

# Microsoft

## Exam Questions MD-102

Endpoint Administrator



### NEW QUESTION 1

- (Exam Topic 4)

You have an Azure subscription.

You have an on-premises Windows 11 device named Device 1. You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription. To what should you associate DCR1 ?

- A. Azure Network Watcher
- B. Device1
- C. a Log Analytics workspace
- D. a Monitored Object

**Answer:** B

#### Explanation:

To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it. A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1. To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2. You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.

The other options are not correct for this scenario because:

➤ Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources. It is not related to data collection rules or Azure Monitor4.

➤ A Log Analytics workspace is a destination where you can send the data collected by a data collection rule. It is not an entity that you can associate a DCR with5.

➤ A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules. References: Data collection rules in Azure Monitor, Configure data collection for Azure Monitor Agent, U

Azure Policy to install Azure Monitor Agent and associate with a DCR, What is Azure Network Watcher?, Log Analytics workspaces in Azure Monitor

### NEW QUESTION 2

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage Windows 11 devices.

You need to implement passwordless authentication that requires users to use number matching Which authentication method should you use?

- A. Microsoft Authenticator
- B. voice calls
- C. FIDO2 security keys
- D. text messages

**Answer:** A

### NEW QUESTION 3

- (Exam Topic 4)

You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to upgrade the computers to Windows 11 Enterprise. What should you configure in Intune?

- A. a device compliance policy
- B. a device cleanup rule
- C. a device enrollment policy
- D. a device configuration profile

**Answer:** D

### NEW QUESTION 4

- (Exam Topic 4)

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

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

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

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

- Assignments
  - o Users or workload identities: User 1. User1
  - o Cloud apps or actions: Office 365 Exchange Online
  - o Conditions: Device platforms: Windows, iOS

- Access controls
  - o Grant Require multi-factor authentication

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 5

- (Exam Topic 4)  
You have a Microsoft 365 subscription that includes Microsoft Intune.  
You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:

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

What should you configure? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all.  
You may need to drag the split bar between panes or scroll to view content.  
NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in Defender for Endpoint. You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. References:  
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/conditional-access  
To prevent suspicious scripts from running on devices, you need to configure an attack surface reduction (ASR) rule in Intune. ASR rules are part of the endpoint protection settings that you can apply to devices by using device configuration profiles. You can use the ASR rule “Block Office applications from creating child processes” to prevent Office applications from launching child processes such as scripts or executables. References:  
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#attack-surface-reduction

NEW QUESTION 6

- (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:

Join the devices to Azure AD:

#### NEW QUESTION 7

- (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 8

- (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 9

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.

Which extension should you select for the app package file?

- A. .intunemac
- B. .apk
- C. .jpa
- D. .appx

**Answer:** C

**Explanation:**

iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.

Reference:

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

**NEW QUESTION 10**

- (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 configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 10**

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 1,000 iOS devices. The devices are enrolled in Microsoft Intune as follows:

- Two hundred devices are enrolled by using the Intune Company Portal.
- Eight hundred devices are enrolled by using Apple Automated Device Enrollment (ADE).

You create an iOS/iPadOS software updates policy named Policy 1 that is configured to install iOS/iPadOS 15.5.

How many iOS devices will Policy1 update, and what should you configure to ensure that only iOS/iPadOS 15.5 is installed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Number of devices:

Configure a:

200  
800  
1000

Compliance policy  
Conditional Access policy  
Device restriction policy

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Policy 1 will update 800 iOS devices that are enrolled by using Apple Automated Device Enrollment (ADE). This is because ADE devices are supervised devices that support software update policies in Intune<sup>1</sup>. Devices that are enrolled by using the Intune Company Portal are not supervised devices and do not support software update policies<sup>2</sup>.

To ensure that only iOS/iPadOS 15.5 is installed, you should configure a device restriction policy that restricts visibility of software updates. This will prevent users from manually updating the OS to a newer version than the one you specified in Policy 1. You can use the Deployment Workbench to create and assign a device restriction profile to your ADE devices<sup>3</sup>.

**NEW QUESTION 14**

- (Exam Topic 4)

You manage 1,000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

- A. 30 days
- B. 60 days
- C. 90 days
- D. 365 days

**Answer:** B

**Explanation:**

The Device compliance trends report shows the number of devices that are compliant, noncompliant, and not evaluated over time. The report displays trend data for the last 60 days by default, but you can change the time range to view data for the last 7, 14, or 30 days as well. The report does not show data for more than 60

days. References: [Device compliance trends report]



#### NEW QUESTION 17

- (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 22

- (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 27

- (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 32

- (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 36

- (Exam Topic 4)

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

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

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

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

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

## Create profile

Windows PC

✓ Basics

✓ Out-of-box experience (OOBE)

✓ Assignments

4 Review

### Summary

#### Basics

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

#### Out-of-box experience (OOBE)

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

#### Language (Region)

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 39**

- (Exam Topic 4)  
 You have following types of devices enrolled in Microsoft Intune:

- Windows 10
- Android
- iOS

For which types of devices can you create VPN profiles in Microsoft Intune admin center?

