

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

<https://www.2passeasy.com/dumps/220-1102/>



NEW QUESTION 1

A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

- A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.
- B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.
- C. The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.
- D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

Answer: D

Explanation:

The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

NEW QUESTION 2

A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?

- A. Changing channels
- B. Modifying the wireless security
- C. Disabling the SSID broadcast
- D. Changing the access point name

Answer: A

Explanation:

Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

NEW QUESTION 3

Upon downloading a new ISO, an administrator is presented with the following string: 59d15a16ce90cBcc97fa7c211b767aB
Which of the following BEST describes the purpose of this string?

- A. XSS verification
- B. AES-256 verification
- C. Hash verification
- D. Digital signature verification

Answer: C

Explanation:

Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1

NEW QUESTION 4

A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state but the malware persists. Which of the following would MOST likely resolve the issue?

- A. Quarantining system files
- B. Reimaging the workstation
- C. Encrypting the hard drive
- D. Disabling TLS 1.0 support

Answer: C

Explanation:

Encrypting the hard drive would most likely resolve the issue1

NEW QUESTION 5

When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

- A. Have the user provide a callback phone number to be added to the ticket
- B. Assign the ticket to the department's power user
- C. Register the ticket with a unique user identifier
- D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Answer: D

Explanation:

The technician should provide the user with a unique ticket number that can be referenced on subsequent calls to make sure the ticket is associated with the correct user. This is because registering the ticket with a unique user identifier, having the user provide a callback phone number to be added to the ticket, or assigning the ticket to the department's power user will not ensure that the ticket is associated with the correct user2.

NEW QUESTION 6

A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?

- A. Multifactor authentication will be forced for Wi-Fi.
- B. All Wi-Fi traffic will be encrypted in transit.
- C. Eavesdropping attempts will be prevented.
- D. Rogue access points will not connect.

Answer: A

Explanation:

Multifactor authentication will be forced for Wi-Fi after deploying a client certificate to be used for Wi-Fi access for all devices in an organization.

References:

➤ [CompTIA Security+ \(Plus\) Practice Test Questions | CompTIA](https://www.comptia.org/training/resources/comptia-security-practice-tests). Retrieved from <https://www.comptia.org/training/resources/comptia-security-practice-tests>

NEW QUESTION 7

A technician has just used an anti-malware removal tool to resolve a user's malware issue on a corporate laptop. Which of the following BEST describes what the technician should do before returning the laptop to the user?

- A. Educate the user on malware removal.
- B. Educate the user on how to reinstall the laptop OS.
- C. Educate the user on how to access recovery mode.
- D. Educate the user on common threats and how to avoid them.

Answer: D

Explanation:

educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again.

NEW QUESTION 8

A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

- A. Scope of change
- B. Risk level
- C. Rollback plan
- D. End user acceptance

Answer: C

Explanation:

The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

NEW QUESTION 9

Which of the following is the STRONGEST wireless configuration?

- A. WPS
- B. WPA3
- C. WEP
- D. WMN

Answer: B

Explanation:

The strongest wireless configuration is B. WPA3. WPA3 is the most up-to-date wireless encryption protocol and is the most secure choice. It replaces PSK with SAE, a more secure way to do the initial key exchange. At the same time, the session key size of WPA3 increases to 128-bit in WPA3-Personal mode and 192-bit in WPA3-Enterprise, which makes the password harder to crack than the previous Wi-Fi security standards.

<https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/>

NEW QUESTION 10

A user reports that a workstation is operating sluggishly. Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should the systems administrator most likely attempt NEXT?

- A. Increase the paging file size.
- B. Run the chkdsk command.
- C. Rebuild the user's profile.
- D. Add more system memory.
- E. Defragment the hard drive.

Answer: C

Explanation:

Since the systems administrator has validated that the workstation functions normally and other users operate on the same workstation without any issues, the

next step should be to rebuild the user's profile. This will ensure that any corrupted files or settings are removed and the user's profile is restored to its default state.

NEW QUESTION 10

Each time a user tries to go to the selected web search provider, a different website opens. Which of the following should the technician check FIRST?

- A. System time
- B. IP address
- C. DNS servers
- D. Windows updates

Answer: C

Explanation:

When a user experiences unexpected or erratic behavior while browsing the internet, it could be caused by the DNS servers. DNS translates human-readable domain names (like google.com) into IP addresses, which computers can use to communicate with web servers. If the DNS servers are not functioning correctly or have been compromised, it can result in the browser being redirected to unintended websites.

NEW QUESTION 15

As part of a CYOD policy a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

- A. Use Settings to access Screensaver settings
- B. Use Settings to access Screen Timeout settings
- C. Use Settings to access General
- D. Use Settings to access Display.

Answer: A

Explanation:

The systems administrator should use Settings to access Screensaver settings to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity¹

NEW QUESTION 18

A technician receives a ticket indicating the user cannot resolve external web pages. However, specific IP addresses are working. Which of the following does the technician MOST likely need to change on the workstation to resolve the issue?

- A. Default gateway
- B. Host address
- C. Name server
- D. Subnet mask

Answer: A

Explanation:

The technician most likely needs to change the default gateway on the workstation to resolve the issue. The default gateway is the IP address of the router that connects the workstation to the internet, and it is responsible for routing traffic between the workstation and the internet. If the default gateway is incorrect, the workstation will not be able to access external web pages.

NEW QUESTION 20

A user contacted the help desk to report pop-ups on a company workstation indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Select TWO)

- A. Scan the computer with the company-provided antivirus software
- B. Install a new hard drive and clone the user's drive to it
- C. Deploy an ad-blocking extension to the browser.
- D. Uninstall the company-provided antivirus software
- E. Click the link in the messages to pay for virus removal
- F. Perform a reset on the user's web browser

Answer: CF

Explanation:

"The user thought the company-provided antivirus software would prevent this issue."

The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

NEW QUESTION 22

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?

- A. A bad antivirus signature update was installed.
- B. A router was misconfigured and was blocking traffic.
- C. An upstream internet service provider was flapping.
- D. The time or date was not in sync with the website.

Answer: B

Explanation:

The most likely cause of this issue is that a router was misconfigured and was blocking traffic. This would explain why remote users who were not connected to corporate resources did not have any issues.

NEW QUESTION 26

Which of the following command-line tools will delete a directory?

- A. md
- B. del
- C. dir
- D. rd
- E. cd

Answer: D

Explanation:

To delete an empty directory, enter `rd Directory` or `rmdir Directory`. If the directory is not empty, you can remove files and subdirectories from it using the `/s` switch. You can also use the `/q` switch to suppress confirmation messages (quiet mode).

NEW QUESTION 29

A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?

- A. Removed all jewelry
- B. Completed an inventory of tools before use
- C. Practiced electrical fire safety
- D. Connected a proper ESD strap

Answer: D

Explanation:

The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity. Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.

NEW QUESTION 31

During a recent flight an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

- A. set AirDrop so that transfers are only accepted from known contacts
- B. completely disable all wireless systems during the flight
- C. discontinue using iMessage and only use secure communication applications
- D. only allow messages and calls from saved contacts

Answer: A

Explanation:

To best resolve this issue, the executive should set AirDrop so that transfers are only accepted from known contacts (option A). AirDrop is a feature on iOS devices that allows users to share files, photos, and other data between Apple devices. By setting AirDrop so that it only accepts transfers from known contacts, the executive can ensure that unwanted files and photos are not sent to their device. Additionally, the executive should ensure that the AirDrop setting is only enabled when it is necessary, as this will protect their device from any unwanted files and photos.

NEW QUESTION 33

The command `cac cor.ptia. txt` was issued on a Linux terminal. Which of the following results should be expected?

- A. The contents of the text `comptia.txt` will be replaced with a new blank document
- B. The contents of the text `compti`
- C. `txt` would be displayed.
- D. The contents of the text `comptia.txt` would be categorized in alphabetical order.
- E. The contents of the text `compti`
- F. `txt` would be copied to another `compti`
- G. `txt` file

Answer: B

Explanation:

The command `cac cor.ptia. txt` was issued on a Linux terminal. This command would display the contents of the text `comptia.txt`.

NEW QUESTION 35

A user is attempting to make a purchase at a store using a phone. The user places the phone on the payment pad, but the device does not recognize the phone. The user attempts to restart the phone but still has the same results. Which of the following should the user do to resolve the issue?

- A. Turn off airplane mode while at the register.
- B. Verify that NFC is enabled.
- C. Connect to the store's Wi-Fi network.

