

Microsoft

Exam Questions MD-102

Endpoint Administrator



NEW QUESTION 1

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 2

- (Exam Topic 4)

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 3

- (Exam Topic 4)

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

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

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

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

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

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

- Assignments
- o Users or workload identities: Used, User2
 - o Cloud apps or actions: Office 365 Exch
 - o Conditions
 - Device platforms: Android, iOS
 - Filter for devices
 - Device matching the rule: Exclude filtered devices from policy
 - Rule syntax: device. displayName- contains "1"
- Access controls Grant Block access
- For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 4

- (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 5

- (Exam Topic 4)

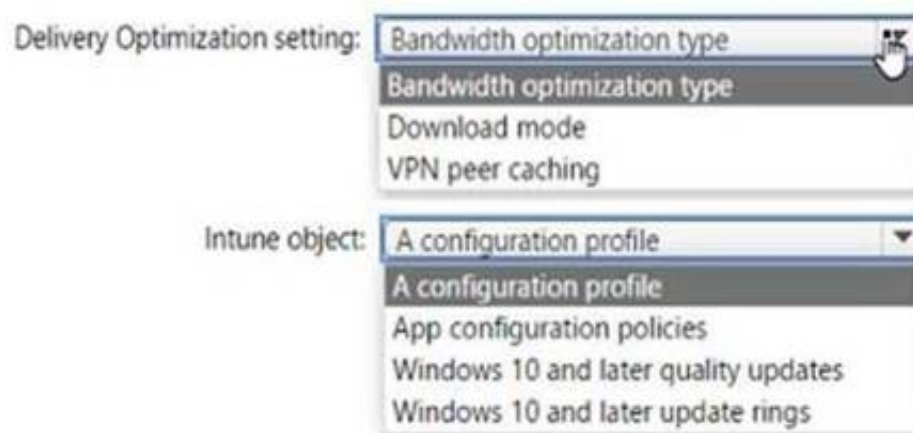
You have 100 Windows 10 devices enrolled in Microsoft Intune.

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

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

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 6

- (Exam Topic 4)

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 7

- (Exam Topic 4)

You have a computer that runs Windows 10 and contains two local users named User1 and User2. You need to ensure that the users can perform the following actions:

- User1 must be able to adjust the date and time.
- User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Groups

Administrators

Event Log Readers

Performance Log Users

Power Users

System Managed Accounts Group

Answer Area

User1:

User2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Groups

Administrators

Event Log Readers

Performance Log Users

Power Users

System Managed Accounts Group

Answer Area

User1: Administrators

User2: Event Log Readers

NEW QUESTION 8

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table. All devices have Microsoft Edge installed. From the Microsoft Intune admin center, you create a Microsoft You need to apply Edge1 to all the supported devices. To which devices should you apply Edge1?

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

Answer: E

NEW QUESTION 9

- (Exam Topic 4)

You have the on-premises servers shown in the following table.

Name	Description
DC1	Domain controller that runs Windows Server 2022
Server1	Standalone server that runs Windows Server 2022
Server2	Member server that runs Windows Server 2022 and has the Remote Access role installed
Server3	Member server that runs Windows Server 2019
Server4	Red Hat Enterprise Linux (RHEL) 8.4 server

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune. You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports. To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Server:

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 4)
You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

You add an Autopilot deployment profile as shown in the following exhibit.

Create profile

Windows PC

✓ Basics

✓ Out-of-box experience (OOBE)

✓ Assignments

4 Review

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No

Language (Region)

Operating system default	
--------------------------	--

Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

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

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

Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.

Answer Area

Statements	Yes	No
If you reset Device1, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you reset Device2, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you restart Device3, the device will be deployed by using Autopilot.	<input checked="" type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If you reset Device1, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you reset Device2, the device will be deployed by using Autopilot.	<input type="radio"/>	<input checked="" type="radio"/>
If you restart Device3, the device will be deployed by using Autopilot.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 10

- (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 15

- (Exam Topic 4)

You have a Hyper-V host. The host contains virtual machines that run Windows 10 as shown in following table.

Name	Generation	Virtual TPM	Virtual processors	Memory
VM1	1	No	4	16 GB
VM2	2	Yes	2	4 GB
VM3	2	Yes	1	8 GB

Which virtual machines can be upgraded to Windows 11?

- A. VM1 only
- B. VM2 only
- C. VM2 and VM3 only
- D. VM1.VM2. andVM3

Answer: C

Explanation:

Windows 11 has certain hardware requirements that must be met in order to upgrade from Windows 10. Some of these requirements are as follows:

- > A processor with at least 1 GHz clock speed and2 cores.
- > A system firmware that supports UEFI andSecure Boot.
- > A Trusted Platform Module (TPM) version2.0 or higher.
- > At least 4 GB
- > At least 64 GB

of system memory (RAM). of storage space.

In this scenario, the virtual machines that run Windows 10 have the following specifications:

- > VM3 is a generation 2 virtual machine with a virtual TPM, 1 virtual processor, and 8 GB of memory.

VM1 cannot be upgraded to Windows 11 because it does not have a virtual TPM and it is not a generation 2 virtual machine. Generation 1 virtual machines do not support UEFI and Secure Boot, which are required for Windows 11. VM2 and VM3 can be upgraded to Windows 11 because they have a virtual TPM and they are generation 2 virtual machines. They also meet the minimum requirements for processor speed, cores, memory, and storage space.

NEW QUESTION 16

- (Exam Topic 4)

Your network contains an Active Directory domain.

You install the Microsoft Deployment Toolkit (MDT) on a server. You have a custom image of Windows 11.

You need to deploy the image to 100 devices by using MDT.

