



TestKingonline.com

No Pass No Pay!

MCSE, CCNA, CCNP, OCP, CIW, JAVA, Sun Solaris, Checkpoint

World No 1 Cert Exams

**TS:MS Windows Mobile Designing, Implementing, and Managing
70-500**

Congratulations!

You have purchased a TestKingonline. Study Guide.

This study guide is a complete collection of questions and answers that have been developed by our professional & certified team.

You must study the contents of this guide properly in order to prepare for the actual certification test. The average time that we would suggest you for studying this study guide is approximately 10 to 20 hours and you will surely pass your exam. We guarantee it!

GOOD LUCK!

DISCLAIMER

This study guide and/or material is not sponsored by, endorsed by or affiliated with Microsoft, Cisco, Oracle, Citrix, CIW, Checkpoint, Novell, Sun/Solaris, CWNA, LPI, ISC, etc. All trademarks are properties of their respective owners.

Guarantee

If you use this study guide correctly and still fail the exam, send a scanned copy of your official score notice at:

Sales@Testkingonline.com

We will gladly refund the cost of this study guide or give you an exchange of study guide of your choice of the Free.

This material is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Question: 1

You deploy a Microsoft Exchange mobile messaging solution that uses Microsoft Windows Mobile 5.0 with Microsoft Messaging and Security Feature Pack.

The messaging infrastructure is configured to support the remote wipe feature.

When an administrator attempts to perform a remote wipe of a Windows Mobile based device, the administrator receives a 401 error message.

You need to ensure that the administrator is authorized to perform remote wipes only.

What should you do?

- A - Grant the administrator membership in the Domain Administrators group.
- B - Grant the administrator membership in the Exchange Administrators group.
- C - Add the new administrator account to the Discretionary Access Control List (DACL) of the Microsoft Exchange ActiveSync Administration folder.
- D - Select the Directory Security tab of the Exchange Server administration Web site, and then configure Read, Write, and Directory Browsing permissions.

Answer: C

Question: 2

You deploy a mobile messaging solution with the Microsoft Exchange Server 2003 server.

The IIS logs on the Exchange Server 2003 server show an excessive number of 401 errors.

You need to reduce the number of 401 errors identified in the logs.

What should you do?

- A - Instruct all the users to perform a desktop synchronization at least once every 42 days.
- B - Instruct all the users to change the Microsoft ActiveSync configuration password when they change their domain user account password.
- C - Instruct all the users to reset their Microsoft Windows Mobile based device password when they change their domain user account password.
- D - Enable the This server requires an encrypted SSL connection option in the Microsoft ActiveSync settings of each Microsoft Windows Mobile based device.

Answer: B

Question: 3

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 Service Pack 2.

All remote users use mobile devices that run Microsoft Windows Mobile 5.0 with Microsoft Messaging and Security Feature Pack (MSFP).

A remote user reports the loss of a Windows Mobile based device

You need to ensure that the information from the Microsoft Exchange ActiveSync (EAS) server is no longer available on the Windows Mobile based device.

What should you do?

- A - Recreate the Active Directory remote user account.
- B - Perform a remote wipe on the Windows Mobile based device of the remote user.
- C - On the Properties tab of the remote user account, disable the user-initiated synchronization option.

D - On the Device Security Settings tab, configure the Wipe device after failed attempts option to a value of zero.

Answer: B

Question: 4

A Microsoft Exchange mobile messaging solution uses Microsoft Windows Mobile 5.0 with Microsoft Messaging and Security Feature Pack. You deploy the solution by using front-end and back-end servers. Microsoft Exchange Server 2003 Service Pack 2 is installed on the front-end server.

You need to use the remote wipe feature.

What should you do?

A - Install Microsoft Windows Server 2003 Service Pack 2 on all domain controllers.

B - Install Microsoft Exchange Server 2003 Service Pack 2 on the back-end server.

C - Install Microsoft Exchange Server ActiveSync Web Administration Tool on the front-end server.

D - Install Microsoft Exchange Server ActiveSync Web Administration Tool on the back-end Server. Reset Instructions Calculator.

Answer: C

Question: 5

You deploy a mobile messaging infrastructure with front-end and back-end Microsoft Exchange Server 2003 servers. Both servers have Service Pack 2 installed.

Company security policy requires that all information from the Exchange Server 2003 servers must be encrypted.

You need to audit the mobile messaging infrastructure to verify that it complies with company security policy.

What should you do?

A - Review the Internet Information Services (IIS) logs on the front-end Microsoft Exchange Server 2003 server by looking for Microsoft Server ActiveSync log entries and verifying that these entries use the SSL port for access.

B - Review the Internet Information Services (IIS) logs on the back-end Microsoft Exchange Server 2003 server by looking for Microsoft Server ActiveSync log entries and verifying that these entries use the SSL port for access.

C - Install Network Monitor on the back-end Microsoft Exchange Server 2003 server. Execute and review a packet capture session by tracing the packets that originate from the Windows Mobile devices of the users.

