



Microsoft

Exam Questions MD-102

Endpoint Administrator

NEW QUESTION 1

- (Exam Topic 4)

You have an Azure subscription.

You have an on-premises Windows 11 device named Device 1. You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription. To what should you associate DCR1 ?

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

Answer: B

Explanation:

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

The other options are not correct for this scenario because:

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

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

➤ A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules. References: Data collection rules in Azure Monitor, Configure data collection for Azure Monitor Agent, U

Azure Policy to install Azure Monitor Agent and associate with a DCR, What is Azure Network Watcher?, Log Analytics workspaces in Azure Monitor

NEW QUESTION 2

- (Exam Topic 4)

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

Answer: A

NEW QUESTION 3

- (Exam Topic 4)

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

What should you use?

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

Answer: B

NEW QUESTION 4

- (Exam Topic 4)

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

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

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

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

- Assignments
 - o Users or workload identities: User 1. User1
 - o Cloud apps or actions: Office 365 Exchange Online
 - o Conditions: Device platforms: Windows, iOS
- Access controls
 - o Grant Require multi-factor authentication

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

Assignments

o Users or workload identities: Used, User2 o Cloud apps or actions: Office 365 Exch
o Conditions

Device platforms: Android, iOS Filter for devices

Device matching the rule: Exclude filtered devices from policy Rule syntax: device. displayName- contains "1"

Access controls Grant Block access

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screen shot of a computer Description automatically generated with low confidence

NEW QUESTION 5

- (Exam Topic 4)

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

Answer: D

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:
- > 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-link-powerbi>

NEW QUESTION 6

- (Exam Topic 4)

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. On Computer1, you need to run the

Invoke-Command cmdlet to execute several PowerShell commands on Computer2. What should you do first?

- A. On Computed, run the Enable-PSRemoting cmdlet.
- B. On Computed, add Computer! to the Remote Management Users group.
- C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computed.
- D. On Computer1, run the HcK-PSSession cmdlet.

Answer: C

NEW QUESTION 7

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

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

What should you configure?

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

Answer: D

Explanation:

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

The other options are not relevant for this scenario because:

- Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune. It does not control the local administrator role of the users who join the devices2.
- Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users3.
- Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role4.

References: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security defaults?

NEW QUESTION 8

- (Exam Topic 4)

You have a Windows 10 device named Device1 that is joined to Active Directory and enrolled in Microsoft Intune.

Device1 is managed by using Group Policy and Intune.

You need to ensure that the Intune settings override the Group Policy settings. What should you configure?

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

Answer: A

Explanation:

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

NEW QUESTION 9

- (Exam Topic 4)

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.

Answer Area

Sales:

Windows Autopilot with automatic registration

Configuration Manager

Windows Autopilot with automatic registration

Windows Autopilot with manual registration

Windows Autopilot with OEM registration

Marketing:

Configuration Manager

Configuration Manager

Windows Autopilot with automatic registration

Windows Autopilot with manual registration

Windows Autopilot with OEM registration

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Sales:

Windows Autopilot with automatic registration

Configuration Manager

Windows Autopilot with automatic registration

Windows Autopilot with manual registration

Windows Autopilot with OEM registration

Marketing:

Configuration Manager

Configuration Manager

Windows Autopilot with automatic registration

Windows Autopilot with manual registration

Windows Autopilot with OEM registration

NEW QUESTION 10

- (Exam Topic 4)

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

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

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

Basics Edit

Name	Policy1
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings Edit

Device Health

Require BitLocker	Require
-------------------	---------

Actions for noncompliance Edit

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

Scope tags Edit

Default

Assignments Edit

Included groups

Group
Group1
Group3

Excluded groups

Group
Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

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

Yes

☒

No

☐

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

☐
☒

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

☐
☒

NEW QUESTION 10

- (Exam Topic 4)

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.

Answer: B

NEW QUESTION 12

- (Exam Topic 4)

You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

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.

Answer Area

Device1:

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"

Device2:

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"

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device1:

```
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"
```

Device2:

```
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"
```

NEW QUESTION 13

- (Exam Topic 4)

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

Answer: B

NEW QUESTION 16

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 1,000 iOS devices. The devices are enrolled in Microsoft Intune as follows:

- Two hundred devices are enrolled by using the Intune Company Portal.
- Eight hundred devices are enrolled by using Apple Automated Device Enrollment (ADE).

You create an iOS/iPadOS software updates policy named Policy 1 that is configured to install iOS/iPadOS 15.5.

How many iOS devices will Policy1 update, and what should you configure to ensure that only iOS/iPadOS 15.5 is installed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Number of devices:

200
800
1000

Configure a:

Compliance policy
Conditional Access policy
Device restriction policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy 1 will update 800 iOS devices that are enrolled by using Apple Automated Device Enrollment (ADE). This is because ADE devices are supervised devices that support software update policies in Intune1. Devices that are enrolled by using the Intune Company Portal are not supervised devices and do not support software update policies2.

To ensure that only iOS/iPadOS 15.5 is installed, you should configure a device restriction policy that restrict visibility of software updates. This will prevent users from manually updating the OS to a newer version than the one you specified in Policy 11. You can use the Deployment Workbench to create and assign a device restriction profile to your ADE devices3.

NEW QUESTION 18

- (Exam Topic 4)

You manage 1,000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

- A. 30 days

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

Answer: B

Explanation:

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

NEW QUESTION 19

- (Exam Topic 4)

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 JOS/iPadOS update profile as shown in the following exhibit.

Create profile

iOS/iPadOS

✓ Basics

✓ Update policy settings

✓ Assignments

ⓘ Review + create

Summary

Basics

Update policy settings

Assignments

Name

Profile1

Description

--

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

Assigned to

Included groups

Excluded groups

Group

Group Members ⓘ

Group1

3 devices, 0 users

Group

Group Members ⓘ

Group2

1 devices, 0 users

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 24

- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.
What should you select in the Microsoft Endpoint Manager admin center?