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

Actions

Enable multicast.

Install Windows Deployment Services (WDS).

Create a deployment share.

Add the Windows 11 image.

Create a task sequence.

Answer Area



- A. Mastered
B. Not Mastered

Answer: A

Explanation:

To deploy the Windows 11 image to 100 devices by using MDT, you should perform the following three actions in sequence:

- Install Windows Deployment Services (WDS) on the server. WDS is a role that enables you to deploy Windows operating systems over the network by using PXE boot and multicast technologies. You need to install WDS before you can enable multicast and configure the boot images for MDT. You can install WDS by using the Server Manager or PowerShell1.
 - Create a deployment share on the server. A deployment share is a folder that contains the MDT files, scripts, applications, drivers, operating systems, and task sequences that you use to deploy Windows. You need to create a deployment share by using the MDT Deployment Workbench2.
 - Add the Windows 11 image and create a task sequence in the deployment share. An image is a file that contains a snapshot of a Windows installation. A task sequence is a set of steps that MDT executes to install Windows and configure the settings. You need to add the Windows 11 image by importing it from a source folder or a WIM file, and create a task sequence by using a template or customizing your own3.
- These are the basic steps to prepare for deploying Windows 11 with MDT. For more details and guidance, you can refer to the web search results I found for you by using search_web("deploy Windows 11 image with MDT").

NEW QUESTION 19

- (Exam Topic 4)

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

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

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

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

Answer: CE

Explanation:

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

- Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to create device groups and assign roles and permissions12.
- Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices34.

The other options are not correct for this scenario because:

- Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune. However, this method requires user interaction and consent, and does not enroll the devices as supervised devices5.
- Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings. However, a compliance policy does not deploy or manage software updates on the devices6.
- Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune. However, an iOS app provisioning profile does not affect the software updates on the devices7.

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

NEW QUESTION 21

- (Exam Topic 4)

You have a Microsoft 365 subscription.

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

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

The solution must minimize user disruption.

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

NOTE: Each correct selection is worth one point.

Answer Area

Windows 11 devices managed by using Configuration Manager:	<div>Windows Autopilot</div> <div>Co-management</div> <div>User enrollment</div> <div>Windows Autopilot</div>
Personal iOS devices:	<div>Automated Device Enrollment (ADE)</div> <div>Apple Configurator</div> <div>Automated Device Enrollment (ADE)</div> <div>User enrollment</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 22

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Task sequence template:

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

Operating system image:

Image1.wim
Image2.wim
Install.wim

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Standard Client Upgrade Task Sequence

Use Template: Standard Client Upgrade Task Sequence

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

Box 2: Install.wim

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

Reference:

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

NEW QUESTION 26

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You use Windows Autopilot to deploy Windows 11 to devices. A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device. You need to ensure that when a deployment fails, the deployment logs can be collected. What should you configure?

- A. the automatic enrollment settings
- B. the Windows Autopilot deployment profile
- C. the enrollment status page (ESP) profile
- D. the device configuration profile

Answer: B

NEW QUESTION 27

- (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 28

- (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:

	✓
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

User2 can enroll a maximum of:

	✓
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:

	✓
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

User2 can enroll a maximum of:

	✓
5 devices	
10 devices	
15 devices	
1,000 devices	
An unlimited number of devices	

NEW QUESTION 31

- (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 36

- (Exam Topic 2)

You need to meet the device management requirements for the developers. What should you implement?

- A. folder redirection
- B. Enterprise State Roaming
- C. home folders
- D. known folder redirection in Microsoft OneDrive

Answer: B

Explanation:

Litware identifies the following device management requirements:

➤ Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in. Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-refer>

NEW QUESTION 38

- (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 40

- (Exam Topic 1)

You implement Boundary1 based on the planned changes.

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 43

- (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 46

- (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: C

Explanation:

Reference:

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

NEW QUESTION 50

- (Exam Topic 4)

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

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

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

What should you use?

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

Answer: B

Explanation:

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

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

NEW QUESTION 53

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
 LON-CL2	✔ Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	✔ Yes
 LON-CL4	✔ Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	✔ Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Identified by Intune as a personal device:

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join> <https://docs.microsoft.com/en-us/azure/active-directory/devices/concept->

