Google.Chrome-Enterprise-Administrator.v2025-06-18.q18

Exam Code:	Chrome-Enterprise-Administrator
Exam Name:	Professional Chrome Enterprise Administrator Certification Exam
Certification Provider:	Google
Free Question Number:	18
Version:	v2025-06-18
# of views:	128
# of Questions views:	180
https://www.freeqas.com/qa/Google/Chrome-Enterprise-Administrator/Google.Chrome-Enterprise-Administrator.v2025-06-18.q18.html	

NEW QUESTION: 1
A company uses Chrome Enterprise Core to manage Chrome browsers for its employees and contractors who share devices They need a way to ensure the following:
* Full-Time Employees (FTEs) can only see and use extensions assigned to them
* Contractors can only see and use extensions assigned to them
* Both FTEs and contractors have access to a set of shared extensions
How can the Chrome administrator configure Chrome Enterprise Core to achieve this'?
A. Create Organizational Units (OUs) for Shared devices, assign shared extensions to the OU. Use Group Policy Objects to assign specific extensions by user group
B. Create separate groups in the Google Admin Console for FTEs and Contractors. Assign extensions to respective groups based on their needs
C. Ask users to install all the extensions they need on the shared device
D. Create Organizational Units (OUs) for Shared devices, assign shared extensions to the OU. Create a separate group in the Google Admin Console for FTEs. Assign extensions to the group based on their needs
Answer: (SHOW ANSWER)
The most effective way to manage extensions in this scenario is to use a combination of OUs and groups.
Create an OU for the shared devices and force-install the shared extensions at this OU level. Then, create separate user groups for FTEs and Contractors in the Google Admin console and force-install their specific extensions to these groups. User group policies have a higher precedence than OU policies, ensuring the correct extensions are available to each user type when they sign in to the shared devices. Option A mentions Group Policy

Objects, which are for Windows environments and less relevant in a cloud-managed scenario across potentially different OSes. Option B doesn't address the shared device aspect effectively. Option C is not a managed approach.

NEW QUESTION: 2
A small business wants to have all of their macOS devices enroll in Chrome Enterprise Core. They do not have a Mobile Device Management solution but do maintain a base image for their Mac computers Where should they put the enrollment token*?
A. HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome \CloudManagementEnrollmentToken
B. /Library/Google/Chrome/CloudManagementEnrollmentToken
C. /etc/opt/chrome/policies/enrollment/CloudManagementEnrollmentToken
D. /Library/Google/Chrome/Enrollment/DeviceManagementToken
Answer: B (LEAVE A REPLY)
For macOS devices without MDM, the enrollment token can be embedded in the base image. The correct path for placing the cloud management enrollment token on macOS is `/Library/Google/Chrome /CloudManagementEnrollmentToken`. The other paths listed are for Windows Registry (A), a non-standard Linux path (C), and a potentially incorrect macOS path (D).

NEW QUESTION: 3
A company is reviewing the permissions of extensions that are popular among employees The security team wants to make sure all extensions in the environment have these capabilities disabled:
* Modify to internal home page: `internal.acme.com`
* Access to the storage
* Access to history
Which actions should be taken in the company default extension Permissions and URLs fields to meet the security team's requirements?
A. Add `*.acme.com` to runtime blocked hosts; Disable storage permission; Disable history permission
B. Add `*.acme.com` to runtime blocked hosts; Enable storage permission; Enable history permission
C. Add `internal.acme.com` to runtime blocked hosts; Disable storage permission; Disable history permission
D. Add `internal.acme.com` to runtime blocked hosts; Enable storage permission; Enable history permission
Answer: (SHOW ANSWER)
To prevent extensions from modifying the internal homepage, the administrator should add `*.acme.com` to the "Runtime blocked hosts" list. The wildcard `*` ensures that any attempt to access or modify this domain by an extension will be blocked at runtime. Additionally, to

disable access to storage and history, the administrator needs to explicitly disable the "Storage" and "History" permissions within the extension management settings. Therefore, the correct combination is to block the host and disable the permissions.