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

Answer: A

Explanation:

App report: You can search by platform and app, and then this report will provide two different app protection statuses that you can select before generating the report. The statuses can be Protected or Unprotected.
Reference:
<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-monitor>

NEW QUESTION 28

- (Exam Topic 4)
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

Answer: D

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:
- 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-link-powerbi>

NEW QUESTION 29

- (Exam Topic 4)

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.

Server:

Ports:

- A. Mastered
- B. Not Mastered

Answer: A

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>

NEW QUESTION 33

- (Exam Topic 4)

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

Answer: C

NEW QUESTION 35

- (Exam Topic 4)

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

Answer: D

NEW QUESTION 37

- (Exam Topic 4)

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

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

Which images can be used in the Standard Client Task Sequence, and which images can be used in the Standard Client Upgrade Task Sequence?

NOTE: Each correct selection is worth one point.

Answer Area

Standard Client Task Sequence:

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

Standard Client Upgrade Task Sequence:

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Standard Client Task Sequence:

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

Standard Client Upgrade Task Sequence:

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

NEW QUESTION 40

- (Exam Topic 4)

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

Answer: E

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

NEW QUESTION 41

- (Exam Topic 4)

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

You have a Microsoft 365 subscription

You plan to use Windows Autopilot to deploy new Windows devices. You plan to create a deployment profile.

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

- Devices must be joined to AD DS regardless of their current working location.
 - Users in the marketing department must have a line-of-business (LOB) app installed during the deployment. The solution must minimize administrative effort.
- What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

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

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

NEW QUESTION 43

- (Exam Topic 4)

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

You plan to integrate Intune with Microsoft Defender for Endpoint.

You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

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

Answer: A

Explanation:

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

As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.

Reference: <https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/>

NEW QUESTION 46

- (Exam Topic 4)

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

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

- > Prevent Microsoft Office applications from launching child processes.
- > Block users from transferring files over FTP.

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

NOTE: Each correct selection is worth one point.

Answer Area

Create Profile

*Name

MD101

Description

Enter a description

*Platform

Windows 10 and later

*Profile type

Endpoint protection

Settings

Configure

Scope (Tags)

0 scope(s) selected

Endpoint protection

Windows 10 and later

Select a category to configure settings

Windows Defender Application Gu...
11 settings available

Windows Defender Firewall
40 settings available

Windows Defender SmartScreen
2 settings available

Windows Encryption
37 settings available

Windows Defender Exploit Guard
20 settings available

Windows Defender Application Co...
2 settings available

Windows Defender Application Gua...
1 setting available

Windows Defender Security Center
14 settings available

Local device security options
46 settings available

Xbox services
5 settings available

OK

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

References:

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

NEW QUESTION 48

- (Exam Topic 4)

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

Answer: B

NEW QUESTION 53

- (Exam Topic 4)

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

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>

NEW QUESTION 57

- (Exam Topic 4)

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

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

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: CE

Explanation:

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

➤ Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to create device groups and assign roles and permissions¹².

➤ Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices³⁴.

The other options are not correct for this scenario because:

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

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

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

References: What is Apple Business Manager?, Enroll iOS/iPadOS devices in Intune, Manage iOS/iPadOS software update policies in Intune, Software updates planning guide and scenarios for supervised iOS/iPadOS devices in Microsoft Intune, Enroll your personal device in Intune, Device compliance policies in Microsoft Intune, Add an iOS app provisioning profile with Microsoft Intune

NEW QUESTION 58

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.

Computer1 has apps that are compatible with Windows 10.

You need to perform a Windows 10 in-place upgrade on Computer1.

Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment

share. You create a task sequence, and then you run the MDT deployment wizard on Computer1. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 60

- (Exam Topic 4)

You have a Microsoft 365 subscription.

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

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

The solution must minimize user disruption.

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

NOTE: Each correct selection is worth one point.

Answer Area

Windows 11 devices managed by using Configuration Manager:

- Windows Autopilot
- Co-management
- User enrollment
- Windows Autopilot**

Personal iOS devices:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Windows 11 devices managed by using Configuration Manager:

- Windows Autopilot
- Co-management
- User enrollment
- Windows Autopilot**

Personal iOS devices:

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

NEW QUESTION 65

- (Exam Topic 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

Answer: D

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. References: 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>

NEW QUESTION 69

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 11 deployment tasks. MDT contains the operating system images shown in the following table.

Name	Description
Image1.wim	Custom-built Windows 10 image that has preinstalled custom apps
Image2.wim	Custom-built Windows 10 image without apps
Install.wim	Default Windows 10 image

You need to perform a Windows 11 in-place upgrade on several computers that run Windows 10. From the Deployment Workbench, you open the New Task Sequence Wizard.

You need to identify which task sequence template and which operating system image to use for the task sequence. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Task sequence template:

Standard Client Task Sequence
Standard Client Replace Task Sequence
Standard Client Upgrade Task Sequence

Operating system image:

Image1.wim
Image2.wim
Install.wim

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Standard Client Upgrade Task Sequence

Use Template: Standard Client Upgrade Task Sequence

In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not plan to significantly change the device's configuration or applications. MDT includes an in-place upgrade task sequence template that makes the process really simple.

Box 2: Install.wim

In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. I

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the>

NEW QUESTION 73

- (Exam Topic 4)

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

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

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

NOTE: Each correct selection is worth one point.

Settings

Require BitLocker.

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings

Require BitLocker.

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

Answer Area

Device1: Require BitLocker.

Device2: Prevent jailbroken devices from having corporate access.

Device3: Prevent rooted devices from having corporate access.

NEW QUESTION 74

- (Exam Topic 4)
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

Answer: B

NEW QUESTION 78

- (Exam Topic 4)
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

Answer: B

NEW QUESTION 82

- (Exam Topic 4)
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\$

[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.

Statements

Yes

No

TB1 will download the image from MDT3.

☐
☐

DT1 will have a KeyboardLocale of en-gb.

☐
☐

LT1 will download the image from MDT1.

☐
☐

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Statements

Yes

No

TB1 will download the image from MDT3.

☐
☒

DT1 will have a KeyboardLocale of en-gb.

