Microsoft

Exam Questions MD-102

Endpoint Administrator

NEW QUESTION 1
- (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 2
- (Exam Topic 1)
Which users can purchase and assign App1?

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

Answer: B

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

NEW QUESTION 3
- (Exam Topic 1)
User1 and User2 plan to use Sync your settings.
On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

User1:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

User2:
No devices
Device4 and Device5 only
Device1, Device2 and Device3 only
Device1, Device2, Device3, Device4, and Device5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/

NEW QUESTION 4
- (Exam Topic 1)
You implement the planned changes for Connection1 and Connection2
How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2? To answer select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.

Answer Area

Device1:	1 2 3 4 5
Device2:	

Device2:	1 2 3 4 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, table Description automatically generated

NEW QUESTION 5
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device4 is marked as compliant.	○	○
Device5 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated

NEW QUESTION 6
- (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 7
- (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
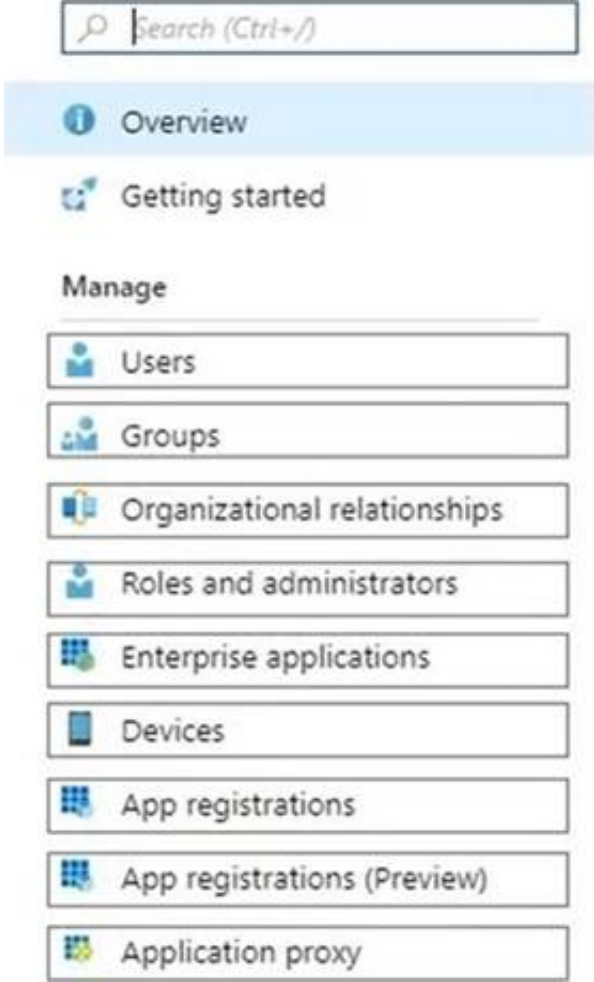
NEW QUESTION 8
- (Exam Topic 2)
You need to meet the technical requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 9
- (Exam Topic 2)
You need to meet the OOBE requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Overview

Getting started

Manage

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 10
- (Exam Topic 2)
You need to recommend a solution to meet the device management requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

For the Research department employees:

An app configuration policy
An app protection policy
Azure information Protection
iOS app provisioning profiles

For the Sales department employees:

An app configuration policy
An app protection policy
Azure information Protection
iOS app provisioning profiles

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md
https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-not-forward-option-fo

NEW QUESTION 10
- (Exam Topic 2)
What should you use to meet the technical requirements for Azure DevOps?

A. An app protection policy
B. Windows Information Protection (WIP)
C. Conditional access
D. A device configuration profile

Answer: C

Explanation:
 References:
https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access? view=azure-devops

NEW QUESTION 13
- (Exam Topic 2)
You need to resolve the performance issues in the Los Angeles office.
How should you configure the update settings? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Change Delivery Optimization download mode to:	▽
	Bypass mode
	HTTP blended with internet peering
	HTTP blended with peering behind same NAT
	Simple download mode with no peering

Update Active Hours Start to:	▽
	10 AM
	11 AM
	10 PM
	11 PM

Update Active Hours End to:	▽
	10 AM
	11 AM
	10 PM
	11 PM

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 16
- (Exam Topic 3)
You have a Microsoft 365 subscription.
You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM). You need to deploy the Microsoft 36S Apps for enterprise suite to all the computers.
What should you do?

