

# Microsoft

## Exam Questions MD-102

Endpoint Administrator



### NEW QUESTION 1

- (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 2

- (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 3

- (Exam Topic 4)

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. On Computer1, you need to run the

Invoke-Command cmdlet to execute several PowerShell commands on Computer2. What should you do first?

- A. On Computer2, run the Enable-PSRemoting cmdlet.
- B. On Computer2, add Computer1 to the Remote Management Users group.
- C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computer2.
- D. On Computer1, run the HcK-PSSession cmdlet.

**Answer:** C

### NEW QUESTION 4

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.

What should you configure?

- A. Windows Autopilot
- B. provisioning packages for Windows
- C. Security defaults in Azure AD

D. Device settings in Azure AD

Answer: D

Explanation:

To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users. By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected1.

The other options are not relevant for this scenario because:

- > Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune. It does not control the local administrator role of the users who join the devices2.
- > Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users3.
- > Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role4.

References: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security defaults?

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

A device restriction policy

A security baseline

An attack surface reduction (ASR) rule

An Intune connection

Answer Area

Enforces compliance:

Prevents suspicious scripts:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in Defender for Endpoint. You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/conditional-access>

To prevent suspicious scripts from running on devices, you need to configure an attack surface reduction (ASR) rule in Intune. ASR rules are part of the endpoint protection settings that you can apply to devices by using device configuration profiles. You can use the ASR rule “Block Office applications from creating child processes” to prevent Office applications from launching child processes such as scripts or executables. References:

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

NEW QUESTION 6

- (Exam Topic 4)

You have 100 Windows 10 devices enrolled in Microsoft Intune.

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Delivery Optimization setting:

Intune object:

Bandwidth optimization type

Bandwidth optimization type

Download mode

VPN peer caching

A configuration profile

A configuration profile

App configuration policies

Windows 10 and later quality updates

Windows 10 and later update rings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 7

- (Exam Topic 4)  
You have an on-premises Active Directory domain that syncs to Azure AD tenant.  
The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune. The Microsoft Office settings on the computers are configured by using an Group Policy Object (GPO).  
You need to migrate the GPO to Intune.  
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Assign the policy.

Create a compliance policy.

Set a scope tag to the policy.

Import an ADMX file.

Create a configuration profile.

Configure the Administrative Templates settings.

Assign the profile.

Answer Area

>

<

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Assign the policy.

Create a compliance policy.

Set a scope tag to the policy.

Import an ADMX file.

Create a configuration profile.

Configure the Administrative Templates settings.

Assign the profile.

Answer Area

>

<

Create a configuration profile.

Configure the Administrative Templates settings.

Assign the profile.

NEW QUESTION 8

- (Exam Topic 4)  
You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).  
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.  
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



## Actions

## Answer Area

Obtain the root certificate.

From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.

From the Enterprise CA, configure certificate managers.

From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.

From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.



- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure>

### NEW QUESTION 9

- (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: [Use policy CSP settings to create custom device configuration profiles]

### NEW QUESTION 10

- (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. .ipa
- 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)

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

- A. Assignments
- B. Settings
- C. Scope (Tags)

D. Applicability Rules

**Answer:** D

**Explanation:**

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

**NEW QUESTION 15**

- (Exam Topic 4)

You have a Microsoft 365 subscription. All devices run Windows 10.

You need to prevent users from enrolling the devices in the Windows Insider Program.

What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

- A. a device restrictions device configuration profile
- B. an app configuration policy
- C. a Windows 10 and later security baseline
- D. a custom device configuration profile
- E. a Windows 10 and later update ring

**Answer:** AE

**NEW QUESTION 19**

- (Exam Topic 4)

Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Name	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
5	Group5	Name starts with COMP
Last	Ungrouped machines (default)	Not applicable

You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.



What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Computer1 will be a member of:

▼

Group3 only

Group4 only

Grou5 only

Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

▼

Group1 only

Group2 only

Group1 and Group2 only

Group1, Group2, Group3, Group4, and Group5

- A. Mastered
- B. Not Mastered

**Answer:** A

Explanation:

Answer Area

Computer1 will be a member of:

▼

Group3 only

Group4 only

Grou5 only

Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

▼

Group1 only

Group2 only

Group1 and Group2 only

Group1, Group2, Group3, Group4, and Group5

NEW QUESTION 21

- (Exam Topic 4)

You have a Microsoft 365 ES subscription that uses Microsoft Intune. Devices are enrolled in Intune as shown in the following table.

Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

The devices are the members of groups as shown in the following table.

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

You create an JOS/iPadOS update profile as shown in the following exhibit.

