Number: ChromeOS Administrator
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: ChromeOS Administrator

Exam Name: Professional ChromeOS Administrator

Exam A

QUESTION 1
In regular user mode, how does an admin open the crosh shell on a ChromeOS device to run a ping command?

A. Ctrl + Alt + V
B. Ctrl + Alt + t
C. Ctrl + Alt + Tab +W
D. Ctrl + Alt + i

Correct Answer: B
Section:
Explanation:
In regular user mode on a ChromeOS device, pressing Ctrl + Alt + t opens the crosh shell (Chrome OS developer shell), a command-line interface. From there, you can execute various commands, including ping to test network connectivity.
Other options are incorrect because they either have no assigned function or trigger different actions in ChromeOS.

QUESTION 2
A large marketing company hires interns in the IT department. The interns should see only info from ChromeOS devices but should not be able to manage or update any device.
How should an admin assign this role to Interns?

A. Create a custom services admin role and enable 2FA
B. Create Custom role under Chrome management and assign Telemetry API role
C. Create Custom role under Chrome management and assign Settings rote
D. Create Custom role under Chrome management and assign Manage ChromeOS devices role K.

Correct Answer: B
Section:
Explanation:
To grant interns read-only access to ChromeOS device information without management or update capabilities, you should:
Create Custom Role: In the Google Admin console, navigate to 'Device management' -> 'Chrome management' -> 'User settings' -> 'Roles.'
Assign Telemetry API Role: Within the custom role, assign the 'Telemetry API' role. This allows interns to view device information collected through the API but not make changes.
Exclude Other Roles: Ensure no other roles are assigned that grant management or update permissions.
Option A is incorrect because it involves service admin roles, which typically have broader administrative access.
Option C is incorrect because the 'Settings' role might grant more permissions than intended.
Option D is incorrect because the 'Manage ChromeOS devices' role grants full management capabilities, which is not suitable for interns.
Chrome Browser Cloud Management API: https://developers.google.com/chrome/policy

QUESTION 3
To use Verified Access in your organization, you need to have a Chrome extension that calls Verified Access API on the client devices. Where can you go to get this extension?

A. Google Play Store
B. Independent software vendor (ISV) or Google Verified Access API
C. Independent software vendor (ISV) repository

D. Software API Key store

Correct Answer: B
Section:
Explanation:
Verified Access requires a Chrome extension to communicate with the Verified Access API. While Google doesn't directly provide this extension, it offers detailed documentation and resources through the Verified Access API. Independent software vendors (ISVs) can use these resources to develop and provide compatible extensions.
Option A is incorrect because Google Play Store is for Android apps, not Chrome extensions.
Option C is incorrect because while ISVs might offer extensions, it's not the sole source. Google's documentation is essential.
Option D is incorrect because API keys are for authentication, not the extension itself.

QUESTION 4
You're in charge of deploying video conferencing equipment and it has been decided that you will leverage ChromeOS devices. What initial considerations should you make when deciding on devices?

A. Deploying instructional guides to all users on setup configuration, and use of new equipment
B. A form factor compatible for both remote and site workers is required
C. A precise time window on how to apply security patches and updates to all devices
D. Devices must have 8GB of RAM and obey supported processor models

Correct Answer: B
Section:
Explanation:
When deploying video conferencing equipment using ChromeOS devices, the primary consideration is choosing a form factor (device type) that caters to both remote and on-site workers. This ensures flexibility and consistent user experience regardless of location.
Option A is incorrect because while instructional guides are helpful, they are a secondary concern to device suitability.
Option C is incorrect because security patch timing is important but not the initial consideration when choosing devices.
Option D is incorrect because while specifications matter, they should align with the chosen form factor and user needs.

QUESTION 5
A ChromeOS Administrator has deployed ChromeOS devices in their organization. How can the company evaluate the compatibility with future updates following Google's best practices while still gaining access to new features when they launch?

