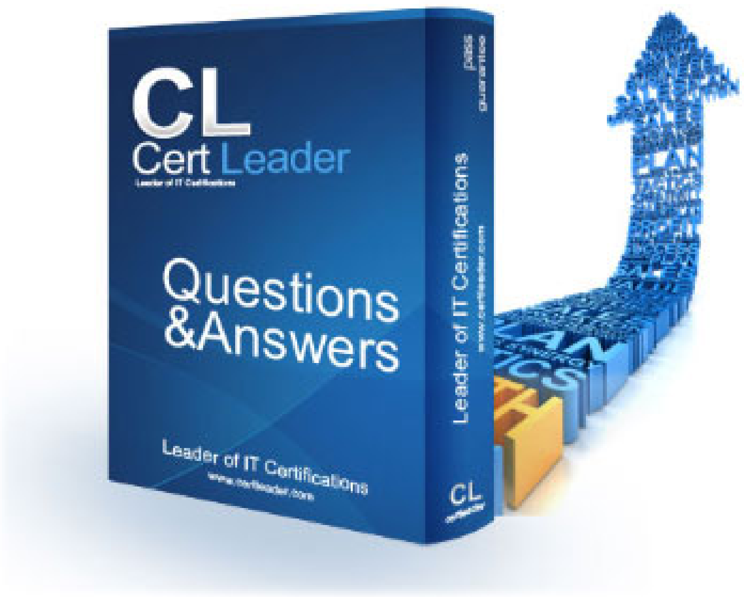
220-1202 Dumps

CompTIA A+ Certification Exam: Core 2

https://www.certleader.com/220-1202-dumps.html



NEW QUESTION 1
Every time a user loads a specific spreadsheet, their computer is temporarily unresponsive. The user also notices that the title bar indicates the application is not responding. Which of the following would a technician most likely inspect?

A. Anti-malware logs
B. Workstation repair options
C. Bandwidth status as reported in the Task Manager
D. File size and related memory utilization

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
If a system becomes unresponsive while opening a specific spreadsheet, the issue is likely tied to the file??s size or the complexity of its content (e.g., embedded formulas, macros, or graphics). High memory utilization caused by the file can lead to temporary freezing or application "Not Responding" messages. Checking the spreadsheet's file size and monitoring system memory in Task Manager will help isolate performance bottlenecks.
* A. Anti-malware logs are important for security troubleshooting but less likely relevant to spreadsheet-related performance issues.
* B. Workstation repair is for system-wide problems and not necessary for a single-file issue.
* C. Bandwidth relates to network usage and wouldn??t impact opening a local file. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application issues.
Study Guide Section: Troubleshooting application slowness and performance using Task Manager and resource monitoring tools
===========================

NEW QUESTION 2
The screen of a previously working computer repeatedly displays an OS Not Found error message when the computer is started. Only a USB drive, a keyboard, and a mouse are plugged into the computer. Which of the following should a technician do first?

A. Run data recovery tools on the disk
B. Partition the disk using the GPT format
C. Check boot options
D. Switch from UEFI to BIOS

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An "OS Not Found" error typically indicates that the computer is attempting to boot from a drive that doesn't contain a valid operating system or bootable partition. The presence of a USB drive might be confusing the boot order. Therefore, the first step a technician should take is to verify and adjust the boot sequence in the system??s firmware (BIOS or UEFI). It's possible that the USB drive is being prioritized over the internal hard drive, which may cause the system to miss the OS entirely.
* A. Running data recovery tools is premature before confirming boot order.
* B. Repartitioning the disk would destroy existing data—this should not be done until confirmed the OS is actually missing.
* D. Switching between UEFI and BIOS (legacy mode) might help in rare cases, but it is not the first step in standard OS boot issue troubleshooting.
Reference:
CompTIA A+ 220-1102 Objective 1.7: Troubleshoot common operating system problems. Study Guide Section: Boot process and boot order configuration.
===========================

NEW QUESTION 3
A technician uses AI to draft a proposal about the benefits of new software. When reading the draft, the technician notices that the draft contains factually incorrect information. Which of the following best describes this scenario?

A. Data privacy
B. Hallucinations
C. Appropriate use
D. Plagiarism

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the context of artificial intelligence, "hallucinations" refer to instances where an AI system generates information that is plausible-sounding but factually incorrect or entirely fabricated. This is a known limitation of large language models, including generative AI tools.
* A. Data privacy refers to the protection of personal or sensitive data, not content accuracy.
* C. Appropriate use relates to ethical and policy-based concerns, not factual correctness.
* D. Plagiarism involves presenting someone else's work as your own — this situation is about accuracy, not ownership.
Reference:
CompTIA A+ 220-1102 Objective 4.4: Identify basic concepts of scripting and automation. Study Guide Section: AI tools and responsible usage — hallucinations and fact-checking outputs
===========================

NEW QUESTION 4
Which of the following describes an attack in which an attacker sets up a rogue AP that tricks users into connecting to the rogue AP instead of the legitimate network?

A. Stalkerware
B. Evil twin
C. Tailgating
D. Shoulder surfing

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An evil twin is a rogue wireless access point set up to mimic a legitimate Wi-Fi network. Unsuspecting users may connect to it, giving attackers the opportunity to intercept traffic, steal credentials, or install malware. The evil twin often uses the same SSID as the real network to fool users.
* A. Stalkerware is spyware installed to track user activity, typically on personal devices.
* C. Tailgating is a physical security breach involving unauthorized entry behind someone with access.
* D. Shoulder surfing involves observing a person entering confidential data, such as PINs or passwords.
Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast social engineering and wireless attacks.
Study Guide Section: Wireless threats — rogue APs and evil twin scenarios
===========================

NEW QUESTION 5
A company wants to use a single operating system for its workstations and servers and avoid licensing fees. Which of the following operating systems would the company most likely select?