Create profile

...

iOS/iPadOS

✓ Basics

✓ Update policy settings

✓ Assignments

⚙ Review + create

Summary

Basics

NameProfile1

Description--

Update policy settings

Update to installInstall iOS/iPadOS Latest update

Schedule typeUpdate outside of scheduled time

Time zoneUTC±00

Time window

Start day

Start time

End day

End time

Monday

1 AM

Wednesday

1 PM

Friday

1 AM

Saturday

11 PM

Assignments

Included groups

Group

Group Members ⓘ

Group1

3 devices, 0 users

Excluded groups

Group

Group Members ⓘ

Group2

1 devices, 0 users

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 an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 22

- (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 27

- (Exam Topic 4)

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

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

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

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

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



# Create profile

Windows PC

✓ Basics

✓ Out-of-box experience (OOBE)

✓ Assignments

4 Review

## Summary

### Basics

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

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

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

### Language (Region)

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

### Automatically configure keyboard

No
----

### Microsoft Software License Terms

Hide
------

### Privacy settings

Hide
------

### Hide change account options

Hide
------

### User account type

Standard
----------

### Allow pre-provisioned deployment

No
----

### Apply device name template

No
----

### Assignments

Included groups	Group1
Excluded groups	Group2

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

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

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

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

## Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

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

### NEW QUESTION 31

- (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 32

- (Exam Topic 4)

You are creating a device configuration profile in Microsoft Intune. You need to configure specific OMA-URI settings in the profile. Which profile type template should you use?

- A. Device restrictions (Windows 10 Team)
- B. Identity protection
- C. Custom
- D. Device restrictions

**Answer:** C

### NEW QUESTION 34

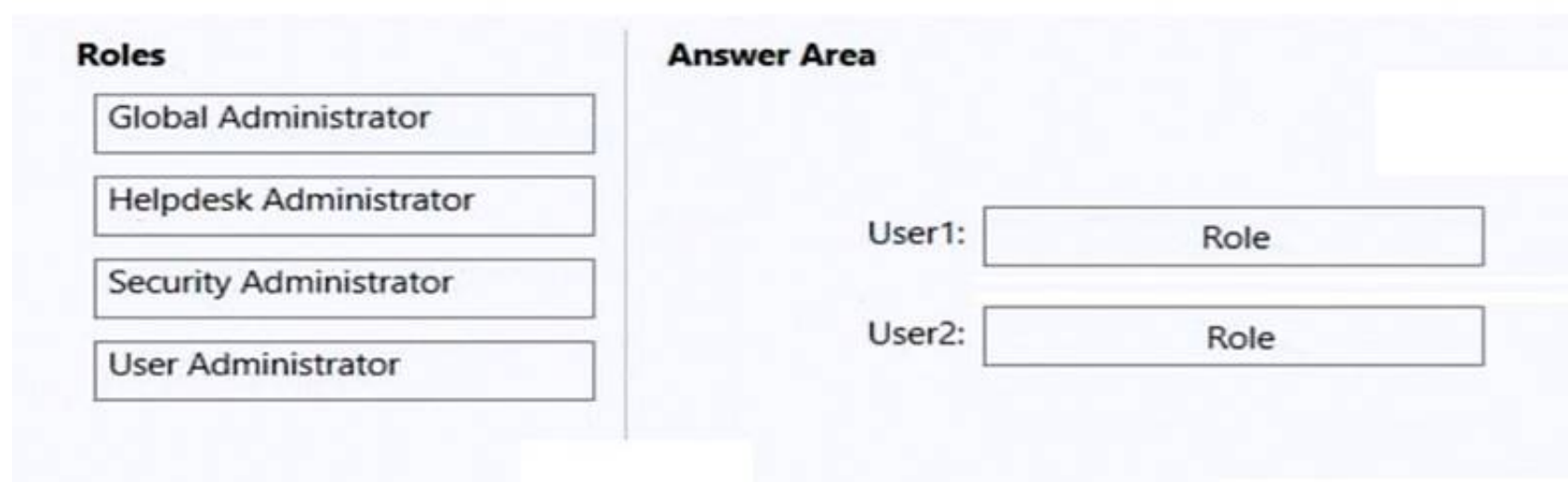
- (Exam Topic 4)

You have a Microsoft 365 subscription that contains two users named User1 and User2. You need to ensure that the users can perform the following tasks:

- User1 must be able to create groups and manage users.
- User2 must be able to reset passwords for non-administrative users. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the Microsoft 365 admin center. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers.

To ensure that User1 can create groups and manage users, you should assign the User Administrator role to User1. This role allows User1 to create and manage all aspects of users and groups, including resetting passwords for non-administrative users.

To ensure that User2 can reset passwords for non-administrative users, you should assign the Helpdesk Administrator role to User2. This role allows User2 to reset passwords, manage service requests, and monitor service health for non-administrative users.

### NEW QUESTION 39

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to configure an Intune device configuration profile to meet the following requirements:

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

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

NOTE: Each correct selection is worth one point.



