MD-102$^{\text{Q\&As}}$

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

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

https://www.pass2lead.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have a computer named Computer1 that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.

What should you do on Computer1?

A. Turn on Reputation-based protection

B. Enable Network Level Authentication (NLA)

C. Turn on Network Discovery

D. Configure the Remote Desktop Configuration service

Correct Answer: B

What is Network Level Authentication?

Network level authentication is used for authenticating Remote Desktop services, such as Windows RDP, and Remote Desktop Connection (RDP Client). You might also hear it called front authentication.

What is Network Level Authentication (NLA) used for?

Before you can start a remote desktop session, the user will need to authenticate themselves - ie, prove that they are who they say they are. Using network level authentication means that a false connection can\\'t be made, which would use

up CPU and cause a strain on the resources of the network. This offers a level of security against some cyberattacks such as Denial of Service attacks, where multiple requests are made all at once towards a network, overwhelming its ability

to cope. To combat this, you can turn on network level authentication to authenticate the user\\'s credentials before starting a remote access session. If the user\\'s credentials aren\\'t authenticated, then the connection is simply denied.

Reference:

https://www.atera.com/blog/what-is-network-level-authenticatio

QUESTION 2

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

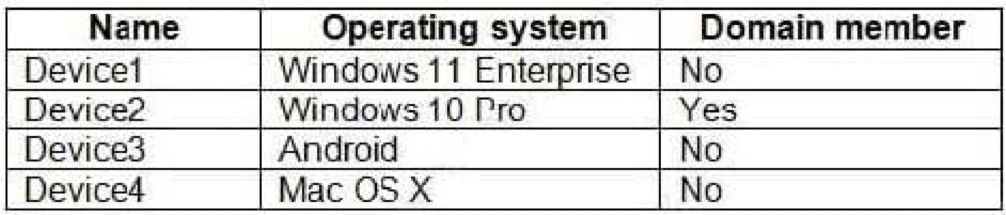
Correct Answer: D

Remote Management Users Group provides the effective rights for PS remote/remote connection. Remote Desktop Users doesn\\'t, would also require also having local Administrator permission, not least privilege having two roles where one defined role will do.

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_requirements?view=powershell-7.3 User permissions - To create remote sessions and run remote commands, by default, the current user must be a member of the Administrators group on the remote computer or provide the credentials of an administrator. Otherwise, the command fails.

QUESTION 3

You have the devices shown in the following table.



Name	Operating system	Domain member
Device1	Windows 11 Enterprise	No
Device2	Windows 10 Pro	Yes
Device3	Android	No
Device4	Mac OS X	No

You plan to implement Microsoft Defender for Endpoint.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint.

What should you identify?

A. Device1 only

B. Device2 only

C. Device1, Device2 only

D. Device1, Device2, and Device3 only

E. Device1, Device2, Device3, and Device4

Correct Answer: D

The Windows versions and Android are supported.

Note: You can onboard the following Windows operating systems:

Windows 8.1 Windows 10, version 1607 or later Windows 11 Windows Server 2012 R2 Windows Server 2016 Windows Server Semi-Annual Channel (SAC), version 1803 or later Windows Server 2019 Windows Server 2022

Note 2: By default, Microsoft Defender for Endpoint for Android includes and enables the web protection feature. Web protection helps to secure devices against web threats and protect users from phishing attacks. While this protection is enabled by default, there are valid reasons to disable it on some Android devices.

Incorrect:

* Not Device4

Network protection for macOS is now available for all Mac devices onboarded to Defender for Endpoint.

Reference:

https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection#bkmk_os

https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-manage-android

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-whatsnew

QUESTION 4

You have a Microsoft Intune subscription associated to an Azure AD tenant named contoso.com.

Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com.

You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment process. The solution must minimize the number of changes.

Which DNS records do you need?

A. one TXT record only

B. three CNAME records

C. three TXT records

D. one CNAME record only

Correct Answer: B

To simplify enrollment, create a domain name server (DNS) alias (CNAME record type) that redirects enrollment requests to Intune servers. Otherwise, users trying to connect to Intune must enter the Intune server name during enrollment.

If the company uses more than one UPN suffix, you need to create one CNAME for each domain name and point each one to EnterpriseEnrollment-s.manage.microsoft.com. For example, users at Contoso use the following formats as their email/UPN:

name@contoso.com name@us.contoso.com name@eu.contoso.com

Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium

QUESTION 5

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 6

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.

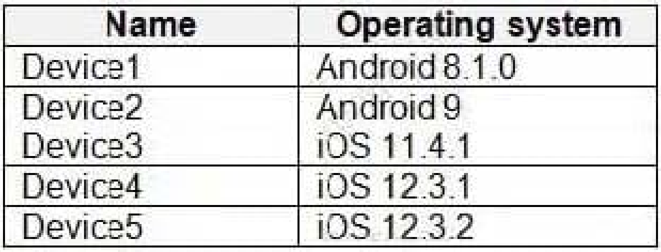
Correct Answer: DE

https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/create-windows-firewall-rules-in-intune https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#microsoft-defender-antivirus

QUESTION 7

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 App1?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: B

One for Android, and one for iOS.