D - Install Network Monitor on the front-end Microsoft Exchange Server 2003 server. Execute and review a packet capture session by tracing the packets that originate from the Windows Mobile based devices of the users.

Answer: A

Question: 6

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 Service Pack 2.

The company security policy requires complex passwords on all the Microsoft Windows Mobile based devices.

You provide a Microsoft Windows Mobile 5.0 smart phone based device to a new user. The first time the user uses the device, the user is not prompted for a password.

You need to ensure that the user is prompted for a password.

What should you do?

A - Instruct the user to set a PIN on the mobile device.

B - Instruct the user to perform Microsoft Exchange ActiveSync synchronization Over-The-Air (OTA)

C - On the Device Security Settings tab, select the Require both numbers and letters option.

D - Add the user account of the user to the Exceptions list on the Device Security Settings tab.

Answer: B

Question: 7

A user uses both a Microsoft Windows Mobile 5.0 Smart phone based device and a Microsoft Windows Mobile 5.0 Pocket PC Phone Edition device for Over-The-Air (OTA) e-mail. Both devices have Microsoft Messaging and Security Feature Pack installed.

A remote wipe command is issued against the Pocket PC device.

The user reconfigures the ActiveSync settings on the Pocket PC device.

When the user attempts synchronization, the device hard-resets again.

You need to ensure that the user can synchronize the Pocket PC device.

What should you do?

A - Cancel the remote wipe issued against the Pocket PC device.

B - Instruct the user to configure only one device for ActiveSync.

C - Instruct the user to perform a soft-reset of the Pocket PC device.

D - Instruct the user to perform a manual hard-reset of the Pocket PC device.

Answer: A

Question: 8

You deploy mobile devices that run Microsoft Windows Mobile 5.0.

A Microsoft Windows Server 2003 server that runs Routing and Remote Access is configured to allow virtual private network (VPN) connections that are as secure as possible.

You need to connect the Windows Mobile based devices to the VPN server. You also need to ensure that both ends of the VPN tunnel are authenticated.

Which two actions should you perform? (Each correct answer presents part of the solution.

Choose two)

A - Select L2TP/IPSec on each Windows Mobile based device.

B - Obtain and install a certificate on each Windows Mobile based device.

C - Configure the appropriate pre-shared key on each Windows Mobile based device.

D - Select Point-to-Point Tunneling Protocol (PPTP) on each Windows Mobile based device.

Answer: A, B

Question: 9

You deploy mobile devices that run Microsoft Windows Mobile 5.0.

Company security policy requires an authentication process that is stronger than a user name and password combination.

You need to ensure that Microsoft ActiveSync sessions use an authentication process that meets the company security policy.

What should you do?

- A - Deploy a two-factor authentication process.
- B - Deploy a single-factor authentication process.
- C - Deploy a simple PIN policy for the Windows Mobile based devices.
- D - Deploy a complex PIN policy for the Windows Mobile based devices.

Answer: A

Question: 10

You deploy a mobile messaging solution by using front-end and back-end servers that run Microsoft Exchange Server 2003 Service Pack 2. Certificates are installed on all Microsoft Windows Mobile based devices.

You need to allow devices that run Microsoft Windows Mobile 5.0 to perform certificate-based authentication for Microsoft Exchange ActiveSync.

What should you do?

- A - Configure the front-end server for Kerberos Constrained Delegation (KCD).
- B - Configure a Routing Group Connector between the front-end and back-end servers.
- C - Configure the Windows Mobile based devices with a Point-to-Point Protocol (PPTP) connection.
- D - Configure the Windows Mobile based devices to use Extensible Authentication Protocol (EAP) and either a smart card or a certificate.

Answer: A

Question: 11

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 Service Pack 2.

When the application is running, it must not be able to access protected registry keys.

You need to ensure that the application meets the outlined requirement.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

- A - Use Microsoft Windows Mobile 5.0 Pocket PC Phone Edition operating system.
- B - Use Microsoft Windows Mobile 2003 for Pocket PC operating system.
- C - Use Microsoft Windows Mobile 5.0 for Smart phone operating system.
- D - Use Microsoft Windows Mobile 2003 for Smart phone operating system.

Answer: C, D

Question: 12

You deploy a mobile messaging solution by using front-end and back-end servers that run Microsoft Exchange Server 2003 Service Pack 2.

Company policy requires that all Microsoft Windows Mobile based devices must support Microsoft Exchange ActiveSync communication that is Federal Information Processing Standard compliant.

You need to deploy the Windows Mobile based devices.

What should you use?

A - Microsoft Windows Mobile 5.0

B - Microsoft Windows Mobile 2003 for Pocket PC

C - Microsoft Windows Mobile 2003 Second Edition

D - Microsoft Windows Mobile 5.0 with Microsoft Messaging and Security Feature Pack

Answer: D

Question: 13

You deploy mobile devices that run Microsoft Windows Mobile 5.0 with Microsoft Messaging and Security Feature Pack. A server that runs Microsoft Exchange Server 2003 Service Pack 2 is configured by using the default installation settings.

Company security policy requires a complex password for unlocking the Windows Mobile based devices.

You need to ensure that the Windows Mobile based devices that perform Microsoft ActiveSync synchronization meet the company security policy.

Which two actions should you perform? (Each correct answer presents part of the solution.

Choose two.)

A - Enter all mobile device users in the Exceptions list.

B - Enable the Require both numbers and letters option.

C - Enable the Allow access to devices that do not fully support password settings option.

D - Enable the Minimum password length (characters) option. Configure a value of 6 or greater.

Answer: B, D

Question: 14

You deploy mobile devices that run Microsoft Windows Mobile 5.0.

A Windows Mobile based device user forgets the PIN for the device.

You need to ensure that the user can unlock the device.

What should you do?

A - Change the password for the domain user account of the user.

B - Perform a hard reset of the user's Windows Mobile based device.

C - Perform a soft reset of the user's Windows Mobile based device.

D - Connect the Windows Mobile based device to the desktop computer of the user and change the password of the local user account of the user.

Answer: B

Question: 15

You deploy a server that runs Microsoft Exchange Server 2003 Service Pack 2. You also deploy

mobile devices that run Microsoft Windows Mobile 5.0 with the Microsoft Messaging and Security Feature Pack.

You need to ensure that the Windows Mobile based devices are as secure as possible from brute force password attacks.

What should you do?

A - Set the Microsoft ActiveSync synchronization schedule on the mobile devices to five-minute intervals.

B - Enable the Wipe devices after failed attempts option and specify a valid value for the option.

C - Configure the Default Domain Group Policy object to enable Password complexity.

D - Configure the Default Domain Group Policy object to specify a valid value for the Account Lockout Threshold.

Answer: B

Question: 16

You deploy a Microsoft Windows Mobile 5.0 for Smart phone based mobile messaging solution that has two-tier authentication with Microsoft Exchange Server 2003 Service Pack 2.

Company security policy requires that only company-approved applications are allowed to run on Windows Mobile 5.0 for Smart phone based devices.

You need to ensure that third-party applications are prevented from running.

Which two actions should you perform? (Each correct answer presents part of the solution.

Choose two.)

A - Remove all the entries in the personal certificates store on each Windows Mobile for Smart phone based device.

B - Remove all the entries in the list of Trusted Root Certification authorities on each Windows Mobile for Smart phone based device.

C - Install a computer certificate in the personal certificate store of each Windows Mobile for Smart phone based device.

D - Install the root certification authority (CA) certificate of the company in the list of Trusted Root Certification authorities on each Windows Mobile for Smart phone based device.

Answer: B, D

Question: 17

You deploy mobile devices that run Microsoft Windows Mobile 5.0. Users store a price list in Microsoft Office Excel Mobile files on the devices.

Users install a new mobile application on the devices.

A user reports that the device performs slowly after the installation. All attempts to remove the application fail.

You need to remove the application without losing the saved price list.

What should you do?

A - Copy the price list to an external storage card and perform a hard reset.

B - Copy the price list by using a Desktop Active sync and perform a soft reset.

C - Copy the price list to another Windows Mobile based device by using Bluetooth and perform a

soft reset.

D - Move the price list to the Program Files directory on the Windows Mobile based device and perform a hard reset.

Answer: A

Question: 18

You deploy mobile devices that run Microsoft Windows Mobile 5.0 Pocket PC Phone Edition. You need to prevent the device screen from turning dark when users view documents.

Which two actions should you perform? (Each correct answer presents part of the solution.

Choose two.)

A - Configure the backlight brightness setting to maximum.

B - Display the soft input panel (SIP) when users read documents.

C - Increase the value of the Turn off device if not used for option.

D - Increase the value of the Turn off backlight if device is not used for option.

Answer: C, D

Question: 19

You use a mobile device that runs Microsoft Windows Mobile 5.0 Pocket PC Phone Edition.

You perform the following tasks:

Read e-mail messages and attachments.

Edit Microsoft Word documents.

Review Microsoft PowerPoint presentations.

Chat through Microsoft Pocket MSN.

Read information through Microsoft Pocket Internet Explorer.

When you attempt to open a custom line-of-business (LOB) application, you receive a low memory error. You need to open the LOB application to enter new sales information.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A - Move all applications to an external storage card.

B - Perform a soft reset of the Windows Mobile based device.

C - Perform a hard reset of the Windows Mobile based device.

D - Stop all applications by using the Running Programs list.

Answer: B, D

Question: 20

You deploy mobile devices that run Microsoft Windows Mobile 5.0. Users will use MSN

Messenger on the devices. You need to ensure that users use their corporate e-mail accounts to sign in to the MSN Messenger service.

What should you do?

A - Instruct users to register for an MSN Messenger e-mail account.

B - Instruct users to reset the passwords for their domain user accounts.

C - Instruct users to clear all saved passwords on their Windows Mobile based devices.

D - Instruct users to register for a valid MSN Messenger account by using their corporate e-mail addresses.

Answer: D

Question: 21

You provide devices that run Microsoft Windows Mobile 5.0 Pocket PC Phone Edition to all employees in the sales department.

