



# Microsoft

## Exam Questions MD-102

Endpoint Administrator

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 have a Microsoft Azure subscription that contains an Azure Log Analytics workspace. You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup. You need to ensure that you can use Log Analytics to query events from Computer1. What should you do on Computer1?

- A. Join Azure AD.
- B. Configure Windows Defender Firewall
- C. Create an event subscription.
- D. Install the Azure Monitor Agent.

Answer: D

NEW QUESTION 3

- (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

&u2191

&u2193

- 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.

&u2191

&u2193

NEW QUESTION 4

- (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

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.

Answer Area

⏪

⏩

⏴

⏵

- 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 5

- (Exam Topic 4)  
You have a computer named Computer1 that runs Windows 11.  
A user named User1 plans to use Remote Desktop to connect to Computer1.  
You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.  
What should you do on Computer1?

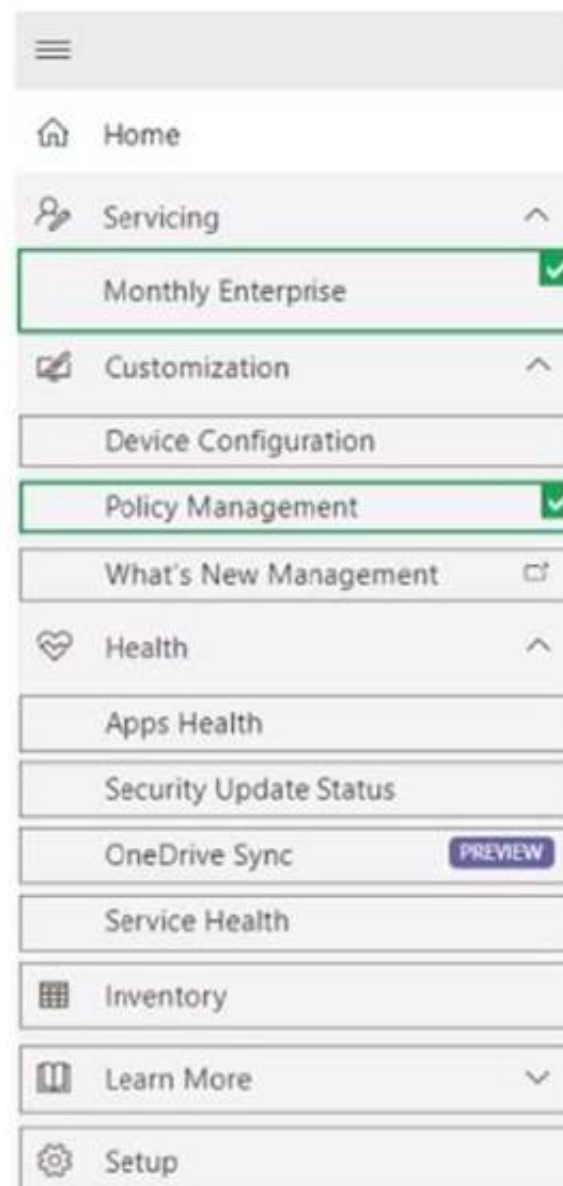
- A. Turn on Reputation-based protection.
- B. Enable Network Level Authentication (NLA).
- C. Turn on Network Discovery.
- D. Configure the Remote Desktop Configuration service.

Answer: B

NEW QUESTION 6

- (Exam Topic 4)  
You have a Microsoft 365 subscription.  
All users have Microsoft 365 apps deployed.  
You need to configure Microsoft 365 apps to meet the following requirements:  
• Enable the automatic installation of WebView2 Runtime.  
• Prevent users from submitting feedback.  
Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.  
NOTE: Each correct selection is worth one point.

