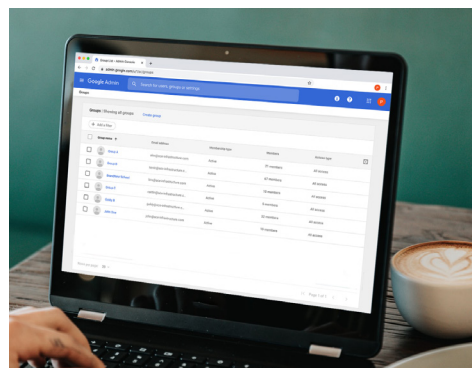




Configurer l'intégration de l'API Postman à la gestion cloud du navigateur Chrome

Dernière mise à jour : février 2022



| | |
|--|----|
| Choisir la méthode d'autorisation à utiliser | 2 |
| Choisir les champs d'application d'API (fonctionnalités) voulus | 2 |
| Créer le compte d'API dans la console d'administration | 3 |
| Créer le projet sur console.cloud.google.com | 4 |
| Option 1 : Accorder l'autorisation avec consentement | 5 |
| Option 2 : Accorder l'autorisation avec l'emprunt d'identité (compte de service) | 8 |
| Configurer l'intégration Postman | 11 |
| Vérifier la connexion à la gestion cloud du navigateur Chrome | 18 |

Ce document vous explique pas à pas comment configurer l'intégration d'API pour la [plate-forme d'API Postman](#). Postman vous permet d'accélérer la conception, la simulation et le test de vos scripts, et ainsi de simplifier grandement l'utilisation des API de la [gestion cloud du navigateur Chrome](#). Grâce à ces API, vous pouvez transmettre des données à la console et en extraire à grande échelle, et profiter de renseignements plus détaillés sur les navigateurs inscrits. Ce document suppose que vous avez déjà :

- accès à la console d'administration Google ;
- un compte de super-administrateur pour la configuration ;
- au moins un appareil inscrit dans la gestion cloud du navigateur Chrome pour le test.

Voici quelques liens utiles :

[Interface GitHub du navigateur Chrome pour les entreprises](#)

[Fichier README pour l'API](#)

[Console Google Cloud](#)

Choisir la méthode d'autorisation à utiliser

Google propose deux méthodes distinctes pour autoriser la connexion entre la gestion cloud du navigateur Chrome, l'API et Postman. Le choix de la méthode à privilégier dépend de votre future utilisation de l'API.

[Accorder l'autorisation avec consentement](#)

Chaque fois que vous demandez un jeton, l'administrateur sera invité à autoriser la requête via l'API.

- Les scripts Postman s'appuient sur cette méthode d'autorisation. Nous vous recommandons de l'utiliser pour le travail d'intégration afin de valider les appels d'API.

[Accorder l'autorisation avec l'emprunt d'identité ou le compte de service](#)

Si l'autorisation a été accordée une fois avec le compte de service, vous n'aurez pas à l'accorder à nouveau à chaque requête.

- Cette méthode est compatible avec les interactions entre serveurs, par exemple entre une application Web et un service Google. Elle est idéale pour les interactions entre serveurs dans un environnement de production.
-

Choisir les champs d'application d'API (fonctionnalités) voulus

L'API fournit quatre API différentes que vous pouvez activer. Les champs d'application que vous activez dépendent des requêtes et des actions que vous souhaitez faire via l'API. Vous pouvez également activer des accès en lecture, en écriture ou les deux.

Vous trouverez des descriptions détaillées de ce que chacun de ces champs d'application permet de faire dans la [documentation GitHub](#).

En voici un aperçu :

| Champ d'application | Description |
|---------------------|-------------|
|---------------------|-------------|

Accès en écriture

| | |
|---|---|
| https://www.googleapis.com/auth/admin.directory.device.chromerowsers | Gestion cloud du navigateur Chrome Vous permet de consulter et de modifier les navigateurs inscrits et les jetons d'inscription |
| https://www.googleapis.com/auth/admin.directory.orgunit | Unités organisationnelles : Vous permet de consulter et de modifier les unités organisationnelles |
| https://www.googleapis.com/auth/chrome.management.policy | Règle Chrome : Vous permet de consulter et de modifier les règles Chrome pour les appareils et les utilisateurs |

