



**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 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 4

- (Exam Topic 4)

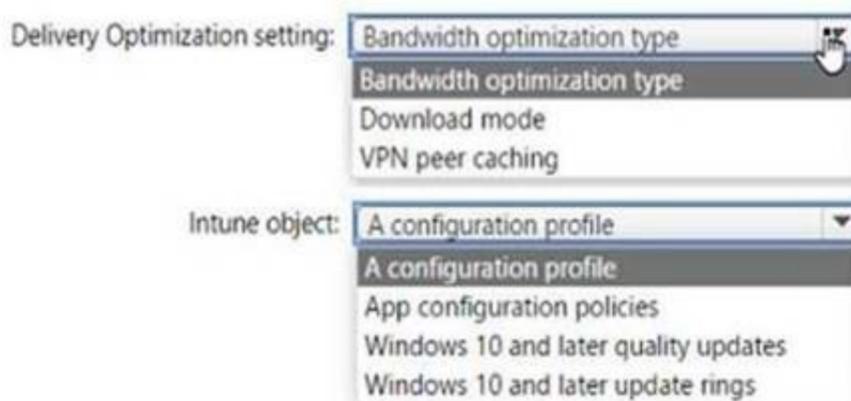
You have 100 Windows 10 devices enrolled in Microsoft Intune.

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 5

- (Exam Topic 4)

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

- Ensure that you can manage the personal devices by using Microsoft Intune.
- Ensure that users can access company data seamlessly from their personal devices.
- Ensure that users can only sign in to their personal devices by using their personal account What should you use to add the devices to Azure AD?

- A. Azure AD registered
- B. hybrid Azure AD join
- C. AD joined

**Answer:** A

**Explanation:**

To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization's resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.

The other options are not suitable for this scenario because:

- > Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories2.
- > AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources3.

References: What are Azure AD registered devices?, What are hybrid Azure AD joined devices?, What is Active Directory domain join?

**NEW QUESTION 6**

- (Exam Topic 4)

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

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

You need to migrate the GPO to Intune.

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

**Actions**

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.
- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

**Answer Area**

>  
<

^  
v

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Actions**

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.
- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

**Answer Area**

- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

>  
<

^  
v

**NEW QUESTION 7**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune.

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

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

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

NOTE: Each correct selection is worth one point.

**Settings**

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

**Answer Area**

Display the progress of app and profile deployments:

Join the devices to Azure AD:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Settings**

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

**Answer Area**

Display the progress of app and profile deployments: Enrollment Status Page

Join the devices to Azure AD: Deployment Profiles

**NEW QUESTION 8**

- (Exam Topic 4)

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

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 9**

- (Exam Topic 4)

You have a computer named Computer1 that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.

What should you do on Computer1?

- A. Turn on Reputation-based protection.
- B. Enable Network Level Authentication (NLA).
- C. Turn on Network Discovery.
- D. Configure the Remote Desktop Configuration service.

**Answer:** B

**NEW QUESTION 10**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

All users have Microsoft 365 apps deployed.

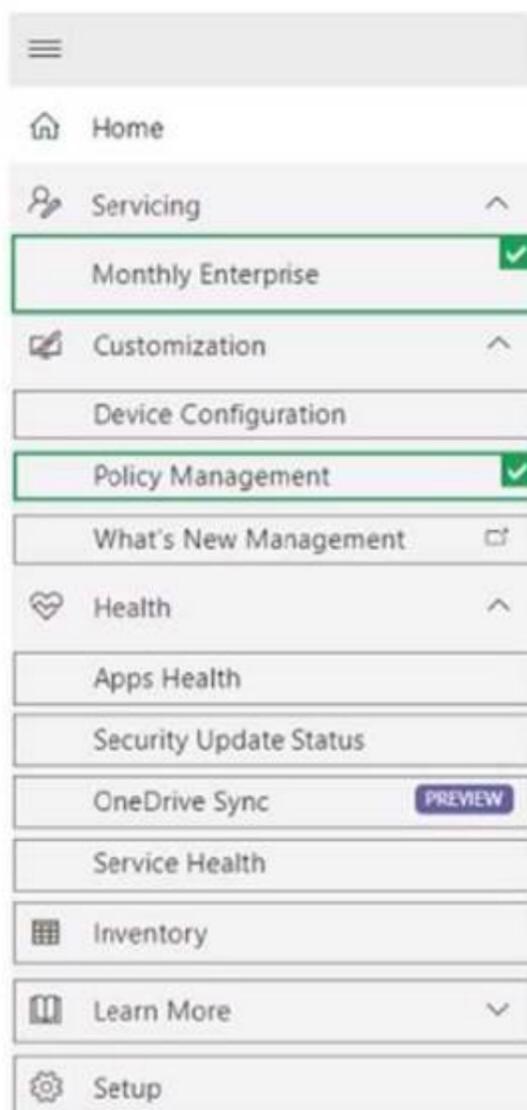
You need to configure Microsoft 365 apps to meet the following requirements:

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

Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

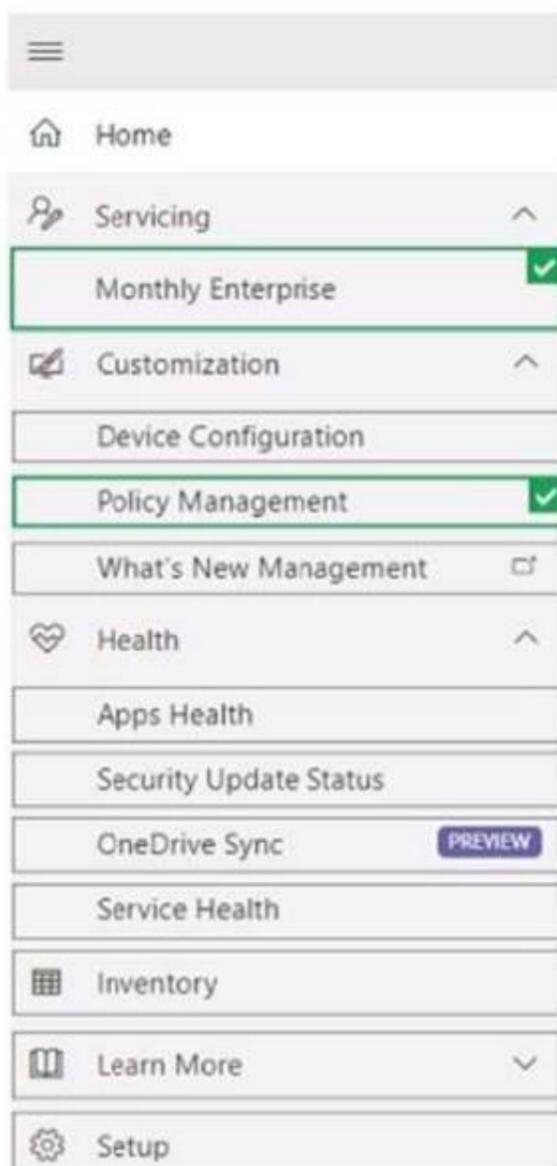
Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area



**NEW QUESTION 10**

- (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:

- User 1 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.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



**NEW QUESTION 13**

- (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 18**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.

What should you select in the Microsoft Endpoint Manager admin center?

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

**Answer: A**

**Explanation:**

App report: You can search by platform and app, and then this report will provide two different app protection statuses that you can select before generating the report. The statuses can be Protected or Unprotected.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-monitor>

**NEW QUESTION 22**

- (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 23**

- (Exam Topic 4)

You have a computer named Computer5 that has Windows 10 installed. You create a Windows PowerShell script named config.ps1. You need to ensure that config.ps1 runs after feature updates are installed on Computer5. Which file should you modify on Computer5?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 26**

- (Exam Topic 4)

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

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

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.

You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.

To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Server:

Ports:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Server4

Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.

Box 2: TCP 443 and UDP 443 only

Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.

By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Saerver Configuration – Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.

Incorrect:

TCP 1723 is not used.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-overview>

**NEW QUESTION 28**

- (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  
  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)**

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 type="radio"/>
If you reset Device2, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If you restart Device3, the device will be deployed by using Autopilot.	<input 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 33**

- (Exam Topic 4)

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- MDM user scope: Group1
- MAM user scope: Group2

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

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 35**

- (Exam Topic 4)

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune. Currently, Windows updates are downloaded without using Delivery Optimization. You need to configure the computers to use Delivery Optimization. What should you create in Intune?

- A. a device compliance policy
- B. a Windows 10 update ring
- C. a device configuration profile
- D. an app protection policy

**Answer: C**

**NEW QUESTION 38**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription and 100 computers that run Windows 10.

You need to deploy Microsoft Office Professional Plus 2019 to the computers by using Microsoft Office Deployment Tool (ODT).

What should you use to create a customization file for ODT?

- A. the Microsoft 365 admin center
- B. the Microsoft Intune admin center
- C. the Microsoft Purview compliance portal
- D. the Microsoft 365 Apps admin center

**Answer: D**

**NEW QUESTION 42**

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share1. You add Windows 10 images to Share1 as shown in the following table.

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

Which images can be used in the Standard Client Task Sequence, and which images can be used in the Standard Client Upgrade Task Sequence?  
 NOTE: Each correct selection is worth one point.

**Answer Area**

Standard Client Task Sequence:

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

Standard Client Upgrade Task Sequence:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Answer Area**

Standard Client Task Sequence:

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

Standard Client Upgrade Task Sequence:

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

**NEW QUESTION 43**

- (Exam Topic 4)

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

You have a Microsoft 365 subscription

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

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

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

**Answer Area**

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

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
**Answer Area**

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

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

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

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

**NEW QUESTION 45**

- (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 49**

- (Exam Topic 4)

You have a Microsoft Intune subscription.

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

### Create profile

Windows PC

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

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

- Deployment mode: User-Driven
- Join to Azure AD as: Azure AD joined
- Microsoft Software License Terms: Hide
- Privacy settings: 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: Hide
- User account type: Standard
- Allow White Glove OOBE: No
- Language (Region): Operating system default
- Automatically configure keyboard: Yes
- Apply device name template: 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

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

- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

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

- computer name
- Cortana settings
- keyboard layout

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

### Answer Area

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

- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

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

- computer name
- Cortana settings
- keyboard layout

NEW QUESTION 50

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer2 that run Windows 10. You install Windows Admin Center on Computer1. You need to manage Computer2 from Computer1 by using Windows Admin Center. What should you do on Computer2?

- A. Update the TrustedHosts list
- B. Run the Enable-PSRemoting cmdlet
- C. Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.
- D. Add an inbound Microsoft Defender Firewall rule.