☒
☐

LT1 will download the image from MDT1.

☒
☐

NEW QUESTION 83

- (Exam Topic 3)

You need to meet the requirements for the MKG department users. What should you do?

A. Assign the MKG department users the Purchaser role in Microsoft Store for Business

B. Download the APPX file for App1 from Microsoft Store for Business

- C. Add App1 to the private store
- D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business
- E. Acquire App1 from Microsoft Store for Business

Answer: E

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store> Enable the users in the MKG department to use App1.

The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store>

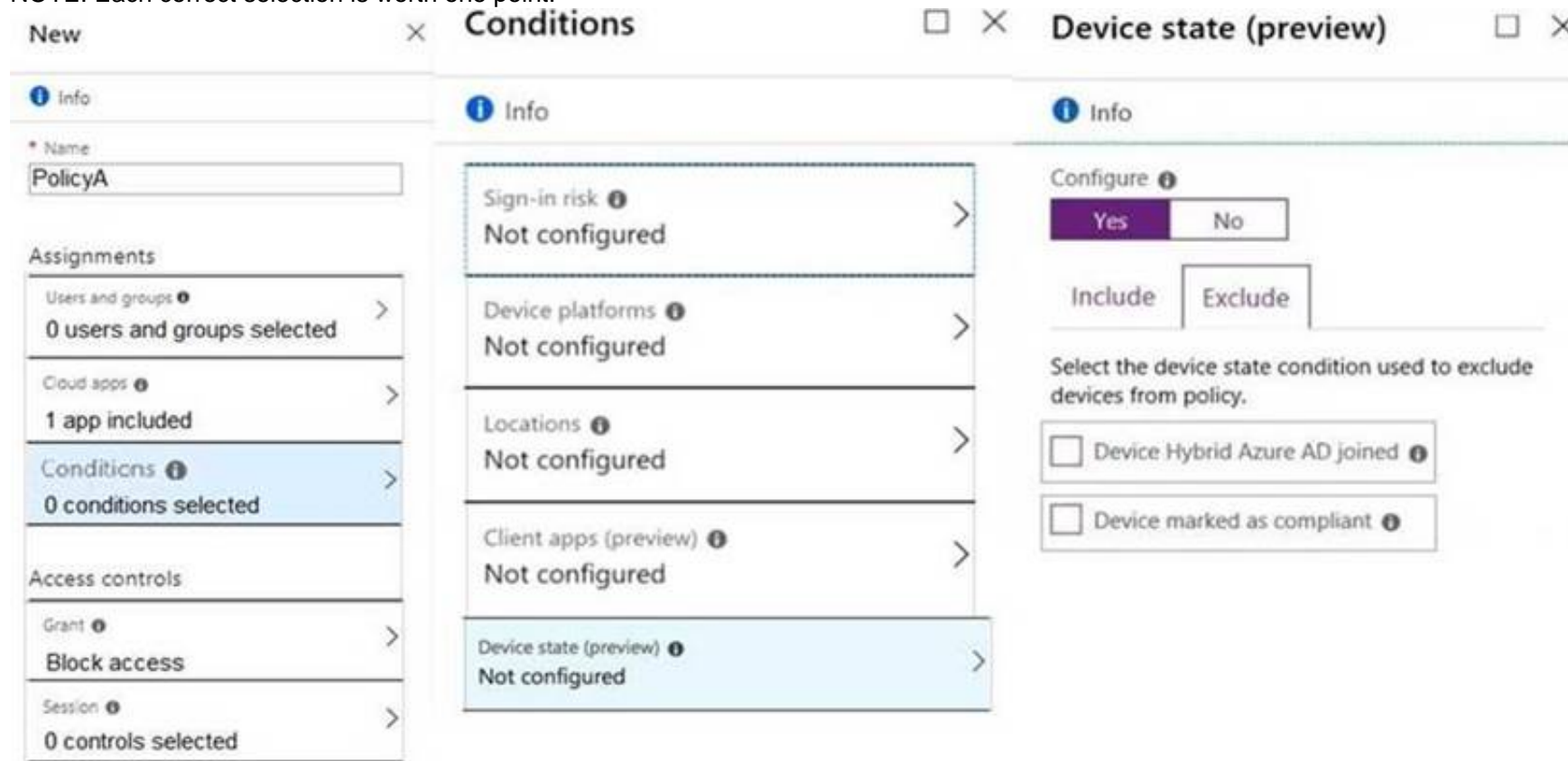
NEW QUESTION 88

- (Exam Topic 3)

You need a new conditional access policy that has an assignment for Office 365 Exchange Online. You need to configure the policy to meet the technical requirements for Group4.

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access

A screenshot of a computer Description automatically generated

We therefore need to exclude compliant devices. From the scenario:

➤ Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions> <https://docs.microsoft.com/en-us/intune/device-compliance-get-started>

NEW QUESTION 89

- (Exam Topic 3)

You are evaluating which devices are compliant.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is compliant	<input type="radio"/>	<input type="radio"/>
Device3 is compliant	<input type="radio"/>	<input type="radio"/>
Device4 is compliant	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is compliant	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant	<input checked="" type="radio"/>	<input type="radio"/>
Device4 is compliant	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 91

- (Exam Topic 3)
You need to meet the technical requirements for the IT department. What should you do first?

- A. From the Azure Active Directory blade in the Azure portal, enable Seamless single sign-on.
- B. From the Configuration Manager console, add an Intune subscription.
- C. From the Azure Active Directory blade in the Azure portal, configure the Mobility (MDM and MAM) settings.
- D. From the Microsoft Intune blade in the Azure portal, configure the Windows enrollment settings.

Answer: C

Explanation:

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

NEW QUESTION 95

- (Exam Topic 2)
What should you configure to meet the technical requirements for the Azure AD-joined computers?

