



- Expert Verified, Online, **Free**.



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

As an administrator, you would like the ability to see and test upcoming changes to the Google Admin console. How would an admin get access to pre-release features and upcoming ChromeOS device management changes to the Admin console?

- A. Enroll in the ChromeOS Factory Software Platform
- B. Join the Chrome Enterprise BETA Testing
- C. Register for the Chrome Enterprise Trusted Tester Program
- D. Create a ChromeOS Developer Account

**Suggested Answer:** C

*Community vote distribution*

C (100%)

🗨️ 👤 **moha413** 6 months, 3 weeks ago

**Selected Answer: C**

To get access to pre-release features and upcoming ChromeOS device management changes in the Admin console, registering for the Chrome Enterprise Trusted Tester Program is the best option

upvoted 1 times


What are two ways customers can open a support case for ChromeOS? (Choose two.)

- A. Chat support via the Admin console
- B. Contact the device manufacturer
- C. File feedback on the device with Alt + Shift + i
- D. File case through Customer Care Portal
- E. Send an email to ChromeOS support

**Suggested Answer:** AD

*Community vote distribution*

AD (100%)

 **moha413** 6 months, 3 weeks ago

**Selected Answer:** AD

A. Chat support via the Admin console: For customers with a ChromeOS enterprise or education account, they can access support directly through the Admin console, including chat support with Google support agents.

D. File case through Customer Care Portal: Google also provides a Customer Care Portal where customers can open and track support cases for their ChromeOS devices.

upvoted 1 times

An admin wants to use a custom extension to install a client certificate on a ChromeOS device so that it can connect to the corporate Wi-Fi. Which step is necessary to accomplish this?

- A. Install on the device via guest mode
- B. Distribute through the Chrome Web Store
- C. Force-install to the device
- D. Encode the certificate in DER-encoded format

**Suggested Answer:** C

*Community vote distribution*

C (100%)

🗨️ 👤 **moha413** 6 months, 3 weeks ago

**Selected Answer: C**

To install a custom extension or application that is necessary for connecting to a corporate Wi-Fi network (such as a client certificate) on ChromeOS devices, force-installing the extension ensures that it is automatically installed on the device without requiring user intervention.

As an admin, you would configure this in the Google Admin Console to force-install the extension for the managed devices. This approach guarantees that the certificate and necessary configurations are installed on the device, allowing it to connect securely to the corporate network.

upvoted 1 times

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 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

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **moha413** 6 months, 3 weeks ago

**Selected Answer: A**

As a ChromeOS administrator, you can block incognito mode by configuring a user policy in the Google Admin Console. The steps would involve:

Navigating to Users & Browser Security Settings in the Admin Console.

Finding the option to set the "Disallow incognito mode" policy, which prevents users from accessing incognito mode in the Chrome browser.

upvoted 1 times


Which management feature makes ChromeOS devices a popular choice for IT administrators in educational organizations and 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

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **moha413** 6 months, 3 weeks ago

**Selected Answer: C**

One of the primary reasons ChromeOS devices are popular in educational organizations and enterprises is their centralized management capability through the Google Admin Console. This feature allows IT administrators to manage and configure settings for large numbers of devices remotely. Administrators can enforce policies, deploy apps, manage security settings, and monitor device status, all from a single web-based interface. This centralized management simplifies device administration, making it more scalable and efficient.

upvoted 1 times

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? (Choose two.)

- 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 ZTE
- 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

**Suggested Answer:** AB

*Community vote distribution*

AB (100%)

🗨️ 👤 **moha413** 6 months, 3 weeks ago

**Selected Answer: AB**

Generate a ZTE pre-provision enrollment token for your specified device OU:

This step involves generating an enrollment token for the specific device organizational unit (OU) in the Google Admin Console. This token ensures that the devices, when they first connect to the internet, will automatically enroll into the correct OU based on the token settings.

Give the company domain name to your Chrome Partner to enable ZTE:

In order to use ZTE, your organization must be set up with a Chrome Partner. The Chrome Partner (usually a reseller or OEM) will need your company domain name to associate the devices you purchase with your Google Admin Console and enable the ZTE process

upvoted 1 times


What is a feature of Verified Boot?

- A. Makes sure that the firmware and OS have not been tampered with
- B. Protects anonymous guests from using the device
- C. Eliminates the need for strict policy controls
- D. Prevents the user from accessing unauthorized websites

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **moha413** 6 months, 3 weeks ago

**Selected Answer: A**

Verified Boot is a security feature in ChromeOS that ensures the integrity of the operating system and firmware. It verifies that the OS and system files have not been tampered with or corrupted during the boot process. If any modification or unauthorized change is detected, the system will attempt to recover to a trusted state. This helps protect the device from malware or unauthorized changes that could compromise its security.

upvoted 1 times

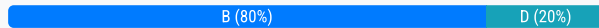


The security department has been informed that a ChromeOS device was stolen out of an employee's car. What should you do in the Admin console to ensure the device is rendered inoperable while still maintaining management of the device?