NEW QUESTION: 4
An organization relies heavily on Chrome browser for daily operations News breaks about two critical hardware vulnerabilities These vulnerabilities allow attackers to potentially access sensitive information stored in the browser's memory, even across different websites and processes Which specific Chrome Enterprise Core policy would an administrator implement to help mitigate the risks?
A. Require Hardware-backed Key Generation for TLS
B. Update Chrome browser to the latest stable version
C. Manage Cross-Origin Extensions by Blocking all except an allowlist
D. Enable Site isolation for every website
Answer: (SHOW ANSWER)
The scenario describes vulnerabilities that could allow cross-site data leakage within the browser's memory.
"Site isolation for every website" is a security feature in Chrome that isolates the rendering process for each website, preventing one site from accessing the data of another, even if a vulnerability is exploited. This policy directly addresses the risk of cross-site information leakage due to memory vulnerabilities. Option A relates to TLS security, option B is a general security best practice but doesn't directly prevent cross-site memory access, and option C manages extension behavior, not core browser memory isolation.

NEW QUESTION: 5
A company deploys policies in a hybrid manner from both on premises and the Google Admin console How would policies set in chrome://policy?
A. Level: Mandatory, Source: Platform
B. Applies To: Machine, Source: Cloud
C. Level: Mandatory, Source: Cloud
D. Level: Recommended, Source: Cloud
Answer: C (LEAVE A REPLY)
When viewing applied Chrome policies in the `chrome://policy` internal page, policies enforced through Chrome Enterprise Core (the cloud management console) will typically be labeled with a "Source" of
"Cloud." If the administrator has enforced the policy, the "Level" will likely be "Mandatory," indicating that users cannot change this setting. "Platform" would refer to policies set locally on the operating system (like Group Policy on Windows). "Recommended" policies are suggestions that users can typically override.

NEW QUESTION: 6

An administrator decides to shorten the default time that a browser may be inactive before automatic deletion from the Google Admin console What policy must be selected for the Device Token Management policy to allow devices to re-enroll in the Google Admin console?

A. Revoke Token

B. Invalidate Token

C. Renew Token

D. Delete Token

Answer: C (LEAVE A REPLY)

When managing inactive device tokens, the "Renew Token" option is crucial for allowing devices to re-enroll after a period of inactivity. If the token is revoked, invalidated, or deleted, the device will likely require a manual re-enrollment process. Renewing the token provides a mechanism for the device to check back in and remain managed.

NEW QUESTION: 7

An organization using Chrome browser on Windows has policies from group policy and Chrome Enterprise Core.

In what order are the policies applied?

A. By the precedence hierarchy

B. From least restrictive to most restrictive

C. Cloud policy takes precedence

D. Group policy takes precedence

Answer: A (LEAVE A REPLY)

When both Group Policy (local machine policy) and Chrome Enterprise Core (cloud policy) are configured on a Windows device, the effective policy is determined by a defined order of precedence. Generally, cloud policies for managed browsers will override conflicting local policies. The specific precedence order is configurable, but it follows a hierarchical structure where certain policy sources take priority over others.

Options C and D present a simplified view that might not always be the case depending on the configuration.

Option B is a general principle of conflict resolution but doesn't describe the specific order in Chrome policy application.

NEW QUESTION: 8

A company has multiple departments, including Engineering, Marketing, Sales, and HR. Each department has different needs and schedules for Chrome updates. For instance, the Engineering team requires the latest updates as soon as they are available to ensure they have the latest features and security patches. However, the HR department prefers a more stable environment and only wants updates after they have been thoroughly tested.

Which feature in the Google Admin console can an administrator use to meet the company's requirements?

A. Create different user groups for each department
B. Create organizational units for each department
C. Set device policies for each department
D. Create active directory forest for each department
Answer: B (LEAVE A REPLY)
Organizational Units (OUs) in the Google Admin console allow administrators to apply different Chrome policies to different groups of devices or users based on their organizational structure. By creating separate OUs for Engineering and HR (and potentially other departments), the administrator can configure different Chrome update policies for each OU, ensuring Engineering gets rapid updates while HR stays on a more stable release. User groups primarily manage access to services, and device policies are generally applied at the device level, not necessarily tied to departmental needs for update cadences. Active Directory forests are a Microsoft concept and not directly used for managing Chrome update policies in the Google Admin console.