## Answer Area

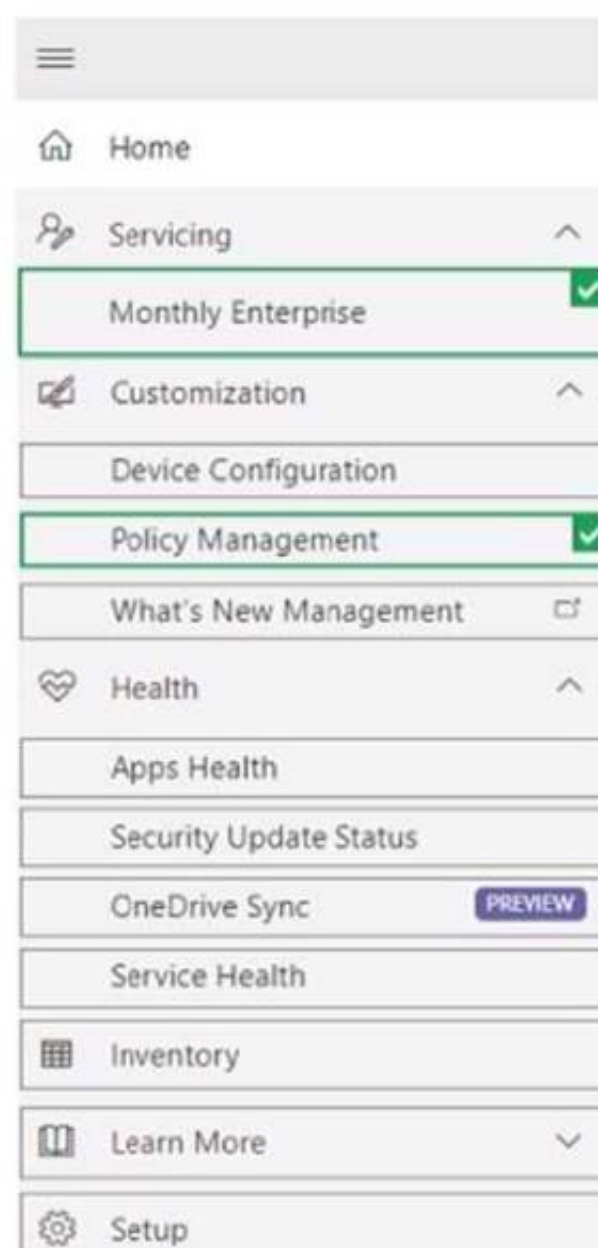


- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**





NEW QUESTION 7

- (Exam Topic 4)

You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

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

Answer: B

Explanation:

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

NEW QUESTION 8

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE\_x64.iso image and connect to MDT1. the welcome screen appears as shown In the following exhibit.



You need to prevent the welcome screen from appearing when the computers connect to MDT1.

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

- Modify the CustomSettings.ini file.
- Update the deployment share.
- Modify the Bootstrap.ini file.
- Replace the ISO image.
- Modify the task sequence.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Modify the Bootstrap.ini file.

Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:

SkipBDDWelcome=YES

Box 2: Modify the CustomSettings.ini file. SkipBDDWelcome

Indicates whether the Welcome to Windows Deployment wizard page is skipped.

For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.

Box 3: Update the deployment share. Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages>

NEW QUESTION 9

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

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

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

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

**Answer:** A

**Explanation:**

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

Reference:

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

**NEW QUESTION 10**

- (Exam Topic 4)

You have a computer named Computer5 that has Windows 10 installed. You create a Windows PowerShell script named config.ps1.

You need to ensure that config.ps1 runs after feature updates are installed on Computer5. Which file should you modify on Computer5?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 10**

- (Exam Topic 4)

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

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

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

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

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



## Create profile

Windows PC

☒ Basics
 ☒ Out-of-box experience (OOBE)
 ☒ Assignments
 ☒ 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 11

- (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 13

- (Exam Topic 4)

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

You have a Microsoft 365 subscription

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

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

- Devices must be joined to AD DS regardless of their current working location.
- Users in the marketing department must have a line-of-business (LOB) app installed during the deployment. The solution must minimize administrative effort.

