PassQueen
a.k.a dumpsqueen.com

Professional ChromeOS Administrator Exam

Google ChromeOS-Administrator

Version Demo

Total Demo Questions: 13

Total Premium Questions: 132

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Planning and implementing a ChromeOS solution	35
Topic 2, Configuring and managing ChromeOS devices	43
Topic 3, Configuring and managing ChromeOS users and policies	38
Topic 4, Troubleshooting ChromeOS devices and policies	16
Total	132

QUESTION NO: 1

As the ChromeOS Administrator, you have been given previously used devices by another organization that have been used, but do not know the current management state of the devices. When are yourequired to wipe a device before enrolling it?

(Choose 2 answers)

A. When the device has been purchased from an authorized reseller.

B. When the device has been previously enrolled in a different domain.

C. When the device has been sitting in a warehouse for more than 90 days.

D. When the device has been signed in to by a user before enrolling it.

E. When a replacement device is sent from an OEM to replace a defective device.

ANSWER: B D

Explanation:

When the device has been previously enrolled in a different domain, it must be returned to a clean, unenrolled state before it can be set up for the new organization. A factory reset removes local user data and device configuration so the device can present the enrollment flow and receive the intended organization's Chrome policies. Administrators should also verify that the former organization has properly deprovisioned or transferred the device, because a reset does not by itself remove enterprise ownership controls such as forced re-enrollment.

When the device has been signed in to by a user before enrolling it, wiping is required to remove the existing user profile, local data, and settings and to restore the out-of-box enrollment experience. This ensures enrollment occurs before ordinary user use and that the organization starts from a known, clean device state. Google's enrollment guidance directs administrators to factory-reset previously used devices before enrollment, and its reset documentation confirms that a Powerwash erases user accounts and locally stored data. See Enroll ChromeOS devices and Reset your Chromebook to factory settings.

QUESTION NO: 2

Your organization uses EAP-TLS Wi-Fi authentication and needs managed ChromeOS devices to obtain client certificates automatically rather than requiring users to import certificates manually. Which two configuration steps are required?

Choose 2 answers

A. Configure a SCEP certificate enrollment profile

B. Configure the managed Wi-Fi network to use EAP-TLS and the issued certificate

C. Upload a client certificate to the Chrome Web Store

D. Force-install a certificate file as a Chrome extension

E. Add only the certificate authority root certificate to the Wi-Fi profile

ANSWER: A B

Explanation:

Configure a SCEP certificate enrollment profile so ChromeOS can request the required client certificate from the organization's certificate service. Then configure the managed Wi-Fi network to use EAP-TLS and reference the certificate enrollment configuration. Uploading a certificate file to the Chrome Web Store does not provision a certificate to ChromeOS, and adding a root certificate alone establishes trust but does not provide each device or user with a client identity certificate.

QUESTION NO: 3

A customer has a mission-critical workload running on ChromeOS and needs devices configured to reduce ChromeOS changes. How can an admin reduce the risk of an unexpected change in an OS update affecting the customer's entire ChromeOS device domain while maintaining security and minimizing admin workload?

A. Force auto reboot after update

B. Enable variations

C. Move to a Long-term Support channel

D. Add an update rollout plan

ANSWER: C

Explanation:

Move to a Long-term Support channel is the best fit for a mission-critical ChromeOS environment that prioritizes stability, continued security, and low administrative overhead. The Long-term Support (LTS) channel holds devices on a feature version for an extended period, so the organization receives substantially fewer functional and user-interface changes than it would on the stable channel. This gives business-critical applications, peripherals, and workflows a more predictable operating environment and reduces the likelihood that a newly introduced feature change disrupts the fleet.

Importantly, LTS does not mean leaving devices unprotected. Google continues to provide security fixes on the LTS release, allowing administrators to maintain a secure ChromeOS deployment without having to repeatedly validate frequent feature releases. Feature updates are delivered on a planned, less frequent cadence, making testing and change-management activities more manageable. This channel therefore directly addresses the need to reduce OS changes across the device domain while avoiding the ongoing monitoring and staged-deployment work associated with managing repeated rollout plans. Google documents the LTS channel and its security-update approach in its ChromeOS Long-term Support documentation. Administrators can configure the selected release channel through the ChromeOS update settings in the Admin console.

