

Microsoft

Exam Questions MD-102

Endpoint Administrator



NEW QUESTION 1

- (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: User2
 - o Cloud apps or actions: Office 365 Exchange Online
 - o Conditions
 - Device platforms: Android, iOS
 - Filter for devices: 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 2

- (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 3

- (Exam Topic 4)

You create a Windows Autopilot deployment profile.

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

- > Include the hardware serial number in the computer name.

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

NOTE: Each correct selection is worth one point.

Answer Area

Create profile ...

Windows PC

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 4

- (Exam Topic 4)

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

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

You need to migrate the GPO to Intune.

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

Actions		Answer Area
<input type="text" value="Assign the policy."/>		
<input type="text" value="Create a compliance policy."/>		
<input type="text" value="Set a scope tag to the policy."/>		
<input type="text" value="Import an ADMX file."/>		
<input type="text" value="Create a configuration profile."/>		
<input type="text" value="Configure the Administrative Templates settings."/>		
<input type="text" value="Assign the profile."/>		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions		Answer Area
<input type="text" value="Assign the policy."/>		
<input type="text" value="Create a compliance policy."/>		<input type="text" value="Create a configuration profile."/>
<input type="text" value="Set a scope tag to the policy."/>		<input type="text" value="Configure the Administrative Templates settings."/>
<input type="text" value="Import an ADMX file."/>		
<input type="text" value="Create a configuration profile."/>		
<input type="text" value="Configure the Administrative Templates settings."/>		
<input type="text" value="Assign the profile."/>		<input type="text" value="Assign the profile."/>

NEW QUESTION 5

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to meet the following requirements during device provisioning:

- Display the progress of app and profile deployments.
- Join the devices to Azure AD.

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings

- CNAME Validation
- Co-management Settings
- Deployment Profiles
- Enrollment notifications
- Enrollment Status Page

Answer Area

Display the progress of app and profile deployments:

Join the devices to Azure AD:

NEW QUESTION 6

- (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 7

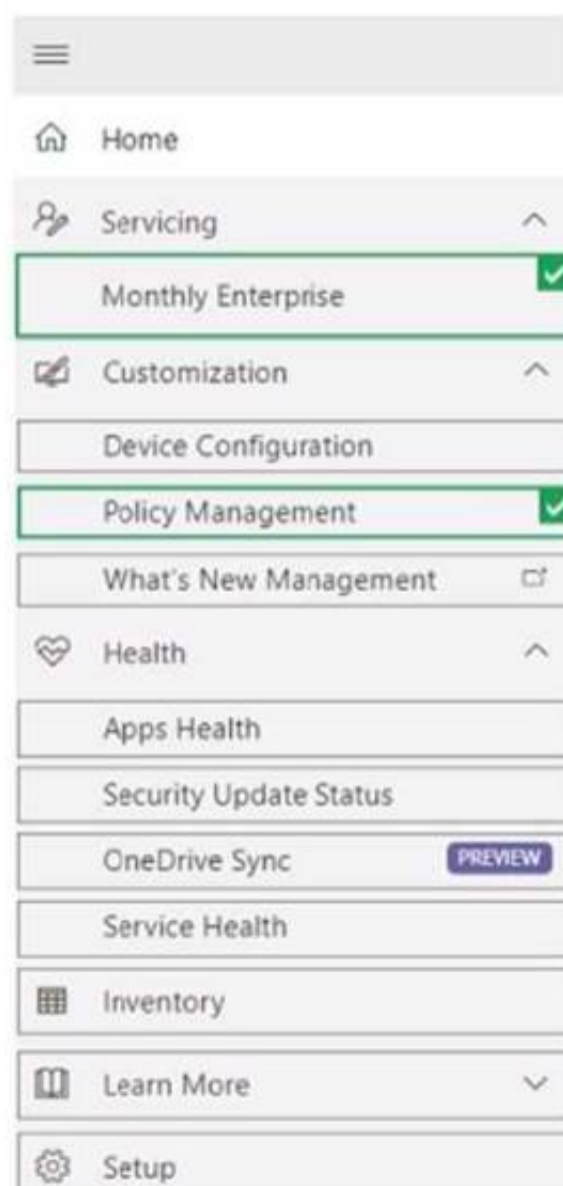
- (Exam Topic 4)

