

Microsoft

Exam Questions MD-102

Endpoint Administrator



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:
<https://blog.matrixpost.net/set-up-windows-autopilot-production-environment-part-2/>

NEW QUESTION 2

- (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 3

- (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.	<input type="radio"/> <input type="radio"/>
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<input type="radio"/> <input type="radio"/>
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	<input type="radio"/> <input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, letter Description automatically generated

NEW QUESTION 4

- (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 5

- (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 6

- (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 7

- (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 8

- (Exam Topic 3)

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 36S 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 9

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and a computer that runs Windows 11. You need to create a customized installation of Microsoft 365 Apps for enterprise.

Which four actions should you perform in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the

correct order.

Actions

Run setup.exe and specify the /packager switch.

Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.

Edit the XML configuration file.

Run setup.exe and specify the /download switch.

Run setup.exe and specify the /configure switch.

Answer Area

>

<

^

v

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. Download ODT application
 - * 2. Create a configuration file (XML)
 - * 3. setup.exe /download to download the installation files
 - * 4. setup.exe /configure to deploy the application
- https://learn.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-local-source

NEW QUESTION 10

- (Exam Topic 3)

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com. Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

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:

Server1

Server2

Server3

Server4

Ports:

TCP 443 only

UDP 443 only

TCP 1723 only

TCP 443 and UDP 443 only

TCP 443, TCP 1723, and UDP 443

- 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 14

- (Exam Topic 3)

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

can access any URL.

cannot view the address bar in Microsoft Edge.

can only access URLs that include contoso.com.

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

Windows 10 devices can have

a single Microsoft Edge instance that has a single tab.

a single Microsoft Edge instance that has multiple tabs.

multiple Microsoft Edge instances that have multiple tabs.

multiple Microsoft Edge instances that each has a single tab.

- 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 18

- (Exam Topic 3)

You have a Microsoft 365 subscription that includes Microsoft Intune.

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

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

What should you configure? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all.

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

NOTE: Each correct selection is worth one point.

Features	Answer Area
A device restriction policy	Enforces compliance: <input type="text"/>
A security baseline	Prevents suspicious scripts: <input type="text"/>
An attack surface reduction (ASR) rule	
An Intune connection	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in Defender for Endpoint. You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. References: <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/conditional-access>

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

NEW QUESTION 19

- (Exam Topic 3)

You have a Microsoft 365 subscription.

All users have Microsoft 365 apps deployed.

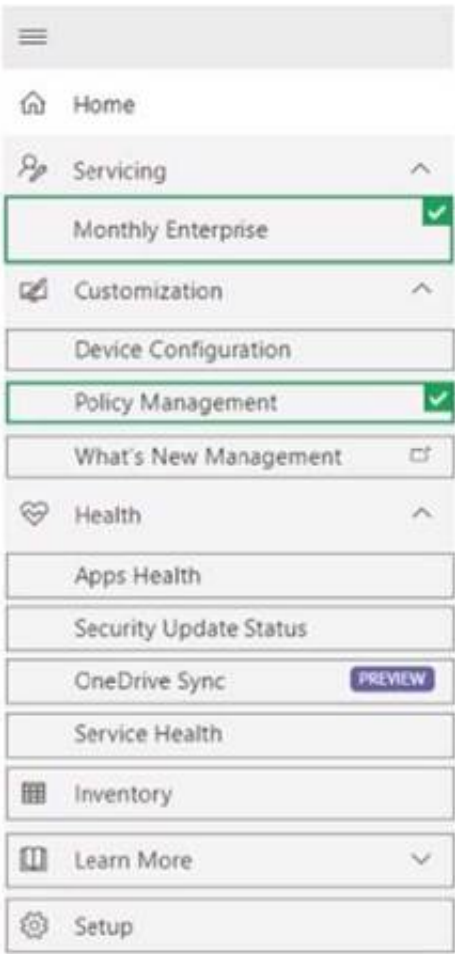
You need to configure Microsoft 365 apps to meet the following requirements:

- 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 20

- (Exam Topic 3)

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

Computer1 has apps that are compatible with Windows 10.

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

Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 24

- (Exam Topic 3)

You have a Microsoft Intune subscription.

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

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

An app named App1 is installed on each device.