QUESTION NO: 4

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. Delete the user

B. Factory reset the device

C. Remove force re-enrollment

D. Clear user profiles

ANSWER: D

Explanation:

Clear user profiles is the appropriate ChromeOS administrative action when a managed device is being reassigned and the goal is to remove the departing user’s local information without taking the device out of management. This command removes the user profiles stored on the device, including locally retained user data and settings, so the next person can sign in to a clean profile environment. Crucially, the device itself remains enrolled in the organization’s ChromeOS management, so organizational units, device policies, apps, network settings, and other configured management controls continue to apply after the profile data is cleared.

This is useful for routine reassignment because it separates the cleanup of local user information from the lifecycle of the managed device. An administrator can issue the action from the Google Admin console for the selected ChromeOS device and then provide the device to its new user. The new user’s sign-in creates a new managed profile while the existing device-management configuration remains in place. Google documents Clear user profiles as a remote device command for

removing profiles while retaining device enrollment and management. See Google's ChromeOS device data management guidance and Google Admin Help for managing ChromeOS devices.

QUESTION NO: 5

What are two reasons that Chromebooks never experienced a ransomware attack?

(Choose 2 answers)

A. All applications run in a sandbox

B. Automatic virus scanning keeps them safe

C. Users are not able to download software

D. All web traffic is SSL inspected

E. Devices go through a Verified Boot process

ANSWER: A E

Explanation:

All applications run in a sandbox and Devices go through a Verified Boot process are the two ChromeOS security design features that directly support resistance to ransomware. ChromeOS sandboxing isolates browser tabs, applications, and system processes with restrictive permissions. This containment reduces the ability of malicious content or a compromised process to access data belonging to other processes or to make broad, persistent changes to the device. The security model is designed so that code runs with only the access it needs rather than with unrestricted system privileges.

Verified Boot protects the integrity of the operating system every time the Chromebook starts. During boot, ChromeOS validates system components against a trusted version. If it detects that the system has been modified or is corrupt, it can recover to a known-good ChromeOS image. This makes it substantially harder for malware to persist by altering core operating-system files, which is a common objective of ransomware and other malware attempting to survive a restart.

These controls are foundational, built into ChromeOS rather than dependent on a user remembering to run a cleanup step. Google describes sandboxing and Verified Boot as core elements of ChromeOS's layered security architecture. See ChromeOS Security Whitepaper and ChromeOS security overview.

QUESTION NO: 6

An organization has created organization units within the Google Admin console for additional management structure. What is the most effective way to manage each OU while not affecting the top-level OU policy?

A. Disable auto updates

B. Override the inheritance for a given policy

C. Delete sublevel OUs and only work from the top level OU

D. Force inheritance from top level OU to all OUs

ANSWER: B

Explanation:

Override the inheritance for a given policy is correct because Google Admin console settings are organized hierarchically: settings configured in a parent organizational unit are inherited by its child OUs unless an administrator explicitly changes that setting at a lower level. An administrator can select a specific child OU, configure the required policy value there, and save it as an override. That policy then applies to the selected OU and, generally, its descendants, while the top-level OU's configured policy remains unchanged. This supports targeted administration for groups with different operational, security, or device-management requirements without disrupting the organization-wide baseline. For example, an administrator might

retain a standard parent policy but override a particular Chrome setting for a dedicated OU containing managed devices with a specialized use case. Google documents that organizational units enable administrators to apply settings to subsets of users or devices, and that child organizations inherit parent settings unless they are overridden. See Google Admin Help: Organizational units and Google Admin Help: Set Chrome policies for users or browsers.

QUESTION NO: 7

What are two ways customers can open a support case for ChromeOS? Choose 2 answers

A. Chat support via the Admin console

B. Contact the device manufacturer

C. File feedback on the device with Alt + Shift +1

D. File case through Customer Care Portal

E. Send an email to ChromeOS support

ANSWER: B D

Explanation:

Contact the device manufacturer is a valid way to initiate support for a ChromeOS device, particularly when the issue involves device hardware, warranty service, repair, or model-specific behavior. ChromeOS devices are sold and supported through their original equipment manufacturers, so the manufacturer can receive, triage, and manage cases within its applicable support process. Google's ChromeOS documentation directs customers to use the appropriate support route for their product and entitlement, including manufacturer support where relevant.

File a case through the Customer Care Portal is also correct because the portal is a formal case-management channel for eligible ChromeOS customers. It enables an administrator or authorized customer contact to submit issue details and follow the case through its lifecycle with Google support. This is distinct from merely sending product feedback: a support case is an actionable service request with case tracking and support engagement. Google documents available Chrome Enterprise and ChromeOS support paths at Get support for Chrome Enterprise and Education. General ChromeOS product and support information is also available through ChromeOS.

QUESTION NO: 8

You need to set a policy that prevents the device from shutting down while idling on the sign-in screen. Where should you navigate to?

A. User Settings > Idle settings

B. User Settings > User Experience

C. Device Settings > Allow shutdown

D. Device Settings > Power management

ANSWER: D

Explanation:

Device Settings > Power management is correct because sign-in-screen behavior is controlled through device-level policies, which apply before any user signs in. In the Google Admin console, ChromeOS administrators can configure power-management policies for managed devices, including the action a device takes when it is idle at the sign-in screen. Set the applicable idle action to a non-shutdown behavior, such as keeping the device awake or sleeping it as required by the organization's operational needs.

This configuration is particularly important for shared, kiosk, or publicly accessible devices. It ensures the device remains available for the next user rather than powering off after an unattended interval at the login prompt. Because no user session

exists at that stage, the policy must be configured in the device settings area rather than in a user policy area. Google documents ChromeOS device configuration under the Chrome device settings page, including the Power management section and its idle-related controls. Administrators should apply the setting to the correct organizational unit or group, save the change, and allow time for the policy to reach enrolled devices.

References: Google Admin Help: Set Chrome device policies and Google Admin Help: Manage ChromeOS device settings.

QUESTION NO: 9

You need to delegate limited ChromeOS device-management responsibilities to a regional administrator. The administrator must manage only devices assigned to the West devices organizational unit and must not receive broad administrative privileges.

Which two actions should you take?

Choose 2 answers

A. Create a custom role with the required Chrome Management privileges

B. Assign the custom role with the West devices organizational unit as its scope

C. Assign the administrator the Super Admin role

D. Scope the role to the West users organizational unit

E. Move the administrator's own account into the West devices organizational unit

ANSWER: A B

Explanation:

Create a custom administrator role with only the necessary Chrome Management privileges, then assign that role with the West devices organizational unit as its scope. This follows least-privilege administration and ensures that the delegated administrator can manage only the intended device population. Assigning Super Admin would provide excessive access, while using the West users organizational unit would not correctly limit device-management authority based on the device organizational unit.

QUESTION NO: 10

A user who is having trouble seeing the cursor on their screen due to a visual impairment contacts a help desk.

What is the best option an admin can use to explore this issue?

A. Update User personalization

B. Review using remote desktop

C. Change the device resolution

D. Configure the LargeCursorEnabled ChromeOS accessibility policy

ANSWER: D

Explanation:

Configuring the `LargeCursorEnabled` ChromeOS accessibility policy is the most direct administrative response to a user who cannot easily see the pointer. ChromeOS includes a Large mouse cursor accessibility feature that increases the pointer's size, making it substantially easier to locate and track for users with low vision. An administrator can manage this setting through the applicable ChromeOS policy scope and target it to the appropriate organizational unit or group, allowing the accommodation to be provided consistently rather than relying on an unsupported diagnostic workflow. The policy can also be adjusted or removed later if the user needs a different cursor size or accessibility configuration.

This approach addresses the reported accessibility need while keeping the change within ChromeOS's managed configuration framework. Google's user accessibility documentation describes how users can enable and adjust a larger mouse cursor, and the Chrome Enterprise policy reference documents the administrative `LargeCursorEnabled` policy. See Google Chromebook Help: Make your Chromebook more accessible and Chrome Enterprise policy reference: LargeCursorEnabled.

