

100% Money Back **Guarantee**

Vendor: CompTIA

Exam Code: MB0-001

Exam Name: CompTIA Mobility+

Version: Demo

Topic 1, Volume A

QUESTION NO: 1

Which of the following would be used to enforce a policy requiring two-factor authentication on certain mobile devices?

- A. Username and password
- B. Facial recognition and PIN
- C. Pattern unlock and password
- D. Fingerprint and retina scan

Answer: B

Explanation:

QUESTION NO: 2

An employee reports a network connectivity issue to the helpdesk. Which of the following steps should be taken before escalating the issue?

- A. Identify and document the issue, questioning the obvious
- B. Attempt to resolve the network issue by rebooting a server
- C. Ask the user to remote their machine and wait 15 minutes before calling back
- D. Document resolution outcomes and lessons learned

Answer: A

Explanation:

QUESTION NO: 3

Which of the following can be applied to a mobile device to support a corporate mandate which does not allow Internet gambling activities?

- A. Network IDS
- B. Host IDS
- C. Software antivirus
- D. Content filtering

Answer: D

Explanation:

QUESTION NO: 4

When setting up a wireless access point for 802.11g, the user must ensure mobile devices utilize which of the following frequency bands?

- A. 2.4 MHz
- B. 5 MHz
- C. 5 GHz

Answer: A

Explanation:

QUESTION NO: 5

Which of the following is a topology that uses multiple access points to communicate with each other to pass data?

- A. Filter
- B. Mesh
- C. Modulate
- D. Backhaul

Answer: B

Explanation:

QUESTION NO: 6

The mobility team has been tasked with placing Wi-Fi access points in a conference room. They have been provided with a floor plan by the building architect. Which of the following are components of a predictive wireless audit? (Select TWO).

- A. Oscilloscope
- B. Spectrum analysis
- C. Distance to nearest cellular tower
- D. Construction materials used in the walls
- E. Time Domain Reflectometer

Answer: B,D

Explanation:

QUESTION NO: 7

The mobility team is evaluating new smartphones for deployment from multiple vendors. Which of the following items is a concern for the adherence to IT Policy? (Select TWO).

- A. No API for remote management
- B. The ability to set complex passwords
- C. Lack of business applications on the vendor application store
- D. The resolution of the display
- E. Duration of the battery life

Answer: A,B

Explanation:

QUESTION NO: 8

An end-user has notified the helpdesk that a tablet was left in a taxi-cab. Which of the following is the order of response?

- A. Wipe device, track device, escalate
- B. Wipe device, confirm end-user identity, escalate
- C. Confirm end-user identity, determine policy response, report incident
- D. Confirm end-user identity, unlock device, track device

Answer: C

Explanation:

QUESTION NO: 9

The IT department has been contacted by Joe, an end-user, reporting he is unable to login to his smart phone. Which of the following would cause this issue?

- A. The certificate for the Wi-Fi has expired
- B. Passwords must be changed after a certain amount of days
- C. Updates are required to the OS

D. The device is not connected to the Internet

Answer: B

Explanation:

QUESTION NO: 10

The IT department is contacted by Joe, an end-user, who is unable to connect to the corporate IPsec VPN from outside of his corporate network. Joe confirms he can connect to popular web pages. Which of the following would cause this issue?

- A. Port 80 is blocked
- B. Port 587 is blocked
- C. Port 4200 is blocked
- D. Port 5223 is blocked

Answer: C

Explanation:

QUESTION NO: 11

Which of the following is a cellular technology that supports data and voice at the same time?

- A. APN
- B. GSM
- C. GPRS
- D. EDVO

Answer: B

Explanation:

QUESTION NO: 12

Which of the following device configuration parameters could be used to change how the mobile device data is routed back to a company on a cellular network?

- A. VLAN ID
- B. APN

- C. SSID
- D. IMEI

Answer: B

Explanation:

QUESTION NO: 13

Which of the following is used so that mobile devices can continue to communicate with a mobile device management service if multiple front-end servers are configured?

- A. Cellular tower
- B. Network load-balancer
- C. Traffic shaper
- D. Proxy server

Answer: B

Explanation:

QUESTION NO: 14

Which of the following secure protocols is used for Microsoft Exchange ActiveSync communications traffic?

- A. HTTPS
- B. MAPI
- C. SMTP
- D. SFTP

Answer: A

Explanation:

QUESTION NO: 15

Which of the following entities performs the final testing and approval of the mobile device before being publically released?

- A. Mobile operator/carrier

- B. IT department
- C. Retailer
- D. End user

Answer: A

Explanation:

QUESTION NO: 16

Which of the following solution features will lower overall support costs for a large scale mobile device deployment?

- A. Compliance management
- B. Self-service portal
- C. Security policy management
- D. Location-based Services

Answer: B

Explanation:

QUESTION NO: 17

Which of the following items are valid placements for an MDM solution? (Select TWO).

- A. SaaS
- B. Cellular tower
- C. Access point
- D. On-premise
- E. Hotspots

Answer: A,D

Explanation:

QUESTION NO: 18

Which of the following sequences is the BEST way to implement a mobile device management solution?