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

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Linux is an open-source operating system that is freely available and does not require traditional licensing fees. It is highly versatile and scalable, making it suitable for both workstations and servers. Many enterprise environments use Linux to reduce software costs and benefit from robust server features.
* B. Windows requires per-device or per-user licensing for both workstation and server editions.
* C. macOS is proprietary and limited to Apple hardware with licensing restrictions.
* D. Chrome OS is designed for lightweight devices and lacks server functionality. Reference:
CompTIA A+ 220-1102 Objective 1.8 & 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Open-source operating systems and licensing considerations
===========================

NEW QUESTION 6
Which of the following is used in addition to a password to implement MFA?

A. Sending a code to the user's phone
B. Verifying the user's date of birth
C. Prompting the user to solve a simple math problem
D. Requiring the user to enter a PIN

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) requires at least two different types of authentication factors:
? Something you know (e.g., password or PIN)
? Something you have (e.g., smartphone or hardware token)
? Something you are (e.g., fingerprint or facial recognition)
Option A, sending a code to the user??s phone, is an example of "something you have" — a physical device that receives a one-time passcode. Combined with a password, this forms a proper MFA implementation.
* B. Date of birth is another knowledge-based factor (like a password), not a second factor type.
* C. Solving a math problem is not a recognized authentication factor.
* D. A PIN is also "something you know" and does not count as a distinct MFA factor when paired with a password.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Authentication factors — password, biometrics, tokens, MFA
===========================

NEW QUESTION 7
A technician is setting up a Windows server to allow remote desktop connections for multiple users. Which of the following should the technician configure on the workstation?

A. Firewall
B. Computer Management
C. User Accounts
D. Ease of Access

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To allow Remote Desktop Protocol (RDP) access, the firewall must be configured to allow inbound connections on TCP port 3389. If the Windows Firewall blocks RDP, users will not be able to connect remotely even if the feature is enabled in system settings.
* B. Computer Management allows configuration of services and local users, but not network access.
* C. User Accounts is for account setup and control, but enabling remote access requires firewall configuration.
* D. Ease of Access is unrelated to remote connectivity—it??s for accessibility features. Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and firewall settings.
Study Guide Section: Enabling and securing RDP via firewall settings
==========================

NEW QUESTION 8
A technician installs VPN client software that has a software bug from the vendor. After the vendor releases an update to the software, the technician attempts to reinstall the software but keeps getting an error message that the network adapter for the VPN already exists. Which of the following should the technician do next to mitigate this issue?

A. Run the latest OS security updates.
B. Map the network adapter to the new software.
C. Update the network adapter's firmware.
D. Delete hidden network adapters.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
VPN clients often create virtual network adapters. If the software wasn't uninstalled properly or crashed during install, leftover (often hidden) virtual adapters can prevent reinstallation. The proper solution is to delete hidden network adapters using Device Manager (with ??Show hidden devices?? enabled).
* A. OS updates won??t fix a leftover driver or adapter issue.
* B. Mapping an adapter to the software is not a standard or viable solution.
* C. Firmware updates apply to physical adapters, not virtual VPN adapters. Reference:
CompTIA A+ 220-1102 Objective 3.1: Troubleshoot common Windows OS and network issues.
Study Guide Section: Troubleshooting network adapter conflicts and VPN client errors

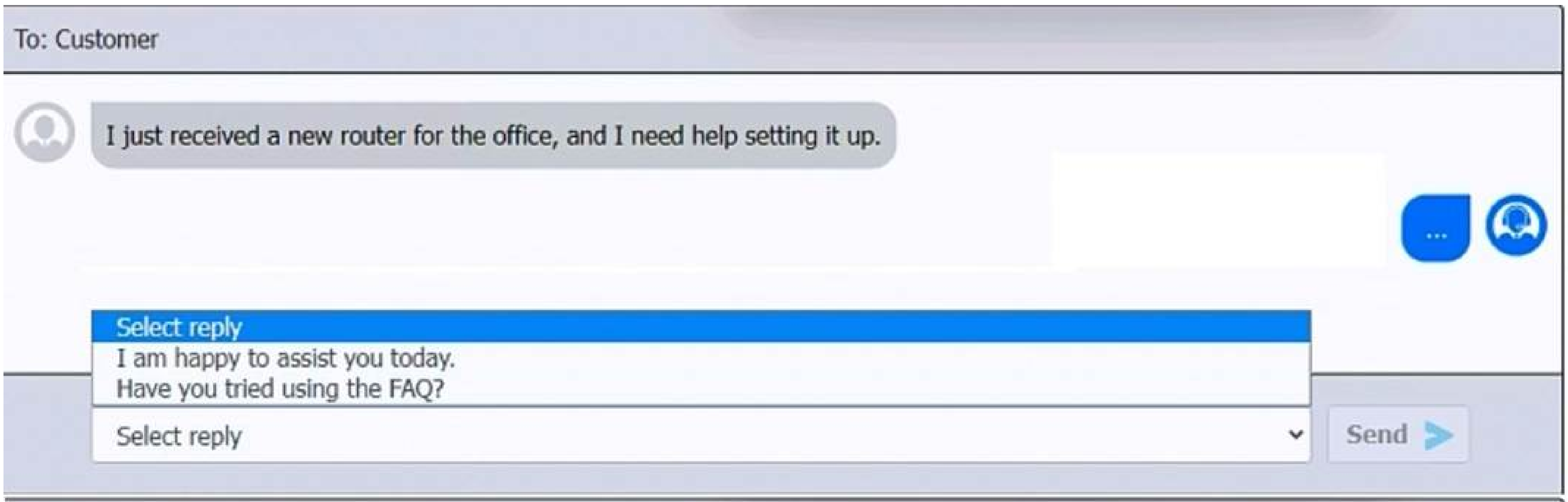
NEW QUESTION 9
A help desk team was alerted that a company-owned cell phone has an unrecognized password-cracking application. Which of the following should the help desk team do to prevent further unauthorized installations from occurring?

