100% Money Back Guarantee

Vendor: IBM

Exam Code: C2010-502

Exam Name: IBM Endpoint Manager for Mobile Devices V2.1 Implementation

Version: Demo

QUESTION NO: 1

What is the recommended maximum number of iOS devices that should report to an iOS management extender?

A. 500
B. 1000
C. 5000
D. 10000

Answer: C
Explanation:

QUESTION NO: 2

An Android device cannot be enrolled with a message similar to: Received an invalid server URL. What should be checked by the IBM Endpoint Manager administrator to identity the problem?

A. confirm the Trusted Service Provider is up and running
B. make sure the provided server name points to the enrollment server
C. make sure the provided URL points to the Trusted Service Provider URL
D. check if the maximum number of device has been reached for the enrollment server

Answer: B
Explanation:

QUESTION NO: 3

What must occur in order to remove an iOS profile from a managed device?

A. The profile must not be encrypted.
B. The profile must contain an administrator password.
C. The profile must have been encrypted at the time of deployment.
D. The profile must have been deployed using IBM Endpoint Manager for Mobile Devices.

Answer: D
Explanation:

QUESTION NO: 4

When creating a Samsung SAFE Capability Profile what are two of the system security'
restrictions that can be set for SAFE compatible mobile devices? (Choose two.)

A. disable Bluetooth
B. disable the microphone
C. enable encryption of internal storage
D. enable encryption of external storage
E. define the required maximum password length

Answer: A,B
Explanation:

QUESTION NO: 5

An employee's corporate mobile device managed by IBM Endpoint Manager (IEM) was stolen.
The device is accessing corporate data both using e-mail and VPN profiles. Which action can be
initiated by the EM console operator to protect access to corporate data?

A. run the action of task Device Wipe against the stolen device
B. run the action of task Selectively Wipe Corporate Device against the stolen device
C. run the action of task Selectively Wipe Android Device (Deprovision) against the stolen device
D. run the action of task Selectively Wipe Apple iOS Device (Deprovision) against the stolen
device

Answer: A
Explanation:

QUESTION NO: 6

Which mobile devices can only be managed using the Management Extender for Microsoft
Exchange?

A. AppleiOS4.xdevices
B. BlackBerry OS 10 devices
C. SAEE enabled Android devices
D. Microsoft Windows Mobile 5.x devices

Answer: B

Explanation:

QUESTION NO: 7

Apple devices are not receiving commands sent from the iOS Management Extender. Which log file should be checked to ensure the iOS extender is communicating with the Apple Push Notification Service?

A. jetty.log
B. apns.log
C. iosmdm.log
D. mdm_tasks.log

Answer: C
Explanation:

QUESTION NO: 8

The Management Extender for iOS devices opens a Command Port to listen for commands received from the IBM Endpoint Manager server. What is the default port value?

A. 23
B. 443
C. 52311
D. 52315

Answer: D
Explanation:

QUESTION NO: 9

Where would a device obtain an APK file during application installation once it has been imported to the IBM Endpoint Manager for Mobile Devices? (Choose two.)

A. relay
B. App Store
C. Google Play
D. corporate intranet site

E. IBM Endpoint Manager server

Answer: A,E
Explanation:

QUESTION NO: 10

An IBM Endpoint Manager administrator who is responsible for managing iOS mobile devices needs to view a list of applications installed on a particular OS device. Where can this be done?

A. Mobile Device dashboard
B. iOS Device View dashboard
C. Single Device View dashboard
D. Enterprise Apps Management dashboard

Answer: C
Explanation:

QUESTION NO: 11

How many days of the iosmdm.log are kept?

A. 3
B. 7
C. 10
D. Unlimited

Answer: D
Explanation:

QUESTION NO: 12

The management extender is located in a DMZto allow communications from roaming devices. To ensure better protection the Trusted Service Provider (TSP) component is installed and configured on a different system that is not in the DMZ. Which default port is used for communications between the two mobile device management components, the self service portal, and the TSP to exchange information about a user's authentication?

A. 443
B. 2195
C. 5223
D. 52316

Answer: D
Explanation:

QUESTION NO: 13

A device is giving this error the certificate for <DNS Name> is invalid. What is a possible issue?

A. Certificates are not supported by the device.
B. Name resolution is not enabled on the device.
C. The key pair used to create the certificate is corrupt.
D. The self-signed certificate has not been installed or is invalid.