A. Enable 'Auto Updates' on all devices on the 'Stable channel*, but let the employees in the IT department run their devices on the 'Beta channel* so they have time to evaluate and adapt the environment to each update before it reaches Stable
B. Disable ''Auto Updates'' on all devices and let the admin test the newest release on the 'Stable channel' on their own device before rolling it out organization-wide
C. Set 5% of the organization across several departments on the 'Beta channel'1, and configure the rest of the fleet to receive auto updates on the 'Stable channel'
D. Set the entire fleet to update in accordance with the 'Long-term Support (LTS) channel'

Correct Answer: A
Section:
Explanation:
This approach balances access to new features with controlled testing. Here's how it works:
Stable Channel: Most devices receive automatic updates on the Stable channel, ensuring security and stability for the majority of users.
Beta Channel: IT staff use the Beta channel to access updates earlier, allowing them to identify and address potential issues before they affect the entire organization.
Evaluation and Adaptation: IT staff can test compatibility, adjust configurations, and prepare for broader deployment based on their experience with the Beta channel.
Option B is incorrect because disabling auto-updates compromises security and delays access to new features.
Option C is incorrect because while a small beta group is useful, it might not be enough to cover all potential issues.
Option D is incorrect because the LTS channel focuses on stability, not early access to new features.

QUESTION 6
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. Remote BIOS controls and firmware update
C. Centralized management through Admin console
D. Inability to remotely control and monitor devices

Correct Answer: C
Section:
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.
About ChromeOS device management: https://support.google.com/chrome/a/answer/1289314?hl=en

QUESTION 7
What should an administrator do to view the number and type of ChromeOS upgrades purchased and in use by their domain?

A. Verify upgrades on devices page
B. Check subscriptions in billing
C. Contact partner to verify
D. Check reports page for upgrades

Correct Answer: B
Section:
Explanation:
To view the number and type of ChromeOS upgrades purchased and in use, administrators should check the 'Subscriptions' section in the billing area of the Google Admin console. This section provides a clear overview of the organization's ChromeOS upgrade subscriptions and usage.
Other options are incorrect because they don't directly provide information about ChromeOS upgrade subscriptions:
Option A (Verify upgrades on devices page): Shows upgrades on individual devices, not the overall purchase and usage.
Option C (Contact partner to verify): Unnecessary if the information is readily available in the Admin console.
Option D (Check reports page for upgrades): Might provide some usage data, but not the purchase details.
Sign in to your Admin console: https://support.google.com/chrome/a/answer/182076?hl=en

QUESTION 8
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 for your specified device OU
B. Give the company domain name to your Chrome Partner to enable ZTF
C. Generate a ZTE pre-provision enrollment token directly for your domain root OU
D. Generate a ZTE pre-provision enrollment token for your specified user OU
E. Use a dedicated ZTE Admin account for device enrollment

Correct Answer: A, B

Section:
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.

QUESTION 9
Which remote command is required to remove a device from management policy updates?

A. Deprovision
B. Reset
C. Disable
D. Powerwash

Correct Answer: A
Section:
Explanation:
The 'Deprovision' command is specifically designed to remove a ChromeOS device from management policy updates. This means the device will no longer receive updates, configurations, or restrictions pushed from the Google Admin console.
Here's what happens when you deprovision a device:
Policy Removal:All enterprise policies and configurations are removed from the device.
Management Removal:The device is disassociated from the Google Admin console and no longer considered managed.
Data Wipe (Optional):You can choose to wipe the device's data during deprovisioning to ensure no company data remains.
Other options like 'Reset,' 'Disable,' or 'Powerwash' may have different effects:
Reset:Resets the device to factory settings but might not remove management if not done through the Admin console.
Disable:Prevents the user from signing in but doesn't remove policies or management.
Powerwash:Factory resets the device,removing all user data and configurations,including management.
Deprovision a device:https://support.google.com/chrome/a/answer/3523633

QUESTION 10
What is the recommended way to provision users from an on-prem Active Directory environment into the Google Admin console?

A. Upload via CSV
B. Admin SDK Directory API
C. Azure AD Google Cloud/G Suite Connector
D. Google Cloud Directory Sync

Correct Answer: D
Section:
Explanation:
The 'Deprovision' command is specifically designed to remove a ChromeOS device from management policy updates. This means the device will no longer receive updates, configurations, or restrictions pushed from the Google Admin console.
Here's what happens when you deprovision a device:
Policy Removal:All enterprise policies and configurations are removed from the device.
Management Removal:The device is disassociated from the Google Admin console and no longer considered managed.
Data Wipe (Optional):You can choose to wipe the device's data during deprovisioning to ensure no company data remains.

Other options like 'Reset,' 'Disable,' or 'Powerwash' may have different effects:
Reset:Resets the device to factory settings but might not remove management if not done through the Admin console.
Disable:Prevents the user from signing in but doesn't remove policies or management.
Powerwash:Factory resets the device,removing all user data and configurations,including management.
Deprovision a device:https://support.google.com/chrome/a/answer/3523633

QUESTION 11
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. 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 lo all ChromeOS devices
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. Add a managed configuration using JSON to the Android app
D. Upload a JSON file with the configuration into the Google Play Store

Correct Answer: C
Section:
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.