A. Configure Group Policy.
B. Implement PAM.
C. Install anti-malware software.
D. Deploy MDM.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Mobile Device Management (MDM) is used to control, monitor, and enforce policies on mobile devices. It allows IT teams to restrict app installations, push approved apps, and monitor device compliance. Deploying MDM would prevent unauthorized applications, such as password crackers, from being installed on company-managed devices.
* A. Group Policy is for managing Windows environments and not applicable to smartphones.
* B. PAM (Privileged Access Management) controls administrative access, not app installation.
* C. Anti-malware can help detect malicious apps but doesn??t prevent their installation proactively.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.
Study Guide Section: Mobile Device Management (MDM) capabilities — app control, security enforcement

NEW QUESTION 10
SIMULATION
You have been contacted through the help desk chat application. A user is setting up a replacement SOHO router. Assist the user with setting up the router.
INSTRUCTIONS
Select the most appropriate statement for each response. Click the send button after each response to continue the chat.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



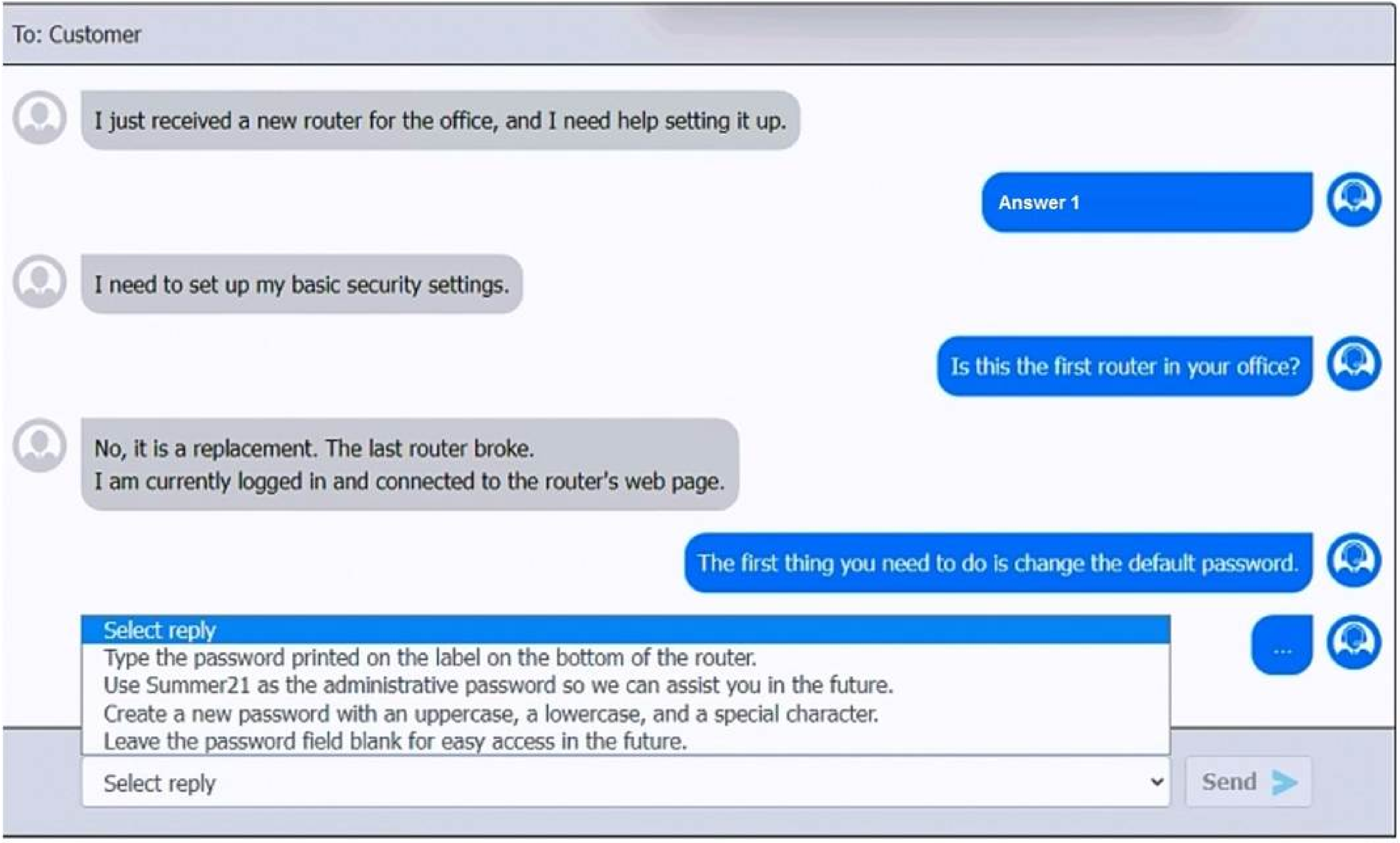
To: Customer

I just received a new router for the office, and I need help setting it up.

...

Select reply
I am happy to assist you today.
Have you tried using the FAQ?

Select reply



To: Customer

I just received a new router for the office, and I need help setting it up.

Answer 1

I need to set up my basic security settings.

Is this the first router in your office?

