Apple Deployment and Management
Exam Preparation Guide
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About the Exam</td>
<td>3</td>
</tr>
<tr>
<td>Preparing for the Exam</td>
<td>3</td>
</tr>
<tr>
<td>Learning Objectives</td>
<td>4</td>
</tr>
<tr>
<td>Understanding MDM</td>
<td>4</td>
</tr>
<tr>
<td>Planning</td>
<td>5</td>
</tr>
<tr>
<td>Preparing</td>
<td>8</td>
</tr>
<tr>
<td>Exploring the Tools</td>
<td>9</td>
</tr>
<tr>
<td>Enrolling Devices</td>
<td>10</td>
</tr>
<tr>
<td>Getting Content</td>
<td>12</td>
</tr>
<tr>
<td>Configuring Devices</td>
<td>14</td>
</tr>
<tr>
<td>Managing Content</td>
<td>18</td>
</tr>
<tr>
<td>Managing Data</td>
<td>19</td>
</tr>
<tr>
<td>Managing Lost Devices</td>
<td>20</td>
</tr>
<tr>
<td>Querying Devices</td>
<td>20</td>
</tr>
<tr>
<td>Managing Traffic</td>
<td>21</td>
</tr>
<tr>
<td>Updating Devices</td>
<td>21</td>
</tr>
<tr>
<td>Recycling Devices</td>
<td>21</td>
</tr>
<tr>
<td>Sample Questions</td>
<td>22</td>
</tr>
<tr>
<td>Answer Key</td>
<td>52</td>
</tr>
<tr>
<td>Exam Details</td>
<td>56</td>
</tr>
<tr>
<td>Taking the Exam</td>
<td>56</td>
</tr>
<tr>
<td>About the Certification</td>
<td>57</td>
</tr>
</tbody>
</table>
About the Exam

The Apple Deployment and Management exam is for technical professionals who deploy and manage Apple devices. This exam verifies that you understand the learning objectives listed in this guide. When you pass the exam, you earn the Apple Certified IT Professional certification. For more information, visit the Apple Training website.

This exam is based on iOS 16, iPadOS 16, and macOS Ventura.

Preparing for the Exam

The exam covers the learning objectives listed in this guide, not only the topics in the Apple Deployment and Management course. To pass the exam, you need to study multiple Apple resources and gain hands-on experience deploying and managing Apple devices. Depending on your background, technical expertise, and experience deploying and managing Apple devices, it could take you 30 to 60 hours to prepare for this exam.

Review the learning objectives in this guide. Identify the topics you need to study, then do the following to prepare for the exam:

• Practice with the sample questions in this guide.
• Complete the Apple Deployment and Management course online. Use the Check Your Understanding questions to reinforce your knowledge of the topics in each article and tutorial.
• Study the resources listed in the Apple Deployment and Management Resources section of the online course.
• Become familiar with iOS, iPadOS, and macOS, then practice the course exercises.
• Gain practical experience in deploying and managing Apple devices in an organization.
Learning Objectives

Understanding MDM

List what can be managed and actions that can be taken on the device in MDM.

- MDM payload list for iPhone and iPad devices
- MDM payload list for Mac computers
- MDM commands for Apple devices

Describe what MDM is and how it works.

- Intro to mobile device management profiles

Explain declarative device management.

- What's new in Apple platform deployment

List the general capabilities of MDM solutions.

- Intro to mobile device management profiles

Identify key management tasks that MDM uses when managing Apple devices.

- MDM payload list for iPhone and iPad devices
- MDM payload list for Mac computers
- MDM commands for Apple devices

Recognize the key purpose and function of Apple's management framework.

- Intro to mobile device management profiles

Describe the Apple device deployment and management life cycle in general terms.

- Apple Lifecycle Management (PDF)

Explain how device ownership models affect an organization's deployment strategy.

- Intro to Apple device enrollment types

Identify key considerations that relate to deploying Apple devices in user-owned deployment scenarios.

- Intro to Apple device enrollment types

Identify key considerations that relate to deploying Apple devices in organization-owned deployment scenarios.

- Intro to Apple device enrollment types

List the requirements to set up an MDM solution for Apple device enrollment.

- Configure your network for MDM

Given a scenario, develop a deployment strategy for different ownership models and device purchase sources.

- Intro to Apple device enrollment types

Compare and contrast the methods for enrolling user-owned devices into an MDM solution.

- User Enrollment and MDM
Planning

Explain the ownership and enrollment options for each enrollment type.

- User Enrollment and MDM
- Device Enrollment and MDM
- Automated Device Enrollment and MDM
- Intro to Apple device enrollment types

Explain the management options and limitations for each enrollment type.

- User Enrollment and MDM
- Device Enrollment and MDM
- Automated Device Enrollment and MDM
- Intro to Apple device enrollment types

Evaluate MDM solutions.

- Choose an MDM solution

Evaluate identity management and authentication services, such as single sign-on (SSO) and Active Directory, to manage secure access to your organization’s resources on Apple devices.

- Intro to single sign-on with Apple devices
- Intro to Apple identity services

Design a security policy that prevents unauthorized use of a managed Apple device.

- Passcode MDM payload settings for Apple devices
- Enforce password policies for your devices

Design a security policy that stores an organization's data securely on a managed Apple device.

- Intro to certificate management for Apple devices
- Automated Device Enrollment MDM payload list
- Device Enrollment MDM payload list
- User Enrollment MDM information
- Intro to Apple device enrollment types

Design a security policy that encrypts data transmitted over an organization’s network on a managed Apple device.

- Use SSL VPN clients for Apple devices
- VPN overview for Apple device deployment
- Secure access to wireless networks
- TLS security
- Use built-in network security features for Apple devices

Design a security policy that allows an organization to install and manage apps on a managed Apple device that work securely without compromising platform integrity.

- Distribute Managed Apps to Apple devices
Evaluate existing policies and determine any modifications or additions required to support and implement those policies on a managed Apple device.

- MDM restrictions for iPhone and iPad devices
- MDM restrictions for Mac computers
- MDM restrictions for Apple TV devices
- MDM restrictions for supervised Apple devices
- Review MDM restrictions for Apple devices

Evaluate existing policies and determine which features from a particular MDM solution can be used to support and implement those policies on a managed Apple device.

- MDM restrictions for iPhone and iPad devices
- MDM restrictions for Mac computers
- MDM restrictions for Apple TV devices
- MDM restrictions for supervised Apple devices
- Review MDM restrictions for Apple devices

Given a set of criteria that an organization defines, evaluate existing policies and determine which built-in features from a managed Apple device can be used to support and implement those policies.

- MDM restrictions for iPhone and iPad devices
- MDM restrictions for Mac computers
- MDM restrictions for Apple TV devices
- MDM restrictions for supervised Apple devices
- Review MDM restrictions for Apple devices

Compare and contrast the actions that an MDM administrator can take on a managed user-owned and organization-owned Apple device.

- User Enrollment and MDM
- Device Enrollment and MDM
- Automated Device Enrollment and MDM
- Intro to certificate management for Apple devices
- Intro to Apple device enrollment types

Compare and contrast the data that an MDM administrator can view on a managed user-owned and organization-owned Apple device.

- User Enrollment and MDM
- Device Enrollment and MDM
- Automated Device Enrollment and MDM
- Intro to certificate management for Apple devices
- Intro to Apple device enrollment types

Discern and classify the key user-configurable, on-device security-related settings on a managed Apple device for iOS and macOS.

- Volume encryption with FileVault in macOS
• Apple Platform Security
• Additional macOS system security capabilities
• Review MDM restrictions for Apple devices
• Manage FileVault with mobile device management

Identify the types of extensions that relate to separating work and personal data on managed Apple devices.

• Supporting extensions in iOS, iPadOS, and macOS
• User Enrollment and MDM

Discern the certificate and identity formats that Apple devices support.

• Certificates MDM payload settings for Apple devices
• Certificate Preference MDM payload settings for Apple devices
• Available trusted root certificates for Apple operating systems
• Distribute certificates to Apple devices

Discern and classify the three categories of certificates stored in the Trust Store on an Apple device.

