MD-101 Q&As

Managing Modern Desktops

Pass Microsoft MD-101 Exam with 100% Guarantee

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

https://www.pass4itsure.com/md-101.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 are assigned the User administrator role.

An Azure AD security group named Group1 was deleted five days ago.

You need to restore Group1.

What should you do?

A. Modify the group expiration policy.

B. From Deleted groups, restore Group1.

C. Manually recreate Group1.

D. Ask a global administrator to restore Group1.

Correct Answer: B

QUESTION 2

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 Office 365 ProPlus suite to all the computers.

What should you do?

A. From the Device Management admin center, add an app.

B. From Microsoft Azure Active Directory (Azure AD), add an app registration.

C. From Microsoft Azure Active Directory (Azure AD), add an enterprise application.

D. From the Device Management admin center, create a Windows 10 device profile.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/windows/client-management/mdm/enterprise-app-management#application-management-goals

QUESTION 3

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. Apps, and then App protection policies

B. Apps, and then Monitor

C. Devices, and then Monitor

D. Reports, and the Device compliance

Correct Answer: B

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

QUESTION 4

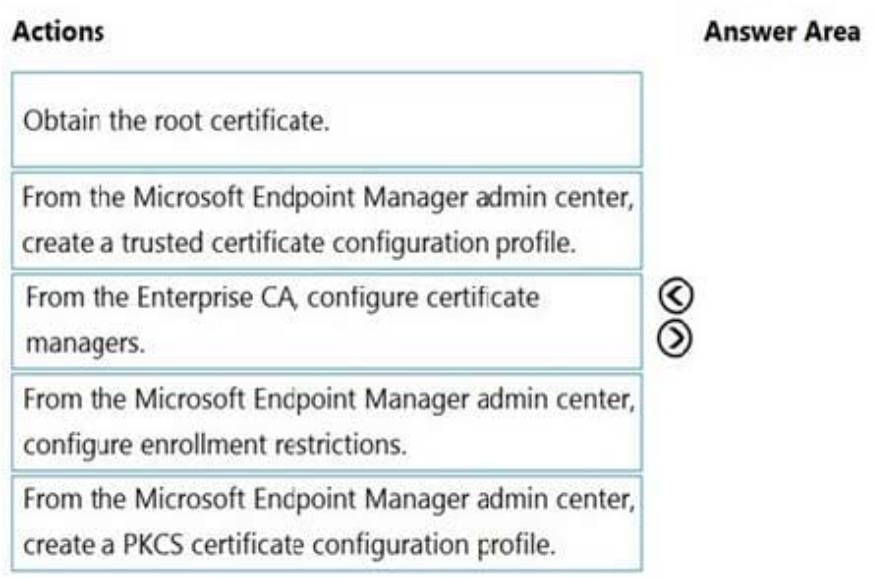
DRAG DROP

You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).

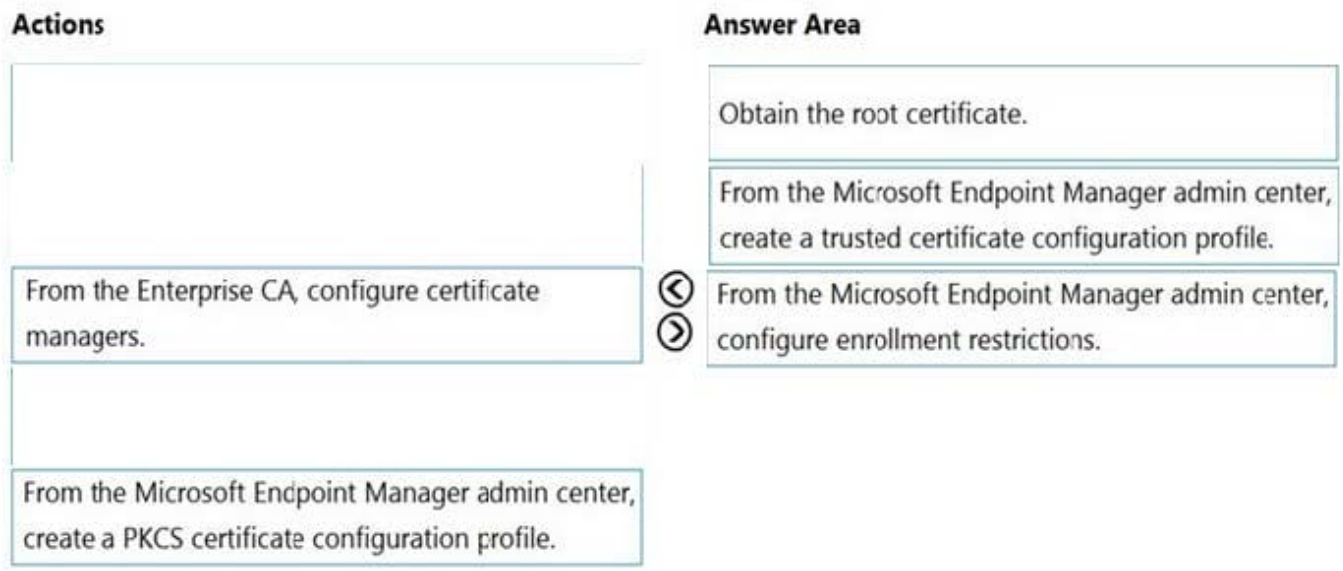
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

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

Select and Place:



Correct Answer:



Step 1: Obtain the root certificate.

Export the root certificate from the Enterprise CA.

