Microsoft Intune Practice Test (Sample)

Study Guide

BY EXAMZIFY

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. **How do compliance policies affect Conditional Access in Intune?**
   A. They allow access to only certain users
   B. They must be met for devices to access corporate resources
   C. They are optional for accessing resources
   D. They provide an alternate way to access applications

2. **What does MAM stand for in the context of Intune?**
   A. Mobile Application Management
   B. Managed Application Monitoring
   C. Mobile Asset Management
   D. Mobile Account Management

3. **What is a primary benefit of using Conditional Access in Intune?**
   A. It enhances personal device use
   B. It ensures only compliant devices access specific resources
   C. It increases network speed
   D. It allows unrestricted access to all users

4. **Does Microsoft Intune support Mac OS X 10.9 and later?**
   A. Yes
   B. No
   C. Conditional support
   D. Only in business settings

5. **Which of the following can indicate the compliance status of a device in Intune?**
   A. Device enrollment status
   B. App installation log
   C. Network usage report
   D. Incident report

6. What is the purpose of an Intune deployment profile?

   A. To store user data securely

   B. To configure settings on devices during enrollment

   C. To monitor application performance

   D. To create software development kits

7. What role is necessary for SCCM to work with an Intune deployment?

   A. Microsoft Intune Connector Site Role

   B. System Administrator Role

   C. Cloud Management Role

   D. Network Administrator Role

8. How does Intune ensure secure mobile application access?

   A. By using VPN configurations

   B. Through application protection policies

   C. By restricting internet access

   D. With firewall settings

9. What can you view in a computer inventory report in Intune?

   A. Network performance data

   B. Hardware specs of Intune Managed devices

   C. Software usage statistics

   D. Active users and sessions

10. What is the difference between "app protection" and "device compliance" in Intune?

   A. App protection safeguards applications, while device compliance pertains to security policies

   B. App protection focuses on device performance, while device compliance governs user access

   C. App protection is device-specific, while device compliance is application-specific

   D. App protection is for individual users, while device compliance is for organizations

Answers

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

Explanations

1. **How do compliance policies affect Conditional Access in Intune?**

   A. They allow access to only certain users

   B. They must be met for devices to access corporate resources

   C. They are optional for accessing resources

   D. They provide an alternate way to access applications

Compliance policies play a critical role in the Conditional Access framework within Microsoft Intune. They establish the requirements that devices must meet to ensure they are secure and compliant with the organization's standards. When a device is evaluated against these compliance policies, it determines whether that device should have access to corporate resources, such as applications and data. If a device meets the compliance policies, Conditional Access allows that device to access the corporate resources. Conversely, if a device does not align with the established compliance requirements, access is effectively blocked. This mechanism ensures that only devices that adhere to the organization's security and compliance standards can access sensitive information, thereby protecting corporate data from potential threats. This relationship emphasizes the importance of compliance policies in ensuring that access to corporate resources is not just granted arbitrarily but is instead conditional upon the security posture of the devices attempting to connect.

2. **What does MAM stand for in the context of Intune?**

   A. Mobile Application Management

   B. Managed Application Monitoring

   C. Mobile Asset Management

   D. Mobile Account Management

In the context of Intune, MAM stands for Mobile Application Management. This refers to the tools and services provided within Microsoft Intune for managing applications on mobile devices. It enables organizations to secure and manage apps used by their employees on personal or company-owned devices without needing full device management. This focus on applications ensures that sensitive corporate data can be protected while also allowing for a level of personal freedom for users in how they use their devices. Mobile Application Management features include the ability to set policies that control how applications are used, ensuring that data can only be accessed or shared with authorized applications. MAM also allows administrators to manage app deployment, updates, and removal while maintaining user privacy by not having access to personal data on devices. This makes it a crucial aspect of Microsoft Intune's comprehensive approach to mobile device and application management.

3. What is a primary benefit of using Conditional Access in Intune?

   A. It enhances personal device use

   B. It ensures only compliant devices access specific resources

   C. It increases network speed

   D. It allows unrestricted access to all users

The primary benefit of using Conditional Access in Intune is that it ensures only compliant devices can access specific resources. This feature allows organizations to implement security policies that require devices to meet certain compliance standards or conditions before they can access sensitive applications and data. By enforcing these policies, businesses can significantly reduce the risk of data breaches and unauthorized access while ensuring that users can only connect using devices that adhere to the organization's security configurations.   This mechanism helps maintain a secure environment, as it allows IT administrators to monitor and verify the status of devices, including whether they have the latest updates, security patches, and configurations as per the organizational requirements. Thus, Conditional Access serves as a safeguard to ensure that only trusted and compliant devices can interact with critical business resources, which is essential in today's threat landscape where security is paramount.

4. Does Microsoft Intune support Mac OS X 10.9 and later?

   A. Yes

   B. No

   C. Conditional support

   D. Only in business settings

Microsoft Intune provides support for macOS beginning with version 10.9 (Mavericks) and continuing for later versions. This allows organizations to manage devices effectively across various operating systems, including macOS. The support for macOS facilitates mobile device management (MDM) and mobile application management (MAM), enabling the enforcement of security policies, distribution of applications, and management of configurations tailored for Mac users.   By supporting macOS, Microsoft Intune helps create a cohesive IT environment that accommodates diverse devices and operating systems commonly used in enterprise settings. This capability is crucial for organizations with mixed-device environments, ensuring security and compliance across all devices. In this context, the other options do not align with Microsoft's support policy for macOS through Microsoft Intune. Conditional support might imply limitations or specific criteria for use, which are not the case with macOS versions 10.9 and later. Additionally, the idea of support being limited to business settings does not reflect Intune's broader capability to manage personal and corporate-owned devices in various environments.

5. Which of the following can indicate the compliance status of a device in Intune?

A. Device enrollment status

B. App installation log

C. Network usage report

D. Incident report

The compliance status of a device in Intune is indicated by the device enrollment status. This is because enrollment status provides critical information regarding whether a device has been properly enrolled in Intune, which is the first essential step in managing and securing the device according to organizational policies. When a device is enrolled, it becomes subject to compliance checks against the policies set up in Intune, and its compliance status is therefore directly linked to this enrollment process.   In contrast, while factors like app installation logs, network usage reports, or incident reports may provide useful information regarding application performance, network behavior, or security incidents respectively, they do not specifically address whether a device meets the compliance requirements dictated by the organization's policies in Intune. These reports might be useful in assessing the device's performance or identifying issues, but they do not serve as primary indicators of compliance status.

6. What is the purpose of an Intune deployment profile?

A. To store user data securely

B. To configure settings on devices during enrollment

C. To monitor application performance

D. To create software development kits

The purpose of an Intune deployment profile is to configure settings on devices during enrollment. When devices are enrolled in Intune, deployment profiles allow administrators to apply specific configurations and policies automatically, ensuring that devices are set up according to organizational standards right from the start. This includes settings related to Wi-Fi, VPN, email, and other necessary configurations that are essential for device operation and security within the enterprise environment. Deploying a well-structured profile streamlines the setup process for users, minimizes configuration errors, and enhances overall security and compliance. The deployment profile is a critical component in managing how devices are integrated into the organization's infrastructure effectively and efficiently.

7. What role is necessary for SCCM to work with an Intune deployment?

A. Microsoft Intune Connector Site Role

B. System Administrator Role

C. Cloud Management Role

D. Network Administrator Role

For SCCM (System Center Configuration Manager) to effectively work with an Intune deployment, the Microsoft Intune Connector Site Role is essential. This role is specifically designed to facilitate communication between SCCM and Intune, enabling the integration of on-premises systems with cloud-based services.   The Intune Connector acts as a bridge, allowing SCCM to manage devices that are enrolled in Intune and to extend its management capabilities to those devices. This role is crucial for tasks such as deploying applications, managing updates, and enforcing compliance policies across devices that may not be directly connected to the corporate network but are managed through Intune. While other roles like System Administrator or Cloud Management might have some necessary functions within the broader context of SCCM and Intune, they do not specifically address the integration of SCCM with Intune. The Network Administrator role also does not pertain directly to this integration. Thus, the Microsoft Intune Connector Site Role is the definitive requirement for a successful collaboration between SCCM and Intune.

8. How does Intune ensure secure mobile application access?

A. By using VPN configurations

B. Through application protection policies

C. By restricting internet access

D. With firewall settings

Intune ensures secure mobile application access primarily through application protection policies. These policies are designed to safeguard applications and data on both managed and unmanaged devices. They play a critical role in securing access by enforcing various restrictions and security measures directly on applications. For instance, application protection policies may require that users authenticate themselves through various means, such as a PIN or biometric data, before accessing sensitive applications. They can also restrict the ability to copy or paste data between applications or control how data is shared. In this way, even if an application is installed on an unmanaged device, the data within it can still be protected, helping prevent data breaches and unauthorized access. The other concepts, while related to security, do not specifically ensure secure mobile application access to the same extent as application protection policies. VPN configurations enable secure connections to corporate resources but do not inherently protect applications themselves. Restricting internet access might limit exposure to threats, but it doesn't directly secure the applications. Firewall settings may help to manage network traffic but are not specific to application-level security. Thus, application protection policies are integral to safeguarding mobile application access in a comprehensive manner.

9. What can you view in a computer inventory report in Intune?

A. Network performance data

B. Hardware specs of Intune Managed devices

C. Software usage statistics

D. Active users and sessions

In a computer inventory report in Microsoft Intune, you can view the hardware specifications of Intune managed devices. This report typically includes detailed information such as the CPU model, amount of RAM, storage capacity, operating system version, and other vital hardware attributes. This data is crucial for IT administrators as it allows them to assess the capabilities of their managed devices, plan for upgrades or replacements, and ensure that the devices meet the organization's requirements for performance and security. While network performance data, software usage statistics, and information about active users and sessions may be valuable in other contexts, they are not typically part of the hardware-focused inventory report that Intune provides. Instead, these aspects could be found in different management features or reports within the Intune ecosystem, serving specific purposes like monitoring performance or user engagement.

10. What is the difference between "app protection" and "device compliance" in Intune?

A. App protection safeguards applications, while device compliance pertains to security policies

B. App protection focuses on device performance, while device compliance governs user access

C. App protection is device-specific, while device compliance is application-specific

D. App protection is for individual users, while device compliance is for organizations

The distinction between app protection and device compliance in Microsoft Intune is fundamental for managing security and access in organizational environments. App protection primarily focuses on securing corporate applications and the data they handle, irrespective of the device being used. This ensures that sensitive information remains protected by applying data protection policies directly to apps. It typically involves measures such as controlling how corporate data can be shared, ensuring scripts can run only on compliant devices, and encrypting sensitive information. On the other hand, device compliance refers to the adherence of devices to certain security policies that have been set by the organization. These compliance policies can include criteria such as requiring a device to have a certain operating system version, enforcing encryption settings, and ensuring that devices are free from malware. When a device meets these compliance criteria, it is deemed secure enough for access to corporate resources. Thus, the correct choice highlights that app protection safeguards the applications directly, focusing on data security at the app level, while device compliance addresses the overall security posture of the devices themselves, ensuring that they conform to the organization's policies for access and security. This clear delineation helps organizations manage risk effectively while allowing users to access corporate resources securely.

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://microsoftintune.examzify.com

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