• Certificates MDM payload settings for Apple devices
• Certificate Preference MDM payload settings for Apple devices
• Available trusted root certificates for Apple operating systems
• Distribute certificates to Apple devices

Identify the resource that contains the list of available trusted root certificates for Apple operating systems.

• Certificates MDM payload settings for Apple devices
• Certificate Preference MDM payload settings for Apple devices
• Available trusted root certificates for Apple operating systems
• Distribute certificates to Apple devices

Discern and classify the key components of a digital certificate.

• Certificates MDM payload settings for Apple devices
• Certificate Preference MDM payload settings for Apple devices
• Available trusted root certificates for Apple operating systems
• Distribute certificates to Apple devices

Identify Automated Certificate Management Environment payloads.

• Device Management Profile — ACME Certificate

Deploy Apple devices with cellular connections.

• Prepare to use eSIMs with Apple devices

Evaluate an organization’s infrastructure with respect to profiles and payloads.

• Use Apple products on enterprise networks
• Configure your network for MDM

Evaluate an organization’s infrastructure with respect to Apple devices.
• Use Apple products on enterprise networks
• Configure your network for MDM

Plan your MDM migration.
• Reenroll devices in MDM
• Intro to planning your MDM migration

Preparing
Evaluate your organization's infrastructure — Wi-Fi coverage and capacity, proxies, firewalls, VPN, and Bonjour — for use of Apple devices.
• WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
• Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
• Extensible Authentication Protocol (EAP) MDM settings for Apple devices
• Wi-Fi MDM settings for Apple devices

Evaluate and recommend strategies for your organization to optimize its network configuration for device access to Apple-specific services.
• WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
• Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
• Extensible Authentication Protocol (EAP) MDM settings for Apple devices
• Wi-Fi MDM settings for Apple devices

Evaluate the integration of core services — email, calendar, and contacts — for optimized use on Apple devices within your organization's network infrastructure.
• WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
• Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
• Extensible Authentication Protocol (EAP) MDM settings for Apple devices
• Wi-Fi MDM settings for Apple devices

Summarize technical considerations for integrating Apple devices into an existing network.
• WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
• Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
• Extensible Authentication Protocol (EAP) MDM settings for Apple devices
• Optimize your Wi-Fi networks for Apple devices
• Use Apple products on enterprise networks
• Wi-Fi MDM settings for Apple devices

Identify the requirements for integrating Apple devices into an existing network.
• WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
• Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
• Extensible Authentication Protocol (EAP) MDM settings for Apple devices
• Wi-Fi MDM settings for Apple devices
Determine the considerations for integrating Apple devices into an existing network.

- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Identify enrollment requirements for Apple Business Manager.

- Requirements for Apple Business Manager

Discern the types and functions of the parameters entered during the enrollment process in Apple School Manager.

- Requirements for Apple School Manager

Given valid credentials, log in to Apple Business Manager and create a location and user account and groups.

- View and assign roles in Apple Business Manager
- Configure locations in Apple Business Manager

In Apple Business Manager or Apple School Manager, link an MDM server by downloading the token and installing it into MDM.

- Manage server tokens in Apple School Manager
- Manage server tokens in Apple Business Manager

Point platforms at the MDM server automatically.

- Device workflow in Apple Business Manager
- Deploy devices using Apple School Manager, Apple Business Manager, or Apple Business Essentials

Explain Directory Sync requirements for Apple Business Manager.

- Intro to federated authentication with Apple Business Manager
- Intro to Google Workspace with Apple Business Manager
- Intro to Google Workspace with Apple School Manager
- Use federated authentication with Google Workspace in Apple School Manager
- Intro to federated authentication with Apple School Manager

Integrate the Schoolwork app, the Classroom app, and tools.

- Create classes synced with Apple School Manager in Classroom
- Use Schoolwork to manage student progress in Apple School Manager

Use federated authentication across multiple systems.

- Intro to federated authentication with Apple School Manager

Exploring the Tools

Define Apple Business Manager.

- Intro to Apple Business Manager

Identify why organizations use Apple Business Manager.
• **Intro to Apple Business Manager**

Explain the purpose of roles and locations in Apple Business Manager.

• **Intro to roles and privileges in Apple Business Manager**

• **Configure locations in Apple Business Manager**

Explain what a Managed Apple ID is and describe its use.

• **Use Managed Apple IDs in Apple Business Manager**

Explain who owns volume purchased app and book licenses after distribution.

• **Intro to purchasing content in Apple Business Manager**

Identify app and book distribution methods based on device type and ownership.

• **Intro to purchasing content in Apple Business Manager**

Define Apple School Manager.

• **Intro to Apple School Manager**

Identify why educational organizations use Apple School Manager.

• **Intro to Apple School Manager**

Explain the purpose of roles and locations in Apple School Manager.

• **Intro to roles and privileges in Apple School Manager**

• **Configure locations in Apple School Manager**

Compare and contrast the features and functions related to managed devices for Apple Configurator versus MDM.

• **Configure devices with Apple Configurator for Mac**

• **Deploy devices using Apple School Manager, Apple Business Manager, or Apple Business Essentials**

Use Apple Configurator to add Mac computers and iPhone devices to Apple Business Manager or Apple School Manager.

• **Add devices from Apple Configurator to Apple Business Manager**

• **Add Apple devices to Apple School Manager, Apple Business Manager, or Apple Business Essentials**

### Enrolling Devices

Complete the MDM enrollment and configuration profile installation process on a user-owned device with SSO.

• **Discover account-driven User Enrollment — WWDC21 Video**

• **Discover Authentication Servers**

• **User Enrollment and MDM**

Use an MDM solution to send configuration profiles to devices.

• **Review MDM payloads for Apple devices**

• **Plan your configuration profiles for Apple devices**

Manually add devices to an MDM solution.

• **Add devices from Apple Configurator to Apple Business Manager**
• Add Apple devices to Apple School Manager, Apple Business Manager, or Apple Business Essentials

Use an MDM solution to create an enrollment profile and deploy it to devices.
  • Device Enrollment MDM payload list
  • Automated Device Enrollment MDM payload list
  • User Enrollment MDM information

Assign organization-owned devices to an MDM server in Apple School Manager.
  • Assign, reassign, or unassign devices in Apple School Manager

Assign devices to an MDM solution with Apple Business Manager.
  • Assign, reassign, or unassign devices in Apple Business Manager

Assign organization-owned devices to an MDM server in Apple Business Manager.
  • Assign, reassign, or unassign devices in Apple Business Manager

Manually enroll an organization-owned iPhone into an MDM solution. (Profile Driven)
  • User Enrollment MDM information
  • User Enrollment and MDM

Use Apple Configurator to enroll iPhone and Apple TV devices into an MDM solution.
  • Add devices from Apple Configurator to Apple Business Manager
  • Add Apple devices to Apple School Manager, Apple Business Manager, or Apple Business Essentials

Manage Setup Assistant.
  • Manage Setup Assistant for Apple devices

Set up devices with Setup Assistant.
  • Manage Setup Assistant for Apple devices

Identify which Setup Assistant options you can configure on iPhone, Mac, and Apple TV devices.
  • Add content to devices in Apple Configurator
  • Automated Device Enrollment and MDM
  • Manage Setup Assistant for Apple devices

Use an MDM solution to configure Setup Assistant for organization-owned Apple devices.
  • Automated Device Enrollment and MDM
  • Manage Setup Assistant for Apple devices

Describe the ways that users can customize organization-owned devices.
  • Review MDM restrictions for Apple devices
  • Device Enrollment MDM payload list

Identify key methods for creating a personal experience using policy controls on managed Apple devices.
  • Review MDM restrictions for Apple devices
  • Security MDM payload settings for Apple devices

Recognize key considerations that relate to creating a personal experience using policy controls on managed Apple devices.
• Review MDM restrictions for Apple devices
• Security MDM payload settings for Apple devices

Prepare a shared iPad. (Temporary Sessions)
• Shared iPad overview
• Prepare Shared iPad