To authenticate a device with VPN, WiFi, or other resources, a device needs a root or intermediate CA certificate.

Step 2: From the Microsoft Endpoint Manager admin center, create a trusted certificate profile

Create a trusted certificate profile

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

Select and go to Devices > Configuration profiles > Create profile.

3.

Enter the following properties:

Platform:

Profile: Select Trusted certificate. Or, select Templates > Trusted certificate.

Select Create.

4.

Etc.

Step 3: From the Microsoft Endpoint Manager admin center, create a PKCS certificate profile

Create a PKCS certificate profile

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

Select and go to Devices > Configuration profiles > Create profile.

3.

Enter the following properties:

Platform:

Profile: Select PKCS certificate. Or, select Templates > PKCS certificate.

Select Create.

4.

Etc.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

QUESTION 5

You manage one hundred Microsoft Azure Active Directory (Azure AD) joined Windows 10 devices.

You want to make sure that users are unable to join their home PC\\'s to Azure AD.

Which of the following actions should you take?

A. You should configure the Enrollment restriction settings via the Device enrollment blade in the Intune admin center.

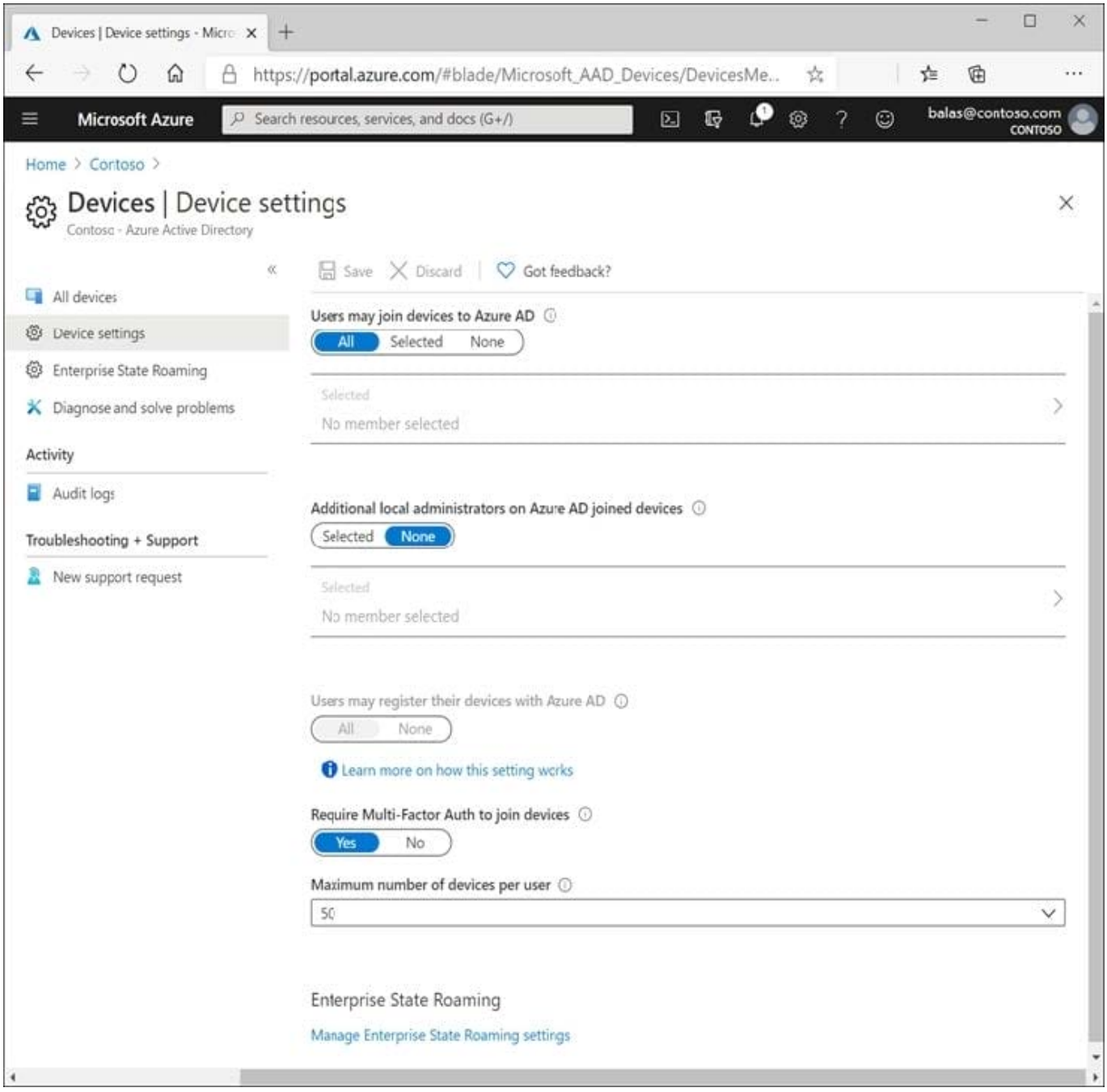
B. You should configure the Enrollment restriction settings via the Security and Compliance admin center.

C. You should configure the Enrollment restriction settings via the Azure Active Directory admin center.

D. You should configure the Enrollment restriction settings via the Windows Defender Security Center.

Correct Answer: C

Azure Active Directory (Azure AD) provides a central place to manage device identities and monitor related event information. Configure device settings.



* Users may join devices to Azure AD: This setting enables you to select the users who can register their devices as Azure AD joined devices. The default is All.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal