ChromeOS

Chrome OS is a lightweight operating system developed by Google, primarily designed for Chromebook devices. It is based on the Linux kernel and primarily revolves around the Google Chrome web browser. Chrome OS is known for its simplicity, speed, and security. It focuses on cloud-based computing, with most applications and data stored and accessed through the Chrome web browser and cloud services. Chromebooks running Chrome OS offer a streamlined user experience, automatic updates, and integration with Google services such as Gmail, Google Drive, and Google Docs. With its emphasis on web-centric usage and cloud-based productivity, Chrome OS provides an efficient and secure computing environment for users who primarily rely on web-based applications and services.

- Chromebook Management
- Chrome OS: FileWave Inventory Extension Behavior (FAQ)
- Chrome Troubleshooting Guide
- Chrome OS: FileWave Inventory Extension Capabilities
- Disable Chrome OS in FileWave
- Powerwash / Wipe Users on ChromeOS (15.3+)
- Reboot for ChromeOS (15.3+)
- Google Admin Sync Interval for ChromeOS (15.3+)
- Custom Field Annotated Field Sync for ChromeOS (15.3+)
- Forcing wiped ChromeOS devices to re-enroll (15.3+)
- Confirming Firebase APIs are enabled for Chromebooks (15.4+)

Chromebook Management

FileWave has support for Chromebook management with the data that syncs from the Google Admin Console. Though this is not a total replacement for the Google Admin, FileWave does arm you with helpful tools and assets guaranteed to help your Chromebook deployment.

So what can we do?

With FileWave you will get all the same great inventory data you are used to with any other types of devices in FileWave. Maybe you would like to know how much disk space is left on those devices, or what user and at what time did they logged into any Chromebook? With FileWave all this data and more is available at your fingertips to run reports, scheduled email with this data, apply custom fields, or maybe you would like it easily exported out to a txt file.

Inventory is just the beginning of what you can do with Chromebooks in FileWave, you also have the ability to gather a location and then view it right in the FileWave Admin on a map.

How do I set all this up?

To start managing your Chromebooks in FileWave there is some backend and prep work that needs to be done:

1. Make sure you have Chromebook Licenses in FileWave, you can check this by selecting Activation Code under the Server menu in the FileWave Admin:
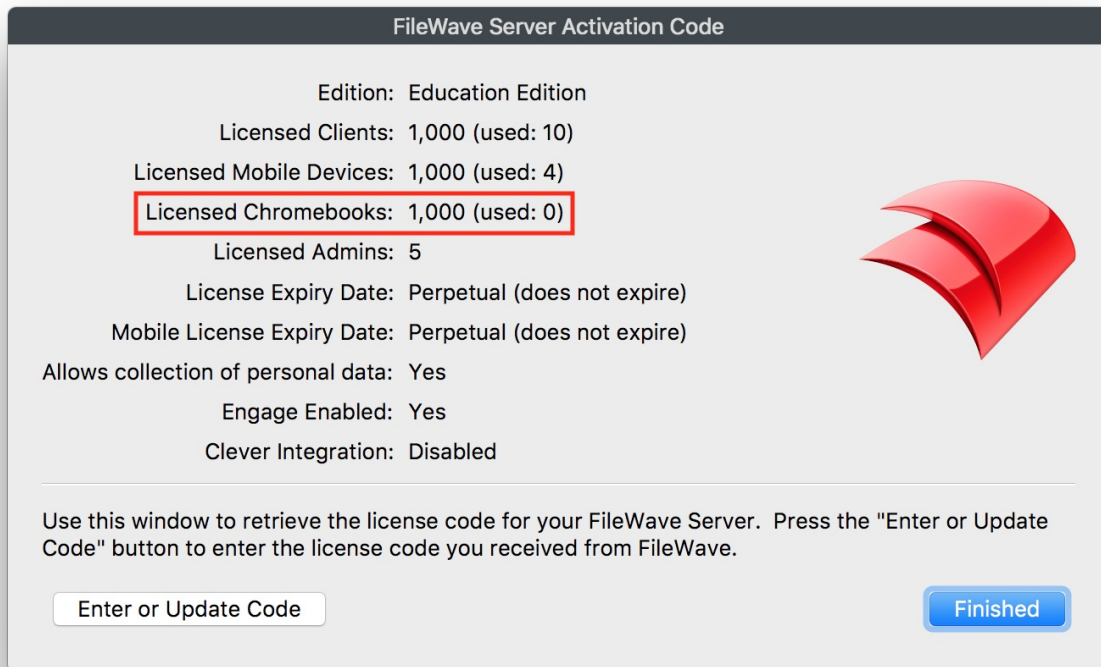
*You will need to be sure you have enough Chromebook licenses in FileWave to match the number of Devices you are managing in the Google Admin. We will sync over the full list of devices, and you will not be able to update the model if FileWave does not have sufficient licenses.

1. You will need to follow the Quick Start Guide linked here to fully sync with Google Admin and get your Chromebooks talking to FileWave: Quick Start Guide for Chromebooks

With all that done you will notice there is now a new group structure in your Clients view that you can see all of your sync Chromebook devices:

These devices and groups are synced with Google and therefore cannot be deleted directly out of FileWave.

Chrome OS: FileWave Inventory Extension Behavior (FAQ)

What

The FileWave Chromebook Inventory extension provides abilities to manage your devices beyond what can be done from the Google Admin console. Below you will find some answers to frequently asked questions about the extension's behavior.

When/Why

We'll use the Inventory Extension mainly to collect additional inventory data from our Chromebooks, but also to request updated inventory information and to initiate remote control sessions.

How Does it Work?

Q: How do I install the Inventory Extension?

A: Reference the following link to see how to install the Inventory extension: Quick Start Guide

Q: What does the Inventory Extension do?

A: Reference the following article for details on what the extension does: Chrome OS: FileWave Inventory Extension Capabilities

Q: How frequently does the extension report data?

A: The extension reports data based on the frequency specified in the JSON configuration file. It defaults to once per day, but is configurable by changing the value in the json

Q: Will the extension send data/verify no matter what?

A: No, there are a number of pre-requisites for data to be sent, as follows:

- Device must be on and connected to a network
- The device must not be in a sleep state
- A user must be logged into the device (the extension is executed in the user context)
- The extension must actually be installed for the user above
- The FileWave server must be reachable by the endpoint (i.e. if on the internet, the device must be able to reach the FW server)

Q: What will happen if the device is offline/off/asleep when it should send inventory?

A: Nothing immediately. But, when the device comes back online with a user logged in, it should submit inventory right away.

Q: Will the Inventory Extension work if the Chrome browser is not open?

A: It will not work in this case. The extensions is specifically a browser extension, so it only works with a user logged in and browser open.

Q: When I look in inventory, I see a last sync date and a last connected date. Why are these two dates different?

A: Last connected date is the more important and meaningful data. It tells you when the device last talked to your FileWave server directly (i.e. the extension talks to FW). Last sync date is the date/time at which the device last checked in with the Google Admin console.

Q: A lot of data comes to FileWave from the Google Admin Console. How frequently does this data get sent?

A: By default your FileWave server synchronizes with Google nightly at midnight. You can force an immediate on-demand synchronization from the Google preferences tab.

Q: When I look in the Google admin console, I see different data than what I see in FileWave for some data. Why?

A: Most likely this is because the data changed since the last Google→ FileWave synchronization. (See item above). But note, the device checks in with Google on a certain frequency, and then we sync with Google on another schedule, so there can be discrepancies simply based on time. A manual synchronization though should always bring the data up to date.

Related Content

- [Quick Start Guide for Chromebooks](#)
- [Chrome OS: FileWave Inventory Extension Capabilities](#)

Chrome Troubleshooting Guide

You have already:

- Enrolled devices into your Google Suite (https://support.google.com/chrome/a/answer/1360534?hl=en)
- Followed the Quick Start Guide for Chromebooks to install the extension on your devices
- Verified you have a license for Chrome devices

Problem

Having issues with Chrome OS devices communicating with FileWave Admin.