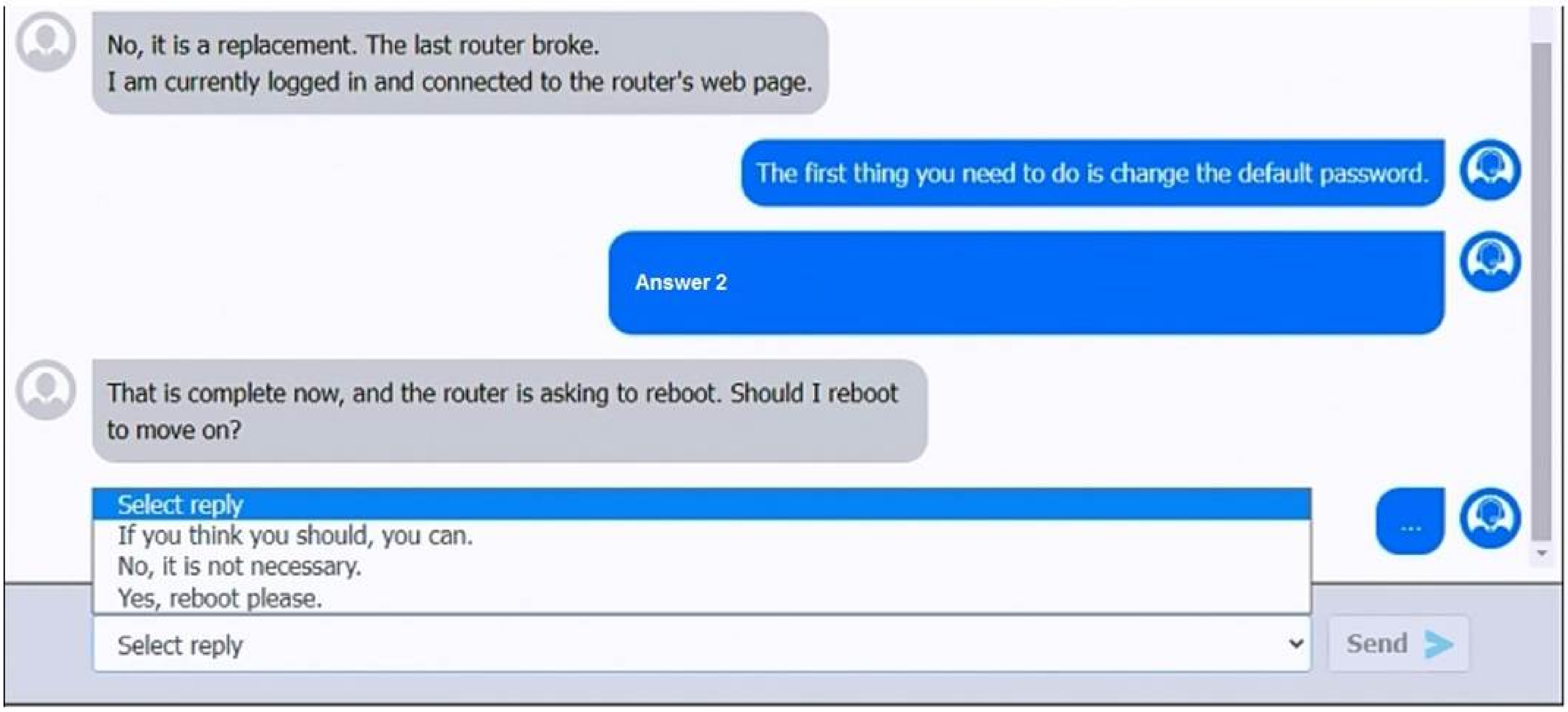
No, it is a replacement. The last router broke.
I am currently logged in and connected to the router's web page.

The first thing you need to do is change the default password.

...

Select reply
Type the password printed on the label on the bottom of the router.
Use Summer21 as the administrative password so we can assist you in the future.
Create a new password with an uppercase, a lowercase, and a special character.
Leave the password field blank for easy access in the future.

Select reply



No, it is a replacement. The last router broke.
I am currently logged in and connected to the router's web page.

The first thing you need to do is change the default password.

Answer 2

That is complete now, and the router is asking to reboot. Should I reboot to move on?

...

Select reply
If you think you should, you can.
No, it is not necessary.
Yes, reboot please.

Select reply

A. Mastered
B. Not Mastered

Answer: A

Explanation:
First Chat Response:When the user mentions setting up a new router, the best initial response to maintain a helpful and professional tone is:
>Select reply:"I am happy to assist you today."
Second Chat Response:When the user states that they need to set up basic security settings:
>Select reply:"Is this the first router in your office?"
Third Chat Response:After learning it's a replacement router and the user is logged into the router's web page:
>Select reply:"The first thing you need to do is change the default password."
Fourth Chat Response:For the response about password settings:
>Select reply:"Create a new password with an uppercase, a lowercase, and a special character."
Fifth Chat Response:When the router prompts to reboot:
>Select reply:"Yes, reboot please."
Study Guide Reference: The CompTIA A+ Core 2 guide highlights the importance of changing default credentials and using strong password policies, particularly in SOHO environments where routers are often targeted.