Answer: D
Explanation:

QUESTION NO: 14

A customer is restricting their mobile device environment to 1000 iOS devices and 1000 Android devices. What is the minimum number of relays needed and in what configuration?

A. 1 relay with no management extenders
B. 1 relay with the iOS Management Extender
C. 1 relay with the Multi-platform Management Extender
D. 1 relay with the iOS Management Extender and 1 relay with no management extenders

Answer: B
Explanation:

QUESTION NO: 15

What does the Refresh Interval setting refer to when configuring the Management Extender for Lotus Traveler?

A. How often in minutes that the mobile devices being managed report to the management extender.
B. How often in seconds that the console refreshes when viewing the managed mobile device inventory.
C. How often in seconds that the IBM Lotus Traveler server attempts to contact the devices being managed.
D. How often in minutes that the management extender will refresh the managed device reports sent to the IBM Endpoint Manager server.

Answer: D
Explanation:

QUESTION NO: 16

Which certificate needs to be installed on the iOS Management Extender for an iOS device to be managed?

A. HTTPS certificate
B. Encryption certificate
C. IBM Endpoint Manager client certificate
D. Apple Push Notification Service certificate

Answer: D
Explanation:

QUESTION NO: 17

How can access to the App Store be restricted on iOS devices using IBM Endpoint Manager for Mobile Devices?

A. black list the AppStore
B. run the Block App Store fixlet
C. create and deploy a Restriction profile
D. create and deploy a Credentials profile

Answer: C
Explanation:

QUESTION NO: 18

Where is the NitroDesk TouchDown installation package available?

A. It is provided by the IBM account team.
B. It is available for download from the Google Play store.
C. It is installed simultaneously with the IBM Mobile Client application on iOS devices.
D. It is installed simultaneously with the IBM Mobile Client application on Android devices.

Answer: B
Explanation:

QUESTION NO: 19

Which API supports the optional Advanced Device Correlation feature if enabled during the configuration of the Microsoft Exchange Management Extender?

A. MDM API
B. SOAP API
C. Big Fix Platform API
D. Exchange Web Services Managed API

Answer: B
Explanation:

QUESTION NO: 20

On an Android device, which port does the Mobile Client use for communication with a relay or server?

A. 80
B. 443
C. 5223
D. 52311

Answer: D
Explanation:

QUESTION NO: 21

Which statement is true regarding managed applications on iOS devices?

A. Managed applications are custom developed.
B. Managed applications can be silently uninstalled.
C. Data can be exchanged between managed applications.
D. A mobile devices operator can browse and check application data.

Answer: B
Explanation:

QUESTION NO: 22

How can it be determined which devices are being managed using the IBM Sync protocol when viewing a list of devices in the Single Device View dashboard?

A. The value displayed in the Protocol column of the dashboard is set to IBM Sync.
B. The value displayed in the Extender Type column of the dashboard is set to Lotus Traveler.
C. The value displayed in the Data Source column of the dashboard is set to Lotus Traveler.
D. There is no way to determine the management protocol while viewing the dashboard in list mode.

Answer: C
Explanation:

QUESTION NO: 23

How can the requirement for installing a self-signed certificate before enrollment be removed?

A. Encrypt the device before enrollment.
B. Register the certificate with a third parte certificate manager.
C. Replace the self-signed certificate with a certified certificate signed by a trusted party.
D. Create an IBM Endpoint Manager policy that automatically installs the self-signed certificate.

Answer: C
Explanation:

QUESTION NO: 24

What can be enforced regardless of the kind of managed mobile devices either with direct management or with e-mail sync protocols?

A. apps blacklist
B. disable camera
C. password policy
D. disable Bluetooth

Answer: C
Explanation:

QUESTION NO: 25

An IBM Endpoint Manager operator wants to edit an existing ActiveSync Mailbox policy. After accessing the MS Exchange Security Policies dashboard, they discover that no Exchange Mailbox profiles currently exist. What must be done before they can edit a mailbox profile?

A. Activate the ActiveSync User Agent analysis.
B. Run the List ActiveSync Mailbox Policy task to update the policy definition file.
C. Update the Mailbox policy list by clicking the dashboard refresh icon in the upper-right area of the dashboard.
D. Create an Exchange Mailbox profile by clicking the Add Policy button on the MS Exchange Security Policies dashboard.

Answer: B
Explanation:

QUESTION NO: 26

What needs to be set in an iOS profile to prevent users from copying e-mail from a corporate account to a personal account?