**Answer: B**

**Explanation:**

To manage a remote computer from Windows Admin Center, you need to enable PowerShell remoting on the remote computer. You can do this by running the Enable-PSRemoting cmdlet, which configures the WinRM service, creates a listener, and allows inbound firewall rules for PowerShell remoting. The other options are not sufficient or necessary for this task. References: Installation and configuration for Windows Remote Management

**NEW QUESTION 55**

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune. You need to configure an Intune device configuration profile to meet the following requirements:

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

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

NOTE: Each correct selection is worth one point.

Answer Area

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

A screenshot of a computer Description automatically generated

References:

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

**NEW QUESTION 57**

- (Exam Topic 4)

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings. Does this meet the goal?

- A. Yes
- B. No

Answer: B

**NEW QUESTION 58**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8, 9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:

- > Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.
- > Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

▼

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

▼

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

A screenshot of a computer Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set> <https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

**NEW QUESTION 61**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune.

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

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

Answer: D

**NEW QUESTION 62**

- (Exam Topic 4)

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

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

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

Answer: D

**Explanation:**

The correct answer is D because app configuration policies can be applied to managed devices and managed apps<sup>1</sup>. Managed devices are enrolled and managed by Intune, while managed apps are integrated with Intune App SDK or wrapped using the Intune Wrapping Tool<sup>1</sup>. Device2, Device3, and Device4 are either enrolled in Intune or have managed apps installed, so they can receive app configuration policies<sup>2</sup>. Device1 is not enrolled in any MDM solution and does not have any managed apps installed, so it cannot receive app configuration policies<sup>2</sup>. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Policy sets - Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets>

**NEW QUESTION 66**

- (Exam Topic 4)

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

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

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

NOTE: Each correct selection is worth one point.

**Settings**

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

**Answer Area**

Device1:

Device2:

Device3:

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

**Settings**

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

**Answer Area**

Device1:

Device2:

Device3:

**NEW QUESTION 70**

- (Exam Topic 4)

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

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

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

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

Answer: C

**Explanation:**

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

**NEW QUESTION 71**

- (Exam Topic 4)

You have a Microsoft Intune deployment that contains the resources shown in the following table.

Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	Not applicable
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	Not applicable

You create a policy set named Set1 and add Comply1 to Set1. Which additional resources can you add to Set1?

- A. Conf1 only
- B. Comply2 only
- C. Comply2 and Conf1 only
- D. CA1, Conf1, and Office 1 only
- E. Comply2, CA1, Conf1, and Office1

**Answer:** B

**NEW QUESTION 74**

- (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 75**

- (Exam Topic 3)

You need to meet the technical requirements for the LEG department computers.

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**

Configure the commercial ID on the LEG department computers.

Create an Azure Machine Learning service workspace.

Create an Azure Log Analytics workspace.

Install the Microsoft Monitoring Agent on the LEG department computers.

Add a solution to a workspace.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a white box Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-azure-portal>