- A. Windows 10 only
- B. Windows 10 and Android only
- C. Windows 10 and iOS only
- D. Android and iOS only
- E. Windows 10, Android, and iOS

**Answer:** E

**NEW QUESTION 40**

- (Exam Topic 4)  
 Your company has a Remote Desktop Gateway (RD Gateway).  
 You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.  
 You need to configure a Remote Desktop connection to connect through the gateway. Which setting should you configure?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 41**

- (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 ⓘ

Show

Hide

Important information about hiding license terms

Privacy settings ⓘ

Show

Hide

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

Hide change account options ⓘ

Show

Hide

User account type ⓘ

Administrator

Standard

Allow White Glove OOBE ⓘ

No

Yes

Language (Region) ⓘ

Operating system default

Automatically configure keyboard ⓘ

No

Yes

Apply device name template ⓘ

No

Yes

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

Answer Area

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

are prevented from modifying any desktop settings

can create additional local users on the device

can modify the desktop settings for all device users

can modify the desktop settings only for themselves

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

computer name

Cortana settings

keyboard layout

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

are prevented from modifying any desktop settings

can create additional local users on the device

can modify the desktop settings for all device users

can modify the desktop settings only for themselves

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

computer name

Cortana settings

keyboard layout

#### NEW QUESTION 43

- (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 46

- (Exam Topic 4)

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

- A. From the Microsoft Endpoint Manager admin center, create a configuration profile.
- B. From the Microsoft Endpoint Manager admin center, create a security baseline.
- C. Onboard the macOS devices to the Microsoft 365 compliance center.
- D. Install Defender for Endpoint on the macOS devices.

**Answer: D**

#### Explanation:

Just install, and use Defender for Endpoint on Mac. Reference:  
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac>

#### NEW QUESTION 51

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You need to assign roles in Intune to meet the following requirements:

- The members of Group1 must manage Intune roles and assignments.
- The members of Group2 must assign existing apps and policies to users and devices.

The solution must follow the principle of least privilege.

Which role should you assign to each group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

#### Answer Area



Group1: Intune Service Administrator  
 Help Desk Operator  
 Intune Role Administrator  
 Intune Service Administrator  
 Policy and Profile Manager

Group2: Policy and Profile Manager  
 Help Desk Operator  
 Intune Role Administrator  
 Intune Service Administrator  
 Policy and Profile Manager

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

To assign roles in Intune to meet the requirements, you should assign the following roles to each group: Group1: Intune Role Administrator Group2: Help Desk Operator

- The Intune Role Administrator role is the only Intune role that can manage custom Intune roles and add assignments for built-in Intune roles1. This role meets the requirement for Group1 to manage Intune roles and assignments.
- The Help Desk Operator role can perform remote tasks on users and devices, and can assign applications or policies to users or devices1. This role meets the requirement for Group2 to assign existing apps and policies to users and devices.

**NEW QUESTION 54**

- (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 55**

- (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 57**

- (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 58**

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.

You enable Windows PowerShell remoting on the computers.

You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.

To which group should you add Admin1?

- A. Access Control Assistance Operators
- B. Remote Desktop Users



- C. Power Users
- D. Remote Management Users

**Answer:** B

#### NEW QUESTION 60

- (Exam Topic 4)

You have a Microsoft 365 subscription.

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

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

The solution must minimize user disruption.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Windows 11 devices managed by using Configuration Manager:

Windows Autopilot
Co-management
User enrollment
<b>Windows Autopilot</b>

Personal iOS devices:

Automated Device Enrollment (ADE)
Apple Configurator
<b>Automated Device Enrollment (ADE)</b>
User enrollment

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Windows 11 devices managed by using Configuration Manager:

Windows Autopilot
Co-management
User enrollment
<b>Windows Autopilot</b>

Personal iOS devices:

Automated Device Enrollment (ADE)
Apple Configurator
<b>Automated Device Enrollment (ADE)</b>
User enrollment

#### NEW QUESTION 64

- (Exam Topic 4)

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

Computer1 has apps that are compatible with Windows 10.

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

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

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 69

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

#### NEW QUESTION 74

- (Exam Topic 4)

You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard. You need to create a deployment share on Server1.

What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

##### Answer Area

On Server1:
Import the Deployment Image Servicing and Management (DISM) PowerShell module.
Import the WindowsAutopilotIntune Windows PowerShell module.
Install the Windows Assessment and Deployment Kit (Windows ADK).
Install the Windows Deployment Services server role.

Add to the MDT deployment share:
Windows 10 image and package only
Windows 10 image and task sequence only
Windows 10 image only
Windows 10 image, task sequence, and package

- A. Mastered
- B. Not Mastered

**Answer: A**

##### Explanation:

Box 1: Install the Windows Deployment Services role. Install and initialize Windows Deployment Services (WDS) On the server:

Open an elevated Windows PowerShell prompt and enter the following command: `Install-WindowsFeature -Name WDS -IncludeManagementTools WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall" WDSUTIL /Set-Server /AnswerClients:All`

Box 2: Windows 10 image and task sequence only Create the reference image task sequence

In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment>

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-im>

#### NEW QUESTION 79

- (Exam Topic 3)

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

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

**Answer: A**

##### Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#manage-autopilot-deployment-profiles>

#### NEW QUESTION 84

- (Exam Topic 3)

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

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

**Answer: A**

##### Explanation:

Reference:

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

#### NEW QUESTION 86

- (Exam Topic 3)

You need to meet the requirements for the MKG department users. What should you do?