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

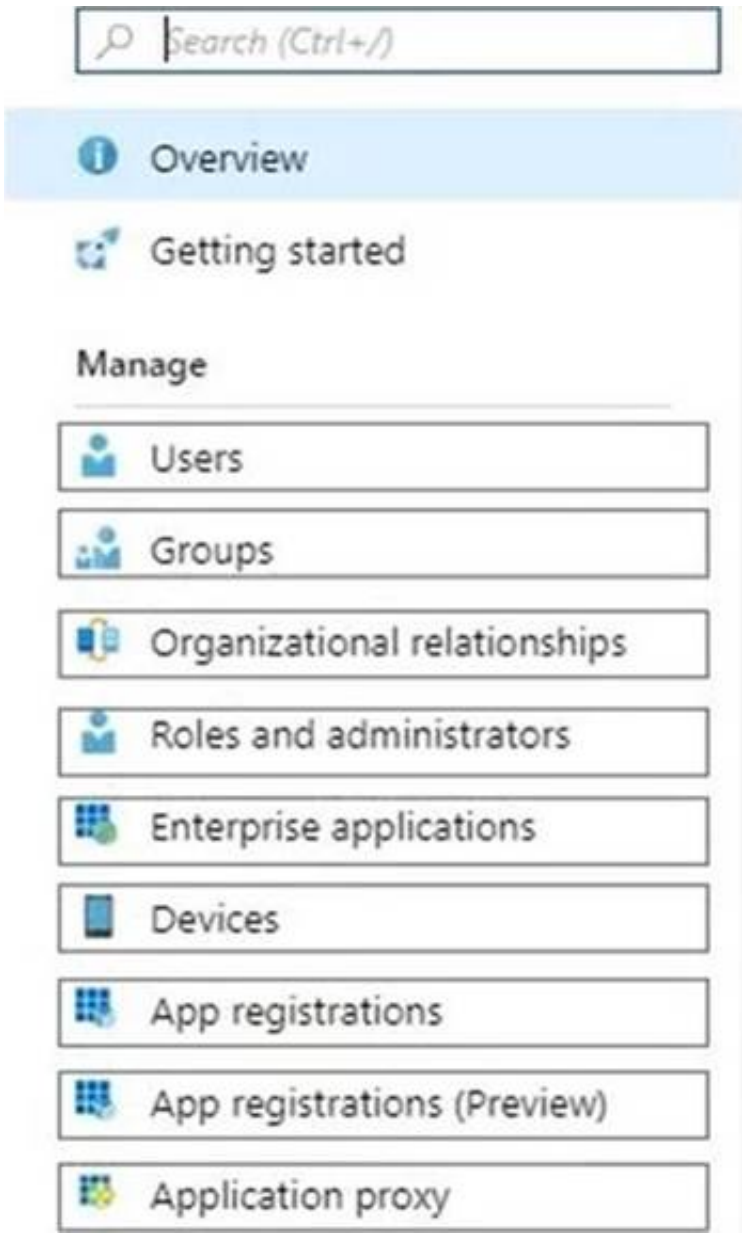
Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-inorgani>

NEW QUESTION 98

- (Exam Topic 2)
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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
References:
<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset>

NEW QUESTION 101

- (Exam Topic 2)
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.

For the Research department employees:

An app configuration policy

An app protection policy

Azure information Protection

iOS app provisioning profiles

For the Sales department employees:

An app configuration policy

An app protection policy

Azure information Protection

iOS app provisioning profiles

- A. Mastered
- B. Not Mastered

Answer: A

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-not-forward-option-fo>

NEW QUESTION 106

- (Exam Topic 2)
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

Answer: B

Explanation:

References:

<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"

NEW QUESTION 107

- (Exam Topic 2)

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

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

Answer: C

Explanation:

References:

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

NEW QUESTION 108

- (Exam Topic 2)

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.

Answer Area

Change Delivery Optimization download mode to:

<input type="checkbox"/>
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:

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

Update Active Hours End to:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with low confidence

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization> <https://2pintsoftware.com/delivery-optimization-dl-mode/>

NEW QUESTION 113

- (Exam Topic 2)

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

Answer: B

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-roaming-windows-settings-refer>

NEW QUESTION 115

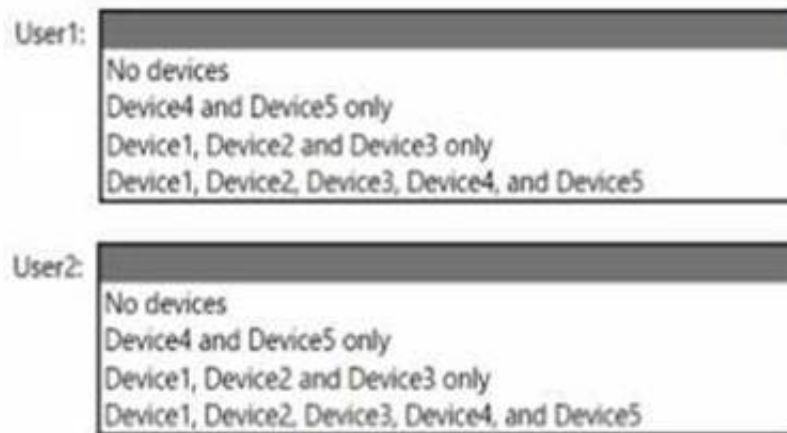
- (Exam Topic 1)

User1 and User2 plan to use Sync your settings.

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

NOTE: Each correct selection is worth one point.

Answer Area



User1:

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

User2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

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

NEW QUESTION 120

- (Exam Topic 1)

You implement Boundary1 based on the planned changes.

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 121

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Scenario: Windows Autopilot Configuration Assignments

Included groups: Group1

Excluded groups: Group2 Device1 is member of Group1.

Device2 is member of Group1 and member of Group2. Device3 is member of Group1.

Group1 and Group2 have a Membership type of Assigned.

Exclusion takes precedence over inclusion in the following same group type scenarios. Reference: <https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments>

NEW QUESTION 126

- (Exam Topic 1)

You implement the planned changes for Connection1 and Connection2

How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2? To answer select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Answer Area

Device1:

1

2

3

4

5

Device2:

1

2

3

4

5

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Device1:

1

2

3

4

5

Device2:

1

2

3

4

5

NEW QUESTION 131

- (Exam Topic 1)

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

NEW QUESTION 136

- (Exam Topic 4)

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

Answer: C

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

NEW QUESTION 139

- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.

Home > Apps >

Create policy

✓ Basics

2 Apps

① Data protection

④ Access requirements

...

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

Target to apps on all device types ⓘ

YesNo

Device types * ⓘ

Unmanaged

Target policy to

All Apps

ⓘ

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

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

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

install the Company Portal app on the device

install the Microsoft Authenticator app on the device

onboard the device to Microsoft Defender for Endpoint

onboard the device to the Microsoft 365 compliance center

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

users only

devices only

users and devices

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Install the Intune Company Portal app on the device
On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.
Box 2: Devices only
For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.
Reference:
<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipado>

NEW QUESTION 140

- (Exam Topic 4)
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

Answer: AC

NEW QUESTION 145

- (Exam Topic 4)

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 A
- D. add an enterprise application.
- E. From the Microsoft Intune admin center, add an app.

Answer: D

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. References:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management>

NEW QUESTION 149

- (Exam Topic 4)

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.

Answer Area

Windows Autopilot: Device1 and Device3 only

In-place upgrade: Device1 and Device3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



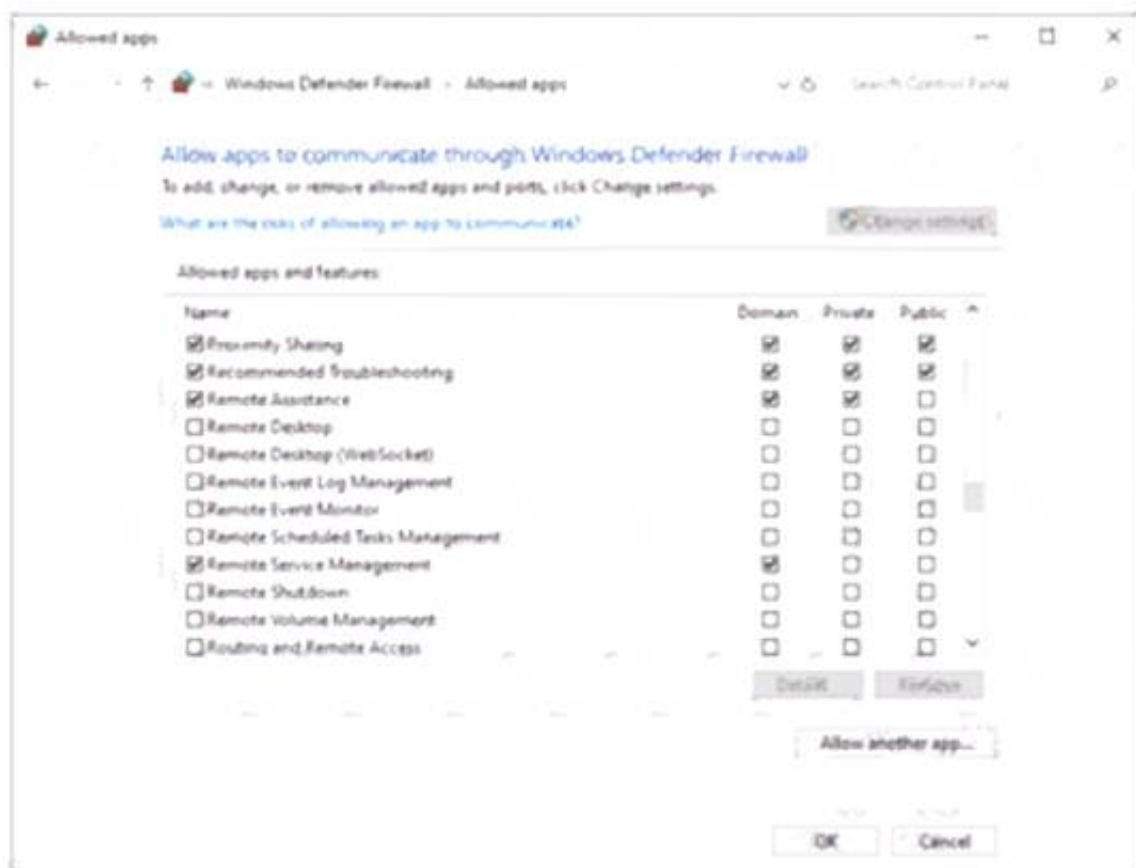
NEW QUESTION 152

- (Exam Topic 4)

Your network contains an Active Directory domain named adatum.com, a workgroup, and computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of	Active Windows Defender Firewall profile
Computer1	Adatum.com	Domain
Computer2	Adatum.com	Domain
Computer3	Workgroup	Public

The local Administrator accounts on Computer1, Computer2, and Computer3 have the same user name and password. On Computer1, Windows Defender Firewall is configured as shown in the following exhibit.



Status	Name	DisplayName
-----	-----	-----
Stopped	RasAuto	Remote Access Auto Connection Manager
Running	RasMan	Remote Access Connection Manager
Stopped	RemoteAccess	Routing and Remote Access
Stopped	RemoteRegistry	Remote Registry
Stopped	RetailDemo	Retail Demo Service
Running	RmSvc	Radio Management Service
Running	RpcEptMapper	RPC Endpoint Mapper
Stopped	RpcLocator	Remote Procedure Call (RPC) Locator
Running	RpcSs	Remote Procedure Call (RPC)

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

NEW QUESTION 153

- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You plan to use Endpoint analytics. You need to create baseline metrics. What should you do first?

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

Answer: C

Explanation:

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

NEW QUESTION 154

- (Exam Topic 4)
You have 1,000 computers that run Windows 10 and are members of an Active Directory domain. You need to capture the event logs from the computers to Azure. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Azure service to provision:

☒

An Azure Storage account

☒

Azure Cosmos DB

☒

Azure SQL Database

☒

Log Analytics

Action to perform on the computers:

☒

Create a collector-initiated subscription

☒

Install the Microsoft Monitoring Agent

☒

Enroll in Microsoft Intune

☒

Register to Azure Active Directory (Azure AD)

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure service to provision:

<input type="checkbox"/>	An Azure Storage account
<input type="checkbox"/>	Azure Cosmos DB
<input type="checkbox"/>	Azure SQL Database
<input checked="" type="checkbox"/>	Log Analytics

Action to perform on the computers:

<input type="checkbox"/>	Create a collector-initiated subscription
<input checked="" type="checkbox"/>	Install the Microsoft Monitoring Agent
<input type="checkbox"/>	Enroll in Microsoft Intune
<input type="checkbox"/>	Register to Azure Active Directory (Azure AD)

NEW QUESTION 157

- (Exam Topic 4)

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

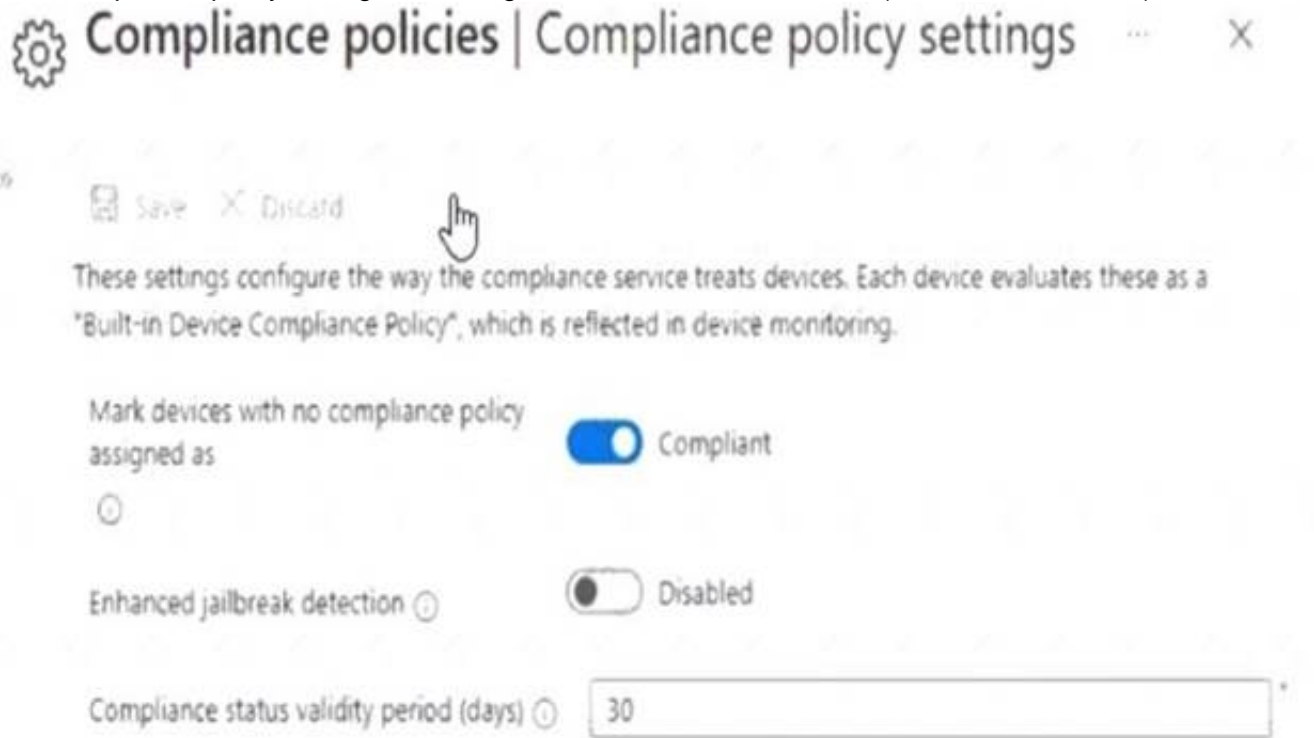
Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.

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

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

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



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

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 162

- (Exam Topic 4)

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

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

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

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

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

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Device1 is marked as compliant = No Device2 is marked as compliant = Yes Device3 is marked as comp
 = No

- Device1 is marked as noncompliant because it does not meet the minimum OS version requirement of Policy1, which is 11.0.0. Device1 has an OS version of 10.0.0, which is lower than the required version1.
- Device2 is marked as compliant because it meets all the requirements of Policy2, which are: minimum OS version of 10.0.0, password required, and encryption enabled. Device2 has an OS version of 11.0.0, a password set, and encryption enabled1.
- Device3 is marked as noncompliant because it does not meet the encryption requirement of Policy3, which is enabled. Device3 has encryption disabled1.

NEW QUESTION 167

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

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

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 171

- (Exam Topic 4)

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.

Answer: B

NEW QUESTION 174

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a group named Group1.

You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.

You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.

What should you configure?

- A. Session access controls
- B. an assignment that uses a User risk condition
- C. an assignment that uses a Sign-in risk condition
- D. Grant access controls

Answer: A

Explanation:

User sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.

Sign-in frequency control

- > Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
- > Browse to Azure Active Directory > Security > Conditional Access.
- > Select New policy.
- > Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
- > Choose all required conditions for customer's environment, including the target cloud apps.
- > Under Access controls > Session.

Select Sign-in frequency.

Choose Periodic reauthentication and enter a value of hours or days or select Every time.

- > Save your policy. Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life>

NEW QUESTION 176

- (Exam Topic 4)

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.

Answer: CE

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. References:

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

NEW QUESTION 178

- (Exam Topic 4)

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

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

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

 Save
  Discard

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

Mark devices with no compliance policy assigned as 

Compliant

Not Compliant

Enhanced jailbreak detection 

Enabled

Disabled

Compliance status validity period (days) 

30 

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

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

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO. Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until june 10th.
 Source:
 Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.
 When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.
 This action is supported on all platforms supported by Intune. <https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance>

NEW QUESTION 180

- (Exam Topic 4)

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

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

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

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

Answer: B

Explanation:

* Admin1
 An application admin has full access to enterprise applications, applications registrations, and application proxy settings.
 * Admin2
 Mark your app as publisher verified.
 In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.
 * Admin3
 Office Apps admin - Assign the Office Apps admin role to users who need to do the following:
 - Use the Office cloud policy service to create and manage cloud-based policies for Office
 - Create and manage service requests
 - Manage the What's New content that users see in their Office apps
 - Monitor service health Reference:
 Office Apps admin - Assign the Office Apps admin role to users who need to do the following <https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified>

NEW QUESTION 183

- (Exam Topic 4)

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.