D. Enable Bluetooth on the phone.

Answer: B

Explanation:

The user should verify that NFC is enabled on their phone. NFC is a technology that allows two devices to communicate with each other when they are in close proximity².

NFC (Near Field Communication) technology allows a phone to wirelessly communicate with a payment terminal or other compatible device. In order to use NFC to make a payment or transfer information, the feature must be enabled on the phone. Therefore, the user should verify that NFC is enabled on their phone before attempting to make a payment with it. The other options, such as turning off airplane mode, connecting to Wi-Fi, or enabling Bluetooth, do not pertain to the NFC feature and are unlikely to resolve the issue. This information is covered in the CompTIA A+ Core2 documents/guide under the Mobile Devices section.

NEW QUESTION 39

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

- A. Security and Maintenance
- B. Network and Sharing Center
- C. Windows Defender Firewall
- D. Internet Options

Answer: D

Explanation:

The best choice for accessing the necessary configuration to configure the desktop systems to use a new proxy server is the Internet Options utility. This utility can be found in the Control Panel and allows you to configure the proxy settings for your network connection. As stated in the CompTIA A+ Core 2 exam objectives, technicians should be familiar with the Internet Options utility and how to configure proxy settings.

NEW QUESTION 40

A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

- A. Rights management
- B. Audit trail
- C. Chain of custody
- D. Data integrity

Answer: C

Explanation:

The process of documenting who had possession of evidence at every step of the process is called chain of custody

NEW QUESTION 43

A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

- A. resmon.exe
- B. dfrgui.exe
- C. msinf032.exe
- D. msconfig.exe

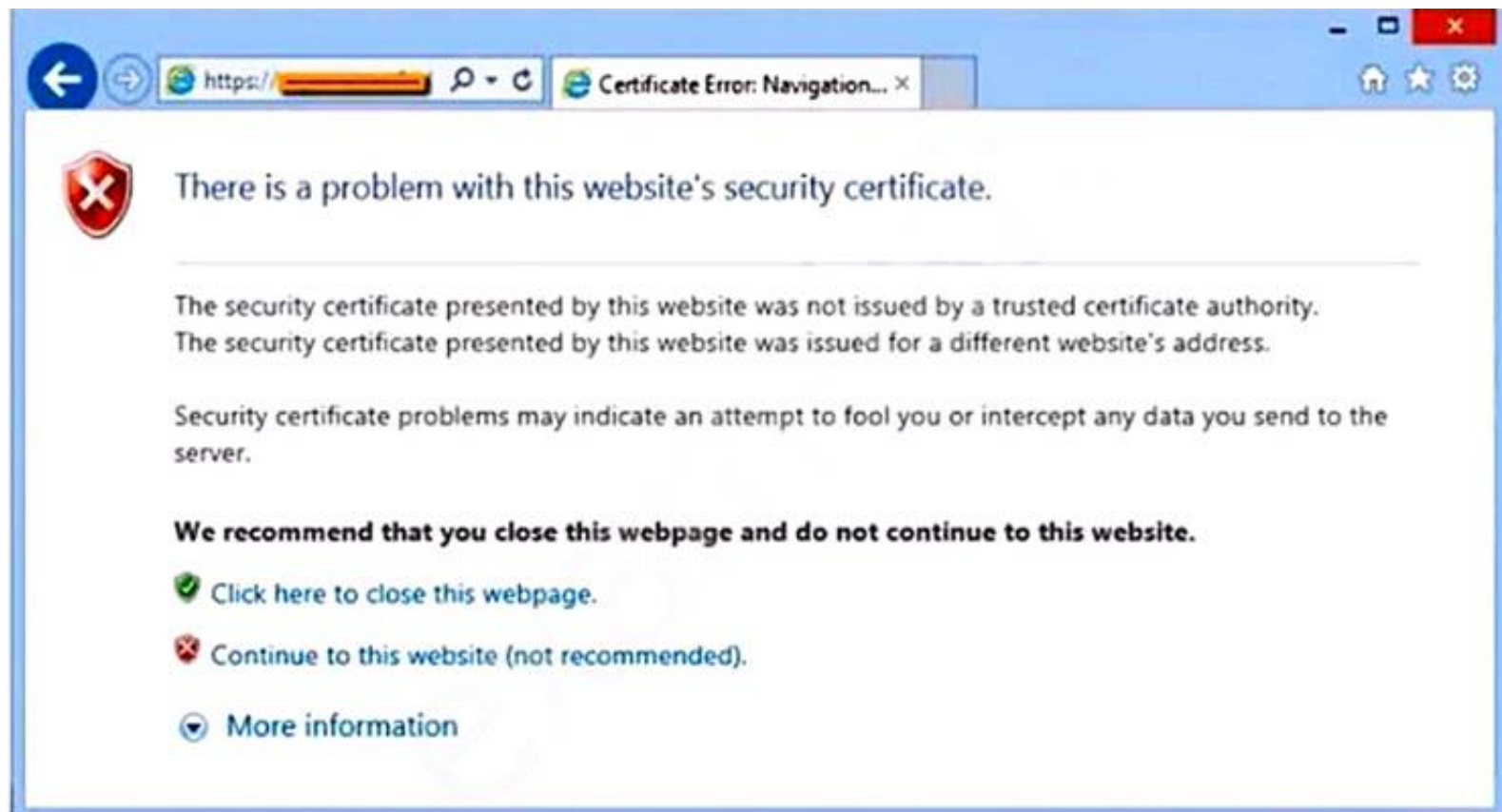
Answer: A

Explanation:

If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O¹. Resource Monitor provides detailed information about the system's resource usage, including disk I/O¹. The technician can use this information to identify the process that is causing the high disk I/O and take appropriate action¹.

NEW QUESTION 47

After clicking on a link in an email a Chief Financial Officer (CFO) received the following error:



The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

- A. Update the browser's CRLs
- B. File a trouble ticket with the bank.
- C. Contact the ISP to report the CFCs concern
- D. Instruct the CFO to exit the browser

Answer: A

Explanation:

The technician should update the browser's CRLs first. The error message indicates that the certificate revocation list (CRL) is not up to date. Updating the CRLs will ensure that the browser can verify the authenticity of the bank's website.

NEW QUESTION 52

Which of the following is a proprietary Cisco AAA protocol?

- A. TKIP
- B. AES
- C. RADIUS
- D. TACACS+

Answer: D

Explanation:

TACACS+ is a proprietary Cisco AAA protocol

NEW QUESTION 53

A technician received a call stating that all files in a user's documents folder appear to be Changed, and each of the files now has a look file extension Which pf the following actions is the FIRST step the technician should take?

- A. Run a live disk clone.
- B. Run a full antivirus scan.
- C. Use a batch file to rename the files
- D. Disconnect the machine from the network

Answer: D

Explanation:

The CompTIA A+ Core 2 220-1002 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

NEW QUESTION 55

A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

- A. Drilling
- B. Degaussing
- C. Low-level formatting
- D. Erasing/wiping

Answer: D

Explanation:

Erasing/wiping the hard drives is the best method to dispose of the drives containing PII

NEW QUESTION 57

A user's system is infected with malware. A technician updates the anti-malware software and runs a scan that removes the malware. After the user reboots the system, it once again becomes infected with malware. Which of the following will MOST likely help to permanently remove the malware?

- A. Enabling System Restore
- B. Educating the user
- C. Booting into safe mode
- D. Scheduling a scan

Answer: B

Explanation:

Although updating the anti-malware software and running scans are important steps in removing malware, they may not be sufficient to permanently remove the malware if the user keeps engaging in behaviors that leave the system vulnerable, such as downloading unknown files or visiting malicious websites. Therefore, educating the user on safe computing practices is the best way to prevent future infections and permanently remove the malware.

Enabling System Restore, Booting into safe mode, and scheduling a scan are not the most efficient ways to permanently remove the malware. Enabling System Restore and Booting into safe mode may help in some cases, but they may not be sufficient to permanently remove the malware. Scheduling a scan is also important for detecting and removing malware, but it may not be sufficient to prevent future infections.

[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

NEW QUESTION 60

A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

- A. Avoid distractions
- B. Deal appropriately with customer's confidential material .
- C. Adhere to user privacy policy
- D. Set and meet timelines

Answer: A

Explanation:

The technician's action of setting the phone to silent while troubleshooting the customer's PC is an example of avoiding distractions. By setting the phone to silent, the technician is ensuring that they are able to focus on the task at hand without any distractions that could potentially disrupt their workflow. This is an important practice when handling customer's confidential material, as it ensures that the technician is able to focus on the task and not be distracted by any external sources. Furthermore, it also adheres to user privacy policies, as the technician is not exposing any confidential information to any external sources.