You have a Microsoft 365 subscription. All users have Microsoft 365 apps deployed. You need to configure Microsoft 365 apps to meet the following requirements:

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

Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 8

- (Exam Topic 4)

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

Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.

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

NOTE: Each correct selection is worth one point.

Device1:

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

Device2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:
 Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
 Graphical user interface, text, application, email Description automatically generated

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

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

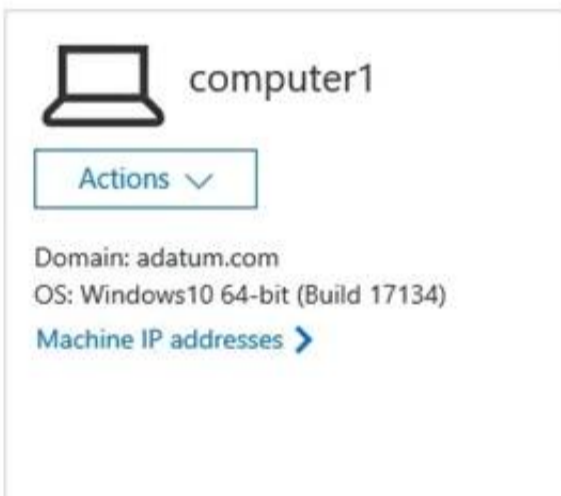
NEW QUESTION 9

- (Exam Topic 4)

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

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

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



What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of:

▼
Group3 only
Group4 only
Group5 only
Group3, Group4, and Group5 only

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1 will be a member of:

▼
Group3 only
Group4 only
Grou5 only
Group3, Group4, and Group5 only

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

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

NEW QUESTION 10

- (Exam Topic 4)

You have a computer named Computed that has Windows 10 installed. You create a Windows PowerShell script named config.psl. You need to ensure that config.psl runs after feature updates are installed on Computer5. Which file should you modify on Computer5?

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

Answer: B

Explanation:

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

NEW QUESTION 10

- (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 12

- (Exam Topic 4)

Your company has a Remote Desktop Gateway (RD Gateway). You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway. You need to configure a Remote Desktop connection to connect through the gateway. Which setting should you configure?

- A. Connect from anywhere
- B. Server authentication
- C. Connection settings
- D. Local devices and resources

Answer: A

Explanation:

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

NEW QUESTION 17

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share 1. You add Windows 10 images to Share1 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:

- 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

- 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

- (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 19

- (Exam Topic 4)