Reference: https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

QUESTION 8

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 9

Your company has a Microsoft 365 subscription.

All the users in the finance department own personal devices that run iOS or Android. All the devices are enrolled in Microsoft Intune.

The finance department adds new users each month.

The company develops a mobile application named App1 for the finance department users.

You need to ensure that only the finance department users can download App1.

What should you do first?

A. Register App1 in Azure AD.

B. Add App1 to the vendor stores for iOS and Android applications.

C. Add App1 to a Microsoft Deployment Toolkit (MDT) deployment share.

D. Add App1 to Intune.

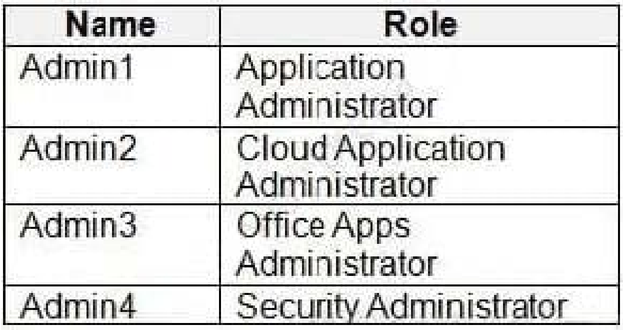
Correct Answer: D

Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.

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

QUESTION 10

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



Name	Role
Admin1	Application Administrator
Admin2	Cloud Application Administrator
Admin3	Office Apps Administrator
Admin4	Security Administrator

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization. Which users can download the Office customization file from the admin center?

A. Admin3 only

B. Admin1 and Admin3 only

C. Admin3 and Admin4 only

D. Admin1, Admin2, and Admin3 only

E. Admin1, Admin2, Admin3, Admin4

Correct Answer: C

QUESTION 11

You have following types of devices enrolled in Microsoft Intune:

1.

Windows 10

2.

Android

3.

iOS

For which types of devices can you create VPN profiles in Microsoft Intune admin center?

A. Windows 10 only

B. Windows 10 and Android only

C. Windows 10 and iOS only

D. Android and iOS only

E. Windows 10, Android, and iOS

Correct Answer: E

https://learn.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure#step-2---create-the-profile

QUESTION 12

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

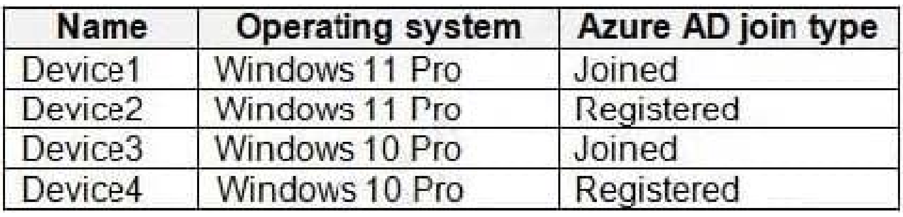
D. a device configuration profile

Correct Answer: C

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

QUESTION 13

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



Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

A. Device1 only

B. Device1 and Device2 only

C. Device1 and Device3 only

D. Device1, Device2, Device3, and Device4

Correct Answer: C

Windows subscription activation The subscription activation feature enables you to "step-up" from Windows Pro edition to Enterprise or Education editions. You can use this feature if you\\'re subscribed to Windows Enterprise E3 or E5 licenses. Subscription activation also supports step-up from Windows Pro Education edition to Education edition.

Devices must be Azure AD-joined or hybrid Azure AD joined. Workgroup-joined or Azure AD registered devices aren\\'t supported.

Reference: https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

QUESTION 14

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.

You need to remove User1 from the local Administrators group on all enrolled devices.

What should you configure?

A. a device compliance policy

B. an account protection policy

C. an app configuration policy

Correct Answer: B

Account protection policy for endpoint security in Intune

Use Intune endpoint security policies for account protection to protect the identity and accounts of your users and manage the built-in group memberships on devices.

Manage local groups on Windows devices

Use the Local user group membership (preview) profile to manage the users that are members of the built-in local groups on devices that run Windows 10 20H2 and later, and Windows 11 devices.

Reference:

https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy

QUESTION 15

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

1.

Ensure that you can manage the personal devices by using Microsoft Intune.

2.

Ensure that users can access company data seamlessly from their personal devices.

3.

Ensure that users can only sign in to their personal devices by using their personal account. What should you use to add the devices to Azure AD?

A. Azure AD registered

B. hybrid Azure AD join

C. Azure AD joined

Correct Answer: A

Azure AD registered devices are personal devices that are associated with Azure AD. This allows users to access company data from their personal devices without having to join the devices to the company\\'s domain. Additionally, Azure AD registered devices can be managed by Microsoft Intune.