Information about product inventory is stored in a database on a server that runs Microsoft SQL Server 2005 Compact Edition. Sales employees require current updates of product inventory data 20 times per day.

You need to set up a publication in SQL Server 2005 Standard Edition to replicate data to mobile devices.

What should you do?

A - Create a script to transfer the data from tables in the SQL Server database to text files. Email the text files to mobile users.

B - Configure the Microsoft Windows PC ActiveSync on all the Microsoft Windows Mobile based devices to synchronize files by using Microsoft SQL Server 2005 Compact Edition.

C - Create a snapshot folder. Set appropriate permissions on the folder. Set up a publication in SQL Server and point the database snapshot to the snapshot folder. Create a merge replication to Microsoft SQL Server 2005 Compact Edition.

D - Create a snapshot folder. Set appropriate permissions on the folder. Set up a publication in SQL Server and point the database snapshot to the snapshot folder. Configure Microsoft ActiveSync to synchronize the snapshot folder to the mobile device.

Answer: C

Question: 22

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 Service Pack 2. The Exchange server is protected from the Internet by a Microsoft Internet Security and Acceleration (ISA) Server 2004 server.

The Microsoft Windows Mobile 5.0 devices have the Microsoft Messaging and Security Feature Pack (MSFP).

You need to ensure that e-mail messages are received by using the Direct Push method.

What should you do?

A - Configure the Connection Timeout value of the Microsoft Exchange Server 2003 server to 120 seconds.

B - Enable the bandwidth throttling setting on the default Web site of the Microsoft Exchange Server 2003 server.

C - Enable the Maximum Connections option on the Microsoft ISA Server 2004 computer and set it to a value of 3000.

D - Configure the Connection Timeout (seconds) value of the Microsoft ISA Server 2004 computer to reduce the number of heartbeats on the device.

Answer: D

Question: 23

You deploy mobile devices that run Microsoft Windows Mobile 5.0.

The following servers reside on the perimeter network:

A Microsoft Exchange Server 2003 server

A Microsoft Windows Server 2003 server configured as a virtual private network (VPN)

All VPN connections must perform the following tasks:

Support tunnel authentication.

Transfer user names and passwords in the most secure manner.

Employees access Microsoft Exchange ActiveSync e-mail messages and other company data located on the internal network.

You need to ensure that access to all information is as secure as possible.

Which two security mechanisms should you use? (Each correct answer presents part of the solution. Choose two.)

A - SSL

B - L2TP/IPSec

C - Pre-shared key

D - PPTP

Answer: A, B

Question: 24

You deploy a messaging solution to support Microsoft Office Outlook Web Access (OWA). You configure a Microsoft Exchange Server 2003 front-end server and a Microsoft Exchange Server 2003 back-end server.

You need to deploy Microsoft Windows Mobile 5.0 devices that perform an Over-The-Air (OTA) synchronization of e-mail, calendar, tasks, and contact items with the Exchange Server 2003 server.

What should you do?

A - Configure ActiveSync for the Windows Mobile 5.0 devices.

B - Deploy a Microsoft Internet Security and Acceleration Server (ISA) 2004 computer.

C - Install and configure an additional Exchange Server 2003 front-end server.

D - Install Microsoft Messaging and Security Feature Pack on the Windows Mobile 5.0 devices.

Answer: A

Question: 25

You deploy a mobile messaging infrastructure with Microsoft Exchange Server 2003. The messaging infrastructure supports 20,000 users.

You need to redesign the messaging infrastructure to support reliable access to e-mail messages in the event of a single server failure.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A - Create a server cluster of back-end Microsoft Exchange Server 2003 servers.
- B - Create a Network Load Balancing (NLB) cluster of back-end Microsoft Exchange Server 2003 servers.
- C - Create a Network Load Balancing (NLB) cluster of front-end Microsoft Exchange Server 2003 servers.
- D - Create a group of Domain Name System (DNS) load balanced front-end Microsoft Exchange Server 2003 servers.
- E - Create a Microsoft Internet Security and Acceleration (ISA) Server 2004 proxy' for the frontend Microsoft Exchange Server 2003 server.

Answer: A, C

Question: 26

You deploy a mobile messaging solution with front-end and back-end Microsoft Exchange Server 2003 servers. You implement a third-party firewall appliance to protect all servers.

You need to ensure that the Microsoft Windows Mobile-based devices are denied direct access to the Exchange Server 2003 servers.

What should you do?

- A - Enable the Windows firewall on all internal servers.
- B - Deploy a Microsoft Internet Security and Acceleration Server (ISA) 2004 server.
- C - Enable the This server requires an encrypted SSL connection option on all the Windows Mobile based devices.
- D - Create a new access rule on the firewall appliance to permit traffic over port 443 to the Microsoft Exchange Server 2003 server.

Answer: B

Question: 27

You are deploying a Microsoft Windows Mobile messaging solution with Microsoft Exchange Server 2003 on a Microsoft Windows Small Business Server 2003 server.

The messaging solution must meet the following requirements:

Pre-authenticate Exchange traffic.

