Implementation of Google Admin Console to Manage Chrome OS Devices

This document will begin with introducing the steps of obtaining a Google Admin trial account and elaborating some of the essential steps, e.g., planning your OUs before moving on to Chrome OS device enrollment as well as get an understanding of some of the device and managed Google account settings.

1. Mobile device administrators can apply for a 14-day trial subscription for Google Workspace with device management capability to carry out a try-out.

2. The registered Google Workspace account should be cancelled before the end of the trial to stop you from incurring charges for Google Workspace services.

3. Understand how the Organization Unit (OU) works in Google admin console

   Organization Unit (OU) – All users and devices are initially placed in the top-level OU. All settings that make in the Admin Console apply to that top-level OU. You can create a child OU and store the desired users and devices. This way, you can tailor settings for managed devices and managed users as needed.

   Apply settings to different users and devices

   The administrator can control which services and features are available to users or devices in your school. Services and features can be turned on or off for each organizational unit.

4. The Google Admin console administrator can uplift the control level by enabling advanced mobile device management to activate further device management capabilities, including, enforce encryption, use stronger password protection, and more.

5. Add the Wi-Fi profile of your premises to enable automatic Wi-Fi network assignment while signing in to the devices by users.

6. Configure Chrome Settings
   Device settings and policies can be tailored for all users and devices in your organization. You can tie the policies to the user's profile. User settings can be configured at User & browser settings under Chrome management. Whereas device policies can be configured at Device settings for the enrolled devices.

7. Administrator to configure the **Enrollment Permission policy** in "User & browser settings" under Device management to enable managed Google Workspace accounts to perform device enrollment. By default, users can enroll a new or re-enroll a deprovisioned device.

8. Users can self-enroll their ChromeOS devices with Chrome Enterprise/Education Upgrade right after accepting the end-user license agreement. Alternatively, when you turn on your Chromebook, and the sign-in screen appears, do not sign in with user credentials. Instead, press Ctrl+Alt+E on your keyboard to access the enrollment screen. A device license is required if an insufficient licensing message is prompted during the enrollment process.

9. Chrome Device is not enrollable if a user has signed in before enrollment. To resolve this issue, you need to wipe the device and restart enrollment.

10. Mass Enroll Chromebooks
    You can mass enroll devices running Chrome OS to speed up the enrollment process. The way to do mass enrollment is familiar with the way to manually enroll.

11. Automatically install apps and extensions on managed devices or accounts

    The Google Admin console administrator can force-install specific Chrome apps and extensions for users in your organization. Users cannot remove items that are force-installed. Use Apps & extensions under Chrome management to proceed with the installation.

12. What information can be seen by the device administrator

    The administrator can see each device's user and device details, including hardware and OS information, custom fields, and system activities.

- END -