- A. Assign the MKG department users the Purchaser role in Microsoft Store for Business
- B. Download the APPX file for App1 from Microsoft Store for Business
- C. Add App1 to the private store
- D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business
- E. Acquire App1 from Microsoft Store for Business

**Answer: E**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store> Enable the users in the MKG department to use App1.

The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store>

**NEW QUESTION 87**

- (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 92**

- (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:

	<input type="checkbox"/>
Device1 only	<input type="checkbox"/>
Device2 only	<input type="checkbox"/>
Device3 only	<input type="checkbox"/>
Device4 only	<input type="checkbox"/>
Device2 and Device3 only	<input type="checkbox"/>
Device1 and Device3 only	<input type="checkbox"/>
Device1, Device2, and Device 3	<input type="checkbox"/>

Policy2:

	<input type="checkbox"/>
Device1 only	<input type="checkbox"/>
Device2 only	<input type="checkbox"/>
Device3 only	<input type="checkbox"/>
Device4 only	<input type="checkbox"/>
Device2 and Device3 only	<input type="checkbox"/>
Device1 and Device3 only	<input type="checkbox"/>
Device1, Device2, and Device 3	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 94

- (Exam Topic 3)

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

User1 can enroll a maximum of:

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

User2 can enroll a maximum of:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:

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

User2 can enroll a maximum of:

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

NEW QUESTION 96

- (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 101

- (Exam Topic 3)

You need to meet the technical requirements for the new HR department computers.

How should you configure the provisioning package? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Specify ComputerName as:

<input type="checkbox"/>
<input checked="" type="checkbox"/> "HR"+ RAND(4)
<input checked="" type="checkbox"/> "HumanResources-"+ RAND(????)
<input type="checkbox"/> HR-%RAND:4%
<input type="checkbox"/> HR-????
<input type="checkbox"/> HumanResources-%RAND:4%

Specify AccountOU as:

<input type="checkbox"/>
<input checked="" type="checkbox"/> CN=Computers, CN=HR, DC=Contoso, DC=com
<input checked="" type="checkbox"/> Computers/HumanResources/Contoso.com
<input type="checkbox"/> Contoso.com/HR/Computers
<input type="checkbox"/> OU=Computers, OU=HR, DC=Contoso, DC=com

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts>

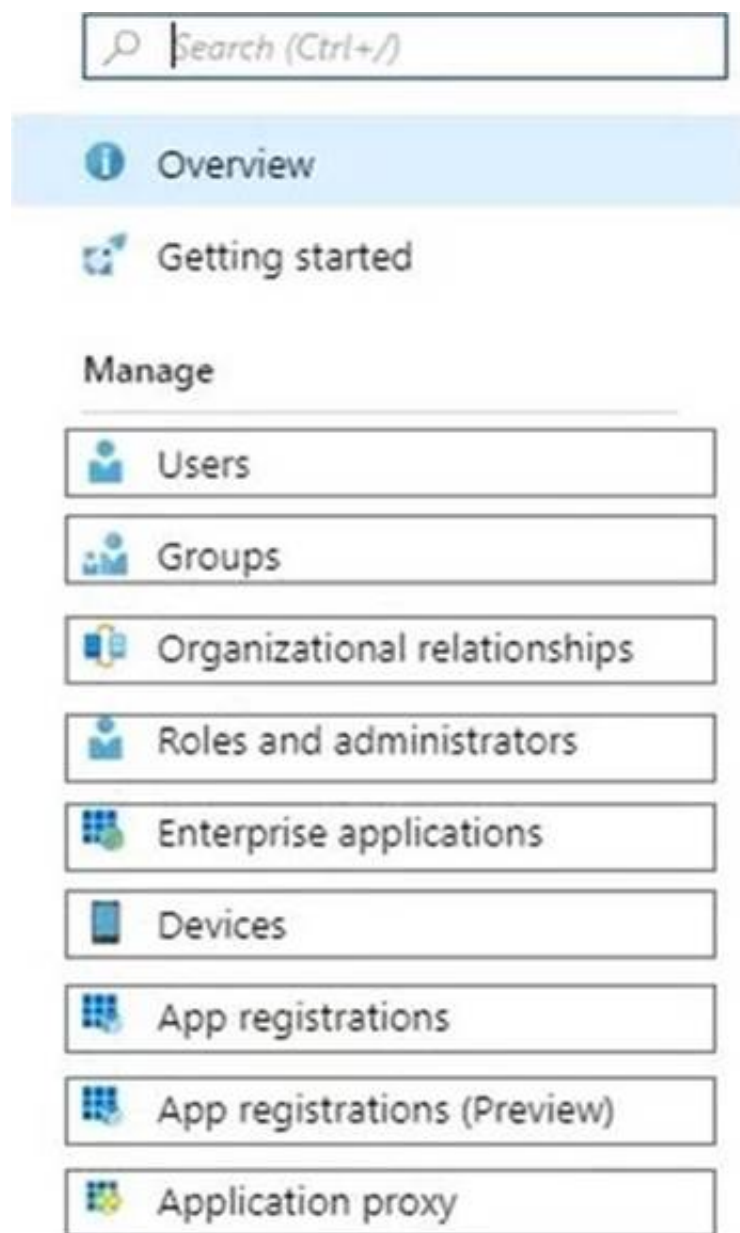
NEW QUESTION 104

- (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 105**

- (Exam Topic 2)

You need to capture the required information for the sales department computers to meet the technical requirements. Which Windows PowerShell command should you run first?

