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

Study Guide

Everything you need from our exam experts!

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 strategy would most effectively streamline the deployment of Windows updates across devices in an organization?**

   A. Using Windows Update manually for each device

   B. Creating an update schedule in Microsoft Intune

   C. Utilizing a dedicated update server

   D. Deploying updates using Microsoft Deployment Toolkit

2. **Which feature enables single sign-on (SSO) for Microsoft 365 services using corporate credentials?**

   A. Azure AD Domain Services

   B. Azure AD Connect Health

   C. Azure AD Identity Protection

   D. Azure AD Connect

3. **How can sensitive data access be restricted to authorized users using Azure AD?**

   A. Azure AD Connect Health

   B. Azure AD Application Proxy

   C. Azure AD Identity Protection

   D. Azure AD Privileged Identity Management

4. **When application updates fail to install, what could be a potential workaround to address the issue?**

   A. Request users to manually install the updates.

   B. Create a dependency rule for the application update and existing applications.

   C. Remove the failing applications and redeploy them.

   D. Increase the bandwidth of user internet connections.

5. **Which tool helps determine the compatibility of a new version of Windows with existing devices?**

   A. Windows Assessment and Deployment Kit (ADK)

   B. Windows Configuration Designer

   C. Windows Upgrade Analytics

   D. Windows PowerShell

6. Which feature allows an administrator to verify the health and readiness of devices before Windows 10 deployment?

A. Configuration Manager.

B. Deployment Toolkit.

C. Intune Management.

D. Assessment Toolkit.

7. Which tool can you use to monitor and manage device compliance?

A. Windows Defender Firewall

B. Windows Security Center

C. Windows BitLocker Drive Encryption

D. Microsoft Intune

8. To ensure devices meet compliance before granting access, which Azure AD feature can assist?

A. Azure AD Identity Protection

B. Azure AD Privileged Identity Management

C. Azure AD Conditional Access

D. Azure AD Connect Health

9. Which feature of attack surface reduction rules helps in blocking unwanted applications from running?

A. They use machine learning algorithms to detect suspicious behavior.

B. They allow you to block communication with malicious IP addresses.

C. They provide protection against malware and other types of threats.

D. They block potentially unwanted applications from running.

10. What is the maximum app size that can be deployed via Microsoft Intune?

A. 10 MB

B. 100 MB

C. 1 GB

D. 5 GB

Answers

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

Explanations

1. What strategy would most effectively streamline the deployment of Windows updates across devices in an organization?

A. Using Windows Update manually for each device

B. Creating an update schedule in Microsoft Intune

C. Utilizing a dedicated update server

D. Deploying updates using Microsoft Deployment Toolkit

Creating an update schedule in Microsoft Intune is the most effective strategy to streamline the deployment of Windows updates across devices in an organization. This approach allows administrators to automate and manage the update process centrally, ensuring that all devices receive timely updates without requiring individual user intervention. With Microsoft Intune, organizations can create a structured update schedule that aligns with their IT policies and operational needs. This can include setting specific times for updates to minimize disruptions, as well as defining the types of updates to be applied, such as critical security patches or feature updates. Intune also provides features for monitoring update compliance, making it easier to ensure that all devices within the organization are up to date and secure. In contrast, manually using Windows Update for each device is not scalable, particularly in larger organizations, as it requires significant manual effort and oversight. Utilizing a dedicated update server can centralize updates but may introduce additional complexity in terms of infrastructure management. Lastly, deploying updates using the Microsoft Deployment Toolkit is typically suited for initial deployment scenarios rather than ongoing updates, which can lead to inefficiencies in managing regular update cycles.

2. Which feature enables single sign-on (SSO) for Microsoft 365 services using corporate credentials?

A. Azure AD Domain Services

B. Azure AD Connect Health

C. Azure AD Identity Protection

D. Azure AD Connect

The feature that enables single sign-on (SSO) for Microsoft 365 services using corporate credentials is Azure AD Connect. This tool synchronizes on-premises directories with Azure Active Directory, allowing users to utilize their corporate credentials to access Microsoft 365 services seamlessly. When Azure AD Connect is implemented, it facilitates not only the synchronization of user identities and directories but also enables the configuration of SSO capabilities. With SSO, users can log in once with their corporate credentials and gain access to multiple applications and services, enhancing user experience and increasing productivity by minimizing the number of times they need to enter their credentials. This is essential for organizations that want to manage access securely while simplifying the login process across various Microsoft 365 services. The other options are related to identity management and security, but they do not primarily focus on enabling SSO in the same way that Azure AD Connect does. Azure AD Domain Services provides managed domain services but does not directly facilitate SSO. Azure AD Connect Health offers monitoring for Azure AD Connect, and Azure AD Identity Protection focuses on risk-based conditional access policies rather than SSO itself.

