# Google ChromeOS-Administrator Practice Questions

**Shared by Dennis on 24-08-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

## Question 1

Question Type: MultipleChoice

You have been tasked with organizing separated policies that apply to devices or users. Using Google's best practices, how would you structure your OUs to best achieve this?

### Options:

A- Apply all policies to a single OU, then move devices and users to that OU
B- Create a unique OU to apply devices and user policies
C- Create a dedicated OU branch for devices, and another one for the users
D- Manage all policies from the root OU

### Answer:

C

### Explanation:

Following Google's best practices, it is recommended to create separate OU branches for devices and users. This organizational structure allows administrators to apply distinct policies to users and devices, minimizing the risk of conflicting settings and ensuring better control and management.

Verified Answer from Official Source:

The correct answer is verified from the Google Workspace Organizational Units Best Practices, which highlights the importance of keeping user and device policies separate for clarity and management efficiency.

'To efficiently manage users and devices, it is recommended to create separate organizational units (OUs) for devices and users. This approach allows for targeted policy application.'

By creating separate OUs, admins can manage device-specific settings independently from user policies, reducing complexity and potential errors.

Objectives:

Structure OUs efficiently for device and user management.

Implement best practices for organizational management.

Google Workspace Organizational Units Best Practices

## Question 2

Question Type: MultipleChoice

Your security team asks you to deploy on ChromeOS only a specific Android app for your security department. As a ChromeOS Administrator, you need to find a way to block all other Android apps except the one that you need. How are you going to proceed?

### Options:

A- From the 'Apps & extensions' page add the Android app on the security team user OU
B- On the 'Users & Browser Settings'' tab. for the Play Store, use the 'Block all apps, admin manages allowlist' policy and allow only the
C- Android app that you want from 'Apps & extensions ' On the 'Users & Browser Settings'' tab. for the Chrome Web Store use the 'Block all apps, admin manages allowlist' policy and allow only the Android app that you want on 'Apps & extensions '
D- From trio 'Apps & extensions' page add the Android app on the security team user OU and select 'Force Install * pin to ChromeOS taskbar'

### Answer:

B

### Explanation:

Access Google Admin Console: Sign in to your Google Admin console.

Navigate to Device Management: Go to Devices > Chrome > Settings > Users & browsers.

Locate Play Store Settings: Find the section related to the Play Store.

Enable Allowlist Policy: Activate the policy 'Block all apps, admin manages allowlist.'

Add the Security App: Go to the 'Apps & extensions' section and add the specific Android app that you want to allow for the security team's organizational unit (OU).

This configuration ensures that all other Android apps are blocked from installation on ChromeOS devices, except the specified security app. This provides granular control over app deployment and enhances security by preventing unauthorized app usage.

## Question 3

Question Type: MultipleChoice

Your team has members that work remotely. Your CTO would like to verify that your fleet of ChromeOS devices remains managed by corporate policy even after a device wipe. What would you configure to complete this objective?

## Options:

A- Set the setting 'Powerwash' to 'Do not allow powerwash to be triggered'
B- Create strict password rules
C- Edit the setting 'Verified Access' to 'Require verified mode for boot for verified access'
D- Set up the Admin console to force the device to automatically re-enroll after wiping

## Answer:

D

## Explanation:

To ensure that ChromeOS devices remain managed after a wipe, you need to enable forced re-enrollment. This setting automatically re-enrolls the device into the management domain after it has been wiped (Powerwashed). This feature is crucial for organizations that manage devices remotely, as it prevents unauthorized users from removing management settings.

Verified Answer from Official Source:

The correct answer is verified from the Google ChromeOS Device Management Best Practices Guide, which recommends enabling forced re-enrollment to maintain device management continuity.

'To ensure devices remain managed after wiping, enable the 'Forced Re-enrollment' policy in the Admin console. This setting ensures automatic re-enrollment upon startup.'

Forced re-enrollment prevents the loss of device management, which is essential for maintaining security and policy compliance, especially in remote or dispersed environments.

Objectives:

Enforce device management after Powerwash.

Maintain compliance in remote work environments.

Google ChromeOS Device Management Best Practices Guide

## Question 4

Question Type: MultipleChoice

You need to create a recovery image on a USB stick. Which two steps should you take?

(Choose 2 answers)

### Options:

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

### Answer:

B, C

### 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.

ChromeOS Recovery Guide

## Question 5

Question Type: MultipleChoice

What are the steps to enroll a previously used, non-managed ChromeOS device in your domain?

### Options:

A- Reboot the ChromeOS device, and at the login screen, press CTRL+ALT+M to enroll it.
B- Powerwash the ChromeOS device, complete the out-of-box experience (OOBE), and before signing in, press CTRL+ALT+E to enroll it.
C- Use the Chrome Recovery Utility with a USB Flash drive to reimage the device's OS. Then, after completing the OOBE, press CTRL+ALT+M to enroll the Chromebook.
D- Switch the ChromeOS device to developer mode, wipe the device, and switch back to normal mode. Then, after completing the OOBE, press CTRL+ALT+E to enroll the ChromeOS device.