- A. Install-Module WindowsAutoPilotIntune
- B. Install-Script Get-WindowsAutoPilotInfo
- C. Import-AutoPilotCSV
- D. Get-WindowsAutoPilotInfo

**Answer:** B

**Explanation:**

References:

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

"This topic describes how to convert Windows 7 or Windows 8.1 domain-joined computers to Windows 10 devices joined to either Azure Active Directory or Active Directory (Hybrid Azure AD Join) by using Windows Autopilot"

**NEW QUESTION 108**

- (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 110**



- (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 114

- (Exam Topic 1)  
Which user can enroll Device6 in Intune?

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

Answer: B

NEW QUESTION 116

- (Exam Topic 1)  
User1 and User2 plan to use Sync your settings.  
On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

User1:

No devices

Device4 and Device5 only

Device1, Device2 and Device3 only

Device1, Device2, Device3, Device4, and Device5

User2:

No devices

Device4 and Device5 only

Device1, Device2 and Device3 only

Device1, Device2, Device3, Device4, and Device5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Reference:

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

NEW QUESTION 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.

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
A screenshot of a computer Description automatically generated with medium confidence

NEW QUESTION 122

- (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 123

- (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 128

- (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	<div>YesNo</div>
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	<div><input type="radio"/><input type="radio"/></div>
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<div><input type="radio"/><input type="radio"/></div>
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.	<div><input type="radio"/><input type="radio"/></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Text, letter Description automatically generated

NEW QUESTION 130

- (Exam Topic 1)  
You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.  
To what should you grant the right to create the computer objects?

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 135**

- (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 configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**NEW QUESTION 136**

- (Exam Topic 4)

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

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

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 141**

- (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 143**

- (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 App11. 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<sup>2</sup>. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos<sup>2</sup>. 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<sup>13</sup>. 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 148

- (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**

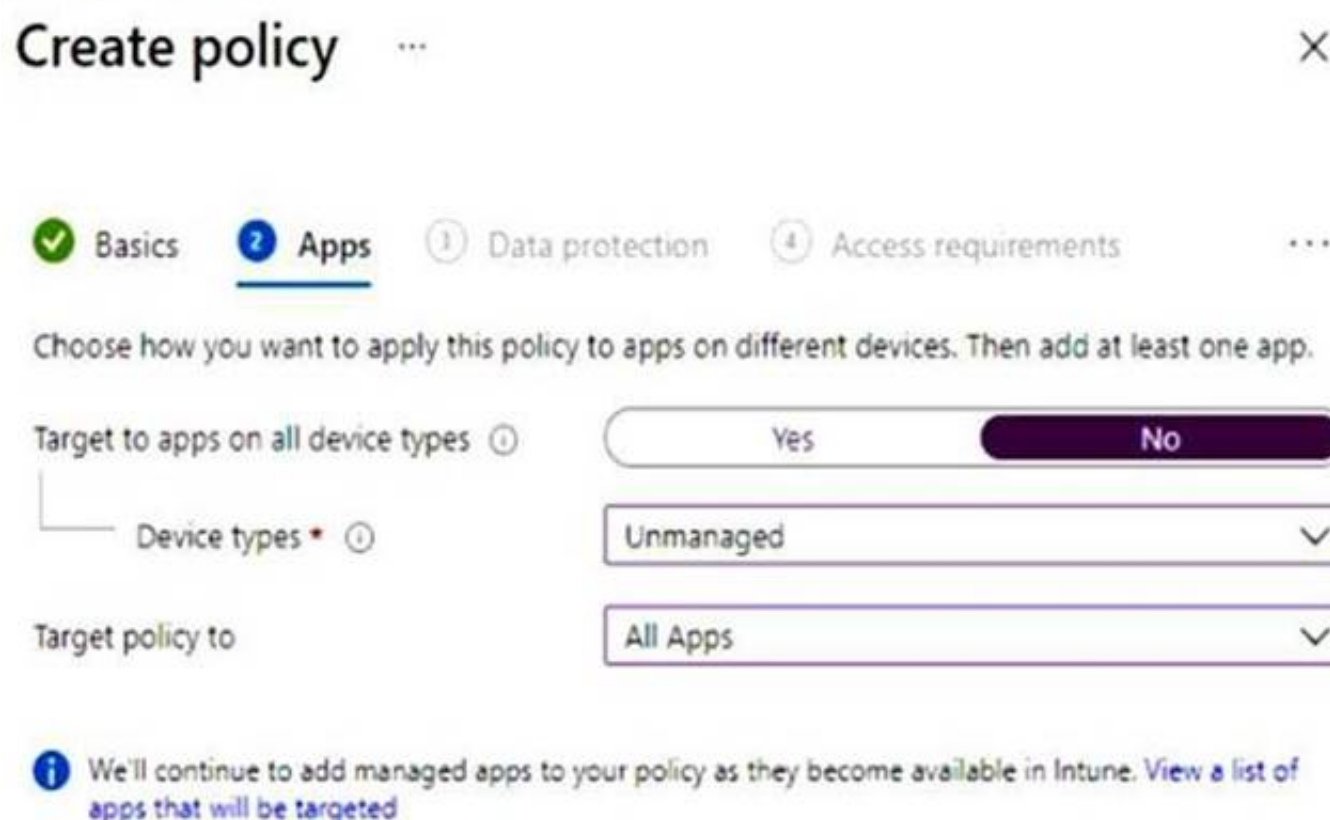
#### NEW QUESTION 149

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.