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

**Suggested Answer: B**

Community vote distribution



🗳️ 👤 **juansfunes** 4 months, 2 weeks ago

**Selected Answer: B**

Disable the device is the correct answer. If you deprovision the device you give free access to wipe and reuse the device and there is no way to enroll it back with

out the physical device making it loss forever.

upvoted 1 times

🗳️ 👤 **flokra** 6 months, 1 week ago

**Selected Answer: B**

Disabling the device will render it unusable.

This prevents any unauthorized access to the device and its data.

upvoted 3 times

🗳️ 👤 **moha413** 6 months, 3 weeks ago

**Selected Answer: D**

D. Deprovision the ChromeOS device

Explanation:

To ensure the device is rendered inoperable while still maintaining management over the device in the Admin console, you should deprovision the device.

When you deprovision a ChromeOS device, it effectively removes it from your domain and renders it unusable. The device will be wiped of all enterprise data, policies, and configurations. This ensures that the device can't be used to access any company resources. However, it does not physically destroy the device or remove it from the Admin console immediately; it just prevents it from being used in your organization's environment.

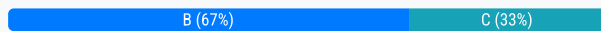
upvoted 1 times

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

**Suggested Answer: B**

*Community vote distribution*



**a5f0d39** 6 months, 2 weeks ago

**Selected Answer: B**

There's a Setting in Devices > Settings > Users & Browsers to Upload Terms that users must agree to.  
upvoted 1 times

**a5f0d39** 6 months, 2 weeks ago

**Selected Answer: C**

There's a Setting in Devices > Settings > Users & Browsers to Upload Terms that users must agree to.  
upvoted 1 times

**moha413** 6 months, 3 weeks ago

**Selected Answer: B**

To deploy a Terms of Service (ToS) page to all managed ChromeOS devices, you can use the Managed Guest Session (MGS) settings within the Google Admin Console. In the Managed Guest Session settings, there is an option to display a custom Terms of Service (ToS) page before users can sign in to the device. This is a common method for organizations to ensure users acknowledge the terms and conditions when they first use a device, especially for guest users or shared devices.

upvoted 1 times

You have a number of applications that you rely upon. You want to ensure that your applications continue to run smoothly with each new version of Chrome. What should you do?

- A. Ask users to provide feedback on the applications within a week of a new Chrome release.
- B. Advise them to take no action. All applications are automatically supported on the latest version of Chrome.
- C. Always install the latest version of those applications when they become available so they are always compatible with the latest version of Chrome.
- D. Implement a QA strategy and put their IT group and 5% of users on the beta channel of ChromeOS so they can find and report bugs early for upcoming Chrome releases.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗨️ 👤 **moha413** 6 months, 3 weeks ago

**Selected Answer: D**

it's important to have a proactive approach to testing new releases before they are rolled out to all users. The best practice is to implement a Quality Assurance (QA) strategy that includes putting a small group of users (like IT staff or a select group of end users) on the beta channel of ChromeOS. This way, you can catch compatibility issues and bugs with upcoming ChromeOS versions before they are deployed to everyone.

upvoted 1 times

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 to 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.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **serialx86** 5 months ago

**Selected Answer: A**

When deploying ChromeOS devices in an environment that requires web filtering with TLS (or SSL) inspection, you must ensure that these devices trust the inspection process while maintaining proper security controls. The best practice involves:

Configuring a hostname allowlist – This ensures that critical ChromeOS services (such as system updates and device policies) are not blocked or broken by SSL inspection.

Setting up a TLS/SSL certificate – You must deploy a trusted root CA certificate to all managed ChromeOS devices via the Google Admin console. This allows devices to trust the SSL/TLS inspection process.

Verifying TLS/SSL inspection – Test web filtering and SSL interception to confirm that the policies work without breaking key ChromeOS functionalities.

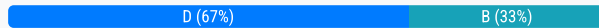
upvoted 1 times

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

**Suggested Answer: D**

Community vote distribution



🗉 👤 **information\_technology\_tim** 4 months, 3 weeks ago

**Selected Answer: D**

The answer is D

according to the zero-touch enrollment for chrome OS devices pdf, there are 7 steps.

1. purchase the chrome OS device
2. generate a pre-provisioning token
3. partner registers device with Google
4. device is shipped to the user
5. user powers on the device
6. Google confirms device identity
7. the user can now log in

upvoted 1 times

🗉 👤 **sushil1607** 5 months ago

**Selected Answer: B**

To enable Zero-Touch Enrollment (ZTE) for ChromeOS devices, you need to set up the Organizational Units (OUs) to which the devices will be assigned during the enrollment process. This allows for the streamlined deployment of devices, as they can be automatically placed into the correct OU based on the configuration during the setup.