Answer Area

Create Profile

**\*Name**

MD101

**Description**

Enter a description

**\*Platform**

Windows 10 and later

**\*Profile type**

Endpoint protection

Settings

Configure

Scope (Tags)

0 scope(s) selected

Endpoint protection

Windows 10 and later

Select a category to configure settings

Windows Defender Application Gu...  
11 settings available

Windows Defender Firewall  
40 settings available

Windows Defender SmartScreen  
2 settings available

Windows Encryption  
37 settings available

Windows Defender Exploit Guard  
20 settings available

Windows Defender Application Co...  
2 settings available

Windows Defender Application Gua...  
1 setting available

Windows Defender Security Center  
14 settings available

Local device security options  
46 settings available

Xbox services  
5 settings available

OK

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

References:

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

NEW QUESTION 43

- (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 47

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 11 deployment tasks.

MDT contains the operating system images shown in the following table.

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Task sequence template:

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

Operating system image:

Image1.wim  
Image2.wim  
Install.wim

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Box 1: Standard Client Upgrade Task Sequence  
Use Template: Standard Client Upgrade Task Sequence  
In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not plan to significantly change the device's configuration or applications. MDT includes an in-place upgrade task sequence template that makes the process really simple.  
Box 2: Install.wim  
In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. I  
Reference:  
<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the>

**NEW QUESTION 49**  
- (Exam Topic 4)  
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system build can access network resources.  
Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.  
NOTE: Each correct selection is worth one point.

Settings

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

Answer Area

Device1:  
Device2:  
Device3:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings

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

Answer Area

Device1: Require BitLocker.  
Device2: Prevent jailbroken devices from having corporate access.  
Device3: Prevent rooted devices from having corporate access.



#### NEW QUESTION 51

- (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 56

- (Exam Topic 4)

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

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

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

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

**Answer: B**

#### NEW QUESTION 61

- (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 63

- (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.

New

Conditions

Device state (preview)

Info

Name

PolicyA

Assignments

Users and groups

0 users and groups selected

Cloud apps

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Info

Configure

Yes

No

Include

Exclude

Select the device state condition used to exclude devices from policy.

☐ Device Hybrid Azure AD joined

☐ Device marked as compliant

- 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/active-directory/conditional-access/conditions](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 66**

- (Exam Topic 3)

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

**Policy1:**

Device1 only

Device2 only

Device3 only

Device4 only

Device2 and Device3 only

Device1 and Device3 only

Device1, Device2, and Device 3

**Policy2:**

Device1 only

Device2 only

Device3 only

Device4 only

Device2 and Device3 only

Device1 and Device3 only

Device1, Device2, and Device 3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

NEW QUESTION 68

- (Exam Topic 3)

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

User1 can enroll a maximum of:

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

User2 can enroll a maximum of:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:

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

User2 can enroll a maximum of:

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

NEW QUESTION 72

- (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 77

- (Exam Topic 2)

You need to meet the OOBЕ 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.

**Overview**

Getting started

**Manage**

Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:  
<https://blogs.msdn.microsoft.com/sgern/2018/10/11/intune-intune-and-autopilot-part-3-preparing-your-environm>  
<https://blogs.msdn.microsoft.com/sgern/2018/11/27/intune-intune-and-autopilot-part-4-enroll-your-first-device/>

**NEW QUESTION 79**

- (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 82**

- (Exam Topic 2)  
You need to resolve the performance issues in the Los Angeles office.  
How should you configure the update settings? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Change Delivery Optimization download mode to:

Bypass mode

HTTP blended with internet peering

HTTP blended with peering behind same NAT

Simple download mode with no peering

Update Active Hours Start to:

10 AM

11 AM

10 PM

11 PM

Update Active Hours End to:

10 AM

11 AM

10 PM

11 PM

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated with low confidence  
Reference:  
<https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization> <https://2pintsoftware.com/delivery-optimization-dl-mode/>

NEW QUESTION 86

- (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 91

- (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 94**

- (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 98**

- (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 102**

- (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 106**

- (Exam Topic 4)

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

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

**Answer:** C

**Explanation:**

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

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

Prevent users from updating the OS manually

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

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

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

Delay default visibility of software updates = 1 to 90 90 days is the maximum delay that Apple supports.  
 Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/software-updates-ios>

#### NEW QUESTION 109

- (Exam Topic 4)

You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs. The computers have the logged events shown in the following table.

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

Which events are collected in the Log Analytics workspace?

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

**Answer: E**

#### Explanation:

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

#### NEW QUESTION 113

- (Exam Topic 4)

You have an Azure AD tenant that contains the devices shown in the following table. You purchase Windows 11 Enterprise E5 licenses. Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

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

**Answer: B**

#### NEW QUESTION 118

- (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 access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. 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 protocols13. 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 123

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune.