NEW QUESTION 62

A technician is configuring a SOHO device Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same IP address at all times. Which of the following should the technician use?

- A. DHCP reservation
- B. Port forwarding
- C. DNS A record
- D. NAT

Answer: A

Explanation:

The technician should use DHCP reservation to maintain the same IP address for the server at all times. DHCP reservation allows the server to obtain an IP address dynamically from the DHCP server, while ensuring that the same IP address is assigned to the server each time it requests an IP address.

NEW QUESTION 63

A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

- A. resmon.exe
- B. msconfig.extf
- C. dfrgui.exe
- D. msmf32.exe

Answer: C

Explanation:

The technician should use dfrgui.exe to defragment the hard drive¹

NEW QUESTION 65

The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

- A. Encryption at rest
- B. Account lockout
- C. Automatic screen lock
- D. Antivirus

Answer: B

Explanation:

Account lockout would best mitigate the threat of a dictionary attack¹

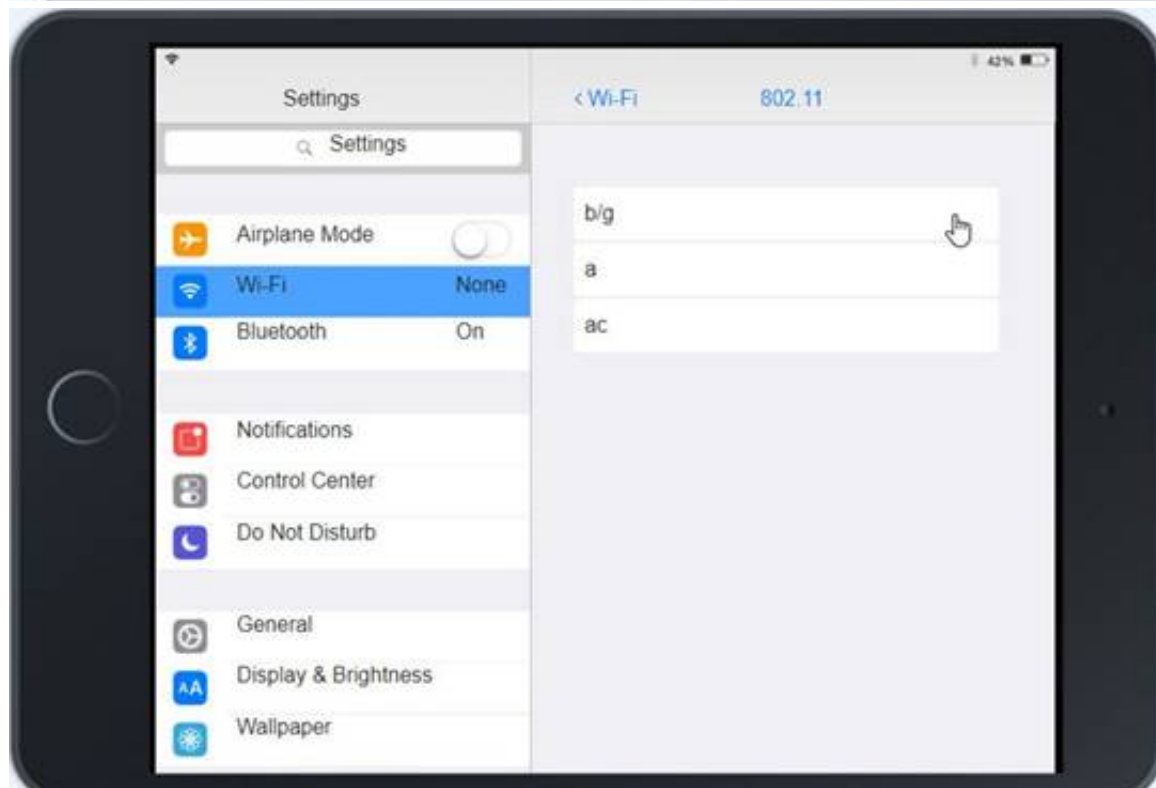
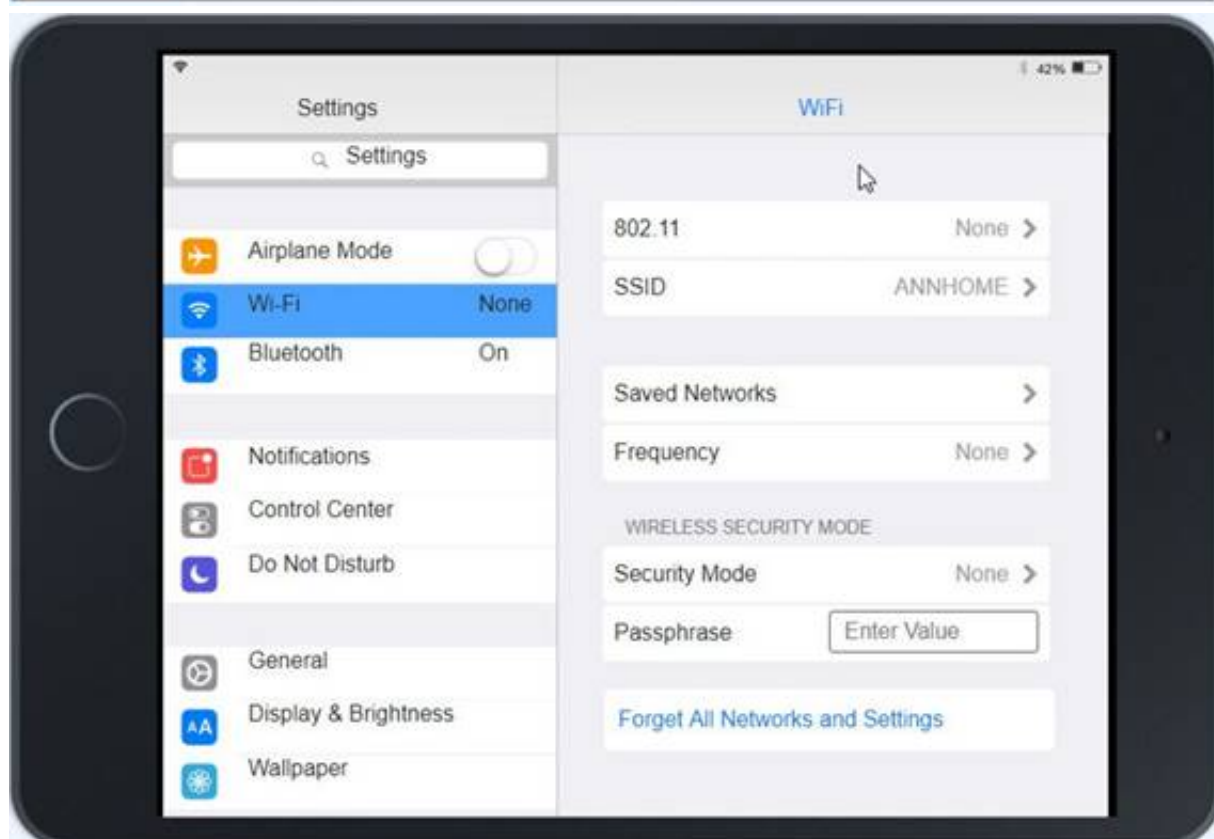
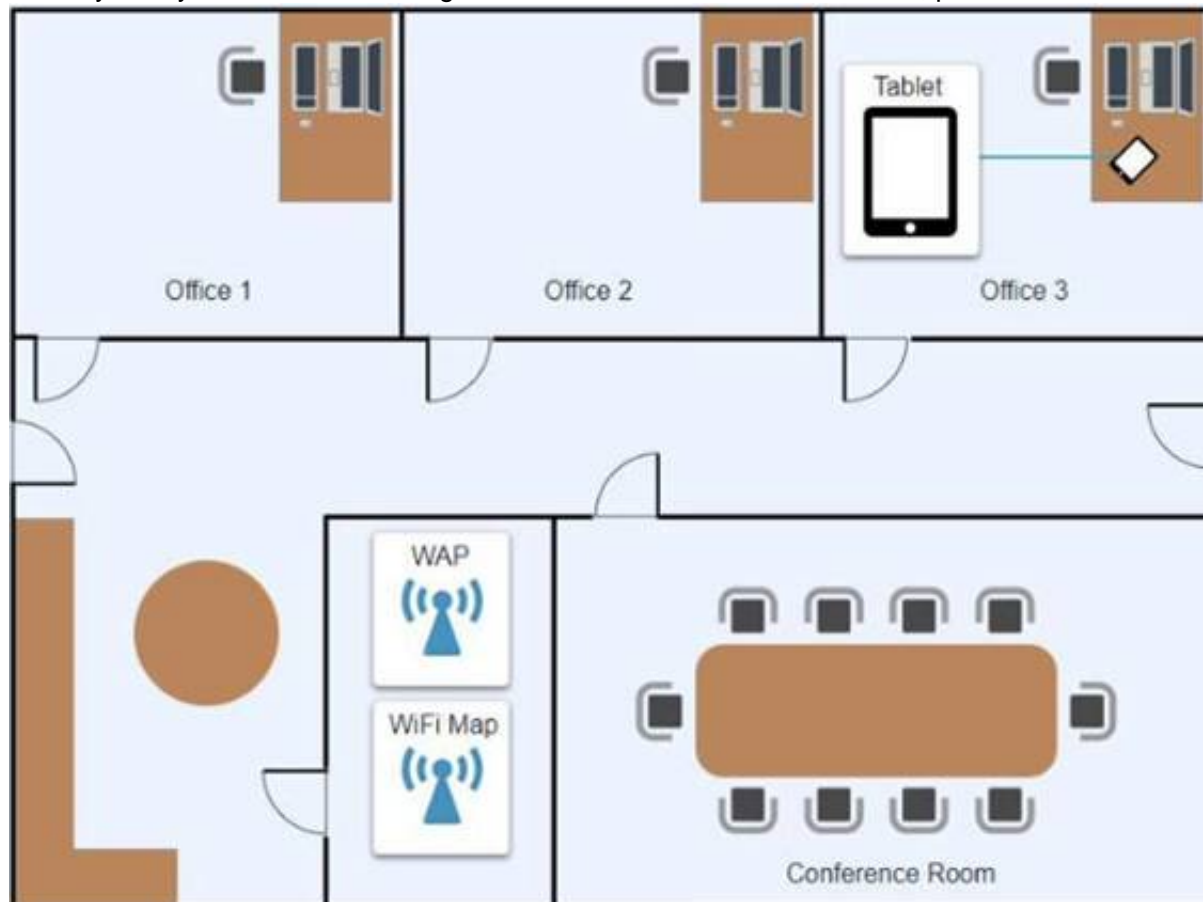
NEW QUESTION 67

