# 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. FI002 security keys
D. text messages

**Answer:** A

**NEW QUESTION 2**
- (Exam Topic 4)
You have an Azure AD tenant that contains the users shown in the following table.

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

You have the devices shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Android |
| Device2 | iOS |

You have a Conditional Access policy named CAPolicy1 that has the following settings:
• Assignments
o Users or workload identities: User 1. User1
o Cloud apps or actions: Office 365 Exchange Online o Conditions: Device platforms: Windows, iOS
• Access controls
o Grant Require multi-factor authentication
You have a Conditional Access policy named CAPolicy2 that has the following settings:
Assignments
o Users or workload identities: Used, User2 o Cloud apps or actions: Office 365 Exch
o Conditions
Device platforms: Android, iOS Filter for devices
Device matching the rule: Exclude filtered devices from policy Rule syntax: device. displayName- contains "1"
Access controls Grant Block access
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
**Answer Area**

| Statements | Yes | No |
|---|---|---|
| If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA. | ○ | ○ |
| If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA. | ○ | ○ |
| User2 can access Microsoft Exchange Online from Device2. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 3**
- (Exam Topic 4)
You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

A. the Azure portal app
B. Endpoint analytics
C. the Company Portal app
D. Microsoft Power Bl

**Answer:** D

**Explanation:**
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:
Devices Enrollment
App protection policy Compliance policy
Device configuration profiles Software updates
Device inventory logs
Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.

- Sign in to the Microsoft Endpoint Manager admin center.
- Select Reports > Intune Data warehouse > Data warehouse.
- Retrieve the custom feed URL from the reporting blade, for example:
- Open Power BI Desktop.
- Choose File > Get Data. Select OData feed.
- Choose Basic.
- Type or paste the OData URL into the URL box.
- Select OK.
- If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
- Select Organizational account.
- Type your username and password.
- Select Sign In.
- Select Connect.
- Select Load.

Reference: https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

**NEW QUESTION 4**
- (Exam Topic 4)
Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer! and Computer2 that run Windows 10. On Computer1, you need to run the
Invoke-Command cmdlet to execute several PowerShell commands on Computed. What should you do first?

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

**Answer:** C

**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.


A. Mastered
B. Not Mastered

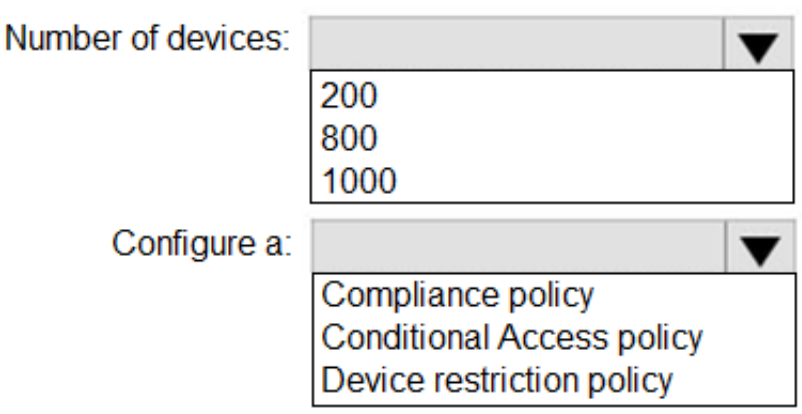
**Answer:** A

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

processes" to prevent Office applications from launching child processes such as scripts or executables. References:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#attack-surface-reduction

**NEW QUESTION 6**
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 iOS devices. The devices are enrolled in Microsoft Intune as follows:
• Two hundred devices are enrolled by using the Intune Company Portal.
• Eight hundred devices are enrolled by using Apple Automated Device Enrollment (ADE).
You create an iOS/iPadOS software updates policy named Policy 1 that is configured to install iOS/iPadOS 15.5.
How many iOS devices will Policy1 update, and what should you configure to ensure that only iOS/iPadOS 15.5 is installed? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Policy 1 will update 800 iOS devices that are enrolled by using Apple Automated Device Enrollment (ADE). This is because ADE devices are supervised devices that support software update policies in Intune1. Devices that are enrolled by using the Intune Company Portal are not supervised devices and do not support software update policies2.
To ensure that only iOS/iPadOS 15.5 is installed, you should configure a device restriction policy that restric visibility of software updates. This will prevent users from manually updating the OS to a newer version than the one you specified in Policy 11. You can use the Deployment Workbench to create and assign a device restriction profile to your ADE devices3.

**NEW QUESTION 7**
- (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 8**
- (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

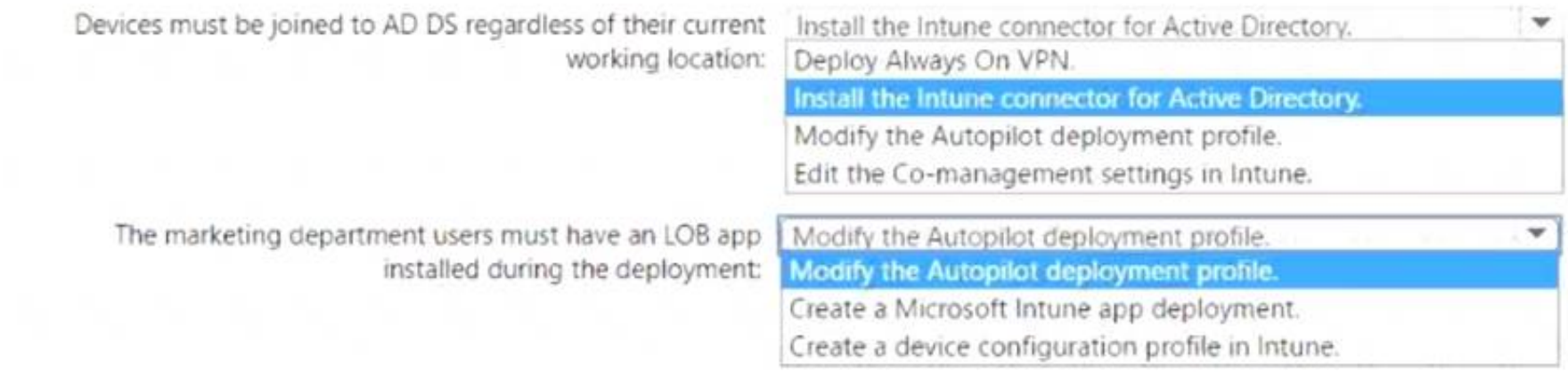
**NEW QUESTION 9**
- (Exam Topic 4)
Your company has a Remote Desktop Gateway (RD Gateway).
You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.
You need to configure a Remote Desktop connection to connect through the gateway. Which setting should you configure?