QUESTION NO: 11

You want to restrict who can sign in to a managed device during working hours. Which two settings do you need to use?

Choose 2 answers

A. Single sign-on IdP redirection

B. Device off hours

C. User Data (Ephemeral)

D. Family Link accounts

E. Restrict sign-in to a list of users

ANSWER: B E

Explanation:

Device off hours and **Restrict sign-in to a list of users** work together to enforce this requirement. Device off hours lets an administrator define the periods in which a managed ChromeOS device is unavailable for use. Setting the off-hours schedule outside the organization's working hours ensures that the device cannot be used or signed in to outside the intended operating window. The schedule is configured at the organizational-unit level, allowing different groups of devices to have different permitted hours when necessary.

Restrict sign-in to a list of users controls the identities permitted to access the device while it is available. Administrators can allow only specified managed Google accounts, groups, or domains, depending on the sign-in restriction configuration. This prevents unauthorized users from signing in during the hours when the device is operational. Used together, these settings provide both the time-based control and the user-based control described in the question. Google documents ChromeOS device-level policy configuration in its Chrome Enterprise device policy documentation, and sign-in access controls are covered in the Chrome policy management documentation.

QUESTION NO: 12

Due to security threats, your security team would like to immediately prevent any apps on a ChromeOS device from being able to use USB devices. How can you as the admin implement this security practice as quickly and efficiently as possible?

A. Create an allowlist and add apps that do not need USB permissions

B. Create a blocklist and add apps that use USB permissions

C. Create a blocklist, add apps that use USB permissions, and allow users to 'request' apps that are not approved

D. Block apps by using the "Block apps by permissions settings" which will allow you to select "USB" as permission type to block

ANSWER: D

Explanation:

Use the Admin console's **Block apps by permissions** setting and select **USB** as the permission to block. This applies a policy-based restriction to apps in the selected organizational unit or group, providing a centralized and immediate way to prevent managed Android apps from accessing USB devices. It is more efficient than identifying every application individually because the policy targets the capability itself: any app that requires the USB permission is blocked according to

the configured scope. Administrators can deploy the setting at the appropriate organizational level, allowing the restriction to take effect consistently for users and devices that inherit that policy. Google documents app-management controls in the Admin console, including permission-based app blocking, as part of Android app and managed Google Play configuration for ChromeOS. For implementation details, see Google's Manage Android apps on ChromeOS devices documentation and the Chrome Enterprise and Education Help Center. Selecting USB directly addresses the stated security need by preventing app access to USB peripherals without requiring manual review and maintenance of separate app lists.

QUESTION NO: 13

As a ChromeOS Administrator, you are tasked with blocking incognito mode in the ChromeOS Browser. How would you prevent users from using incognito mode?

A. Navigate to "Users & browsers" and set "Incognito mode" to "Disallow incognito mode."

B. Go to "User & Browser Settings" to restrict sign-in to pattern and "Disallow incognito mode."

C. From "Device Settings", change Kiosk settings to "Disallow incognito mode."

D. In "Enrollment Settings", disable verified access and incognito mode for content protection.

ANSWER: A

Explanation:

Navigate to "Users & browsers" and set "Incognito mode" to "Disallow incognito mode." This is the Chrome Enterprise user policy that controls whether Chrome users can open Incognito windows. Apply the setting to the organizational unit or configuration group containing the intended users, then save the policy. Once the policy is received by managed ChromeOS devices, the Incognito option is unavailable in the Chrome browser for those users. Because this is a user-and-browser policy, its scope follows the managed user configuration rather than being configured through device enrollment, kiosk configuration, or verified-access settings. Administrators can use policy status reporting or open `chrome://policy` on a managed device to confirm that the Incognito mode availability policy has been applied. Google documents this setting in its Chrome user and browser policy guidance; the underlying Chrome policy is `IncognitoModeAvailability`, whose disabled value prevents Incognito mode from being used. See Google's Chrome policy management documentation and the IncognitoModeAvailability policy reference.