A. From the Microsoft Intune admin center, create a Windows 10 device profile.
B. From Azure AD, add an app registration.
C. From Azure A
D. add an enterprise application.
E. From the Microsoft Intune admin center, add an app.

Answer: D

Explanation:
To deploy Microsoft 365 Apps for enterprise to Windows 10 devices that are enrolled in Intune, you need to add an app of type "Windows 10 app (Win32)" in the Microsoft Intune admin center and configure the app settings. You can then assign the app to groups of users or devices. References:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management

NEW QUESTION 19
- (Exam Topic 3)
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.
Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 21
- (Exam Topic 3)
You have the on-premises servers shown in the following table.

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

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.
You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.
To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Server:

Server1
Server2
Server3
Server4

Ports:

TCP 443 only
UDP 443 only
TCP 1723 only
TCP 443 and UDP 443 only
TCP 443, TCP 1723, and UDP 443

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Server4
Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.
Box 2: TCP 443 and UDP 443 only
Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.
By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Saerver Configuration – Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.
Incorrect:
TCP 1723 is not used.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-overview

---

NEW QUESTION 24
- (Exam Topic 3)
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.

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

Which groups can you add to Group4?

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

Answer: C

NEW QUESTION 27
- (Exam Topic 3)
You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

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

AH devices contain an app named App1 and are enrolled in Microsoft Intune.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Policy type:	App protection policy
	App configuration policy
	App protection policy
	Conditional access policy
	Device compliance policy

Minimum number of policies:	1
	1
	2
	3
	4
	5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
 of Corre Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices1. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps2. You only need one policy to apply this setting to all devices that have App1 installe1d.
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 29
- (Exam Topic 3)
You have the device configuration profile shown in the following exhibit.

Kiosk
Windows 10 and later

✕

✓ Basics   ② Configuration settings   ③ Assignments   ...

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

Select a kiosk mode * ⓘ   [Single app, full-screen kiosk   ⌄]

User logon type * ⓘ   [Auto logon (Windows 10, version 1803+)   ⌄]

Application type * ⓘ   [Add Microsoft Edge browser   ⌄]

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. Learn more about Microsoft Edge kiosk mode.

Edge Kiosk URL * ⓘ   [https://contoso.com   ✓]

Microsoft Edge kiosk mode type ⓘ   [Public Browsing (InPrivate)   ⌄]

Refresh browser after idle time ⓘ   [5]

Specify Maintenance Window for App Restarts * ⓘ   [Require   **Not configured**]

Maintenance Window Start Time   [MM/DD/YYYY 📅] [h:mm:ss A]

Maintenance Window Recurrence ⓘ   [Daily (recommended)   ⌄]

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

Answer Area

Users	
	can access any URL.
	cannot view the address bar in Microsoft Edge.
	can only access URLs that include contoso.com.
	can only access URLs that start with https://contoso.com/ .

Windows 10 devices can have	
	a single Microsoft Edge instance that has a single tab.
	a single Microsoft Edge instance that has multiple tabs.
	multiple Microsoft Edge instances that have multiple tabs.
	multiple Microsoft Edge instances that each has a single tab.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Users can only access URLs that start with https://contoso.com/ Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab
he device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:
≫ Kiosk mode: Enabled
≫ Kiosk type: Multi-app
≫ Allowed URLs: https://contoso.com/*
≫ Address bar: Disabled
These settings mean that users can only access URLs that start with https://contoso.com/ and cannot view the address bar in Microsoft Edge. The kiosk type of Multi-app allows users to open multiple instances of Microsoft Edge, but each instance can only have a single tab. Therefore, users cannot access any URL, cannot view the address bar in Microsoft Edge, and can have multiple Microsoft Edge instances that each has a single tab. References: https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings#kiosk-browser-settings

NEW QUESTION 30
- (Exam Topic 3)
You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune. You need to review the startup processes and how often each device restarts.
What should you use?