Distribute organization-owned devices to users.
• Deploy devices using Apple School Manager, Apple Business Manager, or Apple Business Essentials

Getting Content

Sign up for Apps and Books in Apple Business Manager.
• Sign up for Apple Business Manager

Link Apps and Books purchases to your MDM solution.
• Manage server tokens in Apple Business Manager

Buy content in volume with Apps and Books in Apple Business Manager.
• Select and purchase content in Apple Business Manager
• Intro to purchasing content in Apple Business Manager

Buy apps and books in Apple Business Manager.
• Select and purchase content in Apple Business Manager
• Intro to purchasing content in Apple Business Manager

Sign up for Apps and Books in Apple School Manager.
• Sign up for Apple School Manager

Link Apps and Books purchases to your MDM solution.
• Manage server tokens in Apple School Manager

Purchase content in volume with Apps and Books in Apple School Manager.
• Select and purchase content in Apple School Manager
• Intro to purchasing content in Apple School Manager

Explain how content caching in macOS caches and optimizes downloaded Apple content on your network.
• Content types supported by content caching in macOS
• Plan for and set up content caching
• Content caching metrics on Mac
• Apple Platform Deployment
• Content caching from the command line on Mac
• Intro to content caching

Give examples of downloaded Apple content that’s cached.
• Content types supported by content caching in macOS
• Plan for and set up content caching
Explain how caching across subnets works.

Give examples of when to use additional content caching configuration to bypass firewalls or compensate for network traffic management.

Explain how tethered caching works.

Set up content caching in macOS.

Manage content caching.

Set up tethered caching.
Set up a shared internet connection for iPhone and iPad

Optimize content caching by configuring advanced content cache settings.

- Content types supported by content caching in macOS
- Plan for and set up content caching
- Content caching metrics on Mac
- Apple Platform Deployment
- Content caching from the command line on Mac
- Intro to content caching

Manage content caching from the command line.

- Content types supported by content caching in macOS
- Plan for and set up content caching
- Content caching metrics on Mac
- Apple Platform Deployment
- Content caching from the command line on Mac
- Intro to content caching

Transfer purchased app licenses for managed distribution to another location in Apple Business Manager.

- Transfer licenses to another location in Apple Business Manager

Transfer purchased app licenses for managed distribution to another location in Apple School Manager.

- Transfer licenses to another location in Apple School Manager

Configuring Devices

Identify MDM payloads that can be used to configure security-related settings on managed Apple devices for iOS, iPadOS, and macOS.

- MDM restrictions for supervised Apple devices
- Security MDM payload settings for Apple devices

Recognize key considerations that relate to joining managed Apple devices to Wi-Fi networks.

- macOS wireless roaming for enterprise customers
- Secure access to wireless networks
- Optimize your Wi-Fi networks for Apple devices

List common wireless authentication methods that Apple devices use to connect to a network.

- macOS wireless roaming for enterprise customers
- Secure access to wireless networks
- Optimize your Wi-Fi networks for Apple devices

Identify the purpose or function of a proxy auto-configuration (PAC) file on managed Apple devices.

- Filter content for Apple devices
Identify key payloads and settings that MDM uses to configure a managed Apple device to use proxy settings using a PAC URL on a specific network.

- Apple Platform Deployment

Discern and classify the key references for iOS, iPadOS, and macOS that relate to common MDM settings associated with configuring managed Apple devices for wireless network authentication.

- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Identify key methods for joining managed Apple devices to Wi-Fi networks.

- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Identify key wireless network authentication standards that Apple devices support.

- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Recognize key considerations that relate to configuring 802.1X in iOS, iPadOS, and macOS.

- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Identify key methods for configuring 802.1X in iOS, iPadOS, and macOS.

- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Identify the purpose or function of Apple Push Notification service (APNs) for managing Apple devices.

- Configure devices to work with APNs

Identify key ports and protocols that MDM uses to communicate with APNs.

- Configure devices to work with APNs

Identify key payloads and settings that MDM uses to configure a managed Apple device to connect automatically to a supported Wi-Fi network using a supported authentication protocol.

- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Using MDM, configure a managed Apple device to use proxy settings using a PAC URL on a specific network.
- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Explain the benefits of deploying devices with cellular connectivity.
- Prepare to use eSIMs with Apple devices

Deploy devices with cellular connectivity.
- Prepare to use eSIMs with Apple devices
- Deploy iPad with cellular connections

Using MDM, configure a managed Apple device to connect automatically to a supported Wi-Fi network using a supported authentication protocol.
- WEP, WPA, WPA2, WPA2/WPA3 MDM settings for Apple devices
- Dynamic WEP, WPA Enterprise, and WPA2 Enterprise MDM settings for Apple devices
- Extensible Authentication Protocol (EAP) MDM settings for Apple devices
- Wi-Fi MDM settings for Apple devices

Configure device payloads for VPN to work with APNs.
- Filter content for Apple devices

Configure devices to connect to VPN using SSL through MDM.
- Use SSL VPN clients for Apple devices

Configure devices to automatically use Always-On VPN using MDM.
- VPN settings overview for Apple devices
- VPN overview for Apple device deployment

Configure devices to automatically use VPN On Demand using MDM.
- VPN settings overview for Apple devices
- VPN overview for Apple device deployment

Create custom configuration profiles for Apple devices.
- Review MDM payloads for Apple devices
- Plan your configuration profiles for Apple devices

Use Apple Configurator to automate bulk deployments by combining actions using Blueprints.
- Use Blueprints in Apple Configurator

View log messages and activity in Apple Configurator.
- View log messages and activity in Apple Configurator

Automate repetitive tasks with scripting that Apple Configurator can't do.
• **Use Blueprints in Apple Configurator**
  Use `cfgutil` scripting to automate repetitive tasks not present in Apple Configurator.
  • **Use the Apple Configurator command-line tool**

**Manage accessory restrictions.**

• **Manage Thunderbolt and USB pairing with Apple devices**
• **What’s new in Apple platform deployment**

**Configure a managed Apple device to use certificates and identities with an MDM solution.**

• **Certificates MDM payload settings for Apple devices**
• **Certificate Preference MDM payload settings for Apple devices**
• **Distribute certificates to Apple devices**

**Identify the purpose or function of using restrictions to manage Apple devices.**

• **Intro to mobile device management profiles**

**Identify restrictions that apply only to supervised Apple devices.**

• **MDM restrictions for supervised Apple devices**

**Restrict the use of Touch ID to unlock a device.**

• **Review MDM restrictions for Apple devices**

**List Active Directory certificate MDM payload settings.**

• **Active Directory Certificate MDM payload settings for Apple devices**

**Discern and classify the key references that relate to managing digital certificates and identities on Apple devices.**

• **Certificates MDM payload settings for Apple devices**
• **Certificate Preference MDM payload settings for Apple devices**
• **Distribute certificates to Apple devices**

**Identify key payloads and settings that MDM uses to configure a managed Apple device to use certificates and identities.**

• **Certificates MDM payload settings for Apple devices**
• **Certificate Preference MDM payload settings for Apple devices**
• **Distribute certificates to Apple devices**

**Discern and classify the key uses of a digital certificate as they relate to deploying and managing Apple devices.**

• **Certificates MDM payload settings for Apple devices**
• **Certificate Preference MDM payload settings for Apple devices**
• **Distribute certificates to Apple devices**

**Discern and classify the key formats of a digital certificate identity that Apple devices support.**

• **Certificates MDM payload settings for Apple devices**
• **Certificate Preference MDM payload settings for Apple devices**
• **Distribute certificates to Apple devices**
Recognize key considerations that relate to trusting and verifying digital certificates with managed Apple devices.

- Certificates MDM payload settings for Apple devices
- Certificate Preference MDM payload settings for Apple devices
- Distribute certificates to Apple devices

Recognize the key purpose, components, and function of the chain of trust as it relates to managed Apple devices.

- Certificates MDM payload settings for Apple devices
- Certificate Preference MDM payload settings for Apple devices
- Distribute certificates to Apple devices

Recognize key considerations that relate to managing certificates and identities on Apple devices.

