

Most Trusted Platform to Buy Google ChromeOS-Administrator Actual Dumps



BONUS!!! Download part of iPassleader ChromeOS-Administrator dumps for free: <https://drive.google.com/open?id=1Ry3TMJXCk5bvR2bcpyfOnUwlmzgcLadG>

Firmly believe in an idea, the ChromeOS-Administrator exam questions are as long as the user to follow our steps, follow our curriculum requirements, users can be good to achieve their goals, to obtain the ChromeOS-Administrator qualification certificate of the target. Before you make your decision to buy our ChromeOS-Administrator learning guide, you can free download the demos to check the quality and validity. Then you can know the ChromeOS-Administrator training materials more deeply.

Google ChromeOS-Administrator Exam Syllabus Topics:

Topic	Details
Topic 1	• Identity Management: The primary focus of the topic identity management is on identity features.
Topic 2	• Understand ChromeOS security processes: It focuses on deploying certificates and uChromeOS policies.
Topic 3	• 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 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.

>> ChromeOS-Administrator Latest Mock Test <<

Golden Opportunity to Get a 50% Discount on Google ChromeOS-Administrator PDF Questions with 365 days Free Updates

There are many benefits after you pass the ChromeOS-Administrator certification such as you can enter in the big company and double your wage. Our ChromeOS-Administrator study materials boost high passing rate and hit rate so that you needn't worry that you can't pass the test too much. We provide free tryout before the purchase to let you decide whether it is valuable or not by yourself. To further understand the merits and features of our ChromeOS-Administrator Practice Engine you could look at the introduction of our product in detail.

Google Professional ChromeOS Administrator Exam Sample Questions (Q101-Q106):

NEW QUESTION # 101

You want users to sign in to ChromeOS devices via SAML Single Sign-On and be able to access websites and cloud services that rely on the same identity provider without having to re-enter credentials. How should you configure SAML?

- A. Enable SAML-based Single Sign-On for each application via Chrome App Management
- B. Enable SAML identity provider-initiated login for Google authentication
- C. Enable SAML-based Single Sign-On for ChromeOS devices and set the Single Sign-On cookie behavior to enable transfer of SAML SSO cookies into user sessions during login
- D. Use Chrome App Builder to enable SSO for application and force-install the application using ChromeOS user policies

Answer: C

Explanation:

To achieve seamless SSO between ChromeOS devices and other web services using the same identity provider, you need to configure SAML SSO in the Google Admin console:

* Enable SAML-based SSO for ChromeOS devices.

* In the SSO settings, find the Single Sign-On cookie behavior and set it to "Enable transfer of SAML SSO cookies into user sessions during login." This allows the SAML authentication cookie to be passed between the ChromeOS login and other web services, eliminating the need for re-authentication.

Option A is incorrect because it relates to the initial login method, not cookie transfer for subsequent SSO.

Options C and D are incorrect because they involve application-specific SSO configurations, not the general SAML SSO setup for the device.

NEW QUESTION # 102

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. Upload a JSON file with the configuration into the Google Play Store
- B. 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
- C. 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
- D. Add a managed configuration using JSON to the Android app

Answer: D

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 # 103

Within what time frame does the ChromeOS Flex upgrade transfer program support reusing Chrome Education/Enterprise Upgrades?

- A. 2 years
- B. 3 years
- C. 6 months
- D. 1 year

Answer: D

Explanation:

The ChromeOS Flex upgrade transfer program allows organizations to reuse Chrome Education or Enterprise Upgrades within 1 year of deprovisioning or transferring the device. This policy is designed to ensure that licenses can be reused efficiently when upgrading or replacing devices.

Verified Answer from Official Source:

The correct answer is verified from the ChromeOS Flex Upgrade Transfer Policy, which states that licenses can be reused within a 1-year period following device deprovisioning.

"The ChromeOS Flex upgrade transfer program permits reuse of licenses within one year of the device being deprovisioned or transferred." This policy helps organizations maintain cost efficiency when transitioning from older ChromeOS devices to ChromeOS Flex devices.

Objectives:

- * Efficient license management during device transitions.
- * Maximize the use of Chrome Education/Enterprise Upgrades.

NEW QUESTION # 104

Your organization is using a third-party IdP. Users report that they can only log in to the device when connected to the Internet. Which setting is causing this problem?

- A. Online revocation checks
- B. Single sign-on IdP redirection
- **C. SAML single sign-on login frequency**
- D. Single sign-on cookie behavior

Answer: C

Explanation:

When using a third-party Identity Provider (IdP) with SAML-based Single Sign-On (SSO), users might only be able to log in when connected to the Internet if the SAML single sign-on login frequency setting is configured in a way that requires online authentication. This configuration means that users must reauthenticate against the IdP whenever they log in, rather than using cached credentials.

Verified Answer from Official Source:

The correct answer is verified from the Google ChromeOS SSO Configuration Guide, which specifies that configuring login frequency to "Always" forces online reauthentication.

"If the SAML single sign-on login frequency is set to 'Always', users must be online to authenticate through the third-party IdP each time they log in." To allow offline login, configure the setting to allow cached credentials, which enables users to log in even without an active Internet connection.

Objectives:

- * Enable offline login for SAML-based SSO.
- * Manage login frequency settings effectively.

NEW QUESTION # 105

You're the lead for the technology department and you're working with your teammate on a hardware refresh in the upcoming year. A major part of the refresh is to consider ChromeOS devices for the majority of the users in the company. What are some organization level objectives you should consider during this hardware refresh in regard to ChromeOS?

- A. ChromeOS will need a rollout and execution plan commensurate with hardware supply availability
- B. Verifying if all the terms and conditions in the Chrome Online Agreement are applicable to ChromeOS
- **C. ChromeOS allows for advanced security flexible access, and simplified orchestration within the business**
- D. ChromeOS integration with current technological standards and practices can be worked on with trusted Google partners

Answer: C

Explanation:

When considering a hardware refresh with ChromeOS devices, organizational-level objectives should focus on the strategic advantages that ChromeOS brings to the business:

- * Advanced Security: ChromeOS is known for its robust security features, including sandboxing, verified boot, automatic updates, and data encryption. These can significantly reduce the risk of malware infections and data breaches.
- * Flexible Access: ChromeOS devices support cloud-based applications and services, enabling employees to work from anywhere.

* Chrome Enterprise overview: <https://chromeenterprise.google/>

• • • • •

[illegible]

civilconstruct.in, Disposable vapes

P.S. Free 2025 Google ChromeOS-Administrator dumps are available on Google Drive shared by iPassleader:
<https://drive.google.com/open?id=1Ry3TMJXCk5bvR2bcpyfOnUwlmzgcLadG>