While other steps like creating a token (option C) are part of the process, identifying the OUs is a key requirement for Zero-Touch Enrollment to work.

upvoted 1 times

🗉 👤 **moha413** 6 months, 3 weeks ago

**Selected Answer: D**

To enable Zero-Touch Enrollment (ZTE) for ChromeOS devices, you need to create a pre-provisioning token. This token is crucial because it allows devices to be automatically enrolled into the Google Admin Console and placed into a specific organizational unit (OU) when they are first powered on, without requiring manual intervention from administrators

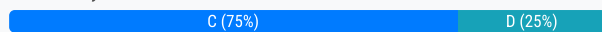
upvoted 1 times

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

**Suggested Answer: C**

Community vote distribution



🗳️ 👤 **jaxclain** 1 month, 3 weeks ago

**Selected Answer: C**

C. Move to a Long-term Support channel

Here's why:

Long-Term Support (LTS) Channel, Reduces Changes, Maintains Security, Reduces Risk of Unexpected Change, Minimizes Admin Workload, Entire Domain.

upvoted 1 times

🗳️ 👤 **flokra** 6 months, 2 weeks ago

**Selected Answer: D**

An update rollout plan allows for a phased rollout of Chrome OS updates to a small subset of devices first.

This enables administrators to:

Monitor for any unexpected issues with the new update on a limited scale.

Identify and mitigate any potential problems before rolling out the update to the entire fleet.

Reduce the impact of a problematic update by limiting the number of affected devices.

upvoted 1 times

🗳️ 👤 **a5f0d39** 6 months, 2 weeks ago

**Selected Answer: C**

Moving to LTS would be the least amount of administration while applying less OS Changes and maintaining security updates.

<https://support.google.com/chrome/a/answer/3168106?hl=en>

upvoted 1 times

🗳️ 👤 **n2183712847** 7 months, 1 week ago

**Selected Answer: C**

Long-term support

upvoted 1 times

🗳️ 👤 **Quinas** 8 months ago

Answer should be D

Update rollout plans in the Google Admin console allow administrators to gradually roll out ChromeOS updates to a subset of devices first. This allows for testing in a controlled environment before deploying to the entire fleet, reducing the risk of unexpected issues impacting all devices.

Steps to add an update rollout plan:

Access Google Admin Console: Sign in with your administrator credentials.

Navigate to Device Management: Go to Devices > Chrome > Settings > Updates.

Create Rollout Plan: Click on "Add an update rollout plan."

Select Devices: Choose the specific devices or organizational units (OUs) to include in the initial rollout.

Set Timeline: Define the start and end dates for the rollout.

Save and Apply: Save the plan and apply it to the selected devices.

upvoted 2 times

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.

**Suggested Answer:** C

*Community vote distribution*

C (100%)

  **casuarz** 6 months ago

**Selected Answer:** C

Explanation:

Blocking Google services traffic in the network will prevent ChromeOS devices from accessing Google's services, such as Google Search, Gmail, Drive, or any other Google-hosted services.

upvoted 1 times



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 identity provider-initiated login for Google authentication
- B. 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
- C. Enable SAML-based Single Sign-On for each application via Chrome App Management
- D. Use Chrome App Builder to enable SSO for application and force-install the application using ChromeOS user policies

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **flokra** 6 months, 1 week ago

**Selected Answer: B**

B. 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

This approach allows for seamless Single Sign-On across various applications and services. Here's why:

**Centralized Authentication:** By enabling SAML-based SSO for ChromeOS devices, you establish a single point of authentication for all users.

**Cookie Transfer:** Setting the SSO cookie behavior to enable transfer ensures that the user's authentication credentials (represented by the SAML cookie) are automatically used to access other applications and services that rely on the same identity provider.

**Improved User Experience:** Users only need to authenticate once, eliminating the need to repeatedly enter their credentials for different applications.  
upvoted 1 times

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

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

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. Delete sublevel OUs and only work from the top level OU
- B. Disable auto updates
- C. Override the inheritance for a given policy
- D. Force inheritance from top level OU to all OUs

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

You are setting up ChromeOS devices in a public library and need to prevent your ChromeOS devices from sleeping when not in use. How would you set up your policy to achieve this?

- A. In "Power management settings" apply "Do not allow device to sleep/shut down when idle on the sign-in screen"
- B. In "User & Browser Settings" for Power and shutdown set the policy to "Do not allow wake locks"
- C. In "Power management settings" set the policy to "Only allow users to turn off the device using the physical power button"
- D. In "Managed Guest Session settings", set the maximum user session length to "unlimited"

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

An organization was recently hacked through an admin's choice of an operating system. Leadership decides to move to Chromebooks for their security.



While the organization waits for Chromebooks to be delivered, what will allow them to continue using their existing devices securely?

- A. ChromeOS Readiness Guide
- B. ChromeOS Managed Browser
- C. ChromeOS Bytes
- D. ChromeOS Flex

**Suggested Answer:** D

*Community vote distribution*

D (100%)

  **flokra** 6 months, 1 week ago

**Selected Answer:** D

ChromeOS Flex is designed to bring the ChromeOS experience to existing devices.

This would allow the organization to continue using their current hardware while they transition to Chromebooks.

ChromeOS Flex offers many of the same security features as ChromeOS, such as sandboxing applications and regular security updates.

upvoted 1 times

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?