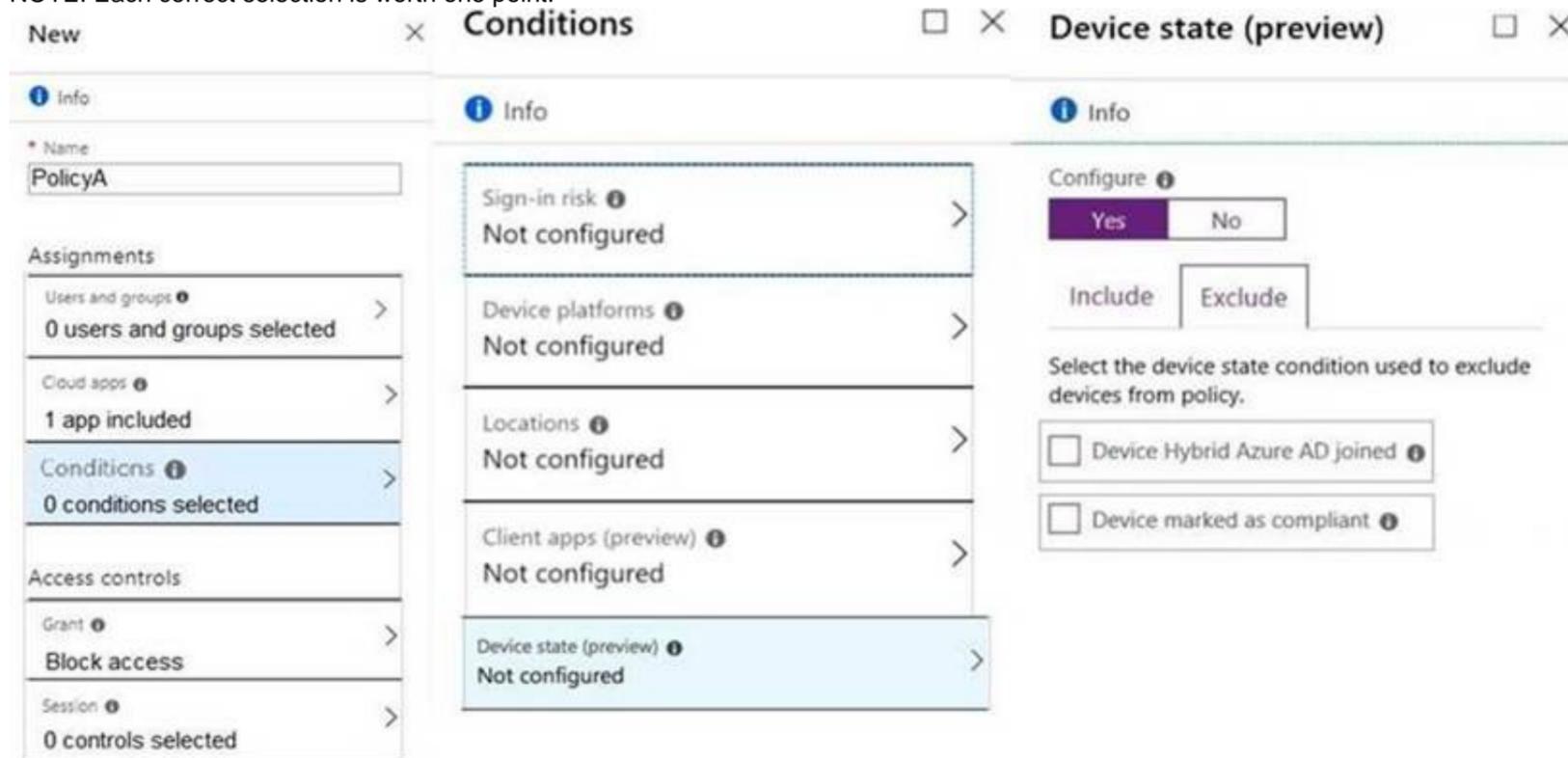
**NEW QUESTION 77**

- (Exam Topic 3)

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

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

A screenshot of a computer Description automatically generated

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

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

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

References:

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

**NEW QUESTION 82**

- (Exam Topic 3)

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Policy1:**

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device 3

**Policy2:**

Device1 only
Device2 only
Device3 only
Device4 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device 3

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/intune/device-profile-assign>

**NEW QUESTION 87**

- (Exam Topic 3)

You are evaluating which devices are compliant.

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 88**

- (Exam Topic 3)

You need to meet the technical requirements for the IT department. What should you do first?

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

**Answer:** C

**Explanation:**

Reference:

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

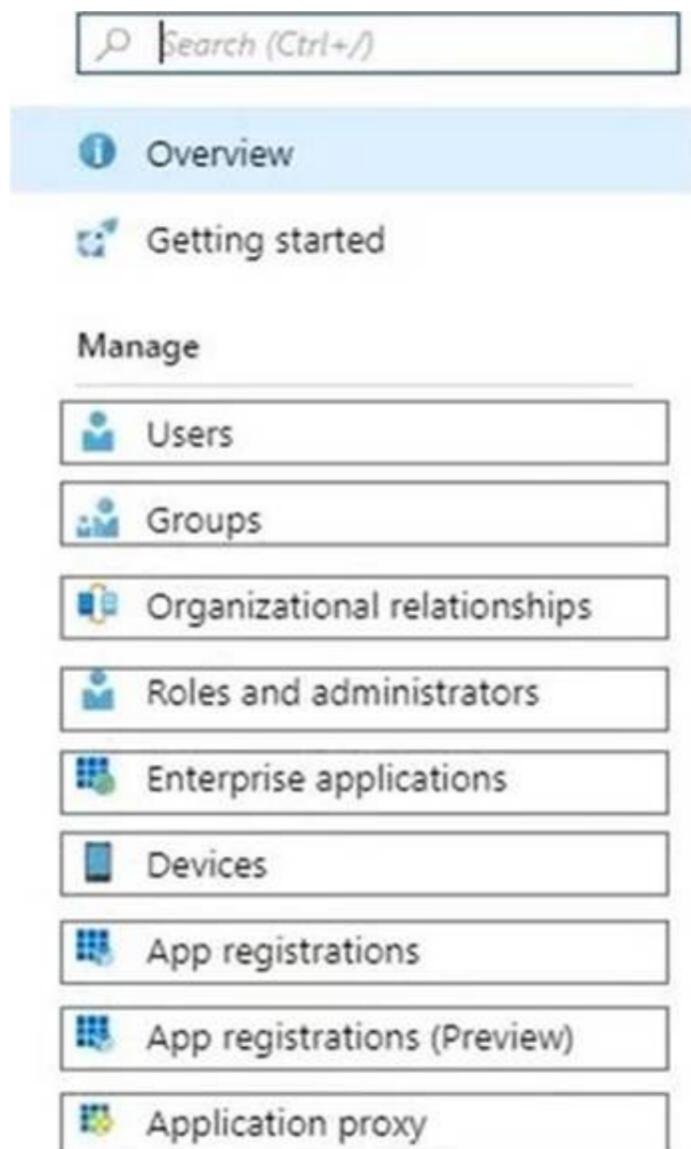
**NEW QUESTION 92**

- (Exam Topic 2)

You need to meet the technical requirements for Windows AutoPilot.

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 97**

- (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 98**

- (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 102**

- (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 104**

- (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 108**

- (Exam Topic 1)

You implement the planned changes for Connection1 and Connection2

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

NOTE; Each correct selection is worth one point.

**Answer Area**

Device1:  1  
 2  
Device2:  3  
 4  
 5

Device2:  1  
 2  
 3  
 4  
 5

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Device1:  1  
 2  
Device2:  3  
 4  
 5

Device2:  1  
 2  
 3  
 4  
 5

**NEW QUESTION 113**

- (Exam Topic 1)

Which users can purchase and assign App1?