Be able to remotely wipe devices.

Provide immediate e-mail delivery from the Microsoft Exchange Server 2003 to Microsoft Windows Mobile 5.0 with Microsoft Messaging and Security Feature Pack based devices.

You need to ensure that the messaging solution meets the outlined requirements.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A - Set up a back-end Microsoft Exchange Server 2003 server.
- B - Set up a front-end Microsoft Exchange Server 2003 server.
- C - Install Exchange Server ActiveSync Web Administration Tool.
- D - Enable Direct Push on the Microsoft Exchange Server 2003 server.
- E - Install Microsoft ActiveSync on the client computers that are connected to the server

Answer: C, D

Question: 28

You distribute mobile devices that run Microsoft Windows Mobile 5.0 to all employees in your company. All devices support Wi-Fi and are configured to connect to an access point deployed for the employees.

You need to ensure that access to corporate resources over Wi-Fi is as secure as possible. What should you do?

- A - Configure the Windows Mobile based devices to support L2TP/IPSec.
- B - Configure Wired Equivalency Protocol on the access point and the Windows Mobile based devices.
- C - Enable Lightweight Extensible Authentication Protocol (LEAP) on the Windows Mobile based devices.
- D - Configure Wi-Fi Protected Access (WPA) with a pre-shared key on the access point and the Windows Mobile based devices.

Answer: A

Question: 29

You deploy a mobile messaging solution with Microsoft Exchange Server 2003.

A two-tier, custom sales application delivers an updated list of products in text format to an internal Web site after every five minutes.

You need to ensure that the Microsoft Windows Mobile based devices can download the list from the Web site as securely as possible.

What should you do?

- A - Configure all Windows Mobile based devices to use a complex password.
- B - Configure an IPSec tunnel between the Web server and the database server.
- C - Configure Encrypted File System (EFS) on the directory that contains the product list.
- D - Configure Windows Mobile based devices to establish a virtual private network (VPN) tunnel that connects to the corporate network.

Answer: D

Question: 30

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 for your company.

Your company employs both full-time and contract employees.

You discover that both full-time and contract employees are performing Microsoft ActiveSync synchronizations from their Microsoft Windows Mobile based devices.

You need to ensure that only full-time employees can perform ActiveSync synchronizations.

What should you do?

- A - Disable the Up-to-date Notifications option for contract employees.
- B - Disable the User Initiated Synchronization option for contract employees.
- C - Disable the Enable User Initiated Synchronization option for all employees.
- D - Enable the User Initiated Synchronization option for full-time employees.

Answer: B

Question: 31

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 Service Pack 2. Mobile devices that run Microsoft Windows Mobile 5.0 and Microsoft Messaging and Security Feature Pack receive Microsoft ActiveSync e-mail messages.

You need to ensure that the new e-mail messages are delivered at minimum Short Message Service (SMS) cost. You also need to ensure that the e-mail messages that arrive at the Exchange server 2003 are delivered immediately.

What should you do?

- A - Enable the Enable Outlook Mobile Access option.
- B - Enable the Enable Direct Push over HTTP(S) option.
- C - Disable the Microsoft Exchange Routing Service service.
- D - Disable the Enable up-to-date notifications via SMTP and Text Messaging option.

Answer: B

Question: 32

You deploy a mobile messaging solution with front-end and back-end Microsoft Exchange Server 2003 servers.

All the mobile devices that run Microsoft Windows Mobile 2003 currently perform Over-The-Air (OTA) synchronization of e-mail messages and contacts.

You need to configure the environment to support Direct Push.

Which two technologies are required? (Each correct answer presents part of the solution. Choose two.)