- 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 Android app that you want from "Apps & extensions"
- C. 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 the "Apps & extensions" page, add the Android app on the security team user OU and select "Force Install + pin to ChromeOS taskbar"

**Suggested Answer: B**

*Community vote distribution*

B (100%)

serialx86 5 months ago

**Selected Answer: B**

As a ChromeOS Administrator, if you need to allow only a specific Android app while blocking all others, you should use the Google Admin Console to apply a managed allowlist policy for Android apps on ChromeOS.

Steps to Achieve This:

Go to Google Admin Console → Devices > Chrome > Settings > Users & Browsers

Locate the Google Play Store settings

Enable "Block all apps, admin manages allowlist"

Go to "Apps & Extensions" → Add the specific Android app you want to allow

Save and apply the policy to the Organizational Unit (OU) of the security team

upvoted 1 times

serialx86 5 months ago

**Selected Answer: B**

As a ChromeOS Administrator, if you need to allow only a specific Android app while b

upvoted 1 times

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

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

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **serialx86** 5 months ago

**Selected Answer: A**

If you need to remove a ChromeOS device from management policy updates, you must deprovision the device in the Google Admin Console. This action removes the device from enterprise management, preventing it from receiving new policies and updates.

Steps to Deprovision a ChromeOS Device:

Go to Google Admin Console → Devices > Chrome > Devices

Find and select the device you want to remove

Click "Deprovision"

Select the appropriate deprovisioning reason (e.g., device is lost, retired, or being reassigned)

Confirm the action

Once a device is deprovisioned, it will no longer receive enterprise policies and must be re-enrolled to regain management.

upvoted 1 times



You want to enterprise enroll a device that has existing consumer accounts. What should you do first?

- A. Contact Google support to convert the device into an enterprise device
- B. Delete all consumer accounts, and then follow the same steps for enrolling a brand new device
- C. Follow the same steps for enrolling a brand new device
- D. Wipe the device

**Suggested Answer:** D

Community vote distribution

D (67%)

B (33%)

🗳️ 👤 **jaxclain** 1 month, 3 weeks ago

**Selected Answer: D**

I believe that Wiping the device would be enough, you don't need to delete the accounts and then wipe the device, it makes no sense to do that, just wipe the device and start the enrollment process.

upvoted 1 times

🗳️ 👤 **serialx86** 5 months ago

**Selected Answer: B**

B. Check subscriptions in billing

Explanation:

To view the number and type of ChromeOS upgrades purchased and in use by your domain, the Billing section in the Google Admin Console provides the relevant information regarding subscriptions. This includes the number of licenses purchased, the types of upgrades (such as ChromeOS Enterprise), and usage details.

Steps to Check Subscriptions in Billing:

Go to Google Admin Console → Billing

Select the Subscriptions tab

Review the details for ChromeOS upgrades, including the number of licenses in use, license types, and renewal information

upvoted 1 times

🗳️ 👤 **flokra** 6 months, 1 week ago

**Selected Answer: D**

D. Wipe the device

Before you can enterprise enroll a device that has existing consumer accounts, you must wipe the device.

Wiping the device will erase all existing data and settings, including any consumer accounts.

Once the device is wiped, you can proceed with the standard enterprise enrollment process.

upvoted 1 times



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

**Suggested Answer: A**

*Community vote distribution*

B (100%)

  **a5f0d39** 6 months, 2 weeks ago

**Selected Answer: B**

Under Billing > Subscriptions you can find Subscribing Upgrade type, Status, and Licenses  
upvoted 2 times

What are two methods for signing in to a Chrome OS device? (Choose two.)

- A. SMS code sent to mobile phone
- B. Single sign-on
- C. Google Friend Connect
- D. Facebook Connect
- E. Google Account username and password (with optional 2-factor)

**Suggested Answer:** *BE*

Currently there are no comments in this discussion, be the first to comment!

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 to 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.

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **jaxclain** 1 month, 3 weeks ago

**Selected Answer: C**

Managed Configurations (App Config):

This is the standard Android Enterprise way for developers to allow IT admins to remotely configure their apps.

If the VPN app developer has implemented support for managed configurations (which most enterprise-focused VPN clients do), they will expose specific keys (like hostname, port, username\_template, etc.) that you can set.

You define these settings as key-value pairs, often structured in JSON, within the Google Admin console when you approve and configure the app for deployment.

When the app is pushed to the ChromeOS devices, it automatically receives and applies these configurations.

upvoted 1 times

🗳️ 👤 **serialx86** 5 months ago

**Selected Answer: C**

C. Add a managed configuration using JSON to the Android app.

Explanation:

To automatically configure Android VPN clients with the correct hostname on ChromeOS devices, the best practice is to use a Managed Configuration. This is done via the Google Admin Console, where you can apply JSON-based configurations to Android apps deployed on managed ChromeOS devices.

Steps to Configure Android VPN Client via JSON:

Go to Google Admin Console → Devices > Chrome > Apps & Extensions

Locate and select the Android VPN app you are deploying

Click on "Managed Configurations"

Enter the JSON configuration with the correct hostname and settings

Save and deploy the configuration to the relevant Organizational Units (OUs)

upvoted 1 times

You need to get to the enterprise enrollment screen. What should you do?