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

- A. Privacy URL

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

**Answer:** AC

**NEW QUESTION 126**

- (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 127**

- (Exam Topic 4)

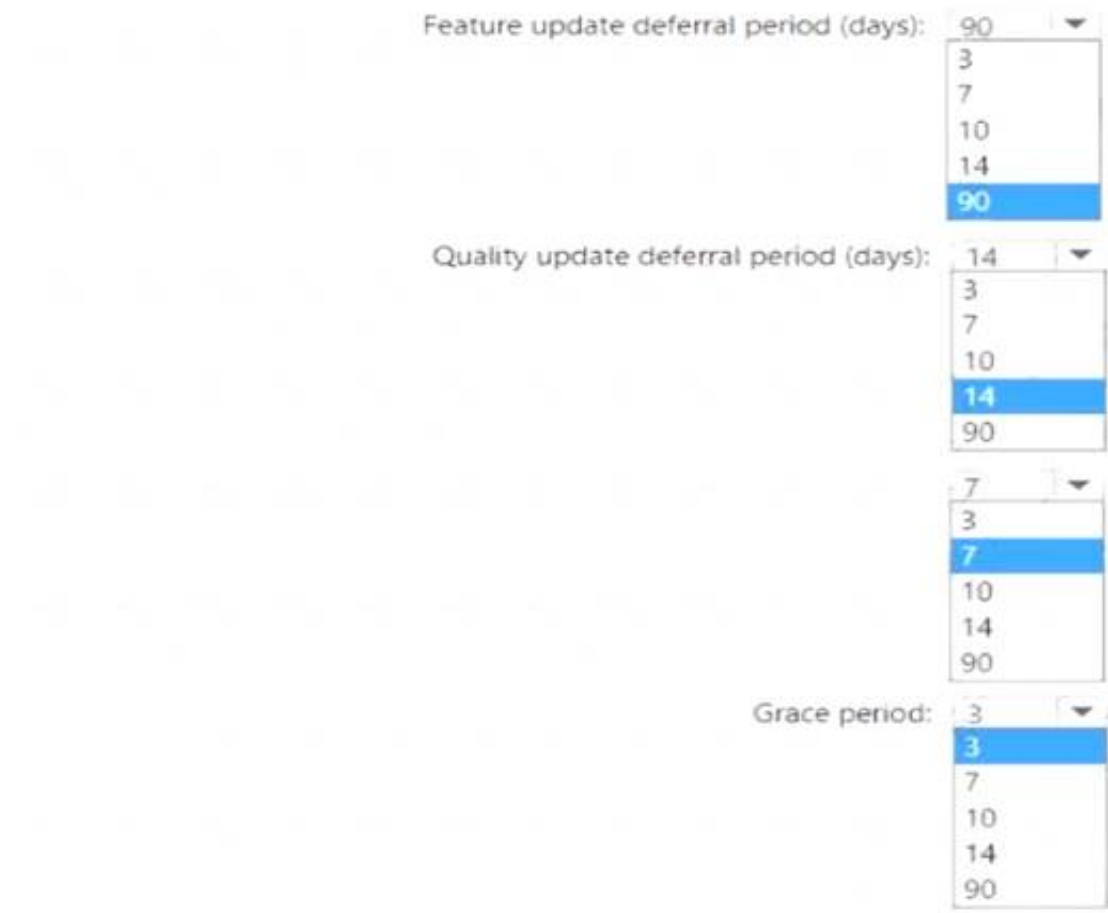
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

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

Quality update deferral period (days): 14

Grace period: 7

Grace period: 3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



Answer Area

Feature update deferral period (days):  

3  
7  
10  
14  
90

Quality update deferral period (days):  

3  
7  
10  
14  
90

7  
3  
10  
14  
90

Grace period:  

3  
7  
10  
14  
90

NEW QUESTION 129

- (Exam Topic 4)  
You have a Microsoft 365 tenant and an internal certification authority (CA).  
You need to use Microsoft Intune to deploy the root CA certificate to managed devices.  
Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Policy type:  

App configuration policy  
App protection policy  
Compliance policy  
Configuration profile

Profile:  

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Box 1: Configuration profile Create a trusted certificate profile. Box 2: Trusted certificate  
When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.  
Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root>

NEW QUESTION 134

- (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 139**

- (Exam Topic 4)  
 You are replacing 100 company-owned Windows devices.  
 You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices. The solution must meet the following requirements:

- Back up the user state.
- Minimize administrative effort.

Which task sequence template should you use?

- A. Standard Client Task Sequence
- B. Standard Client Replace Task Sequence
- C. Litetouch OEM Task Sequence
- D. Sysprep and Capture

**Answer:** B

**NEW QUESTION 140**

- (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 141

- (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 143

- (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 145

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

Name	Memory	TPM
Device1	16 GB	None
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

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

**Answer:** C

#### Explanation:

Windows Autopilot self-deploying mode requires devices that have a firmware-embedded activation key for Windows 10 Pro or Windows 11 Pro. This feature allows devices to automatically activate Windows Enterprise edition using the subscription license assigned to the user. Device1 does not have a firmware-embedded activation key, so it cannot use self-deploying mode. Device2 and Device3 have firmware-embedded activation keys for Windows 10 Pro, so they can use self-deploying mode. References: Windows Autopilot self-deploying mode (Public Preview), Deploy Windows Enterprise licenses

#### NEW QUESTION 149

- (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 150

- (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 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 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 155

- (Exam Topic 4)

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

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

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

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

Answer: CE

#### Explanation:

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

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

#### NEW QUESTION 156

- (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 ⓘ	<b>Allow</b> Skip
Option to pause Windows updates ⓘ	<b>Enable</b> Disable
Option to check for Windows updates ⓘ	<b>Enable</b> Disable
Change notification update level ⓘ	Use the default Windows Update notifications ▼
Use deadline settings ⓘ	<b>Allow</b> Not configured
Deadline for feature updates ⓘ	5 ✓
Deadline for quality updates ⓘ	2 ✓
Grace period ⓘ	1 ✓
Auto reboot before deadline ⓘ	<b>Yes</b> No

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

NOTE: Each correct selection is worth one point.