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

**Answer: B**

**Explanation:**

Reference:

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

**NEW QUESTION 117**

- (Exam Topic 1)

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

**Answer Area**

Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	<input type="radio"/>	<input type="radio"/>
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<input type="radio"/>	<input type="radio"/>
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Text, letter Description automatically generated

**NEW QUESTION 120**

- (Exam Topic 4)

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 121**

- (Exam Topic 4)

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 125**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1@contoso.com.

You join a Windows 10 device named Client1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Administrators /add " [Dropdown] \user1@contoso.com"

Dropdown 1 options: net accounts, net localgroup, net user

Dropdown 2 options: AzureAD, CONTOSO, UPN

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Administrators /add " [Dropdown] \user1@contoso.com"

Dropdown 1 options: net accounts, net localgroup, net user

Dropdown 2 options: AzureAD, CONTOSO, UPN

*Note: In the original image, 'net localgroup' and 'AzureAD' are highlighted with red boxes.*

**NEW QUESTION 129**

- (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 130**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

- A. an attack surface reduction (ASR) policy
- B. a security baseline
- C. an endpoint detection and response (EDR) policy
- D. an account protection policy
- E. an antivirus policy

**Answer:** C

**Explanation:**

To onboard the devices to Microsoft Defender for Endpoint, you need to create an endpoint detection and response (EDR) policy in the Microsoft Intune admin center. This policy enables EDR capabilities on devices that are enrolled in Intune and allows you to configure various settings for EDR functionality. You can then assign the policy to groups of users or devices. References:  
<https://docs.microsoft.com/en-us/mem/intune/protect/edr-windows>

**NEW QUESTION 135**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1 and a web app named Appl. App1 must only accept modern authentication requests. You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:

- Assignments
  - Users or workload identities: User1
  - Cloud apps or actions: App1
- Access controls
  - Grant: Block access

You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

- A. Filter for devices
- B. Device platforms
- C. User risk
- D. Sign-in risk
- E. Client apps

**Answer:** E

**Explanation:**

you can use the client apps condition to block legacy authentication requests to App1. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols. References: 1: Conditional Access: Block legacy authentication | Microsoft Learn <https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy-authentication> 2: What is legacy authentication? | Microsoft Learn <https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/legacy-authentication> 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn <https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client-apps-condition>

**NEW QUESTION 137**

- (Exam Topic 4)

You have two computers named Computer1 and Computer2 that run Windows 10. Computer2 has Remote Desktop enabled. From Computer1, you connect to Computer2 by using Remote Desktop Connection. You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session. What should you do?

- A. From Computer 2, configure the Remote Desktop settings.
- B. From Windows Defender Firewall on Computer 1, allow Remote Desktop.
- C. From Windows Defender Firewall on Computer 2, allow File and Printer Sharing.
- D. From Computer1, configure the Remote Desktop Connection settings.

**Answer:** D

**NEW QUESTION 140**

- (Exam Topic 4)

Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active Directory (Azure AD).

There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.

You plan to implement Microsoft Defender Exploit Guard.

You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Tool to use to configure the settings:

▼
Security & Compliance in Microsoft 365
Windows Security app
Microsoft Endpoint Manager admin center

Distribution method:

▼
An Azure policy
An Endpoint Protection configuration profile
An Intune device compliance policy
A device restrictions configuration profile

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a computer Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/import-export-expl> <https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-prot>

**NEW QUESTION 143**

- (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 146**

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices. From the Microsoft Intune admin center, you add a Microsoft Store app. Which two App information types are visible in the Company Portal? NOTE: Each correct selection is worth one point.

- A. Privacy URL
- B. Information URL
- C. Developer
- D. Owner

**Answer:** AC

**NEW QUESTION 147**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM). You need to deploy the Microsoft 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>