azure-ad-register

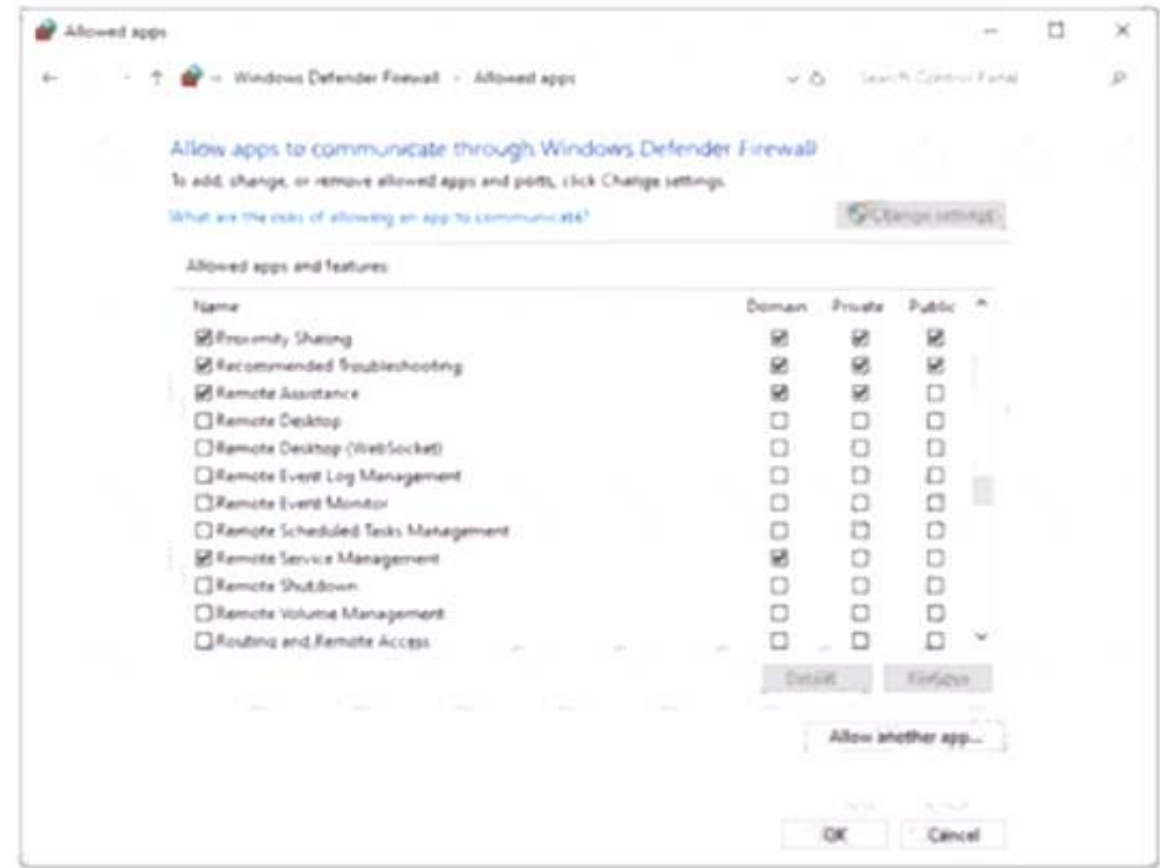
NEW QUESTION 55

- (Exam Topic 4)

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

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

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



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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 58

- (Exam Topic 4)

You have 1,000 computers that run Windows 10 and are members of an Active Directory domain. You need to capture the event logs from the computers to Azure.

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

Answer Area

Azure service to provision:

☒

An Azure Storage account

☐

Azure Cosmos DB

☐

Azure SQL Database

☐

Log Analytics

Action to perform on the computers:

☒

Create a collector-initiated subscription

☐

Install the Microsoft Monitoring Agent

☐

Enroll in Microsoft Intune

☐

Register to Azure Active Directory (Azure AD)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure service to provision:

☒

An Azure Storage account

☐

Azure Cosmos DB

☐

Azure SQL Database

☒

Log Analytics

Action to perform on the computers:

☒

Create a collector-initiated subscription

☒

Install the Microsoft Monitoring Agent

☐

Enroll in Microsoft Intune

☐

Register to Azure Active Directory (Azure AD)

NEW QUESTION 61

- (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) ⓘ

30

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 65

- (Exam Topic 4)

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

Name	Member of	License
User1	Group1	None
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

Group2 has been assigned in the Enrollment Status Page. You have the devices shown in the following table.

Name	Operating system	Department
Device1	Windows 10 Pro	Marketing
Device2	Windows 11 Home	Research
Device3	Windows 10 Pro	Marketing

You capture and upload the hardware IDs of the devices in the marketing department. You configure Windows Autopilot. 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 complete the Autopilot process on Device1.	<input type="radio"/>	<input type="radio"/>
User2 can complete the Autopilot process on Device1.	<input type="radio"/>	<input type="radio"/>
User3 can view device setup information during the enrollment phase of Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can complete the Autopilot process on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can view device setup information during the enrollment phase of Device1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 66

- (Exam Topic 4)

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

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

You are deploying Microsoft 365 apps.
 You have devices enrolled in Microsoft Intune as shown in the following table.

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

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

App Information
[Edit](#)

Name

Description

Microsoft 365 Apps for Windows 10

Microsoft 365 Apps for Windows 10

Publisher

Category

Show this as a featured app in the Company Portal

Information URL

Privacy URL

Developer

Owner

Notes

Logo

Microsoft

Productivity


No

<https://products.office.com/en-us/explore-office-for-home>
<https://privacy.microsoft.com/en-US/privacystatement>

Microsoft

Microsoft

...



Teams, Word

Architecture

Update channel

Remove other versions

Version to install

Use shared computer activation

Accept the Microsoft Software License

Teams on behalf of users

Install background service for Microsoft

Search in Bing

Apps to be installed as part of the suite

64-bit

Current Channel

Yes

Latest

No

No

No

No

1 language(s) selected

Assignments
[Edit](#)

Group mode

Required

Included

Group

Group1

Available for enrolled devices

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Graphical user interface, text, application Description automatically generated
 Reference:

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

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

NEW QUESTION 67

- (Exam Topic 4)

You have the Microsoft Deployment Toolkit (MDT) installed. You install and customize Windows 11 on a reference computer

You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.

Which command should you run before you capture the image?

- A. dism
- B. wpeinit
- C. sysprep
- D. bcdedit

Answer: C

Explanation:

To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the sysprep command with the /generalize option. This option removes all unique system information from the Windows installation, such as the computer name, security identifier (SID), and driver cache.

The other commands are not used for this purpose. References: Sysprep (Generalize) a Windows installation

NEW QUESTION 72

- (Exam Topic 4)

You have a Microsoft 365 tenant.

You have devices enrolled in Microsoft Intune.

You assign a conditional access policy named Policy1 to a group named Group1. Policy1 restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.

You need to identify which noncompliant devices attempt to access OneDrive for Business. What should you do?

- A. From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.
- B. From the Microsoft Intune admin center, review Device compliance report.
- C. From the Microsoft Intune admin center, review the Noncompliant devices report.
- D. From the Microsoft Intune admin center, review the Setting compliance report.

Answer: C

NEW QUESTION 76

- (Exam Topic 4)

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

You have 100 devices from users that left your company.

You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

- A. Deploy a new configuration profile to the devices.
- B. Perform a Windows Autopilot reset on the devices.
- C. Perform an in-place upgrade on the devices.
- D. Perform a clean installation of Windows 11 on the devices.

Answer: B

NEW QUESTION 79

- (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 81

- (Exam Topic 4)

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 83

- (Exam Topic 4)

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

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

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

 Save
  Discard

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

Mark devices with no compliance policy assigned as: ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30
 

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

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO. Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until june 10th.

Source:

Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.

When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.

This action is supported on all platforms supported by Intune. <https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance>

NEW QUESTION 87

- (Exam Topic 4)

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 92

- (Exam Topic 4)

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

You discover that Group Policy settings override the settings configured in Microsoft Intune policies. You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings. What should you do?

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

Answer: C

NEW QUESTION 94

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices. You need to create Intune configuration profiles to perform the following actions on the devices:

- Deploy a custom Start layout.
- Rename the local Administrator account.

Which profile type template should you use for each action? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

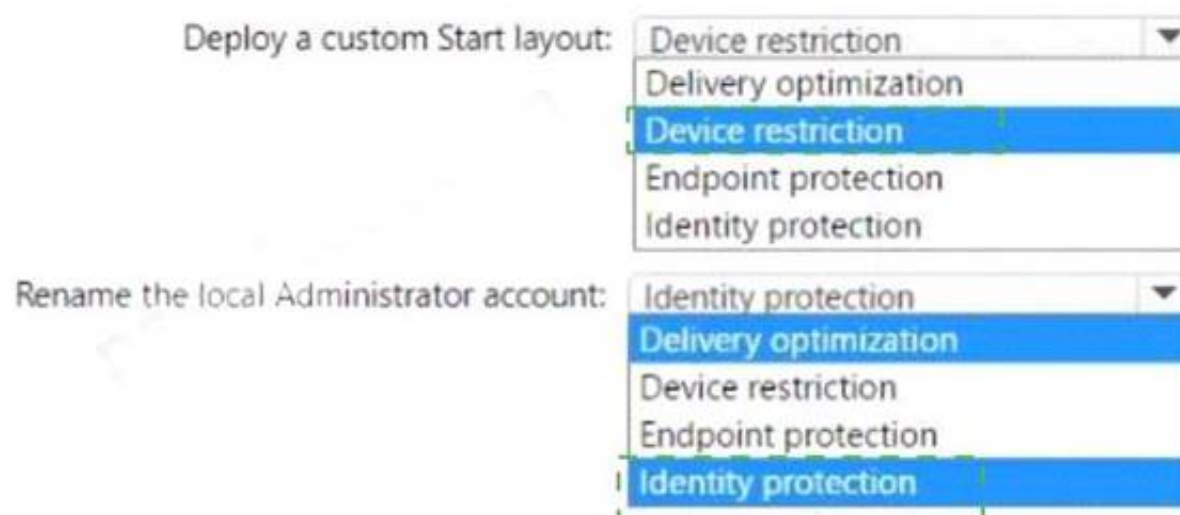
Deploy a custom Start layout:	<div>Device restriction</div> <div>Delivery optimization</div> <div>Device restriction</div> <div>Endpoint protection</div> <div>Identity protection</div>
Rename the local Administrator account:	<div>Identity protection</div> <div>Delivery optimization</div> <div>Device restriction</div> <div>Endpoint protection</div> <div>Identity protection</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 95

- (Exam Topic 4)

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

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

NOTE: Each correct selection is worth one point.

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

Answer: ACE

Explanation:

You can collect error events from the System log, third-party application logs stored as text files, and the average processor utilization from the computers by using Log Analytics. These are some of the types of data that you can collect by using data sources such as Windows event logs, custom logs, and performance counters. You cannot collect failure events from the Security log or the list of processes and their execution times by using Log Analytics. References: <https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-overview>

NEW QUESTION 97

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

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

Update ring settings Edit	
Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

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

Answer Area

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

can be deferred for 30 days

can be deferred indefinitely

can be deferred for 30 days

will be installed immediately

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

1 day

1 day

30 days

60 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

This is because the update rings policy named Policy1 has the “Feature updates deferral period (days)” setting set to 60. This means that feature updates, which include new Windows functionality, can be deferred for up to 60 days from the date they are released by Microsoft. After 60 days, the devices will automatically install the feature updates. References:

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

NEW QUESTION 99

- (Exam Topic 4)

You have an on-premises server named Server1 that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

- A. Multipath I/O (MPIO)
- B. Multipoint Connector
- C. Windows Deployment Services (WDS)
- D. Windows Server Update Services (WSUS)

