chrome enterprise

# Best Practices for using Chrome Browser Cloud Management

## Contents

## Introduction

Welcome to Chrome Browser Cloud Management. This guide is meant to be a companion to the Chrome Browser Cloud Management Deployment Guide. This document  will take you through the process of:

- Getting your Google Admin Console setup.
- Setting up an organizational unit structure to divide up your machines.
- How to enroll and manage your browsers on various operating systems including discussing any known limitations,
- How policies will work if you have existing GPO in place.
- Get reporting enabled on your devices for extensions and more.

This guide is written in chronological order as if you are just starting the step-up process.  Here is a high level overview of the steps you need to follow:

| Windows | Mac | Linux |
|---|---|---|
| Step 1.<br>Get access to the Admin console (admin.google.com)<br>Options are:<br>● Google assigned domain<br>● Use your own domain<br>● Use existing admin console | | |
| Step 2. Setup your Organizational units (detailed steps here) | | |
| Step 3. Setup your admin accounts (detailed steps here) | | |
| Step 4. Enroll Devices<br>Windows<br>● GPO or Reg file (see step 2 Windows)<br>● Workspace One | Mac<br>● Plist<br>● Jamf Pro<br>● Workspace One | Linux<br>● Txt file (see step 2 Linux) |

## Access options for Chrome Browser Cloud Management

Following this guide for the setup of Chrome Browser Cloud Management is the best place to start. It covers all of the initial setup steps. Chrome Browser Cloud Management itself is no additional cost. Note that there are three options on how to setup your account:

| Type of Domain | Pros | Cons |
|---|---|---|
| Google assigned domain (i.e. “xxx.deviceadmin.goog”) | ● No additional cost<br>● No domain verification process<br>● Unlimited amount of devices can be enrolled | ● Limit of one admin account<br>● No path to transition to a different domain in the future |
| Use your own domain (no existing Google services associated) | ● Multiple Admins accounts allowed (dependent on associated Google Service)<br>● Associated directly with your enterprise domain | Requires a Google service to gain access to the console<br>● Admins require a Google service only to gain the benefits of this option<br>● They do not need to purchase any service for their users<br>○ Contact Google Sales for the most up to date pricing<br>○ See the table in Use your own domain for example services |
| Use your own domain (Google Services already associated) | ● Admin console is already set up and verified<br>● No additional cost<br>● Multiple Admins accounts allowed (dependent on associated Google Service) | ● Requires finding existing Super Admin to gain access and provide user accounts |

Out of the three, if it is possible to use your company’s existing Google admin console, that is the best option. As the console is already set up, Chrome Browser Cloud Management is already present. You just need to visit that section in the console and accept the terms of service.

## Getting access to an existing Google Admin console

Check internally if your company has an existing Google Admin account prior to setting up your own. Many companies have accounts set up for various Google services like Chrome OS, G Suite or others.

- The Super Admin at your company would need to provide you access to the console where Chrome Browser Cloud Management is located.
- The console does provide role based administration so the Super Admin can provide you access just to what you need to manage Chrome Browser
  - Note that a Super Admin account is required to generate additional admin accounts
    - Consider asking for a Super Admin account for your team so you can generate your own in the future if needed
    - If you can't find the original owner internally (like that person has left the company) here is a link for more information on domain reclamation.

If your company does have an existing account but you are not the super admin, here is the process of gaining access to Chrome Browser Cloud Management:

1. Have a Super Admin first log into admin.google.com and accept the two terms of service agreements for Chrome Browser Cloud Management. This is required to use the service. The path do to do this within admin.google.com is:
   a. Devices>Chrome and accept TOS that appears
   b. Devices>Chrome>Managed Browsers and click on the yellow plus mark and accept the TOS that appear.
2. Have the Super Admin either create an account with super admin rights or if they just want to provide access just to Chrome Browser management, then they can provide the following rights in the admin console:
   a. Under Admin roles>Privileges> Organizational Units select:
      i. Read, Create, Update, Delete
   b. Under Admin roles>Privileges> Chrome Management select:
      i. Manage user settings
      ii. Manage Browsers
      iii. View Extensions list report