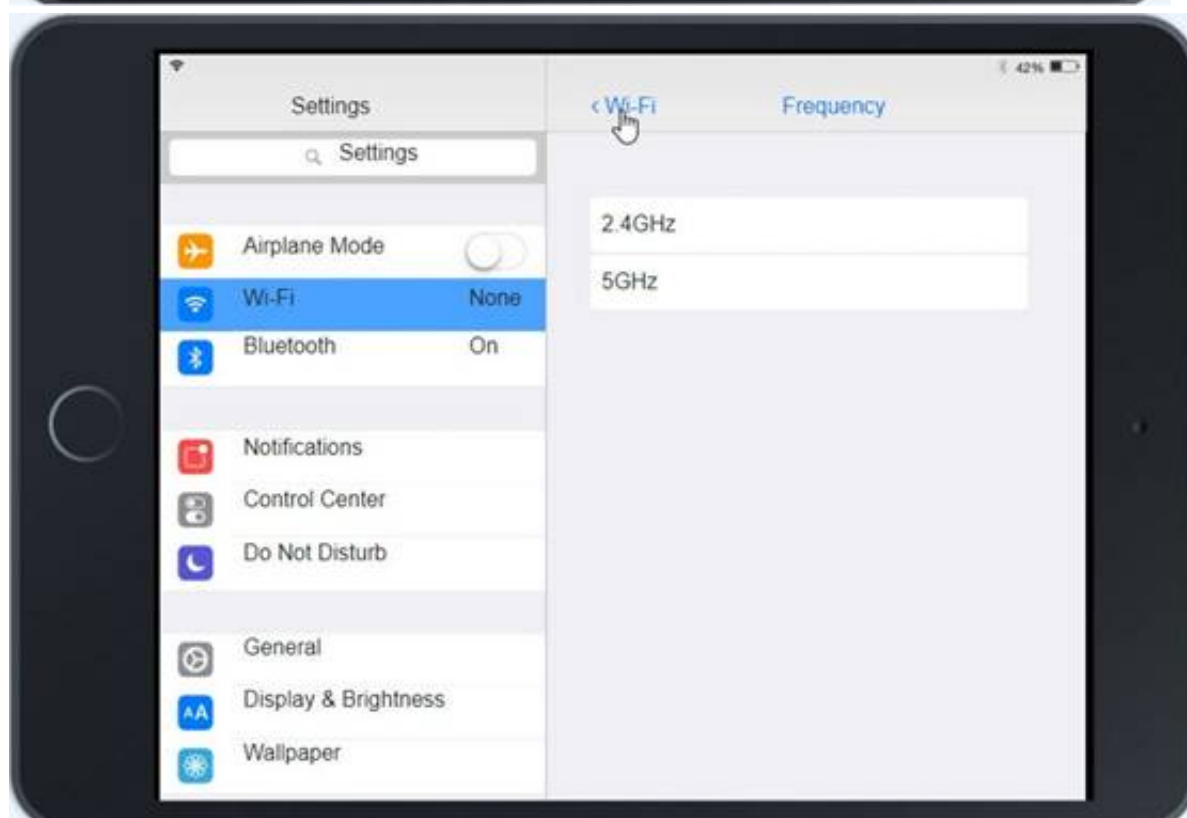
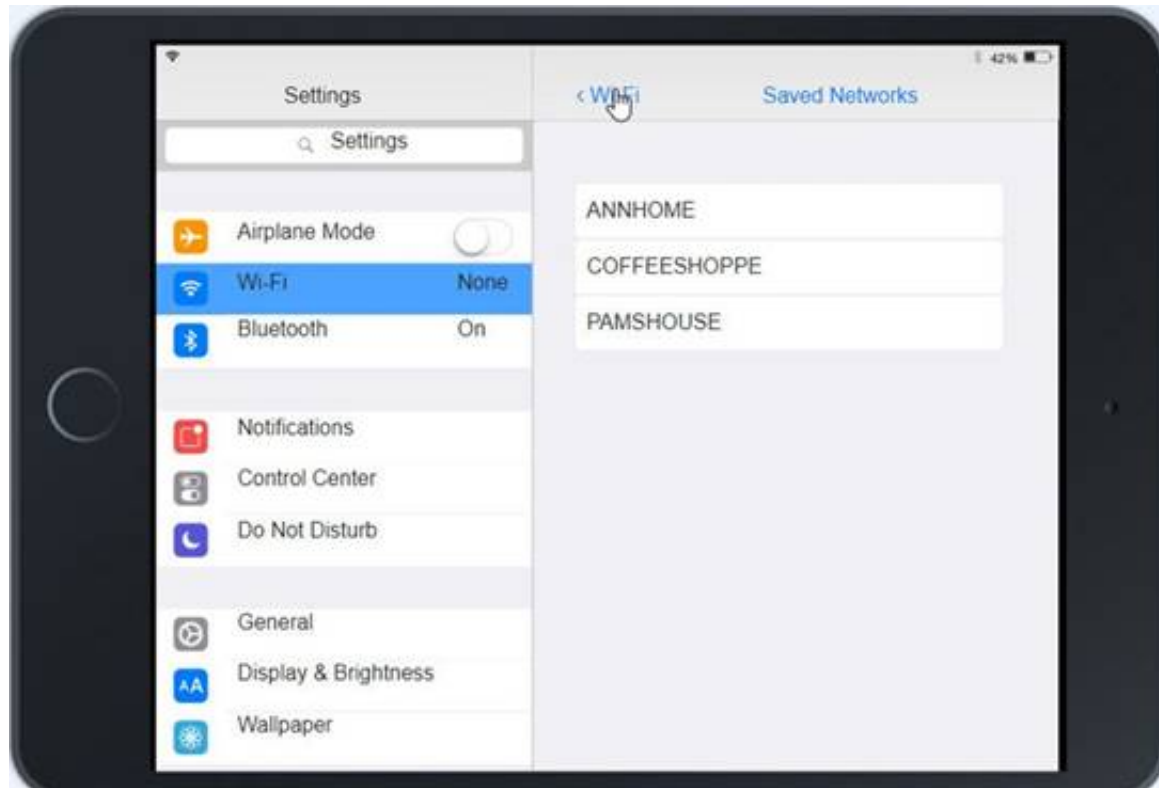
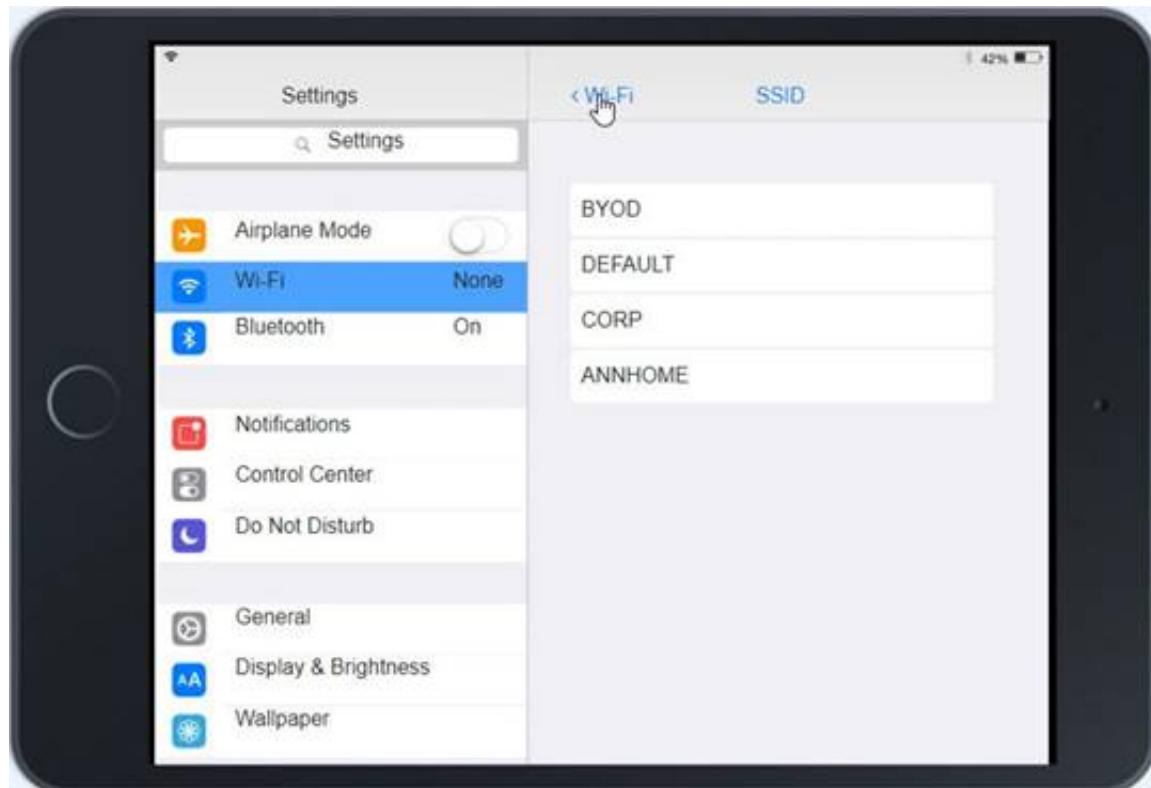
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect it to the company's wireless network. All the corporate laptops are connecting without issue. She has asked you to assist with getting the device online.