[Home](#) > [Apps](#) >



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

NOTE: Each correct selection is worth one point.

To apply Policy1 to an Android device, you must [answer choice].

- install the Company Portal app on the device
- install the Microsoft Authenticator app on the device
- onboard the device to Microsoft Defender for Endpoint
- onboard the device to the Microsoft 365 compliance center

When Policy1 is assigned, the policy will apply to [answer choice].

- users only
- devices only
- users and devices

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Box 1: Install the Intune Company Portal app on the device

On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.

Box 2: Devices only

For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party

MDM vendors.  
 Reference:  
<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipado>

**NEW QUESTION 150**

- (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 151**

- (Exam Topic 4)  
 You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device1	64-bit version of Windows 10 Pro	Yes	No
Device2	32-bit version of Windows 10 Pro	No	Yes
Device3	64-bit version of Windows 10 Pro	No	Yes

You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11. You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications.  
 Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

Windows Autopilot:

Device1 and Device3 only

None of the devices

Device1 only

Device1 and Device3 only

Device1, Device2, and Device3

In-place upgrade:

Device1 and Device3 only

None of the devices

Device1 only

Device1 and Device3 only

Device1, Device2, and Device3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Windows Autopilot: Device1 and Device3 only  
 None of the devices  
 Device1 only  
**Device1 and Device3 only**  
 Device1, Device2, and Device3

In-place upgrade: Device1 and Device3 only  
 None of the devices  
 Device1 only  
**Device1 and Device3 only**  
 Device1, Device2, and Device3

**NEW QUESTION 153**

- (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 154**

- (Exam Topic 4)

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

You need to configure an update ring that meets the following requirements:

- Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.
- The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.
- Devices must restart automatically three days after an update is installed.

How should you configure the update ring? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Feature update deferral period (days): 90  
 3  
 7  
 10  
 14  
**90**

Quality update deferral period (days): 14  
 3  
 7  
 10  
**14**  
 90

Grace period: 7  
 3  
**7**  
 10  
 14  
 90

Grace period: 3  
**3**  
 7  
 10  
 14  
 90

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



Answer Area

Feature update deferral period (days):  

90  
3  
7  
10  
14  
90

Quality update deferral period (days):  

14  
3  
7  
10  
14  
90

7  
3  
7  
10  
14  
90

Grace period:  

3  
7  
10  
14  
90

NEW QUESTION 156

- (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 160

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft intune as shown in the following table.

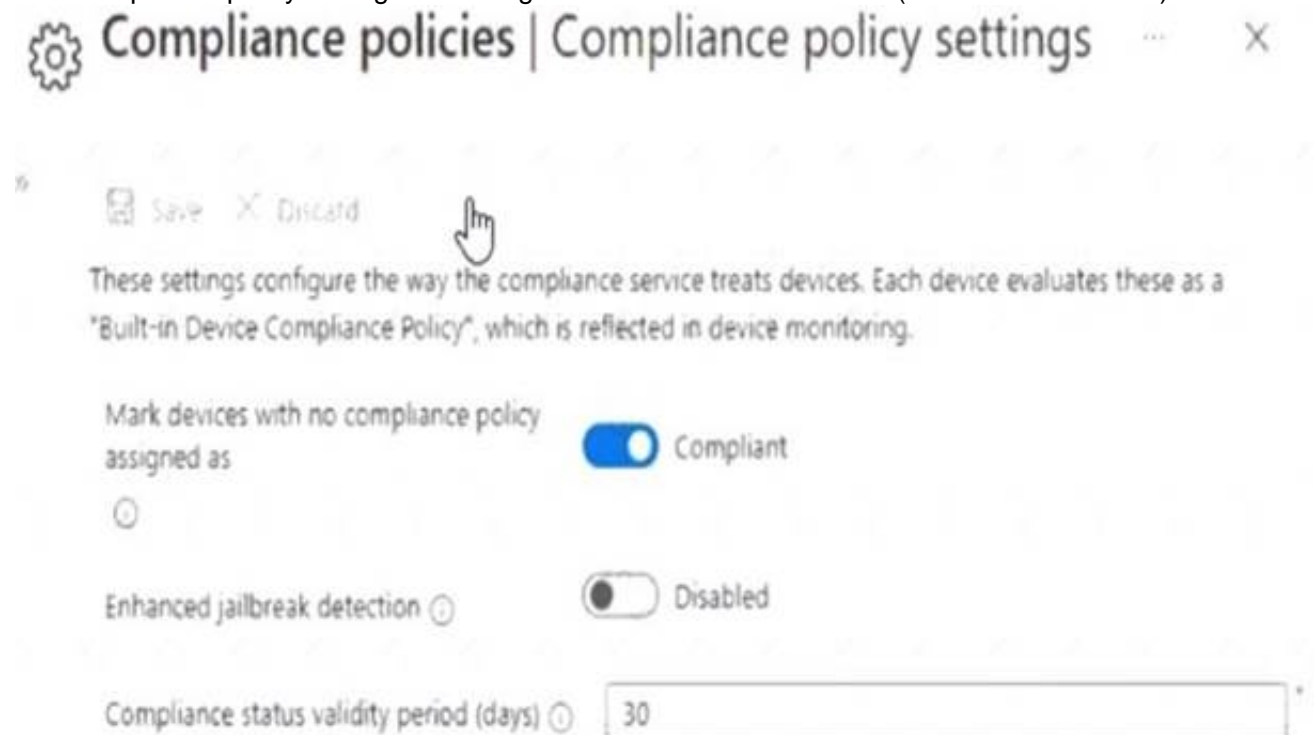
Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.