QUESTION 12
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?

A. Configure a hostname allowlist, set up a TLS (or SSL) certificate, then verify TLS (or SSL) inspection is working
B. Reach out lo Google Workspace Security and Compliance for tailored configurations for your customer
C. Configure a transparent proxy, set up your allowlist to use * google com. then verify TLS (or SSL) inspection is working
D. ChromeOS devices are preconfigured to adhere to company TLS (or SSL) inspection by default and can therefore be deployed with no additional configuration

Correct Answer: A
Section:
Explanation:
To set up TLS (or SSL) inspection for web filtering on ChromeOS devices, you need to follow these steps:
Configure Hostname Allowlist:Create an allowlist of hostnames (e.g.,*.google.com,*[invalid URL removed]) that should bypass TLS inspection.This ensures that essential services like Google services and your own domain can function properly.
Set up TLS Certificate:Obtain the required TLS/SSL certificate from your web filter provider and install it on your web filter.ChromeOS devices need this certificate to establish a secure connection with the web filter for TLS inspection.
Verify TLS Inspection:Once the configuration is in place,test and verify that TLS inspection is working as expected.This involves checking if the web filter can correctly intercept and decrypt HTTPS traffic for websites not on the allowlist.
Why other options are not correct:
Option B:While reaching out to Google Workspace Security and Compliance can be helpful,it's not the primary step in setting up TLS inspection.The configuration needs to be done on the web filter and ChromeOS devices.
Option C:Transparent proxies are generally not recommended for ChromeOS devices as they can interfere with certain functionalities.While it might work with an allowlist for Google domains,it's not the best practice.
Option D:ChromeOS devices do not come preconfigured to adhere to company TLS inspection.This configuration needs to be set up explicitly by the administrator.

About TLS (or SSL) inspection on ChromeOS devices:https://support.google.com/chrome/a/answer/3504942
Verify TLS (or SSL) inspection works:https://support.google.com/chrome/a/answer/3504943

QUESTION 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 & Browser Security Settings' and set the 'Disallow incognito mode' policy
B. Go ,0 '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 vended access and incognito mode (or content protection

Correct Answer: A
Section:
Explanation:
Access the Google Admin Console: Sign in to the Admin console using your ChromeOS administrator credentials.
Locate User Settings: Navigate to 'Device Management' > 'Chrome Management' > 'User & browser settings'.
Find Incognito Mode Policy: Within the settings, search for 'Incognito mode'.
Disable Incognito Mode: Select the option to 'Disallow incognito mode'.
Save Changes: Click 'Save' to apply the policy to the designated users or organizational units.
Set up Chrome browser on managed devices: https://support.google.com/chrome/a/answer/3523633?hl=en

QUESTION 14
What format of certificate encoding is incompatible with ChromeOS devices?

A. PEM
B. CER
C. DER
D. CRT

Correct Answer: C
Section:
Explanation:
ChromeOS primarily uses the PEM format for certificate encoding. While it can handle other formats like CER and CRT, it does not support the DER format. DER is a binary format, while ChromeOS requires certificates in a text-based format.

QUESTION 15
A customer deploys a large number of ChromeOS devices and would like to start the process of turning on Zero-Touch Enrollment (ZTE) to streamline their deployment process. As an administrator, what would be required to enable ZTE?

A. Grant partner admin access
B. identify OU to place devices during enrollment
C. Create a zero-touch token
D. Create a pre-provisioning token

Correct Answer: B
Section:
Explanation:

Zero-touch enrollment (ZTE) automates the device enrollment process when users first power on their ChromeOS devices. Before you can enable ZTE, you need to determine the organizational unit (OU) where the devices should be placed during enrollment. This is crucial because different OUs can have different policies and configurations applied to them.
Plan Your OU Structure:If you haven't already,create a well-organized OU structure in your Google Admin console that reflects your organization's hierarchy and device management needs.
Select the Target OU:Choose the specific OU where you want the ZTE-enrolled devices to reside.Consider factors like department,location,or device type when making your decision.
Once you've identified the appropriate OU, you can proceed with creating a zero-touch enrollment token and associating it with that OU. This will ensure that newly enrolled devices are automatically placed in the correct OU and inherit the desired policies.