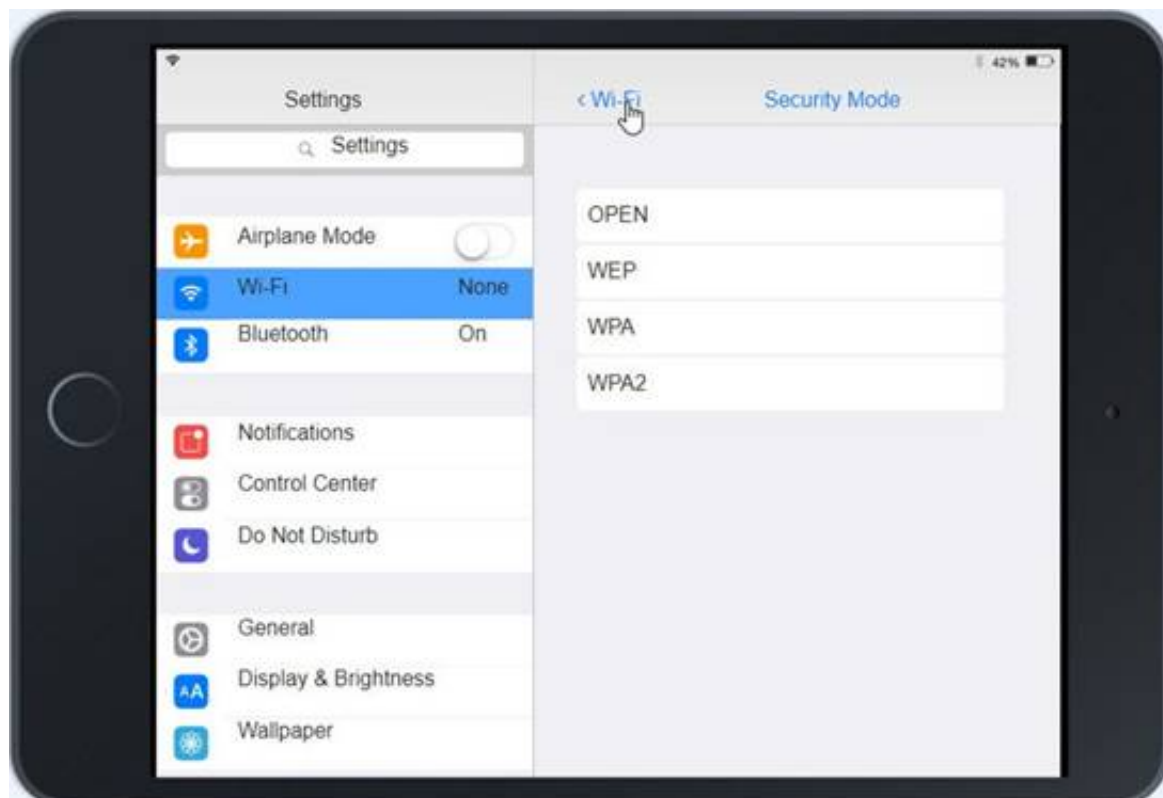
INSTRUCTIONS

Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





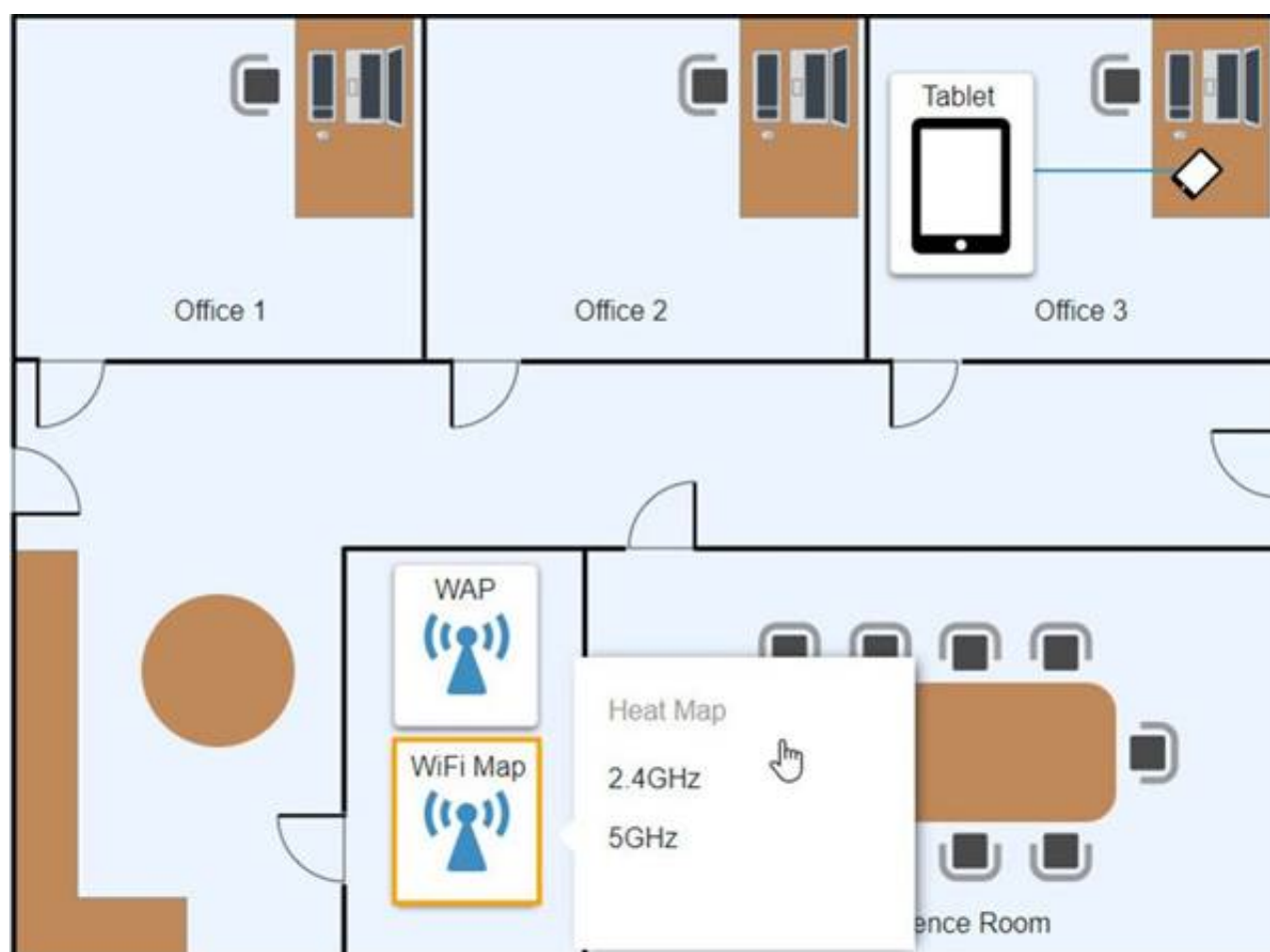


Settings

Site	Wireless Networks			
Wireless Networks				
Networks				
Guest Control				
Admins				
User Groups				
VOIP				
Controller				
Cloud Access				
Maintenance				

SSID	Frequency	Security	Totally Secure!
CORP	2.4GHz/5GHz	WPA2	Corpsecure1
BYOD	2.4GHz/5GHz	WPA-PSK	TotallySecure1

Create New Wireless Network

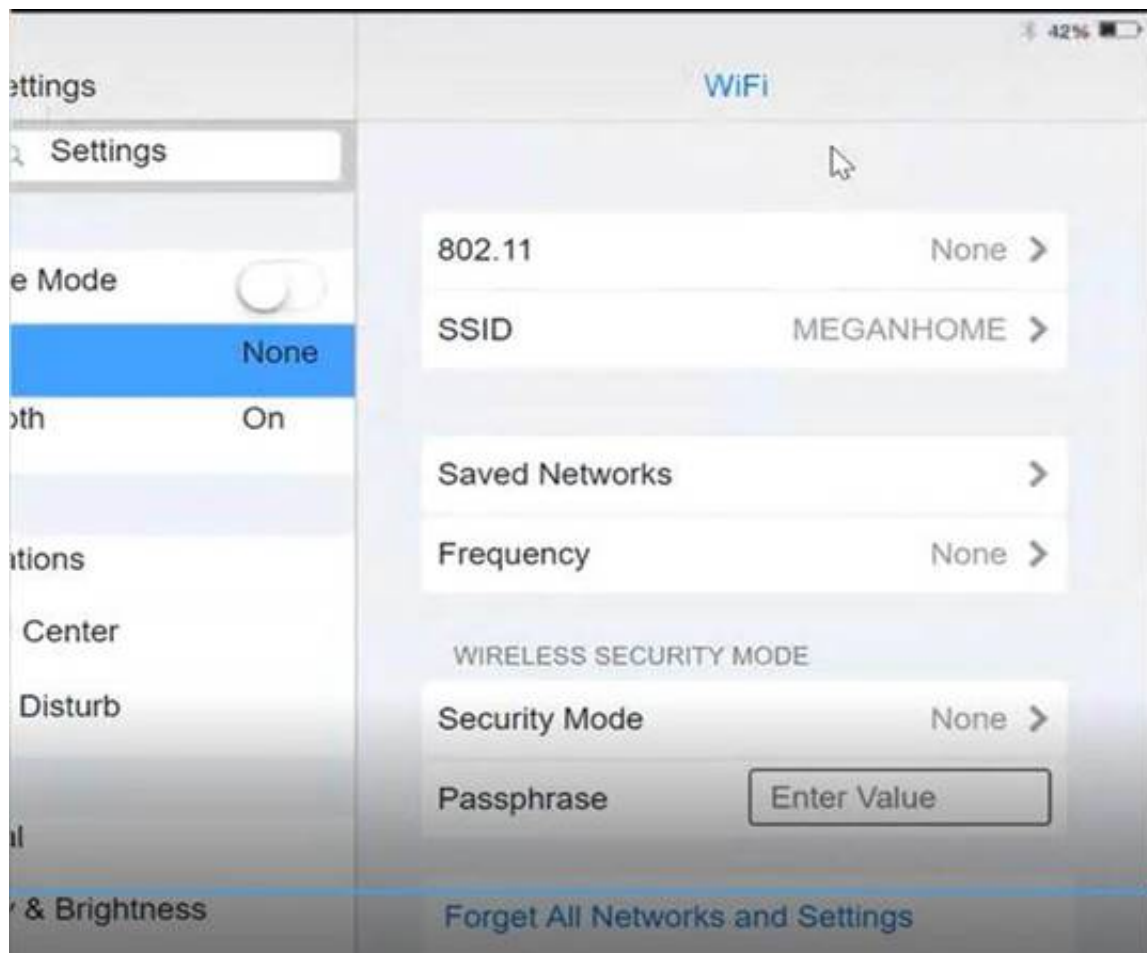


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

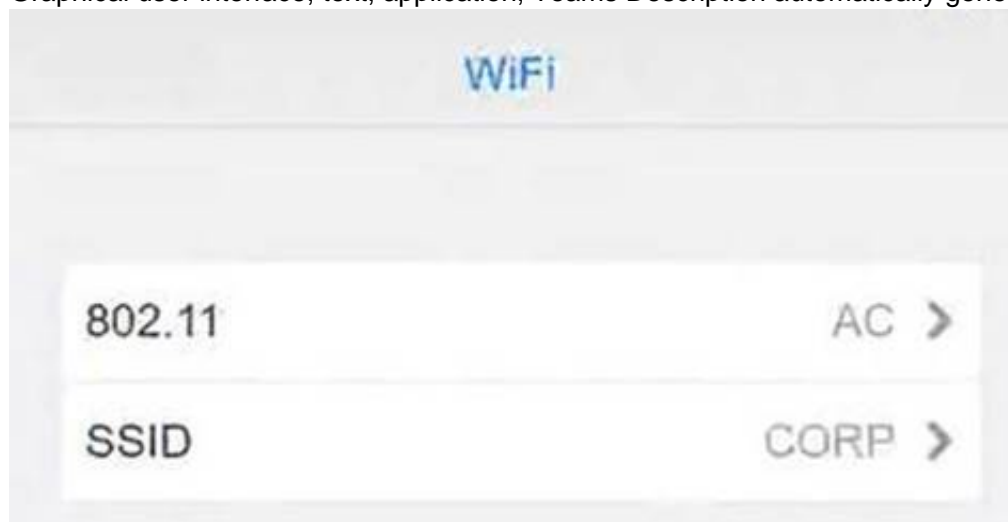
Graphical user interface, application Description automatically generated



Click on 802.11 and Select ac
Graphical user interface, application Description automatically generated



Click on SSID and select CORP
Graphical user interface, text, application, Teams Description automatically generated



Click on Frequency and select 5GHz
A picture containing background pattern Description automatically generated



At Wireless Security Mode, Click on Security Mode
Graphical user interface, text, application Description automatically generated



Select the WPA2

Graphical user interface, application, Teams Description automatically generated with medium confidence



Ann needs to connect to the BYOD SSID, using 2.4GHZ. The selected security method chose should be WPA PSK, and the password should be set to TotallySecret.