Solution

Verify Chrome extension is installed in the policy

Verify FileWave extension has registered with FCM/GCM by looking at the log

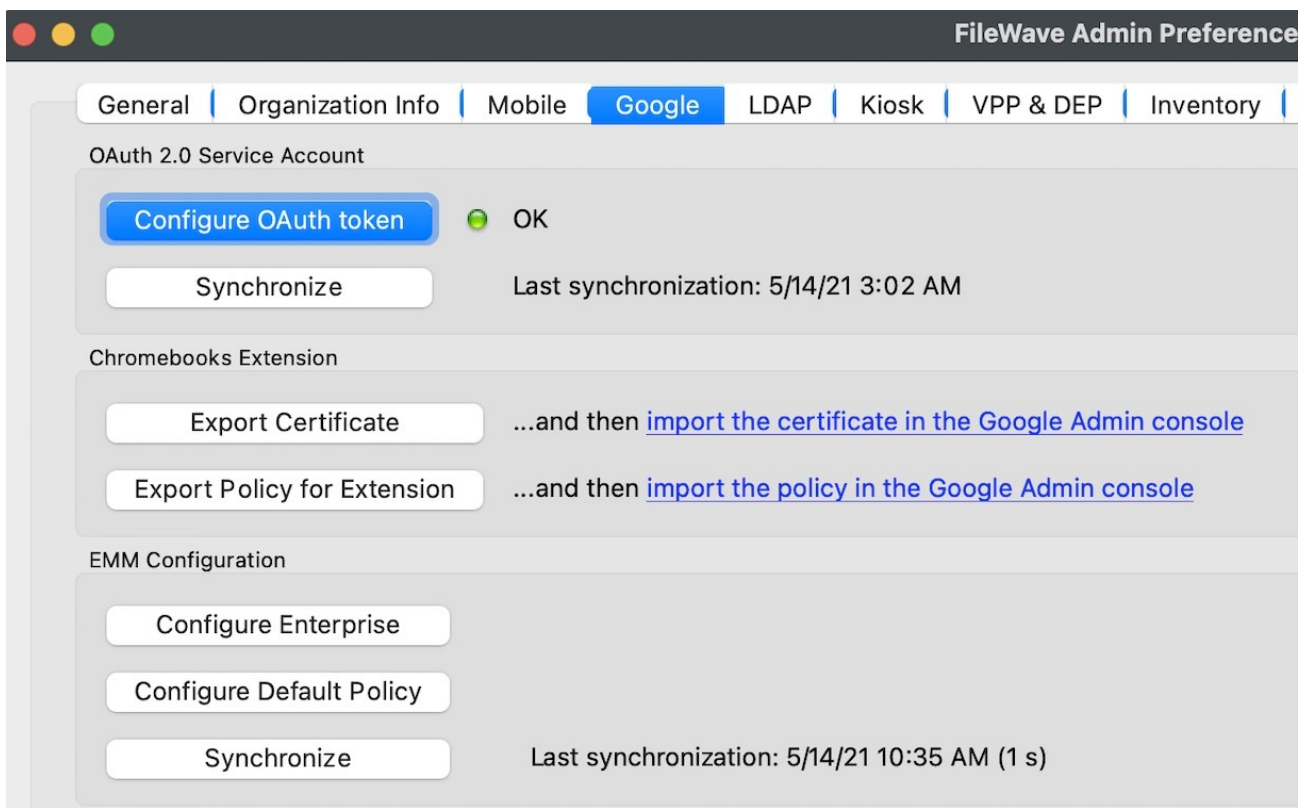## Devices are not showing at all in FileWave

1. In the native client open Preferences > Google as shown
2. Is the status icon not green? Anything other than green would indicate an issue
3. If you have a large number of ChromeOS devices it is possible that the server is timing out when trying to sync with Google. This can be especially true on the first sync
4. A solution is to edit this file on the FileWave server: /usr/local/filewave/apache/conf/httpd.conf
5. Look for a section in the file like this:

```
    # chrome app
    WSGIDaemonProcess chrome display-name=filewave-chrome processes=1 threads=2 python-
eggs=/usr/local/filewave/apache/.python-eggs shutdown-timeout=5 deadlock-timeout=300 inactivity-
timeout=3600 request-timeout=3600 socket-timeout=3600
```

6. Change the timeout values so that deadlock-timeout=600 but otherwise the values above should match your server. If any values are lower in your config you should make them at least match the above listed values
7. Restart everything with;

```
fwcontrol server restart
```

8. If the issue was a timeout then the sync should now complete. For about 50,000 devices the sync can take 10+ minutes to complete on first sync.
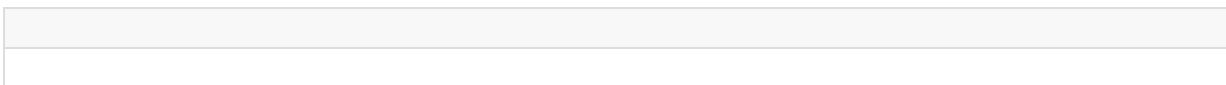
Devices are not showing Geolocation information in FileWave

If devices are showing in FileWave, but Geolocation details are not showing up, and possibly the FileWave Inventory Extension icon is not showing even if you set it to Force Install + Pin then you very likely enabled Geolocation as well as the Extension for an OU that only includes the Device, but not the User who is logging in. You must ensure that both OUs are enabled or put the User and Device in the same OU for testing. This should not be an issue if you have set Geolocation and the Inventory Extension enabled for your entire domain, but frequently when someone is evaluating FileWave they might enable it for only one OU for testing. If you do that then make sure that the User and Device are in that same testing OU.

View the device policy

1. Open a Google Chrome window
2. Browse to the URL: chrome://policy
3. Scroll down to ExtensionInstallForcelist and select show more
4. Look for the ID of the FileWave Inventory Extension (ldhgnmkjehdokljjhcpkbhcmhoficdio Figure 1.1)
5. If you see it there, scroll to the very bottom
6. There will be a whole section for the FileWave Inventory Extension
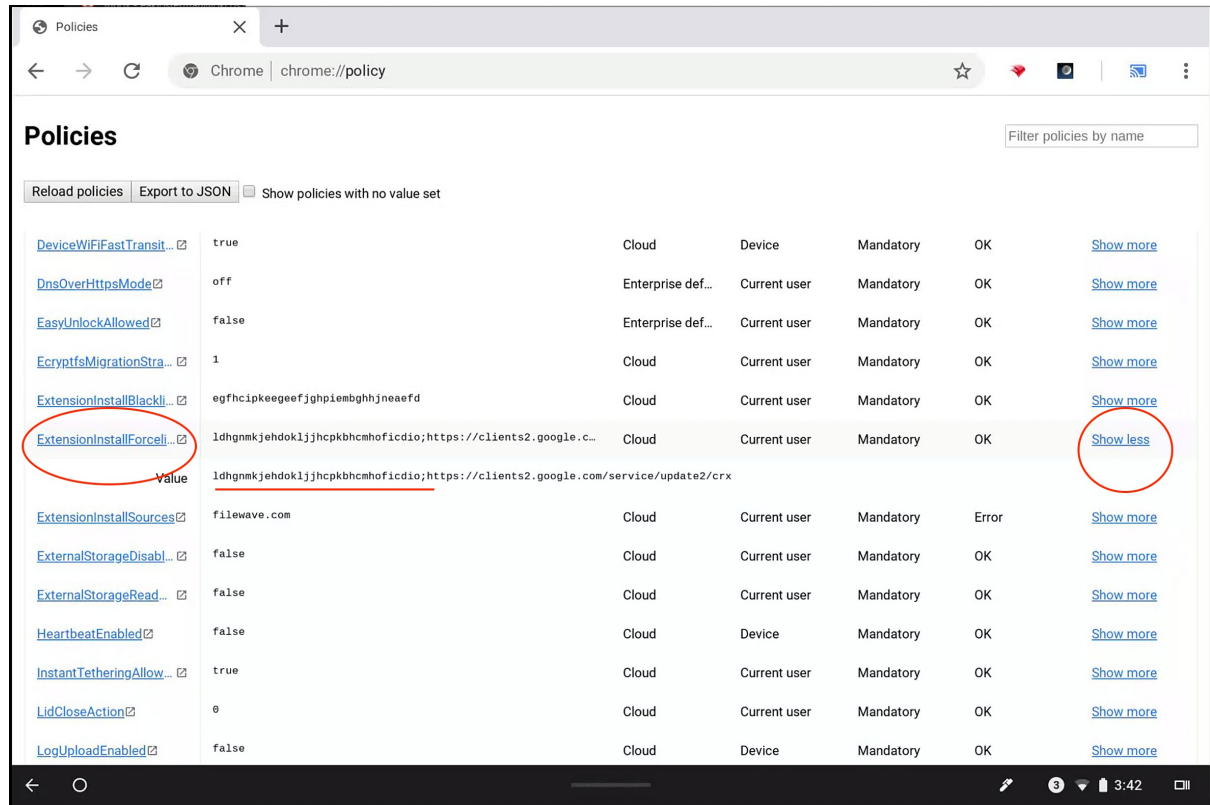7. Verify all the policy fields are there (Figure 1.2)