QUESTION 16
You are tasked with adding a security key to a single user account Where should you navigate to?

A. Users > Select User > Password
B. Users > Select User > Security
C. Security > 2-step Verification
D. Security > Password Management

Correct Answer: B
Section:
Explanation:
To add a security key to a specific user account in the Google Admin console, follow these steps:
Sign in to Google Admin console:Use your administrator credentials to access the console.
Navigate to Users:Click on 'Users' in the left sidebar to view the list of users in your domain.
Select User:Choose the specific user account to which you want to add the security key.
Go to Security Tab:In the user's profile,click on the 'Security' tab.
Add Security Key:Under the '2-Step Verification' section,you'll find the option to add a security key.Follow the on-screen instructions to register the security key with the user's account.
This method allows you to manage the security settings of individual users, including the addition of security keys for enhanced login protection.

QUESTION 17
How would you deploy a Progressive Web Application to all managed user accounts?

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

Correct Answer: A
Section:
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.

QUESTION 18
How would you deploy your 'Terms of Services' page to all managed ChromeOS devices?

A. Navigate to 'Chrome Verified Access' and enable the policy for content protection
B. Go to 'User & Browser and 'Managed Guest Session' settings to upload your terms of service
C. In 'User & Browser Settings' upload the 'Terms of Service' as a wallpaper
D. Navigate to 'User & Browser' and 'Managed Guest Session' settings to upload your custom avatar

Correct Answer: B
Section:
Explanation:
Go to the Google Admin console.
Navigate to 'Device Management' > 'Chrome Management' > 'User & browser settings'.
Find the section for 'Managed Guest Session'.
Locate the setting for 'Terms of Service'.
Upload your 'Terms of Service' document in plain text format.
This will present your Terms of Service to users when they log in as a guest on any managed ChromeOS device.
Why other options are incorrect:
A . Chrome Verified Access: This is for controlling access to corporate resources, not displaying terms of service.
C . Wallpaper: Using the wallpaper to display terms of service is not practical or user-friendly.
D . Custom avatar: The avatar is for user personalization and not related to terms of service.

QUESTION 19
Your network administrator wants to block Google services traffic. What is the result?

A. Google Search will not work
B. Chrome devices will crash
C. Chrome devices will not be able to reach Google
D. Nothing This isn't an issue

Correct Answer: A
Section:
Explanation:
Blocking Google services traffic will prevent Chrome devices from accessing any Google-owned domains, including google.com. This will directly impact Google Search, as it relies on communication with Google servers to provide results.
Other Google services like Gmail, YouTube, Google Drive, etc., will also be inaccessible. However, the Chrome device itself will not crash, as it can still function with other websites and applications.

QUESTION 20
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?

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

Correct Answer: C
Section:
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 21
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?

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.

Correct Answer: A
Section:
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 22
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 integration with current technological standards and practices can be worked on with trusted Google partners
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 will need a rollout and execution plan commensurate with hardware supply availability

Correct Answer: C
Section:
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 with an internet connection. This flexibility enhances productivity and collaboration.
Simplified Orchestration: ChromeOS devices are centrally managed through the Google Admin console, simplifying device deployment, configuration, and updates. This reduces IT overhead and streamlines device management processes.
Option A is relevant but not a primary organizational objective. While partner collaboration can be beneficial, the focus should be on how ChromeOS directly improves the organization's operations.
Option B is incorrect because verifying the terms of the Chrome Online Agreement is a legal requirement, not a strategic objective.
Option D is relevant but not as impactful as the other objectives. While a rollout plan is necessary, the focus should be on the long-term benefits of ChromeOS for the organization.
Chrome Enterprise overview: https://chromeenterprise.google/

QUESTION 23
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

Correct Answer: D
Section:
Explanation:
To prevent a ChromeOS device from shutting down while idling on the sign-in screen, you need to adjust the power management settings. This can be done through the following steps:
Go to the Google Admin console.
Navigate to Device Management > Chrome Management > Device Settings.
Find the Power management section and locate the setting that controls idle behavior on the sign-in screen.
Adjust the setting to prevent shutdown during idle periods.
Option A is incorrect because idle settings primarily control screen dimming and sleep behavior.
Option B is incorrect because user experience settings generally focus on visual and interaction aspects, not power management.
Option C is incorrect because there isn't a specific 'Allow shutdown' setting in ChromeOS device settings.