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

Name	Platform	Setting	Applied to
Compliance1	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	Group3

The Compliance policy settings are configured as shown in the exhibit. (Click the Exhibit tab.) You create the following Conditional Access policy:



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

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

### Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

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

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

**NEW QUESTION 162**  
 - (Exam Topic 4)  
 You have groups that use the Dynamic Device membership type as shown in the following table.


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

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

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

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

**App Information**
[Edit](#)

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	<a href="https://products.office.com/en-us/explore-office-for-home">https://products.office.com/en-us/explore-office-for-home</a>
Privacy URL	<a href="https://privacy.microsoft.com/en-US/privacystatement">https://privacy.microsoft.com/en-US/privacystatement</a>
Developer	Microsoft
Owner	Microsoft
Notes	...
Logo	 <div>Office</div> <div>Teams, Word</div>
Architecture	64-bit
Update channel	Current Channel
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License	No
Teams on behalf of users	No
Install background service for Microsoft Search in Bing	No
Apps to be installed as part of the suite	1 language(s) selected

**Assignments**
[Edit](#)

Group mode	Group
<input checked="" type="radio"/> Required	
<input type="radio"/> Included	Group1

**Available for enrolled devices**

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



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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

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

**NEW QUESTION 163**

- (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 167**

- (Exam Topic 4)

You have the Microsoft Deployment Toolkit (MDT) installed. You install and customize Windows 11 on a reference computer  
You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.  
Which command should you run before you capture the image?

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

**Answer:** C

**Explanation:**

To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the sysprep command with the /generalize option. This option removes all unique system information from the Windows installation, such as the computer name, security identifier (SID), and driver cache. The other commands are not used for this purpose. References: Sysprep (Generalize) a Windows installation

**NEW QUESTION 169**

- (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 173**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to deploy and manage Windows devices.  
You have 100 devices from users that left your company.  
You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.  
What should you do?

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

**Answer:** B

**NEW QUESTION 178**

- (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 183

- (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 186

- (Exam Topic 4)

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

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

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

**Answer:** D

#### Explanation:

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

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

#### NEW QUESTION 191

- (Exam Topic 4)

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

You have a device named Device1 that is enrolled in Intune.

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

NOTE: Each correct selection is worth one point.

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

**Answer:** ABF

#### NEW QUESTION 194

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices that run Windows 11.

User1 provides remote support for 75 devices in the marketing department.

You need to add User1 to the Remote Desktop Users group on each marketing department device. What should you configure?

- A. an app configuration policy
- B. a device compliance policy
- C. an account protection policy
- D. a device configuration profile

**Answer:** D

#### NEW QUESTION 197

- (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 ⓘ

Auto install and restart at maintenance time

Active hours start \* ⓘ

8 AM

Active hours end \* ⓘ

5 PM

Restart checks ⓘ

AllowSkip

Option to pause Windows updates ⓘ

EnableDisable

Option to check for Windows updates ⓘ

EnableDisable

Change notification update level ⓘ

Use the default Windows Update notifications

Use deadline settings ⓘ

AllowNot configured

Deadline for feature updates ⓘ

5

Deadline for quality updates ⓘ

2

Grace period ⓘ

1

Auto reboot before deadline ⓘ

YesNo

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].

between 8 AM and 5 PM

before 8 AM

between 8 AM and 5 PM

after 5 PM

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

5 days

1 day

2 days

5 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

Automatic restarts are blocked [answer choice].

between 8 AM and 5 PM

before 8 AM

between 8 AM and 5 PM

after 5 PM

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

5 days

1 day

2 days

5 days

NEW QUESTION 198

- (Exam Topic 4)  
You have an Azure AD tenant named contoso.com.  
You have a workgroup computer named Computer1 that runs Windows 11. You need to add Computer1 to contoso.com.  
What should you use?

- A. dsreecmd.exe
- B. Computer Management
- C. netdom.exe
- D. the Settings app

Answer: A

NEW QUESTION 201

- (Exam Topic 4)  
You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

- A. an app configuration policy
- B. a security baseline
- C. an app protection policy
- D. an iOS app provisioning profile

**Answer:** C

**Explanation:**

An app protection policy is a set of rules that controls how data is accessed and handled by managed apps on mobile devices. App protection policies can prevent the printing of corporate data from managed apps on iOS devices by using the Restrict cut, copy, and paste with other apps setting. This setting can be configured to block printing from the iOS share menu. An app configuration policy is used to customize the behavior of a managed app, such as specifying a VPN profile or a web link. A security baseline is a collection of recommended security settings for Windows 10 devices that are managed by Intune. An iOS app provisioning profile is a file that contains information about the app's identity, entitlements, and distribution method

**NEW QUESTION 205**

- (Exam Topic 4)

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

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

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

**Answer Area**

Deploy a custom Start layout:

Device restriction

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Rename the local Administrator account:

Identity protection

Delivery optimization

Device restriction

Endpoint protection

Identity protection

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Deploy a custom Start layout:

Device restriction

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Rename the local Administrator account:

Identity protection

Delivery optimization

Device restriction

Endpoint protection

Identity protection

**NEW QUESTION 208**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Auto-enrollment in Intune is configured.

You have 100 Windows 11 devices in a workgroup.