Policies

Chrome | chrome://policy

Policies

Filter policies by name

Reload policies | Export to JSON | ☐ Show policies with no value set

DeviceWiFiFastTransit...	true	Cloud	Device	Mandatory	OK	Show more
DnsOverHttpsMode	off	Enterprise def...	Current user	Mandatory	OK	Show more
EasyUnlockAllowed	false	Enterprise def...	Current user	Mandatory	OK	Show more
EcryptfsMigrationStra...	1	Cloud	Current user	Mandatory	OK	Show more
ExtensionInstallBlackli...	egfhcipkeegeefjghpiembghhjneaefd	Cloud	Current user	Mandatory	OK	Show more
ExtensionInstallForceli...	ldhgnmkjehdokljjhcpkbhcmhoficdio;https://clients2.google.c...	Cloud	Current user	Mandatory	OK	Show less
Value	ldhgnmkjehdokljjhcpkbhcmhoficdio;https://clients2.google.com/service/update2/crx					
ExtensionInstallSources	filewave.com	Cloud	Current user	Mandatory	Error	Show more
ExternalStorageDisabl...	false	Cloud	Current user	Mandatory	OK	Show more
ExternalStorageRead...	false	Cloud	Current user	Mandatory	OK	Show more
HeartbeatEnabled	false	Cloud	Device	Mandatory	OK	Show more
InstantTetheringAllow...	true	Cloud	Current user	Mandatory	OK	Show more
LidCloseAction	0	Cloud	Current user	Mandatory	OK	Show more
LogUploadEnabled	false	Cloud	Device	Mandatory	OK	Show more

3:42

Figure 1.1 - Chrome Policy Force List

Policies

Chrome | chrome://policy

Policies

Filter policies by name

Reload policies | Export to JSON | ☐ Show policies with no value set

ghbmnnjooekpmoecnnnilnnbdlolhkhi

Policy name	Policy value	Source	Applies to	Level	Status
			No policies set		

FileWave Inventory

ldhgnmkjehdokljjhcpkbhcmhoficdio

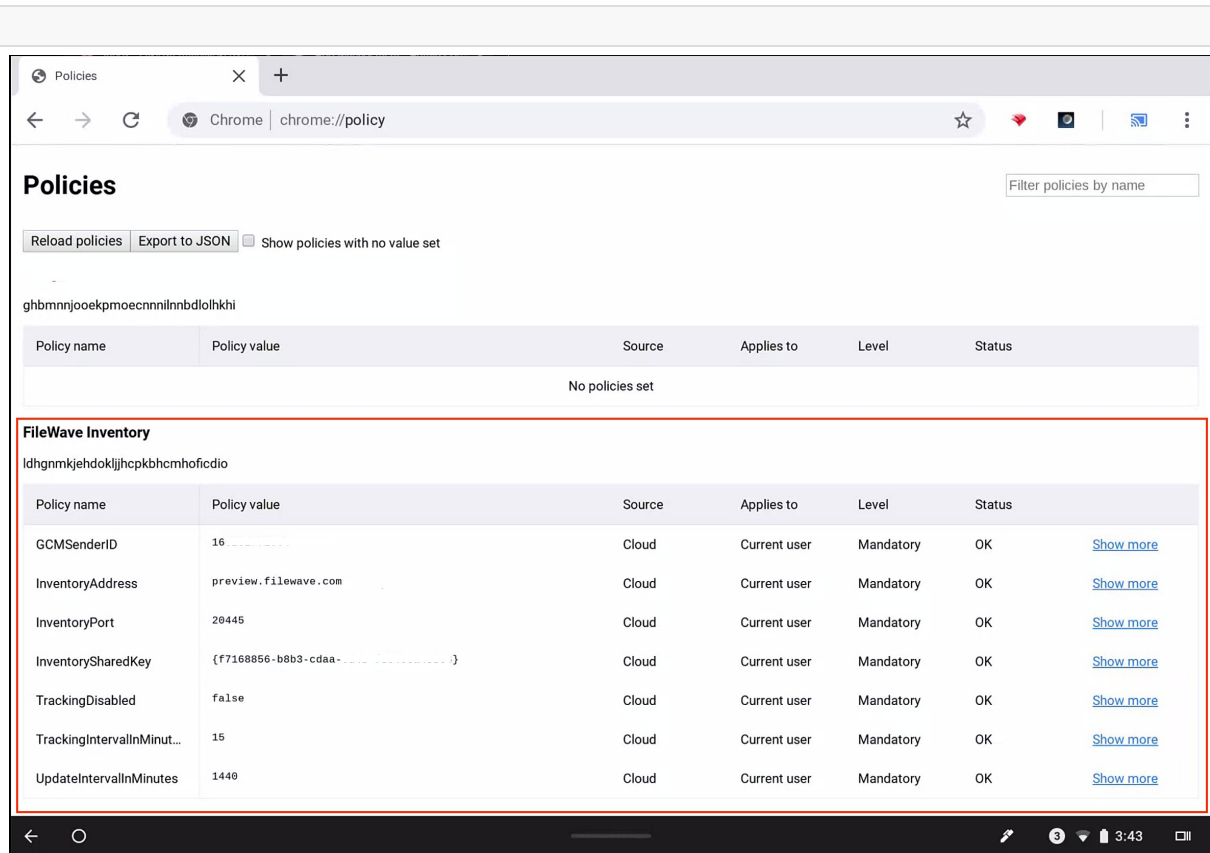| Policy name	Policy value	Source	Applies to	Level	Status	
GCMSenderID	16 _____	Cloud	Current user	Mandatory	OK	Show more
InventoryAddress	preview.filewave.com	Cloud	Current user	Mandatory	OK	Show more
InventoryPort	20445	Cloud	Current user	Mandatory	OK	Show more
InventorySharedKey	{f7168856-b8b3-cdaa-__ _____ }	Cloud	Current user	Mandatory	OK	Show more
TrackingDisabled	false	Cloud	Current user	Mandatory	OK	Show more
TrackingIntervalInMinut...	15	Cloud	Current user	Mandatory	OK	Show more
UpdateIntervalInMinutes	1440	Cloud	Current user	Mandatory	OK	Show more

3:43

Figure 1.2 - Chrome Policy for FileWave

View the Extension Console Log

1. Open a Google Chrome window
2. Browse to the URL: chrome://extensions
3. Be sure Developer mode is enabled
4. Click Details (Figure 2.1)
5. Open the Background page (Figure 2.2)
6. Select the Console tab to view the log
7. Verify the log contains "FCM Registration" (Figure 2.3)