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

**Answer:** A

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

**NEW QUESTION 10**
- (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**




A. Mastered
B. Not Mastered

**Answer:** A

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


**NEW QUESTION 10**
- (Exam Topic 4)
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**NEW QUESTION 11**
- (Exam Topic 4)
You have a Microsoft 365 subscription.

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

| Platform | Version |
|---|---|
| Android | 8, 9 |
| iOS | 11, 12 |

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

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

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager: [ ▼ ]
- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment: [ ▼ ]
- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

**NEW QUESTION 12**
- (Exam Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

| Name | Platform |
|---|---|
| Device1 | Windows 10 |
| Device2 | macOS |

In Microsoft Intune Endpoint security, you need to configure a disk encryption policy for each device. Which encryption type should you use for each device, and which role-based access control (RBAQ role in
Intune should you use to manage the encryption keys? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**

Device1: [ ▼ ]
- FileVault
- Cryptsetup
- Encrypting File System (EFS)
- BitLocker Drive Encryption (BitLocker)

Device2: [ ▼ ]
- FileVault
- Cryptsetup
- Encrypting File System (EFS)
- BitLocker Drive Encryption (BitLocker)

RBAC role: [ ▼ ]
- Help Desk Operator
- Application Manager
- Intune Role Administrator
- Policy and Profile Manager

A. Mastered
B. Not Mastered

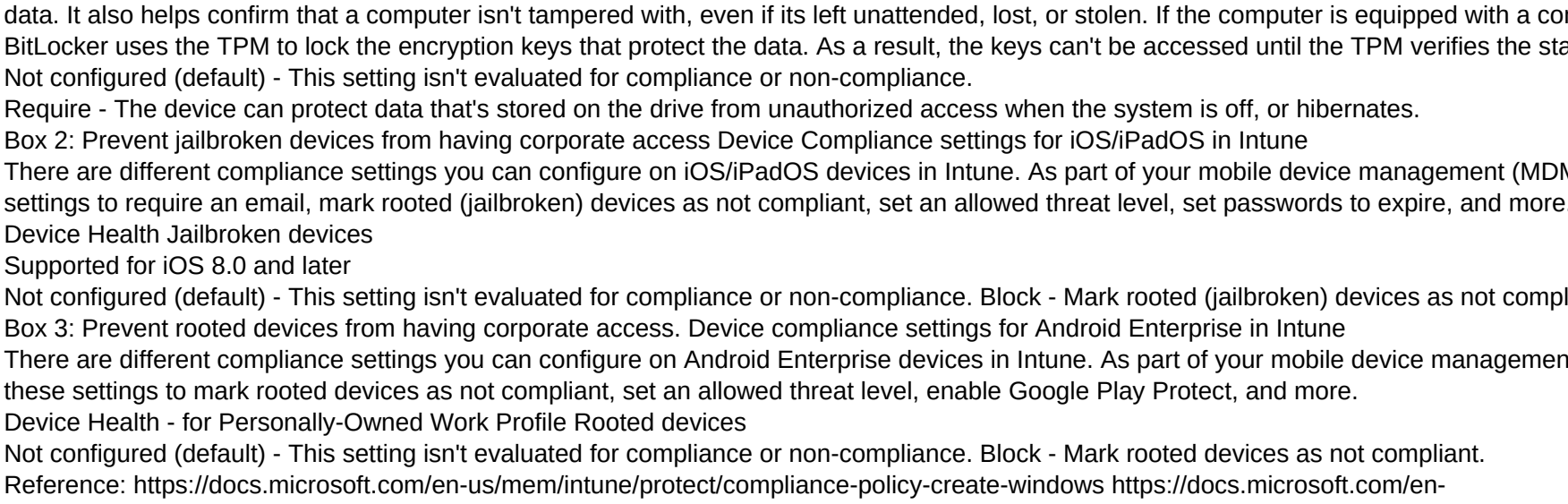
**Answer:** A

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

**NEW QUESTION 15**
- (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.




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 20**
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
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 Microsoft Deployment Toolkit (MDT) deployment
share. You create a task sequence, and then you run the MDT deployment wizard on Computer1. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**NEW QUESTION 25**
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You use Windows Autopilot to deploy Windows 11 to devices.
A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.
You need to ensure that when a deployment fails, the deployment logs can be collected.
What should you configure?

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

**Answer:** B

**NEW QUESTION 28**
- (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 30**
- (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 31**
- (Exam Topic 4)
You have a Microsoft Intune subscription.
You have devices enrolled in intune as shown in the following table.

| Name | Operating system |
|---|---|
| Device1 | Android 8.1.0 |
| Device2 | Android 9 |
| Device3 | iOS 11.4.1 |
| Device4 | iOS 12.3.1 |
| Device5 | iOS 12.3.2 |

An app named App1 is installed on each device.
What is the minimum number of app configuration policies required to manage Appl ?

A. 1
B. 2
C. 3
D. 4
E. 5

**Answer:** B

**Explanation:**
The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn
https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios

**NEW QUESTION 34**
- (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 37**
- (Exam Topic 2)
What should you configure to meet the technical requirements for the Azure AD-joined computers?

A. Windows Hello for Business from the Microsoft Intune blade in the Azure portal.
B. The Accounts options in an endpoint protection profile.
C. The Password Policy settings in a Group Policy object (GPO).
D. A password policy from the Microsoft Office 365 portal.

**Answer:** A

**Explanation:**
References:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-inorgani

**NEW QUESTION 40**
- (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 42**
- (Exam Topic 1)
Which devices are registered by using the Windows Autopilot deployment service?

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

**Answer:** C

**Explanation:**

Scenario: Windows Autopilot Configuration Assignments
Included groups: Group1
Excluded groups: Group2 Device1 is member of Group1.
Device2 is member of Group1 and member of Group2. Device3 is member of Group1.
Group1 and Group2 have a Membership type of Assigned.
Exclusion takes precedence over inclusion in the following same group type scenarios. Reference: https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

**NEW QUESTION 44**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.
You need to configure the devices to run a single app in kiosk mode.
Which Configuration settings should you modify in the device restrictions profile?