## Using your own domain

If you want to use your company's own domain  but do not currently own any Google services, below are some paid Google offerings that could be considered to access the Google Admin Console with minimum cost and flexibility for the number of admin accounts that you require. This table provides a ballpark on pricing. Contact Google Sales for the most up to date pricing.

| Product | Cost<br>(prices subject to change and reflect current pricing in 2020) | Comments |
|---|---|---|
| Google Cloud Identity Premium | • $6/mo/user (£4.50 / €5)<br>• Sold direct or via reseller | • Purchase the # of admin accounts you would like<br>• There is a 14-day free trial to test. |
| Google Cloud Identity free*<br>*Minimum 1 license of GSuite required or paid GCP license | • Free for GCP customers<br>OR<br>• Existing GSuite customers | • 50 users with free option<br>• Minimum 1 license of GSuite required or paid GCP license |
| Chrome Enterprise Upgrade | • $150/ per managed device (MSRP)<br>  • (€ 109.50, £ 90.00)<br>• Sold via reseller* | • Purchase one license for every 10 admin accounts you would like.<br>• Can use this license towards managing Chrome OS devices. |
| Chrome Browser Enterprise Support | • $4/£2.70/€3.60user/yr (MSRP)<br>• Sold direct or via reseller** | • Minimum purchase of 1000 users |

## Moving machines from one domain to another

If you are testing Chrome Browser Cloud Management in one domain (like a test domain) and need to move it to another domain (like your production domain), here are the steps to do so:

1. Delete the DMToken AND EnrollmentToken from the devices you want to move. (see this link under the "Unenroll Device" section)
2. (Optional) Delete the devices from the old domain in the admin console. (This is a clean-up only task, it has no other effect).
3. Install your new domain Enrollment Token on your clients.
4. Launch Chrome

If you want to add multiple domains to the same console (and are not using the free Google provided domain) here is a link on how to set that up.

## Setting up your Organizational Units

Once you have access to the Google admin console, then the next step would be to set up the Organizational Units that your devices will be managed in.

- These are the “buckets” that you will separate your different enrolled devices into.
- They are set up in a parent-child structure so anything that is set at the top level will be applied to the lower OUs.
  - Just note that you can override any top level policy at the sub OU level. To prevent extra work, be conservative on what you apply at the root level.
- Some examples of grouping of devices could be by: geolocation, OS, department, pilot or production.

- For more information about managing organizational units, check out this link.

If you are an existing G suite or Chrome OS customer, it is recommended that you create a separate Organizational Unit structure so there is not any conflict in policies that are applied.

- This is to prevent policies originally intended as user policies inadvertently being applied to newly enrolled browsers placed into those organisational units

## Setting up Role Based Access control

Once you have your organizational units setup, then you can start setting up accounts for your administrators. This way you can delegate access to the various admins that need access.

- Note that if you go with the Google provided domain you are limited to only one administrator.

You can create admin accounts with just access to Chrome Browser Cloud Management, or to specific Organizational Units or just provide read only access. For more information about setting up different admin accounts, please refer to this link for more information.

- The privileges that are needed for full management of Chrome Browser devices are:
    - Found under admin roles>privileges> Chrome Management
        - Manage user settings
        - Manage Browsers
        - View Extensions list report
    - Under Organizational Units:
        - Read, Create, Update, Delete

You can also view changes made in the console for auditing purposes. See Admin audit log.

## Setting up integration with 3rd party SAML SSO

You can set up a single sign-on for your Google Admin console. For more information, please take a look at this link.  Note that super admin users are not supported for SAML.

## Enrolling browsers

For more information about enrolling browsers please refer to this link that covers all of the steps getting your devices enrolled in the console. It includes steps for Windows, Mac and Linux and the various methods and tools that you can use to deploy the token.