1. The is the messaging system FileWave uses to talk to the device, if it does not register then we can not communicate.
        2. If it failed or is empty. make sure the JSON used in the extension configuration contained FCM information
8. Verify the log contains "... Report sent successfully"
    1. This confirms that the device is able to talk to your FileWave server
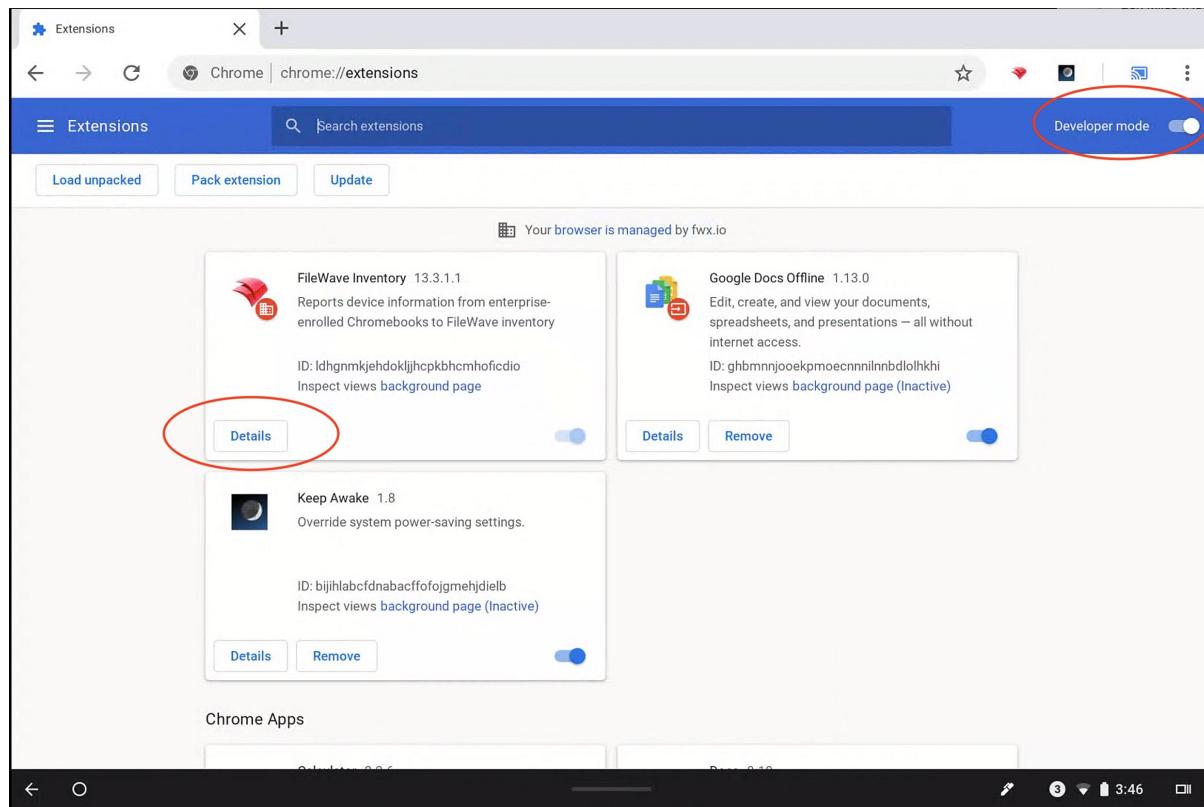   2. if it is unable to send reports, then verify your JSON contains your server name and an inventory token

Figure 2.1 - Chrome Extensions
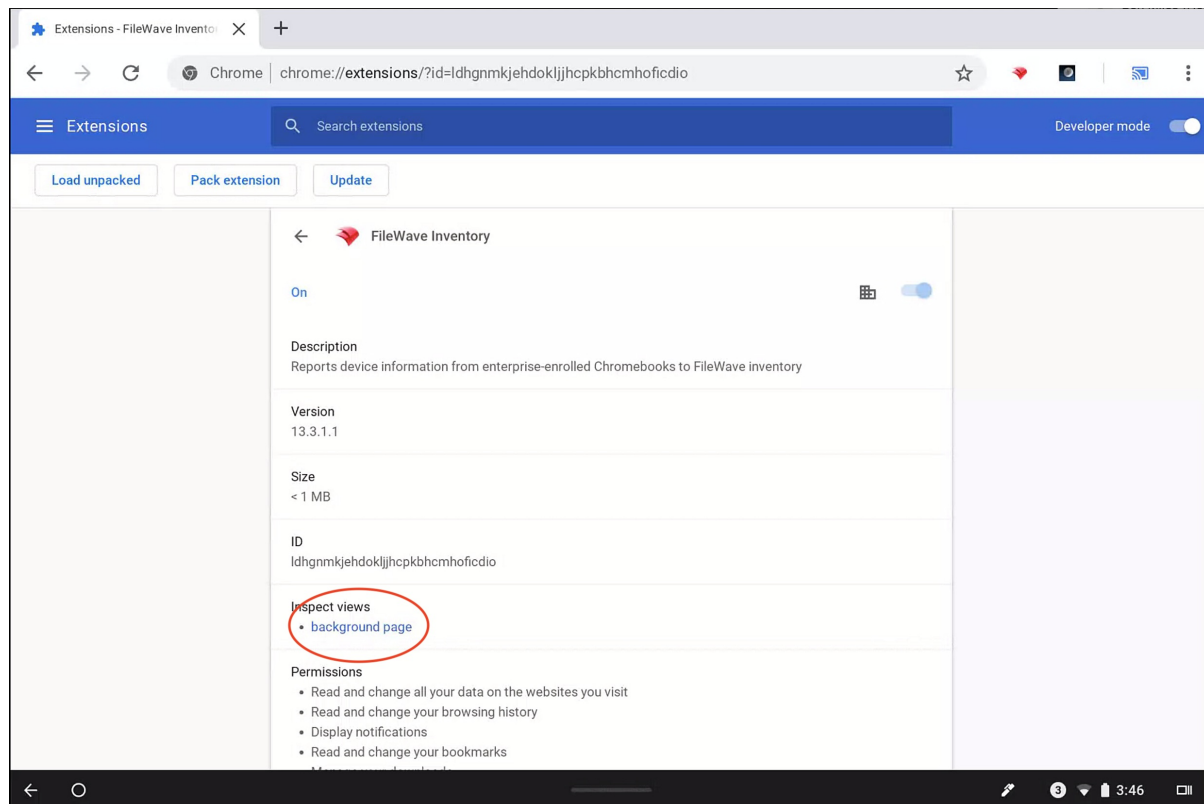
Figure 2.2 - Chrome Extension Details
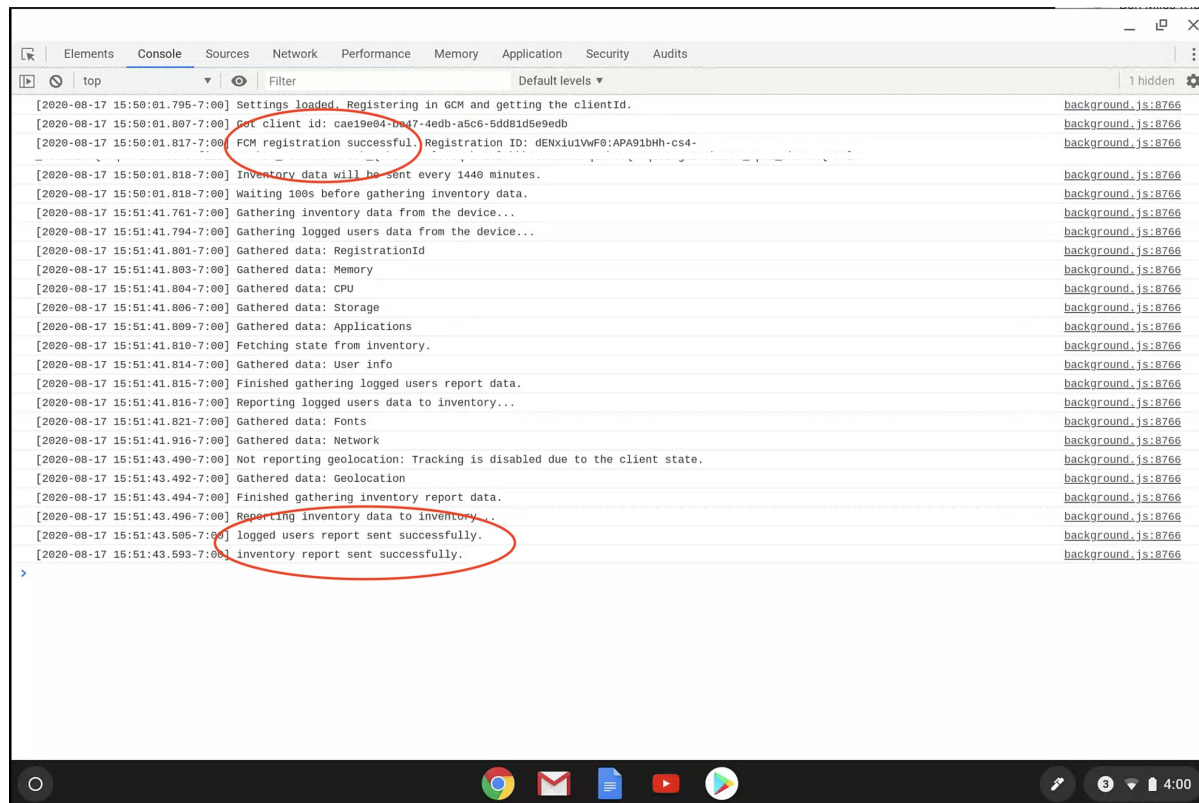
Figure 2.3 - Extension log