3. How can sensitive data access be restricted to authorized users using Azure AD?

A. Azure AD Connect Health

B. Azure AD Application Proxy

C. Azure AD Identity Protection

D. Azure AD Privileged Identity Management

Restricting access to sensitive data for authorized users using Azure Active Directory (Azure AD) involves implementing a series of policies and security measures that ensure only the right users can access specific resources. Azure AD Identity Protection plays a crucial role in this context by using risk-based conditional access policies to mitigate potential threats. This service assesses the risk levels associated with user sign-in activities and sets conditions for access based on those risks. For instance, if a user tries to access sensitive data from an unusual location or from an unrecognized device, Azure AD Identity Protection can enforce stricter authentication requirements, such as multi-factor authentication. By utilizing risk detection and automated responses, organizations can proactively prevent unauthorized access to sensitive information, ensuring that only those users who meet specific criteria can gain access. This is essential in maintaining compliance with data protection regulations and safeguarding organizational data. The other options focus on different aspects of Azure AD functionality. Azure AD Connect Health is primarily for monitoring and ensuring the health of AD Connect synchronization. The Azure AD Application Proxy allows secure remote access to on-premises applications but does not inherently restrict data access. Azure AD Privileged Identity Management helps manage and control privileged accounts and their access but isn't specifically focused on real-time risk assessment for standard user access to

4. When application updates fail to install, what could be a potential workaround to address the issue?

A. Request users to manually install the updates.

B. Create a dependency rule for the application update and existing applications.

C. Remove the failing applications and redeploy them.

D. Increase the bandwidth of user internet connections.

Creating a dependency rule for the application update and existing applications can effectively address issues with application updates failing to install. Dependency rules help ensure that certain conditions are met before an update can proceed. For instance, if an application update requires specific configurations or versions of related applications to be present on the device, defining those dependencies can help the update process succeed. By establishing these rules, administrators can prevent conflicts and ensure that the correct versions of software components are in place, which can often be a reason for installation failures. This proactive approach helps streamline the update process and minimizes disruptions caused by unforeseen circumstances, leading to a more stable application environment without necessitating user intervention or drastic measures like removing and redeploying applications. Other options present alternative methods but may not directly resolve the underlying issues leading to the update failures. For instance, manually requesting users to install updates places the onus on the users and may not ensure a successful installation if the underlying issues aren't resolved. Similarly, removing failing applications can lead to downtime and may not address the core problem at hand, rather than making the update process more robust with dependency rules. Increasing internet bandwidth might help in specific scenarios, but it doesn't necessarily address the dependency requirements or underlying conflicts during the installation process.

5. Which tool helps determine the compatibility of a new version of Windows with existing devices?

A. Windows Assessment and Deployment Kit (ADK)

B. Windows Configuration Designer

C. Windows Upgrade Analytics

D. Windows PowerShell

The tool that assists in determining the compatibility of a new version of Windows with existing devices is Windows Upgrade Analytics. This tool provides insights into the readiness of devices to upgrade by analyzing them for compatibility issues, application functionality, and drivers. It collects data from devices and helps administrators assess whether those devices can successfully transition to a newer version of Windows. Windows Upgrade Analytics is particularly valuable because it can offer detailed reports on potential compatibility concerns, allowing IT professionals to make informed decisions about upgrades, plan for necessary mitigations, and ensure a smoother upgrade process for users. The other tools listed have different primary functions. The Windows Assessment and Deployment Kit (ADK) is more focused on creating tools and resources for evaluating and deploying Windows, rather than directly analyzing compatibility. Windows Configuration Designer is primarily used for configuring provisioning packages to simplify the setup of Windows devices. Windows PowerShell, while a powerful scripting and automation tool, does not inherently provide features specific to Windows compatibility assessments.

6. Which feature allows an administrator to verify the health and readiness of devices before Windows 10 deployment?

A. Configuration Manager.

B. Deployment Toolkit.

C. Intune Management.

D. Assessment Toolkit.

The feature that enables an administrator to verify the health and readiness of devices before deploying Windows 10 is Configuration Manager. This tool allows for comprehensive device management and offers functionality that includes assessing hardware compatibility, checking for updates, and ensuring that system requirements are met prior to deployment. Configuration Manager includes features like the Hardware Inventory and Software Inventory, which can be used to gather valuable information about the devices in the environment. By using these features, administrators can create reports that highlight any devices that may not meet the necessary criteria for a successful Windows 10 deployment. This proactive assessment is crucial in minimizing deployment issues and ensuring a smooth transition to the new operating system. Other options, while important in their own right, serve different purposes. The Deployment Toolkit is primarily focused on streamlining the deployment process but does not inherently verify device readiness; Intune Management deals mostly with mobile device management and application management rather than initial hardware checks; while the Assessment Toolkit could involve evaluating devices, it typically focuses on assessing applications for compatibility rather than the overall device health in preparation for an OS deployment.

