tunnel Gateway
Intune Connector for Active Directory
Microsoft Entra application proxy
Microsoft Tunnel Gateway
The Microsoft Authenticator app

Device types: Android and iOS only
Windows 11 only
Windows 11 and Android only
Windows 11 and iOS only
Android and iOS only
Windows 11, Android, and iOS

Answer Area:

Answer Area

Deploy: Microsoft Tunnel Gateway
Intune Connector for Active Directory
Microsoft Entra application proxy
Microsoft Tunnel Gateway
The Microsoft Authenticator app

Device types: Android and iOS only
Windows 11 only
Windows 11 and Android only
Windows 11 and iOS only
Android and iOS only
Windows 11, Android, and iOS

Section:

Explanation:

QUESTION 127

HOTSPOT

You have a Microsoft 365 E5 subscription that includes Microsoft Intune. The subscription contains a group named Group1. Group1 contains devices enrolled in Intune. You deploy Remote Help in Intune.

You need to configure Remote Help to only allow support administrators to join Remote Help sessions from the devices in Group1.

Which type of Microsoft Entra object should you create, and which type of policy should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Microsoft Entra object: A service principal
A service principal
An app registration
An enterprise application

Policy: Conditional Access
Compliance
Conditional Access
Endpoint Privilege Management

Answer Area:

Answer Area

Microsoft Entra object: A service principal
A service principal
An app registration
An enterprise application

Policy: Conditional Access
Compliance
Conditional Access
Endpoint Privilege Management



Section:

Explanation:

QUESTION 128

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

You plan to use Device query to provide on-demand information about the state of the devices. The solution must minimize costs. What should you do first?

- A. Onboard the devices to Endpoint analytics.
- B. Purchase the Intune Advanced Analytics add-on.
- C. Use the Collect diagnostics remote action.
- D. Purchase the Intune Suite add-on.

Correct Answer: A

Section:

QUESTION 129

DRAG DROP

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Intune. You need to meet the following requirements:

* Only allow the enrollment of devices that have a specific international mobile equipment identifier (IMEI).

* Support the enrollment and management of up to 1,000 devices

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

NOTE: Each correct selection is worth one point.



Select and Place:

Enrollment settings	Answer Area
<input type="checkbox"/> CNAME Validation	Only allow the enrollment of devices with a specific IMEI: <input type="text"/>
<input type="checkbox"/> Corporate device identifiers	Support the enrollment and management of up to 1,000 devices: <input type="text"/>
<input type="checkbox"/> Device enrollment managers	
<input type="checkbox"/> Device limit restriction	
<input type="checkbox"/> Device platform restriction	

Correct Answer:

Enrollment settings

- CNAME Validation
- Device limit restriction
- Device platform restriction

Answer Area

- Only allow the enrollment of devices with a specific IMEI: Corporate device identifiers
- Support the enrollment and management of up to 1,000 devices: Device enrollment managers

Section:

Explanation:

QUESTION 130

HOTSPOT

You have a Microsoft 365 E5 tenant that contains Windows devices enrolled in Microsoft Intune as shown in the following table.

Name	Member of	Join type
Device1	Group1, Group2	Microsoft Entra joined
Device2	Group2	Microsoft Entra joined
Device3	Group1, Group2	Microsoft Entra hybrid joined

You create an Endpoint Privilege Management (EPM) elevation settings policy named ElevationSettings1 that has the following settings:

- * Endpoint Privilege Management: Enabled
- o Default elevation response: Require user confirmation
- o Validation: Business justification

* Assignments: Group1 Each device contains a file named File1.exe that can be run only by an administrator. You create an EPM elevation rules policy named ElevationRules1 that has the following settings:

- * Rule name: Rule1
- o Elevation type: Automatic
- o File name: File1.exe
- o File hash: <File1.exe hash>

* Assignments: Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
A user on Device1 must provide a business justification to run File1.exe.	<input type="radio"/>	<input type="radio"/>
A user on Device2 can run File1.exe.	<input type="radio"/>	<input type="radio"/>
A user on Device3 can run File1.exe without providing a business justification.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements

A user on Device1 must provide a business justification to run File1.exe.

Yes

No

A user on Device2 can run File1.exe.

A user on Device3 can run File1.exe without providing a business justification.

Section:

Explanation:

QUESTION 131

You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune. You create a user named User1.

You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.

Solution: From the Microsoft Entra admin center, you assign the Helpdesk Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