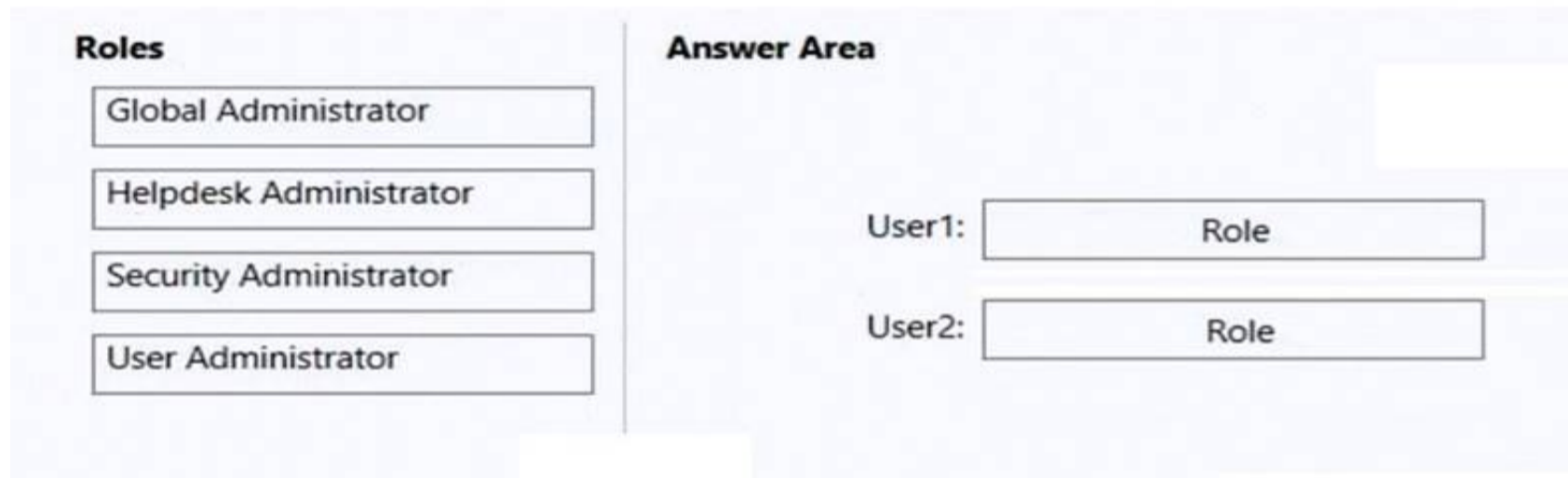
You have a Microsoft 365 subscription that contains two users named User1 and User2. You need to ensure that the users can perform the following tasks:

- User1 must be able to create groups and manage users.
- User2 must be able to reset passwords for non-administrative users. The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

NEW QUESTION 21

- (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 23

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to ensure that you can deploy apps to Android Enterprise devices. What should you do first?

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

Answer: D

NEW QUESTION 25

- (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 builds can access network resources.

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

NOTE: Each correct selection is worth one point.

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:

Box 1:
 Device Compliance settings for Windows 10/11 in Intune
 There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.
 Note: Windows Health Attestation Service evaluation rules Require BitLocker:
 Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user data. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.
 Not configured (default) - This setting isn't evaluated for compliance or non-compliance.
 Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.

Box 2: Prevent jailbroken devices from having corporate access Device Compliance settings for iOS/iPadOS in Intune
 There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.
 Device Health Jailbroken devices
 Supported for iOS 8.0 and later
 Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted (jailbroken) devices as not compliant.

Box 3: Prevent rooted devices from having corporate access. Device compliance settings for Android Enterprise in Intune
 There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.
 Device Health - for Personally-Owned Work Profile Rooted devices
 Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted devices as not compliant.
 Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios>

NEW QUESTION 30

- (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 31

- (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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



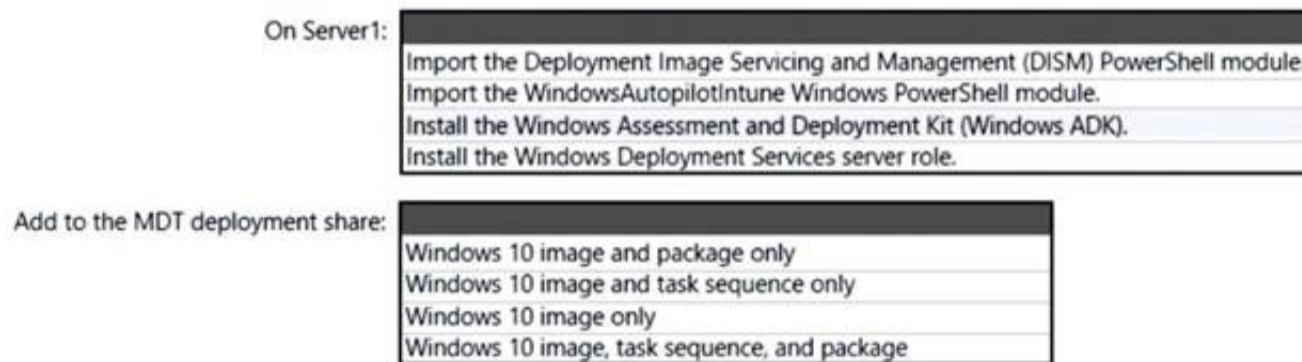
NEW QUESTION 36

- (Exam Topic 4)

