

How Pass4sureCert ChromeOS-Administrator Practice Questions Can Help You Pass the Exam



BONUS!!! Download part of Pass4sureCert ChromeOS-Administrator dumps for free: https://drive.google.com/open?id=1Ww309TtROxhtxyYnCHpd8JfCg_bcRg7Q

Our online resources and events enable you to focus on learning just what you want on your timeframe. You get access to every ChromeOS-Administrator exams files and there continuously update our ChromeOS-Administrator Study Materials; these exam updates are supplied free of charge to our valued customers. Get the best ChromeOS-Administrator exam Training; as you study from our exam-files.

Google ChromeOS-Administrator Exam Syllabus Topics:

Topic	Details
Topic 1	• Configure ChromeOS policies: This topic discusses understanding and configuring ChromeOS policies.
Topic 2	• Understand ChromeOS tenets: It discusses ChromeOS best practices and customers on chromeOS tenets.
Topic 3	• Identity Management: The primary focus of the topic identity management is on identity features.
Topic 4	• Understand ChromeOS security processes: It focuses on deploying certificates and uChromeOS policies.
Topic 5	• Perform actions from the Admin console: This topic delves into troubleshooting customer concerns, setting up a trial, pushing applications, and performing device actions from the Admin console.

>> Exam ChromeOS-Administrator Details <<

Excellent Exam ChromeOS-Administrator Details by Pass4sureCert

Overall, we can say that with the Professional ChromeOS Administrator Exam (ChromeOS-Administrator) exam you can gain a competitive edge in your job search and advance your career in the tech industry. However, to pass the Google ChromeOS-Administrator Exam you have to prepare well. For the quick Google ChromeOS-Administrator exam preparation the ChromeOS-Administrator Questions is the right choice.

Google Professional ChromeOS Administrator Exam Sample Questions (Q39-Q44):

NEW QUESTION # 39

How should you use Chrome Remote Desktop from the Google Admin console to connect a user?

- A. Find the device and click remote desktop
- B. Find the user account and click remote desktop
- C. Open Chrome Remote Desktop and type the device serial number
- D. Open Chrome Remote Desktop and type the user's username

Answer: A

Explanation:

To remotely access a user's ChromeOS device through the Admin console, you must find the specific device and click on the remote desktop option. This approach ensures that you are connecting to the correct managed device associated with the user.

Verified Answer from Official Source:

The correct answer is verified from the Google Admin Console Remote Access Guide, which details the procedure to initiate a remote session.

"To access a ChromeOS device remotely, navigate to Devices > Chrome > Devices in the Admin console, find the specific device, and click 'Remote Desktop'." This method helps ensure accurate device management and support without needing personal user credentials or serial numbers.

Objectives:

- * Provide remote assistance efficiently.
- * Use the Admin console for remote device management.

NEW QUESTION # 40

You have been tasked to deploy shared devices using Managed Guest Sessions. Your IT policy requires blocking access to "google.com" at the parent organization. How would you prevent users from accessing "google.com" for all Managed Guest Sessions at the parent organization?

- A. Add "google.com" to "the list of blocked URLs"
- B. Add "google.com" to "disallowed URLs in content settings"
- C. Add "google.com" to "the blocked URL exceptions"
- D. Add "google.com" to "allow insecure content on these sites"

Answer: A

Explanation:

To block access to a specific website across all managed guest sessions, you need to add the site to the "list of blocked URLs". This ensures that regardless of the session type, users cannot access the specified site.

Verified Answer from Official Source:

The correct answer is verified from the Google ChromeOS Managed Guest Session Guide, which explains that adding URLs to the blocked list restricts access across all sessions.

"To enforce web filtering policies during Managed Guest Sessions, add the URL to the blocked list in the Admin console under User & Browser Settings." By configuring the blocked URL list, you enforce consistent access policies even when devices are used in guest mode.

Objectives:

- * Implement web filtering for Managed Guest Sessions.
- * Enforce consistent security policies across sessions.

NEW QUESTION # 41

You are enrolling several devices to send to a remote location. How can you ensure that these devices will automatically connect to the wireless network at the remote location when powered on for the first time?