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

##### Answer Area

Devices must be joined to AD DS regardless of their current working location:	<div><div>Install the Intune connector for Active Directory.</div><div>Deploy Always On VPN.</div><div>Install the Intune connector for Active Directory.</div><div>Modify the Autopilot deployment profile.</div><div>Edit the Co-management settings in Intune.</div></div>
The marketing department users must have an LOB app installed during the deployment:	<div><div>Modify the Autopilot deployment profile.</div><div>Modify the Autopilot deployment profile.</div><div>Create a Microsoft Intune app deployment.</div><div>Create a device configuration profile in Intune.</div></div>

- A. Mastered
- B. Not Mastered

**Answer:** A

##### Explanation:

##### Answer Area

Devices must be joined to AD DS regardless of their current working location:	<div><div>Install the Intune connector for Active Directory.</div><div>Deploy Always On VPN.</div><div>Install the Intune connector for Active Directory.</div><div>Modify the Autopilot deployment profile.</div><div>Edit the Co-management settings in Intune.</div></div>
The marketing department users must have an LOB app installed during the deployment:	<div><div>Modify the Autopilot deployment profile.</div><div>Modify the Autopilot deployment profile.</div><div>Create a Microsoft Intune app deployment.</div><div>Create a device configuration profile in Intune.</div></div>

#### NEW QUESTION 18

- (Exam Topic 4)

You have a Microsoft Intune subscription.

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

### Create profile

Windows PC

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

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

\* Deployment mode ⓘ

User-Driven

\* Join to Azure AD as ⓘ

Azure AD joined

Microsoft Software License Terms ⓘ

Show Hide

Important information about hiding license terms

Privacy settings ⓘ

Show Hide

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

Hide change account options ⓘ

Show Hide

User account type ⓘ

Administrator Standard

Allow White Glove OOBE ⓘ

No Yes

Language (Region) ⓘ

Operating system default

Automatically configure keyboard ⓘ

No Yes

Apply device name template ⓘ

No Yes

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

## Answer Area

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

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

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

computer name  
 Cortana settings  
 keyboard layout

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

## Answer Area

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

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

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

computer name  
 Cortana settings  
 keyboard layout

NEW QUESTION 23

- (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 no 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.

Roles

Global Administrator

Helpdesk Administrator

Security Administrator

User Administrator

Answer Area

User1:

Role

User2:

Role

- 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 centers1.

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 users1.

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 monito service health for non-administrative users1.

NEW QUESTION 27

- (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 builds 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:

Setting

Device2:

Setting

Device3:

Setting

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Box 1:

Device Compliance settings for Windows 10/11 in Intune

There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.

Note: Windows Health Attestation Service evaluation rules Require BitLocker:

Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help



protect the Windows operating system and user data. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.

Box 2: Prevent jailbroken devices from having corporate access Device Compliance settings for iOS/iPadOS in Intune

There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.

Device Health Jailbroken devices

Supported for iOS 8.0 and later

Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted (jailbroken) devices as not compliant.

Box 3: Prevent rooted devices from having corporate access. Device compliance settings for Android Enterprise in Intune

There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.

Device Health - for Personally-Owned Work Profile Rooted devices

Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted devices as not compliant.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios>

#### NEW QUESTION 29

- (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 32

- (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 33**

- (Exam Topic 4)

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in Intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

- A. From Platform Settings, set Android device administrator Personally Owned to Block.
- B. From Platform Settings, set Android Enterprise (work profile) to Allow.
- C. From Platform Settings, set Android device administrator Personally Owned to Allow
- D. From Platform Settings, set Android device administrator to Block.

