

Online ChromeOS-Administrator Training Materials, ChromeOS-Administrator Actualtest



BTW, DOWNLOAD part of PDFVCE ChromeOS-Administrator dumps from Cloud Storage: <https://drive.google.com/open?id=1Bn5QVpJKsrtmcrqrisOqfmHqG9zg6TF>

Three ChromeOS-Administrator exam questions formats that we have are Professional ChromeOS Administrator Exam (ChromeOS-Administrator) dumps PDF format, web-based ChromeOS-Administrator practice exam and desktop-based ChromeOS-Administrator practice test software. Our Google ChromeOS-Administrator PDF dumps format has actual ChromeOS-Administrator Questions which are printable and portable. Hence, you can go through these ChromeOS-Administrator questions via your smart devices like smartphones, laptops, and tablets.

Google ChromeOS-Administrator Exam Syllabus Topics:

Topic	Details
Topic 1	Understand ChromeOS security processes: It focuses on deploying certificates and uChromeOS policies.
Topic 2	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.
Topic 3	Identity Management: The primary focus of the topic identity management is on identity features.
Topic 4	Understand ChromeOS tenets: It discusses ChromeOS best practices and customers on chromeOS tenets.
Topic 5	Configure ChromeOS policies: This topic discusses understanding and configuring ChromeOS policies.

>> Online ChromeOS-Administrator Training Materials <<

ChromeOS-Administrator Actualtest | ChromeOS-Administrator Certification Dumps

We can promise that we are going to provide you with 24-hours online efficient service after you buy our Professional ChromeOS Administrator Exam guide torrent. If you purchase our ChromeOS-Administrator test guide, we are going to answer your question immediately, because we hope that we can help you solve your problem about our ChromeOS-Administrator exam questions in the shortest time. We can promise that our online workers will be online every day. If you buy our ChromeOS-Administrator Test Guide, we can make sure that we will offer you help in the process of using our ChromeOS-Administrator exam questions. You will have the opportunity to enjoy the best service from our company.

Google Professional ChromeOS Administrator Exam Sample Questions (Q50-Q55):

NEW QUESTION # 50

To allow remote users to securely connect to an internal network, the organization you're supporting is using a VPN. The organization would like you to configure the ChromeOS devices so that the Android VPN clients deployed are automatically configured with the correct hostname. How should you configure this in the Admin Console according to Google best practice?

- A. Contact the VPN provider and ask them to provide you with a custom installable client with the correct configuration pre-configured. Then deploy that installable.
- **B. Add a managed configuration using JSON to the Android app.**
- C. Upload a JSON file with the configuration into the Google Play Store.
- D. Download the Android app on a ChromeOS device, add the hostname manually, then re-upload the app in the organization's private Google Play Store and deploy it to all ChromeOS devices.

Answer: B

Explanation:

This is the most efficient and scalable way to automatically configure Android VPN clients on ChromeOS devices with the correct hostname:

* Obtain Configuration: Get the required VPN configuration details (hostname, authentication methods, etc.) from the VPN provider or your organization's network administrator. This configuration is typically in JSON format.

* Create Managed Configuration: In the Google Admin console, navigate to Devices > Chrome > Settings > Android Apps > Managed Configurations.

* Select the VPN App: Choose the specific Android VPN app you want to configure.

* Add JSON Configuration: Paste the JSON configuration into the provided field. Ensure the configuration is valid and accurate.

* Save and Deploy: Save the managed configuration and apply it to the desired organizational units (OUs) containing the ChromeOS devices.

This method allows you to centrally manage VPN configurations for Android apps on ChromeOS devices, ensuring consistency and reducing the manual effort required from users.

NEW QUESTION # 51

Which site isolation policy will enable site isolation for your entire organization?

- A. IsolateOrigins
- B. SiteOrigins
- **C. SitePerProcess**
- D. IsolatePerProcess

Answer: C

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.

NEW QUESTION # 52

Which management feature makes ChromeOS devices a popular choice for IT administrators in educational organizations and enterprises?

Which management feature makes ChromeOS devices enterprises?

- A. Secure management through on-prem infrastructure
- B. Inability to remotely control and monitor devices
- **C. Centralized management through Admin console**
- D. Remote BIOS controls and firmware update

Answer: C

Explanation:

The ChromeOS Admin console provides centralized management, making it a popular choice for IT administrators. It allows them to manage policies, apps, extensions, and device settings from a single interface, streamlining administration and ensuring consistency across devices.

Option A is incorrect because ChromeOS management is primarily cloud-based, not on-premises.

Option B is incorrect because while BIOS control might be available, it's not the primary management feature.

Option D is incorrect because ChromeOS devices can be remotely controlled and monitored through the Admin console.

References:

* About ChromeOS device management: <https://support.google.com/chrome/a/answer/1289314?hl=en>

NEW QUESTION # 53

How do you validate Chrome policies on a managed device?

- A. In the browser, go to `policy://chrome` to confirm that the device is receiving both user and device policy
- **B. In the browser, go to `chrome://policy` to confirm that the device is receiving both user and device policy**
- C. Download device logs
- D. Go to the admin console and look up the policies

Answer: B

Explanation:

To check which policies are applied to a ChromeOS device, navigate to `chrome://policy` in the Chrome browser. This page displays a list of all policies applied to the device, including both user-specific and device-specific policies. This is the most accurate way to verify that the device is receiving the correct policies from the Google Admin console.

Verified Answer from Official Source:

The correct answer is verified from the Google Chrome Enterprise Policy Guide, which recommends using the `chrome://policy` URL to review current policy settings on a device.

"To see the policies applied to a ChromeOS device, open Chrome and go to `chrome://policy`. This page lists both user and device policies that are currently enforced." This method allows administrators to validate the application of policies directly on the device, confirming that updates from the Admin console have been successfully applied.

Objectives:

- * Validate policy application on managed ChromeOS devices.
- * Use `chrome://policy` to troubleshoot policy issues.

NEW QUESTION # 54

As a ChromeOS Administrator, you have been asked to enroll all of your devices into a specific device OU using Zero-Touch Enrollment (ZTE). What are the next steps?

- A. Generate a ZTE pre-provision enrollment token directly for your domain root OU
- **B. Give the company domain name to your Chrome Partner to enable ZTF**
- C. Use a dedicated ZTE Admin account for device enrollment
- **D. Generate a ZTE pre-provision enrollment token for your specified device OU**
- E. Generate a ZTE pre-provision enrollment token for your specified user OU

Answer: B,D

Explanation:

* Generate a ZTE pre-provision enrollment token for your specified device OU: This token associates devices with the specific organizational unit (OU) during enrollment, allowing for easier management and policy application.

* Give the company domain name to your Chrome Partner to enable ZTF: This enables the Zero-Touch Framework, allowing devices to be automatically enrolled as soon as they connect to the internet.

Why other options are incorrect:

- * C (Generate token for root OU): While possible, it's not ideal as it doesn't allow for granular control over different device groups.
- * D (Generate token for user OU): Zero-Touch Enrollment is specifically for devices, not users.
- * E (Use dedicated admin account): While recommended for security, it's not a mandatory step for ZTE.

• • • • •

ChromeOS-Administrator Actualtest: <https://www.pdfvce.com/Google/ChromeOS-Administrator-exam-pdf-dumps.html>

- DOWNLOAD the newest PDFVCE ChromeOS-Administrator PDF dumps from Cloud Storage for free:
<https://drive.google.com/open?id=1Bn5QVpJKsrtmcrqrisOqfmHgQ9zg6TF>