Answer: C

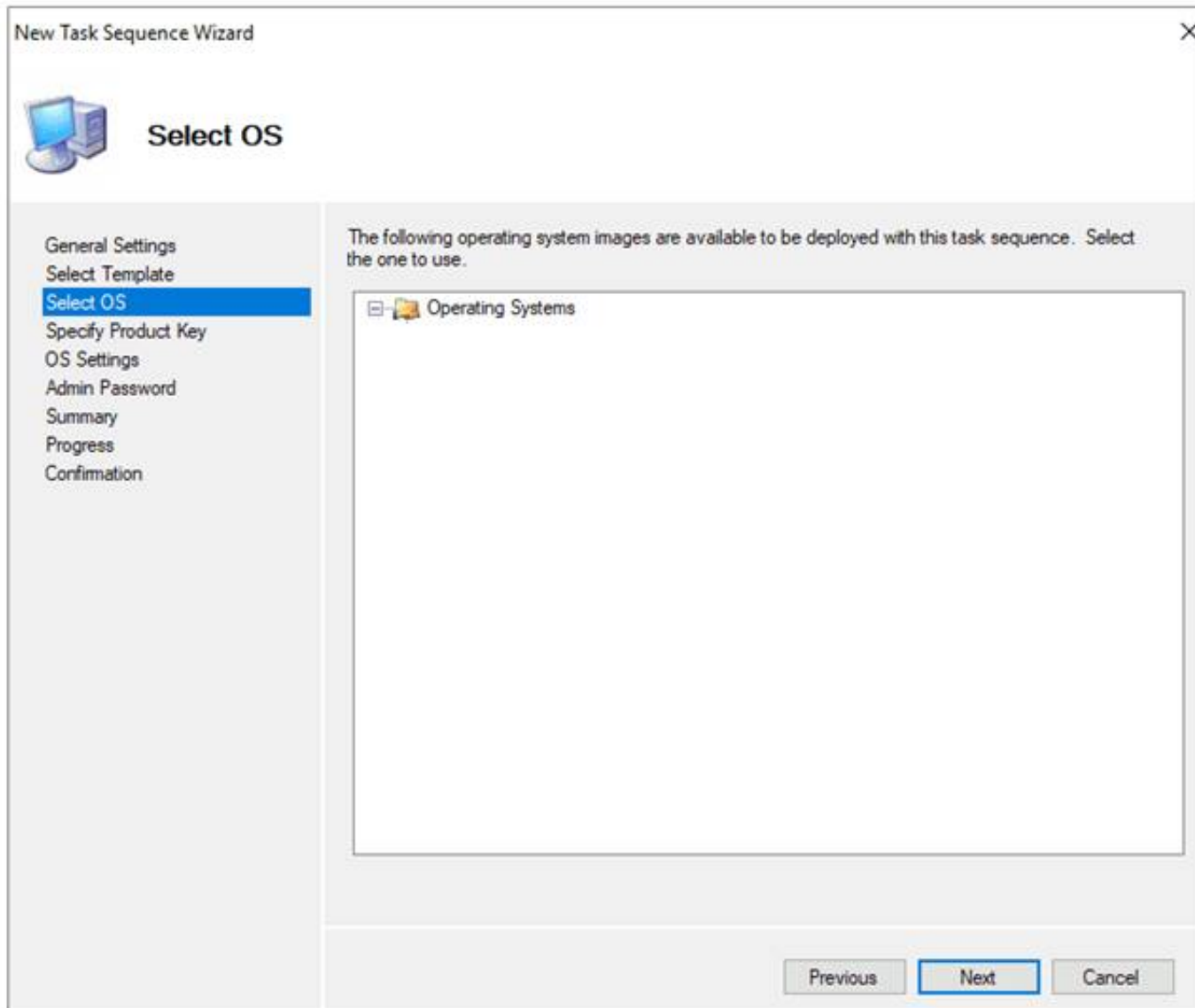
NEW QUESTION 101

- (Exam Topic 4)

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

From the Deployment Workbench, you open the New Task Sequence Wizard and select the Standard Client Upgrade Task Sequence task sequence template.

You discover that there are no operating system images listed on the Select OS page as shown in the following exhibit.



You need to be able to select an operating system image to perform a Windows 11 in-place upgrade. What should you do?

- A. Enable monitoring for the deployment share.
- B. Import a full set of source files.
- C. Import a custom image file.
- D. Run the Update Deployment Share Wizard

Answer: D

NEW QUESTION 105

- (Exam Topic 4)

You have a Microsoft 365 ES subscription that uses Microsoft Intune. You have the apps shown in the following exhibit.

Apps | All apps

Search (Ctrl + /)

Overview

All apps

Monitor

By platform

Windows

iOS/iPadOS

macOS

Android

Policy

App protection policies

App configuration policies

+ Add

Refresh

Filter

Export

Columns

Search by name or publisher

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

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

NOTE: Each correct selection is worth one point.

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

1

2

3

4

5

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

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

1

2

3

4

5

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

1

2

3

4

5

NEW QUESTION 107

- (Exam Topic 4)

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

You use Microsoft Intune to manage devices. All devices are in the same time zone. You create an update rings policy and assign the policy to all Windows devices.

On the November 1, you pause the update rings policy. All devices remain online.

Without further modification to the policy, on which date will the devices next attempt to update?

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

Answer: C

NEW QUESTION 110

- (Exam Topic 4)

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

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

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

Answer: D

NEW QUESTION 115

- (Exam Topic 4)

You use Windows Admin Center to remotely administer computers that run Windows 10.

When connecting to Windows Admin Center, you receive the message shown in the following exhibit.

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

 [Go to your Start page](#)

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

Go on to the webpage (Not recommended)

You need to prevent the message from appearing when you connect to Windows Admin Center. To which certificate store should you import the certificate?

- A. Personal
- B. Trusted Root Certification Authorities
- C. Client Authentication Issuers

Answer: B

NEW QUESTION 117

- (Exam Topic 4)

You have a Hyper-V host that contains the virtual machines shown in the following table.

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

- A. VM1 only
- B. VM3only
- C. VM1 and VM2 only
- D. VM2 and VM3 only
- E. VM1, VM2, and VM3

Answer: E

NEW QUESTION 122

- (Exam Topic 4)

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

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

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

You need to create an app configuration policy named Policy1 for the Android Enterprise platform. Which apps can you manage by using Policy1?