**Answer:** AB

**Explanation:**

To ensure that only Android devices that use Android work profiles can enroll in Intune, you need to perform two configurations in the device enrollment restrictions. First, you need to set Android device administrator Personally Owned to Block. This prevents users from enrolling personal Android devices that use device administrator mode. Second, you need to set Android Enterprise (work profile) to Allow. This allows users to enroll corporate-owned or personal Android devices that use work profiles. References: <https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set>

**NEW QUESTION 34**

- (Exam Topic 4)

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

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

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

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

**Answer:** B

**NEW QUESTION 37**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 42**

- (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 46

- (Exam Topic 3)

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

Policy1:

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

Policy2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 48

- (Exam Topic 3)

You need to meet the technical requirements for the new HR department computers.  
How should you configure the provisioning package? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Specify ComputerName as:

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

Specify AccountOU as:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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



**NEW QUESTION 49**

- (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:**

<input type="checkbox"/>
<b>Bypass mode</b>
<b>HTTP blended with internet peering</b>
<b>HTTP blended with peering behind same NAT</b>
<b>Simple download mode with no peering</b>

**Update Active Hours Start to:**

<input type="checkbox"/>
<b>10 AM</b>
<b>11 AM</b>
<b>10 PM</b>
<b>11 PM</b>

**Update Active Hours End to:**

<input type="checkbox"/>
<b>10 AM</b>
<b>11 AM</b>
<b>10 PM</b>
<b>11 PM</b>

- 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 53**

- (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 54**

- (Exam Topic 1)

Which user can enroll Device6 in Intune?

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

**Answer:** B

**NEW QUESTION 55**

- (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 56**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1 and a web app named Appl. App1 must only accept modern authentication requests.

You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:

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

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

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

**Answer:** E

**Explanation:**

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

What is legacy authentication? | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/legacy-authentication> 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn <https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client-apps-condition>

**NEW QUESTION 61**

- (Exam Topic 4)

You have two computers named Computer1 and Computer2 that run Windows 10. Computer2 has Remote Desktop enabled.

From Computer1, you connect to Computer2 by using Remote Desktop Connection.

You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.

What should you do?

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

**Answer:** D

**NEW QUESTION 64**

- (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 365 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 68

- (Exam Topic 4)

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


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

Microsoft Edge is available on all the devices.

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

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

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

 **Compliance policies** | Compliance policy settings ... X

Save X Discard

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

Mark devices with no compliance policy assigned as ☒ Compliant

Enhanced jailbreak detection ☐ Disabled

Compliance status validity period (days)

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

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

Answer Area

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:



### Answer Area

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

### NEW QUESTION 70

- (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 74

- (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 79

- (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 80

- (Exam Topic 4)

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

You join a Windows 11 device named Client1 to contoso.com. You need to add User1 to the local Administrators group of Client1.

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

#### Answer Area



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

net localgroup Administrators /add "AzureAD\user1@contoso.com"

This command will add the Azure AD user with the UPN of user1@contoso.com to the local Administrators group of the device1. You need to use the AzureAD prefix and double backslashes to specify the user's domain. You also need to enclose the user's name in quotation marks if it contains special characters like @.

You can run this command from an elevated command prompt on Client1, or remotely by using PowerShell or other tools. You can also use the Intune Role Administrator role or the Additional local administrators on all Azure AD joined devices setting to manage the local administrators group on Azure AD joined devices.

#### NEW QUESTION 81

- (Exam Topic 4)

Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows

10. Remote Desktop is enabled on Computer2.

The domain contains the user accounts shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.

Name	Members
Group1	ADATUM\User2 ADATUM\User3
Group2	ADATUM\User2
Group3	ADATUM\User3
Administrators	ADATUM\Domain Admins ADATUM\User3
Remote Desktop Users	Group1

The relevant user rights assignments for Computer2 are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	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
User1 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>

### NEW QUESTION 82

- (Exam Topic 4)

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



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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

Minimum number of policies:

- A. Mastered  
B. Not Mastered

Answer: A

#### Explanation:

of Corre Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices1. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps2. You only need one policy to apply this setting to all devices that have App1 installed. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protection-policies/troubleshoot-cut-copy-paste>

#### NEW QUESTION 85

- (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 87

- (Exam Topic 4)

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

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

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

## Answer Area

Deploy a custom Start layout:

Device restriction
Delivery optimization
Device restriction
Endpoint protection
Identity protection

Rename the local Administrator account:

Identity protection
Delivery optimization
Device restriction
Endpoint protection
Identity protection

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area

Deploy a custom Start layout:

Device restriction
Delivery optimization
Device restriction
Endpoint protection
Identity protection

Rename the local Administrator account:

Identity protection
Delivery optimization
Device restriction
Endpoint protection
Identity protection

## NEW QUESTION 90

- (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 95

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

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

Update ring settings [Edit](#)

Update settings

Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No

Set feature update uninstall period (2 - 60 days) 10

Servicing channel General Availability channel

User experience settings

Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

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

Answer Area

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

can be deferred for 30 days

can be deferred indefinitely

can be deferred for 30 days

will be installed immediately

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

1 day

1 day

30 days

60 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

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

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

NEW QUESTION 100

- (Exam Topic 4)

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

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1. All the users use Microsoft Excel.  
From the Microsoft Endpoint Manager admin center, you create the policies shown in the following table.

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

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

#### Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

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

#### NEW QUESTION 104

- (Exam Topic 4)  
Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.  
The company purchases an Azure subscription.  
You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.  
What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.



## Answer Area

Resource to create in Azure:

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

Configuration to perform on the computers:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

A screenshot of a computer Description automatically generated

Reference:

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

## NEW QUESTION 105

- (Exam Topic 4)

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

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

**This site is not secure**

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

 Go to your Start page

Details

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

Error Code: DLG\_FLAGS\_INVALID\_CA

**Go on to the webpage** (Not recommended)

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

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

**Answer:** B

## NEW QUESTION 110

- (Exam Topic 4)

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

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

On which virtual machines can you install Windows 11?

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

**Answer:** E

**NEW QUESTION 112**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User! 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 117**

- (Exam Topic 4)

You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.

Name	Platform	IP address
Device1	Windows	192.168.10.35
Device2	Android	10.10.10.40
Device3	Android	192.168.10.10

The devices are members of a group named Group1.

In Intune, you create a device compliance location that has the following configurations:

- Name: Network1
- IPv4 range: 192.168.0.0/16

In Intune, you create a device compliance policy for the Android platform. The policy has the following configurations:

- Name: Policy1
- Device health: Rooted devices: Block
- Locations: Location: Network1
- Mark device noncompliant: Immediately
- Assigned: Group1

The Intune device compliance policy has the following configurations:

- Mark devices with no compliance policy assigned as: Compliant
- Enhanced jailbreak detection: Enabled
- Compliance status validity period (days): 20

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

## Answer Area

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

- A. Mastered  
 B. Not Mastered

**Answer:** A

### Explanation:

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

- Device1 is marked as noncompliant because it is rooted and the device compliance policy Policy1 blocks rooted devices under the Device health setting1.
- Device2 is marked as compliant because it is not rooted and it is within the network location Network1 that is specified in the device compliance policy Policy11.
- Device3 is marked as noncompliant because it is outside the network location Network1 that is specified in the device compliance policy Policy11. The device compliance location setting requires devices to be in a specific network range to be compliant2.

## NEW QUESTION 119

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune.

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

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

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

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

**Answer:** C

## NEW QUESTION 121

- (Exam Topic 4)

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

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

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

Which device configuration profile type template should you use?

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

**Answer:** A

### Explanation:

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

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

## NEW QUESTION 126

- (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 127

- (Exam Topic 4)

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

You have the devices shown in the following table.

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

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

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

**Answer: A**

#### NEW QUESTION 128

- (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 131

- (Exam Topic 4)

You have a hybrid Azure AD tenant.

You configure a Windows Autopilot deployment profile as shown in the following exhibit.

