Microsoft 365 Certified Endpoint Administrator (MD-102) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

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

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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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. **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

2. **When managing multiple Windows editions, which option provides the best control over updates?**

   A. Windows 10 Pro

   B. Windows 10 Enterprise

   C. Windows 10 Home

   D. Windows 10 Education

3. **To specify device drivers during a Windows 10 deployment using Microsoft Configuration Manager, what should you do?**

   A. Manually install drivers after OS installation.

   B. Create a bootable USB drive with drivers.

   C. Create a driver package and specify it in the task sequence.

   D. None of the above.

4. **Which Azure feature allows you to manage user roles and access for applications?**

   A. Role-based access control (RBAC)

   B. Azure AD Privileged Identity Management

   C. Network security

   D. Application Security Groups

5. **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

6. **Which tool can an Endpoint Administrator use to generate reports on non-compliant devices?**

   A. Microsoft Word

   B. Microsoft Intune

   C. Microsoft Excel

   D. Microsoft PowerPoint

7. **Which feature ensures only approved applications can be installed on managed devices?**

   A. Microsoft Intune

   B. Microsoft Store for Business

   C. Microsoft Endpoint Configuration Manager

   D. Windows Analytics

8. **Which report provides the necessary information to monitor device compliance within an organization?**

   A. Intune Device Compliance report

   B. Intune Software Update Status report

   C. Azure AD Activity Report

   D. Azure AD Sign-In Report

9. **To restrict device enrollment to only certain users, which option should be implemented?**

   A. Allow only users who are members of a specific Azure AD group to enroll devices

   B. Allow any user to enroll devices

   C. Allow users to enroll devices with a one-time enrollment token

   D. Require users to provide a certificate for device enrollment

10. **Which feature allows admins to define conditions under which users can access applications and data in Azure AD?**

   A. A) App protection policies

   B. B) Conditional access policies

   C. C) Identity Protection

   D. D) Enrollment restrictions

Answers

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

Explanations

1. **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.

2. **When managing multiple Windows editions, which option provides the best control over updates?**

   A. Windows 10 Pro

   B. Windows 10 Enterprise

   C. Windows 10 Home

   D. Windows 10 Education

Windows 10 Enterprise offers the most robust control over updates when managing multiple Windows editions. This version includes advanced features specifically designed for larger organizations, such as group policy management, Windows Autopilot, and the ability to defer updates more extensively compared to other Windows editions. With Windows 10 Enterprise, organizations can implement various update policies to manage when and how updates are applied, allowing for more strategic deployment that minimizes disruption. The edition also provides access to the Windows Update for Business feature, which enables IT administrators to define update rings that can control the rollout of updates based on organizational needs. While Windows 10 Pro also has some control over updates, its features are more limited compared to Enterprise. Windows 10 Home provides minimal management capabilities, and Windows 10 Education, while better than Home, does not match the comprehensive management capabilities of Enterprise. Therefore, for organizations needing the best control over updates across multiple systems, Windows 10 Enterprise is the most suitable choice.

3. To specify device drivers during a Windows 10 deployment using Microsoft Configuration Manager, what should you do?

A. Manually install drivers after OS installation.

B. Create a bootable USB drive with drivers.

C. Create a driver package and specify it in the task sequence.

D. None of the above.

Creating a driver package and specifying it in the task sequence is the correct approach when deploying Windows 10 using Microsoft Configuration Manager. This method allows administrators to streamline the installation process by incorporating necessary drivers for specific hardware directly into the deployment workflow. By using a driver package, you ensure that all required drivers are available during the installation phase, which enhances compatibility and helps avoid potential issues that may arise if drivers are missing or need to be installed post-deployment. Additionally, maintaining and managing driver packages within Configuration Manager facilitates easier updates and organization of drivers as new versions become available or as new hardware is introduced into the environment. This approach is generally more efficient compared to manually installing drivers after the operating system installation, which can be time-consuming and may lead to an inconsistent configuration across multiple devices. Creating a bootable USB drive with drivers also lacks the automation and integration that Configuration Manager provides, thereby not leveraging the full capabilities of the deployment tools available.

4. Which Azure feature allows you to manage user roles and access for applications?

A. Role-based access control (RBAC)

B. Azure AD Privileged Identity Management

C. Network security

D. Application Security Groups

Role-based access control (RBAC) is the feature that allows administrators to manage user roles and access for applications within Azure. It enables a fine-grained access management model to assign permissions to users based on their defined roles. With RBAC, you can specify who has access to various Azure resources, what actions they can perform, and on which resources they can perform those actions. This helps to ensure that users have the appropriate level of access according to their job functions, enhancing security and compliance in managing resources. In contrast, while Azure AD Privileged Identity Management provides management of privileged accounts and their access levels, its focus is more on overseeing the assignment and use of privileged roles rather than general user roles for application access. Network security pertains to securing your network infrastructure and data flows but does not govern user roles and permissions directly. Application Security Groups are primarily used for managing network security within Azure but do not manage user permissions or roles for applications.

5. 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.

