Testpassport Q&A

La meilleure qualité le meilleur service

Exam : ChromeOS Administrator

Title : Professional ChromeOS Administrator

Version : DEMO

1.An admin wants to use a custom extension to install a client certificate on a ChromeOS device so that it can connect to the corporate WI-FI.
Which step Is necessary to accomplish this?
A. Install on the device via guest mode
B. Distribute through the Chrome Web Store
C. Force-install to the device
D. Encode the certificate in DER-encoded format
Answer: C
Explanation:
To install a client certificate on a ChromeOS device for corporate Wi-Fi connectivity, it's necessary to force-install the custom extension containing the certificate. This ensures the extension is installed and activated on the device, enabling it to use the certificate for authentication. Here's how it works: Custom Extension: The admin creates or obtains a custom extension that includes the client certificate.
Force-Installation: Using the Google Admin console, the admin configures a policy to force-install the extension on ChromeOS devices within the organization.
Device Activation: Once the device receives the policy, the extension is automatically installed and activated, even if the user doesn't manually add it.
Wi-Fi Authentication: The installed extension allows the device to use the client certificate for authentication when connecting to the corporate Wi-Fi network.
Option A is incorrect because guest mode installations are not persistent and won't apply the certificate to the device's Wi-Fi settings.
Option B is incorrect because distributing through the Chrome Web Store is not necessary for a custom extension intended for internal use.
Option D is incorrect because while the certificate encoding is important, it's not the primary step for enabling Wi-Fi authentication.
Reference: About ChromeOS device management:
https://support.google.com/chrome/a/answer/1289314?hl=en pen_spark

2.An organization was recently hacked through an admin's choice of an operating system. Leadership decides to move to Chromebooks for their security.
While the organization waits for Chromebooks to be delivered, what will allow them to continue using their existing devices securely?
A. ChromeOS Readiness Guide
B. ChromeOS Managed Browser
C. ChromeOS Bytes
D. ChromeOS Flex
Answer: D
Explanation:
ChromeOS Flex allows the organization to repurpose existing devices by installing a lightweight version of ChromeOS on them. This provides a secure and familiar environment while they await the delivery of new Chromebooks.
Here’s why it’s the best choice:
Security: ChromeOS Flex inherits the security features of ChromeOS, such as sandboxing, verified boot, and automatic updates, mitigating the risks associated with the previous operating system. Quick

Deployment: ChromeOS Flex can be easily installed on existing hardware using a USB drive, minimizing downtime and allowing employees to continue working.
Familiar Interface: The user interface of ChromeOS Flex is similar to ChromeOS, ensuring a smooth transition for employees.
Option A is incorrect because the ChromeOS Readiness Guide is a resource for planning migration, not an immediate security solution.
Option B is incorrect because while ChromeOS Managed Browser enhances security within a browser, it doesn't address vulnerabilities in the underlying operating system.
Option C is incorrect because ChromeOS Bytes is a blog, not a software solution.
Reference: ChromeOS Flex: https://chromeenterprise.google/os/chromeosflex/

3.Which site isolation policy will enable site isolation for your entire organization?
A. SitePerProcess
B. IsolateOfigins
C. IsolatePerProcess
D. SiteOrigins
Answer: A
Explanation:
The SitePerProcess policy enables site isolation for the entire organization. This means that each website opened in Chrome will run in its own dedicated process, improving security and stability by isolating potential vulnerabilities and preventing one compromised site from affecting others.
Option B (IsolateOrigins) and Option D (SiteOrigins) are not valid policy names.
Option C (IsolatePerProcess) is close but not the exact name of the policy.
Reference: Site Isolation in Google Chrome: https://www.chromium.org/Home/chromium-security/site-isolation/

4.What is a feature of Verified Boot?
A. Makes sure that the firmware and OS have not been tampered with
B. Protects anonymous guests from using the device
C. Eliminates the need for strict policy controls
D. Prevents the user from accessing unauthorized websites
Answer: A
Explanation:
Verified Boot is a security feature in ChromeOS that checks the integrity of the system during startup. It verifies that the firmware (low-level software) and the operating system haven't been modified or corrupted by unauthorized sources. If any tampering is detected, Verified Boot can initiate recovery processes to restore the system to a known good state.
Option B is incorrect because Verified Boot doesn't directly manage guest access.
Option C is incorrect because Verified Boot is a security layer that complements, not replaces, policy controls.
Option D is incorrect because website access control is handled by other mechanisms like web filtering or content restrictions.
Reference: https://www.chromium.org/chromium-os/chromiumos-design-docs/verified-boot/

5.You are using a third-party service for SSO. Users are confused when signing onto a Chrome device because they are asked for Google account details before being redirected to the sign-In screen for your SSO provider.
Which setting must be changed so managed devices open the SSO provider login page by default?
A. SAML single sign-on login frequency
B. SAML single sign-on password synchronization flows
C. Single sign-on cookie behavior
D. Single sign-on IdP redirection
Answer: D
Explanation:
The Single sign-on IdP redirection setting controls whether managed devices directly open the login page of the third-party SSO provider (Identity Provider) or first prompt for Google account credentials. By enabling this setting, you streamline the login process for users and eliminate the confusion caused by the extra Google account prompt.
Option A is incorrect because it controls the frequency of re-authentication for SAML SSO, not the initial login page.
Option B is incorrect because it relates to password synchronization between Google and the IdP, not the login page redirection.
Option C is incorrect because it deals with how cookies are handled for SSO, not the login page redirection.