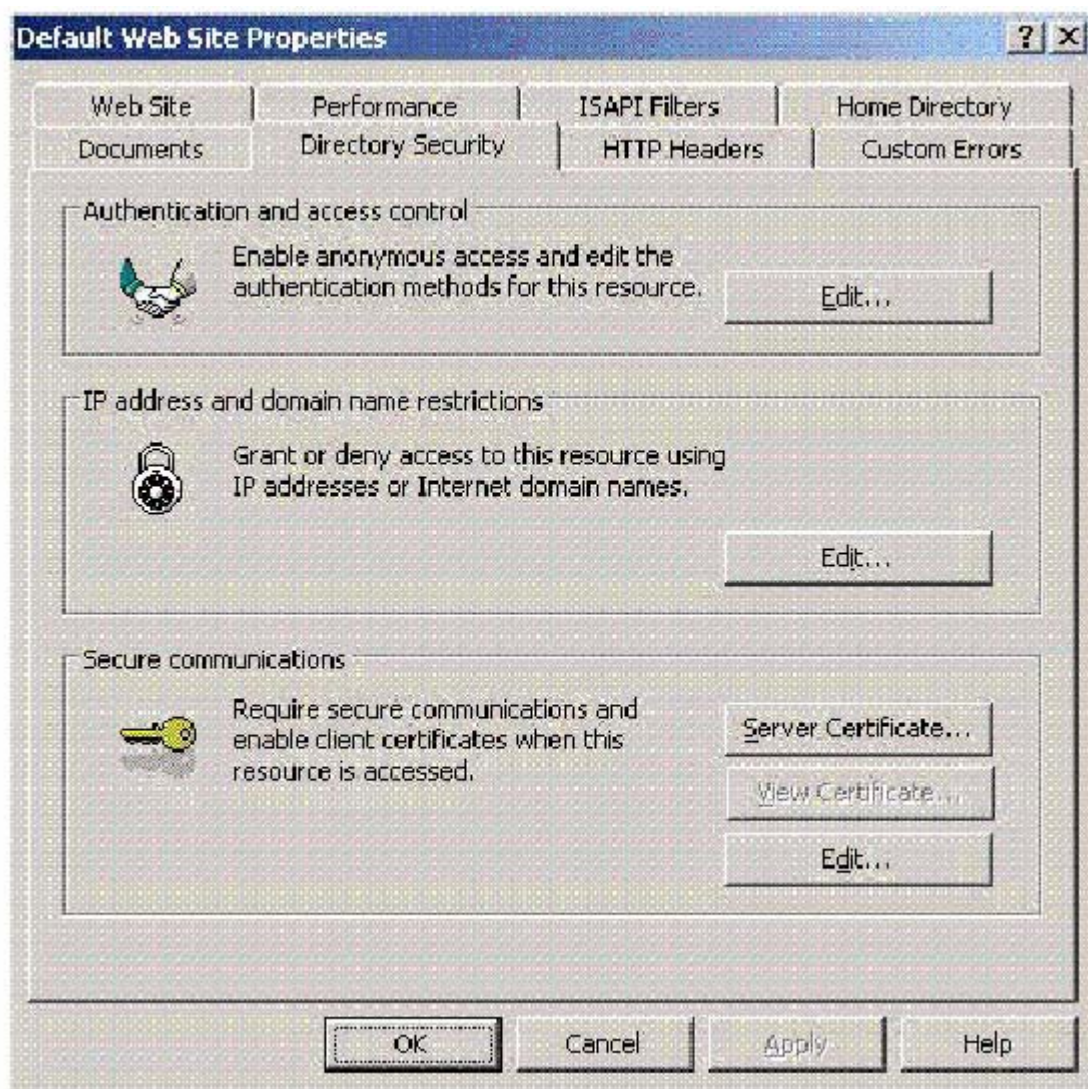
- A - The latest version of Microsoft ActiveSync on all the desktop computers
- B - Microsoft Exchange Server 2003 Service Pack 2 on the back-end server
- C - Microsoft Exchange Server 2003 Service Pack 2 on the front-end server
- D - Microsoft Windows Mobile 5.0 with the Microsoft Messaging and Security Feature Pack on all the mobile devices

Answer: C, D

Question: 33

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 server.

The default Web site on the Exchange Server 2003 server is configured as shown in the following exhibit. (Click the Exhibit button.)



You need to ensure that the data exchanged between the Microsoft Windows Mobile based devices and the Microsoft Exchange Server 2003 server is encrypted. What should you do?

- A - Install a new SSL certificate on the Microsoft Exchange Server 2003 server.
- B - Enable the Encrypting File System (EFS) on the root directory of the Microsoft Exchange Server 2003 server.
- C - Edit the Discretionary Access Control List (DACL) of the mobile admin directory. Configure the Allow-Read & Execute permission for the Authenticated Users group.
- D - Edit the local security policy of the Microsoft Exchange Server 2003 server. Enable the Microsoft network server Digitally sign communications (always) option.

Answer: A

Question: 34

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 for a company. The company has 50,000 employees. The sales department has 5,000 employees. These 5,000

employees are provided with Microsoft Windows Mobile based devices.
You need to allow only these 5,000 sales employees to perform Microsoft Exchange ActiveSync.
You need to achieve this goal by using the least amount of administrative effort.
What should you do?

- A - Create an ADSI script to disable the User Initiated Synchronization option for all the nonsales employees.
- B - Enable the User Initiated Synchronization option on the properties of the sales employees domain user accounts.
- C - Disable the Enable user initiated synchronization option on the Mobile Services Properties page on the front-end Exchange Server 2003.
- D - Create a Group Policy object (GPO) that enables the Deny access to this computer from the network for all non-sales employees. Link the GPO to an organizational unit that contains all front-end Exchange Server 2003 servers.

Answer: A

Question: 35

You deploy a mobile messaging solution by performing the following tasks.
Install Microsoft Exchange Server 2003 on a server.
Configure SSL for Microsoft Exchange Server 2003 server.
Deploy an internal Public Key Infrastructure (PKI) by using Microsoft Windows Certificate Services.
You need to ensure that Windows Mobile based device users can use encryption to obtain e-mail messages and contacts through Microsoft Exchange Active Sync.
What should you do?

- A - Configure RADIUS authentication for Microsoft Exchange Server 2003.
- B - Add a publicly trusted root certificate authority to the internal root CA certificate.
- C - Add the internal root CA certificate to the Root Certificates list on the Windows Mobile based devices.
- D - Add the Exchange Server 2003 SSL certificate to the Personal certificates list on the Windows Mobile based devices.

