PassQueen
a.k.a dumpsqueen.com

Professional Chrome Enterprise Administrator Certification Exam

Google Chrome-Enterprise-Administrator

Version Demo

Total Demo Questions: 6

Total Premium Questions: 66

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Managing Chrome browser	45
Topic 2, Managing Chrome Enterprise security	21
Total	66

QUESTION NO: 1

An organization routes web traffic through a security gateway that cannot inspect QUIC traffic. The gateway can inspect HTTPS traffic over TCP, but users can currently access external websites over UDP port 443 and bypass the expected inspection path.

Which Chrome policy should the administrator configure?

A. Disable QUIC

B. Disable DNS over HTTPS

C. Enable Site Isolation for every website

D. Require Enhanced Safe Browsing

ANSWER: A

Explanation:

Disable QUIC by configuring **QuicAllowed** to false. QUIC commonly uses UDP port 443. When QUIC is disabled, Chrome falls back to HTTPS over TCP where available, allowing traffic to use the organization's existing inspection path.

Disabling DNS over HTTPS affects how Chrome resolves domain names, not the transport protocol used for website traffic. Site Isolation and Safe Browsing provide important browser security protections, but neither prevents Chrome from using QUIC.

QUESTION NO: 2

A company reorganizes its browser-management structure. Several enrolled browsers must receive a new set of browser-level security policies that are assigned to a different managed browsers organizational unit. The browser users and their user-account organizational units will not change.

What should the administrator do?

A. Move the user accounts to the target organizational unit

B. Move the managed browser records to the target managed browsers organizational unit

C. Create a new enrollment token and reenroll every browser

D. Add the users to a Google Group without changing browser placement

ANSWER: B

Explanation:

Move the **managed browser records to the target managed browsers organizational unit** in the Google Admin console. Browser-level policies are assigned according to the organizational unit containing the enrolled browser. Moving the browser changes the browser policy scope without changing the user accounts that might sign in to it.

Moving user accounts affects user and profile policies, not the browser-level policies assigned to enrolled browsers. Creating a new enrollment token is not necessary merely to change the organizational unit of an already enrolled browser.

QUESTION NO: 3

An organization has a critical extension that is force-installed on managed Chrome browsers to meet specific security needs Additionally, the organization has specified that when extensions are unpublished from the Chrome Web Store, they are also disabled The extension has been taken over by a malicious actor and has been unpublished from the Chrome Web Store

What impact will this have to the force-installed extension?

A. The force-installed extension will be disabled for existing users only

B. The force-installed extension will automatically be disabled

C. The force-installed extension will observe no change

D. The admin will receive an alert in the Google Admin console to remediate the conflict

ANSWER: B

Explanation:

The force-installed extension will automatically be disabled. Chrome Enterprise provides the `ExtensionUnpublishedAvailability` policy to control what happens when an extension is unpublished from the Chrome Web Store. When the organization selects the behavior to disable unpublished extensions, Chrome applies that setting even to extensions deployed through force-install policy. Consequently, the extension remains subject to the organization's unpublished-extension protection rather than continuing to run simply because its installation was mandatory.

This setting is particularly important for the stated security scenario. Unpublishing can indicate that an extension is no longer available from its original trusted distribution source, including where it has been compromised or otherwise becomes unsuitable for use. Disabling it prevents the extension from running in managed Chrome while administrators investigate, remove the force-install assignment, or deploy a safe replacement. The policy behavior is enforced by Chrome on managed browsers after the unpublished status is recognized, helping reduce exposure from an extension that should no longer execute.

Google documents the policy and its available behaviors in the Chrome Enterprise policy reference. Administrators can configure extension deployment and related management settings in the Chrome Enterprise extension management documentation.

QUESTION NO: 4

In Chrome's Safe Browsing settings, which option provides the most robust protection againstonline threats and is suitable for a highly secure environment?

A. Advanced Threat Protection

B. Proactive Defense

C. Secure Browsing Mode

D. Enhanced Protection

ANSWER: D

Explanation:

Enhanced Protection is Chrome Safe Browsing's highest protection level and is appropriate where minimizing exposure to web-based threats is a priority. It provides more proactive protection against dangerous websites, downloads, and extensions, including enhanced checks that can identify threats that may not yet be included in standard blocklists. Chrome may also use additional security information, such as URLs and a small sample of page content or downloads, to improve threat detection and provide stronger warnings. This helps protect users from phishing, malware, malicious downloads, and harmful extensions with more timely detection than the standard setting. In a highly secure environment, administrators should assess privacy, data-handling, and organizational policy requirements before enabling it, because the enhanced service sends more security-related data to Google than Standard protection. Chrome Enterprise administrators can manage Safe Browsing behavior through Chrome policies and can use reporting and other enterprise controls alongside this setting as part of a broader security strategy. See Google's overview of Chrome Safe Browsing protection levels and the Chrome Enterprise documentation for SafeBrowsingProtectionLevel policy.

QUESTION NO: 5

An organization is migrating its management from Group Policy to Chrome Enterprise Core

When enrolling the browser into Chrome Enterprise Core, what will happen to conflicting policies on Windows when using the default order of precedence?

A. Cloud Machine policies will be ignored in favor of the Machine Policy

B. Machine Policies will be ignored in favor of cloud machine policy

C. OS User policies will be ignored in favor of the Cloud User policies

D. Machine Policy will be ignored if the token was deployed through Group Policy

ANSWER: B

Explanation:

Machine Policies will be ignored in favor of cloud machine policy. When a Windows Chrome browser is enrolled in Chrome Enterprise Core, it can receive browser-level policies from the cloud management service. Under Chrome's default policy-precedence behavior, cloud machine policies have a higher priority than platform machine policies configured locally through Windows Group Policy when both sources set the same browser policy. Consequently, the cloud value is the effective value applied by Chrome for that conflict.

This precedence is particularly useful during a migration because administrators can move policy administration to Chrome Enterprise Core without needing to remove every existing Group Policy setting before cloud policy is applied. The locally configured policy remains present in Windows, but Chrome resolves the conflict according to its documented policy-source precedence and enforces the cloud machine setting. Administrators can validate the effective value and identify its source on an enrolled browser by opening `chrome://policy`; this helps confirm that the browser is receiving and applying the intended cloud-managed configuration.

Google documents the hierarchy of Chrome policy sources, including the relationship between cloud and platform policies, in its Chrome policy precedence documentation. See also Google's Chrome policy management overview for how policies are deployed and evaluated.

QUESTION NO: 6

An organization wants to prevent users from installing any Chrome Web Store extensions by default. Two approved extensions must remain available for users to install when needed, and the security team does not want to force-install either extension.

Which configuration best meets this requirement?

A. Force-install the two approved extensions and leave all other extensions allowed

B. Block all extensions and do not configure any exceptions

C. Block `*` in the extension installation blocklist and add the two approved IDs to the allowlist

D. Add the two approved IDs to the allowlist and leave the blocklist empty

ANSWER: C

Explanation:

Configure an **extension installation blocklist containing * and add the two approved extension IDs to the extension installation allowlist**. The wildcard blocklist prevents installation of extensions generally, while the allowlist creates controlled exceptions for the approved extensions. Users can choose to install the approved extensions, but cannot install other Web Store extensions.

Force-installing the approved extensions would install them automatically and prevent user removal, which is not required. Allowlisting the two extensions without blocking all other extensions would still allow users to install unapproved extensions.