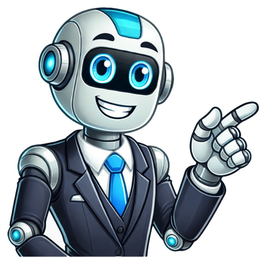
I'm not a bot



Md-102 practice test

Microsoft MD-102 certification is aimed at IT pros who manage and deploy Windows 10, Microsoft 365 technologies within an organization. The exam evaluates expertise in deploying, configuring, protecting, managing, and monitoring client devices and applications in a Microsoft 365 environment. This article provides valuable resources such as free practice questions to help sharpen skills and boost confidence. Moreover, it offers online MD-102 practice tests to assess readiness for the actual exam. Passing the MD-102 Certification can grant the Microsoft 365 Certified: Endpoint Administrator Associate distinction. The top MD-102 Practice Test Exam Questions & Answers feature expert-crafted questions for preparing the Endpoint Administrator (beta) certification with MD-102 exam questions and answers. Taking the online Microsoft MD-102 practice test before appearing for the actual MD-102 exam can determine preparation level. The article compiles the top 25 Microsoft's MD-102 actual exam questions under two domains: Manage identity and compliance, and covers topics such as restricting to a specific resource group on a subscription (Question 1), forest root domain objects not existing in other domains (Question 2), and setting up conditional access policies for granular device and location-based access to company data due to work from home policy (Question 3). User must exchange ActiveSync to enable access for employees using their home network, providing an additional layer of protection through multi-factor authentication (MFA). This feature allows organizations to set criteria for access and restrict devices that do not meet specific requirements, such as outdated security patches. Protect is an android specific app that check's your apps and devices for harmfull behavior. Pizzamania wants to digitize their orders so they give new iphones to their waiters. Which Apple option can deploy an enrollment profile "over the air" to bring device's into management? A company portal lets you securely access those resources, but it is not the correct answer. Enterprise work profile devices separate work and personal information, which is also not correct. Configurator for iPhone enables you to add Macs with T2 chip or Apple silicon to your organization, but that's not the right option. The correct answer is Device Enrollment Program (DEP) because it lets organizations deploy an enrollment profile "over the air" to bring device's into management. In Azure AD, if you're in a federated domain, you are redirected to your on-premises Secure Token Service (STS) server. This is true. Policy sets are not replacing existing concepts or objects. You can continue to assign individual objects and reference individual objects as part of a policy set. Therefore, any changes to those individual objects will be reflected in the policy set. Enrollment Status Page (ESP) and Microsoft Endpoint Manager (MEM) requirements can be complex. When deploying Win32 applications, it's essential to identify the correct field for adding the point of contact. The most suitable field to add this information is typically the Owner field, which indicates the name of the person in your organization who manages licenses or is the point of contact for the app. Other options are not correct because the Publisher and Developer fields represent information about the app's distributor, while the Name field may be visible in lists but does not accurately identify the point of contact. Given text here users were unable to log in Azure Active Directory (AD) even though they have valid credentials, but they were able to log in when connected corporate network. The possible reason behind this is that the user account was created before federated authentication services and therefore the old password hash doesn't match with the on-premises password, which makes it impossible for Azure AD DS to validate user's credentials. Are alternative methods of authentication for users who have forgotten their passwords? A. Security questions, Office phone, Mobile Phone, Alternative email address B. Mobile phone, Alternative email address, Security questions, Biometric thumbprint C. Office phone, Mobile phone, Text message to any phone number, Security questions D. Challenge Handshake Authentication Protocol, or CHAP, Office phone, Mobile Phone, Alternative email address Many LOB apps are written with limited security concerns, making them sometimes perform tasks like malware. To avoid issues, IT can monitor audit data and add exclusions for necessary apps to deploy attack surface reduction rules without impacting productivity. Option A is wrong because trigger alerts don't block users from accessing restricted content. Option B is also incorrect – enabling direct block mode affects LOB apps' daily functions. Option C is incorrect as warn mode shows a dialog box with an option to unblock content, potentially exposing it. Microsoft Advanced Protection Service (MAPS) provides the best antivirus defense on cloud services by enhancing standard real-time protection. It works seamlessly with Microsoft cloud services and is essential for preventing breaches from malware, making it a critical component of attack surface reduction rules. The Threat and Vulnerability Management module in Microsoft Defender for Endpoint prioritizes vulnerabilities considering factors such as A) the threat landscape, C) detections in your organization, and D) business context. This approach aims to reduce organizational exposure, harden endpoint surface area, and increase resilience. When running the exposure score, you may find that a device not active for nearly 90 days is not factored in. This is because devices must be active in the last 30 days to be considered in the evaluation (Option C). Different architecture types offer various tools for onboarding devices to Microsoft Defender for Endpoint. For instance, cloud-native requires Microsoft Endpoint Manager, while on-premises environments utilize Configuration Manager or Group Policy. Microsoft recommends using a deployment ring structure consisting of Pilot, Evaluate, and Full Deployment with Exit Criteria to manage and protect devices in an environment where devices are managed by Microsoft Endpoint Manager. The deployment rings help onboard devices in phases, ensuring potential issues are identified and addressed before moving to the next phase. For small-scale evaluation, 50 devices can be used as a test group. Configure capabilities, create a group, then verify config policies have been applied. In the context of role-based access, device groups can be created in Microsoft Defender for Endpoint to control who can take specific actions or see information by assigning the device group(s) to a user group. This involves previewing several devices that will be matched by the rule, creating a new device group with automation settings and specifying the matching rule that determines which devices belong to the group. User access is granted through user groups assigned to RBAC roles, allowing for control over related alerts and data, different auto-remediation settings, and specific remediation levels during automated investigations. By enabling tamper protection, you can help protect your security settings from being changed by locking them down and making them inaccessible through apps and methods. This feature is exclusively available when using Microsoft Defender Antivirus and cloud-based protection is enabled. EDR in block mode blocks malicious artifacts or behaviors that are detected on a device. You can receive targeted attack notifications from Microsoft Threat Experts through your portal's alerts dashboard and via email if you configure it. This feature is only available if you have an active Office 365 E5 or the Threat Intelligence add-on. Passing the MD-102 exam not only validates their expertise but also opens up new career opportunities in the ever-evolving field of IT administration. To excel in this certification, continuous learning and hands-on experience are key, ensuring that IT professionals remain well-equipped to address the challenges of managing modern desktops. You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table. You plan to create a compliance policy that has the following options enabled: Require Secure Boot to be enabled on the device and require the device to be at or under the machine risk score. You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains devices and groups. You add a Windows Autopilot deployment profile. For each department, you need to select the appropriate authentication method. For the research department, users cannot use mobile devices and must authenticate from unmanaged Linux devices using an alternative method. For the sales department, users must authenticate by using their mobile phone. To minimize administrative effort, you should use passwordless authentication for both departments.