You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed. You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard. You need to create a deployment share on Server1. What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Install the Windows Deployment Services role. Install and initialize Windows Deployment Services (WDS) On the server: Open an elevated Windows PowerShell prompt and enter the following command: `Install-WindowsFeature -Name WDS -IncludeManagementTools WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall" WDSUTIL /Set-Server /AnswerClients:All`
 Box 2: Windows 10 image and task sequence only Create the reference image task sequence
 In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.
 Reference:
<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment>
<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-im>

NEW QUESTION 39

- (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 43

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

NEW QUESTION 47

- (Exam Topic 3)

You need to prepare for the deployment of the Phoenix office computers. What should you do first?

- A. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory admin center.
- B. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.
- C. Extract the hardware ID information of each computer to an XML file and upload the file from the Devices settings in Microsoft Store for Business.
- D. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

Answer: A

Explanation:

Reference:

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

NEW QUESTION 49

- (Exam Topic 3)

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1 can enroll a maximum of:

<input type="checkbox"/>	5 devices
<input type="checkbox"/>	10 devices
<input type="checkbox"/>	15 devices
<input type="checkbox"/>	1,000 devices
<input type="checkbox"/>	An unlimited number of devices

User2 can enroll a maximum of:

<input type="checkbox"/>	5 devices
<input type="checkbox"/>	10 devices
<input type="checkbox"/>	15 devices
<input type="checkbox"/>	1,000 devices
<input type="checkbox"/>	An unlimited number of devices

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:

<input checked="" type="checkbox"/>	5 devices
<input checked="" type="checkbox"/>	10 devices
<input type="checkbox"/>	15 devices
<input type="checkbox"/>	1,000 devices
<input type="checkbox"/>	An unlimited number of devices

User2 can enroll a maximum of:

<input type="checkbox"/>	5 devices
<input type="checkbox"/>	10 devices
<input checked="" type="checkbox"/>	15 devices
<input checked="" type="checkbox"/>	1,000 devices
<input type="checkbox"/>	An unlimited number of devices

NEW QUESTION 54

- (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 57

- (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 58

- (Exam Topic 2)

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

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

Answer: B

Explanation:

References:

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

NEW QUESTION 61

- (Exam Topic 2)

You need to meet the OOB requirements for Windows AutoPilot.

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

NOTE: Each correct selection is worth one point.

Overview

Getting started

Manage

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

- <https://blogs.msdn.microsoft.com/sgern/2018/10/11/intune-intune-and-autopilot-part-3-preparing-your-environm>
- <https://blogs.msdn.microsoft.com/sgern/2018/11/27/intune-intune-and-autopilot-part-4-enroll-your-first-device/>

NEW QUESTION 63

- (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:

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

For the Sales department employees:

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

- 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 66

- (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 69

- (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 73

- (Exam Topic 1)

Which user can enroll Device6 in Intune?

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

Answer: B

NEW QUESTION 78

- (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]

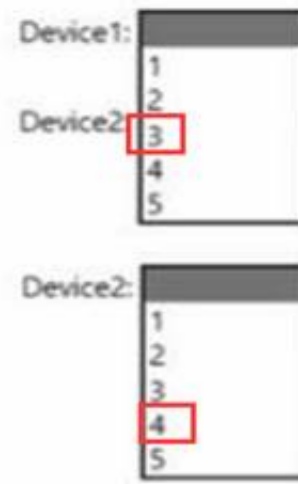
Device2: [1, 2, 3, 4, 5]

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 82

- (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.