- A. App2 only
- B. App3 only
- C. App1 and App3 only
- D. App2 and App3 only
- E. App1, App2, and App3

Answer: D

NEW QUESTION 125

- (Exam Topic 4)

You have 200 computers that run Windows 10 and are joined to an Active Directory domain.

You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Enable the Allow Remote Shell access setting.
- B. Enable the Allow remote server management through WinRM setting.
- C. Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.
- D. Enable the Windows Defender Firewall: Allow inbound Remote Desktop exceptions setting.
- E. Set the Startup Type of the Remote Registry service to Automatic
- F. Enable the Windows Defender Firewall: Allow inbound remote administration exception setting.

Answer: BCF

Explanation:

To enable WinRM on domain computers using Group Policy, you need to perform the following actions:

- Enable the Allow remote server management through WinRM setting under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service. This setting allows you to specify the IP address ranges that can connect to the WinRM service.
- Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic under Computer Configuration > Preferences > Control Panel Settings > Services. This setting ensures that the WinRM service starts automatically on the computers.
- Enable the Windows Defender Firewall: Allow inbound remote administration exception setting under Computer Configuration > Policies > Security Settings > Windows Firewall and Advanced Security > Windows Firewall and Advanced Security > Inbound Rules. This setting creates a firewall rule that allows incoming TCP connections on port 5985 for WinRM. References: How to Enable WinRM via Group Policy, Installation and configuration for Windows Remote Management

NEW QUESTION 129

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You use Microsoft Intune Suite to manage devices.

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

Access requirements

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

Conditional launch

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

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

Answer Area

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

PIN only

account credentials only

PIN only

PIN and account credentials

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

block access

block access

reset the app PIN

reset the device PIN

wipe company data

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1 = PIN only
Box 2 = reset the PIN app
iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios>

NEW QUESTION 134

- (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.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device1 is marked as compliant. = No Device2 is marked as compliant. = Yes Device3 is marked as 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 137

- (Exam Topic 4)

Your company has a computer named Computer1 that runs Windows 10. Computer1 was used by a user who left the company. You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows Autopilot. 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
Upload the file by using Microsoft Intune.	
Generate a CSV file that contains the computer information.	
Reset the computer.	<input type="radio"/>
Generate a JSON file that contains the computer information.	<input type="radio"/>
Upload the file by running azcopy.exe.	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To redeploy Computer1 by using Windows Autopilot, you need to perform the following three actions in sequence:

- Generate a JSON file that contains the computer information. This file specifies the Autopilot profile to be applied during the deployment. You can use the Get-AutopilotProfilesForExistingDevices PowerShell script to generate this file1.
- Reset the computer. You can use the Windows Automatic Redeployment feature to trigger a reset from the login screen by pressing Ctrl + R and providing an

administrator account2. Alternatively, you can use the Windows Autopilot Reset feature to remotely reset the device from Intune1.

➤ Upload the file by running azcopy.exe. This step copies the JSON file to a blob storage account in Azure, where it can be accessed by the device during the deployment. You need to specify the storage account name, access key, and container name as parameters for azcopy.exe1.

NEW QUESTION 138

- (Exam Topic 4)

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 140

- (Exam Topic 4)

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

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

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS devices. You assign CAPolicy1 to Group1. You discover that User1 can still connect to Exchange Online from an iOS device. You need to ensure that CAPolicy1 is enforced. What should you do?

- A. Configure a new terms of use (TOU).
- B. Assign CAPolicy1 to Group2.
- C. Enable CAPolicy1
- D. Add a condition in CAPolicy1 to filter for devices.

Answer: B

Explanation:

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

* User or group membership

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

* Device

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

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

* Etc.