7. Which tool can you use to monitor and manage device compliance?

A. Windows Defender Firewall

B. Windows Security Center

C. Windows BitLocker Drive Encryption

D. Microsoft Intune

Using Microsoft Intune is the primary method for monitoring and managing device compliance within the Microsoft 365 ecosystem. Intune provides comprehensive management capabilities that allow administrators to ensure that devices meet specific compliance criteria and corporate policies. It offers features such as device enrollment, configuration policies, application management, and security baselines, making it an essential tool for controlling access to organizational resources based on compliance status. With Intune, you can implement compliance policies that enforce requirements like password complexity, operating system version, and encryption status. The ability to monitor compliance in real-time allows administrators to take actions such as restricting access to corporate resources for devices that fail to meet the compliance standards. In contrast, the other options focus on security and system management rather than compliance management. For instance, while Windows Defender Firewall and Windows Security Center provide protective measures and security information, they do not specifically handle compliance monitoring and management. Similarly, Windows BitLocker provides disk encryption for securing data but does not offer the comprehensive compliance capabilities that Intune does.

8. To ensure devices meet compliance before granting access, which Azure AD feature can assist?

A. Azure AD Identity Protection

B. Azure AD Privileged Identity Management

C. Azure AD Conditional Access

D. Azure AD Connect Health

The Azure AD Conditional Access feature is designed to help organizations implement policies that evaluate the compliance of devices before granting access to resources. It enables the creation of conditions that must be met for users to access applications and services, such as checking if a device is compliant with defined policies. This can include ensuring that a device is properly enrolled in mobile device management (MDM), running the latest security updates, or using an approved operating system version. By utilizing Conditional Access, an organization can enforce access control based on the compliance status of a device, ensuring that only devices that adhere to specific security standards are allowed to access sensitive data and applications. This is particularly essential in maintaining the security posture of an organization by limiting access based on risk assessments connected with device compliance. The other options serve different purposes: Identity Protection focuses on safeguarding identities through risk-based conditional access based on detected vulnerabilities. Privileged Identity Management is related to managing and controlling administrator permissions. Connect Health is primarily about monitoring the health of on-premises infrastructure related to Azure AD. Each of these features provides valuable capabilities, but for the specific requirement of ensuring device compliance before access is granted, Conditional Access is the appropriate choice.

9. Which feature of attack surface reduction rules helps in blocking unwanted applications from running?

A. They use machine learning algorithms to detect suspicious behavior.

B. They allow you to block communication with malicious IP addresses.

C. They provide protection against malware and other types of threats.

D. They block potentially unwanted applications from running.

The feature that effectively blocks unwanted applications from running is designed to help maintain endpoint security by preventing potentially undesirable or harmful applications from executing on devices within the network. This is critical because such applications might not be inherently malicious but can be unwanted due to their resource consumption, impact on system performance, or lack of user consent. By specifically targeting potentially unwanted applications (PUAs), this feature helps organizations enforce policies that allow only approved software to run, which reduces the attack surface and mitigates risks associated with unverified applications being executed. This proactive approach is part of a comprehensive security strategy aimed at safeguarding user endpoints and protecting sensitive data. The other options, while related to security and threat management, address different aspects. For instance, machine learning algorithms focus on identifying suspicious behaviors rather than blocking specific types of applications. Blocking communication with malicious IP addresses targets external threats rather than controlling which applications can be executed locally. Protection against malware encompasses a broader spectrum of threats but does not specifically relate to controlling unwanted applications. Thus, the option that emphasizes blocking potentially unwanted applications directly aligns with the goal of maintaining a controlled and secure application environment.

10. What is the maximum app size that can be deployed via Microsoft Intune?

A. 10 MB

B. 100 MB

C. 1 GB

D. 5 GB

The maximum app size that can be deployed via Microsoft Intune is 8 GB, which means that the only feasible option from the provided choices is 5 GB. This size limit applies to Win32 apps when using the Intune management platform for application deployment. Understanding these limits is essential for administrators to plan effectively for application rollouts and ensure that larger applications do not exceed the supported sizes, which can impact deployment strategies. The choice of 100 MB, while it may seem substantial, does not reflect the current capabilities of Intune regarding app size limits. It's important for administrators to stay updated on deployment guidelines and the evolving capabilities of Intune to ensure optimal performance and compliance in their environment.

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!