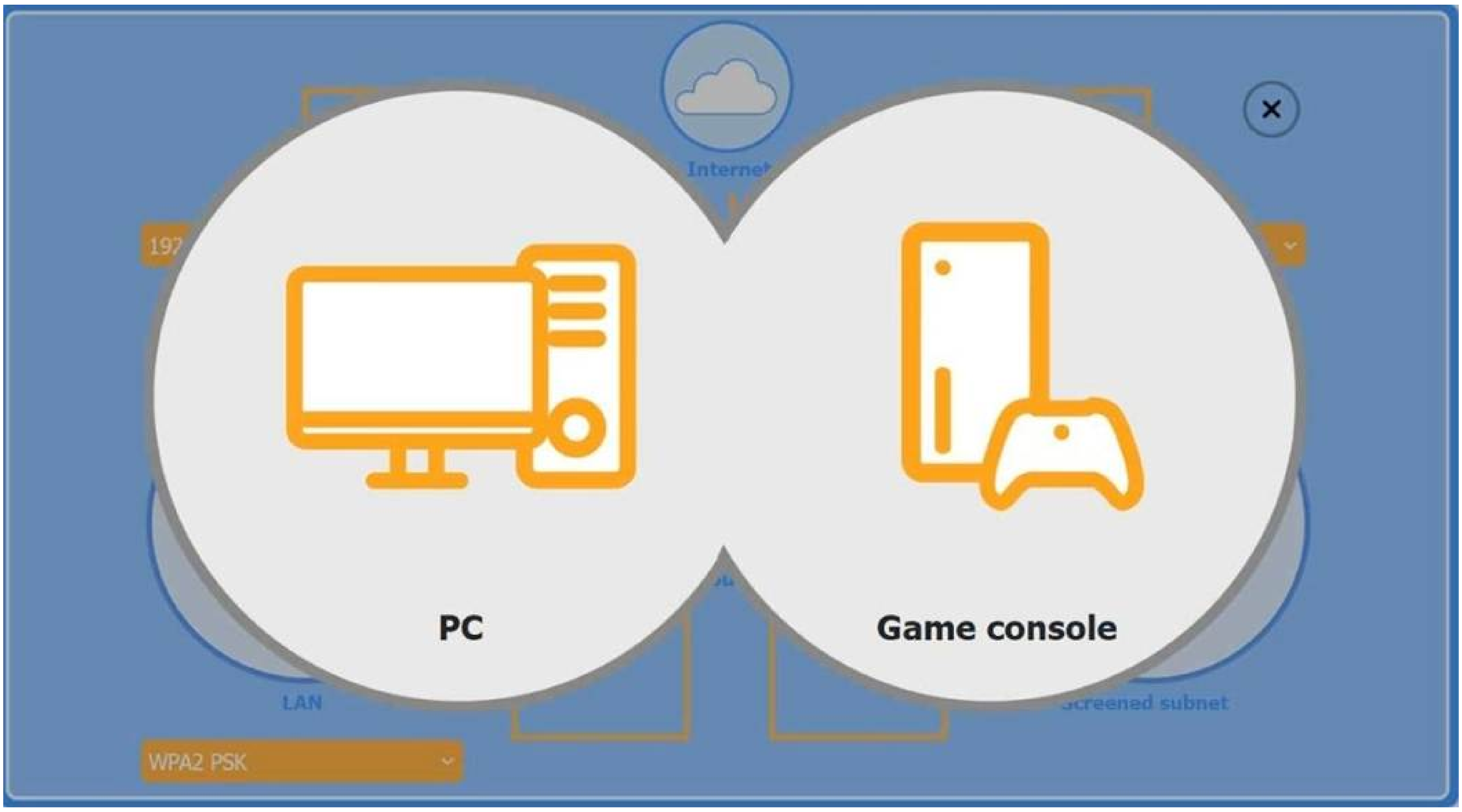
NEW QUESTION 10
A user is experiencing issues with outdated images while browsing websites. Which of the following settings should a technician use to correct this issue?

