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

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **What method allows for dynamic management and update of device configurations based on user and group memberships?**

   A. Intune Autopilot

   B. Group Policy Object (GPO)

   C. Windows Deployment Services (WDS)

   D. System Center Configuration Manager (SCCM)

2. **Which deployment method should be chosen to ensure an application does not interfere with others on users' devices?**

   A. Required installation

   B. Available installation

   C. Required application

   D. Available application

3. **When using Microsoft Endpoint Manager, which report would show the software installed on all managed devices?**

   A. Software inventory report

   B. Hardware inventory report

   C. Compliance report

   D. Configuration Manager dashboard

4. **Which deployment method is suitable for configuring threat detection settings on all Windows client devices using Microsoft Defender for Endpoint?**

   A. Configure the settings manually using the Windows Security app.

   B. Create a new policy using Group Policy for settings.

   C. Deploy a policy using Microsoft Intune for settings.

   D. Create a configuration baseline using Microsoft Endpoint Configuration Manager.

5. **What is true regarding device enrollment using Microsoft Configuration Manager?**

   A. Microsoft Configuration Manager can enroll only Windows devices

   B. Microsoft Configuration Manager can enroll only non-Windows devices

   C. Microsoft Configuration Manager can enroll both Windows and non-Windows devices

   D. Microsoft Configuration Manager does not support device enrollment

SAMPLE

6. Which authentication method ensures that all enrolled devices use a secure method for device enrollment?

A. Usernames and passwords

B. Biometric authentication

C. PIN authentication

D. Certificate-based authentication

7. What should be done if some devices are not receiving Microsoft Defender security updates?

A. Reinstall Windows on each device

B. Update devices with only essential software

C. Use Windows Update for Business to deploy updates

D. Delay updates until a future time

8. Which Windows edition allows management of updates on all devices in a large organization?

A. Windows 10 Home

B. Windows 10 Pro

C. Windows 10 Enterprise

D. Windows 10 Education

9. For users requiring access to specific apps and settings, which profile type should be used?

A. User profile

B. Device profile

C. Shared device configuration profile

D. Endpoint protection profile

10. What is the primary benefit of implementing Windows Autopilot?

A. It simplifies the device deployment process

B. It is only suitable for large organizations

C. It restricts user customizations

D. It requires specialized training to use

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What method allows for dynamic management and update of device configurations based on user and group memberships?

A. Intune Autopilot

B. Group Policy Object (GPO)

C. Windows Deployment Services (WDS)

D. System Center Configuration Manager (SCCM)

The correct method for dynamically managing and updating device configurations based on user and group memberships is Intune Autopilot. This service is designed to simplify the deployment and management of Windows 10 or later devices. With Autopilot, organizations can tailor the out-of-the-box experience for users, enabling settings and configurations that align with specific user roles or group memberships. When a device is enrolled using Autopilot, any configurations, applications, or policies can be dynamically assigned based on the user's Azure Active Directory (Azure AD) group memberships. This means that as users change roles or move between departments, the device's configuration can automatically update to reflect their current role, ensuring they have the tools and settings necessary for their work without the need for manual reconfiguration. This capability is particularly beneficial for organizations looking to streamline device management and ensure compliance with policies while providing a personalized experience for users as they join or leave different groups. In contrast, the other methods listed, such as Group Policy Objects, Windows Deployment Services, and System Center Configuration Manager, typically do not offer the same level of dynamic user and group-based management for device configurations in a cloud-first or modern management scenario as Intune Autopilot does.

2. Which deployment method should be chosen to ensure an application does not interfere with others on users' devices?

A. Required installation

B. Available installation

C. Required application

D. Available application

The choice of deployment method that ensures an application does not interfere with others on users' devices is to use the required installation method. When an application is set up for required installation, it is automatically installed on users' devices without requiring any action on their part. This approach minimizes the risk of conflicts that could arise from user-initiated installations, as the application is installed in a controlled and predictable manner. By using the required installation method, administrators can ensure that the application is compatible with existing software and is installed in a way that adheres to organizational policies. This eliminates variability in installation procedures among users, reducing the likelihood of installation-related issues and ensuring that all necessary prerequisites are satisfied automatically. Additionally, required installations often come with configurations that help avoid potential interference with other applications, promoting a stable environment on users' devices. On the other hand, methods like available installation place the onus on users to install the application themselves, which can lead to inconsistencies in how the application is set up and its interactions with other applications.

