MD-102 Q&As

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You have a Microsoft 365 subscription.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to configure the Out-of-box experience (OOBE) settings.

What should you create in the Microsoft Intune admin center?

A. an enrollment status page (ESP)

B. a deployment profile

C. a compliance policy

D. a PowerShell script

E. a configuration profile

Correct Answer: B

Use Windows Autopilot profiles on new devices to customize a customer\\'s out-of-box experience

In Partner Center, you can create Windows Autopilot deployment profiles and apply them to devices.

Note:

Create a new Autopilot profile

To create a new Autopilot profile, use the following steps:

1.

Sign in to Partner Center and select Customers.

2.

On the Customer List, select a customer.

3.

On the customer\\'s detail page, select Devices.

4.

Under Windows Autopilot profiles, select Add new profile.

5.

Enter the profile\\'s name and description and then configure the OOBE settings. Choose from:

Skip privacy settings in setup Disable local admin account in setup Automatically skip pages in setup (Includes Automatically select setup for work or school and Skip Cortana, OneDrive, and OEM registration setup pages) Skip end user license agreement (EULA)

6.

Select Submit when finished.

Reference: https://learn.microsoft.com/en-us/partner-center/autopilot

QUESTION 2

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. Client Authentication Issuers

B. Personal

C. Trusted Root Certification Authorities

Correct Answer: C

"Error Code: DLG_FLAGS_INVALID_CA" while login to Admin Console after enabling HTTPS in PowerCenter.

Solution

To resolve this issue, add the CA-signed certificates to the "Trusted Root Certification Authorities" in the browser. After adding the certificates, restart the browser.

Reference:

https://knowledge.informatica.com/s/article/578585

QUESTION 3

You have a Microsoft 365 tenant that contains the devices shown in the following table.

Name	Member of
Device1	Group1
Device2	Group1
Device3	Group1

The devices are managed by using Microsoft Intune.

You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the device security settings match the settings specified in the policy.

You discover that devices that are not members of Group1 are shown as Compliant.

You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not compliant.

What should you do from the Microsoft Intune admin center?

A. From Device compliance, configure the Compliance policy settings.

B. From Endpoint security, configure the Conditional access settings.

C. From Tenant administration, modify the Diagnostic settings.

D. From Policy1, modify the actions for noncompliance.

Correct Answer: A

There are two parts to compliance policies in Intune:

Compliance policy settings - Tenant-wide settings that are like a built-in compliance policy that every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that haven\\'t received any device compliance policies are compliant or noncompliant.

Device compliance policy - Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION 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

Correct Answer: D

An app configuration policy is a better way to deliver bookmarks to the Chrome browser on Android devices than a configuration profile.

To deliver bookmarks to the Chrome browser on Android devices, you would create an app configuration policy that specifies the bookmarks that you want to be added to the browser. The policy would then be assigned to your managed devices. Once the policy is applied, the bookmarks will be added to Chrome automatically. To deliver bookmarks using a configuration profile, you would need to create a file that contains the bookmark data. The file would then be pushed to your managed devices. Once the file is on the device, you would need to use a script to

import the bookmarks into Chrome.

This process is more complex and time-consuming than using an app configuration policy. It also requires you to create and maintain a bookmark file, which can be cumbersome if you have a large number of bookmarks or if you need to frequently update them. https://learn.microsoft.com/en-us/mem/intune/apps/apps-configure-chrome-android

---

QUESTION 5

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.

What should you configure?

A. the Azure Monitor agent

B. a device compliance policy

C. a Conditional Access policy

D. an Intune data collection policy

Correct Answer: D

https://learn.microsoft.com/en-us/mem/analytics/data-collection https://learn.microsoft.com/en-us/mem/analytics/enroll-intune#bkmk_onboard

---

QUESTION 6

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices that run Windows 11.

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

You need to add User1 to the Remote Desktop Users group on each marketing department device.

What should you configure?

A. an app configuration policy

B. a device compliance policy

C. an account protection policy

D. a device configuration profile

Correct Answer: C

https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy#manage-local-groups-on-windows-devices

QUESTION 7

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps.