Accès en lecture seule

| | |
|---|---|
| https://www.googleapis.com/auth/admin.directory.device.chromerowsers.readonly | Gestion cloud du navigateur Chrome Vous permet d'obtenir des informations détaillées sur les navigateurs inscrits et les jetons d'inscription (lecture seule) |
| https://www.googleapis.com/auth/chrome.management.reports.readonly | Rapports : Vous permet d'obtenir des rapports sur les versions de Chrome et les applications installées (lecture seule) |
| https://www.googleapis.com/auth/chrome.management.appdetails.readonly | Informations sur les applications : Vous permet d'obtenir des informations détaillées sur les applications demandées ou spécifiées (lecture seule) |
| https://www.googleapis.com/auth/chrome.management.policy.readonly | Règle Chrome : Vous permet de consulter les règles Chrome pour les appareils et les utilisateurs (lecture seule) |
| https://www.googleapis.com/auth/admin.directory.orgunit.readonly | Unités organisationnelles : Vous permet de consulter les unités organisationnelles (lecture seule) |
| https://www.googleapis.com/auth/admin.reports.audit.readonly | Rapports sur la console d'administration : Vous permet de consulter les activités des administrateurs dans la console |

d'administration et les activités liées aux
jetons OAuth
(lecture seule)

Créer le compte d'API dans la console d'administration

Vous devez créer un compte utilisateur d'API pour pouvoir effectuer des appels d'API dans la console d'administration. Tous les droits associés à cette API particulière doivent être accordés à ce compte pour pouvoir transmettre des données à la console d'administration et en extraire.

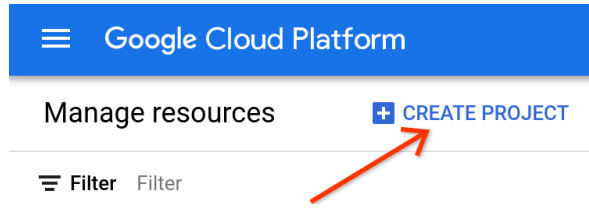
1. Accédez à la console d'administration et connectez-vous à un compte d'administrateur bénéficiant de tous les droits nécessaires pour activer l'accès à l'API et créer des comptes utilisateur (il s'agit généralement d'un compte de super-administrateur).
2. Sélectionnez Rôles d'administrateur > Créer un rôle.
3. Donnez un nom au rôle d'API et sélectionnez les droits voulus sous "Unités organisationnelles", "Gestion de Google Chrome", puis cliquez sur "Créer un rôle".
4. Créez un compte utilisateur auquel vous attribuerez le rôle d'API sous Annuaire > Utilisateurs > Ajouter un nouvel utilisateur.
5. Donnez un nom au compte d'API et créez une adresse e-mail, puis cliquez sur "Ajouter un nouvel utilisateur".
6. Accédez au compte utilisateur créé à l'étape précédente. Dans "Rôles et droits d'administrateur", sélectionnez le rôle créé à l'étape 3.
 - a. Remarque : L'application de la nouvelle autorisation peut prendre quelques minutes.

Créer le projet sur console.cloud.google.com

1. Accédez à console.cloud.google.com.

Assurez-vous d'être connecté à la console Cloud avec le compte que vous venez de créer pour le rôle d'API.

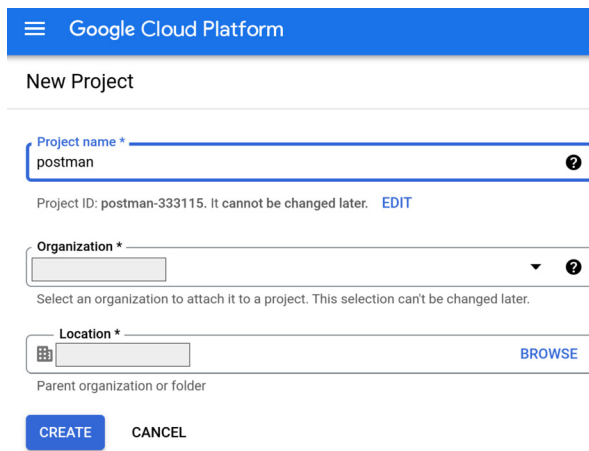
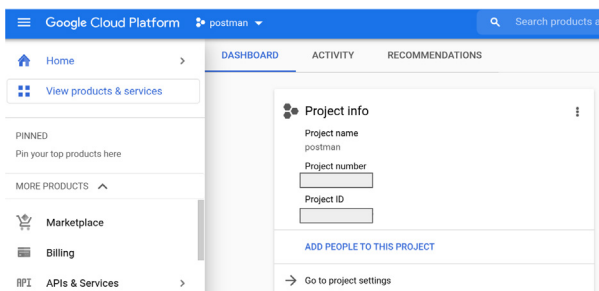
2. Cliquez sur "Créer un projet".



