MICROSOFT 365 CERTIFIED ENDPOINT ADMINISTRATOR (MD-102) PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://microsoft365certifiedendpointadministrator-md102.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **What is a recommended approach for Windows 10 device deployment using Microsoft Intune?**

   A. Use the Windows Autopilot deployment profile and add devices manually to Microsoft Intune.

   B. Use the Windows Autopilot deployment profile and import devices from Active Directory.

   C. Use the Windows Autopilot deployment profile and import devices from Configuration Manager.

   D. Use the Windows Autopilot deployment profile and leverage Azure Active Directory join.

2. **What is a key advantage of using Microsoft Intune for endpoint management?**

   A. It's limited to on-premises management only

   B. Only device-specific settings can be managed

   C. It allows for management of both mobile and desktop devices

   D. It requires a high level of technical expertise to manage

3. **For deploying a Windows-based kiosk device running a single application, which edition would you select?**

   A. Windows 10 Home

   B. Windows 10 Pro

   C. Windows 10 Enterprise

   D. Windows 10 in S mode

4. **Which component is required to deploy an operating system image to a new device using Microsoft Configuration Manager?**

   A. Windows Deployment Services (WDS)

   B. Microsoft Deployment Toolkit (MDT)

   C. Configuration Manager Client Package

   D. Configuration Manager Server Package

5. **In Microsoft Defender for Cloud Apps, which portal is used to create a new security policy for cloud applications?**

   A. Microsoft Defender Security Center.

   B. Microsoft Endpoint Manager admin center.

   C. Microsoft 365 Defender portal.

   D. Microsoft Azure portal.

6. Which service can be used for user account and access management in Microsoft 365?

A. Active Directory Domain Services (AD DS)

B. Azure Active Directory (Azure AD)

C. Windows Server Update Services (WSUS)

D. System Center Configuration Manager (SCCM)

7. What is required to enable automatic enrollment of devices in Microsoft Endpoint Manager?

A. Azure AD Premium P1 license

B. Azure AD Connect

C. Windows 10 Pro or Enterprise edition

D. Intune license

8. Which mechanism allows secure access to internal applications hosted on-premises from the cloud?

A. Azure AD Connect

B. Azure AD Application Proxy

C. Microsoft Defender for Endpoint

D. Microsoft Endpoint Configuration Manager

9. What is the correct method to disable a user account in Azure AD?

A. Search for the user account > Open the user profile > Click on Disable User > Confirm the action

B. Search for the user account > Click on More > Click on Disable > Confirm the action

C. Search for the user account > Click on More > Click on Block sign-in > Confirm the action

D. Search for the user account > Click on Delete > Confirm the action

10. Which tool should you use to generate a compliance report for updates and patches on Windows 10 devices?

A. Microsoft Endpoint Configuration Manager

B. Microsoft Intune

C. Windows Analytics

D. Microsoft System Center Operations Manager

Answers

1. D
2. C
3. D
4. A
5. C
6. B
7. A
8. B
9. C
10. C

Explanations

1. What is a recommended approach for Windows 10 device deployment using Microsoft Intune?

A. Use the Windows Autopilot deployment profile and add devices manually to Microsoft Intune.

B. Use the Windows Autopilot deployment profile and import devices from Active Directory.

C. Use the Windows Autopilot deployment profile and import devices from Configuration Manager.

D. Use the Windows Autopilot deployment profile and leverage Azure Active Directory join.

Using Windows Autopilot deployment profiles in conjunction with Azure Active Directory (Azure AD) join is a recommended approach for Windows 10 device deployment using Microsoft Intune due to several key factors. Windows Autopilot streamlines the deployment process by allowing devices to be configured directly from the cloud, enabling an automated setup experience for end-users. When devices are Azure AD joined, they seamlessly integrate with the organization's identity management policies and practices. This integration allows the devices to automatically enroll in Intune during the setup process, which simplifies the deployment workflow. Azure AD join provides benefits such as single sign-on to cloud resources and improved security through modern authentication mechanisms. It greatly enhances user experience by allowing users to sign in with their organizational credentials, and it also supports compliance and security policies imposed by the organization, providing a uniform experience whether the device is on-site or remote. While other methods mentioned can facilitate deployment, they may not offer the same level of cloud-centric simplicity, automated enrollment, and streamlined management that using Azure AD join in conjunction with Autopilot provides. The combination of these technologies ensures that organizations can rapidly deploy devices that are inherently ready for modern management, security, and usage scenarios.

