Free Questions for ChromeOS-Administrator by certsinside

Shared by Vaughan on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Choose 2 answers

Options:

A- Go to Device Settings

B- Go lo 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 coned device model to a USB stick

Answer:

D, E

Explanation:

To create a recovery image on a USB stick, you need to:

Access Chrome Web Store:Open the Chrome Web Store on a Chrome device (either a Chromebook or a computer with the Chrome browser installed).

Install Chromebook Recovery Utility:Search for and install the 'Chromebook Recovery Utility' extension.

Launch the Utility:Open the installed extension.

Identify Device:Enter the model number of the ChromeOS device for which you want to create the recovery image.

Insert USB Stick:Insert a USB stick with sufficient storage capacity (at least 4GB).

Download and Create:Follow the on-screen instructions in the utility to download the correct recovery image and create the bootable USB stick.

This process will prepare a USB stick that can be used to recover or reinstall ChromeOS on a device that is not functioning properly.

Recover your Chromebook:https://support.google.com/chromebook/answer/1080595?hl=en

Question 2

Question Type: **MultipleChoice**

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

Options:

A- Force-install the Progressive Web Application URL in the 'Chrome Apps & extensions' page

B- Set up Chrome Imprivata shared apps & extensions to force-install the Progressive Web Application URL

C- Go to 'User & Browser Settings' and add the Progressive Web Application URL in the 'Legacy Browser Support' site list

D- Open 'Additional Google services' to force-install the Progressive Web Application URL

Answer:

A

Explanation:

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

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

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

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

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

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

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

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

Question 3

Question Type: MultipleChoice

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

Options:

A- Users > Select User > Password

B- Users > Select User > Security

C- Security > 2-step Verification

D- Security > Password Management

Answer:

B

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 4

Question Type: **MultipleChoice**

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?

Options:

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

Answer:

B

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 5

Question Type: MultipleChoice

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

Options:

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 tor day-to-day activities

D- Group Admins should have access to multiple groups

Answer:

C

Explanation:

The principle of least privilege dictates that users should only have the minimum access necessary to perform their job functions. This applies to super admins as well. Using a separate user account for daily activities reduces the risk of accidental misconfiguration or unauthorized changes due to the elevated privileges associated with the super admin role.

Security:By using a separate account,super admins limit the potential attack surface in case their regular account is compromised.

Accountability:It's easier to track actions and changes when different accounts are used for different purposes.

Recovery:If the super admin account is locked or disabled,having a separate account allows for easier recovery.

Question 6

Question Type: MultipleChoice

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

Options:

A- From the 'Apps & extensions' page add the Android app on the security team user OU

B- On the 'Users & Browser Settings'' tab. for the Play Store, use the 'Block all apps, admin manages allowlist' policy and allow only the

C- Android app that you want from 'Apps & extensions ' On the 'Users & Browser Settings'' tab. for the Chrome Web Store use the 'Block all apps, admin manages allowlist' policy and allow only the Android app that you want on 'Apps & extensions '

D- From trio 'Apps & extensions' page add the Android app on the security team user OU and select 'Force Install * pin to ChromeOS taskbar'

Answer:

B

Explanation:

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

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

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

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

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

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

Question 7

Question Type: MultipleChoice

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?

Options:

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 ChromeQS Developer Account

Answer:

C

Explanation:

The Chrome Enterprise Trusted Tester Program is designed for administrators who want early access to pre-release features and changes in the Google Admin console, including those related to ChromeOS device management. By joining this program, administrators can:

Test New Features:Get hands-on experience with upcoming features and changes before they are officially released.

Provide Feedback:Share feedback directly with Google's product teams,helping to shape the development and prioritization of new functionalities.

Stay Ahead:Be among the first to know about new capabilities and improvements in the Google Admin console.

How to Register:

Visit the Chrome Enterprise Trusted Tester Program website:https://inthecloud.withgoogle.com/trusted-testers/sign-up.html

Fill out the registration form with your organization's details.

Google will review your application and,if approved,provide you with access to pre-release features.

Become a Chrome Enterprise Trusted Tester:https://support.google.com/chrome/a/answer/9036081?hl=en

Question 8

Question Type: MultipleChoice

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?

Options:

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 lo the ChromeOS device

Answer:

A

Explanation:

The error message 'Unable to sign in to Google' in the context of 3rd party IdP login typically points towards an issue with the SAML (Security Assertion Markup Language) connection. SAML is the standard protocol used for authentication between ChromeOS devices and external identity providers.

Here's a breakdown of troubleshooting steps:

Verify SAML Compliance:The most critical step is to ensure that the 3rd party IdP is configured correctly to use SAML 2.0 and is adhering to the required SAML attributes and formatting.

Check IdP Configuration:Review the SAML configuration settings in both the Google Admin console (under Security > Set up single sign-on (SSO) with a third party IdP) and the 3rd party IdP's administration portal.Ensure that the entity IDs,SSO URLs,and certificate information match exactly.

Test SAML Connection:Use a SAML testing tool (e.g.,SAML Tracer) to simulate the login process and inspect the SAML assertions.This can help pinpoint any errors or inconsistencies in the SAML response.

Google Admin Console Logs:Check the Google Admin console logs for any relevant error messages related to the SAML authentication process.

Contact IdP Support:If the issue persists,reach out to the support team of your 3rd party IdP for further assistance.They may have specific troubleshooting steps or logs to help diagnose the problem.

Set up single sign-on (SSO) with a third party IdP:https://support.google.com/a/answer/60224