- A. Setup server(s), configure, go-live, test, make necessary changes, and on-board devices
- B. Gather requirements, setup server(s), management sign-off, and go-live
- C. Create certificates, setup server(s), go-live, and on-board devices
- D. Pilot test group, receive feedback, make necessary changes, receive sign-off, and go-live

Answer: D

Explanation:

QUESTION NO: 19

Which of the following tasks can assist to on-board mobile devices into a mobile device management solution? (Select TWO).

- A. Integrating with LDAP
- B. Compliance reporting
- C. Using self-service portal
- D. Activation of mobile devices
- E. Entering IMEI numbers

Answer: A,C

Explanation:

QUESTION NO: 20

Which of the following must be used to successfully deploy an in-house developed application?

- A. LDAP server
- B. Application certificate store
- C. Content management solution
- D. Enterprise application store

Answer: D

Explanation:

QUESTION NO: 21

Which of the following provides information on potential security risks and threats impacting administration of mobile devices?

- A. Review security incidents within the given industry
- B. Document security incident response and escalate
- C. Recovery of lost mobile devices
- D. Verification of security certificates

Answer: A

Explanation:

QUESTION NO: 22

A network administration team will not be able to support an MDM project within the requested timeline. Which of the following would be the BEST option for deploying the Mobile Device Management software?

- A. Software as a Service Solution
- B. Stand Alone Solution
- C. Private cloud hosted externally
- D. Multi-Instance on Premise Solution

Answer: A

Explanation:

QUESTION NO: 23

Joe, a user, has noticed that his corporate-owned device has been stolen. Which of the following actions should Joe take FIRST?

- A. Report the incident
- B. Revoke the device certificate
- C. Monitor device activity
- D. Capture logs

Answer: A

Explanation:

QUESTION NO: 24

While at a conference, Ann, a user, is attempting to sync data from her device back to the corporate server. Ann has a cellular signal, however the sync will not complete. Which of the

following is MOST likely causing the issue?

- A. Content filtering
- B. Network saturation
- C. Device provisioning
- D. Device storage

Answer: B

Explanation:

QUESTION NO: 25

Which of the following capabilities would ensure that employees do not access an application after leaving a specified physical location?

- A. Wide area network
- B. Geo-fencing
- C. Captive portals
- D. Near field communication

Answer: B

Explanation:

QUESTION NO: 26

An organization is going to deploy a BYOD model to allow users to provision their personally owned devices to receive email on their mobile devices. Which of the following should be completed before allowing users to self provision their devices? (Select TWO).

- A. Directory service setup
- B. Profile creation
- C. Mobile application distribution
- D. Administrative permissions
- E. Device activation

Answer: A,B

Explanation:

QUESTION NO: 27

Which of the following is a messaging protocol that protects the confidentiality of email content?

- A. SSMTP
- B. POP3
- C. SFTP
- D. IMAP

Answer: A

Explanation:

QUESTION NO: 28

Ann, a user, called to report an issue related to authenticating to her mobile device. After resolving the issue, which of the following is the FINAL task that should be completed by the mobility administrator according to troubleshooting best practices?

- A. Establish a theory of probable cause
- B. Verify full system functionality
- C. Document findings, actions, and outcomes
- D. Implement preventative measures

Answer: C

Explanation:

QUESTION NO: 29

After installation of an MDM solution within an organization, the organization should ensure that all users of mobile devices agree to rules stated in which of the following documents?

- A. End-user licensing agreement
- B. Service level agreement
- C. Acceptable use policy
- D. Content filter policy

Answer: C

Explanation:

QUESTION NO: 30

The Chief Information Officer (CIO) has allowed employees to use their personal devices to access the enterprise guest wireless network. The organization has decided to deploy network configurations through a profile. Which of the following should be specified within the profile for the personal devices? (Select TWO).

- A. IPsec configuration
- B. Password expiration date
- C. Wireless SSID
- D. VPN configuration
- E. Authentication methods

Answer: C,E

Explanation:

QUESTION NO: 31

An organization is concerned with employees using cellular data in excess of the established usage thresholds. Which of the following would be BEST for the organization to implement?

- A. Application metering
- B. Data capture
- C. Telecom expense management
- D. Carrier billing

Answer: C

Explanation:

QUESTION NO: 32

Which of the following layers of the OSI model deals with the use of MAC addresses?

- A. Application layer
- B. Transport layer
- C. Physical layer
- D. Datalink layer

Answer: D

Explanation:

QUESTION NO: 33

Which of the following layers of the OSI model is responsible for routing protocols and IP addresses?

- A. Network layer
- B. Datalink layer
- C. Application layer
- D. Session layer

Answer: A

Explanation:

QUESTION NO: 34

A technician receives a ticket that Ann, a wireless customer, cannot access her email. As part of the troubleshooting process, the technician has finished establishing a plan of action to resolve the problem. Which of the following is the NEXT logical step the technician should take?

- A. Verify full system functionality
- B. Document findings
- C. Gather information
- D. Implement the solution

Answer: D

Explanation:

QUESTION NO: 35

A technician receives a trouble ticket that Joe, a wireless customer, cannot access his email. As part of the troubleshooting process, the technician gathered information and identified the symptoms. Which of the following is the NEXT logical step in troubleshooting?

- A. Test the theory
- B. Document findings and outcomes
- C. Establish a theory to determine the cause
- D. Implement the solution

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

[Guarantee & Policy](#) | [Privacy & Policy](#) | [Terms & Conditions](#)

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2015, All Rights Reserved.