Graphical user interface, application Description automatically generated



NEW QUESTION 68

A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in to the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

- A. Time drift
- B. Dual in-line memory module failure
- C. Application crash
- D. Filesystem errors

Answer: A

Explanation:

The most likely cause of the issue is a "time drift". Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC.

NEW QUESTION 71

A technician is unable to join a Windows 10 laptop to a domain. Which of the following is the MOST likely reason?

- A. The domain's processor compatibility is not met
- B. The laptop has Windows 10 Home installed
- C. The laptop does not have an onboard Ethernet adapter
- D. The Laptop does not have all current Windows updates installed

Answer: B

Explanation:

[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

NEW QUESTION 75

A technician is tasked with configuring a computer for a visually impaired user. Which of the following utilities should the technician use?

- A. Device Manager
- B. System
- C. Ease of Access Center
- D. Programs and Features

Answer: C

Explanation:

The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

NEW QUESTION 77

A technician has been tasked with installing a workstation that will be used for point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

- A. Data-in-transit encryption
- B. File encryption
- C. USB drive encryption
- D. Disk encryption

Answer: D

Explanation:

Disk encryption should be used to secure the workstation in case of theft. Disk encryption can help to protect data on the hard drive by encrypting it so that it cannot be accessed without the correct encryption key.

NEW QUESTION 78

Which of the following should be used to control security settings on an Android phone in a domain environment?

- A. MDM
- B. MFA
- C. ACL
- D. SMS

Answer: A

Explanation:

The best answer to control security settings on an Android phone in a domain environment is to use "Mobile Device Management (MDM)". MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities¹²

NEW QUESTION 80

A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the user's account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

- A. acceptable use policy.
- B. regulatory compliance requirements.
- C. non-disclosure agreement
- D. incident response procedures

Answer: A

Explanation:

Logging into a user's account without their explicit permission is a violation of the acceptable use policy, which outlines the rules and regulations by which a user must abide while using a computer system. By logging into the user's account without their permission, the technician would be violating this policy. Additionally, this action could be seen as a breach of confidentiality, as the technician would have access to information that should remain confidential.

NEW QUESTION 82

A suite of security applications was installed a few days ago on a user's home computer. The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

- A. Services in Control Panel to check for overutilization

- B. Performance Monitor to check for resource utilization
- C. System File Checker to check for modified Windows files
- D. Event Viewer to identify errors

Answer: C

Explanation:

System File Checker to check for modified Windows files. System File Checker (SFC) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applications [1][2]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.

NEW QUESTION 86

A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access A technician verifies the user's PC is infected with ransorrware. Which of the following should the technician do FIRST?

- A. Scan and remove the malware
- B. Schedule automated malware scans
- C. Quarantine the system
- D. Disable System Restore

Answer: C

Explanation:

The technician should quarantine the system first¹

NEW QUESTION 87

A user is unable to access a website, which is widely used across the organization, and receives the following error message:

The security certificate presented by this website has expired or is not yet valid.

The technician confirms the website works when accessing it from another computer but not from the user's computer. Which of the following should the technician perform NEXT to troubleshoot the issue?

- A. Reboot the computer.
- B. Reinstall the OS.
- C. Configure a static IP
- D. Check the computer's date and time.

Answer: D

Explanation:

The error message indicates that the security certificate presented by the website has either expired or is not yet valid. This can happen if the computer's clock has the wrong date or time, as SSL/TLS certificates have a specific validity period. If the clock is off by too much, it may cause the certificate to fail to validate. Therefore, the technician should check the computer's date and time and ensure that they are correct.

NEW QUESTION 90

An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

- A. Encrypt the files
- B. Clone any impacted hard drives
- C. Contact the cyber insurance company
- D. Inform law enforcement

Answer: B

Explanation:

The incident handler should clone any impacted hard drives to preserve evidence for possible litigation¹

NEW QUESTION 92

A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

- A. Use the application only on the home laptop because it contains the initial license.
- B. Use the application at home and contact the vendor regarding a corporate license.
- C. Use the application on any computer since the user has a license.
- D. Use the application only on corporate computers.

Answer: B

Explanation:

Use the application at home and contact the vendor regarding a corporate license. The user should use the application only on the home laptop because it contains the initial license. The user should contact the vendor regarding a corporate license if they want to use the application on multiple computers on the corporate network¹

NEW QUESTION 94

A user wants to set up speech recognition on a PC In which of the following Windows Settings tools can the user enable this option?

- A. Language

- B. System
- C. Personalization
- D. Ease of Access

Answer: D

Explanation:

The user can enable speech recognition on a PC in the Ease of Access settings tool. To set up Speech Recognition on a Windows PC, the user should open Control Panel, click on Ease of Access, click on Speech Recognition, and click the Start Speech Recognition link. Language settings can be used to change the language of the speech recognition feature, but they will not enable the feature. System settings can be used to configure the hardware and software of the PC, but they will not enable the speech recognition feature. Personalization settings can be used to customize the appearance and behavior of the PC, but they will not enable the speech recognition feature¹ Open up ease of access, click on speech, then there is an on and off button for speech recognition.

NEW QUESTION 96

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

- A. File Explorer
- B. User Account Control
- C. Windows Backup and Restore
- D. Windows Firewall
- E. Windows Defender
- F. Network Packet Analyzer

Answer: AE

Explanation:

The correct answers are E. Windows Defender and A. File Explorer. Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software¹

NEW QUESTION 98

Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

Click on individual tickers to see the ticket details. View attachments to determine the problem.

Select the appropriate issue from the 'issue' drop-down menu. Then, select the MOST efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the Verify Resolve drop-down menu.

Details

#8675310

Open

Priority

Low

Category

Technical / Bug Reports

Assigned To

helpdesk@fictional.com

Assigned Date

7/13/2022

Subject

Unable to access Z: on my computer, but I can manually enter the location in the window.

Attachments

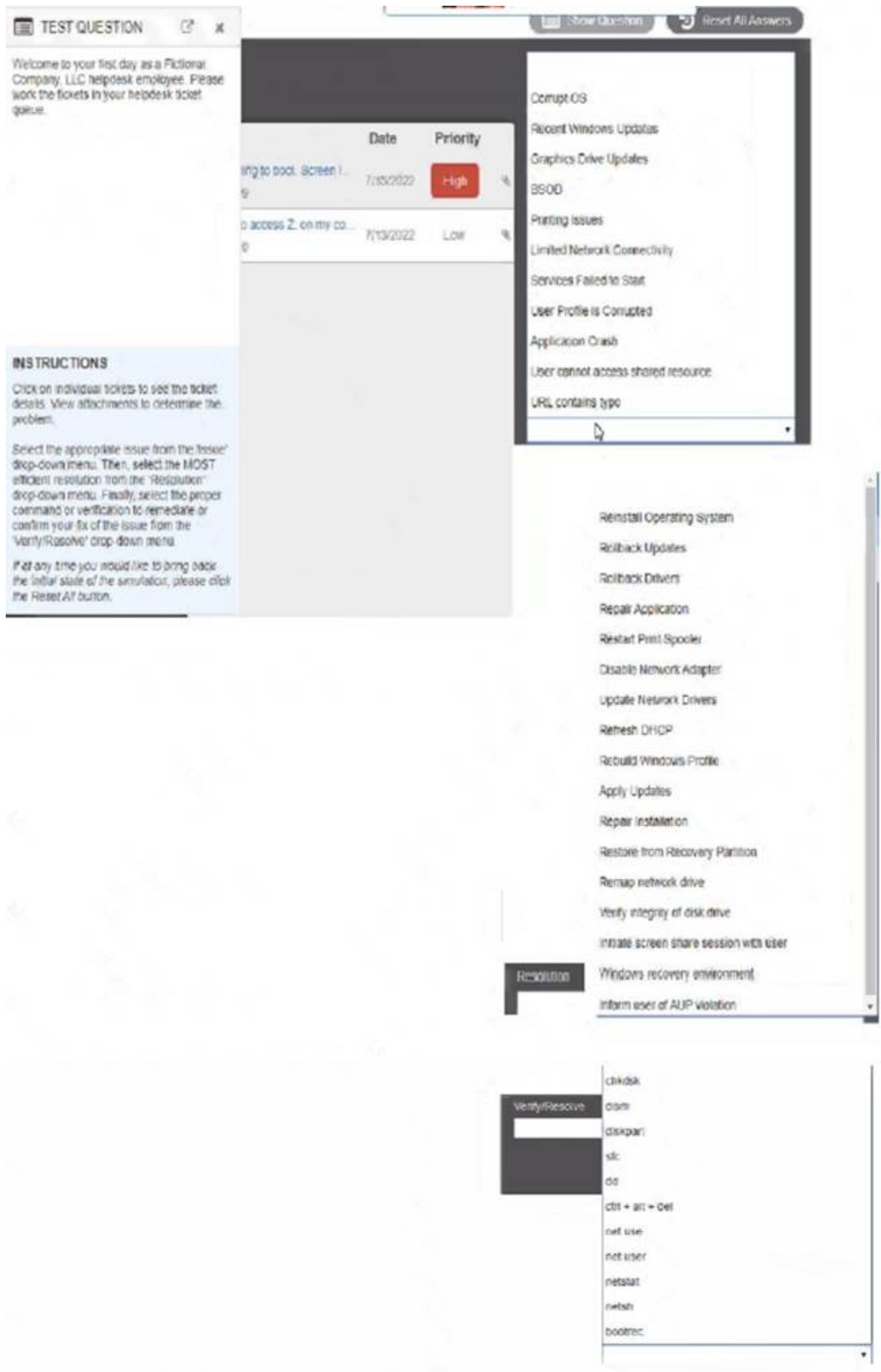
[File Explorer.jpg](#)