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

**Answer:** D

**Explanation:**
To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. References:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work#device-experie

**NEW QUESTION 47**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

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

**Answer:** C

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

**NEW QUESTION 51**
- (Exam Topic 4)
You have two computers named Computer1 and Computed that run Windows 10. Computed 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 52**
- (Exam Topic 4)
Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active Directory (Azure AD).
There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.
You plan to implement Microsoft Defender Exploit Guard.
You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**

Tool to use to configure the settings:

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

Distribution method:

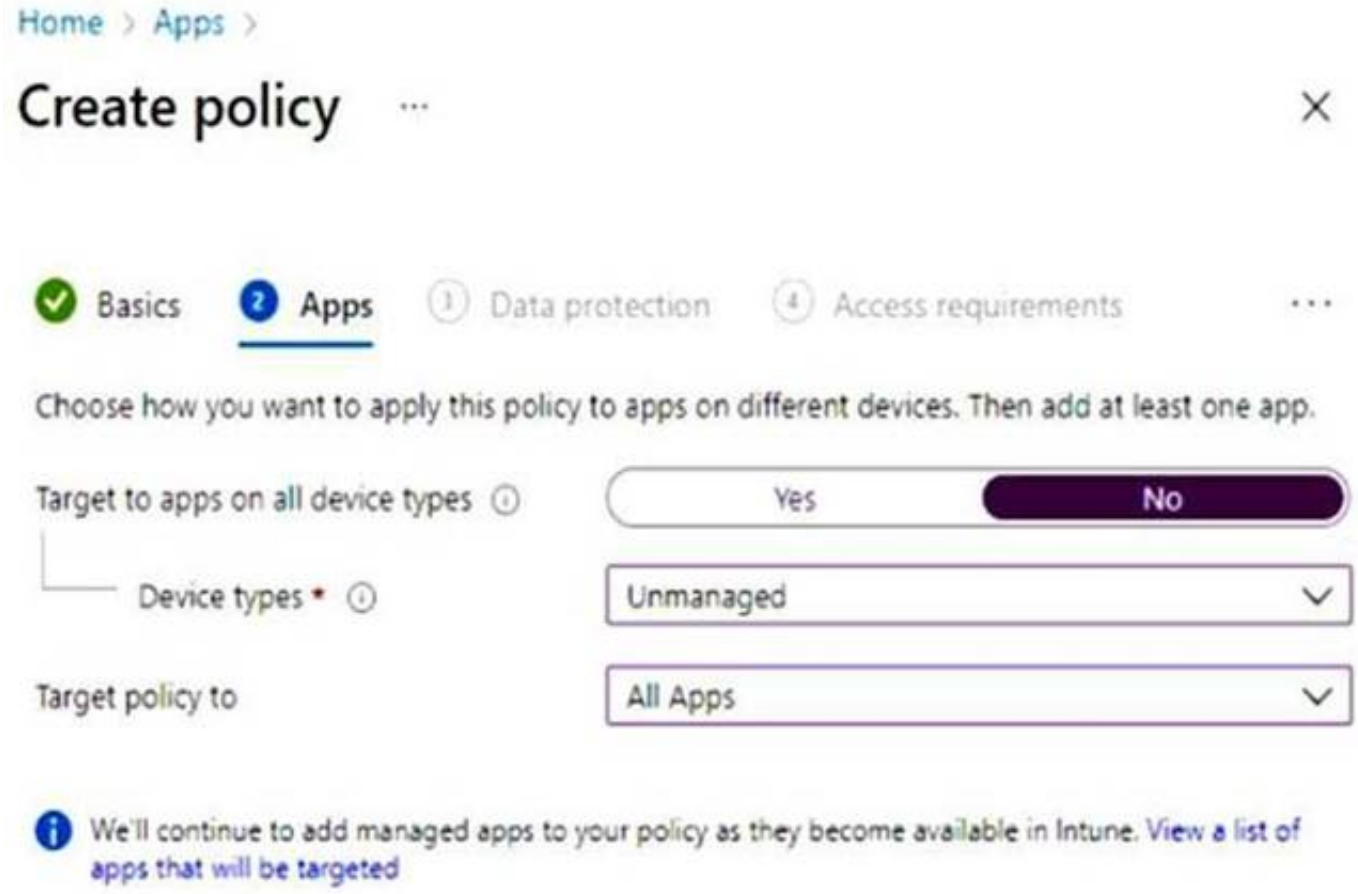
- An Azure policy
- An Endpoint Protection configuration profile
- An Intune device compliance policy
- A device restrictions configuration profile

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/import-export-expl https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-prot

**NEW QUESTION 57**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.




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

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

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

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

- users only
- devices only
- users and devices

A. Mastered
B. Not Mastered

**Answer:** A

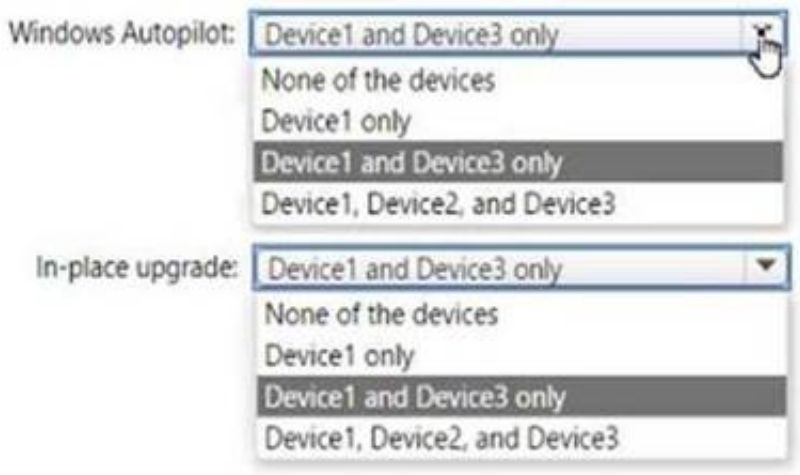
**Explanation:**
Box 1: Install the Intune Company Portal app on the device
On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.
Bix 2: Devices only
For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipado

**NEW QUESTION 60**
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

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

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

**Answer Area**




A. Mastered
B. Not Mastered

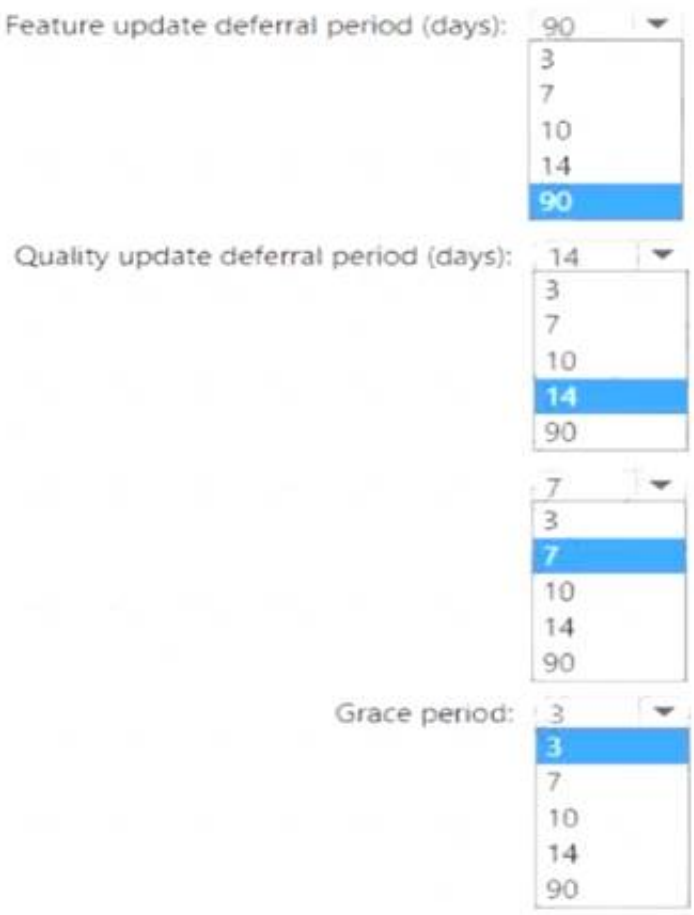
**Answer:** A

**Explanation:**

**Answer Area**


**NEW QUESTION 63**
- (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**




A. Mastered
B. Not Mastered

**Answer:** A

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


**NEW QUESTION 66**
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.

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

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

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

You capture and upload the hardware IDs of the devices in the marketing department. You configure Windows Autopilot.
For each of the following statements, select Yes if the statement is true. Otherwise select No. NOTE: Each correct selection is worth one point.

Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can complete the Autopilot process on Device1. | | |
| User2 can complete the Autopilot process on Device1. | | |
| User3 can view device setup information during the enrollment phase of Device1. | | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can complete the Autopilot process on Device1. | | ☐ |
| User2 can complete the Autopilot process on Device1. | ☐ | |
| User3 can view device setup information during the enrollment phase of Device1. | | ☐ |

**NEW QUESTION 68**
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure the Authentication methods. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**NEW QUESTION 69**
- (Exam Topic 4)
You have groups that use the Dynamic Device membership type as shown in the following table.

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

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

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

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

**App Information** Edit

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

**Assignments** Edit

| Group mode | Group |
|---|---|
| Required | |
| Included | Group1 |
| Available for enrolled devices | |

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

| Statements | Yes | No |
|---|---|---|
| LT1 will have Microsoft Office 365 installed | ○ | ○ |
| LT2 will have Microsoft Office 365 installed | ○ | ○ |
| LT3 will have Microsoft Office 365 installed | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

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

**NEW QUESTION 72**
- (Exam Topic 4)
You have a Microsoft 365 tenant.
You have devices enrolled in Microsoft Intune.
You assign a conditional access policy named Policy1 to a group named Group1. Policy! 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 75**
- (Exam Topic 4)
You use a Microsoft Intune subscription to manage iOS devices.
You configure a device compliance policy that blocks jailbroken iOS devices. You need to enable Enhanced jailbreak detection.
What should you configure?

A. the Compliance policy settings
B. the device compliance policy
C. a network location
D. a configuration profile

**Answer:** D

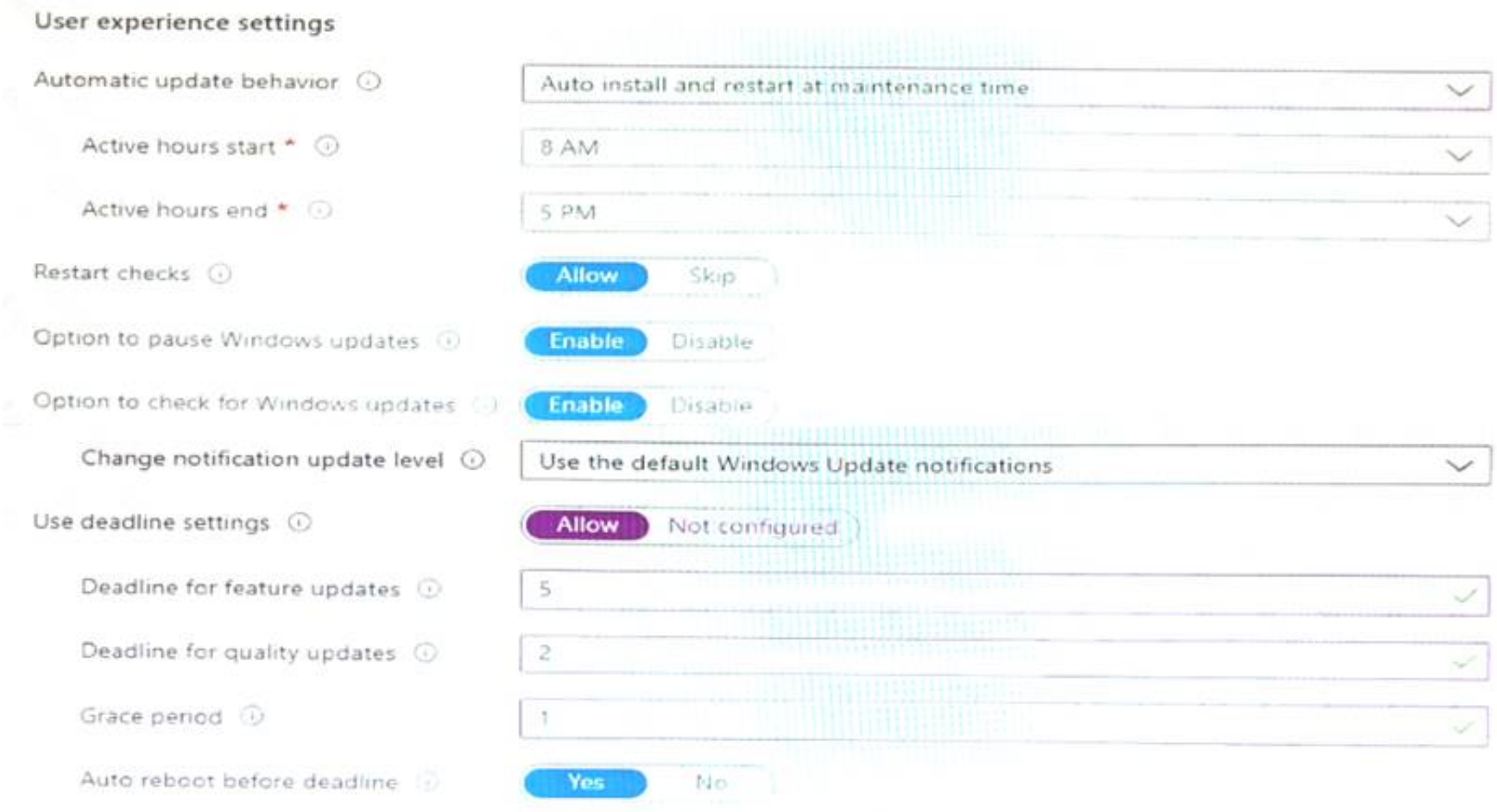
**NEW QUESTION 76**
- (Exam Topic 4)
You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.
You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.
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 80**
- (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.