- Refer to these links for deploying via Jamf Pro and VMware Workspace One

## Workflow of the enrollment process

1. Admin installs Enrollment Token on a device using one of the methods in this link
    a. Stored on **Windows** in RegKey: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome - String value name CloudManagementEnrollmentToken
    b. Stored on **Macs** in/Library/Google/Chrome/CloudManagementEnrollmentToken
    c. Stored on **Linux** in /etc/opt/chrome/policies/enrollment

2. Chrome starts, uses the Enrollment Token to get a DMToken
    a. The DMToken is an encrypted key that is returned by Google servers to the device after enrollment
        i. It contains information like the Customer ID and the Device ID
        ii. Unique for each enrolled browser
        iii. Only Google servers can read this data
3. The DMToken is saved to permanent storage
    a. Stored on **Windows** in RegKey:HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Enrollment -String value name: dmtoken
    b. Stored on **Macs** in ~/Library/Application Support/Google/Chrome Cloud Enrollment/{device-id}
    c. Stored on **Linux** in {user_data_dir}/Policies/Enrollment/{device-id}
4. Chrome is now enrolled for that device within the console

A few things of note for the enrollment process:

- Chrome will need to be restarted for policies to be applied from the console
- It can take up to 24hrs for an enrolled browser to show up in the console.
- Changing the enrollment token in the registry directly is not a method for moving the browser from one OU to another. The browser needs to be moved directly in the console for the change to take effect.
- The console currently has a limit on the number of browsers that are enrolled simultaneously.
    - We recommend enrolling no more than 150 browsers per minute.
    - We are working on significantly increasing the limit in a future release.

## Supporting Virtual and Physical Machines

### Non-persistent VMs

The admin console does not support non-persistent VMs at this time. You are able to enroll them, however since the machine is frequently rebuilt, it will cause multiple entries in the console which will make your reporting inaccurate. This is because the machines are marked as unique through the machine GUID, which will change as the machines are recreated.

### Persistent VMs

The console does support persistent VMs if each machine has a unique SID (machine GUID). This is normally generated by running sysprep on the machine during the imaging process. If you are using a system (like Citrix) that has the same machine GUID on every machine, then you would need to run a script (like a run once script) to change the machine GUID. Doing this will have the machine show up as a unique machine.
Here is a workflow of what that might look like (Windows):

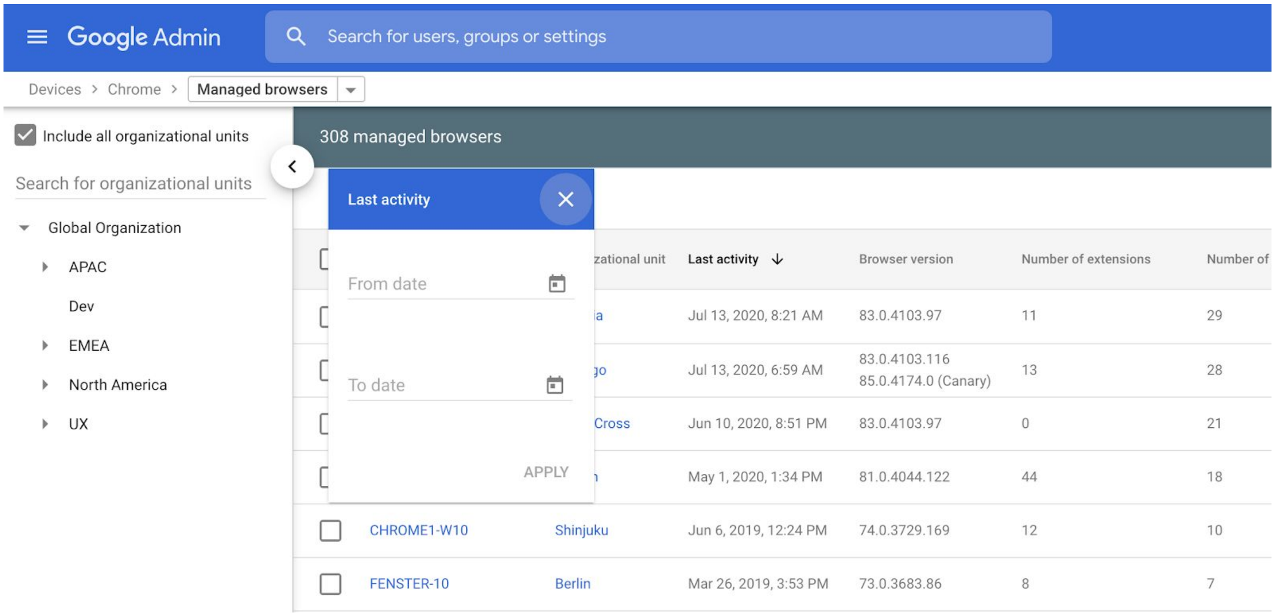
1. Close Chrome
2. Delete Device Token located in:
3. HKLM\Software\Google\Chrome\Enrollment
   String value name: dmtoken