Answer Area

Statements	Yes	No
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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 185

- (Exam Topic 4)

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

AH 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.

Answer Area

• • • • •

Policy type:

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

Minimum number of policies:

1
2
3
4
5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
of Corre 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 installed. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protection-policies/troubleshoot-cut-copy-paste>

NEW QUESTION 188

- (Exam Topic 4)
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.

Answer: C

NEW QUESTION 190

- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices. You need to create Intune configuration profiles to perform the following actions on the devices:
• Deploy a custom Start layout.
• Rename the local Administrator account.
Which profile type template should you use for each action? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Deploy a custom Start layout:

Device restriction

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Rename the local Administrator account:

Identity protection

Delivery optimization

Device restriction

Endpoint protection

Identity protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Deploy a custom Start layout:

Device restriction

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Rename the local Administrator account:

Identity protection

Delivery optimization

Device restriction

Endpoint protection

Identity protection

NEW QUESTION 195

- (Exam Topic 4)
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

Answer: C

NEW QUESTION 197

- (Exam Topic 4)
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 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

- A. Mastered
- B. Not Mastered

Answer: A

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. References:

<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. References:

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

NEW QUESTION 201

- (Exam Topic 4)

Your company implements Azure AD, Microsoft 365, Microsoft Intune, and Azure Information Protection. The company's security policy states the following:

- Personal devices do not need to be enrolled in Intune.
- Users must authenticate by using a PIN before they can access corporate email data.

- Users can use their personal iOS and Android devices to access corporate cloud services.
 - Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.
- You need to configure a solution to enforce the security policy. What should you create?

- A. a device configuration profile from the Microsoft Intune admin center
- B. a data loss prevention (DLP) policy from the Microsoft Purview compliance portal
- C. an insider risk management policy from the Microsoft Purview compliance portal
- D. an app protection policy from the Microsoft Intune admin center

Answer: B

NEW QUESTION 204

- (Exam Topic 4)

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)

Answer: C

NEW QUESTION 209

- (Exam Topic 4)

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

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

- A. Device 1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, Device3, and Device4

Answer: C

NEW QUESTION 214

- (Exam Topic 4)

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).

Answer: A

NEW QUESTION 216

- (Exam Topic 4)

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

NEW QUESTION 221
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the objects shown in the following table. You are creating a compliance policy named Compliance1. Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

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

Answer: C

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

NEW QUESTION 223
- (Exam Topic 4)
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+ /)

Overview

All apps

Monitor

By platform

Windows

iOS/iPadOS

macOS

Android

Policy

App protection policies

App configuration policies

+ Add

Refresh

Filter

Export

Columns

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 227

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 232

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10. You implement hybrid Azure AD and Microsoft Intune.

You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort. What should you use?

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

Answer: D

NEW QUESTION 233

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You add apps to Intune as shown in the following table.

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

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

Answer: D

NEW QUESTION 236

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You use Microsoft Intune Suite to manage devices.

You have the iOS app protection policy shown in the following exhibit.

Access requirements

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS 11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after (minutes of inactivity)	30

Conditional launch

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access

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 Area

After 30 minutes of inactivity, a user will be prompted for their [answer choice].

PIN only

account credentials only

PIN only

PIN and account credentials

Entering the wrong PIN five times will [answer choice].

block access

block access

reset the app PIN

reset the device PIN

wipe company data

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1 = PIN only

Box 2 = reset the PIN app

iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios>

NEW QUESTION 239

- (Exam Topic 4)

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.

Answer Area

Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll> <https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/>

NEW QUESTION 240

- (Exam Topic 4)

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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with medium confidence

Reference:

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

NEW QUESTION 242

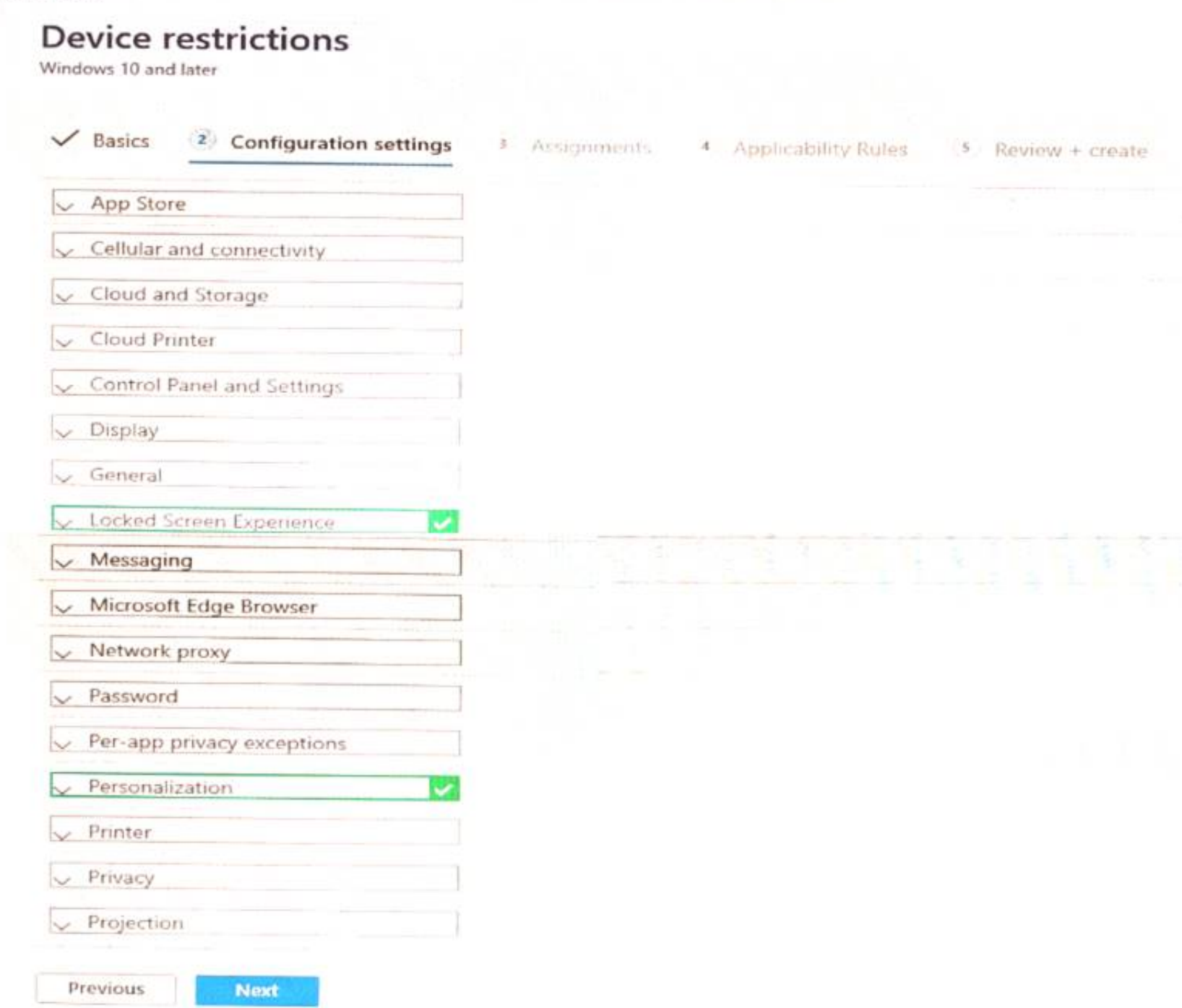
- (Exam Topic 4)