NEW QUESTION: 9
An organization experiences a recent surge in account takeovers and suspicious activity Upon investigation a security team discovers that employees are falling victim to infostealer malware specifically designed to target Chrome browser cookies This malware is spreading through phishing emails and compromised websites, and it is capable of stealing session cookies, login credentials,and other sensitive information stored in the browser Which measure can an administrator implement using Chrome Enterprise Core to mitigate the risks posed by cookie theft?
A. Block the use of third-party cookies
B. Require Enhanced Safe Browsing and enable Application Bound Encryption
C. Invalidate user's session cookies and tokens by resetting the sign-in cookies from the Google Admin console
D. Disallow Chrome Sync and Require Incognito mode
Answer: B (LEAVE A REPLY)
To combat cookie theft from infostealer malware, requiring "Enhanced Safe Browsing" provides proactive protection against malicious websites and downloads that might distribute such malware. Enabling
"Application Bound Encryption" adds an extra layer of security to cookies and other sensitive data stored by Chrome, making them harder for malware to use even if stolen. Blocking third-party cookies (option A) can improve privacy but doesn't directly prevent malware from stealing first-party session cookies. Invalidating existing cookies (option C) is a reactive measure and doesn't prevent future theft. Disallowing Chrome Sync and requiring Incognito mode (option D) changes user behavior but doesn't inherently protect against malware on the local machine.

NEW QUESTION: 10

Chrome Browser Cloud Management has been successfully implemented at a company for the past year.
Recently, the engineering team has received feedback from the security team that Chrome browsers are not meeting patching Service Level Agreements (SLAs). In the Insight report, the engineering team sees that 30% of their companies' browsers are pending updates.
Which browser policy could the engineering team implement to ensure better compliance with the security team's patching requirement?
A. Chrome browser updates
B. Relaunch notification
C. Google updater policy precedence
D. Auto-update check period
Answer: D (LEAVE A REPLY)
To ensure timely patching, the engineering team should adjust the "Auto-update check period" policy. By shortening this period, Chrome browsers will check for updates more frequently, increasing the likelihood of applying security patches sooner and improving compliance with patching SLAs. "Chrome browser updates" is a general category, "Relaunch notification" affects when users are prompted to restart, and "Google updater policy precedence" deals with the order of policy application, not the frequency of checks.

NEW QUESTION: 11
A user reports having frequent issues accessing corporate pages and logging into corporate applications After looking into user reports, it is determined that other users have reported similar issues over the past few months While the broader investigation is launched to identify and resolve the root cause, which Google Admin remote actions for managed Chrome browsers can be used to help alleviate such issues for the user?
A. Clear Cache; Clear Cookies; Clear Cache and Cookies
B. Clear Cookies; Restart Browser; Logout User
C. Clear Cache and Cookies; Delete Temporary Files; Restart User Session
D. Clear Cache; Delete Temporary Files; Delete Swap File
Answer: A (LEAVE A REPLY)
Clearing the browser's cache and cookies is a common first-line troubleshooting step for issues related to website access and login problems. Outdated or corrupted cached data and cookies can often interfere with website functionality and authentication processes.
The Google Admin console provides remote actions to
"Clear Cache," "Clear Cookies," or both. Options B, C, and D include actions that are either more disruptive (restart browser, logout user, restart user session) or not standard remote actions available for managed Chrome browsers through the Admin console (delete temporary files, delete swap file).

NEW QUESTION: 12

A Chrome administrator is using both Cloud policies and Local policies to apply settings to Chrome browsers The administrator wants to ensure that on Windows computers, the Cloud policies will have precedence if Cloud and Local policies conflict What Registry value can be created under HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google \Chrome to achieve this?

A. "Value: LocalPolicyOverride Type: REG_DWORD Data 0"

B. "Value: PolicyOverridePreference Type REG_SZ Data Cloud"

C. "Value: CloudPolicyOverridesPlatformPolicy Type REG_DWORD Data 1"

D. "Value PolicySupercedence Type REG_SZ Data Cloud"

Answer: (SHOW ANSWER)

To ensure cloud policies override local policies on Windows, the administrator needs to create a specific Registry value. The correct value is `"CloudPolicyOverridesPlatformPolicy"` of type `REG_DWORD` with data `1`. This setting explicitly tells the Chrome browser to prioritize cloud-managed policies over local policies.

NEW QUESTION: 13

An end user is returning from an extended leave of absence and finds their browser is no longer active The administrator is not sure if the inactivity policy has been violated What is the minimum action necessary to re-enroll this browser?

A. Verify the policy has been violated and then wipe the browser

B. Close and reopen Chrome

C. Delete the device management token and reopen Chrome

D. Delete the browser from CEC and reopen Chrome

Answer: C (LEAVE A REPLY)

If a browser becomes inactive due to policy, the device management token likely needs to be refreshed or re- established. Deleting the token and then reopening Chrome will typically trigger the browser to attempt re- enrollment and obtain a new token, bringing it back under management. Wiping the browser or deleting it from the CEC might be necessary in more severe cases but is not the minimum action. Simply closing and reopening Chrome might not be sufficient if the token has expired or been invalidated.