Error	Details	Solution
GCM failed to register	The device(s) are unable to use the information they received to contact Google's GCM/Firebase services	Be sure you have GCM registered properly (Google Cloud Messaging (GCM/Firebase) Setup) in your admin preferences BEFORE you exported the settings for upload into Google Suite. You can always export it again.
Failed to load resource: net : : ERR_INSECURE_RESPONSE	The device(s) is unable to connect to your server with a secure connections	* Verify the server has a valid certificate * Verify the server's certificate is either root trusted or has been uploaded to your google suite (see Quick Start Guide for Chromebooks) * Verify the ports between devices and server are open (see: Default TCP and UDP Port Usage)
Error: failed to gather Geolocation data: All attempts exhausted	The FileWave client on the device was unable to receive location information from the devices' OS	* Verify in the devices security preferences the app has admin rights to location information
Failed to send inventory data	The device was unable to contact the inventory port on the server	* Verify the ports between devices and server are open (see: Default TCP and UDP Port Usage) * Verify you have all your settings in preferences BEFORE you exported the settings for upload into Google Suite. You can always export it again.
GET https://server.name:20445/inv/api/v1/client/settings/asdasdasd net : : ERR_NAME_RESOLUTION_FAILED	There was a problem looking up the same of your server from the information received during enrollment	* Verify you have all your settings in preferences BEFORE you exported the settings for upload into Google Suite. You can always export it again.
Uncaught (in Promise) TypeError: Cannot read property 'state' of undefined at ...	Device was unable to contact the FileWave server OR the device was able to contact the FileWave server but the state of the device could not be read.	* Attempt to change the state FileWave Admin and update the mode. Wait for the device to verify or force a verify of the device. * If the problem persists contact FileWave support.

Chrome OS: FileWave Inventory Extension Capabilities

What

An optional add-on for Chromebook management in FileWave is the FileWave Inventory extension. We'll describe what this add-on allows you to do in this article.

When/Why

We'll want to make use of the inventory extension for any of the following functions:

- Additional Inventory Retrieval (Beyond what the Google Admin Console sends us):
  - Application Information (installed app and extensions)
  - User Information (currently logged in user, etc)
  - Network Information (current IP)
  - Font Information
  - Device Storage data (drive space, etc)
  - Geo-location Information (location, but only if explicitly turned on)
  - Submit "Last Connected" time (which should not be confused with last sync time...Last Connected is the last time the device talked directly to the FileWave server)
- Ability to initiate an remote control session through TeamViewer (version 14.6+)
- To send a "Verify" to make the device check in immediately

How

Reference the Quick Start Guide below for instructions on setting up the inventory extension for your Chromebooks.

Disable Chrome OS in FileWave

These steps will walk you through the process of disabling Chrome OS in FileWave

1. Open Preferences in the FileWave Admin
2. Go to the Chromebooks tab
3. Click Configure OAuth token
4. Sign in with your super user credentials
5. In the window that pops up (seen below), click the Clear button
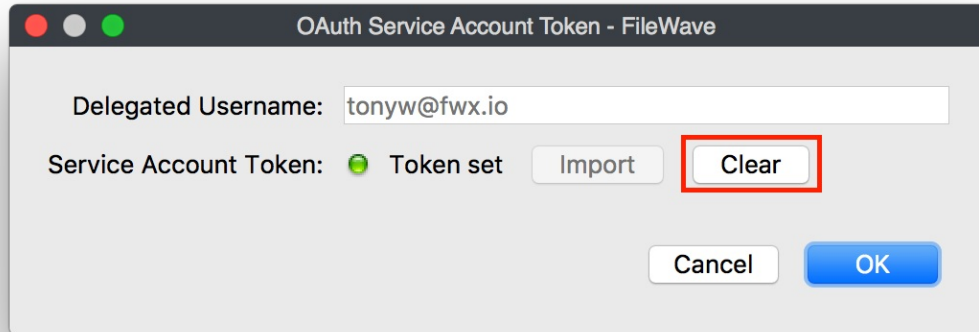
6. Confirm that you wish to process by clicking Yes
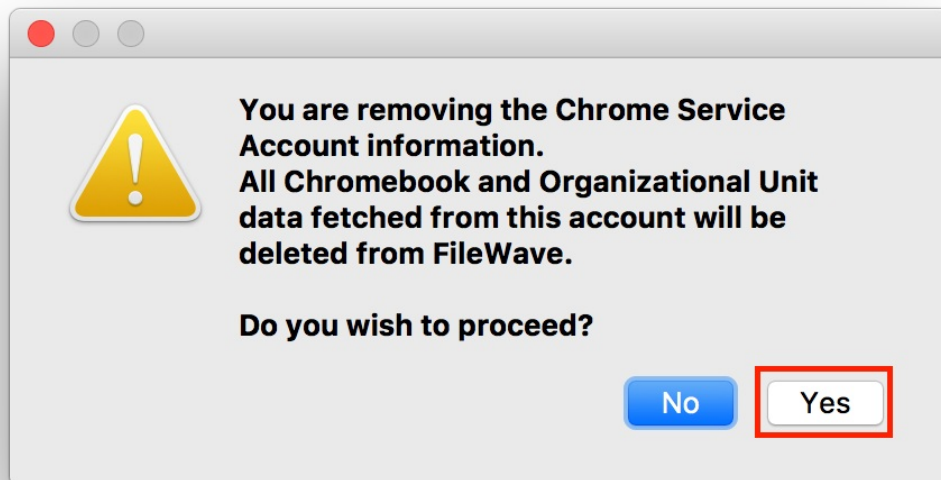
You have now disabled Chrome OS from FileWave. All of your Chrome OS licenses are now at zero.

Powerwash / Wipe Users on ChromeOS (15.3+)

What

Powerwash and Wipe Users are features on ChromeOS that allow users to reset their Chromebook to its original state, effectively erasing all user data and returning the device to its factory settings. These features are particularly useful for managing devices in environments where they are shared among multiple users, such as schools and businesses, or when preparing a device for a new user.

When/Why

Powerwash

Powerwash is the term used by ChromeOS for its factory reset process. When you Powerwash a Chromebook, the device undergoes a complete reset, removing all user accounts, their files, and every setting adjustment made to the device. This process returns the Chromebook to its original state, just as it was out of the box. It's a straightforward way to ensure that no personal data is left on the device, making it ready for a new user or for troubleshooting purposes.

Technical Perspective:

- Use Case: Ideal for individuals returning, selling, or reassigning their Chromebook. Also used for troubleshooting device issues that cannot be resolved through standard fixes.
- Process: Initiated through the settings menu under "Advanced" settings or via a keyboard shortcut at the login screen (pressing Ctrl + Alt + Shift + R).
- Considerations: Before performing a Powerwash, it's crucial to back up any important data stored on the device, as the process will delete everything.

Wipe Users

Wipe Users is a feature aimed more at administrators managing multiple Chromebooks within an organization, such as a school or a corporation. This feature allows administrators to remotely clear all user data from a Chromebook without affecting the device's enrollment status in a domain. It's particularly useful for quickly preparing devices for new users without going through a full device setup process again.

Technical Perspective:

- Use Case: Primarily used by administrators to quickly clear all personal data from devices between different users while retaining device management settings and policies.
- Process: Can be executed remotely via Google Admin Console, under the device management section, allowing for bulk operations across multiple devices.
- Considerations: Ensures that devices remain under organizational control and policies after user data is wiped, streamlining the reassignment process.

Both Powerwash and Wipe Users serve critical roles in the management and maintenance of ChromeOS devices, ensuring data privacy and security while facilitating device transitions between users. Powerwash provides a complete reset for individual users or troubleshooting, while Wipe Users allows administrators to efficiently manage device readiness in a controlled environment without disrupting device enrollment and management settings. For organizations using Chromebooks, understanding and utilizing these features effectively can greatly enhance operational efficiency and device security.

