

権威のあるChromeOS-Administrator科目対策一回合格-最新のChromeOS-Administrator無料模擬試験



2025年Tech4Examの最新ChromeOS-Administrator PDFダンプおよびChromeOS-Administrator試験エンジンの無料共有: <https://drive.google.com/open?id=1TTp4jWmUo44cTVa96GLEpezrUs67qomh>

ChromeOS-Administratorトレーニング資料のPDFバージョン: Professional ChromeOS Administrator Examは読みやすく、覚えやすく、印刷要求をサポートしているため、紙で印刷して練習することができます。練習資料のソフトウェアバージョンは、シミュレーションテストシステムをサポートし、セットアップの時間を与えることには制限がありません。このバージョンはWindowsシステムユーザーのみをサポートすることに注意してください。ChromeOS-Administrator試験問題のオンライン版は、Googleあらゆる種類の機器やデジタルデバイスに適しています。モバイルデータなしで練習することを条件に、オフラインでの運動をサポートします。豊富な練習資料はお客様のさまざまなニーズに対応でき、これらのChromeOS-Administrator模擬練習にはすべて、Googleテストに合格するために知っておく必要がある新しい情報が含まれています。あなたの個人的な好みに応じてそれらを選択することができます。

Google ChromeOS-Administrator 認定試験の出題範囲:

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

>> ChromeOS-Administrator科目対策 <<

実用的ChromeOS-Administrator | 100%合格率のChromeOS-Administrator科目対策試験 | 試験の準備方法Professional ChromeOS Administrator Exam無料模擬試験

現在の社会の中で優秀なIT人材が揃って、競争も自ずからとても大きくなって、だから多くの方はITに関する試験に参加してIT業界での地位のために奮闘しています。ChromeOS-AdministratorはGoogleの一つ重要な認証試験で多くのIT専門スタッフが認証される重要な試験です。

Google Professional ChromeOS Administrator Exam 認定 ChromeOS-Administrator 試験問題 (Q97-Q102):

質問 #97

Your organization's security protocols require you to ensure that any unattended devices log the user out after 24 hours. You have 1000 ChromeOS devices to manage. How would you implement this with the least amount of admin effort?

- A. Force-install a custom app to each device in question that notifies the user that they need to sign out of their device after 24 hours
- **B. Enable the 'User and Browser Settings' and update 'Maximum user session length' to any time up to 24 hours**
- C. Create a corporate policy stating (he users are to manually sign out after the end of every shift
- D. You can remotely access each device and sign out of the user account using Chrome Remote Desktop

正解: B

解説:

This is the most efficient method as it applies the setting to all devices within the organizational unit (OU) through a single policy change in the Admin console.

The other options are less efficient:

* Corporate policy: Relies on user compliance and is difficult to enforce.

* Chrome Remote Desktop: Requires manual intervention for each device.

* Custom app: Adds complexity and potential security risks.

References:

* Set up Chrome browser on managed devices:

<https://support.google.com/chrome/a/answer/3523633?hl=en>

質問 #98

A user has left the organization. What should you do to maintain the device enrollment status and policies but wipe the user's data when reassigning the device?

- **A. Clear user profiles**
- B. Factory reset the device
- C. Delete the user
- D. Remove force re-enrollment

正解: A

解説:

Clearing user profiles from the device removes all personal data and settings while keeping the device enrolled and managed. This is the most efficient way to prepare a device for reassignment while maintaining its management status.

Verified Answer from Official Source:

The correct answer is verified from the ChromeOS Device Management Documentation, which outlines clearing user profiles as a method to reset user data without affecting device enrollment.

"To reassign a device while keeping it enrolled, clear user profiles from the device. This process wipes user data but retains management policies." This method is preferable because it maintains the device's enterprise management, ensuring that it remains enrolled and policy-compliant.

Objectives:

* Efficiently reassign managed devices.

* Retain enrollment while wiping user data.

質問 #99

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

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

正解: C

解説:

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.

質問 # 100

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

正解: C

解説:

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>

質問 # 101

A school wants all new Chromebooks to be enrolled through zero-touch enrollment (ZTE) in their parent organization unit. An admin needs to create tokens.

Where will the admin go to generate the enrollment tokens for Chromebooks?

- A. Devices > Chrome > Enroll
- B. Devices > Chrome > Devices > Enroll
- C. Devices > Chrome > Settings
- D. Devices > Chrome > Connectors

正解: A

解説:

To set up Zero-Touch Enrollment (ZTE), an administrator must go to Devices > Chrome > Enroll within the Admin console. This is where they can generate the necessary enrollment tokens for automatic enrollment of devices when they first connect to the Internet.

Verified Answer from Official Source:

The correct answer is verified from the Google ChromeOS Zero-Touch Enrollment Guide, which specifies the steps to generate enrollment tokens.

"To create Zero-Touch Enrollment tokens, go to Devices > Chrome > Enroll in the Admin console." Zero-Touch Enrollment simplifies the setup process for educational institutions by automatically enrolling devices into management without manual intervention.

Objectives:

さらに、Tech4Exam ChromeOS-Administratorダンプの一部が現在無料で提供されています：<https://drive.google.com/open?id=1TTp4jWmUo44cTVa96GLEpezrUs67qomh>