- Certificates MDM payload settings for Apple devices
- Certificate Preference MDM payload settings for Apple devices
- Distribute certificates to Apple devices

Distinguish the process for managing certificates and identities on Apple devices.

- Certificates MDM payload settings for Apple devices
- Certificate Preference MDM payload settings for Apple devices
- Distribute certificates to Apple devices

Distinguish the process for managing a smart card on Apple devices.

- Smart Card MDM payload settings for Apple devices
- Advanced smart card options on Mac
- Intro to smart card integration

Managing Content

Distribute custom apps to Apple devices.

- Distribute Custom Apps to Apple devices

Distribute unlisted apps to Apple devices.

- Distribute Unlisted Apps to Apple devices

Distribute apps to devices and users.

- Distribute Managed Apps to Apple devices

Configure apps on devices.

- Apple Platform Deployment

Revoke apps distributed to devices and users.

- Intro to content distribution for Apple devices
- Content distribution methods for Apple devices

Prevent users from installing or removing apps.
• Review MDM restrictions for Apple devices
Manage Rapid Security Response on Apple devices.
  • What's new in Apple platform deployment

Managing Data
Use an MDM solution to manage configurations, apps, documents, and data on devices.
  • Distribute Managed Apps to Apple devices
Install managed content on a managed Apple device.
  • Distribute Managed Apps to Apple devices
Install managed apps on a managed Apple device.
  • Distribute Managed Apps to Apple devices
Configure Managed Open In restrictions on a managed iPhone or iPad.
  • Distribute Managed Apps to Apple devices
Configure managed notification previews on a managed Apple device.
  • Notifications MDM payload settings for Apple devices
Distinguish the types of content that MDM can manage on managed Apple devices.
  • Distribute Managed Apps to Apple devices
Enforce the use of passcodes during enrollment.
  • Passcode MDM payload settings for Apple devices
Identify passcode configuration options for Apple devices.
  • Passcode MDM payload settings for Apple devices
Use an MDM solution to configure passcode requirements for Apple devices.
  • Passcode MDM payload settings for Apple devices
Identify the purpose or function of using restrictions to manage Apple devices.
  • Review MDM restrictions for Apple devices
Identify restrictions that apply to all Apple devices.
  • Review MDM restrictions for Apple devices
Use an MDM solution to configure content, functionality, and settings restrictions for Apple devices.
  • Review MDM restrictions for Apple devices
Use an MDM solution to require FileVault on managed Mac computers.
  • Manage FileVault with mobile device management
Describe what’s encrypted on macOS, iOS, and iPadOS, including where keys can be stored for FileVault.
  • Encryption and Data Protection overview
  • Additional macOS system security capabilities
  • Volume encryption with FileVault in macOS
Manage accessory security for Mac computers.
Change Privacy & Security settings on Mac
Recognize when it’s appropriate to use Lockdown Mode, and demonstrate how to exclude apps and websites from Lockdown Mode.

- Use the built-in security and privacy protections of iPhone
- Harden your iPhone from a cyberattack with Lockdown Mode
- About Lockdown Mode

Managing Lost Devices
Recognize the key purpose and function of Lost Mode as it relates to managed Apple devices.

- Lock and locate Apple devices
Issue commands and send payloads that help protect managed devices in the event of loss or theft.

- MDM commands for Apple devices
Define the key purpose and function of Activation Lock as it relates to managed Apple devices.

- Activation Lock for iPhone, iPad, and iPod touch
- Activation Lock on Apple devices
Apply Lost Mode and Activation Lock on managed devices.

- Activation Lock for iPhone, iPad, and iPod touch
- Activation Lock on Apple devices
Demonstrate how to wipe devices safely using an MDM solution.

- Erase Apple devices
- Managed Lost Mode and remote wipe

Querying Devices
Identify the types of queries that are supported on a managed Apple device from MDM.

- Security MDM queries for Apple devices
- Installed app MDM queries for Apple devices
- Device information MDM queries for Apple devices
Discern and classify the key references for iOS and macOS that relate to common MDM queries issued to managed Apple devices.

- Security MDM queries for Apple devices
- Installed app MDM queries for Apple devices
- Device information MDM queries for Apple devices
Use MDM to display detailed information about a managed Apple device.

- Security MDM queries for Apple devices
- Installed app MDM queries for Apple devices
- Device information MDM queries for Apple devices
Identify the categories of information that MDM can display for a managed Apple device.

- Security MDM queries for Apple devices
- Installed app MDM queries for Apple devices
- Device information MDM queries for Apple devices

Use MDM to issue queries to a managed Apple device.

- Security MDM queries for Apple devices
- Installed app MDM queries for Apple devices
- Device information MDM queries for Apple devices

Use MDM to display detailed information about a managed Apple device.

- Security MDM queries for Apple devices
- Installed app MDM queries for Apple devices
- Device information MDM queries for Apple devices

Managing Traffic

Configure app prioritization and proxies to manage traffic.

- Global HTTP Proxy MDM payload settings for Apple devices
- Cisco Fastlane MDM settings for Apple devices

Configure app priorities in your MDM solution.

- Cisco Fastlane MDM settings for Apple devices

Configure proxies in your MDM solution.

- Global HTTP Proxy MDM payload settings for Apple devices

Updating Devices

Manage software updates on Apple devices with an MDM solution.

- About software updates for Apple devices

Defer software updates on managed iPhone and Apple TV devices.

- About software updates for Apple devices

Recycling Devices

Explain different ways to prepare a device for a return to service.

- Reenroll devices in MDM

Explain options for trading in and recycling your organization's retired devices.

- Apple Trade In
- What to do before you sell, give away, or trade in your iPhone or iPad
Sample Questions

To practice for the exam, try to answer each of these sample questions. Then use the answer key to check your answers. These sample questions aren't on the actual exam but represent the types of questions included.

**Question 1**
Which configuration profile payload requires supervision?

A. Enforce setting a passcode
B. Modify Personal Hotspot settings
C. Trusting new enterprise app authors
D. Disable AirDrop as an unmanaged destination

**Question 2**
Which configuration profile payload restriction requires supervision?

A. Disable Safari web browser
B. Enforce setting a passcode
C. Trusting new enterprise app authors
D. Treat AirDrop as an unmanaged destination

**Question 3**
*Select four responses.*

Which four options are good practices before trading in and recycling your organization's retired devices?

A. Back up your device.
B. Reset your device password.
C. Remove the lithium-ion battery.
D. Remove your old device from your list of trusted devices.
E. Sign out of iCloud and the iTunes Store and the App Store.
F. Remove the devices from Apple School Manager and Apple Business Manager.
Question 4

Scenario

Township Schools wants to deploy 150 Apple TV devices in its high schools. The Apple TV devices are a mix of products purchased directly from Apple and some newly donated devices.

Select two responses.

Which two device enrollment types should you use to enroll these Apple TV devices into your MDM solution?

A. User Enrollment
B. Device Enrollment
C. Declarative Enrollment
D. Automated Device Enrollment

Question 5

What are some of the basic network requirements for setting up an on-premise MDM solution?

A. A fully qualified domain name, TLS certificate communication, and a static IP address
B. Activation Lock escrow keys, firewall ports 2195/2196, and a fully qualified domain name
C. A static IP address, a robust disaster recovery solution, and encrypted database connectivity
D. A Transport Layer Security certificate, firewall ports 2195/2196, and a macOS bootstrap token

Question 6

Which enrollment type supports separating personal user data and organization data on iPhone and iPad?

A. User Enrollment
B. Device Enrollment
C. Automated Device Enrollment
D. Declarative Device Enrollment

Question 7

Which cloud identity provider can you use to automatically create Managed Apple IDs with federated authentication?