3. Saisissez le nom du projet.

(Vous pouvez choisir le nom que vous voulez.) L'emplacement indiqué doit correspondre au domaine de votre console d'administration.

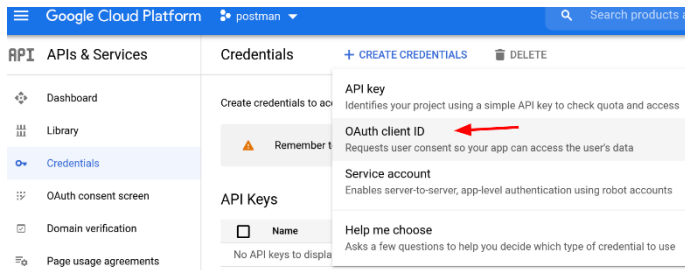
Cliquez sur "Créer".

A screenshot of the 'New Project' form in the Google Cloud Platform console. The form is titled 'New Project' and has a blue header with the Google Cloud Platform logo. The form contains three main sections: 'Project name *' with a text input field containing 'postman' and a question mark icon; 'Organization *' with a dropdown menu and a question mark icon; and 'Location *' with a text input field and a 'BROWSE' button. Below these sections are two buttons: 'CREATE' and 'CANCEL'. The 'Project ID' is displayed as 'postman-333115' and is noted as 'cannot be changed later'.

4. Une fois le projet créé, assurez-vous qu'il reste sélectionné.

Option 1 : Accorder l'autorisation avec consentement

1. Ouvrez console.cloud.google.com, sélectionnez le projet que vous venez de créer et accédez à API et services > Identifiants, puis cliquez sur "Créer des identifiants" et sélectionnez "ID client OAuth".



2. Sélectionnez "Application Web" dans le champ "Type d'application" et indiquez un nom.
3. Sous "URI de redirection autorisés", saisissez les URI suivants :
 - a. <https://www.getpostman.com/oauth2/callback>
 - b. <https://oauth.pstmn.io/v1/browser-callback>
4. Cliquez sur "Créer".

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
Postman
The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ⓘ
For use with requests from a browser
[+ ADD URI](#)

Authorized redirect URIs ⓘ
For use with requests from a web server
URIs *
<https://www.getpostman.com/oauth2/callback>

[+ ADD URI](#)

[CREATE](#) [CANCEL](#)

5. Dans la fenêtre "Client OAuth créé", cliquez sur "Télécharger le fichier JSON".
6. Accédez à l'écran de consentement OAuth > Configurer l'écran de consentement.
Lorsque vous utilisez OAuth 2.0 pour l'autorisation, votre application demande des autorisations pour un ou plusieurs niveaux d'accès à partir d'un compte Google. Google présente à l'utilisateur un écran de consentement sur lequel s'affiche un récapitulatif de votre projet et des règles qui s'y appliquent, ainsi que les niveaux d'accès demandés.

Il existe deux types de niveaux d'accès :

- a. **Interne** : réservé à vos utilisateurs Google Workspace. Une identité Google ou Google Workspace est nécessaire.
 - b. **Externe** : accessible à tous les utilisateurs de test disposant d'un compte Google. Votre application démarrera en mode test et ne sera accessible qu'aux personnes figurant sur votre liste d'utilisateurs de test. Une fois votre application prête pour la production, il est possible que vous deviez la faire valider.
7. **Saisissez le nom de l'application** et l'adresse e-mail d'assistance utilisateur (il s'agit de l'adresse e-mail de votre compte d'administrateur dans la console d'administration). Vous pouvez également choisir d'afficher un logo personnalisé.
 8. Sous "Domaines autorisés", saisissez **getpostman.com**.
 9. **Indiquez l'adresse e-mail** à laquelle vous souhaitez recevoir des notifications de la part de Google sur les modifications apportées à votre projet, puis cliquez sur "Enregistrer et continuer".