**Create profile**  
Windows PC

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

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

\* Deployment mode ⓘ

\* Join to Azure AD as ⓘ

Microsoft Software License Terms ⓘ

Important information about hiding license terms ⓘ

Privacy settings ⓘ

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

Hide change account options ⓘ

User account type ⓘ

Allow White Glove OOBE ⓘ

Apply device name template ⓘ

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

### Answer Area

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

- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

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

- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

### Answer Area

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

- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

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

- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

### NEW QUESTION 135

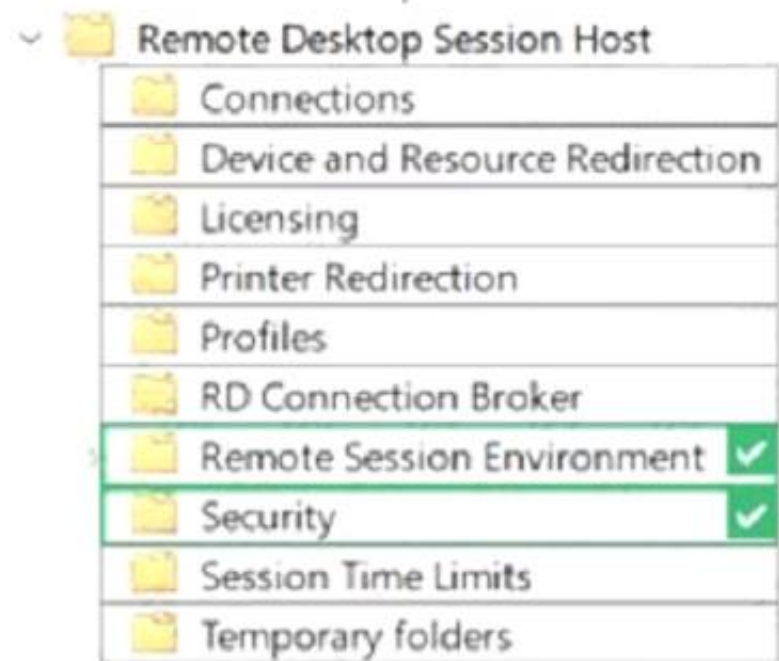
- (Exam Topic 4)

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

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

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

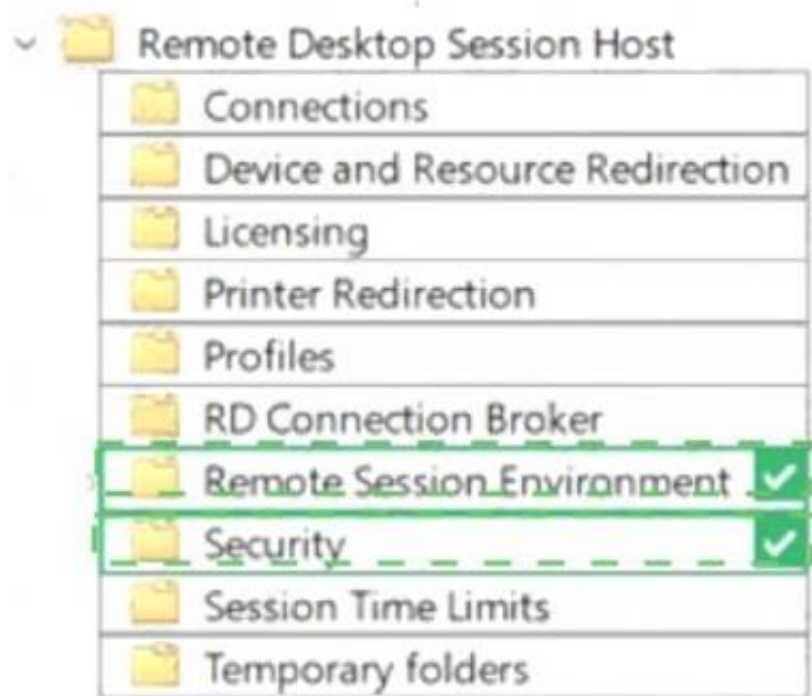
Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 137

- (Exam Topic 4)

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

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

How many more devices can User1 activate?

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

Answer: A

NEW QUESTION 141

.....



## Relate Links

**100% Pass Your MD-102 Exam with Exambible Prep Materials**

<https://www.exambible.com/MD-102-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>