A. Open Directory
B. Google Workspace
C. Microsoft Active Directory
Question 8
Which Managed Open In restriction can you enforce using an MDM solution?
A. Pasting content from a managed app to a managed app
B. Pasting content from a managed app to an unmanaged app
C. Pasting content from an unmanaged app to an unmanaged app

Question 9
What should you use to remotely access private organization networks?
A. SSH
B. SSL
C. TLS
D. VPN

Question 10
What is required to support SSL VPN connections for Apple devices?
A. Provider companion app
B. Push certificate
C. Secure Wi-Fi
D. MDM

Question 11
Which assignment method should you use to distribute book licenses that were bought within Apple School Manager or Apple Business Manager?
A. User assignment
B. Device assignment
C. Either user or device assignment

Question 12
Scenario
Fabiano is leaving ACME, Inc. and you want to unenroll his personal iPhone from your MDM solution.
What happens to the managed apps that your MDM solution installed on his iPhone?
A. It depends on the setting you selected in your MDM solution.
B. They are instantly removed from his device.
C. They stay on the device and keep working.
D. They stay on the device but stop working.
**Question 13**
What happens to an app when you use your MDM solution to revoke its app license?

A. The icon is dimmed.
B. It unexpectedly quits when opened.
C. It is instantly removed from the device.
D. It continues to function for a limited time.

**Question 14**
Which assignment method can you use to distribute app licenses bought with Apple School Manager and Apple Business Manager?

A. User assignment only
B. Device assignment only
C. User and device assignment

**Question 15**
Which macOS utility identifies the Received Signal Strength Indicator when troubleshooting roaming between access points within a wireless network?

A. Activity Monitor
B. networkQuality
C. getnetworkpower
D. Wireless Diagnostics

**Question 16**
*Select three responses.*
Which three options should you use to optimize your Wi-Fi networks for Apple devices?

A. Standardize on the 5 GHz band
B. Standardize on the 2.4 GHz band
C. Create "hidden" service set identifiers
D. Avoid using "hidden" service set identifiers
E. Avoid creating excessive service set identifiers

**Question 17**
How often do MDM server tokens expire in Apple School Manager and Apple Business Manager?

A. Every six months
B. Once a year
C. Every two years
D. Every three years
Question 18
What allows you to grant privileges to a user in Apple School Manager or Apple Business Manager?

A. Groups
B. Locations
C. Rights
D. Roles

Question 19
Which type of Apple IDs does your organization own?

A. Enterprise Apple IDs
B. Managed Apple IDs
C. Business Apple IDs
D. Personal Apple IDs

Question 20
Select three responses.
Which three features are available for Managed Apple IDs?

A. iCloud Backup
B. iCloud Keychain
C. iCloud Drive
D. Notes
E. Sidecar

Question 21
Select three responses.
Which three Apple School Manager roles have the privileges to add, assign, and remove devices?

A. Manager
B. Site Manager
C. Administrator
D. Content Manager
E. Device Enrollment Manager
Question 22
Which type of information about iPhone can you view in Apple Configurator for Mac, but NOT with an MDM solution?
A. Disk usage
B. Console log
C. Installed apps
D. Battery charge

Question 23
Select two responses.
Which two roles allow you to transfer licenses and apps to other locations in Apple Business Manager?
A. Device Enrollment Manager
B. Content Manager
C. People Manager
D. Administrator

Question 24
Which license type should you choose if your organization wants to retain full ownership and control of apps that you bought in Apple School Manager and Apple Business Manager?
A. App Store credits
B. Managed licenses
C. Volume purchases
D. App redemption codes

Question 25
Select four responses.
Which four content types does the content caching service support on Mac computers?
A. Apple TV+
B. OS updates
C. Apple Music
D. mpeg videos
E. Apple Books
F. iCloud data caching
G. Apps from the App Store
Question 26

Scenario

ACME, Inc. has 350 Apple devices installed over three network subnets. You want to turn on content caching on a Mac mini to optimize your network’s internet bandwidth.

How should you configure content caching?

A. Change content caching settings to devices using custom local networks
B. Configure multiple Ethernet services in Network settings
C. Use default content caching settings
D. Set content caching to parent

Question 27

Scenario

ACME, Inc. has 250 Apple devices that connect to both wired and wireless networks. You plan to turn on content caching on a Mac mini connected to the network.

What should you do to optimize content caching?

A. Connect your Mac mini to the network with a cable and disable Wi-Fi.
B. Enable the Optimize Content Caching Over Wi-Fi setting in content caching advanced options.
C. Add your router IP address to the Parent IP Addresses setting in content caching advanced options.
D. Add your firewall IP address to the Parent IP Addresses setting in content caching advanced options.

Question 28

Select three responses.

Which three are best practices for setting up content caching?

A. Use manual proxy settings
B. Specify a TCP port for caching
C. Block rogue cache registration
D. Manage intersite caching traffic
E. Proxy client requests to content caches

Question 29

What happens when you use Safari on iPad to visit a site with a revoked certificate?

A. You are asked to delete the certificate.
B. You are directed to the CA’s website to update the certificate.
C. A dialog appears noting an issue with the website or service.
D. The message “This Connection Is Not Private” appears instead of the webpage.
Question 30
Which MDM feature should you use to restrict content so that organization content is inaccessible in apps that the user installs?

A. App sandboxing
B. Manage Open In
C. iCloud restriction
D. Account modification restriction

Question 31
Scenario
You want to prevent users from using personal apps to open work email attachments from ACME, Inc.’s managed mail account.

Which feature should you apply using your MDM solution?

A. App Sandbox
B. iCloud restriction
C. Managed Open In
D. Account modification restriction

Question 32
Select three responses.
Which three items are always encrypted on Apple devices?

A. FaceTime communications
B. iMessage communications
C. Email communications
D. Wi-Fi communications
E. HTTPS web browsing

Question 33
Which Mac computers implement FileVault using Data Protection Class C with a volume key?

A. ONLY Intel-based Mac computers
B. ONLY Mac computers with Apple silicon
C. ONLY Mac computers with the Apple T2 Security Chip
D. Mac computers with Apple silicon and the Apple T2 Security Chip
Question 34
What happens to volume encryption keys when FileVault is **NOT** turned on during the initial Setup Assistant process on Mac computers with Apple silicon or the Apple T2 Security Chip?

A. The key is encrypted using only AES-128 bit software encryption.
B. The keys are generated when the first user's password is created.
C. The keys are generated when the first user's password is logged in.
D. The key is protected only by the hardware UID in the Secure Enclave.

Question 35
Scenario
Jesse notifies you that he lost his managed organization-owned iPhone while riding the bus. You want to try to locate the device with your MDM solution.

Which MDM command should you send before you can remotely query the device’s location?

A. Erase device
B. Enable Lost Mode
C. Allow Activation Lock
D. Enable Activation Lock

Question 36
Which query is available for user enrolled devices?

A. FaceTime and phone call logs
B. Installed managed apps
C. SMS and iMessages
D. Device location

Question 37
Scenario
ACME, Inc. is deploying a profile that marks a collaboration app to have a better quality of service than other apps on your Apple device.

Which devices support this setting?

A. iPhone and iPad
B. iPhone, iPad, and Mac
C. iPhone, iPad, Mac, and Apple TV
D. iPhone, iPad, Mac, Apple TV, and Apple Watch
Question 38
Scenario

ACME, Inc. retires 150 iPad devices and turns them in for credit toward new devices through the Apple Trade In program. Twenty iPad devices aren’t eligible for credit.

What happens to the 20 devices that are **NOT** eligible for credit?

A. Apple recycles the devices.
B. Apple refurbishes the devices.
C. Apple returns the devices to you.
D. Apple deducts the recycling fee from your credit.

Question 39
Which profile type is required to send a remote wipe command to a device using MDM?

A. Configuration
B. Enrollment
C. Device
D. User

Question 40
Which macOS version supports declarative status reports?

A. macOS 10.15 and later
B. macOS 11 and later
C. macOS 12 and later
D. macOS 13 and later

Question 41
Select three responses.

Which three restrictions can MDM set in a profile for supervised Apple devices?

A. Use Safari
B. Set passcode
C. Safari AutoFill
D. Password AutoFill
E. Enable Location Services
Question 42
Select three responses.

When User Enrollment is completed on iPhone or iPad, which types of organization data are separated from user data on different volumes?