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *
Postman API

The name of the app asking for consent

User support email *

For users to contact you with questions about their consent

App logo [BROWSE](#)

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

Authorized domains [?](#)

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

getpostman.com

[+ ADD DOMAIN](#)

Developer contact information

Email addresses *

These email addresses are for Google to notify you about any changes to your project.

10. Cliquez sur "Ajouter ou supprimer des champs d'application" pour ajouter les champs d'application appropriés manuellement. Ils figurent tous dans la [liste des champs d'application accessible dans l'interface GitHub du navigateur Chrome pour les entreprises](#). Cliquez sur "Enregistrer et continuer".

Remarque : La liste contient des accès en lecture seule et des accès complets. Choisissez les champs d'application dont vous avez besoin pour votre cas d'utilisation particulier.

✕ Update selected scopes

i Only scopes for enabled APIs are listed below. To add a missing scope to this screen, find and enable the API in the [Google API Library](#) or use the Pasted Scopes text box below. Refresh the page to see any new APIs you enable from the Library.

Filter Enter property name or value **?**

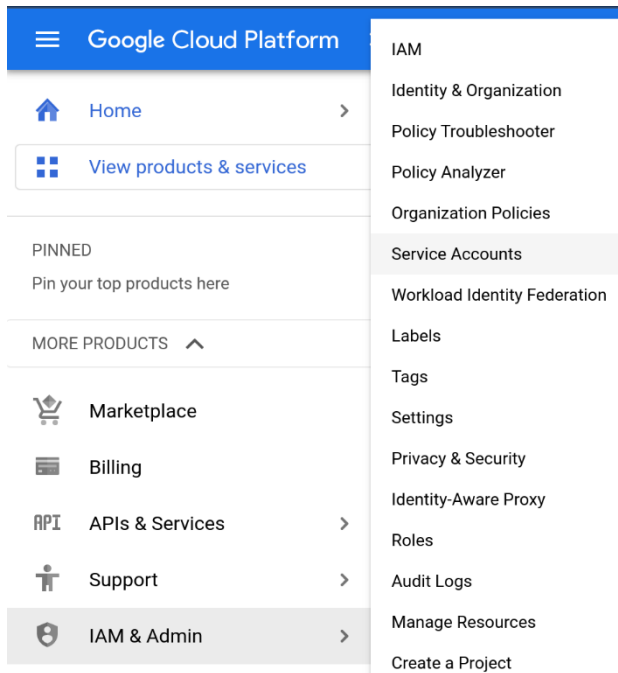
| <input type="checkbox"/> | API ↑ | Scope | User-facing description |
|-------------------------------------|-------|---|--|
| <input checked="" type="checkbox"/> | | .../auth/admin.directory.device.chromebrowsers | See and manage Chrome browsers under your organization |
| <input checked="" type="checkbox"/> | | .../auth/admin.directory.device.chromebrowsers.readonly | See Chrome browsers under your organization |
| <input checked="" type="checkbox"/> | | .../auth/admin.directory.orgunit | View and manage organization units on your domain |
| <input checked="" type="checkbox"/> | | .../auth/admin.directory.orgunit.readonly | View organization units on your domain |
| <input checked="" type="checkbox"/> | | .../auth/admin.reports.audit.readonly | View audit reports for your G Suite domain |
| <input checked="" type="checkbox"/> | | .../auth/chrome.management.appdetails.readonly | See detailed information about apps installed on Chrome browsers and devices managed by your organization |
| <input checked="" type="checkbox"/> | | .../auth/chrome.management.reports.readonly | See reports about devices and Chrome browsers managed within your organization |
| <input checked="" type="checkbox"/> | | .../auth/chrome.management.policy.readonly | See policies applied to Chrome OS and Chrome Browsers managed within your organization |
| <input checked="" type="checkbox"/> | | .../auth/chrome.management.policy | See, edit, create or delete policies applied to Chrome OS and Chrome Browsers managed within your organization |