    - Enrollment token can be left behind unless you want to move the device to a new OU location
4. Delete Machine-GUID and the new unique machine guid will be generated as the key adds itself back in
    - This key is usually located in: HKLM\Software\Microsoft\Cryptography\MachineGuid
5. Restart Chrome
6. Chrome will read the existing enrollment token (or new one if you pushed one out) and will push down a new DMtoken

### Supporting Physical Machines

The console fully supports physical machines, however just note that since the uniqueness of the device is tied to a unique SID (machine GUID), if the machine is reimaged or if that GUID changes, it will register as a new machine within the console.

It is recommended if a machine is reimaged, that it is deleted from the console and then re-enrolled under the new image to prevent duplicate counts.  Another tool to prevent inactive machines from remaining in your console is to the filter feature  in the managed devices view by the last activity column or click on the “search or add a filter button” and select Last activity.


Google Admin
Search for users, groups or settings
Devices > Chrome > Managed browsers
☑ Include all organizational units
Search for organizational units
Global Organization
APAC
Dev
EMEA
North America
UX
Last activity
From date
To date
APPLY

308 managed browsers

| | | zational unit | Last activity ↓ | Browser version | Number of extensions | Number of |
|---|---|---|---|---|---|---|
| | | a | Jul 13, 2020, 8:21 AM | 83.0.4103.97 | 11 | 29 |
| | | go | Jul 13, 2020, 6:59 AM | 83.0.4103.116<br>85.0.4174.0 (Canary) | 13 | 28 |
| | | Cross | Jun 10, 2020, 8:51 PM | 83.0.4103.97 | 0 | 21 |
| | | ı | May 1, 2020, 1:34 PM | 81.0.4044.122 | 44 | 18 |
| □ | CHROME1-W10 | Shinjuku | Jun 6, 2019, 12:24 PM | 74.0.3729.169 | 12 | 10 |
| □ | FENSTER-10 | Berlin | Mar 26, 2019, 3:53 PM | 73.0.3683.86 | 8 | 7 |

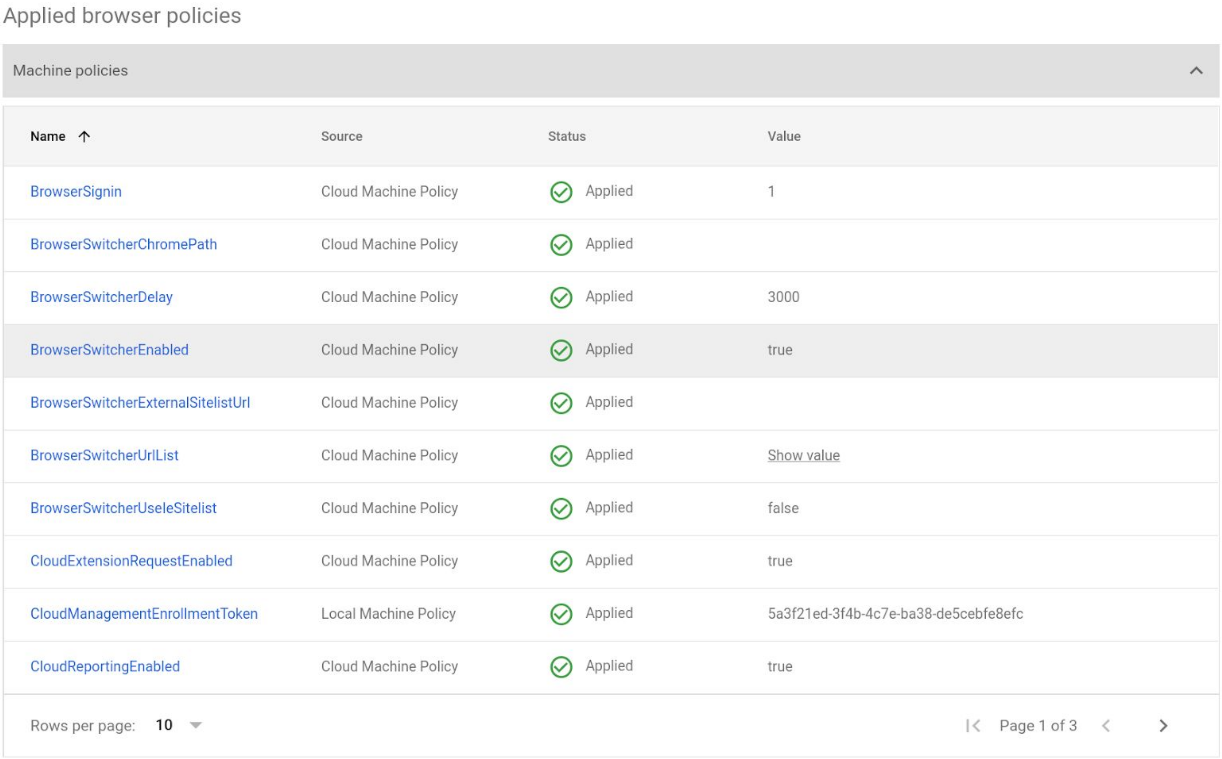
Decide a timeframe of how long you want machines to remain in the console after being inactive (like 90 days , a year etc.) and consider deleting them out.