Issue

Resolution

Verify/Resolve

Close Ticket



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Details

#8675310

Open

Priority

Low

Category

Technical / Bug Reports

Assigned To

helpdesk@fictional.com

Assigned Date

7/13/2022

Subject

Unable to access Z: on my computer, but I can manually enter the location in the window.

Attachments

[File Explorer.jpg](#)

Issue

Corrupt OS

Resolution

Reinstall Operating System

Verify/Resolve

chkdsk

Close Ticket

NEW QUESTION 101

A user reports that the hard drive activity light on a Windows 10 desktop computer has been steadily lit for more than an hour, and performance is severely degraded. Which of the following tabs in Task Manager would contain the information a technician would use to identify the cause of this issue?

- A. Services
- B. Processes
- C. Performance
- D. Startup

Answer: B

Explanation:

Processes tab in Task Manager would contain the information a technician would use to identify the cause of this issue. The Processes tab in Task Manager displays all the processes running on the computer, including the CPU and memory usage of each process. The technician can use this tab to identify the process that is causing the hard drive activity light to remain lit and the performance degradation¹

NEW QUESTION 102

An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update A technician determines there are no error messages on the device Which of the following should the technician do NEXT?

- A. Verify all third-party applications are disabled
- B. Determine if the device has adequate storage available.
- C. Check if the battery is sufficiently charged
- D. Confirm a strong internet connection is available using Wi-Fi or cellular data

Answer: C

Explanation:

Since there are no error messages on the device, the technician should check if the battery is sufficiently charged¹

If the battery is low, the device may not have enough power to complete the update²

In this scenario, the technician has already determined that there are no error messages on the device. The next best step would be to check if the battery is sufficiently charged. If the battery is low, it could be preventing the device from completing the update process.

Verifying that third-party applications are disabled, determining if the device has adequate storage available, and confirming a strong internet connection are all important steps in troubleshooting issues with mobile devices. However, since the problem in this scenario is related to a failed OS update, it is important to first check the battery level before proceeding with further troubleshooting steps.

NEW QUESTION 107

A technician needs to recommend the best backup method that will mitigate ransomware attacks. Only a few files are regularly modified, however, storage space is a concern. Which of the following backup methods would BEST address these concerns?

- A. Full
- B. Differential
- C. Off-site
- D. Grandfather-father-son

Answer:

B

Explanation:

The differential backup method would best address these concerns. Differential backups only back up files that have changed since the last full backup, which means that only a few files would be backed up each time. This would help to mitigate the risk of ransomware attacks, as only a few files would be affected if an attack occurred. Additionally, differential backups require less storage space than full backups.

NEW QUESTION 112

A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

- A. Enable multifactor authentication.
- B. Increase the failed log-in threshold.
- C. Remove complex password requirements.
- D. Implement a single sign-on with biometrics.

Answer: A

Explanation:

Multifactor authentication (MFA) is a security measure that requires users to provide multiple pieces of evidence when logging in to an account or system. This can include a combination of something the user knows (e.g. a password or PIN), something the user has (e.g. a security token or smartphone) and something the user is (e.g. biometrics such as a fingerprint or face scan). By enabling MFA, the systems administrator can ensure that users are required to provide multiple pieces of evidence when logging in, making it more difficult for unauthorized users to gain access to the system. This can help reduce the number of help desk tickets submitted due to forgotten passwords.

NEW QUESTION 115

A developer is creating a shell script to automate basic tasks in Linux. Which of the following file types are supported by default?

- A. .py
- B. .js
- C. .vbs
- D. .sh

Answer: D

Explanation:

<https://www.educba.com/shell-scripting-in-linux/>

NEW QUESTION 120

Security software was accidentally uninstalled from all servers in the environment. After requesting the same version of the software be reinstalled, the security analyst learns that a change request will need to be filled out. Which of the following is the BEST reason to follow the change management process in this scenario?

- A. Owners can be notified a change is being made and can monitor it for performance impact
- B. Most Voted
- C. A risk assessment can be performed to determine if the software is needed.
- D. End users can be aware of the scope of the change.
- E. A rollback plan can be implemented in case the software breaks an application.

Answer: A

Explanation:

change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

NEW QUESTION 124

A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?

- A. macOS
- B. Linux
- C. Chrome OS
- D. Windows

Answer: C

Explanation:

* 4. Chrome OS. Retrieved from https://en.wikipedia.org/wiki/Chrome_OS 5. What is Chrome OS? Retrieved from <https://www.google.com/chromebook/chrome-os/>
A netbook with a web-based, proprietary operating system is most likely running Chrome OS. Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low-power devices and is designed to be fast, secure, and easy to use.

NEW QUESTION 129

A technician is attempting to mitigate micro power outages, which occur frequently within the area of operation. The outages are usually short, with the longest occurrence lasting five minutes. Which of the following should the technician use to mitigate this issue?

- A. Surge suppressor

- B. Battery backup
- C. CMOS battery
- D. Generator backup

Answer: B

Explanation:

A battery backup, also known as an uninterruptible power supply (UPS), is a device that provides backup power during a power outage. When the power goes out, the battery backup provides a short amount of time (usually a few minutes up to an hour, depending on the capacity of the device) to save any work and safely shut down the equipment.

NEW QUESTION 131

An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

- A. All updated software must be tested with alt system types and accessories
- B. Extra technician hours must be budgeted during installation of updates
- C. Network utilization will be significantly increased due to the size of CAD files
- D. Large update and installation files will overload the local hard drives.

Answer: C

Explanation:

The IT manager is most likely to be concerned about network utilization being significantly increased due to the size of CAD files. Backing up all CAD files to the software's cloud server can result in a large amount of data being transferred over the network, which can cause network congestion and slow down other network traffic.

NEW QUESTION 136

A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept Which of the following agreements IS MOST likely in use?

- A. DRM
- B. NDA
- C. EULA
- D. MOU

Answer: C

Explanation:

The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

NEW QUESTION 138

A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi When the smartphone is connected to Wi-Fi the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

- A. The smartphone's line was not provisioned with a data plan
- B. The smartphone's SIM card has failed
- C. The smartphone's Bluetooth radio is disabled.
- D. The smartphone has too many applications open

Answer: A

Explanation:

The smartphone's line was not provisioned with a data plan. The user is unable to use any internet-related functions on the smartphone when it is not connected to Wi-Fi because the smartphone's line was not provisioned with a data plan. The user can send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi because these functions do not require an internet connection1

NEW QUESTION 141

A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

- A. MDM
- B. EULA
- C. IRP
- D. AUP

Answer: D

Explanation:

AUP (Acceptable Use Policy) should be updated to reflect this new requirement. The AUP is a document that outlines the acceptable use of technology within an organization. It is a set of rules that employees must follow when using company resources. The AUP should be updated to include a policy on cryptocurrency mining on work desktops

NEW QUESTION 144

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 220-1102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 220-1102 Product From:

<https://www.2passeasy.com/dumps/220-1102/>

Money Back Guarantee

220-1102 Practice Exam Features:

- * 220-1102 Questions and Answers Updated Frequently
- * 220-1102 Practice Questions Verified by Expert Senior Certified Staff
- * 220-1102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 220-1102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year