A. Contacts
B. Reminders
C. Managed apps
D. Keychain items
E. Calendar attachments

Question 43
Select four responses.

What are the four stages of User Enrollment into MDM?

A. Session token
B. User enrollment
C. App installation
D. MDM enrollment
E. Service discovery
F. Create Managed Apple ID

Question 44
Which User Enrollment process, built into the Settings app, makes it easier for users to enroll their personal iPhone?

A. Automated User Enrollment
B. Profile-based User Enrollment
C. Account-based User Enrollment
D. Personal device User Enrollment

Question 45
Which User Enrollment method requires the users to access a given URL to download the enrollment profile?

A. Automated User Enrollment
B. Profile-based User Enrollment
C. Account-based User Enrollment
D. Personal device User Enrollment
**Question 46**  
*Select three responses.*

Which three types of data, essential to continuity of device access, might you lose if you don’t have a robust backup strategy for an on-premises MDM installation?

- A. Bypass codes
- B. User passwords
- C. Device passcodes
- D. macOS bootstrap tokens
- E. Activation Lock escrow keys

**Question 47**  
*Select three responses.*

Which three passcode and password settings can you configure remotely using your MDM solution?

- A. Maximum number of failed attempts before the user account is disabled
- B. Passcode or password history (unable to use previous passwords)
- C. Maximum number of complex characters
- D. Minimum passcode length
- E. Maximum passcode length

**Question 48**  
*Scenario*

Christina enrolled her iPhone in ACME, Inc.’s MDM solution. It deployed a profile requiring her to enter an eight-digit simple passcode. She manually added her Exchange Active Sync account, which requires a six-digit complex passcode.

Which passcode policy is applied to Christina’s iPhone?

- A. Six-digit simple
- B. Six-digit complex
- C. Eight-digit simple
- D. Eight-digit complex
Question 49

Scenario

ACME, Inc. uses its MDM solution to deploy digital certificates to allow iPhone devices access to organization services and protect confidential data.

Which two MDM enrollment types can manage digital certificates on managed Apple devices?

A. Account-Driven User Enrollment
B. Automated Device Enrollment
C. Business Enrollment
D. Device Enrollment
E. User Enrollment

Question 50

What happens when you deploy multiple restriction-based configuration profiles that contain similar payloads with different settings on iPhone or iPad?

A. The least restrictive setting is applied
B. The most restrictive setting is applied
C. No setting is applied if profiles conflict
D. The profile that is assigned last is applied

Question 51

Which formats are the private key part of a certificate identity stored as?

A. .csr, .rsa
B. .cer, .crt
C. .pfx, .p12
D. .der, X.509

Question 52

Which of the following are supported certificate and identity formats for Apple devices?

A. .cer, .crt, .der, .pfx, .p12
B. .cer, .der, .p15, X.509, RSA
C. .pfx, .crt, .p12, 802.1X, SSH
D. .ca, SSH, X.509, TLS 1.0, RADIUS
Question 53
Select three responses.
What are the three categories of trust certificates on Apple devices?
A. Unknown
B. Blocked
C. Trusted
D. Always Ask
E. Pre-approved

Question 54
Which certificate type establishes a chain of trust that verifies other certificates signed by the trusted roots?
A. Root certificate
B. Anchor certificate
C. Trusted certificate
D. Intermediary certificate

Question 55
Where can you find the version of Trust Stores installed on your iPhone and iPad?
A. Settings > General > About > Keychain
B. System Preferences > General > About > Keychain
C. Settings > General > About > Certificate Trust Settings
D. System Settings > General > About > Certificate Trust Settings

Question 56
Select two responses.
Which two devices support the Certificate Revocation MDM payload setting?
A. iPhone
B. iPad
C. Mac
D. Apple TV
E. Apple Watch
**Question 57**

*Scenario*

ACME, Inc. is migrating to a new MDM solution.

How should you delete a nonremovable profile from your Mac?

A. Use your MDM solution to remove the profile.
B. Use Apple Business Manager to remove the profile.
C. Remove the profile by navigating to Settings > General > VPN & Device Management.
D. Remove the profile by clicking the Remove button (-) in System Settings > Privacy & Security > Profiles.

**Question 58**

*Select four responses.*

Which four factors should you consider when you plan to deploy Apple devices on your network?

A. Access to Apple services
B. Security of your organization’s data
C. Complexity of implementing the network
D. Require updating passcodes and passwords
E. Convenience for the user or the technician during setup
F. Set the power levels for all wireless access points to maximum

**Question 59**

How should you configure your firewall to use most Apple services?

A. Allow inbound connections to 17.0.0.0/8
B. Allow outbound connections to *.apple.com
C. Require authentication to identity.apple.com
D. Allow inbound and outbound connections over ports 80 and 443 to *.apple.com
Question 60

Scenario

Township Schools plans on deploying Mac computers and iPad devices to their students. They need to ensure that all devices will be able to successfully connect to the Wi-Fi network.

Select two responses.

Which Wi-Fi configuration profile payload settings will be required to ensure Wi-Fi connectivity?

A. Disable association MAC address randomization
B. Network Authentication Type
C. Network Proxy Configuration
D. Service Set Identifier
E. Auto Join

Question 61

Select three responses.

Which three 802.1X authentication methods are available for Apple devices?

A. ARP
B. EAP
C. PEAP
D. TLS
E. WEP

Question 62

Where should you download an MDM token from Apple Business Manager?

A. MDM Server Assignment
B. Your MDM Servers
C. Token vault
D. Accounts
Question 63
Select three responses.

Which three options are available to teachers from the Apple Classroom app?

A. Lock student's iPad
B. View student's screen
C. Mirror their iPad on student's iPad
D. Launch a specific app on student's iPad
E. Block a specific website on student's iPad

Question 64
Scenario

Township Schools’ teachers and students are using Mac computers. The teachers want to introduce their students to coding.

In addition to the Everyone Can Code Puzzles book, which app should you recommend to the teachers?

A. Homework
B. Classroom
C. Schoolwork
D. Swift Playgrounds

Question 65
Scenario

ACME, Inc. federated its Microsoft Azure Active Directory (Azure AD) @acme.com domain with Apple Business Manager. You want to test that federation is working by using your account with UPN andre@acme.com.

Your account also has these aliases:
andre@dev.acme.com
a.lorico@acme.com
andre.lorico@dev.acme.com

What should you use to log in to your iCloud account?

A. ONLY andre@acme.com
B. andre@acme.com and andre.lorico@dev.acme.com
C. andre.lorico@dev.acme.com, andre@dev.acme.com, and a.lorico@acme.com
D. andre@acme.com, a.lorico@acme.com, andre@dev.acme.com, and andre.lorico@dev.acme.com
Question 66
Select two responses.

What are two ways an organization can benefit from using Apple School Manager or Apple Business Manager?

A. Enables the creation of Managed Apple IDs unique to the organization
B. Contains a store portal to purchase organization-owned devices
C. Allows users to securely use their user-owned devices
D. Enables automatic enrollment into an MDM solution

Question 67
Select three responses.

Which three roles can use their Managed Apple ID using federated authentication to sign in to Apple services?

A. Device Enrollment Manager
B. Content Manager
C. People Manager
D. Administrator
E. Staff

Question 68
Who owns app licenses installed on devices with managed distribution?

A. The device
B. The organization
C. The device owner
D. The Apple ID owner

Question 69
What happens if you install multiple configuration profiles that contain conflicting restrictions on a Mac?

A. An error occurs on subsequent profiles with similar payloads.
B. The most restrictive settings of each profile are applied.
C. The resulting behavior is undefined.
D. The first profile to deploy is applied.
Question 70
Which app should you use to manually add Mac computers to Apple School Manager and Apple Business Manager?

A. Apple Configurator for iPhone
B. iPhone Configuration Utility
C. Apple Business Essentials
D. Profile Manager

Question 71
What is the minimum role required to assign a device to an MDM solution in Apple School Manager and Apple Business Manager?