How

These commands are executed by right clicking one or more Chromebooks and picking Wipe Device or Wipe Users as shown below.
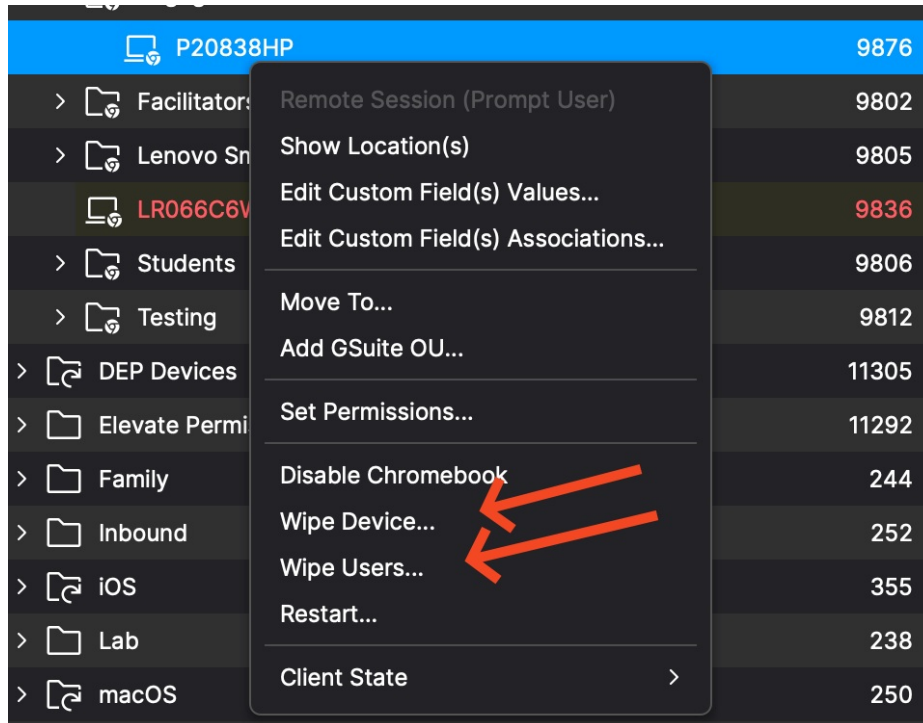
REMOTE_POWERWASH Command (Wipe Device)

- Description: System administrators can remotely Powerwash ChromeOS devices, resetting them to factory settings for efficient troubleshooting and maintaining device security.
- Execution: Initiates the Powerwash process, erasing all user data and configurations.
- Access:
  - The REMOTE_POWERWASH command is accessible through the Central as well as Anywhere Admin for ChromeOS devices.
  - Find the command in the dropdown menu labeled "Wipe device(s)..."
  - Modify Clients/Groups and Wipe Devices permissions are required.

When wiping a device keep in mind it will fully wipe the device and you should consider Force wiped ChromeOS devices to re-enroll (15.3+)
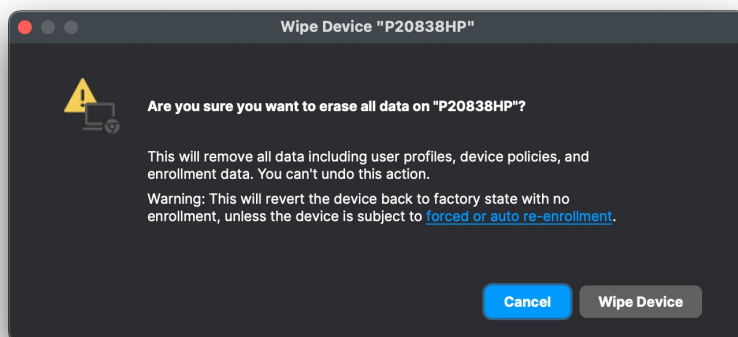
WIPE_USERS Command

- Description: System administrators can remotely and securely wipe user data from devices, ensuring compliance with data protection regulations and maintaining organizational security.
- Execution: Initiates the data-wiping process on all user accounts.
- Access:
  - The WIPE_USERS command is accessible through the Central as well as Anywhere Admin for ChromeOS devices.
  - Find the command in the dropdown menu labeled "Wipe user(s)..."
  - Modify Clients/Groups and Wipe Devices permissions are required.

Command History tab

- Description: Users can now view all information related to sending REMOTE_POWERWASH, WIPE_USERS, and REBOOT Commands in the Command History tab for Chromebook devices. As shown below you can see this when looking at device details for a Chromebook.
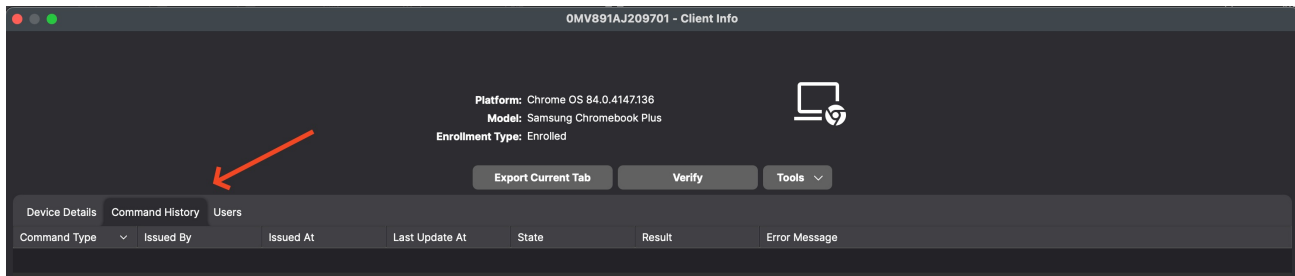
Related Content

- [ChromeOS](#)
- [Reboot for ChromeOS (15.3+)](#)

Reboot for ChromeOS (15.3+)

What

For an MDM (Mobile Device Management) administrator managing ChromeOS devices, the ability to remotely send a reboot command is a powerful tool for device maintenance and troubleshooting. This command ensures that devices are running smoothly, updates are applied, and any minor issues are resolved without the need for manual intervention.

When/Why

Understanding the Reboot Command

- Purpose: The reboot command allows administrators to remotely restart ChromeOS devices, which is essential for applying updates, enforcing new policies, or fixing software issues.
- Execution: Through the MDM solution integrated with Google's Chrome Enterprise services, admins can issue reboot commands directly from the management console. This process ensures that all devices are up-to-date and functioning as expected.
- Considerations: When sending a reboot command, it's important to consider the timing and potential impact on users. Ideally, reboots should be scheduled during off-hours or times when the device is not in active use to minimize disruption. It's also good practice to inform users about planned reboots.

Practical Use Cases

1. Applying Updates: To ensure devices have the latest features and security patches.
2. Resolving Issues: To fix minor glitches that can be cleared with a restart.
3. Enforcing Policies: To apply new configurations or policies that require a reboot to take effect.
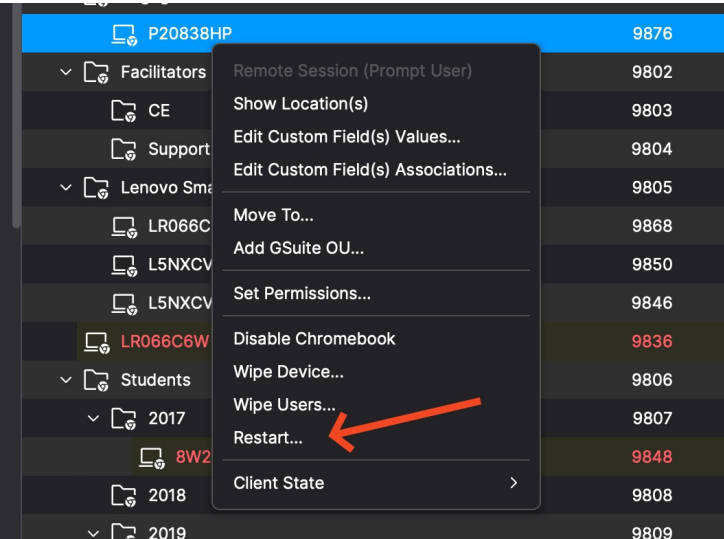
Tips for MDM Administrators

- User Communication: Notify users about scheduled reboots, especially if they are during working hours.
- Scheduling: Plan reboots during times that will least impact users, like after-hours or during known downtime.
- Monitoring: After issuing a reboot command, monitor the devices to ensure they restart successfully and operate as expected.