2. What is a key advantage of using Microsoft Intune for endpoint management?

A. It's limited to on-premises management only

B. Only device-specific settings can be managed

C. It allows for management of both mobile and desktop devices

D. It requires a high level of technical expertise to manage

The key advantage of using Microsoft Intune for endpoint management lies in its ability to manage both mobile and desktop devices seamlessly. This capability is crucial in today's diverse IT environment, where organizations employ a mix of devices and platforms. Intune's unified endpoint management allows administrators to enforce policies, deploy applications, and ensure security across various device types, including smartphones, tablets, and computers. This flexibility supports organizations in maintaining security and compliance while providing end-users the freedom to choose the devices that best suit their needs. By enabling management for different operating systems and device categories from a single platform, Intune simplifies administrative tasks and improves overall efficiency in maintaining an organization's endpoint landscape. The other choices reflect limitations that do not align with the broad capabilities offered by Intune.

3. For deploying a Windows-based kiosk device running a single application, which edition would you select?

A. Windows 10 Home

B. Windows 10 Pro

C. Windows 10 Enterprise

D. Windows 10 in S mode

Selecting Windows 10 in S mode for deploying a Windows-based kiosk device running a single application is the ideal choice due to its streamlined and secure nature. Windows 10 in S mode is designed for performance and security, allowing devices to run only applications from the Microsoft Store. This makes it particularly suitable for kiosk setups, where a single-focus application is preferred for user interaction. Kiosk devices benefit from operating in a controlled environment where administrators can lock down the system effectively and limit the potential for misuse or unauthorized access. Windows 10 in S mode provides a locked-down experience that helps ensure the device remains focused on a specific task without the distractions and vulnerabilities that come from allowing full access to other applications and system settings. This edition also simplifies management and updates, offering a seamless experience when users only need to interact with a single, pre-approved application. The automatic updates from the Microsoft Store also support reliability, which is critical in a kiosk environment where uptime is essential for user experience. Thus, for a kiosk running a single application, Windows 10 in S mode provides the necessary features for security and ease of use.

4. Which component is required to deploy an operating system image to a new device using Microsoft Configuration Manager?

A. Windows Deployment Services (WDS)

B. Microsoft Deployment Toolkit (MDT)

C. Configuration Manager Client Package

D. Configuration Manager Server Package

To deploy an operating system image to a new device using Microsoft Configuration Manager, Windows Deployment Services (WDS) is essential because it provides the necessary infrastructure for network-based installations of operating systems. Specifically, WDS enables the deployment of Windows images to client computers over the network, which aligns with the processes utilized during OSD (Operating System Deployment) within Configuration Manager. WDS functions by allowing the deployment of images stored in a centralized repository directly to clients, eliminating the need for physical media. It works in concert with Configuration Manager to facilitate deployments in environments where multiple devices need to be set up efficiently, making it a key component in the overall image deployment strategy. While other tools like the Microsoft Deployment Toolkit (MDT) are useful for creating and managing deployment processes, and packages related to the Configuration Manager Client and Server are crucial for managing and maintaining devices, the core function of deploying an OS image relies specifically on the capabilities provided by WDS.

5. In Microsoft Defender for Cloud Apps, which portal is used to create a new security policy for cloud applications?

A. Microsoft Defender Security Center.

B. Microsoft Endpoint Manager admin center.

C. Microsoft 365 Defender portal.

D. Microsoft Azure portal.

The Microsoft 365 Defender portal is the correct choice for creating a new security policy for cloud applications in Microsoft Defender for Cloud Apps. This portal serves as a central location where security teams can manage their organization's security posture across various Microsoft services, including Microsoft Defender for Cloud Apps. In this environment, users can define and enforce policies that help protect sensitive data and govern the use of cloud applications within the organization. By utilizing the features of the Microsoft 365 Defender portal, administrators can configure real-time alerts, monitor application activities, and implement restrictions based on organizational requirements. Other portals listed may serve different functions: the Microsoft Defender Security Center is more focused on broader security management functions, the Microsoft Endpoint Manager admin center is dedicated to managing devices and applications within an organization, while the Microsoft Azure portal primarily deals with Azure services and resources. Thus, from a functionality and contextual standpoint regarding security policy management for cloud applications, the Microsoft 365 Defender portal is the most appropriate choice.