### Answer:

B

### Explanation:

To enroll a previously used device, it must first be wiped to remove any prior user data or configuration. The device must then go through the out-of-box experience (OOBE) as if it were new. During the initial setup screen, pressing CTRL+ALT+E will start the enterprise enrollment process.

Verified Answer from Official Source:

The correct answer is verified from the Google Admin Console Guide, which details the steps required for re-enrolling previously used ChromeOS devices.

'To re-enroll a device, perform a factory reset (Powerwash), and during the initial login screen, press CTRL+ALT+E to initiate the enrollment process.'

This method ensures that any residual configuration or data from the previous user is completely removed before re-enrollment, ensuring a clean setup.

Objectives:

Enroll used ChromeOS devices.

Maintain consistent device management.

Google Admin Console Guide - Device Enrollment

## Question 6

Question Type: MultipleChoice

As your organization's administrator, you want to assign a delegated admin custom role in order to perform a limited set of ChromeOS device management tasks only for the Marketing organizational unit. What should you do?

### Options:

A- Create and assign a super admin role
B- Create and assign a custom role with 'Chrome Management permissions' for the root OU
C- Create and assign a custom role with 'Chrome Management permissions' for the Marketing devices OU
D- Create and assign a custom role with 'Chrome Management permissions' for the Marketing Users OU

### Answer:

C

### Explanation:

To delegate ChromeOS device management specifically for the Marketing OU, create a custom role with 'Chrome Management permissions' and assign it specifically to the Marketing devices OU. This ensures that the delegated admin can manage only the devices within that specific OU without impacting the entire organization.

Verified Answer from Official Source:

The correct answer is verified from the Google Admin Console Role Management Guide, which recommends assigning roles at the appropriate OU level for granular access control.

'Assign roles to specific OUs to limit administrative control to relevant organizational units, such as the Marketing devices OU.'

By targeting the role to the Marketing devices OU, you ensure that the delegated admin does not have unnecessary access to devices in other parts of the organization, maintaining the principle of least privilege.

Objectives:

Implement delegated administration for specific OUs.

Limit administrative scope to enhance security.

Google Admin Console Role Management Guide

## Question 7

Question Type: MultipleChoice

Your organization has automatic ChromeOS updates implemented. Your CTO would like to review the documentation on what changes each new version has. How would you assist your CTO in accomplishing this goal?

### Options:

A- Open Chrome and enter chrome://updates in the address bar
B- Search YouTube for Chrome Update stories
C- Direct your CTO to the ''Chrome Release Notes Support' page
D- Have your CTO start a Google Chrome Support ticket

### Answer:

C

### Explanation:

The best way to review detailed changes for each new ChromeOS version is to visit the Chrome Release Notes Support page. This page contains official documentation about new features, improvements, and fixes introduced with each update.

Verified Answer from Official Source:

The correct answer is verified from the Google ChromeOS Release Notes Documentation, which serves as the primary resource for update details.

'For detailed information on ChromeOS updates, visit the Chrome Release Notes Support page, which includes information on version changes and improvements.'

Providing access to official release notes ensures that the CTO gets accurate and up-to-date information without relying on third-party interpretations.

Objectives:

Access official documentation for ChromeOS updates.

Keep stakeholders informed of software changes.

Chrome Release Notes Support

## Question 8

Question Type: MultipleChoice

In line with Google's best practice recommendations, you need to configure an OU of devices to run on an early release of ChromeOS so that users can test new features and verify functionality. Which policy option should you choose?

### Options:

A- LTS
B- Canary
C- Beta
D- Stable

### Answer:

C

### Explanation:

ChromeOS offers different release channels with varying levels of stability and feature availability:

Stable: The most stable and widely used channel, suitable for general deployment.

Beta: Contains newer features and improvements, but with some potential for instability. Ideal for testing in a controlled environment.

Dev: More frequent updates with experimental features, less stable than Beta.

Canary: The least stable channel, updated daily with bleeding-edge features.

To test new features while maintaining reasonable stability, the Beta channel is the recommended choice.

## Question 9

Question Type: MultipleChoice

The security department has been informed that a ChromeOS device was stolen out of an employee's car. What should you do in the Admin console to ensure the device Is rendered Inoperable while still maintaining management of the device?

### Options:

A- Tag the ChromeOS device as stolen
B- Disable the ChromeOS device
C- Powerwash the ChromeOS device
D- Deprovision the ChromeOS device

### Answer:

B

### Explanation:

Disabling a ChromeOS device in the Admin console prevents it from booting up or being used, effectively rendering it inoperable. However, it retains the device's association with the organization, allowing administrators to track its location and manage it remotely if recovered.

The other options are not as suitable:

Tagging as stolen: Doesn't prevent device usage.

Powerwash: Removes all data and enrollment, making management impossible.

Deprovision: Removes device association, making management impossible.

