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

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

QUESTION 1

You have a Microsoft 365 subscription.

You need to provide a user the ability Security defaults and create Conditional Access policies. The solution must use the principle of least privilege.

Which role should you assign to the user?

A. Global Administrator

B. Conditional Access Administrator

C. Security Administrator

D. Intune Administrator

Correct Answer: B

To enable security defaults (or confirm they\\'re already enabled) Important You must be a Security Administrator, Conditional Access administrator, or Global Administrator to perform this task.

Note: Turn on multi-factor authentication

Multi-factor authentication (MFA) is a very important first step in securing your organization. Microsoft 365 Business Premium includes the option to use security defaults or Conditional Access policies to turn on MFA for your admins and user

accounts. For most organizations, security defaults offer a good level of sign-in security. But if your organization must meet more stringent requirements, you can use Conditional Access policies instead.

This article provides information about:

Security defaults (suitable for most businesses)

Conditional Access (for businesses with more stringent security requirements)

Reference:

https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-turn-on-mfa?

QUESTION 2

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 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

Correct Answer: C

Onboard Windows devices to Defender for Endpoint using Intune

Enable Microsoft Defender for Endpoint in Intune

The first step you take is to set up the service-to-service connection between Intune and Microsoft Defender for Endpoint. Set up requires administrative access to both the Microsoft Defender Security Center, and to Intune.

Onboard Windows devices

(After you connect Intune and Microsoft Defender for Endpoint, Intune receives an onboarding configuration package from Microsoft Defender for Endpoint. You use a device configuration profile for Microsoft Defender for Endpoint to deploy

the package to your Windows devices.

The configuration package configures devices to communicate with Microsoft Defender for Endpoint services to scan files and detect threats. The device also reports its risk level to Microsoft Defender for Endpoint based on your compliance

policies.

After onboarding a device using the configuration package, you don\\'t need to do it again.)

You can also onboard devices using:

*-> Endpoint detection and response (EDR) policy. Intune EDR policy is part of endpoint security in Intune. Use EDR policies to configure device security without the overhead of the larger body of settings found in device configuration profiles.

You can also use EDR policy with tenant attached devices, which are devices you manage with Configuration Manager.

Reference:

https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#enable-microsoft-defender-for-endpoint-in-intune

QUESTION 4

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 5

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

Correct Answer: B

Instead, from the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Management admin center, you configure the Windows Hello for Business enrollment options.

Reference: https://docs.microsoft.com/en-us/intune/protect/windows-hello