By leveraging the reboot command through your MDM solution, you can maintain control over the ChromeOS devices within your organization, ensuring they remain secure, up-to-date, and operate without issues. This command is a straightforward yet essential part of device management that helps keep everything running smoothly.

How

This command is executed by right clicking one or more Chromebooks and picking Restart... as shown below.


REBOOT Command

- Description: Introducing the REBOOT command, enabling system administrators to reboot devices for troubleshooting remotely and applying system updates.
- Execution: Initiates the remote reboot process on the selected devices.

- Access:
  - The REBOOT command is accessible through the Central as well as Anywhere Admin for ChromeOS devices.
  - Find the command in the dropdown menu labeled "Reboot..."
  - Read permissions is the only requirement.

Command History tab

- Description: Users can now view all information related to sending REMOTE_POWERWASH, WIPE_USERS, and REBOOT Commands in the Command History tab for Chromebook devices. As shown below you can see this when looking at device details for a Chromebook.
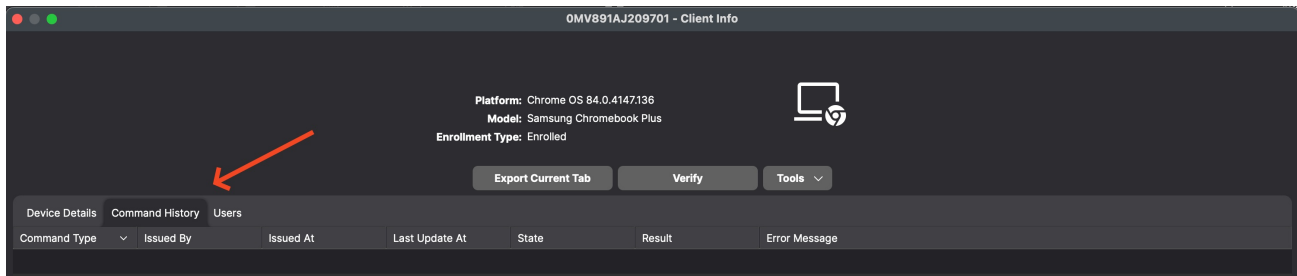
Related Content

- [ChromeOS](#)
- [Powerwash / Wipe Users on ChromeOS (15.3+)](#)

# Google Admin Sync Interval for ChromeOS (15.3+)

What

As an administrator managing ChromeOS devices you may want to change the frequency that FileWave will sync with the Google Admin backend.

When/Why

When FileWave syncs with Google, there is information like what OU a device is in that is synchronized. If you make frequent changes in managing your ChromeOS devices, then you may want to sync more frequently in order to have the data align more often.

How

FileWave Central -> Preferences -> Google and then adjust the amount of hours between sync where it shows "Synchronize with Google Admin every 24 hours" The value can be between 1 and 24 hours with 24 being the default.
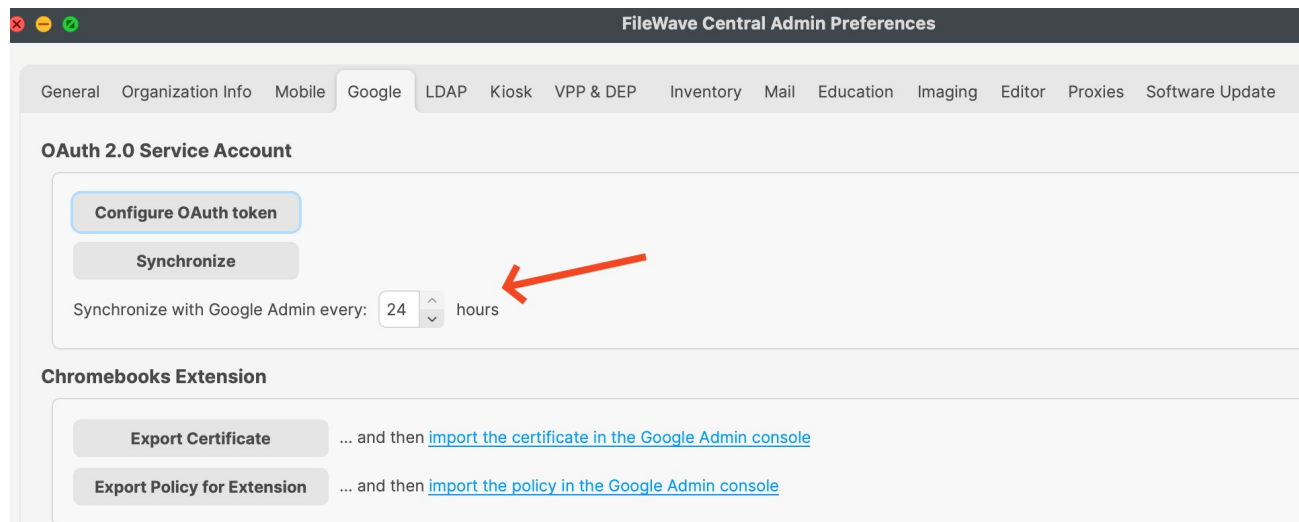
Related Content

- ChromeOS

Custom Field Annotated Field Sync for ChromeOS (15.3+)

What

As an administrator managing ChromeOS devices you want to update the Annotated Custom fields in FileWave, but aren't sure how soon those changes will be reflected in the Google Admin console.

When/Why

In FileWave 15.3+ we have changed how Annotated Custom Fields are synced with Google. In the past there would be issues reported because the fields would only sync on the 24 hour sync interval for all ChromeOS information with Google.

How

Annotated fields in Edit Custom Fields in 15.3+ now update immediately upon clicking Save, independently of the Model Update, ensuring swift and accurate changes.

- The Chromebook Data tab in Device Details is removed. Users can access Chromebook-related info by double-clicking on the device, eliminating the need for an additional tab.
- The Device Details View now offers a more informative and user-friendly experience for Annotated fields.
- Annotated fields are seamlessly displayed and editable in the Edit Custom Fields dialog, like any other custom fields.
- A convenient button in the Client Info dialog allows users to sync annotated fields (one way: Google to FileWave) individually for specific devices, offering granular control over data synchronization.
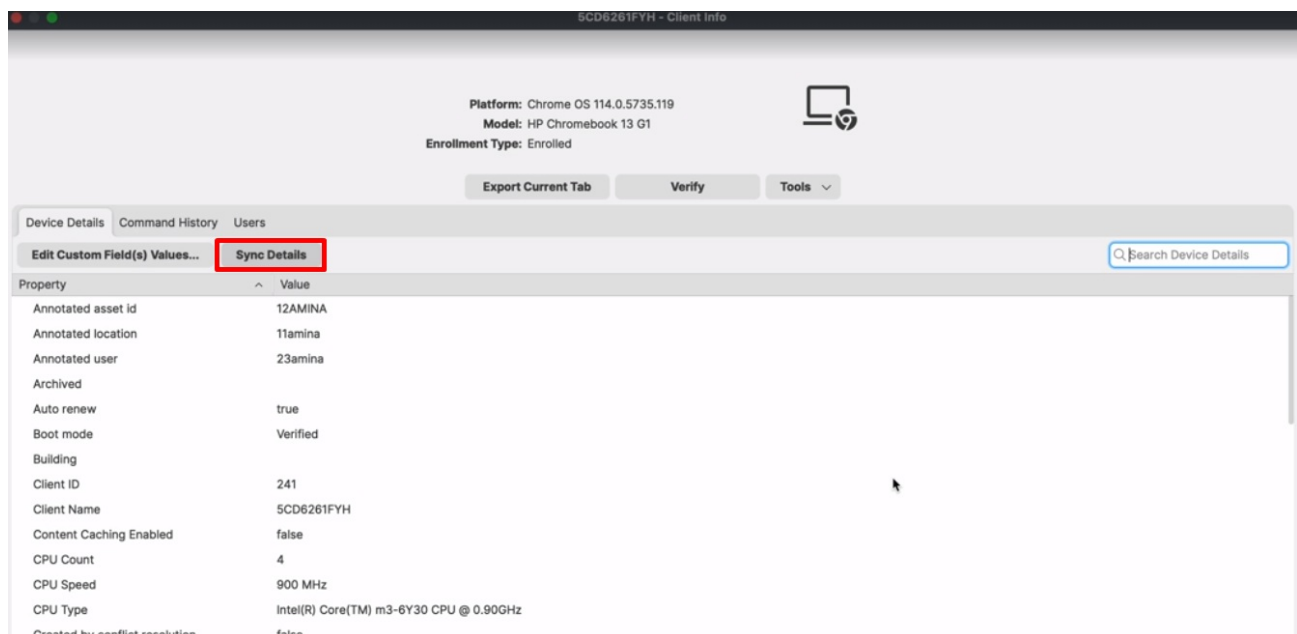