11. **Facultatif** : Ajoutez un ou plusieurs utilisateurs qui bénéficieront de droits d'accès pendant que l'application est à l'état "Test". Incluez le compte que vous avez utilisé pour créer le projet ainsi que tout autre compte auquel vous souhaitez accorder l'accès. Pour ce faire, cliquez sur "Ajouter des utilisateurs".
12. Cliquez sur "Enregistrer et continuer", passez en revue l'écran récapitulatif, puis cliquez sur "Revenir au tableau de bord".
13. Si vous le souhaitez, vous pouvez alors **publier votre application**.
- Une fois que vous définissez l'état de votre application sur **En production**, elle devient disponible pour tous les utilisateurs disposant d'un compte Google. En fonction de la configuration de votre écran OAuth, il est possible que vous deviez faire valider votre application.
-

Option 2 : Accorder l'autorisation avec l'emprunt d'identité (compte de service)

Créer un compte de service (autorisation avec emprunt d'identité)

1. Accédez à [Comptes de service](#) dans "IAM et administration". Si vous y êtes invité, sélectionnez un projet.



2. Cliquez sur "Créer un compte de service", puis saisissez un nom et une description pour ce compte.



3. Vous pouvez utiliser l'ID de compte de service par défaut ou en choisir un autre, unique. Une fois que vous avez terminé, cliquez sur "Créer".

1 Service account details

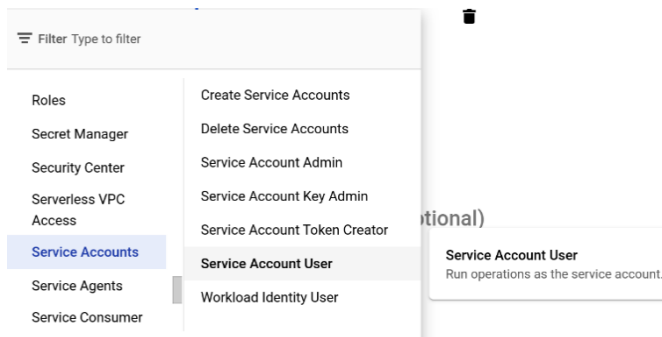
Service account name *
postman
Display name for this service account

Service account ID *
postman @ [redacted] .com X ↺

Service account description
Describe what this service account will do

[CREATE AND CONTINUE](#)

4. Sous "Autorisations de compte de service", veillez à attribuer le rôle **Utilisateur du compte de service** à ce compte. Cliquez sur "Continuer".
5. À l'écran "Autoriser les utilisateurs à accéder à ce compte de service", vous pouvez ajouter des **utilisateurs** auxquels vous souhaitez accorder l'accès, puis cliquer sur "OK".



6. À l'écran suivant, sélectionnez le compte de service que vous venez de créer.

Service accounts for project "postman"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account](#)


Filter Enter property name or value

| <input type="checkbox"/> | Email | Status | Name ↑ | Description | Key ID | Key creation date | OAuth 2 Client ID ? | Actions |
|--------------------------|--------------------|--------|---------|-------------|---------|-------------------|---------------------|--------------|
| <input type="checkbox"/> | postman@[redacted] | ✓ | postman | | No keys | | [redacted] | [redacted] ⋮ |

7. Cliquez sur l'onglet "Clés" en haut de la page, puis sélectionnez "Créer une clé" dans le menu déroulant. Choisissez le type de clé "JSON".

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

 Service account keys could pose a security risk if compromised. We [here](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).
[Learn more about setting organization policies for service accounts](#)

ADD KEY ▾

- Create new key
- Upload existing key

| Key creation date | Key expiration date |
|-------------------|---------------------|
| | |

8. La nouvelle paire de clés publique/privée est générée et téléchargée sur votre ordinateur. Il s'agit de la seule copie dont vous disposez. Elle vous donne accès à la console Cloud, et doit donc être **stockée en sécurité**.
9. Cliquez sur l'onglet "Détails" du compte de service sélectionné et copiez l'adresse e-mail de type `<nom_du_projet>-<id>@<nom_du_projet>.iam.gserviceaccount.com`.

