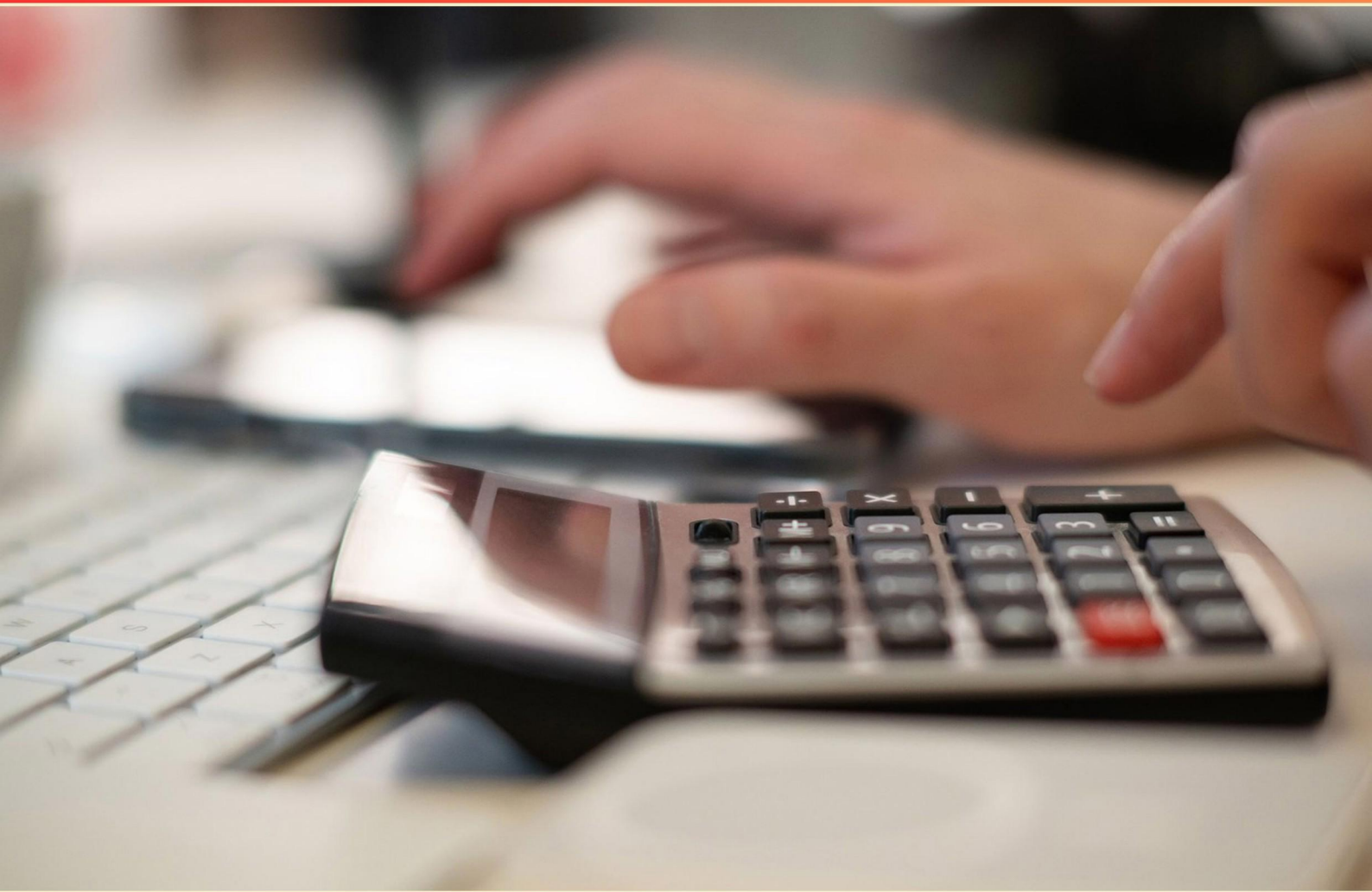


MICROSOFT INTUNE PRACTICE TEST (SAMPLE)

STUDY GUIDE



**SAMPLE STUDY GUIDE
WITH LIMITED QUESTIONS**

**VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE**

<https://microsoftintune.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.

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

SAMPLE

1. What function do device restrictions serve in Intune?

- A. They enhance the performance of all devices
- B. They limit user actions and device functionalities based on organizational policies
- C. They allow users to bypass compliance checks
- D. They provide administrative access to all devices

2. How does Intune simplify app distribution for organizations?

- A. By allowing organizations to deploy and manage apps directly through Intune
- B. By requiring manual installation on each device
- C. By limiting access to only web-based applications
- D. By prohibiting the use of third-party applications

3. What advantage do baselines in Intune provide to organizations?

- A. They create unique configurations for each device
- B. They offer a quick way to apply standard security configurations across devices
- C. They enable remote troubleshooting of applications
- D. They automate user training programs

4. What is the role of enrollment restrictions in Intune?

- A. To set data limits for enrolled devices
- B. To control which types of devices are allowed to enroll in the management program
- C. To restrict user access to applications
- D. To implement physical tracking of devices

5. How can Intune manage Windows devices?

- A. Through the use of virtualization technologies only
- B. Through enrollment of devices using MDM or Co-management with Configuration Manager
- C. By requiring users to use only cloud applications
- D. By relying solely on user manual configurations

6. Where are Service Administrators added in the Intune Management Portal?

- A. Administrator Management > Users
- B. Administration > Service Administrators
- C. Administrator Management > Service Administrators > Add
- D. Settings > User Management

7. Which feature allows users to enroll multiple devices at once?

- A. Active Directory synchronization
- B. Bulk user import via CSV
- C. Individual user registration only
- D. Directory Access Management

8. Through Intune, what capability does the update report provide?

- A. Real-time location tracking of devices
- B. Audit logs for license usage
- C. Status of all updates on Intune Managed Devices
- D. Historical trends of device compliance

9. What is a key feature of Microsoft Intune when managing mobile devices?

- A. Device performance tracking
- B. Multi-channel authentication
- C. Application lifecycle management
- D. Local backup services

10. What is the purpose of Conditional Access in Intune?

- A. To limit user access based on time of day
- B. To ensure only compliant devices can access apps and resources
- C. To prevent data loss during software updates
- D. To restrict bandwidth usage

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What function do device restrictions serve in Intune?

- A. They enhance the performance of all devices
- B. They limit user actions and device functionalities based on organizational policies**
- C. They allow users to bypass compliance checks
- D. They provide administrative access to all devices

Device restrictions in Intune primarily serve to limit user actions and device functionalities based on organizational policies. This means organizations can enforce specific security measures and operational guidelines that devices must adhere to, enhancing the overall security posture of the organization. By setting these restrictions, IT administrators can ensure that users cannot perform certain actions that may expose the organization to risks, such as installing unapproved apps or enabling features that could compromise data security. In practice, this includes controlling access to features like the camera, Bluetooth, or the ability to add personal email accounts, among others. These restrictions help manage and mitigate the potential for data breaches or loss, ensuring that only allowed activities are performed on the devices within the corporate environment. Therefore, the correct answer highlights the critical role of device restrictions in maintaining organizational compliance and security standards.

2. How does Intune simplify app distribution for organizations?

- A. By allowing organizations to deploy and manage apps directly through Intune**
- B. By requiring manual installation on each device
- C. By limiting access to only web-based applications
- D. By prohibiting the use of third-party applications

Intune simplifies app distribution for organizations by allowing them to deploy and manage applications directly through its platform. This central management capability streamlines the entire process, enabling IT administrators to roll out applications to multiple devices efficiently and in a controlled manner. With Intune, organizations can automate the app deployment process, ensuring that users have the necessary applications installed without needing individual manual installations. This approach not only saves time but also reduces the potential for human error that can occur with manual installations. Additionally, the ability to manage applications from a single interface means that updates, security policies, and compliance can be handled promptly, ensuring that all devices have the latest approved versions of applications. This enhances productivity and security within the organization, allowing staff to focus on their core duties instead of spending time on app installations and troubleshooting. The other options suggest methods that would complicate or limit the deployment process, making them less effective in achieving seamless app distribution.

3. What advantage do baselines in Intune provide to organizations?

- A. They create unique configurations for each device
- B. They offer a quick way to apply standard security configurations across devices**
- C. They enable remote troubleshooting of applications
- D. They automate user training programs

Baselines in Intune serve as a streamlined method for organizations to apply consistent security configurations across multiple devices effectively. This consistency is crucial for maintaining a secure environment when managing diverse endpoints within an organization. By using baselines, IT administrators can quickly deploy predefined security settings that adhere to standardized compliance requirements. This approach not only saves time in configuring each device individually but also helps ensure that all devices are governed by the same security policies, reducing the risk of vulnerabilities that may arise from misconfigurations. The deployment of these baseline configurations assists in achieving and maintaining compliance with industry standards and internal policies, making it easier to manage and protect sensitive information across the organization.

4. What is the role of enrollment restrictions in Intune?

- A. To set data limits for enrolled devices
- B. To control which types of devices are allowed to enroll in the management program**
- C. To restrict user access to applications
- D. To implement physical tracking of devices

Enrollment restrictions play a critical role in Microsoft Intune by managing and controlling the types of devices that are permitted to enroll in the management system. This is essential for maintaining security and compliance within an organization, as it ensures that only authorized devices can access corporate resources and data. By defining specific criteria like operating system types, device models, or even specific manufacturer IDs, organizations can tailor their enrollment policies to match their security requirements and usage scenarios. This means that if a user attempts to enroll a device that does not meet the established criteria, the system will deny the enrollment request. This control helps minimize the risks of unauthorized access and potential data breaches, thus reinforcing the overall security posture of the organization. While the other options reference important aspects of device management, such as data limits, application access, and physical tracking, they do not capture the primary objective of enrollment restrictions, which is specifically about controlling the enrollment process itself.

5. How can Intune manage Windows devices?

- A. Through the use of virtualization technologies only
- B. Through enrollment of devices using MDM or Co-management with Configuration Manager**
- C. By requiring users to use only cloud applications
- D. By relying solely on user manual configurations

Microsoft Intune can effectively manage Windows devices primarily through the enrollment of those devices using Mobile Device Management (MDM) capabilities or through co-management in conjunction with Configuration Manager. This allows organizations to enroll Windows devices in a secure and streamlined manner, enabling the application of policies, distribution of software, and management of security settings. When devices are enrolled in Intune, administrators have the ability to push out settings and configurations remotely, enforce compliance policies, and ensure that devices are secure and up-to-date with the latest software. Co-management with Configuration Manager further enhances this by allowing organizations that already utilize Microsoft System Center Configuration Manager to leverage Intune's cloud capabilities for more flexible and integrated management solutions. The other options mentioned do not encapsulate the comprehensive management capabilities that Intune offers through MDM and co-management. Virtualization technologies, cloud applications, and manual configurations may play a role in a device management strategy, but they do not represent the primary methods by which Intune manages Windows devices directly. Thus, the method of enrollment through MDM or co-management is critical for leveraging Intune's full potential in device management.

6. Where are Service Administrators added in the Intune Management Portal?

- A. Administrator Management > Users
- B. Administration > Service Administrators
- C. Administrator Management > Service Administrators > Add**
- D. Settings > User Management

The process of adding Service Administrators in the Intune Management Portal is done through the specified path where Service Administrators are managed directly. By navigating to Administration and then selecting Service Administrators, you can effectively see the roles assigned. The critical step of selecting 'Add' under the Service Administrators section of Administrator Management is where new Service Administrators are specifically added. Choosing this option is correct as it highlights the direct action required to introduce a new Service Administrator into the management portal effectively. Ensuring that users are assigned proper roles and responsibilities is vital for maintaining security and functionality in Intune, as Service Administrators have elevated privileges that allow them to perform essential administrative functions. Thus, understanding the exact navigation path to add users in roles such as Service Administrators is crucial for effective Intune management.

7. Which feature allows users to enroll multiple devices at once?

- A. Active Directory synchronization
- B. Bulk user import via CSV**
- C. Individual user registration only
- D. Directory Access Management

The feature that enables users to enroll multiple devices at once is bulk user import via CSV. This functionality is particularly useful for organizations that need to onboard several devices simultaneously, as it allows administrators to prepare a CSV file containing multiple user details and the associated devices. When this CSV file is imported into Microsoft Intune, Intune processes the information and facilitates enrollment for all the specified devices at once. This effective method streamlines the enrollment process, significantly reducing the administrative overhead that would come from enrolling each device individually. Active Directory synchronization, while important for identity management and ensuring user devices are recognized in the Intune ecosystem, does not directly relate to bulk enrollment of devices. Individual user registration only allows one device to be enrolled at a time, which does not meet the requirement for mass enrollment. Directory Access Management is more focused on controlling access to directories rather than facilitating device enrollment. Thus, the bulk user import via CSV is the optimal solution for enrolling multiple devices efficiently.

8. Through Intune, what capability does the update report provide?

- A. Real-time location tracking of devices
- B. Audit logs for license usage
- C. Status of all updates on Intune Managed Devices**
- D. Historical trends of device compliance

The update report in Intune is designed to provide a comprehensive overview of the status of updates on devices that are managed through the platform. This capability is crucial for IT administrators as it allows them to monitor which updates have been applied successfully, which updates are pending, and which devices may be facing issues with updates. By having this visibility, organizations can ensure that their devices are kept secure and up-to-date with the latest features and security patches. This capability is especially important in environments where multiple devices are being managed, as it helps streamline the update process and ensures compliance with organizational policies regarding software updates. Effective management of device updates is key to maintaining system integrity and security, which is essential for any organization leveraging cloud-based management solutions like Intune. Thus, the correct answer highlights a fundamental aspect of device management within Microsoft Intune, emphasizing the importance of keeping track of updates in a managed environment.

9. What is a key feature of Microsoft Intune when managing mobile devices?

- A. Device performance tracking
- B. Multi-channel authentication
- C. Application lifecycle management**
- D. Local backup services

A key feature of Microsoft Intune is application lifecycle management. This functionality is crucial for organizations that need to manage the entire lifecycle of applications on mobile devices, from deployment to updates and eventually removal. Intune allows administrators to deploy apps to devices, manage their configurations, monitor usage, and ensure compliance with organizational policies. This feature is particularly important for maintaining security, ensuring that users have access to the necessary applications for their work, and simplifying the management of app versions across a diverse range of devices. In contrast, device performance tracking, multi-channel authentication, and local backup services are not primary functionalities of Intune. Device performance tracking might be managed through other tools but is not a core feature of Intune. Multi-channel authentication is related to security and user access but is handled through Azure Active Directory rather than Intune specifically. Local backup services typically involve device-level backups for personal user data, which is outside the primary scope of Intune's focus on application and device management.

10. What is the purpose of Conditional Access in Intune?

- A. To limit user access based on time of day
- B. To ensure only compliant devices can access apps and resources**
- C. To prevent data loss during software updates
- D. To restrict bandwidth usage

The purpose of Conditional Access in Intune is to ensure that only compliant devices can access applications and resources. This feature plays a crucial role in managing security and compliance within an organization's digital environment. By implementing Conditional Access policies, administrators can establish specific conditions under which users can access apps and data. These conditions often include device compliance checks, user identity verification, and location-based access requirements. Conditional Access allows businesses to enhance their security posture by enforcing policies that monitor and assess device compliance with organizational standards. For instance, if a device does not meet certain security criteria, such as having the latest updates or required security settings, access to sensitive applications is denied. This helps to mitigate risks associated with data breaches or unauthorized access, thereby protecting both corporate resources and sensitive information. The other options, while relevant to various security and IT management concerns, do not capture the core functionality of Conditional Access in the context of Microsoft Intune. Limiting access based on time of day, preventing data loss during updates, or restricting bandwidth usage do not directly relate to the compliance-driven access controls provided by Conditional 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://microsoftintune.examzify.com>

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

SAMPLE