#### Answer Area

Automatic restarts are blocked [answer choice]. between 8 AM and 5 PM ▼

A restart will be forced on a device [answer choice] after the deadline. 1 day ▼

- 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 161**

- (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 166**

- (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

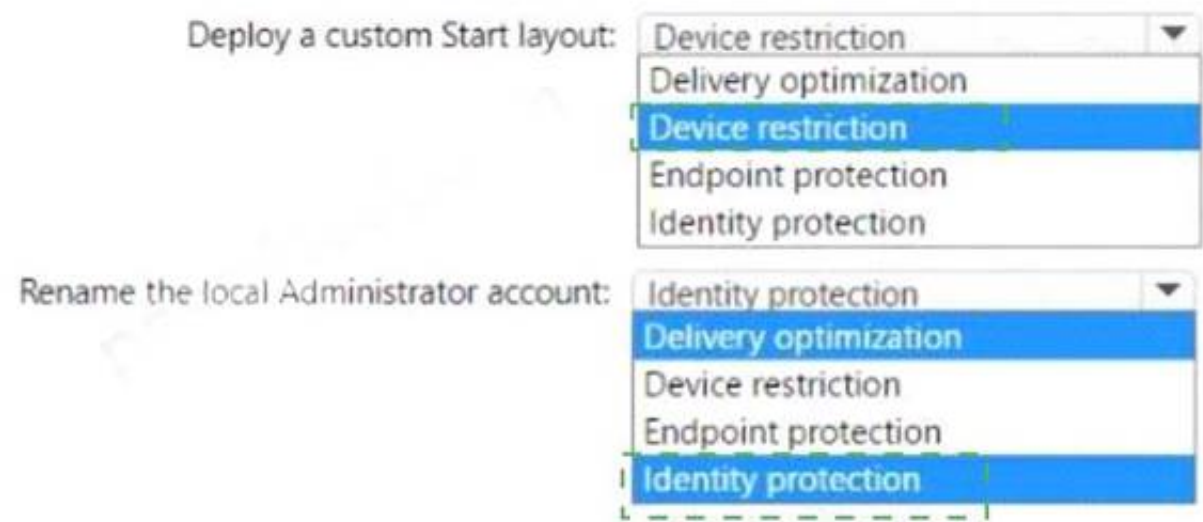
- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



Answer Area



NEW QUESTION 171

- (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 175

- (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

1

 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 177

- (Exam Topic 4)

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

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

NOTE: Each correct selection is worth one point.