SAMPLE

3. When using Microsoft Endpoint Manager, which report would show the software installed on all managed devices?

A. Software inventory report

B. Hardware inventory report

C. Compliance report

D. Configuration Manager dashboard

The software inventory report is specifically designed to display a list of software installed on all managed devices within Microsoft Endpoint Manager. This report aggregates data from the managed devices to provide a comprehensive overview of which applications are installed, their versions, and additional relevant details. This is crucial for administrators who need to track software assets, ensure compliance with software licenses, and manage updates or configurations effectively. By utilizing this report, administrators can quickly identify any unauthorized or outdated software present on devices, helping to enhance security and maintain a consistent software environment across the organization. In contrast, other reports such as the hardware inventory report focus on the physical components and specifications of the devices rather than the software installed. The compliance report addresses security and configuration compliance based on predetermined policies but does not provide a detailed list of software. Meanwhile, the Configuration Manager dashboard offers a high-level overview of various metrics and statuses but does not specifically drill down into installed software details like the software inventory report does.

4. Which deployment method is suitable for configuring threat detection settings on all Windows client devices using Microsoft Defender for Endpoint?

A. Configure the settings manually using the Windows Security app.

B. Create a new policy using Group Policy for settings.

C. Deploy a policy using Microsoft Intune for settings.

D. Create a configuration baseline using Microsoft Endpoint Configuration Manager.

Using Microsoft Intune to deploy a policy for configuring threat detection settings on all Windows client devices is an effective and efficient method for several reasons. Intune provides a centralized management platform that allows administrators to apply security settings across all enrolled devices seamlessly. With Intune, you can leverage Mobile Device Management (MDM) capabilities to ensure that all devices adhere to specific compliance and security configurations, including threat detection settings. Additionally, Intune allows for the easy deployment of policies that can be updated and adjusted as needed, ensuring that any changes to threat detection can be propagated quickly across all devices. This capability minimizes the risk of inconsistent application of security settings, which is crucial for maintaining a robust security posture in an organization. In contrast, manually configuring settings using the Windows Security app may result in inconsistencies across devices, as this method does not allow for centralized management. Creating a Group Policy for settings might be more suited for on-premises environments and wouldn't apply to remote or cloud-based scenarios as effectively. Similarly, while creating a configuration baseline with Microsoft Endpoint Configuration Manager is a viable option, it typically involves more complex setup and management processes compared to the streamlined approach offered by Intune, especially in a modern desktop management context.

SAMPLE

5. What is true regarding device enrollment using Microsoft Configuration Manager?

A. Microsoft Configuration Manager can enroll only Windows devices

B. Microsoft Configuration Manager can enroll only non-Windows devices

C. Microsoft Configuration Manager can enroll both Windows and non-Windows devices

D. Microsoft Configuration Manager does not support device enrollment

Microsoft Configuration Manager is designed to manage a wide range of devices within an organization's IT ecosystem. It has robust capabilities that allow for the enrollment of both Windows and non-Windows devices, which makes it a versatile tool for endpoint management. The support for enrollment of Windows devices is well-established, as Configuration Manager is deeply integrated into the Windows operating system and can leverage native Windows management features effectively. Additionally, organizations can use Configuration Manager to manage non-Windows devices, such as macOS computers and Linux servers, through various configurations and extensions. This dual capability enhances the administration of devices across different operating systems, providing a unified approach to device management. The ability to manage both types of devices allows IT administrators to consolidate management tasks under one platform, ensuring a more streamlined and efficient process for maintaining security, compliance, and performance across all endpoints in an organization.

6. Which authentication method ensures that all enrolled devices use a secure method for device enrollment?

A. Usernames and passwords

B. Biometric authentication

C. PIN authentication

D. Certificate-based authentication

Certificate-based authentication is the most secure method for device enrollment because it relies on the use of digital certificates, which are much harder to forge or compromise than traditional credentials. When a device is enrolled using certificate-based authentication, a unique certificate is issued to the device that confirms its identity and establishes a trusted relationship between the device and the network. This ensures that only authorized devices can access the resources within the organization, thereby maintaining the integrity and security of the network. On the other hand, usernames and passwords can be susceptible to various attacks such as phishing or brute force, making them less secure for device enrollment. Similarly, biometric authentication, while more secure than passwords, can still be vulnerable to spoofing attacks and may not be universally supported across all devices. PIN authentication adds a layer of security over usernames and passwords, but it still falls short of the robust protections offered by certificate-based methods. Overall, utilizing certificate-based authentication for device enrollment not only enhances security but also streamlines the process, ensuring that only trusted and enrolled devices are allowed access to the network.