A. Administrative Tools
B. Windows Defender Firewall
C. Internet Options
D. Ease of Access

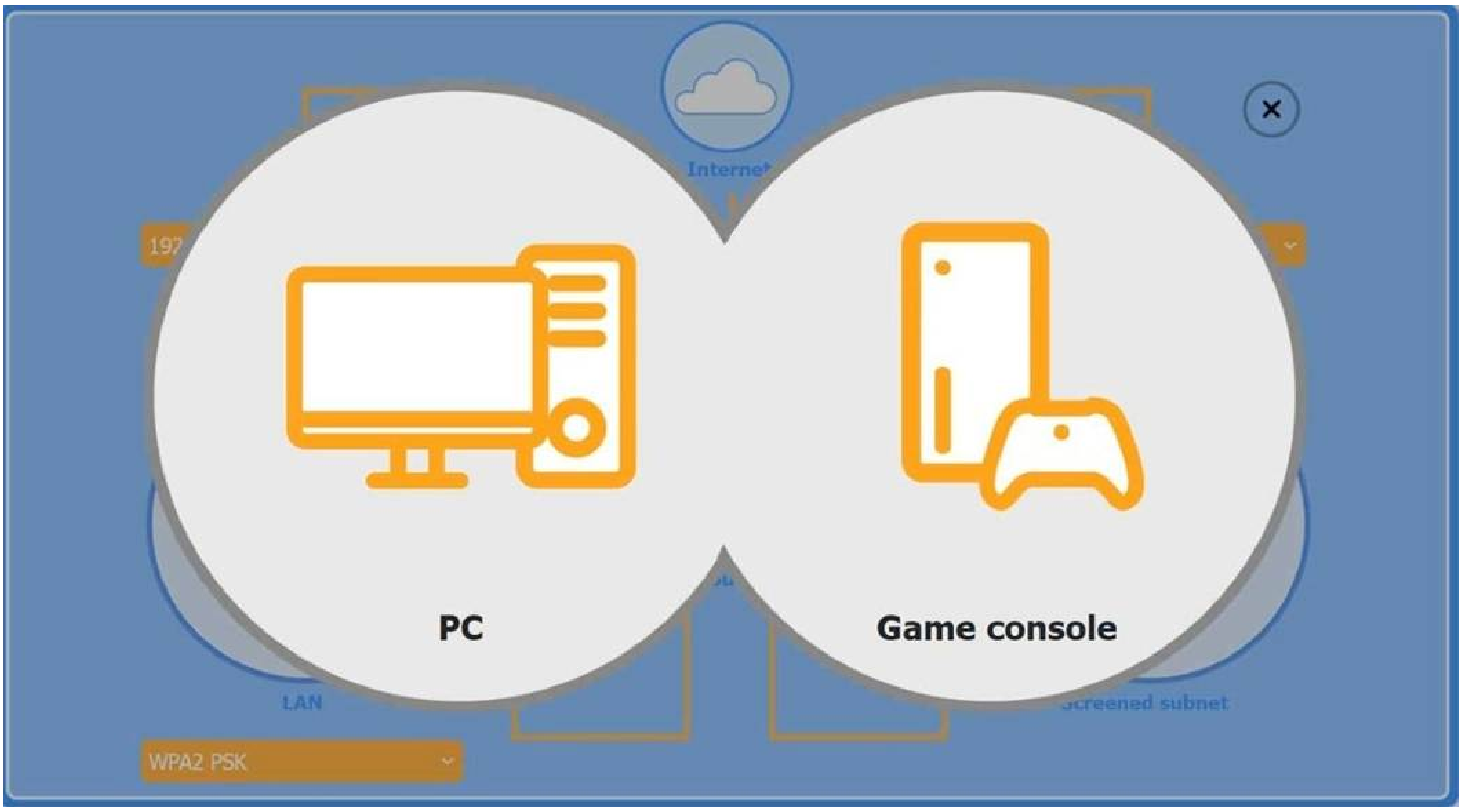
Answer: C

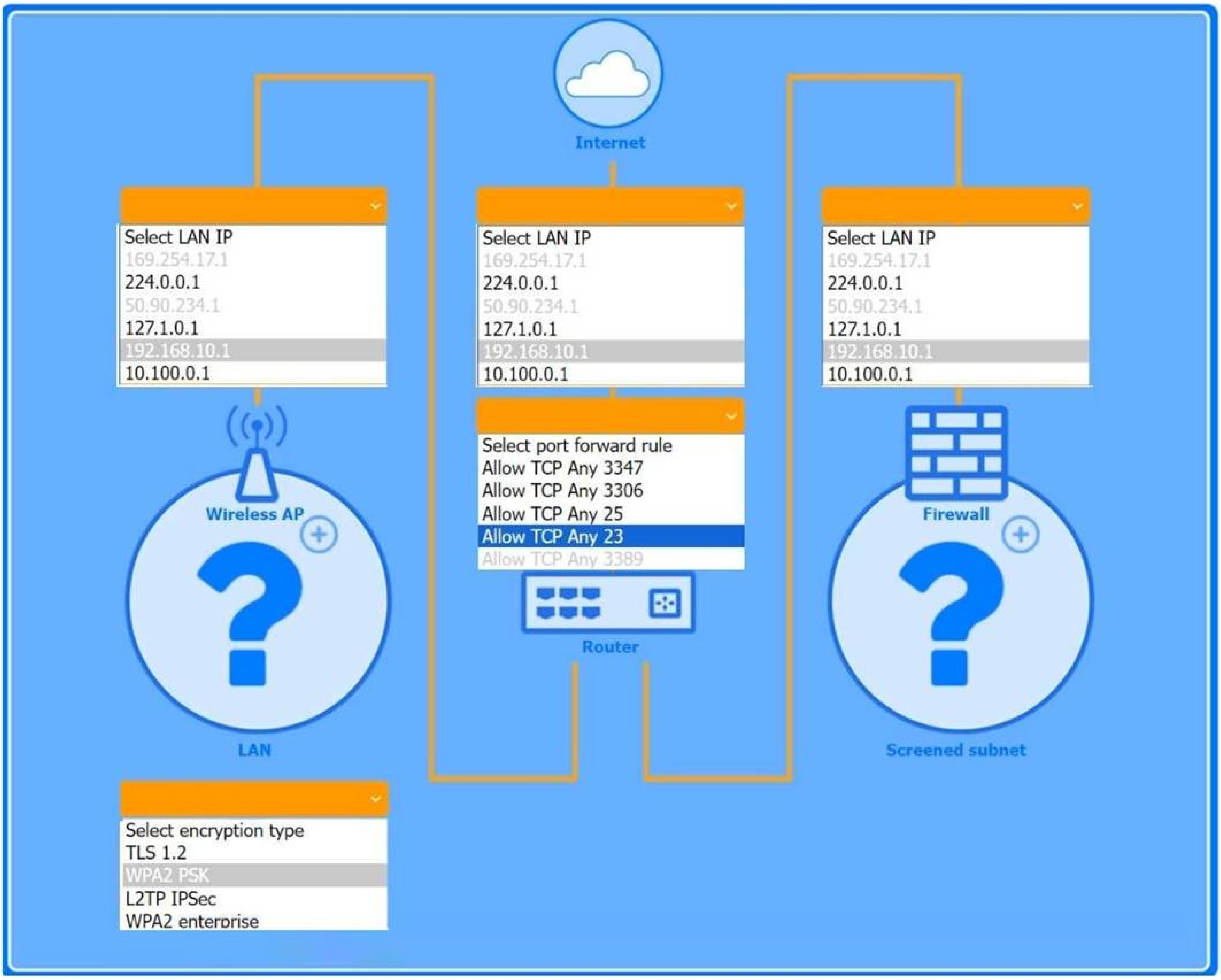
Explanation:
Comprehensive and Detailed Explanation From Exact Extract: Outdated images and website data often result from cached files in the browser. The Internet Options panel in Windows (specifically under the General tab) allows users to clear browsing history, including cached images and files, which forces the browser to load the most current versions of web content.
* A. Administrative Tools is used for advanced system management, not browser settings.
* B. Windows Defender Firewall controls network traffic and security rules, not caching.
* D. Ease of Access provides accessibility features for users with disabilities — unrelated to web browsing issues.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.
Study Guide Section: Internet Options and browser cache clearing for display issues

NEW QUESTION 11
SIMULATION
You are configuring a home network for a customer. The customer has requested the ability to access a Windows PC remotely, and needs all chat and optional functions to work in their game console.
INSTRUCTIONS
Use the drop-down menus to complete the network configuration for the customer. Each option may only be used once, and not all options will be used.
Then, click the + sign to place each device in its appropriate location.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Wireless AP LAN



Firewall Screened Subnet





A. Mastered
B. Not Mastered

Answer: A

Explanation:
The completed configuration:
* 1. Wireless AP (LAN side) 1. LAN IP: 192.168.10.1
* 2. Encryption: WPA2 PSK
* 2. Router (port-forward rule)
* 1. Allow TCP Any 3389
This forwards inbound RDP traffic (TCP/3389) from the Internet to the Windows PC, enabling Remote Desktop access.
* 3. Firewall (screened subnet side) 1. LAN IP: 10.100.0.1
* 4. Device placement
* 1. PC: place behind the router (where the port-forward rule points).
* 2. Game console: place on the Wireless AP (so it can use chat and extra services over WPA2 PSK).
* 3. Firewall: place in front of the screened subnet (with its 10.100.0.1 IP facing that subnet).
? The Windows PC is placed in the screened subnet (behind the firewall) for enhanced security. Remote access to this PC requires port forwarding of TCP port 3389 (RDP), which is correctly configured through the router.
? The Game Console is placed on the Wireless AP LAN, using WPA2 PSK for a secure wireless connection. Game consoles typically use peer-to-peer chat and online services that require open access without firewall restrictions, which is why the console is not placed behind the firewall.
CompTIA A+ 220-1102 Reference Points:
? Objective 3.4: Given a scenario, implement best practices associated with data and device security.
? Objective 2.4: Given a scenario, use appropriate tools to support and configure network settings.
? Study Guide Reference: CompTIA A+ Core 2 guides recommend using screened subnets (a type of DMZ) for systems needing controlled external access, such as remote desktops, while placing gaming and media devices on less restricted networks for full functionality.

