



Microsoft

Exam Questions MD-102

Endpoint Administrator

NEW QUESTION 1

- (Exam Topic 1)

User1 and User2 plan to use Sync your settings.

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

NOTE: Each correct selection is worth one point.

Answer Area

User1:

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

User2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Reference:

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

NEW QUESTION 2

- (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 3

- (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 4

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

For the Sales department employees:

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

- 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 5

- (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 6

- (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

- 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 7

- (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 8

- (Exam Topic 3)

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

You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method. What should you do first?

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

Answer: C

Explanation:

Reference:

https://www.manageengine.com/mobile-device-management/help/enrollment/mdm_creating_apns_certificate.ht Prerequisites for iOS enrollment Before you can enable iOS devices, complete the following steps: Make sure your device is eligible for Apple device enrollment. Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority. Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS and macOS devices.

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

NEW QUESTION 9

- (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 10

- (Exam Topic 3)
You have 100 computers that run Windows 10.
You plan to deploy Windows 11 to the computers by performing a wipe and load installation. You need to recommend a method to retain the user settings and the user data.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Configure known folder redirection in Microsoft OneDrive.

Run scanstate.exe.

Run loadstate.exe.

Enable Enterprise State Roaming.

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

>

<

Answer Area

&u2191

⇊

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Configure known folder redirection in Microsoft OneDrive.

Run scanstate.exe.

Run loadstate.exe.

Enable Enterprise State Roaming.

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

>

<

Answer Area

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

&u2191

⇊

NEW QUESTION 10

- (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

A device restriction policy

A security baseline

An attack surface reduction (ASR) rule

An Intune connection

Answer Area

Enforces compliance:

Prevents suspicious scripts:

- 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>

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 16

- (Exam Topic 3)

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

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

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

Answer: D

Explanation:

Endpoint analytics is a feature of Microsoft Intune that provides insights into the performance and health of devices. You can use endpoint analytics to review the startup times and restart frequencies of the devices, as well as other metrics such as sign-in times, battery life, app reliability, and software inventory. References:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

NEW QUESTION 20

- (Exam Topic 3)

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

App configuration policy
App protection policy
Compliance policy
Configuration profile

Profile:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Configuration profile Create a trusted certificate profile. Box 2: Trusted certificate

When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.

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

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 30

- (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 35

- (Exam Topic 3)

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

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

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

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

Answer: B

Explanation:

* Admin1

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

* Admin2

Mark your app as publisher verified.

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

* Admin3

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

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

Reference:

Office Apps admin - Assign the Office Apps admin role to users who need to do the following <https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified>

NEW QUESTION 39

- (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 44

- (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 48

- (Exam Topic 3)

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

Name	Member of
User1	Group1
User2	Group2

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with medium confidence
Reference:
<https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications>

NEW QUESTION 49

- (Exam Topic 3)

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.
You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

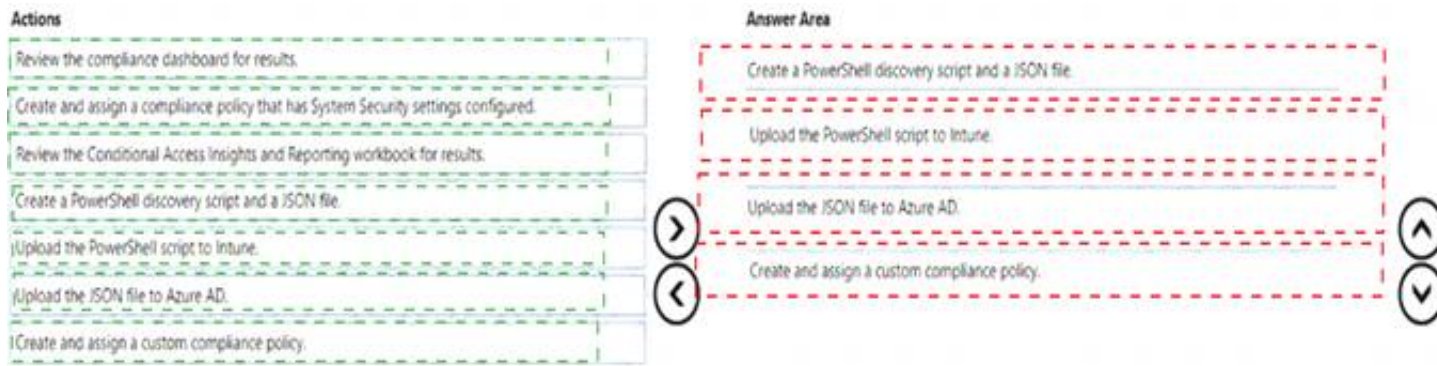
Create and assign a custom compliance policy.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 51

- (Exam Topic 3)

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: B

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 53

- (Exam Topic 3)

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD). The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements:

- > The configuration must be managed from a central location.
- > Internet traffic must be minimized.
- > Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Windows Update technology to use:

Windows Server Update Services (WSUS)
Microsoft Endpoint Configuration Manager
Windows Update for Business

Manage the configuration by using:

A Group Policy object (GPO)
Microsoft Endpoint Configuration Manager
Microsoft Intune

Manage the traffic by using:

Delivery Optimization
BranchCache
Peer cache

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.

Windows Server Update Services is a built-in server role that includes the following enhancements: Can be added and removed by using the Server Manager Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS Etc.

Box 2: A Group Policy object

In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).

Box 3: BranchCache

BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them. BranchCache has two operating modes: Distributed Cache mode and Hosted Cache mode.

Reference: <https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache> <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-conf>

NEW QUESTION 54

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You have a device named Device1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: ABF

NEW QUESTION 57

- (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 58

- (Exam Topic 3)

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

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

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

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

Answer: D

Explanation:

To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. References:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work#device-experie>

NEW QUESTION 59

- (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 61

.....

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](#)