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

**Answer:** ACE

#### Explanation:

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

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-overview>

#### NEW QUESTION 181

- (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 186

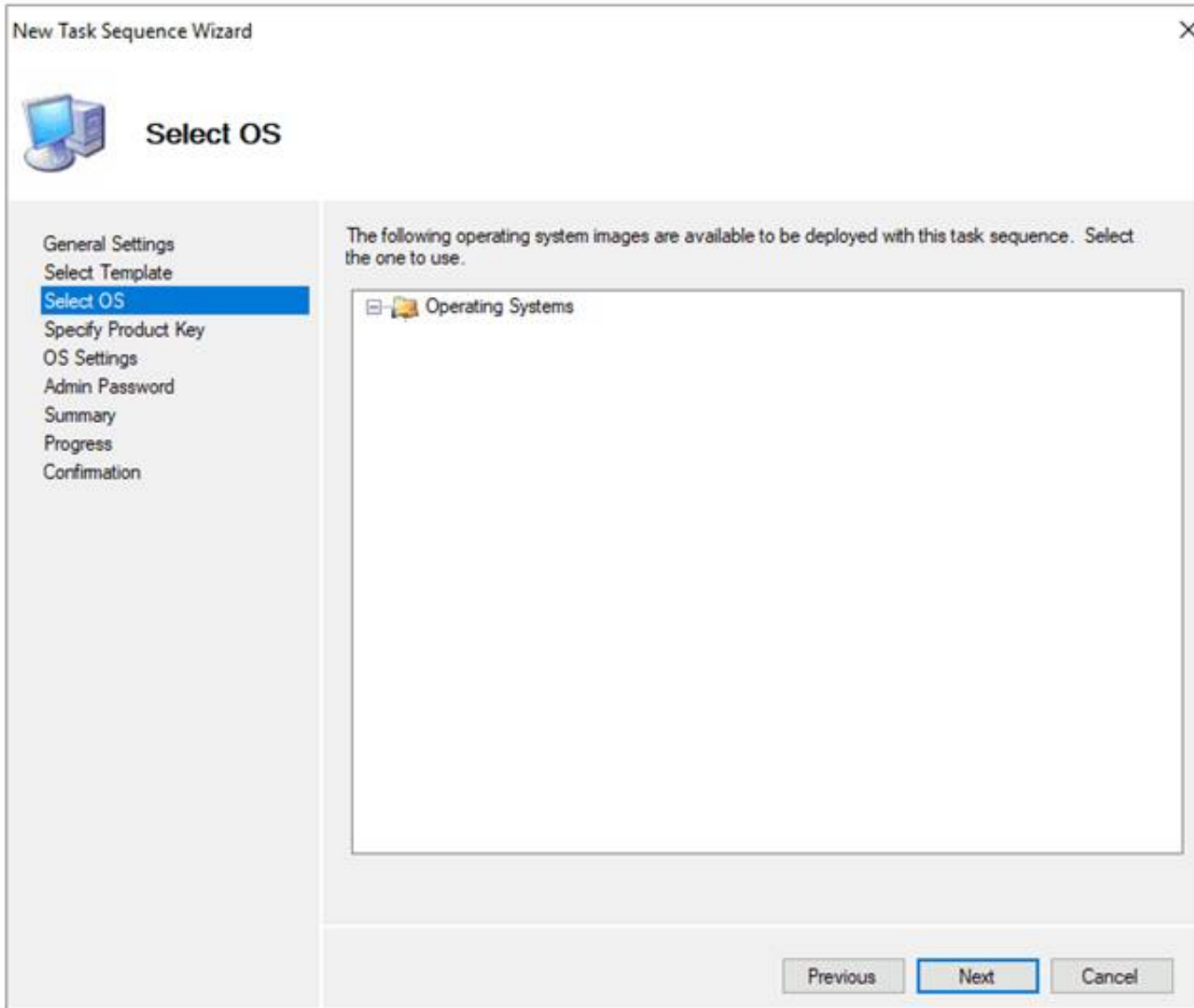
- (Exam Topic 4)

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

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

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





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

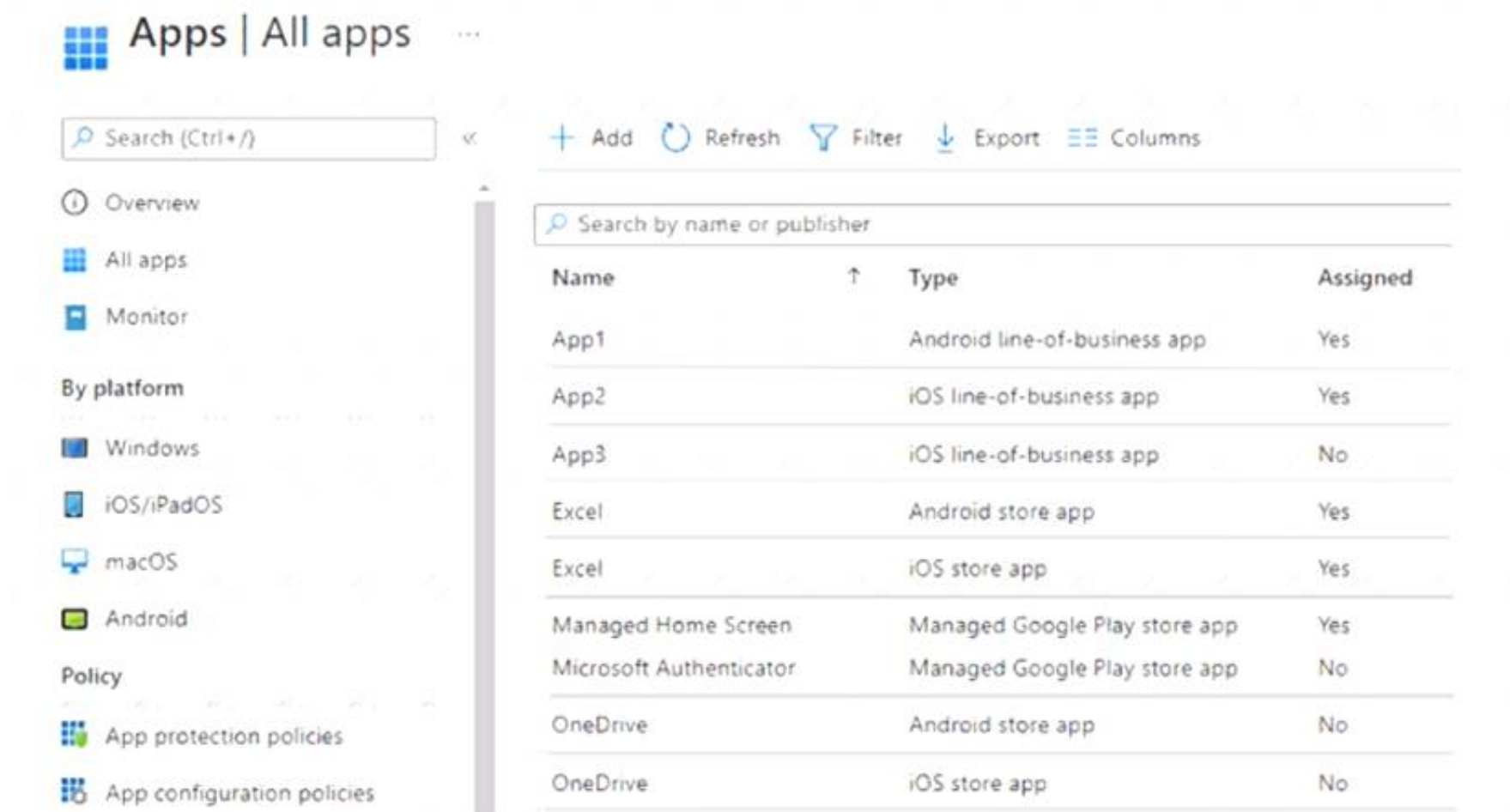
- A. Enable monitoring for the deployment share.
- B. Import a full set of source files.
- C. Import a custom image file.
- D. Run the Update Deployment Share Wizard