A. Prevent Move must be checked
B. Prevent Copy must be checked
C. Allow Move must be unchecked
D. Allow Copy must be unchecked

Answer: C

Explanation:

QUESTION NO: 27

Which software is needed on iOS devices to take advantage of all IBM Endpoint Manager management features on Apple devices?

A. the IBM Mobile Client application from the Apple App Store
B. the Apple Push Notifier application from the Apple App Store
C. no software is required on the devices, just install a management profile
D. the Mobile Management Dashboard application from the Apple App Store

Answer: A
Explanation:

QUESTION NO: 28

How many BlackBerry' Management Extenders must be deployed at a customer who has 3 BlackBerry Enterprise Servers and has already setup and configured a Management Extender for Lotus Traveler?

A. 3; one for each BlackBerry Enterprise Server.
B. 1; one configuration profile for each BlackBerry Enterprise Server.
C. None; a customer can use the Management Extender for Lotus Traveler.
D. It depends on how the network is configured; one for each subnet which hosts one or more BlackBerry' Enterprise Servers.

Answer: A
Explanation:

QUESTION NO: 29

What condition allows an iOS application to be silently uninstalled?

A. If the application has been imported as managed.
B. If the application has been deployed using the prompt install task.
C. The mobile devices operator can only notify a user to uninstall an application.
D. Applications can be silently uninstalled on all devices types through the IBM Endpoint Manager

infrastructure.

Answer: A
Explanation:

QUESTION NO: 30

Which functionality is available when using e-mail-based management of an iOS device?

A. track device location
B. deployment of applications
C. configuration of passcodes
D. disable access to the App Store

Answer: C
Explanation:

QUESTION NO: 31

Which type of account must be used to install and configure the IBM Endpoint Manager (IEM) Self Service Portal?

A. a domain admin
B. master operator account
C. any IEM console user account
D. a local admin on the IEM server

Answer: C
Explanation:

QUESTION NO: 32

Which two statements are true about using the Self Service Portal? (Choose two.)

A. A device can be wiped.
B. The screen can be locked.
C. Configuration changes can be made.
D. A device can be assigned to another user.

E. A user can add corporate applications to the device.

Answer: A,B
Explanation:

QUESTION NO: 33

How can the IBM Endpoint Manager for Mobile Devices component diagnostic web pages help troubleshoot an issue with the Trusted Service Provider (TSP)?

A. It has a link to test the login to LDAP.
B. It has a link to import the client error log.
C. It has a link to view the tsp.log file directly.
D. It provides a link to a fixlet that will reconfigure the TSP component.

Answer: A
Explanation:

QUESTION NO: 34

Which component is required to manage iOS devices through e-mail management?

A. Native Agent Installation
B. Apple Push Notification Service
C. Google Cloud Messaging (GCMS)
D. Lotus Traveler Management Extender

Answer: D
Explanation:

QUESTION NO: 35

An employee is using a corporate Android device with access to corporate e-mail using NitroDesk TouchDown and with a corporate application used to offer services.

The employee has lost the device and notifies the IT department. What is the best action that an IBM Endpoint Manager console operator can take to prevent any access to corporate data from the lost device?

A. issue the task action Device Wipe against the device
B. enable GPS localization to retrieve and regain the lost device
C. issue the task action Wipe NitroDesk TouchDown - Android against the device
D. issue the task action Selectively Wipe Android Device (Deprovision) against the device

Answer: A
Explanation:

QUESTION NO: 36

What is the simplest way for the IBM Endpoint Manager (IEM) administrator to obtain a log from a managed Android device?

A. Install and run the Android Device Notifier Service (GCM).
B. Issue a task from the IEM console to retrieve the desired log.
C. Ask the end user to e-mail the IEM client log directly from the IBM Mobile Client application.
D. Ask the end user to connect the Android device to a PC and browse directly to the client log.

Answer: C
Explanation:

QUESTION NO: 37

What does the Recommend Apps task offer?

A. A prompt to the end user to install enterprise applications.
B. A voucher to buy applications from the vendor marketplace.
C. A pre-defined e-mail to the end user listing URLs of highly rated available applications.
D. It allows the end user to install applications from a list in the IBM Mobile Client application.

Answer: D
Explanation:

QUESTION NO: 38

An administrator wants to create a new security policy to disable the camera on managed Android devices using the Android Security Policies dashboard. What are the platform requirements to support this policy?

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:

Guarantee & Policy | Privacy & Policy | Terms & Conditions