Answer: C

Question: 36

You deploy a mobile messaging solution with Microsoft Exchange Server 2003.
You need to ensure that all users of the Microsoft Windows Mobile based devices can receive email messages by using Over-The-Air (OTA) Microsoft ActiveSync synchronization.
What should you do?

- A - Configure the front-end server to use the Basic authentication option.
- B - Configure the front-end server to use the Digest authentication option.
- C - Configure the front-end server to use the Anonymous authentication option.
- D - Disable the Allow Anonymous authentication option on the front-end server.

Answer: A

Question: 37

You deploy devices that run Microsoft Windows Mobile 5.0.
When users attempt to access the Internet, a message is displayed as shown in the following exhibit. (Click the Exhibit button.)



You need to configure the devices to connect to the Internet.
What should you do?

- A - Perform a soft reset of all devices.
- B - Perform a hard reset of all devices.
- C - Configure the Programs that automatically connect to the Internet should connect using: option to use the My ISP profile.
- D - Configure the Programs that automatically connect to the private network should connect using: option to use the My Work profile.

Answer: C

Question: 38

You deploy mobile devices that run Microsoft Windows Mobile 5.0. The devices support Wi-Fi. You need to ensure that the devices can connect to a wireless local area network (WLAN) that does not broadcast the Service Set Identifier (SSID).

What should you do?

- A - Configure 802.1x authentication.
- B - Configure the SSID in the Network Cards utility.
- C - Configure the devices to use Wired Equivalency Protocol (WEP).
- D - Configure a new Access Point Name (APN) in the Connections settings.

Answer: B

Question: 39

You deploy mobile devices that run Microsoft Windows Mobile 5.0. The internal network contains a wireless access point that is configured for Remote Authentication Dial In User Service (RADIUS) authentication. You need to configure the devices to authenticate the connection to the wireless local area network (WLAN). What should you do?

- A - Configure the Windows Mobile based devices to use 802.1x for authentication.
- B - Configure the IP address of the RADIUS server as a proxy on the Windows Mobile based devices.
- C - Configure the Windows Mobile based devices to use Wired Equivalency Protocol (WEP) for authentication.
- D - Configure the Windows Mobile based devices to use Wi-Fi Protected Access-Temporal Key Integrity Protocol (WPA-TKIP) for authentication.

Answer: A

Question: 40

You use a mobile device that runs Microsoft Windows Mobile 5.0. You need to ensure that files can be transferred to another Windows Mobile based device when the device is out of the network coverage area. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

- A - Enable Bluetooth on both Windows Mobile based devices.
- B - Enable Bluetooth discovery on one Windows Mobile based device.
- C - Enable the Receive All Incoming Beams option on both Windows Mobile based devices.
- D - Create a pairing between the Windows Mobile based devices.
- E - Create a unique passkey on each Windows Mobile based device.

Answer: A, B, D

Question: 41

You deploy mobile devices that run Microsoft Windows Mobile 5.0 for Smart phone.

You need to ensure that the devices access the Internet Over-The-Air (OTA). You also need to ensure that the access to the corporate intranet is as secure as possible.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A - Configure the devices to use certificate-based 802W authentication.
- B - Configure the work connection to use a virtual private network (VPN) connection.
- C - Configure the devices to use Lightweight Extensible Authentication Protocol (LEAP).
- D - Verify that the Internet connection is set to use the network of the wireless carrier.

Answer: B, D

Question: 42

You deploy mobile devices that run Microsoft Windows Mobile 5.0. The devices support Wi-Fi, global positioning system (GPS), Bluetooth, and cellular data connectivity.

Users of the devices report that they are prompted to connect to public wireless local area networks (WLANs).

You need to configure the devices to prevent prompts to connect to WLANs.

You also need to ensure that users retain the ability to synchronize e-mail messages Over-The-Air (OTA).

What should you do?

- A - Turn off GPS.
- B - Turn off Wi-Fi.
- C - Turn on flight mode.
- D - Disable the cellular data connection.

Answer: B

Question: 43

You deploy mobile devices that run Microsoft Windows Mobile 5.0 to remote users.

The remote users are not on the corporate network.

You need to ensure that the remote users can access internal corporate network resources without using a virtual private network (VPN) connection.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A - Install a Wi-Fi repeater on the perimeter network.
- B - Configure the Windows Mobile based device with a new Access Point Name (APN).
- C - Configure the Windows Mobile based device with a new wireless local area network (WLAN).
- D - Create a back-end connection from the network of your cellular carrier to the corporate network.

Answer: B, D

Question: 44

You deploy mobile devices that run Microsoft Windows Mobile 5.0 for Smart phone. The mobile devices are purchased from a mobile operator.

A mobile device user who works remotely reports an error message that states: "Cannot connect for unknown reason." You attempt to diagnose the problem but are unable to do so. You discover that the user's device is currently connected to a mobile computer. You need to restore the cellular APN connection settings of the user. What should you do?