**Answer:** D

#### NEW QUESTION 187

- (Exam Topic 4)

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



The screenshot shows the Microsoft Intune 'Apps | All apps' page. The page has a header with the title 'Apps | All apps' and a search bar. Below the header, there is a navigation pane on the left with the following options: Overview, All apps (selected), Monitor, and a 'By platform' section with Windows, iOS/iPadOS, macOS, and Android. Below the 'By platform' section, there is a 'Policy' section with App protection policies and App configuration policies. The main area of the page shows a table of installed apps. The table has three columns: Name, Type, and Assigned. The table contains the following data:

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

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

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

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

1

2

3

4

5

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

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

1

2

3

4

5

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

1

2

3

4

5

NEW QUESTION 188

- (Exam Topic 4)  
You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

In the Microsoft Intune admin center, you are creating a Microsoft 365 Apps app named App1. To which objects can you assign App1?

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

Answer: C

Explanation:

In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using device groups. In this scenario, the objects shown in the table are as follows:

- > Admin1 is an individual user account that belongs to the Global administrators
- > Group1 is a user group that contains 100 users.
- > Group2 is a device group that contains 50 devices.
- > Group3 is a user group that contains 200 users.
- > Group4 is a device group that contains 150 devices.

role group.  
Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment. Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

NEW QUESTION 189

- (Exam Topic 4)  
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.  
You use Microsoft Intune to manage devices. All devices are in the same time zone. You create an update rings policy and assign the policy to all Windows devices.  
On the November 1, you pause the update rings policy. All devices remain online.

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

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

Answer: C

NEW QUESTION 192

- (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

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker:

Requires a minimum operating system version:

- 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 196

- (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 197**

- (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 199**

- (Exam Topic 4)

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

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

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

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

➤ MDM user scope: Group1

➤ MAM user scope: Group2

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

NOTE: Each correct selection is worth one point.

**Answer Area**

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

A. Mastered

B. Not Mastered

Answer: A

**Explanation:**

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

**NEW QUESTION 201**

- (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 202**

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 500 Android Enterprise devices. All the devices are enrolled in Microsoft Intune.

You need to deliver bookmarks to the Chrome browser on the devices What should you create?

A. a compliance policy

B. a configuration profile

C. an app protection policy

D. an app configuration policy

Answer: D

NEW QUESTION 205

- (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

&u2191

&u2193

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Configure known folder redirection in Microsoft OneDrive.

Run scanstate.exe.

Run loadstate.exe.

Enable Enterprise State Roaming.

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

>

<

Answer Area

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

&u2191

&u2193

NEW QUESTION 207

- (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 208

- (Exam Topic 4)

You have a Microsoft 365 subscription.

All computers are enrolled in Microsoft Intune.

You have business requirements for securing your Windows 11 environment as shown in the following table.

Requirement	Detail
Requirement1	Ensure that Microsoft Exchange Online can be accessed from known locations only.
Requirement2	Lock a device that has a high Microsoft Defender for Endpoint risk score.