- A. Press Ctrl-Alt-E during the Chrome bootup sequence (Chrome logo animation)
- B. Sign in with enterprise enrollment credentials provided by the customer at the user sign-in screen
- C. Press Ctrl-Alt-E on the initial welcome screen to set initial settings
- D. Press Ctrl-Alt-E at the user login screen before any user has signed in to the device

**Suggested Answer:** D

*Community vote distribution*

D (100%)

 **serialx86** 5 months ago

**Selected Answer:** D

D. Press Ctrl-Alt-E at the user login screen before any user has signed in to the device.

Explanation:

To enroll a ChromeOS device into enterprise management, you need to access the Enterprise Enrollment screen. The correct method is to press Ctrl + Alt + E at the user login screen, before any user has signed in.

Steps for Enterprise Enrollment:

Power on the ChromeOS device

At the initial login screen, do not sign in

Press Ctrl + Alt + E to bring up the Enterprise Enrollment screen

Enter the enterprise credentials (provided by the administrator)

Complete the enrollment process

upvoted 1 times

You are using a third-party service for SSO. Users are confused when signing onto a Chrome device because they are asked for Google account details before being redirected to the sign-in screen for your SSO provider. Which setting must be changed so managed devices open the SSO provider login page by default?

- A. SAML single sign-on login frequency
- B. SAML single sign-on password synchronization flows
- C. Single sign-on cookie behavior
- D. Single sign-on IdP redirection

**Suggested Answer:** D

*Community vote distribution*

D (100%)

serialx86 5 months ago

**Selected Answer:** D

D. Single sign-on IdP redirection

Explanation:

When using a third-party SSO (Single Sign-On) provider for authentication, ChromeOS devices may first prompt users for their Google account details before redirecting them to the SSO login page. To skip the Google login prompt and go directly to the SSO provider's sign-in page, you need to enable Single sign-on IdP redirection in the Google Admin Console.

How to Enable IdP Redirection for ChromeOS Devices:

Go to Google Admin Console → Devices > Chrome > Settings > Users & browsers

Locate Single sign-on IdP redirection

Enable the setting to force redirection to the SSO provider

Save and apply changes to the appropriate Organizational Unit (OU)

upvoted 1 times

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

**Suggested Answer: A**

*Community vote distribution*

C (100%)

 **serialx86** 5 months ago

**Selected Answer: C**

C. ChromeOS allows for advanced security, flexible access, and simplified orchestration within the business.

Explanation:

When considering ChromeOS devices as part of a hardware refresh, key organizational objectives should focus on security, accessibility, and management. ChromeOS is designed for enterprise environments, offering:

- ✓ Advanced Security – Built-in security features like sandboxing, verified boot, and enforced updates.
  - ✓ Flexible Access – Cloud-based management and seamless access to corporate resources.
  - ✓ Simplified Orchestration – Centralized administration via Google Admin Console for device provisioning, policy enforcement, and updates.
- upvoted 1 times

An admin is setting up third-party SSO for their organization as the super admin. When they test with their account, they do not see the SSO screen.

What is causing this behavior?

- A. SSO settings are misconfigured
- B. The account is in the wrong OrgUnit
- C. Third-party SSO is not enabled
- D. Super admin bypassed the third-party

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!



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

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!



What format of certificate encoding is incompatible with ChromeOS devices?

- A. PEM
- B. CERC. DER
- D. CRT

**Suggested Answer:** C

Community vote distribution

D (100%)

  **jaxclain** 1 month, 3 weeks ago

**Selected Answer: D**

Option C is not visible but here is the answer:

ChromeOS devices, particularly when managing certificates via the Google Admin console for trusted CAs (e.g., for TLS/SSL inspection or internal services), primarily support:

PEM (.pem, .crt, .cer): This is a Base64 encoded ASCII format, very common.

DER (.der, .cer): This is a binary encoding of the certificate.

PKCS#7 / P7B (.p7b, .p7c): This format can contain a certificate or a chain of certificates, often used for distributing CA chains.

The format that is generally incompatible or problematic, especially for uploading CA certificates (certificates you want devices to trust) via the Admin Console, is:

PKCS#12 (.p12, .pfx)

upvoted 1 times

You are tasked with converting hundreds of Windows & Mac machines across multiple locations to ChromeOS Flex and enrolling them into the Admin console. The available network bandwidth is limited at many of the locations and the devices are not currently managed with any endpoint management system. Which two operations are required to perform the task? (Choose two.)

- A. Create a dedicated enrollment account for each location and place them into the OUs you want the devices enrolled into. Then enable the "Place ChromeOS device in user organization" policy and enroll the devices using the respective enrollment account for each location.
- B. Install the Recovery Tool extension on all devices that are to be converted, and follow the step-by-step installer to convert each device directly without the need of USB drives.
- C. Use PXE boot to load the ChromeOS Flex image onto devices and have them automatically convert across all locations after they're restarted.
- D. Contact an authorized Zero-Touch Enrollment (ZTE) reseller and share the serial numbers of the devices you're converting and the domain you're enrolling them into to have them pre-provisioned into the Admin console.
- E. Distribute USB flash drives with the ChromeOS Flex image to the different locations and ask local personnel or a services partner to manually convert each device.