NEW QUESTION: 14

An external entity is conducting a penetration test on an organization's Chrome Browser environment They report that a significant number of Manifest V2 (MV2) extensions are installed none of which are critical to business operations IT leadership has requested either block or upgrade How should an administrator proceed?

A. Collect the extension IDs and configure an installation policy of block

B. Configure the Manifest V2 availability policy

C. Configure the installation mode to reflect removed for each extension ID

D. Auto-upgrade the extensions from MV2 to MV3

Answer: B (LEAVE A REPLY)

Given that the MV2 extensions are not critical, and the requirement is to either block or upgrade, the most direct and efficient approach is to configure the "Manifest V2 availability" policy. This policy allows administrators to control the usage of Manifest V2 extensions, including blocking them entirely or allowing them until a specified date. Option A involves manually collecting and blocking each extension, which is less efficient. Option C ("removed") is not a standard installation mode policy. Option D is not a policy that an administrator can directly configure; the upgrade to MV3 is a developer-driven process.

NEW QUESTION: 15
A Chrome administrator's organization has recently introduced a new security compliance requirement that mandates all software, including web browsers, be updated within 48 hours of a security patch release Which steps should the administrator take to ensure compliance with the new security requirement company wide'?
A. Implement a policy in the Google Admin console to force automatic updates and recommend Chrome relaunches to apply updates within the required timeframe
B. Rely on users to manually update their browsers within the required timeframe
C. Disable automatic updates and manually check all managed browsers for updates every 48 hours to comply with the new security requirements
D. Implement a policy in the Google Admin console to force automatic updates and ensure Chrome relaunches to apply updates within the required timeframe
Answer: (SHOW ANSWER)
To meet a strict 48-hour update requirement for security patches, the administrator must enforce automatic updates through the Google Admin console. Additionally, ensuring Chrome relaunches after updates are downloaded is crucial for applying the patches promptly. Recommending relaunches (option A) might not guarantee timely application. Relying on manual updates (option B) is unreliable and doesn't ensure compliance. Manually checking all browsers (option C) is not scalable or efficient for a company-wide deployment.

NEW QUESTION: 16
Which percentage of Chrome is recommended during Beta before general availability'?
A. 10%
B. 2%
C. 1%
D. 5%
Answer: D (LEAVE A REPLY)
While the exact percentage isn't explicitly stated in the provided material, industry best practices for software deployment, including browser updates, recommend testing in a Beta environment with a representative but limited subset of users before a full rollout. A common recommendation for Beta testing is around 5% of the user base. This provides sufficient feedback and issue detection without impacting the majority of users.

NEW QUESTION: 17
What policy and value provides the most protection against malicious websites?
A. Allow the user ability to bypass Safe Browsing warnings
B. Set the Safe Browsing policy to Enhanced mode
C. Set the site isolation policy to be required for all websites
D. Enable site isolation for all websites
Answer: B (LEAVE A REPLY)
Setting the **Safe Browsing policy to Enhanced mode** provides the most direct and comprehensive protection against malicious websites by leveraging Google's real-time threat intelligence. Allowing users to bypass warnings (option A) defeats the purpose of Safe Browsing. While site isolation (options C and D) protects against cross-site data leakage, it doesn't directly prevent users from accessing malicious sites in the first place. Enhanced Safe Browsing actively warns and blocks access to dangerous websites.

NEW QUESTION: 18
A systems engineer recently cloud enrolled Chrome browsers, which were previously managed via group policy, and deployed a policy through Chrome Enterprise Core. However, the policy is not applying. After validating the policy via chrome://policy, the status shows a warning conflict What is the best way to resolve this issue?
A. Restart the computer to apply the policy changes
B. Adjust the policy merge list setting
C. Check and configure the precedence order
D. Re-enroll the Chrome browser to reset the policy
Answer: C (LEAVE A REPLY)
A "warning conflict" in `chrome://policy` indicates that multiple policy sources are trying to control the same setting. Since the browsers were previously managed by Group Policy, there's likely a conflict between the cloud policy and the local Group Policy. The best way to resolve this is to **check and configure the precedence order** of policy sources. Ensure that Cloud Policy is set to have the desired precedence over Group Policy if that's

the intention. Restarting the computer might apply existing policies but won't resolve the conflict in precedence. Adjusting a "policy merge list setting" is not a standard term for resolving this type of conflict. Re-enrolling might give a fresh start but doesn't address the underlying conflict in policy sources.