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

NEW QUESTION 144

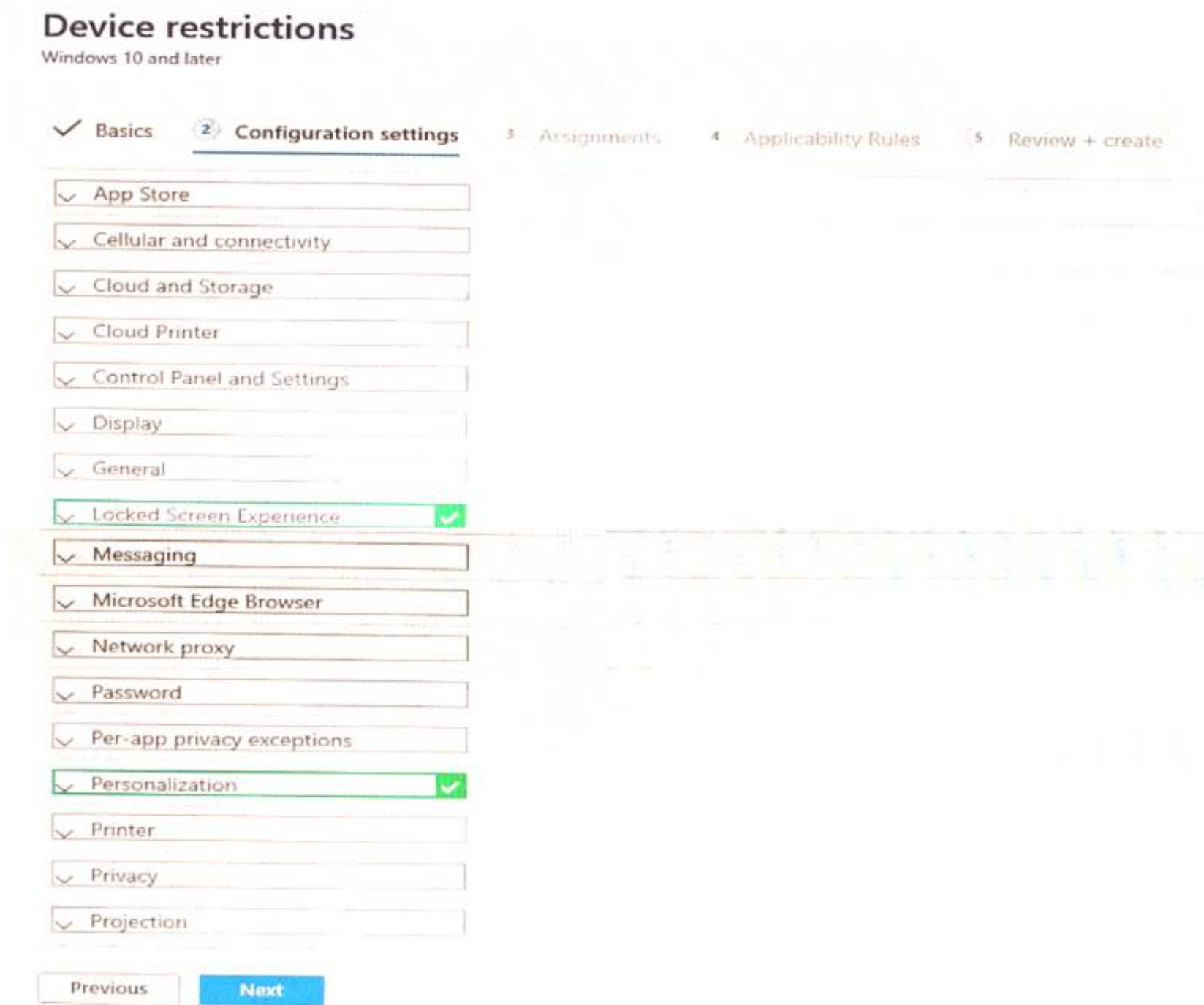
- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to set a custom image as the wallpaper and sign-in screen.

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

NOTE: Each correct selection is worth one point.

Answer Area



Device restrictions
Windows 10 and later

1 Basics 2 **Configuration settings** 3 Assignments 4 Applicability Rules 5 Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience** ✓
- Messaging
- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization** ✓
- Printer
- Privacy
- Projection

Previous Next

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device restrictions

Windows 10 and later

✓ Basics

2 Configuration settings

3 Assignments

4 Applicability Rules

5 Review + create

✓ App Store

✓ Cellular and connectivity

✓ Cloud and Storage

✓ Cloud Printer

✓ Control Panel and Settings

✓ Display

✓ General

✓ Locked Screen Experience ✓

✓ Messaging

✓ Microsoft Edge Browser

✓ Network proxy

✓ Password

✓ Per-app privacy exceptions

✓ Personalization ✓

✓ Printer

✓ Privacy

✓ Projection

Previous

Next

NEW QUESTION 149

- (Exam Topic 4)

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

>

<

↑

↓

- 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.

NEW QUESTION 154
- (Exam Topic 4)
You have the device configuration profile shown in the following exhibit.

Kiosk

Windows 10 and later

✓ Basics

2 Configuration settings

3 Assignments

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

Select a kiosk mode *

Single app, full-screen kiosk

User login type *

Auto login (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 158

- (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 162

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune. You have computers that run Windows 11 as shown in the following table.

Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

You create and assign the compliance policies shown in the following table.

Name	Configuration	Action for noncompliance	Assignment
Policy1	Require BitLocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Group1
Policy2	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group2

The next day, you review the compliance status of the computers.

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

Answer Area	Statements	Yes	No
	The compliance status of Computer1 is In grace period.	<input type="checkbox"/>	<input type="checkbox"/>
	The compliance status of Computer2 is Compliant.	<input type="checkbox"/>	<input type="checkbox"/>
	The compliance status of Computer3 is Not compliant.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area	Statements	Yes	No
	The compliance status of Computer1 is In grace period.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	The compliance status of Computer2 is Compliant.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	The compliance status of Computer3 is Not compliant.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

NEW QUESTION 166

- (Exam Topic 4)
You use Microsoft Defender for Endpoint to protect computers that run Windows 10.
You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.
Which tool should you use?

- A. Microsoft Defender for Endpoint Power 81 app
- B. Microsoft Secure Score
- C. Endpoint Analytics
- D. Microsoft 365 Defender portal

Answer: B

NEW QUESTION 167

- (Exam Topic 4)
You have SOO Windows 10 devices enrolled in Microsoft Intune.
You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASLR)

You need to configure a Windows 10 device that will be used to create a template file.
Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings. Each protection area may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Protection areas	Answer Area
<div>Account protection</div>	DEP: <input type="text"/>
<div>App & browser control</div>	Mandatory ASLR: <input type="text"/>
<div>Device security</div>	
<div>Virus & threat protection</div>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Exploit protection is a feature that helps protect against malware that uses exploits to infect devices and spread. Exploit protection consists of many mitigations that can be applied to either the operating system or individual apps1.

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

- > DEP: Device security. Data Execution Prevention (DEP) is a mitigation that prevents code from running in memory regions marked as non-executable. You can enable DEP system-wide or for specific apps in the Device security section of the Windows Security app1.
- > Mandatory ASLR: App & browser control. Force randomization for images (Mandatory ASLR) is a mitigation that randomizes the location of executable images in memory, making it harder for attackers to predict where to inject code. You can enable Mandatory ASLR system-wide or for specific apps in the App & browser control section of the Windows Security app1.