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

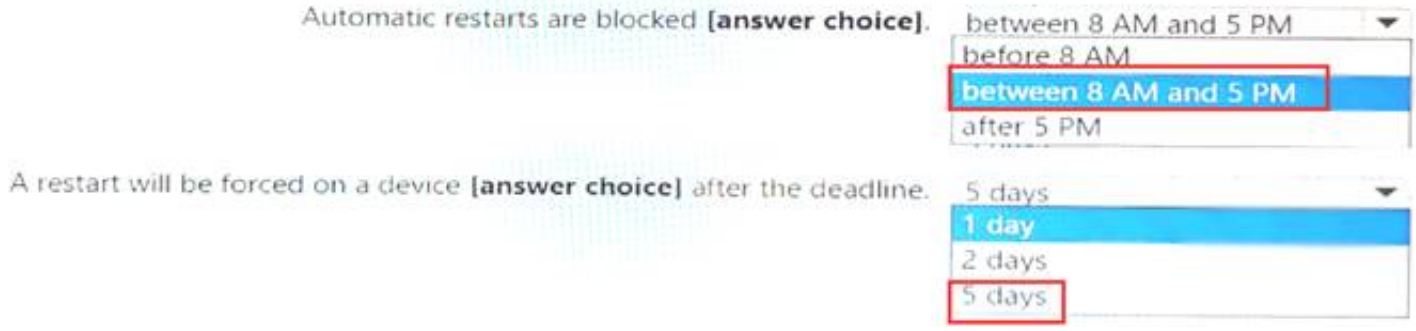
**Answer Area**


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**




**NEW QUESTION 82**
- (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<br>ADATUM\User3 |
| Group2 | ADATUM\User2 |
| Group3 | ADATUM\User3 |
| Administrators | ADATUM\Domain Admins<br>ADATUM\User3 |
| Remote Desktop Users | Group1 |

The relevant user rights assignments for Computed 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. | ○ | ○ |
| User2 can establish a Remote Desktop session to Computer2. | ○ | ○ |
| User3 can establish a Remote Desktop session to Computer2. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can establish a Remote Desktop session to Computer2. | ○ | ○ |
| User2 can establish a Remote Desktop session to Computer2. | ○ | ○ |
| User3 can establish a Remote Desktop session to Computer2. | ○ | ○ |

**NEW QUESTION 86**
- (Exam Topic 4)
You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices. You purchase a Microsoft 365 E5 subscription.
You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.
Which upgrade method should you use?

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

**Answer:** C

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

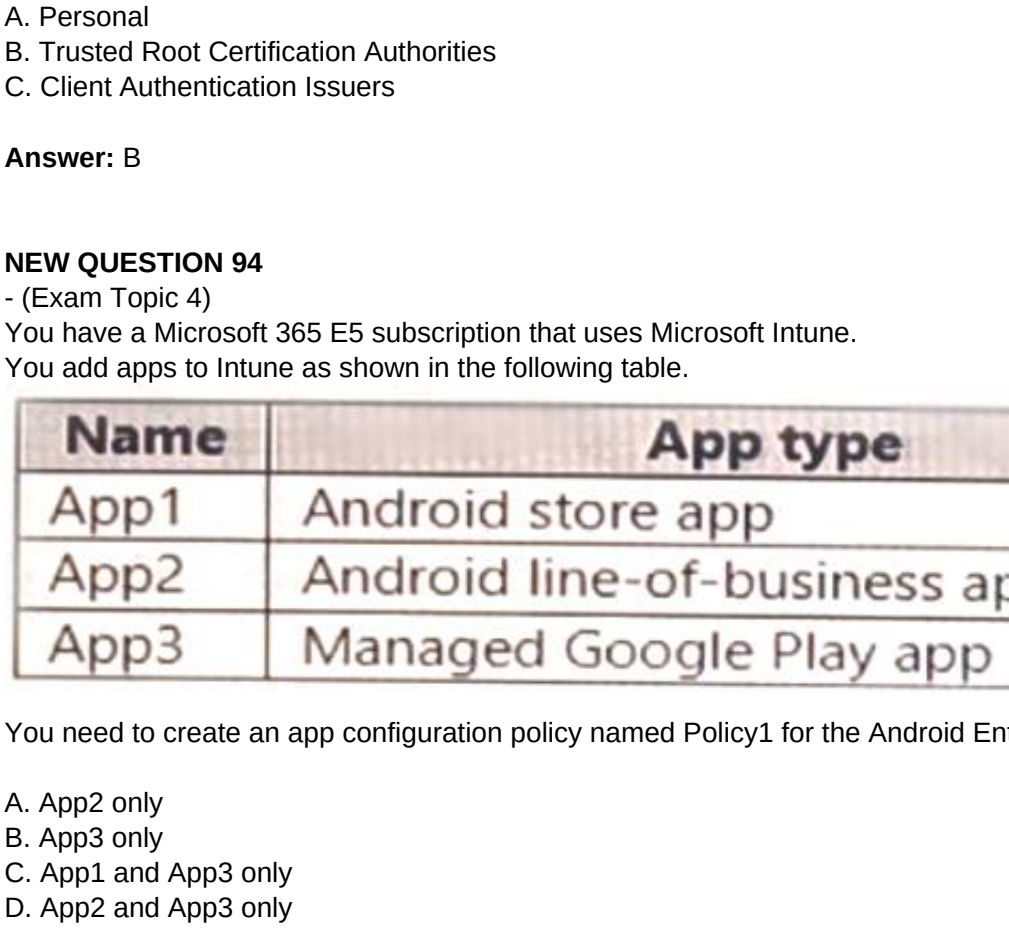
licenses

**NEW QUESTION 87**
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10. You implement hybrid Azure AD and Microsoft Intune.
You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort.
What should you use?