- A - Instruct the user to remove and replace the device battery.
- B - Instruct the user to perform a soft reset of the Windows Mobile based device.
- C - Deploy a .cab file that contains a CAB provisioning format (CPF) file. Instruct the user to install the .cab file on the device.
- D - Instruct the user to connect the device to the desktop computer of the user to perform a Microsoft Windows PC Active sync synchronization.

Answer: C

Question: 45

You need to configure ActiveSync to receive updates from Server2. What should you do?

- A - Disable SSL in the ActiveSync configuration.
- B - Configure ActiveSync to use the fully qualified domain name mail.contoso.com.
- C - Configure ActiveSync to use the fully qualified domain name server2.contoso.com.
- D - Install the Microsoft Messaging and Security Feature Pack on the mobile devices that run Microsoft Windows Mobile 5.0.

Answer: B

Question: 46

You deploy mobile devices that run Microsoft Windows Mobile 5.0. You need to provision each device to obtain corporate e-mail Over-The-Air (OTA). Your solution must minimize user calls to help desk. What should you do?

- A - Create a .txt file that provides step-by-step instructions for configuring Microsoft Active sync. Distribute the .txt file to all users.
- B - Create an .xml file that has the appropriate Microsoft Active sync settings. Distribute the xml file to all users.
- C - Create an xml file that has the appropriate Microsoft ActiveSync settings. Generate a .cab file that applies the settings from the .xml file. Distribute the .cab file to all users.
- D - Use the Connection Manager Administration Kit (CMAK) to create a self-installing .exe file to install a Virtual Private Network (VPN) connection. Distribute the .exe file to all users.

Answer: C

Question: 47

You deploy mobile devices that run Microsoft Windows Mobile 5.0 to users who have no access to desktop or portable computers. Each Windows Mobile based device runs a custom line-of-business (LOB) application. An update

of the new .cab file for the LOB applications is available at the Web site of the vendor with proper licensing.

You need to deploy the update to the devices by using the least amount of user effort and administrative effort.

What should you do?

A - Create an .msi package from the update of the .cab file. Create a Group Policy object (GPO) that deploys the update of the LOB application. Link the GPO to the domain object.

B - Download the update of the .cab file from the Web site of the vendor and e-mail the .cab file as an attachment to all users. Instruct users to double-click the attachment.

C - Download the update of the .cab file from the Web site of the vendor and store it on an internal Web site. Instruct all employees to use the Microsoft Pocket Internet Explorer to download and install the update of the LOS .cab file from the internal Web site.

D - Download the update of the cab file from the Web site of the vendor and store it on an internal Web site. Send a Short Message Service (SMS) message that has the URL of the internal Web site to all users. Instruct all users to visit the URL to download and install the update of the LOB .cab file.

Answer: B

Question: 48

You deploy a mobile messaging solution with Microsoft Exchange Server 2003 Service Pack 2.

Users of the mobile devices that run Microsoft Windows Mobile must immediately receive e-mails that arrive at the Exchange Server.

You need to ensure that the user requirements are met.

What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A - Configure the Microsoft ActiveSync schedule to 5 minutes.

B - Configure Windows Mobile 2003 Second Edition devices to use Always Up-to-Date (AUTD) functionality.

C - Certify all the mobile devices that run Microsoft Windows Mobile 2003 from a public certification authority.

D - Deploy the Microsoft Messaging and Security Feature Pack on all the mobile devices that run Microsoft Windows Mobile 5.0.

Answer: B, D

Question: 49

You deploy a mobile messaging solution with Microsoft Exchange Server 2003.

Users of the mobile devices that run Microsoft Windows Mobile synchronize contacts, calendar, e-mail, and tasks Over-The-Air (OTA).

You need to ensure that users can synchronize their favorites, files, and media.

What should you do?

A - Disable Windows Firewall on the desktop computers of the users.

- B - Grant administrative privileges to users on their desktop computers.
- C - Instruct the users to select all the available items in the Microsoft Exchange ActiveSync configuration.
- D - Instruct the users to select all the available items in the Microsoft ActiveSync configuration on the desktop.

Answer: D

Question: 50

You deploy mobile devices that run Microsoft Windows Mobile 5.0 to a group of users in your company. The Windows Mobile based devices are configured to access corporate e-mail accounts.

The group of users has the following requirements:

Must be able to retrieve and view personal e-mail messages and corporate e-mail messages separately from a third-party Internet e-mail provider.

Must be able to access all previously viewed e-mail messages, even when a wireless signal is unavailable.

You need to ensure that the outlined requirements are met.

What should you do?

- A - Configure corporate e-mail to be forwarded to the third-party personal e-mail provider.
- B - Configure a POP3 e-mail account on the Windows Mobile based devices of the users for their personal e-mail.
- C - Configure personal e-mail from the third-party provider to be forwarded to the corporate email account of the users.
- D - Instruct the users to use Microsoft Pocket Internet Explorer to retrieve personal e-mail from the third-party e-mail provider.

Answer: B