A. Endpoint analytics
B. Intune Data Warehouse
C. Azure Monitor
D. Device Management

Answer: B

NEW QUESTION 32
- (Exam Topic 3)
You have 100 computers that run Windows 10.
You plan to deploy Windows 11 to the computers by performing a wipe and load installation. You need to recommend a method to retain the user settings and the user data.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Configure known folder redirection in Microsoft OneDrive.	
Run scanstate.exe.	
Run loadstate.exe.	
Enable Enterprise State Roaming.	
Create a system image backup.	
Deploy Windows 11.	
Restore a system image backup.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Configure known folder redirection in Microsoft OneDrive.	Create a system image backup.
Run scanstate.exe.	
Run loadstate.exe.	Deploy Windows 11.
Enable Enterprise State Roaming.	
Create a system image backup.	Restore a system image backup.
Deploy Windows 11.	
Restore a system image backup.	

NEW QUESTION 34
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains a user named User! and a web app named Appl. App1 must only accept modern authentication requests.
You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:
• Assignments
° Users or workload identities: User1
° Cloud apps or actions: App1
• Access controls
° Grant: Block access
You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

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

Answer: E

Explanation:
you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13. References: 1: Conditional Access: Block legacy authentication | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy-authentication 2:
What is legacy authentication? | Microsoft Learn
https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/legacy-authentication 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client-apps-condition

NEW QUESTION 38
- (Exam Topic 3)
You have a Microsoft 365 subscription that includes Microsoft Intune.
You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:
• Enforces compliance for Defender for Endpoint by using Conditional Access
• Prevents suspicious scripts from running on devices

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

Features	Answer Area
A device restriction policy	Enforces compliance: [ ]
A security baseline	Prevents suspicious scripts: [ ]
An attack surface reduction (ASR) rule	
An Intune connection	

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 39
- (Exam Topic 3)
You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:
• Requires BitLocker Drive Encryption (BitLocker) on each device
• Requires a minimum operating system version
Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point,

Settings	Answer Area
Device Health	Requires BitLocker: [ ]
Device Properties	Requires a minimum operating system version: [ ]
Microsoft Defender for Endpoint	
System Security	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Settings	Answer Area
Device Health	Requires BitLocker: System Security
Device Properties	Requires a minimum operating system version: Device Properties
Microsoft Defender for Endpoint	
System Security	

NEW QUESTION 43
- (Exam Topic 3)
You have an on-premises server named Server! that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

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

Answer: C

NEW QUESTION 47

- (Exam Topic 3)
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 52
- (Exam Topic 3)
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 54
- (Exam Topic 3)
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 56
- (Exam Topic 3)
You have a Microsoft 365 subscription.
You use Microsoft Intune Suite to manage devices.
You have the iOS app protection policy shown in the following exhibit.

Access requirements

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

Conditional launch

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

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

Answer Area

After 30 minutes of inactivity, a user will be prompted for their **[answer choice]**. PIN only ▾
- account credentials only
- PIN only
- PIN and account credentials

Entering the wrong PIN five times will **[answer choice]**. block access ▾
- block access
- reset the app PIN
- reset the device PIN
- wipe company data

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 58
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS
devices. The solution must minimize administrative effort. What should you do?

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

Answer: D

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

NEW QUESTION 63
- (Exam Topic 3)
You have a Microsoft 365 tenant and an internal certification authority (CA).

You need to use Microsoft Intune to deploy the root CA certificate to managed devices.
Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

| App configuration policy |
| App protection policy |
| Compliance policy |
| Configuration profile |

Profile:

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 66
- (Exam Topic 3)
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 71
- (Exam Topic 3)
You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

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

Answer: D

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

Choose File > Get Data. Select OData feed.
- Choose Basic.
- Type or paste the OData URL into the URL box.
- Select OK.
- If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
- Select Organizational account.
- Type your username and password.
- Select Sign In.
- Select Connect.
- Select Load.

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

NEW QUESTION 72
- (Exam Topic 3)
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 73
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS
devices. The solution must minimize administrative effort.
What should you do?

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

Answer: C

Explanation:

To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices. References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-install-with-int

NEW QUESTION 78
- (Exam Topic 3)
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 81
- (Exam Topic 3)
You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.
You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.
Which four 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:

NEW QUESTION 84
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You plan to use Endpoint analytics.
You need to create baseline metrics. What should you do first?