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

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

Answer: B

Explanation:

The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn

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

NEW QUESTION 25

- (Exam Topic 3)

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

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2, and Device3 only

Device1, Device2, Device3, and Device4

Registered in contoso.com:

Device1 and Device2 only

Device1 and Device2 only

Device2 and Device3 only

Device3 and Device4 only

Device2, Device3, and Device4 only

Device1, Device2, Device3, and Device4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure AD joined:

Device1 and Device2 only

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2, and Device3 only

Device1, Device2, Device3, and Device4

Registered in contoso.com:

Device1 and Device2 only

Device1 and Device2 only

Device2 and Device3 only

Device3 and Device4 only

Device2, Device3, and Device4 only

Device1, Device2, Device3, and Device4

NEW QUESTION 26

- (Exam Topic 3)

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

The screenshot shows two dropdown menus. The 'Sales' dropdown is open, showing options: 'Windows Autopilot with automatic registration' (selected), 'Configuration Manager', 'Windows Autopilot with automatic registration', 'Windows Autopilot with manual registration', and 'Windows Autopilot with OEM registration'. The 'Marketing' dropdown is also open, showing options: 'Configuration Manager' (selected), 'Configuration Manager', 'Windows Autopilot with automatic registration', 'Windows Autopilot with manual registration', and 'Windows Autopilot with OEM registration'.

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

The screenshot shows the same two dropdown menus as before. In the 'Sales' dropdown, 'Windows Autopilot with automatic registration' is highlighted with a red box. In the 'Marketing' dropdown, 'Configuration Manager' is highlighted with a red box.

NEW QUESTION 31

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:

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

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

Answer: A

Explanation:

A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more. A configuration profile is a template that contains one or more settings that you can apply to groups of devices. References:

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

NEW QUESTION 32

- (Exam Topic 3)

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 33

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released. What should you create?

- A. a device configuration profile based on the Device features template
- B. a device configuration profile based on the Device restrictions template
- C. an update policy for iOS/iPadOS
- D. an iOS app provisioning profile

Answer: C

Explanation:

Manage iOS/iPadOS software update policies in Intune, delay visibility of software updates.

When you use update policies for iOS, you might have need to delay visibility of an iOS software update. Reasons to delay visibility include:

Prevent users from updating the OS manually

To deploy an older update while preventing users from installing a more recent one

To delay visibility, deploy a device restriction template that configures the following settings: Defer software updates = Yes

This doesn't affect any scheduled updates. It represents days before software updates are visible to end users after release.

Delay default visibility of software updates = 1 to 90 90 days is the maximum delay that Apple supports.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/software-updates-ios>

NEW QUESTION 37

- (Exam Topic 3)

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 42

- (Exam Topic 3)

You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs.

The computers have the logged events shown in the following table.

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

Which events are collected in the Log Analytics workspace?

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

Answer: E

Explanation:

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

NEW QUESTION 47

- (Exam Topic 3)

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 52

- (Exam Topic 3)

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 54

- (Exam Topic 3)

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in Intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

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

Answer: AB

Explanation:

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

NEW QUESTION 57

- (Exam Topic 3)

You have a Microsoft Intune subscription.

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

Create profile

Windows PC

1 Basics

2 Out-of-box experience (OOBE)

3 Scope tags

4 Assignments

5 Review + create

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

* Deployment mode ⓘ

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

Language (Region) ⓘ

Operating system default

Automatically configure keyboard ⓘ

No

Yes

Apply device name template ⓘ

No

Yes

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

NOTE: Each correct selection is worth one point.

Answer Area

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

are prevented from modifying any desktop settings

can create additional local users on the device

can modify the desktop settings for all device users

can modify the desktop settings only for themselves

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

computer name

Cortana settings

keyboard layout

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

are prevented from modifying any desktop settings

can create additional local users on the device

can modify the desktop settings for all device users

can modify the desktop settings only for themselves

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

computer name

Cortana settings

keyboard layout

NEW QUESTION 60

- (Exam Topic 3)
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	Yes	No
Device1 will have Policy1 assigned and will be marked as compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 62

- (Exam Topic 3)

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

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

From the Intune admin center, you create and deploy two Windows app (Win32) apps. You need to ensure that App1 is installed before App2 on every device. What should you configure?

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

Answer: D

Explanation:

The correct answer is D because you can configure the dependencies for a Win32 app in the deployment configurations1. Dependencies are other Win32 apps that must be installed before your Win32 app can be installed1. You can add Win32 app dependencies only after your Win32 app has been added and uploaded to Intune2. In this case, you need to configure the App2 deployment configurations to add App1 as a dependency2. References: 1: Microsoft Intune Win32 App Dependencies - MSEndpointMgr <https://msendpointmgr.com/2019/06/03/new-intune-feature-win32-app-dependencies/> 2: Add and assign Win32 apps to Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add>

NEW QUESTION 64

- (Exam Topic 3)

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

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

Answer: D

Explanation:

To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1. You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability rule that matches Device1's properties and excludes Device2's properties. References: <https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#applicability-rules>

NEW QUESTION 66

- (Exam Topic 3)

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 68

- (Exam Topic 3)

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 70

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to perform the following tasks for User1:

- > Set the Usage location to Canada.
- > Configure the Phone and Email authentication contact info for self-service password reset (SSPR). Which two settings should you configure in the Azure Active Directory admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Manage

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 74

- (Exam Topic 3)

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 79

.....

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](#)