NEW QUESTION 16
A technician is troubleshooting an issue in which a service runs momentarily and stops at certain points in the process. The technician needs to determine the root cause of this issue. Which of the following tools should the technician use?

A. Event Viewer
B. Task Manager
C. Internet Options
D. Process Explorer

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the best tool to analyze the root cause of service failures in Windows. It provides detailed logs from system processes, including errors, warnings, and crash reports related to services and applications. When a service starts and stops unexpectedly, Event Viewer will often record the cause, such as dependency failures or access violations.
* B. Task Manager shows active processes but doesn't retain logs or causes of failure.
* C. Internet Options is used for configuring browser settings, not troubleshooting services.
* D. Process Explorer is powerful but more suited for live monitoring and detailed process trees, not post-failure log analysis.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Log file analysis using Event Viewer
==========================

NEW QUESTION 21
Which of the following filesystem types does the Linux OS use?

A. exFAT
B. APFS
C. ext4
D. NTFS

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The ext4 (Fourth Extended Filesystem) is the most widely used default filesystem in modern Linux distributions. It is designed for high performance, scalability, and reliability, and is supported by all mainstream Linux kernels.
* A. exFAT is used for cross-platform external drives, not native Linux systems.
* B. APFS is Apple's proprietary filesystem for macOS and iOS.
* D. NTFS is the default filesystem for Windows, not Linux. Reference:
CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Filesystem types in Linux — ext3, ext4, and their characteristics

NEW QUESTION 26
Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?

A. Using gpupdate
B. Image deployment
C. Clean install
D. In-place upgrade

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

An in-place upgrade is the fastest and most efficient way to upgrade from Windows 10 to Windows 11 while keeping all user data, applications, and settings intact. This method is often used when the hardware meets Windows 11 requirements and no system reconfiguration is necessary.
* A. gpupdate is used to refresh Group Policy settings — unrelated to OS upgrades.
* B. Image deployment typically replaces the current OS and may not retain user data unless specifically customized.
* C. A clean install requires formatting the drive and starting fresh, which removes all data. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: In-place upgrade vs. clean install methods
===========================

NEW QUESTION 31
A user receives a new personal computer but is unable to run an application. An error displays saying that .NET Framework 3.5 is required and not found. Which of the following actions is the best way to resolve this issue?

A. Resolve the dependency through the 'Turn Windows features on or off' menu.
B. Download the dependency via a third-party repository.
C. Ignore the dependency and install the latest version 4 instead.
D. Forward the trouble ticket to the SOC team because the issue poses a great security risk.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
NET Framework versions are often required for applications to run. If an older app requires
.NET Framework 3.5, it must be explicitly installed as it is not included by default in newer versions of Windows. The best method to do this safely is through the built-in "Turn Windows features on or off" utility, which downloads and installs it via official Microsoft services.
* B. Using third-party repositories is unsafe and not recommended.
* C. Installing .NET 4 does not include 3.5; versions are not fully backward compatible.
* D. The issue is technical, not a security incident for the SOC team. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Managing application dependencies (e.g., .NET Framework, Java)
===========================

NEW QUESTION 33
Technicians are failing to document user contact information, device asset tags, and a clear description of each issue in the ticketing system. Which of the following should a help desk management team implement for technicians to use on every call?

A. Service-level agreements
B. Call categories
C. Standard operating procedures
D. Knowledge base articles

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Standard Operating Procedures (SOPs) define the mandatory steps and expectations technicians must follow during support calls. This includes documentation standards such as logging user info, asset details, and issue descriptions in the ticketing system. Implementing SOPs ensures consistency and accountability.
* A. SLAs define response/resolution times but not documentation practices.
* B. Call categories organize types of issues but don't guide technician actions.
* D. Knowledge base articles provide solutions to known problems but don't ensure proper ticket documentation.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize best practices associated with types of documentation and support systems information.
Study Guide Section: Documentation practices, SOPs, ticketing protocols
===========================

NEW QUESTION 37
Which of the following is the best way to distribute custom images to 800 devices that include four device vendor classes with two types of user groups?

A. Use xcopy to clone the hard drives from one to another
B. Use robocopy to move the files to each device
C. Use a local image deployment tool for each device
D. Use a network-based remote installation tool

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In enterprise environments, network-based deployment solutions (such as Windows Deployment Services or SCCM) allow administrators to push images across the network to hundreds of devices efficiently. These tools support hardware-specific drivers (for different vendor classes) and can accommodate user-group configurations using task sequences or answer files.
A and B (xcopy and robocopy) are file-level tools and not designed for full OS image deployment.
* C. Using local tools per device is inefficient for large-scale rollouts (800 devices).
* D. Network-based deployment is the industry standard for this scale. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods (including PXE boot, image deployment)
===========================

NEW QUESTION 41
A user has been adding data to the same spreadsheet for several years. After adding a significant amount of data, they are now unable to open the file. Which of

the following should a technician do to resolve the issue?