6. Which service can be used for user account and access management in Microsoft 365?

A. Active Directory Domain Services (AD DS)

B. Azure Active Directory (Azure AD)

C. Windows Server Update Services (WSUS)

D. System Center Configuration Manager (SCCM)

Azure Active Directory (Azure AD) serves as the primary service for user account and access management in Microsoft 365. It provides a comprehensive set of identity management capabilities, allowing organizations to create and manage user accounts, enforce access policies, and facilitate single sign-on (SSO) for various applications. With Azure AD, users can access Microsoft 365 apps and services through a unified authentication platform, which enhances security and user experience. Additionally, Azure AD supports features such as multi-factor authentication (MFA), conditional access policies, and self-service password reset, all of which are crucial for managing user access securely in a cloud-based environment. This makes Azure AD a vital component in ensuring that organizations can manage their users effectively, maintain security compliance, and streamline access to resources. The other services mentioned, while they play important roles within IT environments, do not focus on user account and access management in the context of Microsoft 365. Active Directory Domain Services (AD DS) is primarily used in on-premises environments for directory services but is not optimized for cloud-based identity management. Windows Server Update Services (WSUS) is designed for managing updates and patches for Windows operating systems, and System Center Configuration Manager (SCCM) focuses on system management rather than user

7. What is required to enable automatic enrollment of devices in Microsoft Endpoint Manager?

A. Azure AD Premium P1 license

B. Azure AD Connect

C. Windows 10 Pro or Enterprise edition

D. Intune license

To enable automatic enrollment of devices in Microsoft Endpoint Manager, an Azure AD Premium P1 license is required because it provides the necessary features for conditional access and management of devices within an organization. This license allows for automatic enrollment specifically in a hybrid environment and is essential for employing advanced management capabilities. While Azure AD Connect is useful for synchronizing on-premises directories with Azure Active Directory, it does not directly pertain to the automatic enrollment process itself. Windows 10 Pro or Enterprise edition is indeed needed to utilize certain features of Microsoft Endpoint Manager but does not enable automatic enrollment by itself. An Intune license is also necessary for mobile device management (MDM) capabilities, but it is the Azure AD Premium P1 license that specifically allows for automatic enrollment functionality.

8. Which mechanism allows secure access to internal applications hosted on-premises from the cloud?

A. Azure AD Connect

B. Azure AD Application Proxy

C. Microsoft Defender for Endpoint

D. Microsoft Endpoint Configuration Manager

The Azure AD Application Proxy is specifically designed to provide secure remote access to on-premises applications from users outside the corporate network. This service allows organizations to publish their internal applications to be accessible via the internet without needing to expose the applications directly to the public network, thus enhancing security. By utilizing the Azure AD Application Proxy, users can authenticate through Azure Active Directory, ensuring that access is managed and secure. The proxy routes the traffic to the on-premises application while maintaining controls through Azure AD, providing features like pre-authentication and user access policies. This makes it an ideal solution for organizations looking to extend the reach of their internal applications while protecting sensitive data and meeting compliance requirements. Other options listed, while relevant to different use cases within the Microsoft 365 ecosystem, do not focus specifically on securely enabling access to on-premises applications from the cloud.

9. What is the correct method to disable a user account in Azure AD?

A. Search for the user account > Open the user profile > Click on Disable User > Confirm the action

B. Search for the user account > Click on More > Click on Disable > Confirm the action

C. Search for the user account > Click on More > Click on Block sign-in > Confirm the action

D. Search for the user account > Click on Delete > Confirm the action

The correct method to disable a user account in Azure Active Directory is to block the sign-in for that user. This action effectively prevents the user from accessing resources while keeping the account in the directory for future reference or reactivation if necessary. Blocking the sign-in allows organizations to manage user access without fully deleting the account, which would remove all associated data and history. The process involves searching for the user account, clicking on "More" to access additional options, selecting "Block sign-in," and then confirming the action. This method is preferred for maintaining user management and security compliance without permanently losing account data. Other options involve either disabling the user in a way that might not be standard practice or deleting the account entirely, which would permanently remove the user's access and data, rather than just suspending it temporarily.

10. Which tool should you use to generate a compliance report for updates and patches on Windows 10 devices?

A. Microsoft Endpoint Configuration Manager

B. Microsoft Intune

C. Windows Analytics

D. Microsoft System Center Operations Manager

The tool that is best suited for generating a compliance report for updates and patches on Windows 10 devices is Windows Analytics. This service, part of the Microsoft 365 suite, provides insights into the deployment status, compliance, and health of updates for Windows devices. Windows Analytics includes components like Device Health and Update Compliance, which specifically help administrators track the installation status of feature and quality updates across all managed devices. By utilizing this tool, organizations can assess whether devices are compliant with required updates and identify any areas that need attention, making it integral for maintaining optimal security and performance in an enterprise environment. While other tools like Microsoft Endpoint Configuration Manager and Microsoft Intune are also capable of managing updates and patches, they focus more on deployment management and policy enforcement rather than compliance reporting. System Center Operations Manager is primarily geared toward infrastructure and application monitoring, which does not specifically target compliance reporting for updates.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://microsoft365certifiedendpointadministrator-md102.examzify.com

We wish you the very best on your exam journey. You've got this!