You need to connect the devices to the corporate wireless network and enroll 100 new Windows devices in Intune.

What should you use?

- A. a provisioning package
- B. a Group Policy Object (GPO)
- C. mobile device management (MDM) automatic enrollment
- D. a device configuration policy

**Answer:** C

NEW QUESTION 210

- (Exam Topic 4)

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

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	None
Device2	Windows 10	Joined	None
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured as shown in the following exhibit.

## Create profile

Windows PC

✓ Basics
✓ Out-of-box experience (OOBE)
✓ Assignments
⚙ Review + create

### Summary

#### Basics

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

#### Out-of-box experience (OOBE)

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

#### Assignments

Included groups	Group1
Excluded groups	--

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
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

Device1 has no Mobile device Management (MDM) configured.

Note: Device1 is running Windows 8.1, and is registered, but not joined. Device1 is in Group1.

Profile1 is assigned to Group1. Box 2: No

Device2 has no Mobile device Management (MDM) configured. Note: Device2 is running Windows 10, and is joined.

Device2 is in Group2. Group2 is in Group1.

Profile1 is assigned to Group1. Box 3: Yes

Device3 has Mobile device Management (MDM) configured. Device3 is running Windows 10, and is joined

Device1 is in Group1.

Profile1 is assigned to Group1.

Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD, Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations, policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.

Reference: <https://xo.xello.com.au/blog/windows-autopilot>

#### NEW QUESTION 214

- (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 218

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 223

- (Exam Topic 4)

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

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

- A. Device 1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2. Device3, and Device4

Answer: C

NEW QUESTION 225

- (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 229

- (Exam Topic 4)

Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.  
The company purchases an Azure subscription.  
You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.  
What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

## Answer Area

Resource to create in Azure:

	▼
An Azure event hub	
An Azure Log Analytics workspace	
An Azure SQL database	
An Azure Storage account	

Configuration to perform on the computers:

	▼
Configure the Event Collector service	
Create an event subscription	
Install the Microsoft Monitoring Agent	

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

A screenshot of a computer Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

## NEW QUESTION 231

- (Exam Topic 4)

You have a Microsoft 365 tenant that contains the objects shown in the following table. You are creating a compliance policy named Compliance1. Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

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

**Answer:** C

### Explanation:

Reference:

<https://www.ravenswoodtechnology.com/microsoft-intune-compliance-notifications/> <https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

## NEW QUESTION 236

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You have devices enrolled in Microsoft Intune as shown in the following table. To which devices can you deploy apps by using Intune?

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

**Answer:** E

## NEW QUESTION 241

- (Exam Topic 4)

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices. You purchase a Microsoft 365 E5 subscription.

You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.

Which upgrade method should you use?

- A. Windows Autopilot
- B. a Microsoft Deployment Toolkit (MDT) lite-touch deployment
- C. Subscription Activation
- D. an in-place upgrade by using Windows installation media

**Answer:** C

### Explanation:

Subscription Activation is a feature that allows you to upgrade from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise without needing a product key or reinstallation. You just need to assign a subscription license (such as Microsoft 365 E5) to the user in Azure AD, and then sign in to the device with that user account. The device will automatically activate Windows Enterprise edition using the firmware-embedded activation key for Windows Pro edition. This method minimizes administrative effort and simplifies the upgrade process. References: Windows subscription activation, Deploy Windows Enterprise licenses

NEW QUESTION 242

- (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 243

- (Exam Topic 4)

You use Windows Admin Center to remotely administer computers that run Windows 10. When connecting to Windows Admin Center, you receive the message shown in the following exhibit.



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

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

Answer: B

NEW QUESTION 244

- (Exam Topic 4)

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

- Requires BitLocker Drive Encryption (BitLocker) on each device
- Requires a minimum operating system version

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered



**Answer:** A

**Explanation:**

**Settings**  

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

**Answer Area**  

Requires BitLocker: System Security

Requires a minimum operating system version: Device Properties

**NEW QUESTION 245**

- (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 246**

- (Exam Topic 4)  
 You have 200 computers that run Windows 10 and are joined to an Active Directory domain.  
 You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy. Which three actions should you perform? Each correct answer presents part of the solution.  
 NOTE: Each correct selection is worth one point.