Device4 is marked as compliant.

Device5 is marked as compliant.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

NEW QUESTION 83

- (Exam Topic 1)

Which users can purchase and assign App1?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 86

- (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.

Answer Area

Statements

Yes No

If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.

If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.

If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Text, letter Description automatically generated

NEW QUESTION 87

- (Exam Topic 4)

You have an Azure AD tenant that contains the devices shown in the following table. You purchase Windows 11 Enterprise E5 licenses. Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

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

Answer: B

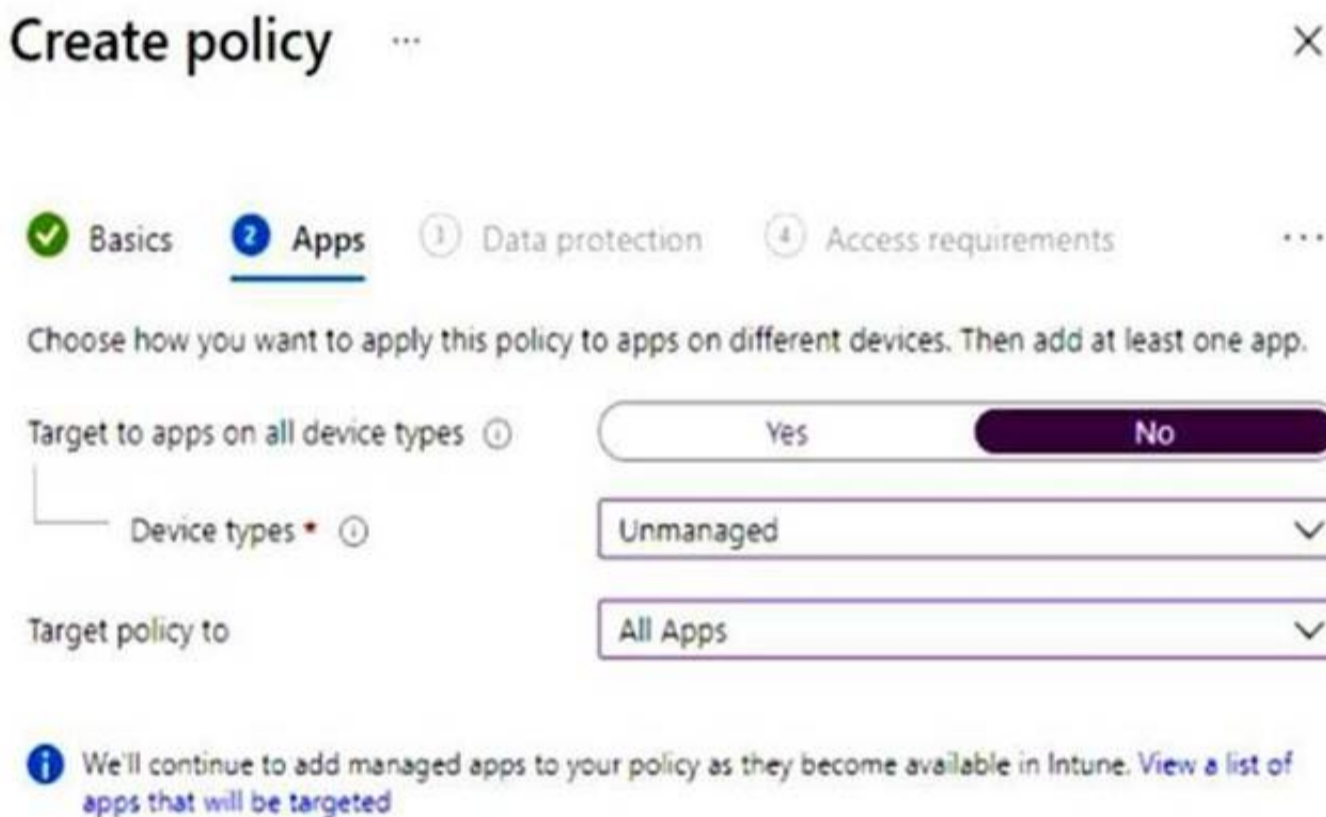
NEW QUESTION 90

- (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](#) >



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 91

- (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 92

- (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 94

- (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:

 **Compliance policies | Compliance policy settings** ... X

Save X 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

Enhanced jailbreak detection Disabled

Compliance status validity period (days)

- Name: Policy1
- Assignments
 - o Users and groups: User1
 - o Cloud apps or actions: Office 365 SharePoint Online

- Access controls
 - 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 99

- (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 102

- (Exam Topic 4)

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

You use Microsoft Intune to manage devices.

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

What should you configure?

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

Answer: D

NEW QUESTION 107

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort. What should you do?

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

Answer: C

Explanation:

To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices. References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-install-with-int>

NEW QUESTION 111

- (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 112

- (Exam Topic 4)

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

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1. All the users use Microsoft Excel.

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	<input type="radio"/>	<input type="radio"/>
When User2 saves a new spreadsheet, the .xlsb format is used.	<input type="radio"/>	<input type="radio"/>
When User3 saves a new spreadsheet, the .xlsx format is used.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No
 User1 is member of Group1 and Group2.
 Policy1 with priority 0 is assigned to Group1: default file format for Excel is.ods. Policy2 with priority 1 is assigned to Group2: default file format for Excel is.xlsb.
 Note: Key points to remember about policy order
 Policies are assigned an order of priority. Devices receive the first applied policy only.
 You can change the order of priority for policies. Default policies are given the lowest order of priority. Box 2: Yes
 User2 is member of Group2.
 Group2 and Group3 are members of Group1. Box 3: No
 User3 is member of Group3.
 Group2 and Group3 are members of Group1.
 Reference: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-policy-order>

NEW QUESTION 115

- (Exam Topic 4)
 You have a Microsoft 365 tenant that contains the objects shown in the following table.

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

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

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

Answer: C

Explanation:

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

- > Admin1 is an individual user account that belongs to the Global administrators
- > Group1 is a user group that contains 100 users.
- > Group2 is a device group that contains 50 devices.
- > Group3 is a user group that contains 200 users.
- > Group4 is a device group that contains 150 devices.

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

NEW QUESTION 117

- (Exam Topic 4)
 You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:

- Requires BitLocker Drive Encryption (BitLocker) on each device

- Requires a minimum operating system version

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings	Answer Area
Device Health	Requires BitLocker: System Security
Device Properties	Requires a minimum operating system version: Device Properties
Microsoft Defender for Endpoint	
System Security	

NEW QUESTION 122

- (Exam Topic 4)

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

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

The devices are members of a group named Group1.

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

- Name: Network1
- IPv4 range: 192.168.0.0/16

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

- Name: Policy1
- Device health: Rooted devices: Block
- Locations: Location: Network1
- Mark device noncompliant: Immediately
- Assigned: Group1

The Intune device compliance policy has the following configurations:

- Mark devices with no compliance policy assigned as: Compliant
- Enhanced jailbreak detection: Enabled
- Compliance status validity period (days): 20

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

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 compliant. = No

- > Device1 is marked as noncompliant because it is rooted and the device compliance policy Policy1 blocks rooted devices under the Device health setting1.
- > Device2 is marked as compliant because it is not rooted and it is within the network location Network1 that is specified in the device compliance policy Policy11.
- > Device3 is marked as noncompliant because it is outside the network location Network1 that is specified in the device compliance policy Policy11. The device compliance location setting requires devices to be in a specific network range to be compliant2.

NEW QUESTION 123

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune. You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

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

Which three provisioning options can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: BDE

NEW QUESTION 125

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune.