**Suggested Answer:** *AE*

Currently there are no comments in this discussion, be the first to comment!

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. Enable the "User and Browser Settings" and update "Maximum user session length" to any time up to 24 hours
- B. Create a corporate policy stating the users are to manually sign out after the end of every shift
- C. You can remotely access each device and sign out of the user account using Chrome Remote Desktop
- D. 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

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

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

- A. Single sign-on IdP redirection
- B. Device off hours
- C. User Data (Ephemeral)
- D. Family Link accounts
- E. Sign-in Restrictions

**Suggested Answer:** *BE*

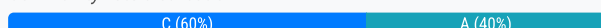
Currently there are no comments in this discussion, be the first to comment!

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", 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", 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".

**Suggested Answer: C**

Community vote distribution



**serialx86** 4 months, 3 weeks ago

**Selected Answer: A**

This approach follows Google's best practices, ensuring that most users remain on the Stable channel, receiving tested and secure updates. At the same time, it allows the IT team to use the Beta channel, giving them early access to new features and allowing them to evaluate compatibility issues before the update reaches all users.

upvoted 1 times

**Goodtechbiz2** 6 months ago

**Selected Answer: C**

Google's best practices for ChromeOS updates recommend evaluating compatibility with future updates while ensuring access to new features without disrupting operations:

**Stable Channel for Most Users:** The majority of the organization's devices should remain on the Stable channel for the most reliable and well-tested ChromeOS experience.

**Beta Channel for Testing:** A small subset (e.g., 5%) of devices across multiple departments should be placed on the Beta channel to test new features and ensure compatibility with organizational tools and workflows. This approach allows IT teams to identify and resolve potential issues before the update is rolled out broadly.

upvoted 2 times

**a5f0d39** 6 months, 2 weeks ago

**Selected Answer: C**

Google Specifically recommends putting 5% of Users in the Beta Channel.

"Note: We recommend that you keep most of your users on the latest stable release of Chrome OS or the Long-term support (LTS) channel and 5% of your users on the Beta channel. You may choose to also keep your IT team on the Beta or Dev channels."

<https://support.google.com/a/answer/9028950?hl=en#zippy=%2Cchrome>

upvoted 1 times

**bl01** 10 months, 2 weeks ago

**Selected Answer: A**

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.

upvoted 1 times

Help Desk administrators need a limited set of privileges to perform actions in the Google Admin console. How should an administrator grant these permissions while conforming to the practice of least privilege?

- A. Create a Service Desk Group and add Service Desk admins to the group
- B. Create a new custom admin role and assign
- C. Grant service desk administrators the Services Admin Role
- D. Allow Help Desk administrators full access to manage users

**Suggested Answer:** B

*Community vote distribution*

B (100%)

serialx86 4 months, 3 weeks ago

**Selected Answer: B**

To follow the principle of least privilege, you should grant only the necessary permissions required for the Help Desk administrators to perform their tasks.

By creating a custom admin role, you can specifically tailor the permissions to give them limited access without providing full access to sensitive settings or actions outside their scope.

upvoted 1 times


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

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **serialx86** 4 months, 3 weeks ago

**Selected Answer: A**

To deploy a Progressive Web Application (PWA) to all managed user accounts in your organization, you can force-install the PWA by adding its URL to the Chrome Apps & Extensions page in the Google Admin Console. This ensures that the PWA is automatically installed on users' devices when they sign in, and it is available for use.

upvoted 1 times



A user reports that their Chrome device has been stolen. What should the administrator do?

- A. Use the Google Admin console to turn on the stolen Chromebook's webcam
- B. Use the Google Android Device Manager to locate the Chromebook
- C. Set the stolen Chromebook to disabled mode to prevent user sign-ins
- D. Remotely wipe user data from the Chromebook

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **serialx86** 4 months, 3 weeks ago

**Selected Answer: C**

The best immediate action to take when a Chromebook is stolen is to disable the device to prevent unauthorized users from signing in and accessing sensitive information.

By using the Google Admin Console, the administrator can disable the Chromebook so that no one can use it to access the user's account or data, thus securing the device from misuse.

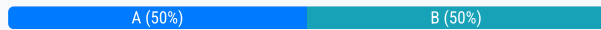
upvoted 1 times


Which site isolation policy will enable site isolation for your entire organization?

- A. SitePerProcess
- B. IsolateOrigins
- C. IsolatePerProcess
- D. SiteOrigins

**Suggested Answer: A**

*Community vote distribution*



 **jaxclain** 1 month, 3 weeks ago


**Selected Answer: A**

The policy that enables site isolation for all websites (effectively for your entire organization's browsing sessions) is A. SitePerProcess.

Here's why:

SitePerProcess: This is the policy that enforces full Site Isolation. When enabled, Chrome creates a dedicated renderer process for each site a user visits. This is the most comprehensive form of site isolation

upvoted 1 times

 **serialx86** 4 months, 3 weeks ago

**Selected Answer: B**

✓ B. IsolateOrigins

Explanation:

The IsolateOrigins policy is used to enable site isolation for your entire organization. This policy ensures that sites are isolated from one another in separate processes to improve security and prevent cross-site attacks.

upvoted 1 times

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

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗳️ 👤 **jaxclain** 1 month, 3 weeks ago

**Selected Answer: D**

D. Device Settings > Power management

Here's why:

Device Settings: The behavior of the device on the sign-in screen (before any user logs in) is controlled by Device Settings, not User Settings. User settings apply after a user has signed in.