- A. During the enrollment process add the wireless credentials manually to each device in the Admin console ensuring that they are applied to ChromeOS devices By User
- B. Use the Google Zero-Touch Enrollment (ZTE) process and generate the provisioning token by clicking on the 'Enroll device' button in the Admin console "Devices" page
- C. Add the wireless network credentials to the "Networks" section in the Admin console ensuring that they are applied to the ChromeOS devices By Device
- D. Add the wireless network credentials to the "Networks" section in the Admin console ensuring that they are applied to the ChromeOS devices By User

Answer: C

Explanation:

To ensure ChromeOS devices automatically connect to a specific wireless network upon initial power-on at a remote location, follow these steps in the Google Admin console:

- * Navigate to Device Management > Chrome Management > Networks.
- * Add the Wi-Fi network credentials (SSID and password) to the list of networks.
- * Set the network configuration to apply By Device. This ensures that the credentials are pushed to the device itself, not tied to a specific user.

When the devices are powered on at the remote location, they will automatically detect and connect to the configured Wi-Fi network without requiring any manual intervention from the user.

Option B (Zero-Touch Enrollment) simplifies the initial setup process but doesn't automatically configure Wi-Fi.

Options C and D are incorrect because applying network settings by user won't ensure automatic connection on first boot before any user logs in.

NEW QUESTION # 42

You need to create a recovery image on a USB stick. Which two steps should you take?
(Choose 2 answers)

- A. Go to Device Settings.
- **B. Go to Chrome Web Store on a Chrome device**
- C. Go to Google Play store
- **D. Install Chrome Recovery Utility and download the image for the correct device model to a USB stick.**
- E. Go to google.com/chromebooks

Answer: B,D

Explanation:

Creating a recovery image for ChromeOS involves using the Chrome Recovery Utility, which is available in the Chrome Web Store. This tool allows users to create a recovery USB drive by downloading the necessary OS image and writing it to the USB stick.

Verified Answer from Official Source:

The correct answers are verified from the ChromeOS Recovery Guide, which specifies the use of the Chrome Recovery Utility from the Chrome Web Store.

"To create a ChromeOS recovery image, download the Chrome Recovery Utility from the Chrome Web Store.

Follow the on-screen instructions to create a recovery USB stick."

The Recovery Utility is the recommended method for creating a USB recovery device, ensuring compatibility and correctness of the OS image.

Objectives:

- * Perform system recovery for ChromeOS devices.
- * Utilize official recovery tools.

NEW QUESTION # 43

You are tasked with adding a security key to a single user account. Where should you navigate to?

- A. Security > Password Management
- B. Users > Select User > Security
- C. Users > Select User > Password
- **D. Security > 2-step Verification**

Answer: D

Explanation:

To add a security key to a user account, navigate to Security > 2-step Verification in the Google Admin console. Security keys are part of the two-factor authentication (2FA) setup, enhancing account protection by requiring physical key-based verification.

Verified Answer from Official Source:

The correct answer is verified from the Google Workspace Security Guide, which outlines how to add a security key via the 2-step verification settings.

"To add a security key, go to Security settings, select 2-step Verification, and follow the prompts to register a physical security key."

Security keys provide strong, phishing-resistant two-factor authentication, making them ideal for securing sensitive accounts.

Objectives:

- * Implement secure authentication methods for users.

* Manage 2-step verification settings.

NEW QUESTION # 44

• • • • •

We believe that if you can learn about several advantages of ChromeOS-Administrator preparation questions, I believe you have more understanding of the real questions and answers. You can download the trial versions of the ChromeOS-Administrator Exam Questions for free. After using the trial version of our ChromeOS-Administrator study materials, I believe you will have a deeper understanding of the advantages of our ChromeOS-Administrator training engine.

ChromeOS-Administrator Pdf Torrent: <https://www.pass4surecert.com/Google/ChromeOS-Administrator-practice-exam-dumps.html>

- [illegible]

2025 Latest Pass4sureCert ChromeOS-Administrator PDF Dumps and ChromeOS-Administrator Exam Engine Free Share:
https://drive.google.com/open?id=1Ww309TtROxhtxyYnCHpd8JfCg_bcRg7Q