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

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

From the Microsoft Intune admin center, you select Uninstall for the feature updates of UpdateRing1. When will devices start to remove the feature updates?

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

Answer: C

NEW QUESTION 128

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You need to create Endpoint security policies to meet the following requirements:

- > Hide the Firewall & network protection area in the Windows Security app.
- > Disable the provisioning of Windows Hello for Business on the devices.

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

NOTE: Each correct selection is worth one point.

Answer Area

Manage

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

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

Windows Hello for Business settings are configured in Identity protection. Reference:

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

NEW QUESTION 131

- (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

- ✓ 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

NEW QUESTION 135

- (Exam Topic 4)

You have computers that run Windows 10 and are managed by using Microsoft Intune. Users store their files in a folder named D:\Folder1.

You need to ensure that only a trusted list of applications is granted write access to D:\Folder1. What should you configure in the device configuration profile?

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

Answer: A

NEW QUESTION 139

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers. You need to prevent users from disabling Microsoft Defender Antivirus, What should you do?

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

Answer: B

Explanation:

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

NEW QUESTION 140

- (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

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

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

* Deployment mode

* Join to Azure AD as

Microsoft Software License Terms

i Important information about hiding license terms

Privacy settings

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

Hide change account options

User account type

Allow White Glove OOBE 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 145

- (Exam Topic 4)

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

shown in the following table.

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

You assign Windows 10/11 Enterprise E5 licenses to Gtoup1 and Uset2. You deploy the devices shown in the following table.

Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device3	Windows 10 Pro	Azure AD

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 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input checked="" type="checkbox"/>
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	<input checked="" type="checkbox"/>	<input type="radio"/>
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.	<input type="radio"/>	<input checked="" type="checkbox"/>

NEW QUESTION 146

- (Exam Topic 4)

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

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

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

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

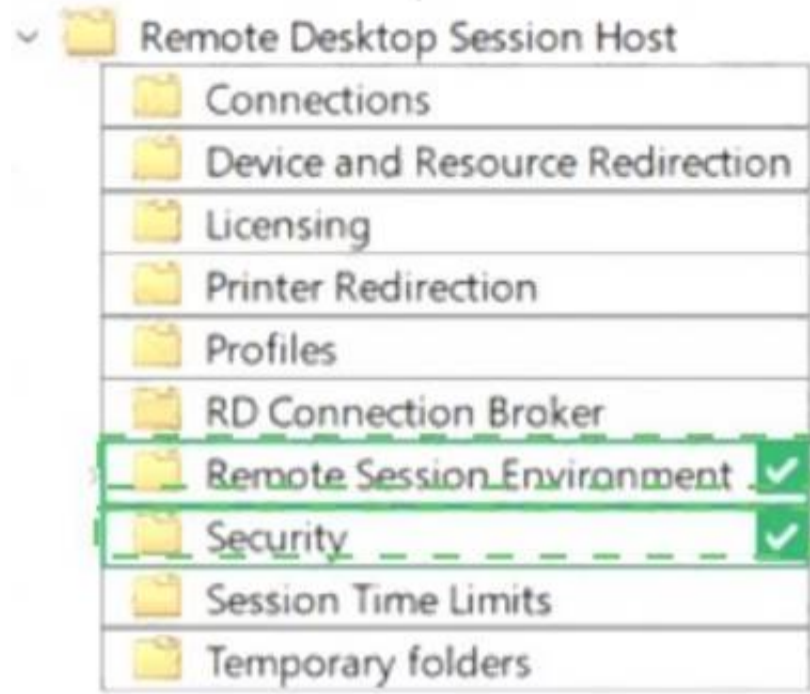
Remote Desktop Session Host

Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment <input checked="" type="checkbox"/>
Security <input checked="" type="checkbox"/>
Session Time Limits
Temporary folders

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 150

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * MD-102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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