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.

Answer Area



Device restrictions
Windows 10 and later

1 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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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**

NEW QUESTION 247

- (Exam Topic 4)

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.

Answer Area

Azure AD joined: **Device1 and Device2 only**

Registered in contoso.com: **Device1 and Device2 only**

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 250

- (Exam Topic 4)
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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 252

- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:
• For the WinRM service, set Startup type to Automatic.

- Create a listener that accepts requests from any IP address.
- Enable a firewall exception for WS-Management communications. Which PowerShell cmdlet should you use?

- A. Connect-WSMan
- B. Enable-PSRemoting
- C. Invoke-WSManAction
- D. Enable-PSSessionConfiguration

Answer: B

NEW QUESTION 257

- (Exam Topic 4)
You have the device configuration profile shown in the following exhibit.

Kiosk

Windows 10 and later

✓ Basics

2 Configuration settings

③ 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 *

Single app, full-screen kiosk

User logon type *

Auto logon (Windows 10, version 1803+)

Application type *

Add Microsoft Edge browser

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 *

https://contoso.com

Microsoft Edge kiosk mode type

Public Browsing (InPrivate)

Refresh browser after idle time

5

Specify Maintenance Window for App Restarts *

Require

Not configured

Maintenance Window Start Time

MM/DD/YYYY

☐

h:mm:ss A

Maintenance Window Recurrence

Daily (recommended)

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 Area

Users	<div>can access any URL.</div> <div>cannot view the address bar in Microsoft Edge.</div> <div>can only access URLs that include contoso.com.</div> <div>can only access URLs that start with https://contoso.com/ .</div>
Windows 10 devices can have	<div>a single Microsoft Edge instance that has a single tab.</div> <div>a single Microsoft Edge instance that has multiple tabs.</div> <div>multiple Microsoft Edge instances that have multiple tabs.</div> <div>multiple Microsoft Edge instances that each has a single tab.</div>

- A. Mastered
- B. Not Mastered

Answer: A

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

he 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. References:

<https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings#kiosk-browser-settings>

NEW QUESTION 260

- (Exam Topic 4)

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

Answer: B

NEW QUESTION 262

- (Exam Topic 4)

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

Answer: A

NEW QUESTION 264

- (Exam Topic 4)

You use Microsoft Endpoint Manager to manage Windows 10 devices.

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

- Compliance policy trends
- Trends in device and user enrolment
- App and operating system version breakdowns of mobile devices

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

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Data source:

Audit logs in Azure Active Directory (Azure AD)

Audit logs in Microsoft Intune

Azure Synapse Analytics

The Microsoft Intune Data Warehouse

Data visualization tool:

Azure Data Studio

Microsoft Power BI

The Azure portal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports> <https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi>

NEW QUESTION 268
- (Exam Topic 4)
You have a hybrid Azure AD tenant.
You configure a Windows Autopilot deployment profile as shown in the following exhibit.

Create profile

Windows PC

Basics

2 Out-of-box experience (OOBE)

3 Scope tags

4 Assignments

5 Review + create

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

* Deployment mode ⓘ

User-Driven

* Join to Azure AD as ⓘ

Azure AD joined

Microsoft Software License Terms ⓘ

Show

Hide

ⓘ Important information about hiding license terms

Privacy settings ⓘ

Show

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 ⓘ

Show

Hide

User account type ⓘ

Administrator

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.

Answer Area

To apply the profile to a new computer, you must first

▼

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

When the Windows Autopilot profile is applied to a computer, the computer will be

▼

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

To apply the profile to a new computer, you must first

▼

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

When the Windows Autopilot profile is applied to a computer, the computer will be

▼

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

NEW QUESTION 272

- (Exam Topic 4)

Your company standardizes on Windows 10 Enterprise for all users.

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

You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to 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)

Answer: A

NEW QUESTION 275

- (Exam Topic 4)

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

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

Which groups can you add to Group4?

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

Answer: C

NEW QUESTION 277

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

MD-102 Practice Exam Features:

- * MD-102 Questions and Answers Updated Frequently
- * MD-102 Practice Questions Verified by Expert Senior Certified Staff
- * MD-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * MD-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The MD-102 Practice Test Here](#)