A. Device Enrollment Manager
B. People Manager
C. Site Manager
D. Administrator

Question 72
Which Setup Assistant pane should you be on before you prepare to enroll Apple TV devices using Apple Configurator into your MDM solution?

A. Choose your language
B. Pair your remote
C. Screen saver
D. Update tvOS
E. Home Screen

Question 73
Select three responses.

Which three types of content and configurations can you add or assign to iPhone and iPad devices using Apple Configurator for Mac?

A. App config
B. Books and PDFs
C. Enrollment profiles
D. Configuration profiles
E. Exchange web services
**Question 74**
Which Setup Assistant pane always appears the first time an iPhone or iPad device is set up, even when using MDM?

A. Device-to-device migration  
B. Passcode lock  
C. Quick Start  
D. Apple ID

**Question 75**
Which privacy setting is enforced when Setup Assistant panes are skipped on Apple devices?

A. More privacy-preserving setting  
B. Least privacy-preserving setting  
C. Setup Assistant panes can't be skipped  
D. Setup Assistant pane is skipped with a privacy warning

**Question 76**
When using Automated Device Enrollment, on which Apple device can all Setup Assistant panes be skipped?

A. Supervised Apple TV with tvOS 10 or later installed  
B. Supervised Mac with macOS 11 or later installed  
C. Supervised iPad with iPadOS 15 or later installed  
D. Supervised iOS device with iOS 15 or later installed

**Question 77**
*Scenario*
ACME, Inc. chooses to **NOT** allow users to interact with specific Setup Assistant panes, such as Apple Pay.

What is the expected device behavior after completing Setup Assistant?

A. The setting is grayed out.  
B. The user can modify the setting.  
C. Options to manage the setting are hidden.  
D. The MDM profile must be removed before modifying.
**Question 78**  
*Scenario*

ACME, Inc. wants to ensure that users CANNOT wipe an enrolled iPad from an unpaired Mac computer. What is the earliest version of iPadOS to restrict this by default?

A. iPadOS 13.4  
B. iPadOS 14.0  
C. iPadOS 14.5

**Question 79**  
How does restricting Proximity AutoFill affect iPadOS?

A. Devices do not advertise to nearby devices for Wi-Fi passwords  
B. Devices do not advertise to nearby devices for Safari passwords  
C. Devices do not advertise to nearby devices for any password fields  
D. Devices do not advertise to nearby devices for administrator passwords

**Question 80**  
What is required for a Mac with a serial number in Apple Business Manager to skip all Setup Assistant panes using Auto Advance?

A. A paired keyboard and mouse  
B. Have an active Wi-Fi connection  
C. Have an active Ethernet connection  
D. Mac notebook computers must be plugged into a power source

**Question 81**  
*Select three responses.*

Which three are situations where a network administrator should use content caching?

A. iCloud Drive storage has been maxed out for numerous Apple IDs  
B. Large numbers of apps and books are not installing promptly  
C. iTunes Store movie purchases are slow to download  
D. Network traffic to Apple services is extremely high  
E. Shared iPad login times are slow
**Question 82**
Which licenses can you transfer from one location to another in Apple School Manager and Apple Business Manager?

A. ONLY assigned licenses to another location.
B. ONLY unassigned licenses to another location.
C. You CANNOT transfer licenses to another location.
D. Both assigned and unassigned licenses to another location.

**Question 83**
What is the recommended best practice when you create SSIDs on a network?

A. Create six or fewer SSIDs
B. Create five or fewer SSIDs
C. Create four or fewer SSIDs
D. Create three or fewer SSIDs

**Question 84**
Select three responses.

Which three authentication methods do Apple devices support?

A. ARP
B. DLP
C. RADIUS
D. WPA2
E. WPA3

**Question 85**
When should you refer to a PAC file in a configuration profile?

A. To use VPN proxy automatic configuration
B. To use DNS Proxy automatic configuration
C. To use Global HTTP proxy automatic configuration
D. To use Content filter providers automatic configuration
**Question 86**

Select two responses.

Which two settings are required when you create a Wi-Fi configuration profile for the TTLS 802.1X authentication method?

A. Identity certificate  
B. Account user name  
C. Inner authentication  
D. Two-factor authentication  
E. Use directory authentication

**Question 87**

Scenario

Township Schools' IT department will use its MDM solution to deploy a global HTTP proxy to provide internet content filtering on devices both at school or at home.

Select three responses.

Which three items are supported when using a global HTTP proxy payload?

A. Proxy PAC URL  
B. Identity certificate  
C. SOCKS extension  
D. IP address of the proxy server  
E. DNS name of the proxy server

**Question 88**

What is required when you configure devices to use SSL VPN through MDM?

A. The provider’s VPN app  
B. A certificate configuration  
C. A configuration profile with SSL VPN settings  
D. An additional network interface in System Settings

**Question 89**

What can you use Apple Configurator Blueprints for?

A. To export device console logs  
B. To create Automator workflows  
C. To create shell scripts and automate specific processes  
D. To create device templates and apply them to multiple devices
**Question 90**
Which tool should you use to create Apple Configurator automated workflows that you can share with your colleagues?

A. Xcode  
B. Blueprints  
C. Automator  
D. Swift Playgrounds

**Question 91**
*Scenario*
You are using Apple Configurator to prepare your iPad devices. You’d like to automate the process by using command-line script with the cfgutil command.

What should you do before using the cfgutil command?

A. Install Xcode tools.  
B. Install the cfgutil from the App Store.  
C. Install the Automation Tools in the Apple Configurator menu.  
D. Download and install the cfgutil from the developer website.

**Question 92**
*Select four responses.*
Which four Touch ID restrictions are possible using MDM?

A. Users can’t add Touch ID fingerprints  
B. Users can remove Touch ID fingerprints  
C. Users can authenticate only with Touch ID  
D. Users can’t use Touch ID to unlock a device  
E. Users can’t use Touch ID to autofill app data  
F. Users can’t use Touch ID to perform software updates

**Question 93**
What does macOS use for user and group resolution to integrate with Active Directory?

A. Lightweight Directory Access Protocol  
B. Distributed File System  
C. Identity as a service  
D. Kerberos
**Question 94**

*Scenario*

ACME's IT department needs to deploy a profile containing a Microsoft Exchange payload that requires certificates.

*Select two responses.*

Which two Certificates payload settings are required?

A. PAC URL
B. Passphrase
C. Certificate name
D. Certificate UUID

**Question 95**

*Select three responses.*

What are three optional Smart Card MDM payload settings for Apple devices?

A. User pairing
B. Smart Card use
C. Disable screen saver
D. Restrict one smart card per user
E. Allow multiple smart cards per user

**Question 96**

Which option should you use as an authentication method for VPN On Demand?

A. User-based authentication
B. Client-based authorization
C. System-based authentication
D. Certificate-based authentication

**Question 97**

*Select three responses.*

Which three wireless network authentication and encryption protocols do Apple products support?

A. WPA2 Enterprise
B. WPA3 Enterprise
C. WPA2 Personal
D. WPA4 Personal
E. WPA2 Personal
Question 98
How long must you wait to reassign an app after you’ve revoked it from a device or user?

A. You can reassign the app immediately.
B. You must wait 30 days before reassigning the app.
C. You must wait 24 hours before reassigning the app.
D. You must wait 60 minutes before reassigning the app.

Question 99
What is required to prevent a user from installing apps when the “Allow installing apps” restriction is on an iOS device?

A. The device must be supervised.
B. A VPN configuration is required.
C. A personal Apple ID is required on the device.
D. It must be used with the “Allow removing apps” restriction.

Question 100
Select three responses.

Which three restrictions should you set to protect your organization's app data in your MDM solution?

A. Allow documents from unmanaged sources in managed destinations
B. Allow documents from managed sources in unmanaged destinations
C. Allow opening a PDF from a website
D. Allow opening a PDF from an email
E. Managed Pasteboard

Question 101
Select three responses.

Which three of the following are a managed source?