## Viewing the reports in Chrome Browser Cloud Management

Once the devices are enrolled and present within the console, you can start viewing the data that is coming in. It is recommended that before you start applying policies (especially around extensions) that you first take a look at what is already present.

- You must turn on the cloud reporting feature in order for data to populate into the console.

Under the managed browsers section, you can select one of your enrolled devices and browse to the Applied Browser Policies section to see what policies are already in effect.



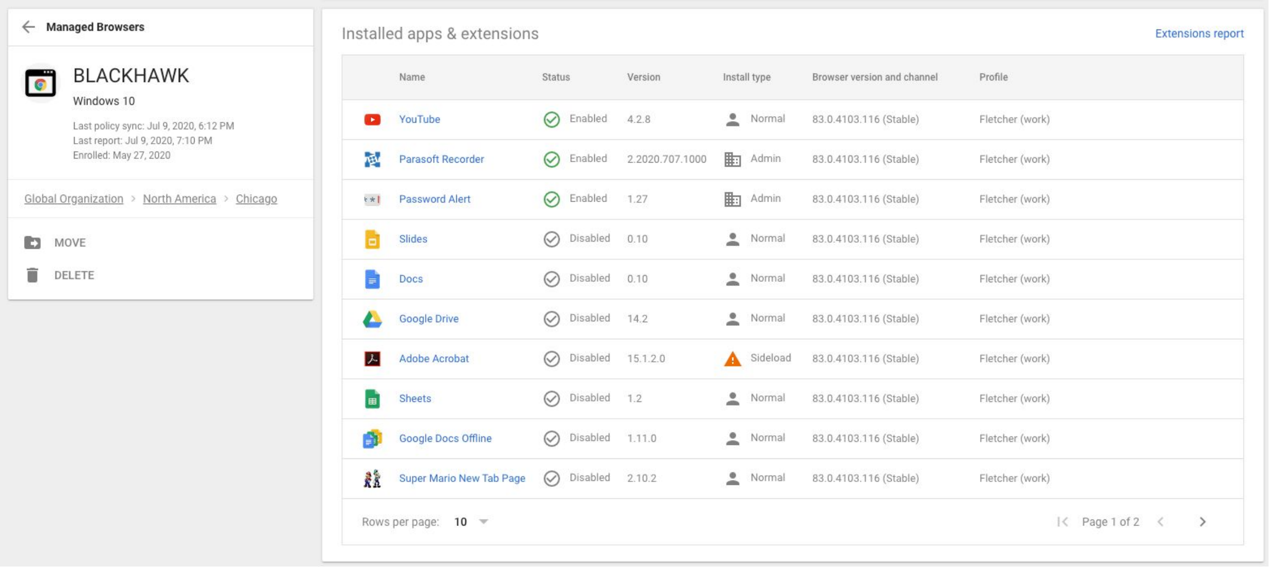
Applied browser policies

Machine policies

| Name ↑ | Source | Status | Value |
|---|---|---|---|
| BrowserSignin | Cloud Machine Policy | ✓ Applied | 1 |
| BrowserSwitcherChromePath | Cloud Machine Policy | ✓ Applied | |
| BrowserSwitcherDelay | Cloud Machine Policy | ✓ Applied | 3000 |