DETAILS PERMISSIONS KEYS METRICS LOGS

Service account details

Name
postman SAVE

Description SAVE

Email
postman@


10. Accédez à la page "API et services" pour le projet que vous avez créé plus tôt dans la console Google Cloud. Cliquez sur "Activer les API et les services".

Google Cloud Platform postman

API APIs & Services APIs & Services + ENABLE APIS AND SERVICES

Enabled APIs & services

11. Recherchez les API suivantes, sélectionnez-les une par une et cliquez sur le bouton "Gérer".

 **Chrome Management API**
Google

The Chrome Management API is a suite of services that allows Chrome administrators to view, manage...

MANAGE TRY THIS API

- a. API Chrome Management =
<https://console.developers.google.com/apis/api/chromemanagement.googleapis.com/overview>
- b. API Chrome Policy =
<https://console.developers.google.com/apis/api/chromepolicy.googleapis.com/overview>
- c. API Admin SDK =
<https://console.developers.google.com/apis/api/admin.googleapis.com/overview>

12. Reconnectez-vous à la [console d'administration Google](#) avec votre compte de super-administrateur.


13. Accédez à [Compte > Rôles d'administrateur](#) et sélectionnez le rôle de compte de service que vous avez créé à l'étape de [création de votre compte d'API](#).

14. Sélectionnez la rubrique "Administrateurs" en haut de la page.

Admin roles > Service Account User

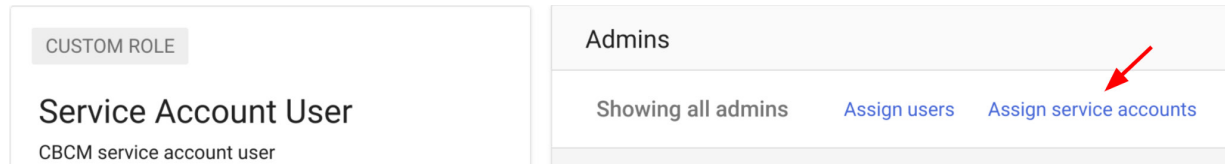
CUSTOM ROLE

Service Account User
CBCM service account user

Admins 

Admins assigned
Service Account, niro-api man, Service account

15. Cliquez sur "Attribuer aux comptes de service".

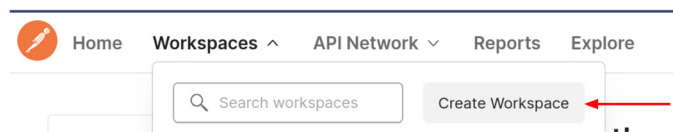


16. Collez l'adresse e-mail copiée à l'étape 9 et cliquez sur "Ajouter".

Configurer l'intégration Postman

Configuration d'un compte

1. Accédez à [Postman.com](https://postman.com) et créez un compte ou connectez-vous à un compte existant.
2. Une fois votre compte configuré, sélectionnez **Workspaces > Create Workspace (Espaces de travail > Créer un espace de travail)**. Indiquez un nom et sélectionnez le niveau de visibilité souhaité, puis cliquez sur le bouton "Create Workspace" (Créer un espace de travail).



Create workspace

Name

Summary

Add a brief summary about this workspace.

Visibility

Determines who can access this workspace.

Personal

Only you can access

Private

Only invited team members can access

Team

All team members can access

Public

Everyone can view

Create Workspace

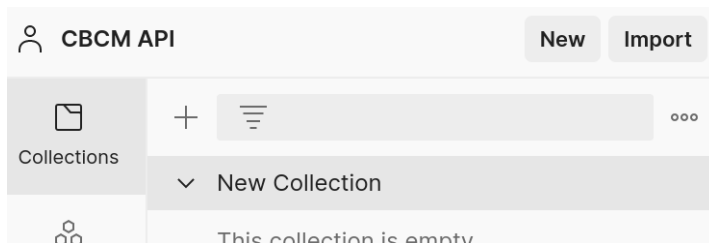
Cancel

Importation d'une collection depuis l'interface GitHub du navigateur Chrome pour les entreprises