Power management: This section within Device Settings contains policies that dictate how the device behaves in terms of power, including what happens when it's idle.

Specifically, within Devices > Chrome > Settings > Device > Power management, you would look for settings like:

upvoted 1 times

🗳️ 👤 **jaxclain** 1 month, 3 weeks ago

Action on idle on AC power (sign-in screen)

Action on idle on battery (sign-in screen)

You would set these to "Do nothing" or "Sleep" instead of "Shutdown" to prevent the device from shutting down while idling on the sign-in screen.

upvoted 1 times

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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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?

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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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

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

**Suggested Answer:** *DE*

Currently there are no comments in this discussion, be the first to comment!

Your hardware OEM issues a recall for a safety issue. You need to deprovision devices from management before returning to the OEM. They will replace your existing ChromeOS devices with a different model. Which option should you choose when deprovisioning to make sure you can reuse your Chrome Education/Enterprise Upgrade and remain compliant?

- A. Retiring from fleet
- B. Different model replacement
- C. ChromeOS Flex upgrade transfer
- D. Same model replacement

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

At a specific location in your organization, users cannot log in to their ChromeOS devices. The ChromeOS Administrator has also noticed that devices have not synced in the past 24 hours. You have updated policies in the Admin console for your fleet of ChromeOS devices, but the devices are not getting the updated policies. What is a probable change in the environment that can cause these issues?

- A. A different location enrolled a large number of new devices
- B. Your network administrator has blocked all network traffic to Google services
- C. Your root Certificate Authority expired
- D. Your organization's licenses have recently expired

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!



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

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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

What is a best practice for admin accounts on the Google Admin console?

- A. Super Admins should be used for all changes to the domain
- B. Group Admins should have 2FA enabled only if given security policy controls
- C. Super Admins should use a separate user account for day-to-day activities
- D. Group Admins should have access to multiple groups

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

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 role
- D. Create Custom role under Chrome management and assign Manage ChromeOS devices role

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **jaxclain** 1 month, 3 weeks ago

**Selected Answer: B**

B. Create Custom role under Chrome management and assign Telemetry API role

Here's why:

Custom Role: This is essential for granting granular, least-privilege access. Pre-built roles might provide too much or not exactly the right permissions.

Under Chrome management: This ensures the role is specific to ChromeOS device administration.

Assign Telemetry API role (or a similar "View ChromeOS Devices" / "Read ChromeOS Device Information" privilege):

The "Telemetry API" privilege typically grants read-only access to device information, attributes, and status. This is exactly what's needed for interns to see info without being able to manage or update.

upvoted 1 times

The security team is requiring Wi-Fi connectivity to be disabled on ChromeOS devices. Using the Google Admin console, how would you configure ChromeOS devices to block all Wi-Fi connectivity and hide the Wi-Fi icon?

- A. Configure "Restricted Wi-Fi Networks"
- B. Prevent WiMax connectivity
- C. Remove Wi-Fi from "Enabled network interfaces"
- D. Restrict "Auto Connecting" to Wi-Fi

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

You have been tasked with selecting a 3rd party IdP to allow logging into ChromeOS devices. Your ChromeOS devices are displaying an "Unable to sign in to Google" message. How should you troubleshoot this?

- A. Ensure the identity provider is using an SAML compliant connection
- B. Check Multi-Factor Authentication for the user account in the Google Admin console
- C. Disable the SSO connection in the Google Admin console
- D. Apply the SSO certificate to the ChromeOS device

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗨️ 👤 **jaxclain** 1 month, 3 weeks ago

**Selected Answer: A**

A. Ensure the identity provider is using an SAML compliant connection

Here's why:

SAML (Security Assertion Markup Language) is the protocol: This is the standard that allows the 3rd party IdP to communicate authentication and authorization data to Google (the Service Provider in this case). If the SAML assertion sent by the IdP is malformed, missing required attributes (like NameID), incorrectly signed, or if the endpoints are misconfigured, Google will not be able to process the sign-in attempt and will show an error.

"Unable to sign in to Google" often points to Google receiving an assertion but being unable to validate or understand it.

upvoted 1 times

You are enrolling several devices to send to a remote location. How can you ensure that these devices will automatically connect to the wireless network at the remote location when powered on for the first time?

- A. Add the wireless network credentials to the "Networks" section in the Admin console ensuring that they are applied to the ChromeOS devices By Device
- B. Use the Google Zero-Touch Enrollment (ZTE) process and generate the provisioning token by clicking on the "Enroll device" button in the Admin console "Devices" page
- C. During the enrollment process, add the wireless credentials manually to each device in the Admin console ensuring that they are applied to ChromeOS devices By User
- D. Add the wireless network credentials to the "Networks" section in the Admin console ensuring that they are applied to the ChromeOS devices By User

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

You are a ChromeOS Administrator of a school district. While working with a teacher in one of the schools, they mention they are having issues downloading files on their ChromeOS device. What are some ways you can help troubleshoot with the least amount of disruption to the user?

- A. Run Diagnostics from the ChromeOS device to troubleshoot
- B. Check how much storage is being used on the device then delete or move files that aren't needed anymore
- C. Reset the user's ChromeOS device to its original factory settings
- D. Check for system updates If any updates are available, install them

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

You have been asked to explain the built-in security features of ChromeOS. What is 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 started up

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!



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

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!


Which setting is required to restrict Chrome Remote Desktop use to only accounts on your domain?

- A. Firewall traversal
- B. URL Blocking
- C. Remote access clients
- D. Chrome Remote Desktop service

**Suggested Answer:** D

*Community vote distribution*

C (100%)

 **a5f0d39** 6 months, 2 weeks ago

**Selected Answer: C**

Remote access clients

Available on ChromeOS devices.

Configures the required domain name for remote access clients and prevents users from changing the setting. Only clients from the specified domain can connect to the host device. Left blank, the host allows connections from authorized users from any domain.

<https://support.google.com/chrome/a/answer/2657289?hl=en#zippy=%2Cremote-access-clients>

upvoted 1 times

You are asked why ChromeOS devices do not require additional antivirus software. How should you respond?

- A. Every time ChromeOS updates, it automatically updates the antivirus software on the device
- B. Every ChromeOS device is pre-installed with antivirus software which automatically updates during the life of the device
- C. As part of a multi-layered security approach ChromeOS uses a read-only operating system which cannot be affected by viruses
- D. The Admin console automatically deploys antivirus software to enrolled ChromeOS devices and is included in the Chrome Enterprise/Education Upgrade

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

What is needed for an admin to remote desktop to a user or managed guest session devices with the Admin console?

- A. The user must accept the connection request
- B. The user must share the session pin with the admin
- C. Both the admin and the remote device must be on the same network
- D. The admin must be in the same OU as the remote device

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

When setting up a Chrome Enterprise trial, what is a benefit of choosing to verify the domain?

- A. Identity management
- B. Application management
- C. Network management
- D. Device management

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

An organization decides to move to ChromeOS. The organization spans three continents and 30 countries. Each are may have different policy settings depending on local laws.

- A. Configure geofencing by location of IP address and assign to groups
- B. Use Google Groups for root level settings and override with OUs
- C. Design an OU structure from broadest bucket of policy setting to narrowest
- D. Set all policies at the office location level

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

An organization changes their logo. The admin needs to update the desktop wallpaper of devices.

Which group of settings should the admin navigate to when implementing this change?

- A. Device
- B. User & browser
- C. Managed guest session
- D. Desktop

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!



To put a device in kiosk mode, which setting must be enabled in Apps & extensions?

- A. Set auto-launch app to the app to be used
- B. Select the correct group when adding the app
- C. Pin the version to the latest version
- D. Select the correct OU when adding the app

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

What are two benefits of purchasing a Chromebook with a bundled license? (Choose two.)

- A. The license follows the device between domains
- B. The license grants advanced security benefits
- C. The license is valid for the life of the product
- D. The license extends the AUE of the device
- E. The license can be transferred to other devices after AUE

**Suggested Answer:** *CD*

Currently there are no comments in this discussion, be the first to comment!

A user is experiencing odd issues related to their device displaying a distorted picture on the screen.

What is the first step they can take to possibly resolve this?

- A. Powerwash the device
- B. Run a virus scan
- C. Reinstall the operating system

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

You are managing the "Customer Kiosk" child organization and need to pin devices to maintain stability and security. How would you configure your Chrome update settings to achieve this?

- A. Long-term Support Candidate channel.
- B. Long-term Support channel.
- C. Choose the "Beta channel".
- D. Select the "Stable channel".

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

A global organization is deploying a fleet of ChromeOS devices to all their users. Organization policy requires all web traffic to be filtered using an existing proxy service to prevent access to 1 million unauthorized websites. What ChromeOS policy should you configure to meet this requirement?

- A. "Always use the proxy specified below", and provide the IP:port to the proxy services.
- B. "Always use the proxy auto-config specified below", and provide the IP:port information.
- C. "Always use the proxy specified below", and provide the URL to pac file configuration.
- D. "Always use a network access control deny" policy to deny the URLs.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

The finance Department is concerned about frequent Chromebook updates and asks you to explore a 6-month update cycle. Which update release option should you configure for these devices?

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

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

What are the minimum device hardware requirements required to test or install ChromeOS Flex?

- A. Intel/AMD x86-64-bit compatible device or ARM based processor, 2GB RAM, 8GB internal storage.
- B. Intel/AMD x86-64-bit compatible device, 4GB RAM, 16GB internal storage.
- C. Intel/AMD x86-64-bit compatible device, 2GB RAM, 8GB internal storage
- D. Intel/AMD x86-64-bit compatible device or ARM based processor, 4GB RAM, 16GB internal storage

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!