Related Content

- ChromeOS

Forcing wiped ChromeOS devices to re-enroll (15.3+)

What

By default, wiped ChromeOS devices automatically re-enroll into your account without users having to enter their username and password. Re-enrollment ensures that the ChromeOS devices remain managed and policies you set are enforced on the ChromeOS device. Otherwise, users can't sign in, browse in guest mode, or see the consumer sign-in screen.
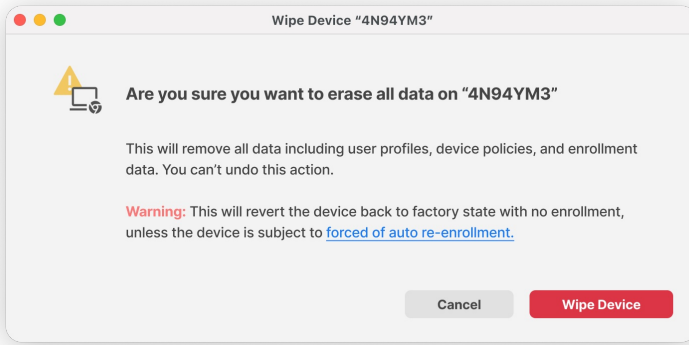
When/Why

Don't force ChromeOS devices that are used in developer mode to re-enroll. Instead, put them in a different organizational unit and turn off forced re-enrollment for that organization. If a ChromeOS device is no longer going to be managed by your account, you should deprovision the device.

How

For convenience we've included Google's documentation below from: Force wiped ChromeOS devices to re-enroll - Chrome Enterprise and Education Help (google.com)

Turn forced re-enrollment on or off

1. Sign in to your Google Admin console.
   Sign in using an administrator account, not your current account bob@gmail.com
2. In the Admin console, go to Menu ☰ > ⊡ Devices > Chrome > Settings > Device settings.
3. To apply the setting to all devices, leave the top organizational unit selected. Otherwise, select a child organizational unit.
4. Go to Enrollment and access.
5. Configure the Forced re-enrollment setting:
   - Force device to automatically re-enroll after wiping—Wiped ChromeOS devices automatically re-enroll into your account without users having to enter their username and password.
   - Force device to re-enroll with user credentials after wiping—Users must manually re-enroll ChromeOS devices into your account.
   - Device is not forced to re-enroll after wiping—Users can use the ChromeOS device without re-enrolling it into your account.
6. Click Save.

Settings typically take effect within minutes, but it might take up to an hour to propagate through your organization.

Sometimes, ChromeOS devices might not be able to automatically re-enroll themselves. If an error occurs during automatic re-enrollment, users are notified. They can click Enroll manually to proceed with manual re-enrollment. ChromeOS devices that don't support automatic re-enrollment show a screen that prompts users to manually re-enroll them.

Related Content

- Force wiped ChromeOS devices to re-enroll - Chrome Enterprise and Education Help (google.com)

Confirming Firebase APIs are enabled for Chromebooks (15.4+)

What

When setting up Chromebooks you need to ensure that the right APIs are enabled. In FileWave 15.4 there are 2 APIs that are required that were not previously needed. You may have these enabled, but you should still do this process just in case they are not.

When/Why

You will want to do this when you are using FileWave 15.4.0 or higher with Chromebooks to make sure everything is right. If you have not previously, you definitely need to enable the 2 APIs. You can enable them on a 15.3.1 server as well, but the APIs are required for 15.4.0 and beyond, and required to be on 15.4.0 after June 20, 2024.

How

To enable the 2 APIS you may go to https://console.cloud.google.com/apis/dashboard and enable them. You would be looking for Firebase Cloud Messaging API and Firebase Management API. To simplify here is a more direct URL to add them to a project: https://console.developers.google.com/flows/enableapi?apiid=firebase.googleapis.com,fcm.googleapis.com which should be straightforward if you only have 1 Firebase project. If you don't really know how Chromebooks were setup in the past you could go through Chromebook Client Pre-Requisites and set it up again.

When you go to the URL you should see something like this next screen where you can pick a project and click Next.
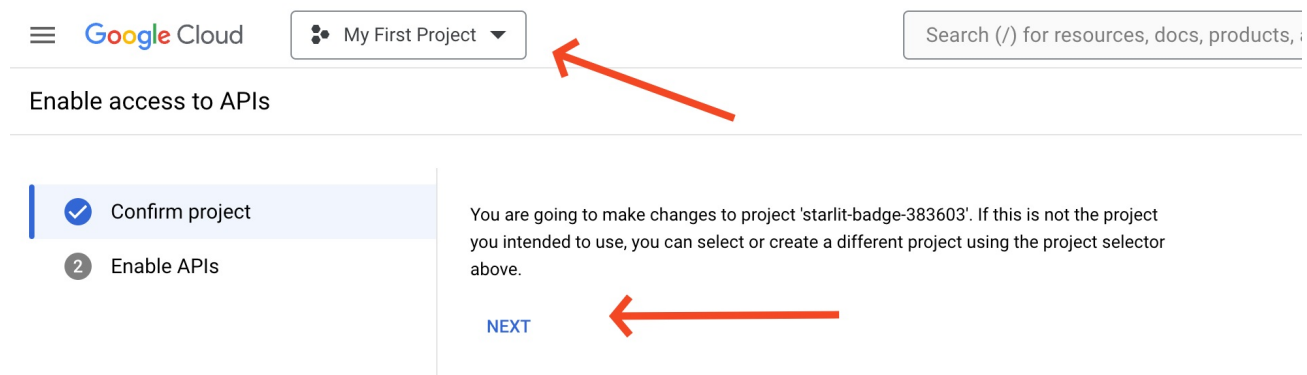
Next you will see the 2 APIs to enable and you'll click Enable.
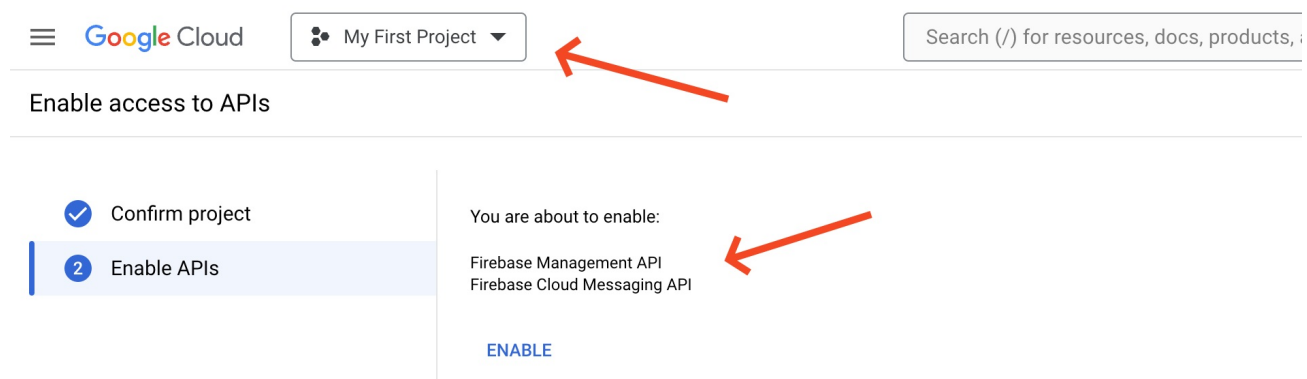
Once you have enabled this you should see in FileWave Central on v15.4 that it is able to sync by going to Settings -> Google and viewing the sync status there.

Related Content

- Chromebook Client Pre-Requisites
- Update your apps to the latest Firebase Cloud Messaging APIs and SDKs