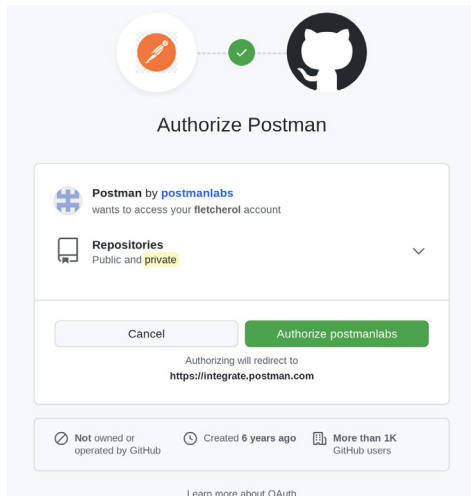
Nous vous conseillons d'importer les collections disponibles dans l'[interface GitHub du navigateur Chrome pour les entreprises](#). Elles fournissent des exemples de scripts pour des cas d'utilisation courants concernant les appels d'API effectués à la gestion cloud du navigateur Chrome. Vous pouvez les importer en téléchargeant les fichiers ou en passant par votre dépôt GitHub.

Importation via le dépôt de code

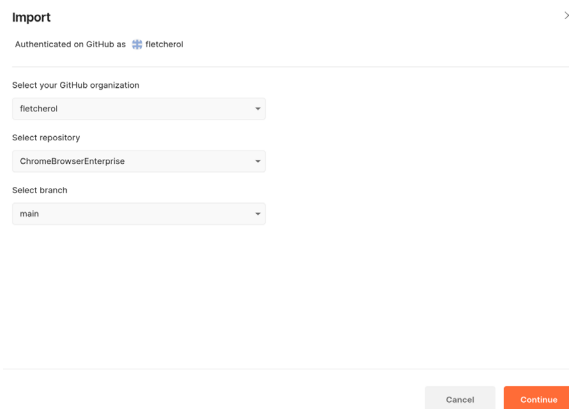
1. Connectez-vous à votre compte GitHub.
2. Accédez à <https://github.com/google/ChromeBrowserEnterprise> et cliquez sur le bouton "Fork" (Duplication) pour ajouter la collection à votre dépôt.
3. Dans Postman, où votre espace de travail est toujours sélectionné, cliquez sur le bouton "Import" (Importer).



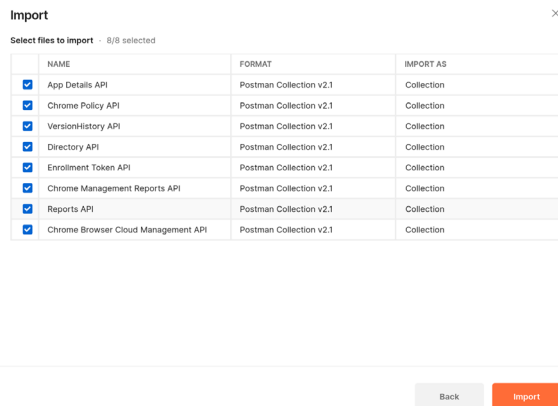
4. Sélectionnez Code repository > GitHub (Dépôt de code > GitHub).
5. Connectez-vous à votre compte GitHub, cliquez sur le bouton "Authorize postmanlabs" (Autoriser postmanlabs) et confirmez votre mot de passe.



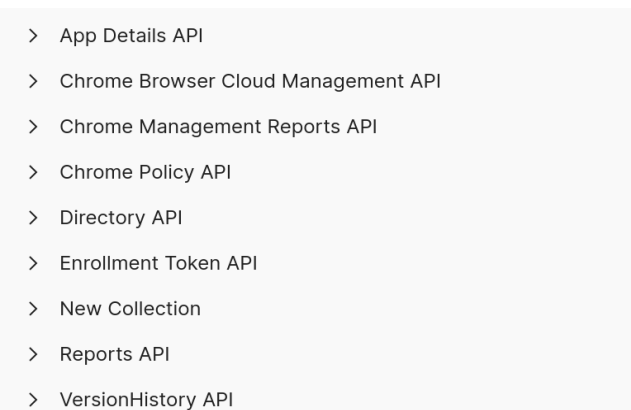
6. Lorsque c'est fait, l'option sélectionnable "ChromeBrowserEnterprise" devrait s'afficher dans le menu déroulant de la section "Import" (Importer), sous "Select repository" (Sélectionnez un dépôt). Cliquez sur "Continue" (Continuer).