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

**Answer:** D

**NEW QUESTION 92**
- (Exam Topic 4)
You use Windows Admin Center to remotely administer computers that run Windows 10.
When connecting to Windows Admin Center, you receive the message shown in the following exhibit.




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

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

**Answer:** B

**NEW QUESTION 94**
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You add apps to Intune as shown in the following table.

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

You need to create an app configuration policy named Policy1 for the Android Enterprise platform. Which apps can you manage by using Policyl1?

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

**Answer:** D

**NEW QUESTION 97**
- (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.

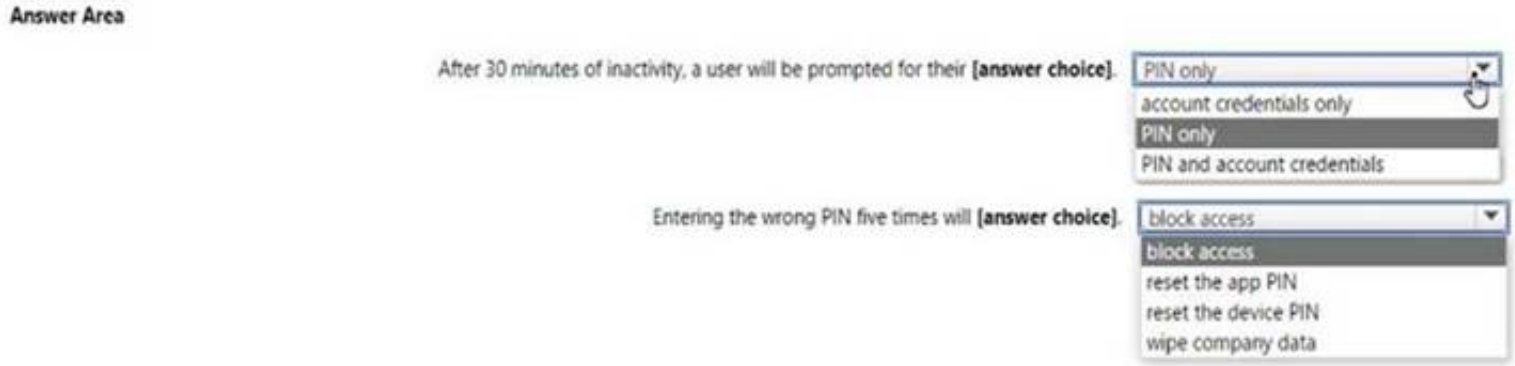
**Access requirements**

| | |
|---|---|
| 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,




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 102**
- (Exam Topic 4)
Your company has a computer named Computer1 that runs Windows 10. Computed was used by a user who left the company.
You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows Autopilot.

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


A. Mastered
B. Not Mastered

**Answer:** A

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

- Generate a JSON file that contains the computer information. This file specifies the Autopilot profile to be applied during the deployment. You can use the Get-AutopilotProfilesForExistingDevices PowerShell script to generate this file1.
- Reset the computer. You can use the Windows Automatic Redeployment feature to trigger a reset from the login screen by pressing Ctrl + R and providing an administrator account2. Alternatively, you can use the Windows Autopilot Reset feature to remotely reset the device from Intune1.
- Upload the file by running azcopy.exe. This step copies the JSON file to a blob storage account in Azure, where it can be accessed by the device during the deployment. You need to specify the storage account name, access key, and container name as parameters for azcopy.exe1.

**NEW QUESTION 104**
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

| Name | Member of |
|---|---|
| User1 | Group1 |
| User2 | Group2 |

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

| Name | Platform | Member of |
|---|---|---|
| Device1 | Windows 10 | Group1 |
| Device2 | Android | Group1 |
| Device3 | iOS | Group2 |

From Intune, you create and send a custom notification named Notification1 to Group1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
A screenshot of a computer Description automatically generated with medium confidence
Reference:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications

**NEW QUESTION 109**
- (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 110**
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com. You have the devices shown in the following table.

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

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


A. Mastered
B. Not Mastered

**Answer:** A

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


**NEW QUESTION 112**
- (Exam Topic 4)
You have a Microsoft Intune subscription that has the following device compliance policy settings: Mark devices with no compliance policy assigned as: Compliant
Compliance status validity period (days): 14
On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

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

On January 4, you create the following two device compliance policies:
- Name: Policy1

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

On January 5, you assign Policy1 and Policy2 to Group1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