A. Revert the spreadsheet to the last restore point.
B. Increase the amount of RAM.
C. Defragment the storage drive.
D. Upgrade the network connection speed.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
When a spreadsheet becomes very large, opening and processing it requires more memory (RAM). If the system doesn't have sufficient memory, it may fail to load the file properly. Upgrading or increasing the available RAM can resolve performance and loading issues with very large files.
* A. Restore points roll back system settings, not individual file content.
* C. Defragmentation optimizes disk performance but won??t help with memory issues.
* D. Network speed has no effect if the file is stored and opened locally. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application and performance issues.
Study Guide Section: Troubleshooting large-file performance and system resource limitations
==========================

NEW QUESTION 45
A technician is preparing to replace the batteries in a rack-mounted UPS system. After ensuring the power is turned off and the batteries are fully discharged, the technician needs to remove the battery modules from the bottom of the rack. Which of the following steps should the technician take?

A. Ensure the fire suppression system is ready to be activated.
B. Use appropriate lifting techniques and guidelines.
C. Place the removed batteries in an antistatic bag.
D. Wear a face mask to filter out any harmful fumes.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
UPS batteries are heavy and often located at the bottom of racks to maintain balance. Safe removal requires the use of correct lifting techniques to avoid injury. OSHA and workplace safety standards emphasize ergonomic handling when dealing with heavy equipment.
* A. Fire suppression readiness is important for fire safety but not specifically relevant to battery removal.
* C. Antistatic bags are for electronic components, not heavy battery modules.
* D. A face mask is not generally necessary unless there is a chemical leak, which is not indicated here.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts
and procedures.
Study Guide Section: Safe handling procedures — lifting techniques, battery handling
==========================

NEW QUESTION 50
An organization is experiencing an increased number of issues. A technician notices applications that are not installed by default. Users are reporting an increased number of system prompts for software licensing. Which of the following would the security team most likely do to remediate the root cause?

A. Deploy an internal PKI to filter encrypted web traffic.
B. Remove users from the local admin group.
C. Implement stronger controls to block suspicious websites.
D. Enable stricter UAC settings on Windows.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
If unauthorized or non-standard applications are appearing on systems and users are receiving licensing prompts, it??s likely users are installing software themselves. Removing users from the local administrators group will prevent them from installing software without approval and reduce the likelihood of introducing unapproved or malicious programs.
* A. Deploying a PKI helps with secure communications but doesn??t address user software installation rights.
* C. Blocking suspicious websites is helpful but doesn??t prevent local installations.
* D. Stricter UAC may add prompts but can still be bypassed by admin users. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast access control methods and user privilege settings.
Study Guide Section: Principle of least privilege and managing local admin rights
==========================

NEW QUESTION 52
A technician needs to install an operating system on a large number of workstations. Which of the following is the fastest method?

A. Physical media
B. Mountable ISO
C. Manual installation
D. Image deployment

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Image deployment is the fastest and most efficient method for installing operating systems on multiple machines. It involves creating a pre-configured image of an

OS and deploying it across systems using tools like Windows Deployment Services (WDS) or third-party imaging solutions. This method saves time and ensures consistency across all devices.
* A. Physical media is slow and not scalable.
* B. Mountable ISOs are useful but still require manual installation.
* C. Manual installation is time-consuming and not suitable for large-scale deployment. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods — image deployment, automation

NEW QUESTION 55
A customer wants to be able to work from home but does not want to be responsible for bringingcompany equipment back and forth. Which of the following would allow the user to remotely access and use a Windows PC at the main office? (Choose two.)

A. SPICE
B. SSH
C. RDP
D. VPN
E. RMM
F. WinRM

Answer: CD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: To work remotely without physically transporting a workstation, the user needs:
? C. RDP (Remote Desktop Protocol): Allows graphical remote access to a Windows
PC at the office.
? D. VPN (Virtual Private Network): Establishes a secure tunnel to access the corporate network remotely, making the internal PC reachable.
* A. SPICE is used in virtual machine environments and is not typically used for end-user remote desktop access.
* B. SSH is a text-based remote access tool used mostly for Linux systems.
* E. RMM (Remote Monitoring and Management) is used by IT administrators for support — not end-user remote access.
* F. WinRM is used for Windows remote management via PowerShell, not for full desktop access.
Reference:
CompTIA A+ 220-1102 Objectives 2.2 & 4.4: Compare and contrast security tools and remote access methods.
Study Guide Section: Remote access tools — RDP and VPN for secure remote work

NEW QUESTION 56
A user reports getting a BSOD (Blue Screen of Death) error on their computer at least twice a day. Which of the following should the technician use to determine the cause?

A. Event Viewer
B. Performance Monitor
C. System Information
D. Device Manager

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the primary tool used to investigate system-level errors and logs, including BSODs. When a BSOD occurs, Windows logs the error codes and associated system behavior under ??System?? logs in Event Viewer. This allows the technician to review crash events, identify error codes (e.g., STOP codes), and pinpoint hardware or driver issues.
* B. Performance Monitor is used for real-time performance tracking and trend analysis, not crash logs.
* C. System Information displays system specs but not crash logs or events.
* D. Device Manager shows device status and driver issues but doesn??t retain error logs related to BSODs.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Troubleshooting BSODs using Event Viewer and system logs
==========================

NEW QUESTION 60
A user reports some single sign-on errors to a help desk technician. Currently, the user is able tosign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?

A. Reenroll the user's mobile device to be used as an MFA token
B. Use a private browsing window to avoid local session conflicts
C. Bypass single sign-on by directly authenticating to the application
D. Reset the device being used to factory defaults

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
SSO issues are often related to cached session data, cookies, or browser artifacts. The fact that the user can access the company portal but not one specific SaaS tool suggests a session or token problem. Using a private/incognito browsing window allows a clean session to be initiated, which often resolves SSO conflicts.
* A. Reenrolling MFA is not related unless access issues stem from failed multifactor authentication.
* C. Bypassing SSO may not be possible depending on the SaaS tool and company policies.
* D. Factory resetting a device is a last resort and unnecessary in this case. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Troubleshooting login and authentication issues, especially with SSO services.
==========================

NEW QUESTION 65

......