## Question 10

Question Type: MultipleChoice

You have been asked to explain the built-in security features of ChromeOS. What i3 the benefit of having verified boot enabled on a ChromeOS device?

## Options:

A- It ensures that the OS is uncompromised
B- It allows updates to happen in the background
C- Running both operating systems on one device at the same time makes It twice as powerful
D- It installs the known safe backup OS every time the device is slatted up.

## Answer:

A

## Explanation:

Verified Boot in ChromeOS is a security mechanism that checks the integrity of the operating system during startup. If it detects any unauthorized modifications or compromises, it can initiate recovery processes to restore the OS to a known good state, ensuring that the device boots up with a secure and untampered operating system.

Option B is incorrect because background updates are a separate feature.

Option C is incorrect because dual-boot is not related to Verified Boot.

Option D is incorrect because Verified Boot doesn't install a backup OS but verifies the existing one.

Verified Boot: https://www.chromium.org/chromium-os/chromiumos-design-docs/verified-boot/

# Question 11

Question Type: MultipleChoice

You are tasked with reducing the risk of a breach of your organization's identities. What should you do to minimize the risk?

## Options:

A- Connect your LDAP
B- Configure individual Google Accounts
C- Set up Single Sign-On (SSO)
D- Set up Client-side encryption

## Answer:

C

## Explanation:

Setting up Single Sign-On (SSO) significantly reduces identity risks by centralizing authentication through a secure, verified identity provider (IdP). This method helps ensure consistent password policies, multi-factor authentication (MFA), and robust security practices. It also minimizes the risk of password reuse and phishing.

Verified Answer from Official Source:

The correct answer is verified from the Google Workspace Security Guide, which recommends implementing SSO to manage authentication securely.

'Single Sign-On (SSO) allows users to access multiple applications with a single set of credentials, reducing the risk of identity breaches by centralizing authentication.'

SSO enhances security by integrating with trusted IdPs, implementing MFA, and reducing credential exposure across multiple applications.

Objectives:

Strengthen identity and access management (IAM).

Implement secure authentication practices with SSO.

Google Workspace Security Guide

# Question 12

Question Type: MultipleChoice

Your customer is deploying ChromeOS devices in their environment and requires those ChromeOS devices to adhere to web filtering via TLS (or SSL) inspection. What recommendations should you make to your customer in setting up the requirements for ChromeOS devices?

## Options:

A- Configure a hostname allowlist, set up a TLS (or SSL) certificate, then verify TLS (or SSL) inspection is working

B- ChromeOS devices are preconfigured to adhere to company TLS (or SSL) inspection by

default
C- Configure a transparent proxy, set up your allowlist to use 'google.com', then verify TLS (or SSL) inspection is working
D- Reach out to Google Workspace Security and Compliance for tailored configurations

## Answer:

A

## Explanation:

To enable web filtering with TLS (or SSL) inspection on ChromeOS devices, configure a hostname allowlist and set up a TLS (or SSL) certificate. Verifying that TLS inspection is working ensures that HTTPS traffic can be inspected without causing certificate errors.

Verified Answer from Official Source:

The correct answer is verified from the Google ChromeOS Security Configuration Guide, which advises configuring hostnames and certificates to enable secure web filtering.

'To perform SSL inspection on ChromeOS devices, configure a hostname allowlist and install the necessary SSL certificates. Verify that the inspection is functioning correctly.'

Without proper configuration, SSL inspection can lead to certificate errors or blocked traffic. Setting up the allowlist and certificates correctly is crucial for maintaining secure and compliant web access.

Objectives:

Implement secure web filtering on ChromeOS.

Configure TLS inspection to prevent certificate issues.

Google ChromeOS Security Configuration Guide

# Question 13

Question Type: MultipleChoice

How would you deploy a Progressive Web Application to all managed user accounts?

## Options:

A- Force-install the Progressive Web Application URL in the 'Chrome Apps & extensions' page
B- Set up Chrome Imprivata shared apps & extensions to force-install the Progressive Web Application URL
C- Go to 'User & Browser Settings' and add the Progressive Web Application URL in the 'Legacy Browser Support' site list
D- Open 'Additional Google services' to force-install the Progressive Web Application URL

## Answer:

A

## Explanation:

To deploy a Progressive Web Application (PWA) to all managed user accounts, follow these steps in the Google Admin console:

Sign in to Google Admin console: Use your administrator credentials to access the console.

Navigate to Device Management: Go to Devices > Chrome > Settings > Apps & extensions.

Select User or Group: Choose the top-level organizational unit or a specific group to apply the PWA deployment.

Add by URL: Click on the yellow '+' icon and select 'Add by URL.'

Enter PWA URL: Paste the URL of the PWA you want to deploy.

Configure Installation Policy: Select 'Force install' to ensure the PWA is automatically installed for all users within the selected scope.

This method allows you to centrally manage and deploy PWAs across your organization, making them easily accessible to users on their ChromeOS devices.