What should you implement to meet each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Requirement1:

A conditional access policy

A conditional access policy

A device compliance policy

A device configuration profile

Requirement2:

A device compliance policy

A conditional access policy

A device compliance policy

A device configuration profile

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Requirement1:

A conditional access policy

A conditional access policy

A device compliance policy

A device configuration profile

Requirement2:

A device compliance policy

A conditional access policy

A device compliance policy

A device configuration profile

NEW QUESTION 209

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

Kiosk

Windows 10 and later

✓ Basics

**2 Configuration settings**

③ Assignments

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

Select a kiosk mode \*

Single app, full-screen kiosk

User login type \*

Auto login (Windows 10, version 1803+)

Application type \*

Add Microsoft Edge browser

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. [Learn more about Microsoft Edge kiosk mode.](#)

Edge Kiosk URL \*

https://contoso.com

Microsoft Edge kiosk mode type

Public Browsing (InPrivate)

Refresh browser after idle time

5

Specify Maintenance Window for App Restarts \*

Require

**Not configured**

Maintenance Window Start Time

MM/DD/YYYY h:mm:ss A

Maintenance Window Recurrence

Daily (recommended)

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

Answer Area

Users

can access any URL.

cannot view the address bar in Microsoft Edge.

can only access URLs that include contoso.com.

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

Windows 10 devices can have

a single Microsoft Edge instance that has a single tab.

a single Microsoft Edge instance that has multiple tabs.

multiple Microsoft Edge instances that have multiple tabs.

multiple Microsoft Edge instances that each has a single tab.

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Users can only access URLs that start with https://contoso.com/ Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab  
he device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:  
➤ Kiosk mode: Enabled

- > Kiosk type: Multi-app
- > Allowed URLs: <https://contoso.com/>\*
- > Address bar: Disabled

These settings mean that users can only access URLs that start with <https://contoso.com/> and cannot view the address bar in Microsoft Edge. The kiosk type of Multi-app allows users to open multiple instances of Microsoft Edge, but each instance can only have a single tab. Therefore, users cannot access any URL, cannot view the address bar in Microsoft Edge, and can have multiple Microsoft Edge instances that each has a single tab. References: <https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings#kiosk-browser-settings>

**NEW QUESTION 213**

- (Exam Topic 4)

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

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

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

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

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

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

**NEW QUESTION 217**

- (Exam Topic 4)

You have 25 computers that run Windows 10 Pro.  
 You have a Microsoft 365 E5 subscription that uses Microsoft Intune.  
 You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.  
 What should you use?

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

**Answer:** C



NEW QUESTION 218

- (Exam Topic 4)

You have SOO Windows 10 devices enrolled in Microsoft Intune.

You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

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

You need to configure a Windows 10 device that will be used to create a template file.

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

NOTE: Each correct selection is worth one point.

Protection areas

Account protection

App & browser control

Device security

Virus & threat protection

Answer Area

DEP:

Mandatory ASLR:

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

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

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

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

NEW QUESTION 223

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains 1.000 computers that run Windows 11.

You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:

- Prevent the sharing of clipboard contents.
- Ensure that users authenticate by using Network Level Authentication (NLA).

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

Remote Desktop Session Host

Connections

Device and Resource Redirection

Licensing

Printer Redirection

Profiles

RD Connection Broker

Remote Session Environment ✓

Security ✓

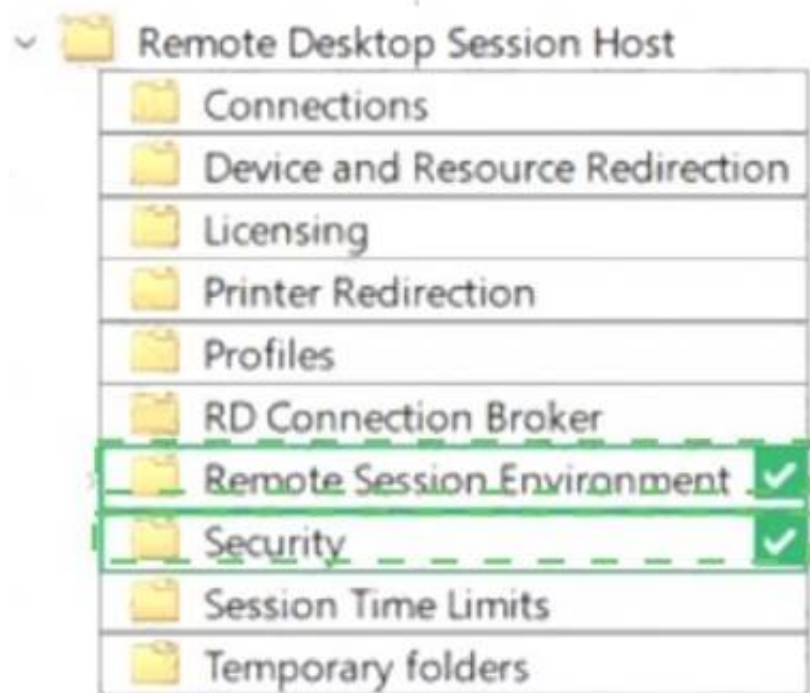
Session Time Limits

Temporary folders

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 225

- (Exam Topic 4)

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

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

Which groups can you add to Group4?

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

Answer: C

NEW QUESTION 227

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You plan to create Windows 11 device builds for the marketing and research departments The solution must meet the following requirements:

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

NOTE: Each correct selection is worth one point

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

Marketing:

Research:

## NEW QUESTION 232

.....



## 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](#)**