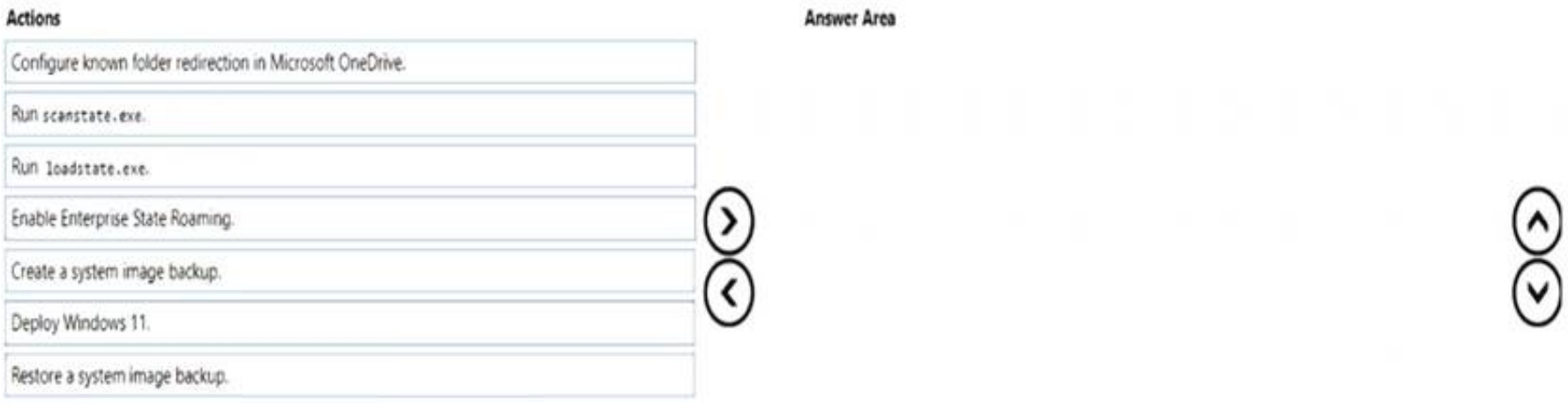
| Statements | Yes | No |
|---|---|---|
| On January 7, Device1 is marked as compliant. | ○ | ○ |
| On January 8, Device1 is marked as compliant. | ○ | ○ |
| On January 8, Device2 is marked as compliant. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: No.
Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.
Box 2: No
For the same reason as Box1. Box 3: Yes
Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.
The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

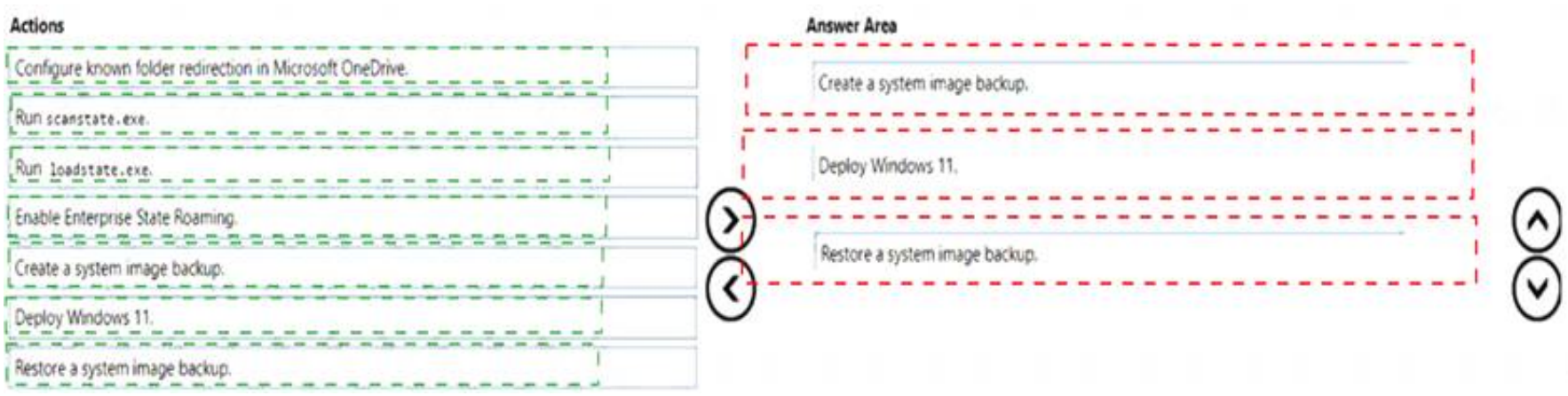
**NEW QUESTION 113**
- (Exam Topic 4)
You have 100 computers that run Windows 10.
You plan to deploy Windows 11 to the computers by performing a wipe and load installation. You need to recommend a method to retain the user settings and the user data.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