NEW QUESTION 169

- (Exam Topic 4)
You use Microsoft Endpoint Manager to manage Windows 10 devices.
You are designing a reporting solution that will provide reports on the following:

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

You need to recommend a data source and a data visualization tool for the design.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Data source:

Audit logs in Azure Active Directory (Azure AD)

Audit logs in Microsoft Intune

Azure Synapse Analytics

The Microsoft Intune Data Warehouse

Data visualization tool:

Azure Data Studio

Microsoft Power BI

The Azure portal

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 170

- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

- A. Import an OS package.
- B. Create a selection profile.
- C. Add a Gather task to the task sequence.
- D. Add a Validate task to the task sequence.

Answer: B

NEW QUESTION 171



- (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  User-Driven 

* Join to Azure AD as  Azure AD joined 


Microsoft Software License Terms  Show Hide


 Important information about hiding license terms


Privacy settings  Show Hide

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

Hide change account options  Show Hide

User account type  Administrator Standard


Allow White Glove OOBE  No Yes

Apply device name template  No Yes

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

Answer Area

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




join the device to Azure AD

enroll the device in Microsoft Intune

import a CSV file into Windows Autopilot

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



joined to Azure AD only

registered in Azure AD only

joined to Active Directory only

joined to Active Directory and registered in Azure AD


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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




join the device to Azure AD

enroll the device in Microsoft Intune

import a CSV file into Windows Autopilot

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



joined to Azure AD only

registered in Azure AD only

joined to Active Directory only

joined to Active Directory and registered in Azure AD

NEW QUESTION 175

- (Exam Topic 4)

Your company standardizes on Windows 10 Enterprise for all users.

Some users purchase their own computer from a retail store. The computers run Windows 10 Pro. You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps. The solution must meet the following requirements:

- Ensure that any applications installed by the users are retained.
- Minimize user intervention.

What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Windows Autopilot
- B. Microsoft Deployment Toolkit (MDT)
- C. a Windows Configuration Designer provisioning package
- D. Windows Deployment Services (WDS)

Answer: A

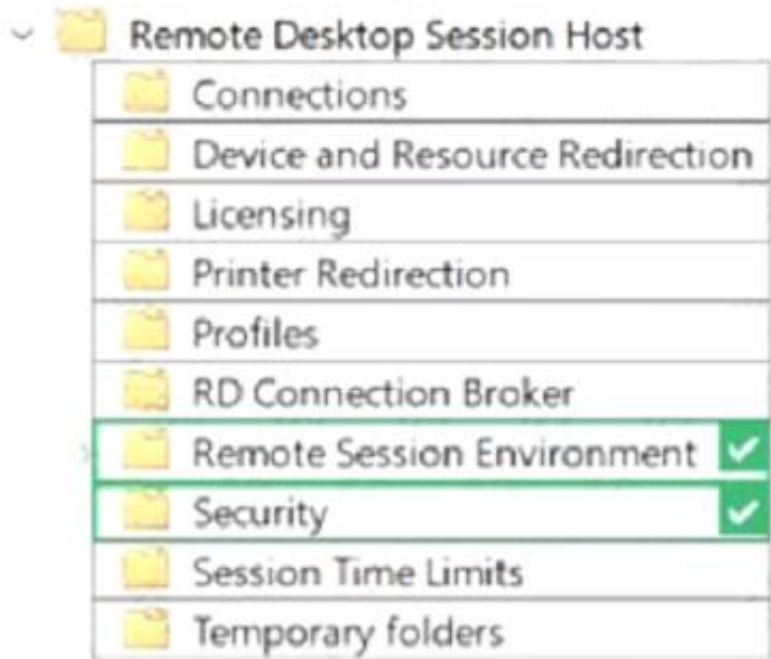
NEW QUESTION 179

- (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).

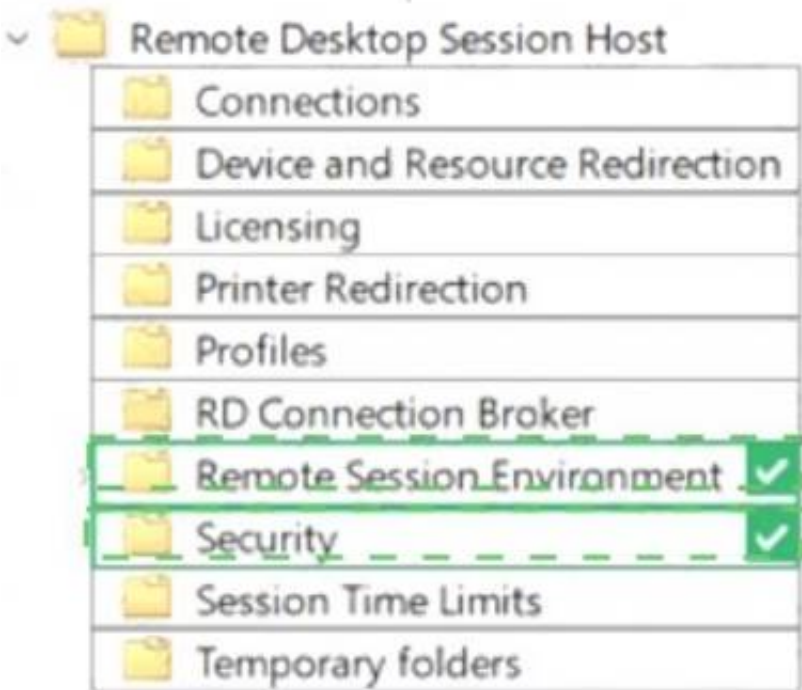
Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 182

- (Exam Topic 4)

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

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

Which groups can you add to Group4?

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

Answer: C

NEW QUESTION 184

.....

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](#)