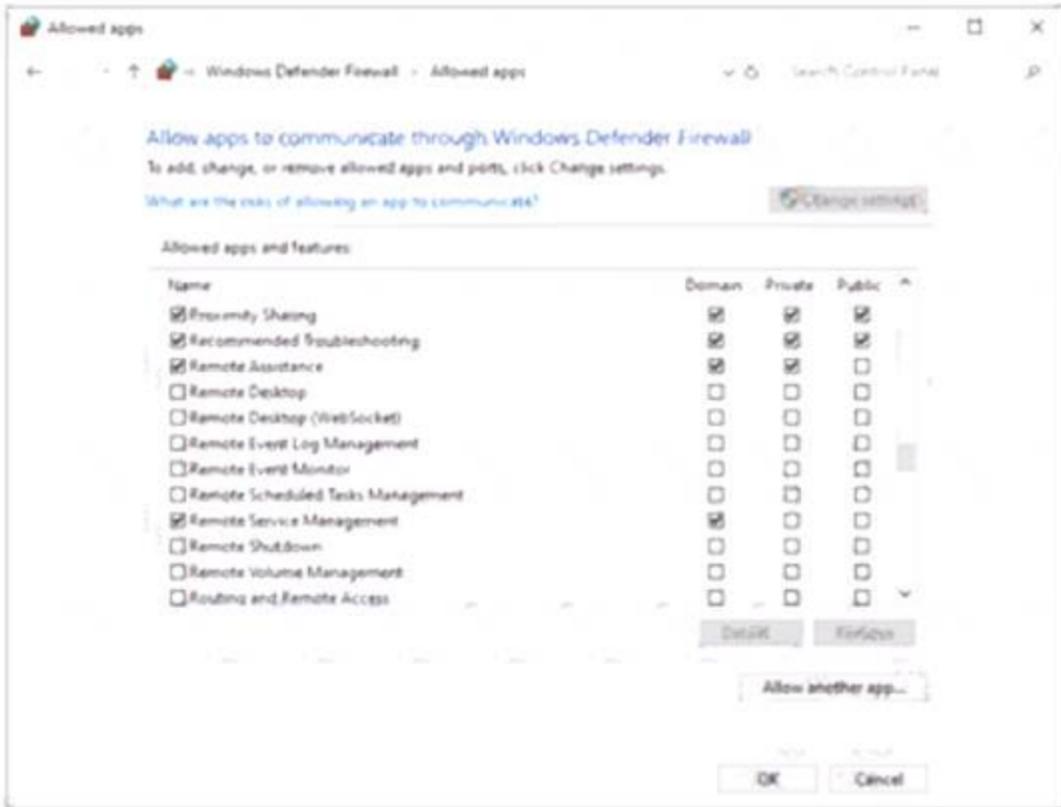
**NEW QUESTION 152**

- (Exam Topic 4)

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

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

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



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

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

**NOTE:** Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.	<input type="checkbox"/>	<input checked="" 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 157**

- (Exam Topic 4)

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 158**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You plan to use Endpoint analytics.

You need to create baseline metrics.

What should you do first?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 163**

- (Exam Topic 4)

You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group1, Group2

Windows 10 update rings are defined in Intune as shown in the following table.

Name	Quality deferral (days)	Assigned
Ring1	3	Yes
Ring2	10	Yes

You assign the update rings as shown in the following table.

Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Quality deferral on Computer1:  ▼

3 days

7 days

10 days

13 days

No effect

Quality deferral on Computer2:  ▼

3 days

7 days

10 days

13 days

No effect

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a computer Description automatically generated

Computer1 and Computer2 are members of Group1. Ring1 is applied to Group1.

Note: The term "Exclude" is misleading. It means that the ring is not applied to that group, rather than that group being blocked.

References:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-intune> <https://allthingscloud.blog/configure-windows-update-business-using-microsoft-intune/>

**NEW QUESTION 168**

- (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="checkbox"/>	<input type="checkbox"/>
User2 can complete the Autopilot process on Device1.	<input type="checkbox"/>	<input type="checkbox"/>
User3 can view device setup information during the enrollment phase of Device1.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

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

**NEW QUESTION 171**

- (Exam Topic 4)

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

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

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

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

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

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

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

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

**NEW QUESTION 173**

- (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 174**

- (Exam Topic 4)

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

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

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

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

**Answer:** A

**Explanation:**

User sign-in frequency

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

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

Sign-in frequency control

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

Select Sign-in frequency.

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

- Save your policy. Reference:

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

**NEW QUESTION 179**

- (Exam Topic 4)

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

You use Microsoft Intune to manage devices.

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

What should you configure?

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

**Answer:** D

**NEW QUESTION 180**

- (Exam Topic 4)

You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.

You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.

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

- A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
- B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
- C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
- D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
- E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
- F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

**Answer:** CE

**Explanation:**

To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices. References:

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

**NEW QUESTION 185**

- (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)  ✓

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

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

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

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

Source:

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

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

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

**NEW QUESTION 189**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune. You plan to manage Windows updates by using Intune.

You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.

**User experience settings**

Automatic update behavior

Active hours start \*

Active hours end \*

Restart checks  Allow  Skip

Option to pause Windows updates  Enable  Disable

Option to check for Windows updates  Enable  Disable

Change notification update level

Use deadline settings  Allow  Not configured

Deadline for feature updates

Deadline for quality updates

Grace period

Auto reboot before deadline  Yes  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**

Automatic restarts are blocked [answer choice].

A restart will be forced on a device [answer choice] after the deadline.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
**Answer Area**

Automatic restarts are blocked [answer choice].

A restart will be forced on a device [answer choice] after the deadline.

**NEW QUESTION 190**

- (Exam Topic 4)

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

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

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

- A. Admin1, Admin2, Admin3. and Admin4
- B. Admin1, Admin2, and Admin3 only

- C. Admin3 only
- D. Admin3 and Admin4 only
- E. Admin1 and Admin3 only

**Answer:** B

**Explanation:**

\* Admin1

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

\* Admin2

Mark your app as publisher verified.

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

\* Admin3

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

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

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

**NEW QUESTION 192**

- (Exam Topic 4)

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

Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

AH devices contain an app named App1 and are enrolled in Microsoft Intune.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

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

Minimum number of policies:

- 1
- 2
- 3
- 4
- 5

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

of Corre Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices1. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps2. You only need one policy to apply this setting to all devices that have App1 installed.

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

**NEW QUESTION 197**

- (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 198**

- (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 202**

- (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](#)

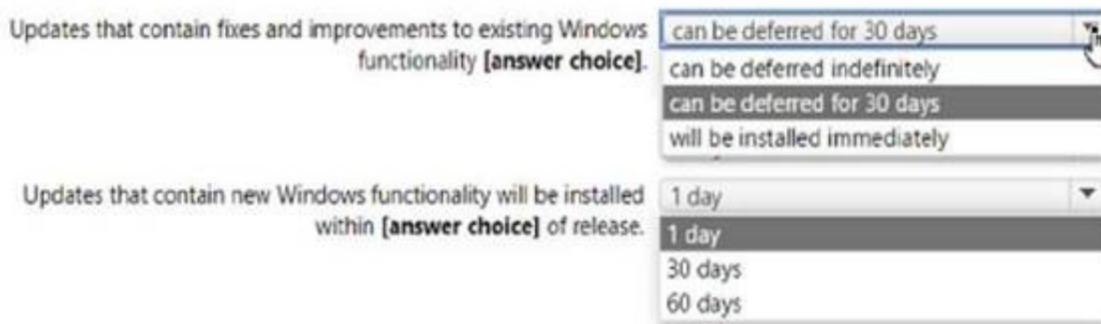
Update settings

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
<b>User experience settings</b>	
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



- 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 205**

- (Exam Topic 4)

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

- Personal devices do not need to be enrolled in Intune.
- Users must authenticate by using a PIN before they can access corporate email data.
- Users can use their personal iOS and Android devices to access corporate cloud services.
- Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.

You need to configure a solution to enforce the security policy. What should you create?

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

Answer: B

**NEW QUESTION 207**

- (Exam Topic 4)

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

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

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

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 209**

- (Exam Topic 4)

You have computers that run Windows 10 and are configured by using Windows AutoPilot. A user performs the following tasks on a computer named Computer1:

- > Creates a VPN connection to the corporate network
- > Installs a Microsoft Store app named App1
- > Connects to a Wi-Fi network

You perform a Windows AutoPilot Reset on Computer1.

What will be the state of the computer when the user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The Wi-Fi connection will be:

Removed  
 Retained and the passphrase will be retained  
 Retained but the passphrase will be reset

App1 will be:

Reinstalled at sign-in  
 Removed  
 Retained

The VPN connection will be:

Removed  
 Retained and the credentials will be cached  
 Retained but the credentials will be reset

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 212**

- (Exam Topic 4)

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

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 214**

- (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 217**

- (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 219**

- (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 224**

- (Exam Topic 4)

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- > MDM user scope: Group1
- > MAM user scope: Group2

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

NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 227**

- (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**

- Upload the file by using Microsoft Intune.
- Generate a CSV file that contains the computer information.
- Reset the computer.
- Generate a JSON file that contains the computer information.
- Upload the file by running azcopy.exe.

**Answer Area**

- 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 232**

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune.

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

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

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

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

**Answer:** C

**NEW QUESTION 237**

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

**Manage**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

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

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

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

**NEW QUESTION 241**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain and an Azure AD tenant.

The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

Which device configuration profile type template should you use?

- A. Administrative Templates
- B. Endpoint protection
- C. Device restrictions
- D. Custom

**Answer:** A

**Explanation:**

To configure the settings shown in the table, you need to use the Administrative Templates device configuration profile type template. This template allows you to configure hundreds of settings that are also available in Group Policy. You can use this template to configure settings such as password policies, account lockout policies, and audit policies. References:

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

**NEW QUESTION 244**

- (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 248**

- (Exam Topic 4)

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

**Device restrictions**

Windows 10 and later

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

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

Previous

Next

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

## Device restrictions

Windows 10 and later

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

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

**NEW QUESTION 252**

- (Exam Topic 4)

You have a Microsoft Intune subscription that has the following device compliance policy settings: Mark devices with no compliance policy assigned as: Compliant  
 Compliance status validity period (days): 14

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

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:

- Name: Policy1
- Platform: Windows 10 and later
- Require BitLocker: Require
- Mark device noncompliant: 5 days after noncompliance
- Scope (Tags): Tag1
- Name: Policy2
- Platform: Windows 10 and later
- Firewall: Require
- Mark device noncompliant: Immediately
- Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No

For the same reason as Box1. Box 3: Yes

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.

The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

**NEW QUESTION 253**

- (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 \* ⓘ

User logon type \* ⓘ

Application type \* ⓘ

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 \* ⓘ

Microsoft Edge kiosk mode type ⓘ

Refresh browser after idle time ⓘ

Specify Maintenance Window for App Restarts \* ⓘ

Maintenance Window Start Time

Maintenance Window Recurrence ⓘ

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

The 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 256

- (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 260

- (Exam Topic 4)

You have 25 computers that run Windows 10 Pro.

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

You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.

What should you use?

- A. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise
- B. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise
- C. Windows Autopilot
- D. Subscription Activation

**Answer:** C

### NEW QUESTION 264

- (Exam Topic 4)

You install a feature update on a computer that runs Windows 10. How many days do you have to roll back the update?

- A. 5
- B. 10
- C. 14
- D. 30

Answer: B

**NEW QUESTION 266**

- (Exam Topic 4)

You have 500 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
Account protection	DEP: <input type="text"/>
App & browser control	Mandatory ASLR: <input type="text"/>
Device security	
Virus & threat protection	

- 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 apps.

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 app.
- > 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 app.

**NEW QUESTION 271**

- (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:

Data visualization tool:

- 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>

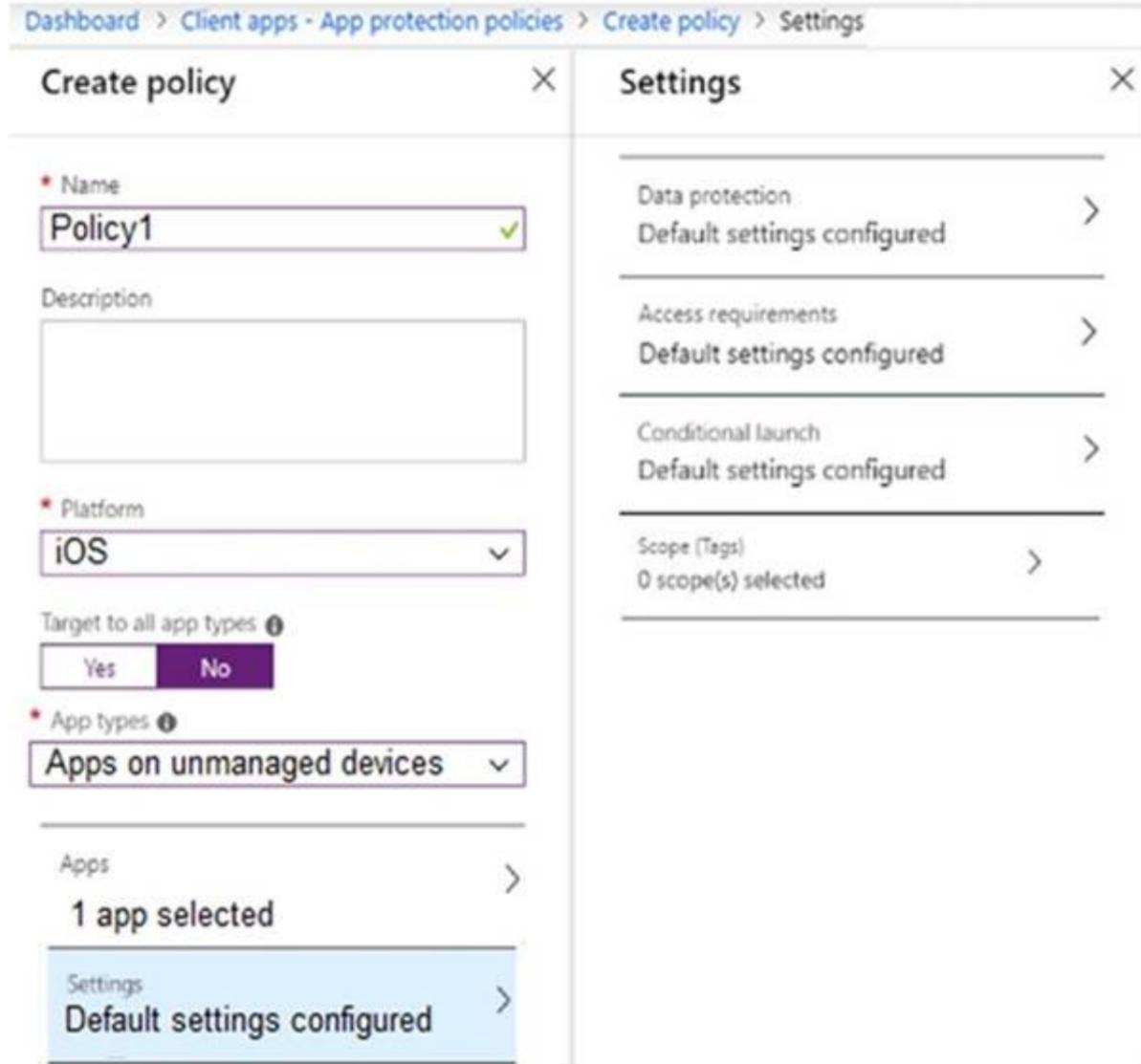
**NEW QUESTION 273**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

Users have iOS devices that are not enrolled in Microsoft 365 Device Management.

You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)



You need to configure the policy to meet the following requirements:

- > Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.
- > Require the users to use an alphanumeric passcode to access the Outlook app.

What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Prevent the users from using Outlook if the operating system version is less than 12.0.0:

▼
Access requirements
Conditional launch
Data protection
Scope

Require the users to use an alphanumeric passcode to access Outlook:

▼
Access requirements
Conditional launch
Data protection
Scope

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:  
<https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios>

**NEW QUESTION 278**

- (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 282**

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune. You plan to manage Microsoft Defender Antivirus on the computers. You need to prevent users from disabling Microsoft Defender Antivirus. What should you do?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 287**

- (Exam Topic 4)

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

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

You assign Windows 10/11 Enterprise E5 licenses to Group1 and User2. You deploy the devices shown in the following table.

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area

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

**NEW QUESTION 289**

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1. User1 is assigned a Windows 10/11 Enterprise E3 license. You use Microsoft Intune Suite to manage devices. User1 activates the following devices:

- Device1: Windows 11 Enterprise
- Device2: Windows 10 Enterprise
- Device3: Windows 11 Enterprise

How many more devices can User1 activate?

- A. 2
- B. 3
- C. 7
- D. 8

Answer: A

**NEW QUESTION 290**

- (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 295**

- (Exam Topic 4)

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

You plan to create Windows 11 device builds for the marketing and research departments. The solution must meet the following requirements:

- Marketing department devices must support Windows Update for Business.
- Research department devices must have support for feature update versions for up to 36 months from release. What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

Marketing: 

- Windows 11 Enterprise
- Windows 11 Pro**
- Windows 11 Pro for Workstations

Research: 

- Windows 11 Enterprise**
- Windows 11 Pro
- Windows 11 Pro for Workstations

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

**Answer Area**

Marketing:  

- Windows 11 Enterprise
- Windows 11 Pro**
- Windows 11 Pro for Workstations

Research:  

- Windows 11 Enterprise**
- Windows 11 Pro
- Windows 11 Pro for Workstations

NEW QUESTION 298

.....

## 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](#)