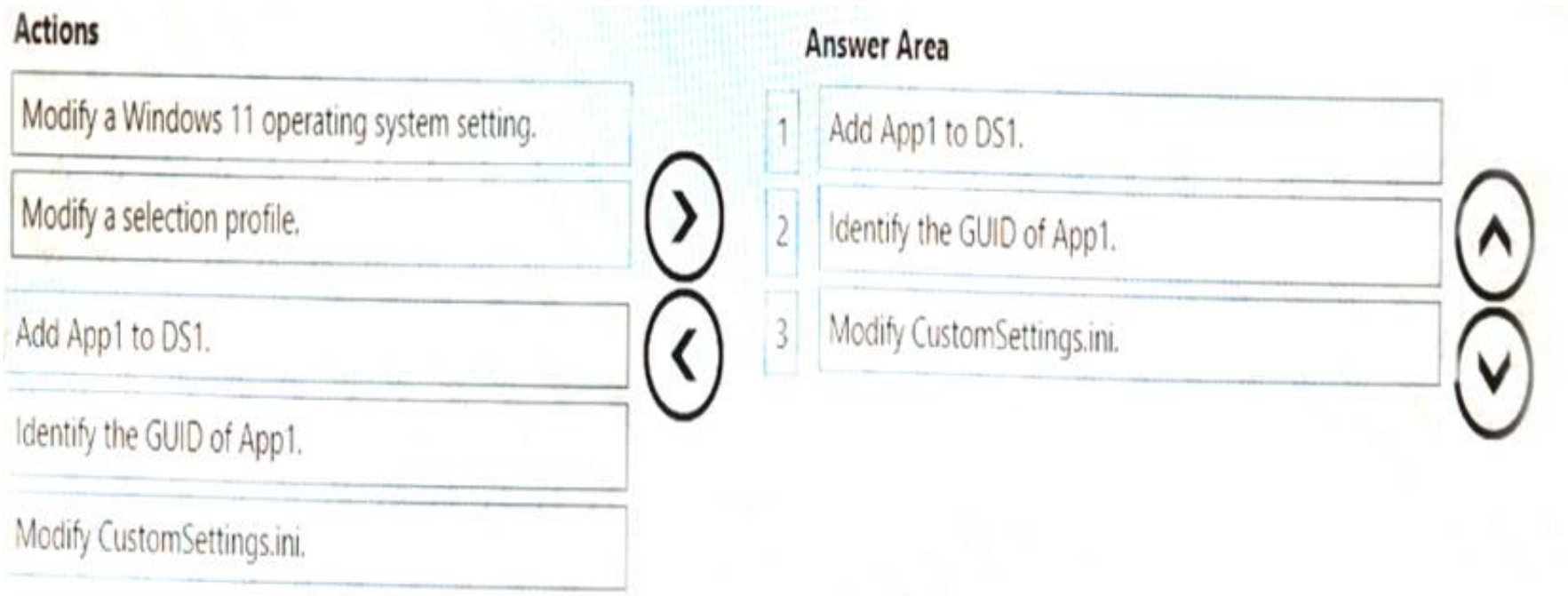

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 114**
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1. You import a Windows 11 image to DS1.
You have an executable installer for an application named App1.
You need to ensure that App1 will be installed for all the task sequences that deploy the image.
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.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
MDT is a tool that allows you to automate the deployment of Windows operating systems and applications. To install an application for all the task sequences that deploy a Windows 11 image, you need to perform the following three actions in sequence:
- Add App1 to DS1. You can use the Deployment Workbench to import the executable installer of App1 to a folder in your deployment share. This will create an application entry with a unique GUID that identifies App11.
- Identify the GUID of App1. You can find the GUID of App1 by opening the application properties in the Deployment Workbench and looking at the Application GUID field1. You can copy the GUID to use it later.
- Modify CustomSettings.ini. You can edit the CustomSettings.ini file in your deployment share to specify which applications to install for each task sequence. You can use the Applications property to list the GUIDs of the applications you want to install, separated by commas1. For example, if you want to install App1 and another application with GUID {1234-5678-90AB-CDEF}, you can use this line:
Applications={GUID of App1},{1234-5678-90AB-CDEF}
These are the three actions you need to perform to ensure that App1 will be installed for all the task sequences that deploy the Windows 11 image from DS1. I hope this helps you.
If you want to learn more about MDT and how to deploy applications with it, you can check out these resources:
- How to deploy applications with the Microsoft Deployment Toolkit

**NEW QUESTION 116**
- (Exam Topic 4)
You install a feature update on a computer that runs Windows 10. How many days do you have to roll back the update?

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

**Answer:** B

**NEW QUESTION 121**
- (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.


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 123**
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

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

**Answer:** B

**NEW QUESTION 127**
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.

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

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

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

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

Answer Area

| Statements | Yes | No |
|---|---|---|
| If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically. | | |
| If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically. | | |
| If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically. | | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Answer Area

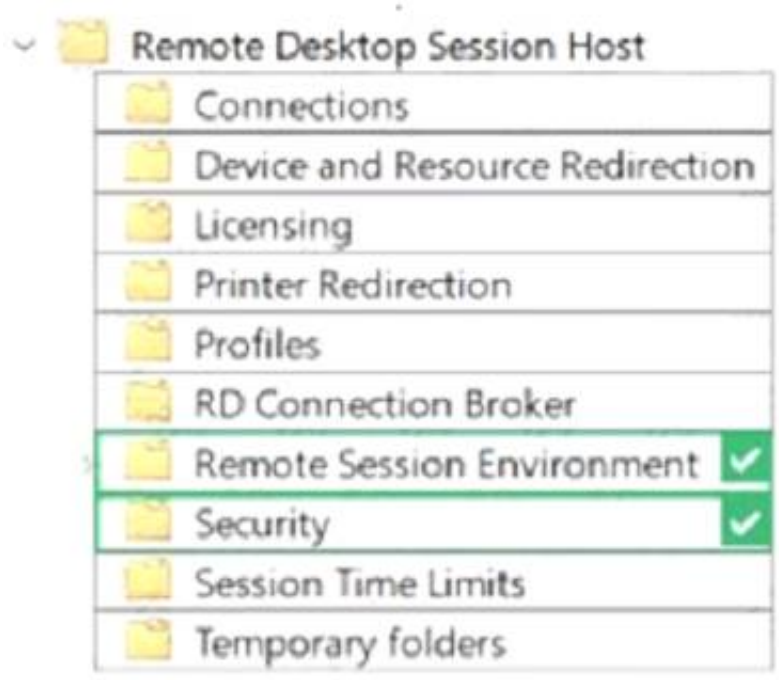
| Statements | Yes | No |
|---|---|---|
| If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically. | | |
| If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically. | | |
| If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically. | | |

**NEW QUESTION 130**
- (Exam Topic 4)
Your company standardizes on Windows 10 Enterprise for all users.
Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.
You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps. The solution must meet the following
requirements:
• Ensure that any applications installed by the users are retained.
• Minimize user intervention.
What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

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

**Answer:** A

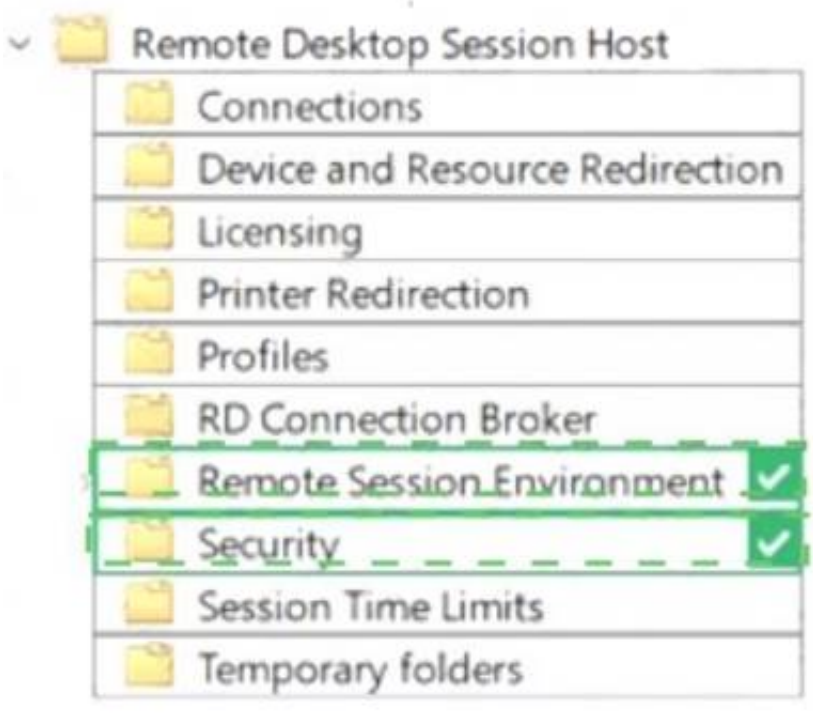
**NEW QUESTION 133**
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains 1.000 computers that run Windows 11.
You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:
• Prevent the sharing of clipboard 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**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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 FirstTry

* MD-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year