6. Which tool can an Endpoint Administrator use to generate reports on non-compliant devices?

A. Microsoft Word

B. Microsoft Intune

C. Microsoft Excel

D. Microsoft PowerPoint

An Endpoint Administrator can utilize Microsoft Intune to generate reports on non-compliant devices due to its comprehensive device management capabilities. Intune is specifically designed for managing and securing devices in an organization, and as part of its functionality, it provides reporting features that allow administrators to assess compliance status across devices. Using Intune, administrators can view detailed reports that include information about devices that do not meet the defined compliance policies. This includes aspects like operating system updates, security settings, application compliance, and other device configurations that are crucial for maintaining organizational security standards. The ability to generate these reports helps in ensuring that all devices are compliant with organizational policies, which is essential for risk management and maintaining a secure IT environment. In contrast, tools like Word, Excel, and PowerPoint are not specifically focused on device management or compliance reporting, making them unsuitable for this particular task. While Excel might be used to analyze data if reports are exported, it does not inherently contain the functionality to generate compliance reports on its own, as Intune does.

7. Which feature ensures only approved applications can be installed on managed devices?

A. Microsoft Intune

B. Microsoft Store for Business

C. Microsoft Endpoint Configuration Manager

D. Windows Analytics

The choice of the Microsoft Store for Business as the appropriate feature that ensures only approved applications can be installed on managed devices is accurate because this platform allows organizations to create a curated list of applications that can be deployed and installed on managed endpoints. By leveraging the Microsoft Store for Business, administrators can specify which applications are available for users, ensuring compliance with internal policies concerning software usage and security. This feature provides enhanced control over the application landscape in the organization, thereby reducing the risk associated with unauthorized or harmful applications being installed on managed devices. It facilitates a more secure environment where only vetted applications, which meet the organization's compliance and security standards, can be made available for installation by users. Other solutions, while capable in their operations, focus on different aspects of device management. Microsoft Intune offers comprehensive mobile device management and mobile application management capabilities, but the specific function of controlling the application installation process directly through an approved list is tied to the features within the Microsoft Store for Business. Microsoft Endpoint Configuration Manager can manage applications as well but is more oriented toward managing and deploying software on-premises rather than specifically controlling app installation through a curated store. Windows Analytics, on the other hand, primarily focuses on providing insights and telemetry data about devices rather than application approval or deployment. Each

8. Which report provides the necessary information to monitor device compliance within an organization?

A. Intune Device Compliance report

B. Intune Software Update Status report

C. Azure AD Activity Report

D. Azure AD Sign-In Report

The Intune Device Compliance report is specifically designed to provide crucial insights into the compliance status of devices within an organization. This report allows administrators to assess whether devices meet the defined compliance policies set in Microsoft Intune, such as security configurations, user settings, and corporate standards. Monitoring device compliance is essential for ensuring that devices accessing corporate resources maintain a secure posture, which helps protect organizational data and mitigate risks associated with non-compliant devices. In contrast, the other reports serve different purposes. The Intune Software Update Status report focuses on the deployment and status of software updates across devices, rather than compliance with security policies. The Azure AD Activity Report tracks activities related to Azure Active Directory, such as user logins and modifications to directory objects, but does not provide information specific to device compliance. Lastly, the Azure AD Sign-In Report provides details about user sign-ins, including success and failure rates, but similarly lacks insight into the compliance status of devices. Therefore, the Intune Device Compliance report stands out as the essential tool for monitoring device compliance within an organization.

9. To restrict device enrollment to only certain users, which option should be implemented?

- A. Allow only users who are members of a specific Azure AD group to enroll devices
- B. Allow any user to enroll devices
- C. Allow users to enroll devices with a one-time enrollment token
- D. Require users to provide a certificate for device enrollment

Implementing the restriction of device enrollment to only certain users can be effectively achieved by allowing only users who are members of a specific Azure AD group to enroll devices. This method leverages Azure Active Directory's group management features, where administrators can create groups that encompass only the users who need to enroll devices. By enforcing this policy, an organization can maintain tighter control over which users are permitted to register their devices, thereby enhancing security and compliance with organizational policies. Establishing this level of restriction is particularly beneficial for organizations that need to ensure that only authorized personnel can access sensitive company resources from personal or company-issued devices. It also simplifies the management of device enrollment since changes in user access happen automatically as users are added or removed from the designated Azure AD group. The other options, while they may have their own use cases, do not provide the same level of control. Allowing any user to enroll devices would open the doors to unauthorized access potentially, while using a one-time enrollment token or requiring a certificate for device enrollment introduces complications and additional management overhead without specifically targeting user restriction effectively.

10. Which feature allows admins to define conditions under which users can access applications and data in Azure AD?

- A. A) App protection policies
- B. B) Conditional access policies
- C. C) Identity Protection
- D. D) Enrollment restrictions

The correct choice, which is Conditional Access Policies, relates directly to the capabilities provided by Azure Active Directory (Azure AD) for managing and securing access to applications and data. Conditional Access Policies enable administrators to set specific conditions that must be met for users to gain access to applications and resources. These conditions might include factors such as user location, device compliance, and the user's role within the organization, among others. The significance of these policies lies in their ability to enforce adaptive access controls, enhancing security by ensuring that users can only access resources when certain criteria are satisfied. This flexibility allows organizations to balance security and user experiences, adapting to different scenarios as needed. In contrast, while app protection policies also focus on securing applications, they are primarily centered around enforcing app-level controls rather than defining access conditions. Identity Protection deals with risk assessments and remediation for user identities, focusing on identifying and responding to potential security threats. Enrollment restrictions involve the management of devices and the conditions under which they can enroll in mobile device management solutions, which does not directly influence application and data access.

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!