| BrowserSwitcherEnabled | Cloud Machine Policy | ✓ Applied | true |
| BrowserSwitcherExternalSitelistUrl | Cloud Machine Policy | ✓ Applied | |
| BrowserSwitcherUrlList | Cloud Machine Policy | ✓ Applied | Show value |
| BrowserSwitcherUseIeSitelist | Cloud Machine Policy | ✓ Applied | false |
| CloudExtensionRequestEnabled | Cloud Machine Policy | ✓ Applied | true |
| CloudManagementEnrollmentToken | Local Machine Policy | ✓ Applied | 5a3f21ed-3f4b-4c7e-ba38-de5cebfe8efc |
| CloudReportingEnabled | Cloud Machine Policy | ✓ Applied | true |

Rows per page: 10 ▾ |< Page 1 of 3 < >

- To get a viewpoint on the extensions that are already installed on that machine, you can view the Apps and Extensions section



Managed Browsers

BLACKHAWK

Windows 10

Last policy sync: Jul 9, 2020, 6:12 PM
Last report: Jul 9, 2020, 7:10 PM
Enrolled: May 27, 2020

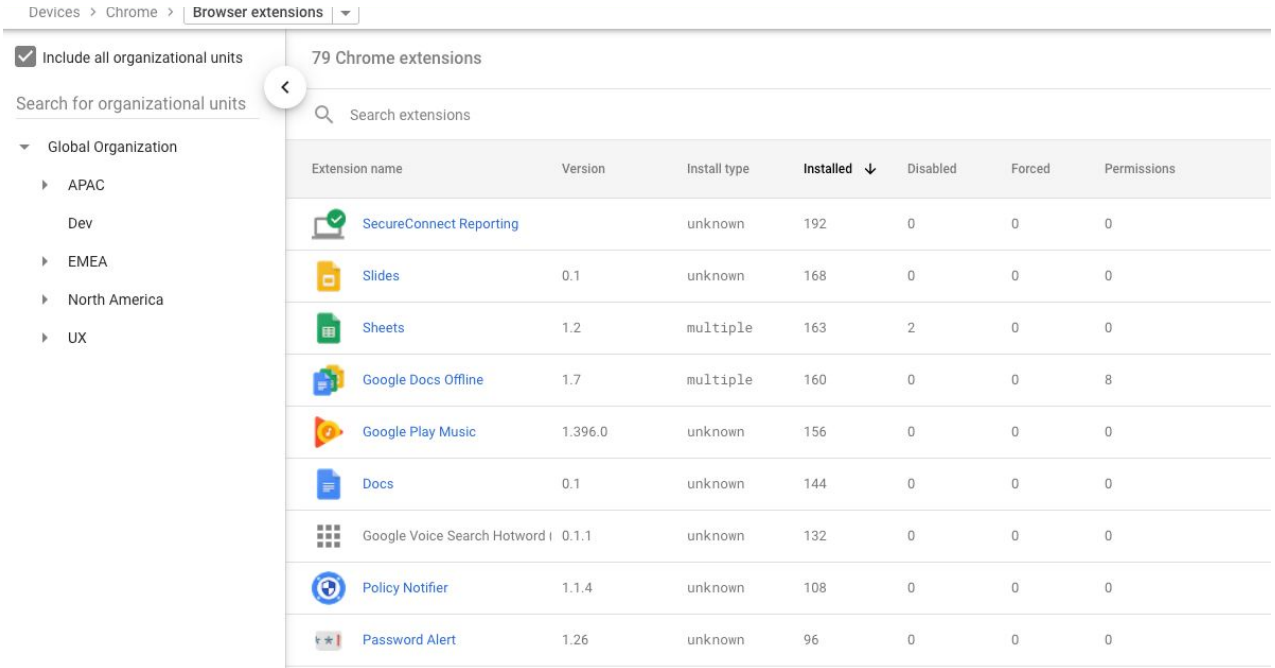
Global Organization > North America > Chicago