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

Answer: B

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

NEW QUESTION 85
- (Exam Topic 3)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You plan to deploy two apps named App1 and App2 to all Windows devices. Appl must be installed before App2.
From the Intune admin center, you create and deploy two Windows app (Win32) apps. You need to ensure that App1 is installed before App2 on every device.
What should you configure?

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

Answer: D

Explanation:
The correct answer is D because you can configure the dependencies for a Win32 app in the deployment configurations1. Dependencies are other Win32 apps that must be installed before your Win32 app can be installed1. You can add Win32 app dependencies only after your Win32 app has been added and uploaded to Intune2. In this case, you need to configure the App2 deployment configurations to add App1 as a dependency2. References: 1: Microsoft Intune Win32 App Dependencies - MSEndpointMgr https://msendpointmgr.com/2019/06/03/new-intune-feature-win32-app-dependencies/ 2: Add and assign Win32 apps to Microsoft Intune | Microsoft Learn
https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add

NEW QUESTION 87
- (Exam Topic 3)
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 92
- (Exam Topic 3)
Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.

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

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

💻 computer1

Actions ∨

Domain: adatum.com
OS: Windows10 64-bit (Build 17134)
Machine IP addresses ❯
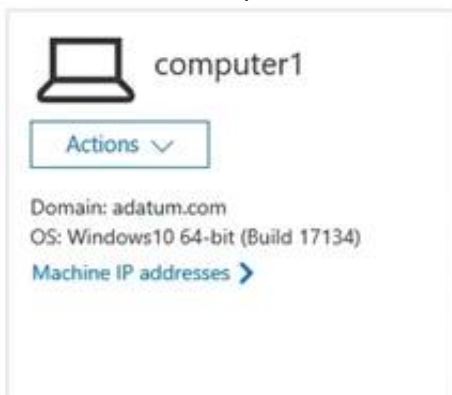
What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of:

Group3 only
Group4 only
Grou5 only
Group3, Group4, and Group5 only

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

Group1 only
Group2 only
Group1 and Group2 only
Group1, Group2, Group3, Group4, and Group5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1 will be a member of:

Group3 only
Group4 only
Grou5 only
Group3, Group4, and Group5 only

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

Group1 only
Group2 only
Group1 and Group2 only
Group1, Group2, Group3, Group4, and Group5

NEW QUESTION 94
- (Exam Topic 3)
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 97
- (Exam Topic 3)
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.
How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Device1:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Device2:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Every three minutes for 15 minutes, then every 15 minutes for two hours, and then around every eight hours
If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:
Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Graphical user interface, text, application, email Description automatically generated

Platform	Frequency
iOS/iPadOS	Every 15 minutes for 1 hour, and then around every 8 hours
macOS	Every 15 minutes for 1 hour, and then around every 8 hours
Android	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 10/11 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 8.1	Every 5 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Box 2: Every 15 minutes for one hour, and then every eight hours iOS/iPadOS: Every 15 minutes for 1 hour, and then around every 8 hours
Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

NEW QUESTION 100
- (Exam Topic 3)
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 104
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to perform the following tasks for User1:
➤ Set the Usage location to Canada.
➤ Configure the Phone and Email authentication contact info for self-service password reset (SSPR). Which two settings should you configure in the Azure Active Directory admin center? To answer, select the
appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Manage

👤	Profile
🟩	Custom security attributes (Preview)
👥	Assigned roles
🏛	Administrative units
👥	Groups
▦	Applications
🔑	Licenses
🖥	Devices
🗝	Azure role assignments
🛡	Authentication methods

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 107
- (Exam Topic 3)
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 109
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.
You plan to integrate Intune with Microsoft Defender for Endpoint.
You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

A. Connectors and tokens
B. Premium add-ons
C. Microsoft Tunnel Gateway
D. Tenant enrollment

Answer: A

Explanation:
Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure Right Now.
As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.
Reference: https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/

NEW QUESTION 114
......

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

100% Actual & Verified — Instant Download, Please Click
Order The MD-102 Practice Test Here