SAMPLE

7. What should be done if some devices are not receiving Microsoft Defender security updates?

A. Reinstall Windows on each device

B. Update devices with only essential software

C. Use Windows Update for Business to deploy updates

D. Delay updates until a future time

Utilizing Windows Update for Business to deploy updates is the most effective solution when some devices are not receiving Microsoft Defender security updates. This approach allows administrators to manage how updates are delivered to devices within an organization. By leveraging this feature, IT administrators can ensure that updates are timely and consistent across all endpoint devices, thus enhancing the security posture of their environment. Windows Update for Business enables policies to be set that can determine when and how updates are applied, such as deferring updates to ensure that devices receive the necessary security patches without interruption to user productivity. This method also allows for monitoring and troubleshooting the update process, making it easier to identify and resolve any issues that may be preventing updates from being delivered. In contrast, reinstalling Windows on each device would be a tedious and time-consuming solution that could lead to data loss and other complications. Updating devices with only essential software does not address the underlying issue of missing security updates, as it could leave the devices exposed to vulnerabilities. Delaying updates until a future time can exacerbate security risks, particularly in environments where threats are constantly emerging. Therefore, employing Windows Update for Business provides a structured and effective way to manage and ensure the timely delivery of security updates across all devices.

8. Which Windows edition allows management of updates on all devices in a large organization?

A. Windows 10 Home

B. Windows 10 Pro

C. Windows 10 Enterprise

D. Windows 10 Education

The Windows 10 Enterprise edition is specifically designed for large organizations and includes advanced features for managing updates across various devices. It provides powerful tools such as Windows Update for Business, which allows IT administrators to control and manage the distribution of updates across the organization efficiently. This functionality includes features like maintaining update compliance, configuring update deferral policies, and managing the deployment of feature updates. Furthermore, Windows 10 Enterprise is built to support complex organizational needs, offering enterprise-grade security features and management capabilities that are not present in other editions. This includes support for Group Policy, Mobile Device Management (MDM), and advanced analytics through Microsoft Endpoint Manager, ensuring that updates can be tailored according to the organization's unique requirements. In contrast, other editions like Windows 10 Home lack the necessary management capabilities for large-scale environments, making them unsuitable for organizational use where update management and security are paramount. Windows 10 Pro provides some level of management tools but doesn't offer the extensive capabilities found in the Enterprise edition, which are essential for overseeing updates in a large organizational context. Windows 10 Education, while similar to Enterprise in some aspects, is primarily aimed at educational institutions and may not include all enterprise-specific features for broader organizational management.

SAMPLE

9. For users requiring access to specific apps and settings, which profile type should be used?

A. User profile

B. Device profile

C. Shared device configuration profile

D. Endpoint protection profile

The user profile type is the most appropriate choice for users requiring access to specific applications and settings. A user profile is designed to personalize the user experience by allowing settings, preferences, and applications to be configured specifically for an individual user. This ensures that when the user logs in to a device, they have access to the tools and resources they need. User profiles allow for tailored settings such as configurations for desktop layouts, access to specific applications, and user-specific policies that can enhance productivity and security based on the individual's role or needs. This personal approach fosters a better user experience, as each user's profile can be adjusted based on their job requirements, which is essential in environments where users may have varied responsibilities and access needs. Other types of profiles, while useful in certain contexts, do not focus specifically on individual user customization. For instance, device profiles are intended for managing settings and configurations at the device level rather than the individual user level. Shared device configuration profiles are meant for devices that multiple users utilize, which wouldn't cater to specific needs of individual users. Endpoint protection profiles focus specifically on security measures rather than access to applications and settings. Therefore, user profiles are the most suitable choice for managing user-specific app access and settings.

10. What is the primary benefit of implementing Windows Autopilot?

A. It simplifies the device deployment process

B. It is only suitable for large organizations

C. It restricts user customizations

D. It requires specialized training to use

Implementing Windows Autopilot primarily simplifies the device deployment process, allowing organizations to provision new devices with minimal IT intervention. This cloud-based solution streamlines the setup and configuration of Windows devices, enabling them to be ready for use directly out of the box. With Autopilot, the deployment process is automated, which reduces the time and resources needed for IT personnel to configure devices manually. Device setup can be tailored based on specific requirements, allowing for a more efficient onboarding experience for users. While it is beneficial for organizations of any size, including small and medium-sized businesses, its ability to simplify workflows and enhance user experience makes it a preferred choice for many. This ease of deployment inherently assists in scaling operations, especially in environments where rapid provisioning or remote work is essential. Other options such as suitability for only large organizations, restrictions on user customizations, and requirements for specialized training do not accurately reflect the core advantages of Windows Autopilot, which is primarily centered around simplifying and accelerating the deployment process.

SAMPLE

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!

SAMPLE