Installed apps & extensions

| Name | Status | Version | Install type | Browser version and channel | Profile |
|---|---|---|---|---|---|
| YouTube | Enabled | 4.2.8 | Normal | 83.0.4103.116 (Stable) | Fletcher (work) |
| Parasoft Recorder | Enabled | 2.2020.707.1000 | Admin | 83.0.4103.116 (Stable) | Fletcher (work) |
| Password Alert | Enabled | 1.27 | Admin | 83.0.4103.116 (Stable) | Fletcher (work) |
| Slides | Disabled | 0.10 | Normal | 83.0.4103.116 (Stable) | Fletcher (work) |
| Docs | Disabled | 0.10 | Normal | 83.0.4103.116 (Stable) | Fletcher (work) |
| Google Drive | Disabled | 14.2 | Normal | 83.0.4103.116 (Stable) | Fletcher (work) |
| Adobe Acrobat | Disabled | 15.1.2.0 | Sideload | 83.0.4103.116 (Stable) | Fletcher (work) |
| Sheets | Disabled | 1.2 | Normal | 83.0.4103.116 (Stable) | Fletcher (work) |
| Google Docs Offline | Disabled | 1.11.0 | Normal | 83.0.4103.116 (Stable) | Fletcher (work) |
| Super Mario New Tab Page | Disabled | 2.10.2 | Normal | 83.0.4103.116 (Stable) | Fletcher (work) |

Rows per page: 10    Page 1 of 2

- To get a viewpoint of all your installed extensions click on the Extensions Report link on the right.



Devices > Chrome > Browser extensions

☑ Include all organizational units

Search for organizational units

- Global Organization
  - APAC
  - Dev
  - EMEA
  - North America
  - UX

79 Chrome extensions

Search extensions

| Extension name | Version | Install type | Installed ↓ | Disabled | Forced | Permissions |
|---|---|---|---|---|---|---|
| SecureConnect Reporting | | unknown | 192 | 0 | 0 | 0 |
| Slides | 0.1 | unknown | 168 | 0 | 0 | 0 |
| Sheets | 1.2 | multiple | 163 | 2 | 0 | 0 |
| Google Docs Offline | 1.7 | multiple | 160 | 0 | 0 | 8 |
| Google Play Music | 1.396.0 | unknown | 156 | 0 | 0 | 0 |
| Docs | 0.1 | unknown | 144 | 0 | 0 | 0 |
| Google Voice Search Hotword ( | 0.1.1 | unknown | 132 | 0 | 0 | 0 |
| Policy Notifier | 1.1.4 | unknown | 108 | 0 | 0 | 0 |
| Password Alert | 1.26 | unknown | 96 | 0 | 0 | 0 |

- This view provides all of the extensions that are present within your enrolled browsers which you can click on to view the permissions (rights) that the extensions need to run as well as examples of machines that have those extensions installed.
  - For a complete list of all extensions and further details, it is recommended to use the Extension Takeout API. Here is a link to instructions on how to set this up as well as a link to an instructional video.
  - For all of the capabilities of the API refer to this link.

## Applying policies

Once you have your devices reporting into the console, any policies that you currently have applied within Group Policies will work with any policies that are pushed from the cloud.

- Local policy will take precedence over cloud policy by default if there is a conflict.
- Refer to this link for more information
  - If you want to override this functionality you can use this GPO policy to have cloud policy take precedence over local policy. There is another policy with the same name that does this for Google Update as well.
  - Not all policies that are available in GPO today are present within the admin console, but they all will be present in the near future.
  - The policies are fetched every ~3 hours. You can change the interval by using this policy.

## Resources

- Setting up Chrome Browser Cloud Management
- Chrome Browser Cloud Management Deployment Guide
- Chrome Browser Policy List
- Managing Extensions in your Enterprise Guide
- Chrome update management strategies