A. Accounts installed using Apple Configurator for Mac
B. Apps installed using Apple Configurator for Mac
C. Apps and accounts installed using MDM
D. Accounts set up manually on the device
E. Apps installed from website
Question 102
Scenario

The Mac computers at Township Schools use Active Directory authentication for students. The school district is enrolling its Mac computers into MDM. Both Active Directory and MDM have password policies being deployed to the computers.

Which password policy will be applied?
A. The more stringent policy will be applied.
B. The strictest settings from each policy will be applied.
C. Directory-based accounts will always defer to Active Directory for a password policy.
D. Both local and directory-based accounts will use password policy settings from MDM.

Question 103
Scenario

ACME, Inc. allows users to personalize their organization-owned iPhone. Users work with client data that contains Personally Identifiable Information (PII). The IT team will enable the Managed Pasteboard restriction using MDM to restrict the copying and pasting of sensitive data.

What else is needed for Managed Pasteboard to function as expected?
A. A managed app
B. A Managed Apple ID
C. Deploy a secure content app
D. A configuration profile to restrict the App Store

Question 104
Select three responses.

Which three restrictions can you apply to iPhone, iPad, and a Mac computer?
A. Handoff
B. Managed Pasteboard
C. iCloud Private Relay
D. Defer software updates
E. Allow network drive connections
Question 105
Scenario

Christina lost her managed organization-owned iPhone at a store. You sent the Enable Managed Lost Mode command to the device with your MDM solution.

Select three responses.

Which three other actions should you take with your MDM solution to locate the device?

A. Display a message on the Lock Screen
B. Query for the device's location
C. Flash the front camera light
D. Vibrate the phone
E. Play a sound

Question 106
Which behavior is expected for an Apple device with Activation Lock enabled?

A. It is impossible to reconfigure or wipe the device.
B. The device is automatically wiped after 10 failed passcode attempts.
C. It is impossible to successfully connect the device to a computer with a USB cable.
D. If the device is wiped, the Apple ID credentials are required to reconfigure the device.

Question 107
Which feature can deter someone from reactivating your Apple device without your permission if you wipe your device remotely?

A. Face ID
B. Activation Lock
C. Secure Enclave
D. Managed Lost Mode

Question 108
What is possible if you enable Lost Mode on an iPhone device with your MDM solution?

A. You can query its location even if it is turned off.
B. You can query the location of unsupervised devices.
C. The device can take a photo with its front camera if it moves.
D. You can query its location even if Location Services are turned off.
Question 109

Select three responses.

Which three MDM queries are available for iPad?

A. Security queries
B. Enrollment queries
C. Installed app queries
D. Device information queries
E. Configuration profile queries

Question 110

Select three responses.

Which three MDM queries are available for iPhone?

A. Device network information queries
B. Configuration profile queries
C. Operating system queries
D. Enrollment queries
E. Security queries

Question 111

Select three responses.

Which three MDM queries are unique to iPhone and iPad?

A. Find My enabled
B. Passcode present
C. Secure boot status
D. Passcode compliant
E. Can Activation Lock be managed

Question 112

Select three responses.

Which three MDM queries are supported for Mac computers?

A. System Integrity Protection enabled
B. Lights Out Management
C. EAS device identifier
D. Find My enabled
E. Apple silicon
Question 113

Scenario
ACME, Inc. needs to prioritize its video conferencing Wi-Fi traffic higher than Safari web traffic. Using ACME's MDM solution, you deploy a network configuration profile with Fastlane Quality of Service (QoS) marking.

Select two responses.

Which two are required when you only want to mark some apps?

A. SSID
B. App name
C. App version
D. App identifier
E. Unique bundle ID
Answer Key

Question 1: B
Question 2: A
Question 3: A, D, E, F
Question 4: B, D
Question 5: A
Question 6: A
Question 7: B
Question 8: B
Question 9: D
Question 10: A
Question 11: A
Question 12: A
Question 13: D
Question 14: C
Question 15: D
Question 16: A, D, E
Question 17: B
Question 18: D
Question 19: B
Question 20: A, C, D
Question 21: B, C, E
Question 22: B
Question 23: B, D
Question 24: B
Question 25: B, E, F, G
Question 26: B
Question 27: A
Question 28: B, C, D
Question 29: D
Question 30: B
Question 31: C
Question 32: A, B, E
Question 33: B
Question 34: D
Question 35: B
Question 36: B
Question 37: C
Question 38: A
Question 39: B
Question 40: D
Question 41: A, C, D
Question 42: C, D, E
Question 43: A, B, D, E
Question 44: C
Question 45: B
Question 46: A, D, E
Question 47: A, B, D
Question 48: D
Question 49: B, D, E
Question 50: B
Question 51: C
Question 52: A
Question 53: B, C, D
Question 54: C
Question 55: C
Question 56: A, B
Question 57: A
Question 58: A, B, C, E
Question 59: B
Question 60: B, D
Question 61: B, C, D
Question 62: B
Question 63: A, B, D
Question 64: D
Question 65: A
Question 66: A, D
Question 67: A, B, E
Question 68: B
Question 69: C
Question 70: A
Question 71: A
Question 72: B
Question 73: B, C, D
Question 74: C
Question 75: A
Question 76: B
Question 77: B
Question 78: C
Question 79: A
Question 80: C
Question 81: B, D, E
Question 82: B
Question 83: D
Question 84: C, D, E
Question 85: C
Question 86: A, B
Question 87: A, D, E
Question 88: A
Question 89: D
Question 90: C
Question 91: C
Question 92: A, B, D, E
Question 93: A
Question 94: C, D
Question 95: A, B, D
Question 96: D
Question 97: A, B, C
Question 98: A
Question 99: A
Question 100: A, B, E
Question 101: A, B, C
Question 102: A
Question 103: A
Question 104: A, C, D
Question 105: A, B, E
Question 106: D
Question 107: B
Question 108: D
Question 109: A, C, D
Question 110: A, C, E
Question 111: A, B, D
Question 112: A, B, E
Question 113: B, E
Exam Details

- The exam name is Apple Deployment and Management Exam (9L0-3025-ENU).
- The exam contains 100 scored technical questions, and you have 120 minutes to complete them.
- The minimum passing score is 74 percent. Scores aren’t rounded.
- The exam uses multiple-choice, multiple-select, and matching questions.
- You may not access any resources or references during the exam.

Taking the Exam

You take the Apple Deployment and Management exam online through the Pearson OnVUE system. Schedule your exam session in advance, and plan to complete the exam in one sitting. You need a private space and a current, government-issued identification card to take the exam.

To learn more about the Pearson OnVUE online proctoring experience, watch this brief video.

Note: Passing the Apple Device Support Exam is a prerequisite to registering for this exam.

To schedule and take the exam, complete these steps:

1. Sign in to ACRS using your Apple ID and password.
2. Click Credentials. Then click Apple Deployment and Management Exam to start the exam registration process.
3. Update the Contact Details for the Testing and Certification section. Answer the additional information questions. If you’re requesting any special accommodations to take the exam, complete the relevant fields. Then click the Submit button.
4. On the notifications page, look for this text: “You may continue to the exam process for Deployment and Management Exam.” Click Continue at Pearson VUE.
5. Follow the instructions to schedule and pay for your exam.

On the day of your scheduled exam, complete these steps:

1. 30 minutes before your scheduled exam time, go to ACRS and sign in with your Apple ID and password.
2. Click the Apple Deployment and Management Exam on the home page.
3. Click Begin Exam, then follow the instructions.

After you complete the exam, Pearson emails you your score. If you don't pass the exam on the first try, you can purchase another exam and retake it after 14 days. You’re allowed four attempts to pass the exam.
About the Certification

The Apple Certified IT Professional certification differentiates you as a skilled professional, gives you a competitive edge in an evolving job market, and associates you with the power of the Apple brand.

When you pass the exam, Credly emails you the instructions to claim your digital badge.

Digital badges are valid for two years from the date earned, but specific expiration dates vary. You keep your badge current by taking the recertification exam when it’s released and before the badge expiration date. Visit training.apple.com and log in to the Apple Certification Records System (ACRS) periodically to ensure that you’re aware as soon as a recertification exam is available.