You need to ensure that App1 is installed before App2 on every device.

What should you configure?

A. the App1 deployment configurations

B. a dynamic device group

C. a detection rule

D. the App2 deployment configurations

Correct Answer: D

Detection rules in Win32 apps are telling Intune how to tell if the application has been installed or not. Configure a dependency in the win32 app deployment screen even has this wording: "Software dependencies are applications that must be installed before this application can be installed"

Configure App1 first so that it\\'ll be selectable in the dependencies section

QUESTION 8

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

Correct Answer: B

Compliance policy settings include the following settings: Enhanced jailbreak detection (applies only to iOS/iPadOS) Etc.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION 9

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to deploy and manage Windows devices.

You have 100 devices from users that left your company.

You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

A. Deploy a new configuration profile to the devices.

B. Perform a Windows Autopilot reset on the devices.

C. Perform an in-place upgrade on the devices.

D. Perform a clean installation of Windows 11 on the devices.

Correct Answer: B

Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

Removes personal files, apps, and settings.

Reapplies a device\\'s original settings.

Sets the region, language, and keyboard to the original values.

Maintains the device\\'s identity connection to Azure AD.

Maintains the device\\'s management connection to Intune.

The Windows Autopilot Reset process automatically keeps information from the existing device:

Wi-Fi connection details.

Provisioning packages previously applied to the device.

A provisioning package present on a USB drive when the reset process is started.

Azure Active Directory device membership and MDM enrollment information.

SCEP certificates.

Windows Autopilot Reset blocks the user from accessing the desktop until this information is restored, including reapplying any provisioning packages. For devices enrolled in an MDM service, Windows Autopilot Reset also blocks until an

MDM sync is completed. When Autopilot reset is used on a device, the device\\'s primary user is removed. The next user who signs in after the reset will be set as the primary user.

Reference:

https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset

QUESTION 10

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

You use Microsoft Intune to manage devices.

You have a device named Devic1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1.

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

A. Deploy the Remote Help app to Device1.

B. Assign the Help Desk Operator role to User1.

C. Assign the Intune Administrator role to User1.

D. Assign a Microsoft 365 E5 license to User1.

E. Rerun device onboarding on Device1.

F. Assign the Remote Help add-on license to User1.

Correct Answer: ABF

QUESTION 11

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

A. Microsoft Defender for Endpoint Power BI app

B. Microsoft Secure Score

C. Endpoint Analytics

D. Microsoft 365 Defender portal

Correct Answer: B

QUESTION 12

You have a computer named Computer1 that runs Windows 10.

You need to configure User Account Control (UAC) to prompt administrators for their credentials.

Which settings should you modify?

A. Administrators Properties in Local Users and Groups

B. User Account Control Settings in Control Panel

C. Security Options in Local Group Policy Editor

D. User Rights Assignment in Local Group Policy Editor

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/useraccountcontrol-security-policy-settings

QUESTION 13

You need to configure Delivery Optimization to meet the technical requirements. Which download mode should you use?

A. Simple (99)

B. Group (2)

C. Internet (3)

D. HTTP Only (0)

E. Bypass (100)

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimizationreference#download-mode

QUESTION 14

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

A. Device restrictions (Windows 10 Team)

B. Identity protection

C. Custom

D. Device restrictions

Correct Answer: C

Windows client custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. These settings are typically used by mobile device manufacturers to control features on the device.

Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10

QUESTION 15

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers.

You need to prevent users from disabling Microsoft Defender Antivirus.

What should you do?

A. From the Microsoft Intune admin center, create a security baseline.

B. From the Microsoft 365 Defender portal, enable tamper protection.

C. From the Microsoft Intune admin center, create an account protection policy.

D. From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.

Correct Answer: B

Manage tamper protection for your organization using Microsoft 365 Defender portal

Tamper protection helps protect certain security settings, such as virus and threat protection, from being disabled or changed. If you\\'re part of your organization\\'s security team, you can turn tamper protection on (or off) tenant wide by using the Microsoft 365 Defender portal (https://security.microsoft.com).

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-tamper-protection-microsoft-365-defender