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

**Answer:** BCF

**Explanation:**

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

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

**NEW QUESTION 249**

- (Exam Topic 4)  
 Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User1 uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1. You need to identify what will occur when User1 next signs in to the devices.  
 What should you identify for each device? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Device1:

Will activate as Windows 11 Enterprise

Will activate as Windows 11 Enterprise

Will not upgrade to Windows 11 Enterprise

Will perform a clean installation of Windows 11 Enterprise

Will perform an in-place upgrade to Windows 11 Enterprise

Device2:

Will not upgrade to Windows 11 Enterprise

Will activate as Windows 11 Enterprise

Will not upgrade to Windows 11 Enterprise

Will perform a clean installation of Windows 11 Enterprise

Will perform an in-place upgrade to Windows 11 Enterprise

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1:

- > Will activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windo 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 1 has Windows 11 Pro, so it meets the requirement. When User1 signs in to Device 1 with their Azure AD account, the device will automatically activate as Windows 11 Enterprise without changing the edition.
- > Will not activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 2 has Windows 10 Home, so it does not meet the requirement. When User1 signs in to Device 2 with their Azure AD account, the device will not activate as Windows 11 Enterprise by subscription.

NEW QUESTION 251

- (Exam Topic 4)  
You have a Microsoft 365 subscription.  
You use Microsoft Intune Suite to manage devices.  
You have the iOS app protection policy shown in the following exhibit.

Access requirements

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

Conditional launch

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

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

Answer Area

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

PIN only

account credentials only

PIN only

PIN and account credentials

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

block access

block access

reset the app PIN

reset the device PIN

wipe company data

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 254

- (Exam Topic 4)  
You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments. From Deployment Workbench, you modify the WinPE settings and add PowerShell support. You need to generate a new set of WinPE boot image files that contain the updated settings. What should you do?

- A. From the Deployment Shares node, update the deployment share.
- B. From the Advanced Configuration node, create new media.
- C. From the Packages node, import a new operating system package
- D. From the Operating Systems node, import a new operating system.

Answer: A

**NEW QUESTION 259**

- (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

^

v

- 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 263**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune. You have five new Windows 11 Pro devices. You need to prepare the devices for corporate use. The solution must meet the following requirements:

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

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

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

Answer: BDE

**NEW QUESTION 265**

- (Exam Topic 4)

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

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

Which devices can be Azure AD joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Azure AD joined:

Device1 and Device2 only

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2, and Device3 only

Device1, Device2, Device3, and Device4

Registered in contoso.com:

Device1 and Device2 only

Device1 and Device2 only

Device2 and Device3 only

Device3 and Device4 only

Device2, Device3, and Device4 only

Device1, Device2, Device3, and Device4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

Azure AD joined:

Device1 and Device2 only

Device1 only

Device1 and Device2 only

Device1 and Device3 only

Device1, Device2, and Device3 only

Device1, Device2, Device3, and Device4

Registered in contoso.com:

Device1 and Device2 only

Device1 and Device2 only

Device2 and Device3 only

Device3 and Device4 only

Device2, Device3, and Device4 only

Device1, Device2, Device3, and Device4

NEW QUESTION 267

- (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 268

- (Exam Topic 4)  
You have 100 computers that run Windows 10.  
You plan to deploy Windows 11 to the computers by performing a wipe and load installation. You need to recommend a method to retain the user settings and the user data.  
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Configure known folder redirection in Microsoft OneDrive.

Run scanstate.exe.

Run loadstate.exe.

Enable Enterprise State Roaming.

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

>

<

Answer Area

↑

↓

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Actions

Configure known folder redirection in Microsoft OneDrive.

Run scanstate.exe.

Run loadstate.exe.

Enable Enterprise State Roaming.

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

>

<

Answer Area

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

↑

↓

NEW QUESTION 270

- (Exam Topic 4)  
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:  
• For the WinRM service, set Startup type to Automatic.  
• Create a listener that accepts requests from any IP address.  
• Enable a firewall exception for WS-Management communications. Which PowerShell cmdlet should you use?

- A. Connect-WSMan  
B. Enable-PSRemoting

- C. Invoke-WSManAction
- D. Enable-PSSessionConfiguration

**Answer:** B

**NEW QUESTION 274**

- (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 276**

- (Exam Topic 4)

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

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

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

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

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

The next day, you review the compliance status of the computers. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

The compliance status of Computer1 is In grace period.

☐

☐

The compliance status of Computer2 is Compliant.

☐

☐

The compliance status of Computer3 is Not compliant.

☐

☐

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Statements

Yes

No

The compliance status of Computer1 is In grace period.

☒

☐

The compliance status of Computer2 is Compliant.

☐

☒

The compliance status of Computer3 is Not compliant.

☐

☒

**NEW QUESTION 279**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You have the devices shown in the following table.



Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

- A. Device3 only
- B. Device2 and Device3 only
- C. Device 1 and Device2 only
- D. Device1, Device2, and Device3

**Answer:** A

#### NEW QUESTION 283

- (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 284

- (Exam Topic 4)

You use Microsoft Endpoint Manager to manage Windows 10 devices.

You are designing a reporting solution that will provide reports on the following:

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

You need to recommend a data source and a data visualization tool for the design.

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

### Answer Area

Data source:

Audit logs in Azure Active Directory (Azure AD)
Audit logs in Microsoft Intune
Azure Synapse Analytics
The Microsoft Intune Data Warehouse

Data visualization tool:

Azure Data Studio
Microsoft Power BI
The Azure portal

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

A screenshot of a computer Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports> <https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi>

#### NEW QUESTION 288

- (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 290

- (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 291

- (Exam Topic 4)

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

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

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

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 293

.....

## 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](#)**