7. Sélectionnez les collections que vous souhaitez importer, puis cliquez sur "Import" (Importer).

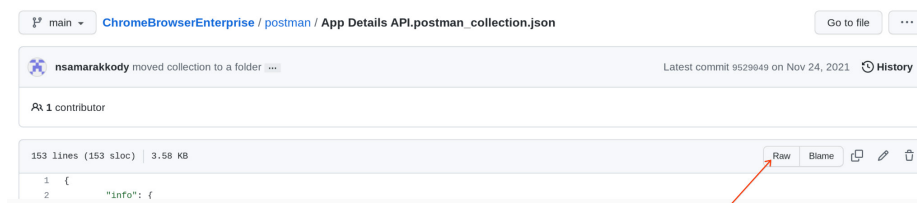


8. Une fois l'importation terminée, toutes les collections sélectionnées devraient apparaître dans votre espace de travail Postman.



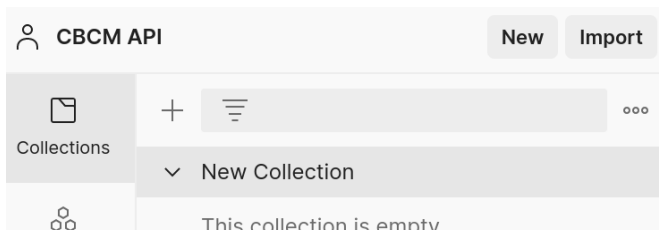
Importation via le téléchargement des fichiers

1. Accédez à l'[interface GitHub du navigateur Chrome pour les entreprises](#) et sélectionnez la collection que vous voulez importer.
2. Cliquez sur le bouton "Raw" (Brut).

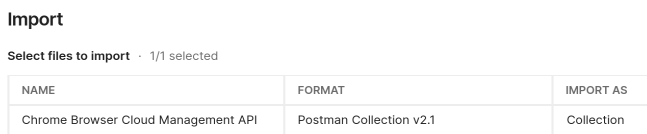


3. Effectuez un clic droit et cliquez sur "Save as .json" (Enregistrer au format .json).

4. Dans Postman, où votre espace de travail est toujours sélectionné, cliquez sur le bouton "Import" (Importer).



5. Cliquez sur "Upload Files" (Importer des fichiers), sélectionnez le fichier JSON que vous venez de télécharger et cliquez sur "Import" (Importer).



Les étapes suivantes sont nécessaires seulement si la méthode d'autorisation avec consentement a été choisie.

6. Lorsque la collection s'affiche, vous devez remplir les champs en rouge.

| | |
|--------------------|--|
| Auth URL ⓘ | <input type="text" value="{{auth_uri}}"/> |
| Access Token URL ⓘ | <input type="text" value="{{token_uri}}"/> |
| Client ID ⓘ | <input type="text" value="{{client_id}}"/> |
| Client Secret ⓘ | <input type="text" value="{{client_secret}}"/> |

7. Pour "Auth URL" (URL d'authentification), saisissez :
<https://accounts.google.com/o/oauth2/auth>
8. Pour "Access Token URL" (URL de jeton d'accès), saisissez :
<https://oauth2.googleapis.com/token>
9. Récupérez l'ID client et le code secret du client dans la section "API et services" de la console Cloud (<https://console.cloud.google.com/> ou [lien direct](#)) et copiez-les respectivement dans le

champ "Client ID" (ID client) et "Client Secret" (Code secret du client) dans Postman.

Client ID for Web application DOWNLOAD JSON RESET SECRET DELETE

Name *
Postman
The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

Client ID
Client secret
Creation date

- a. Nous vous recommandons d'ajouter ces valeurs en tant que variables pour simplifier leur ajout à plusieurs collections à mesure que vous les importez et pour assurer la sécurité des données sensibles.
- b. Pour pouvoir utiliser les mêmes variables pour plusieurs collections, vous devez en faire des variables globales.

Pour en savoir plus sur les variables dans Postman, consultez [cette page](#).

10. Récupérez l'ID client et le code secret du client dans la section "API et services" de la console Cloud (<https://console.cloud.google.com/> ou [lien direct](#)) et copiez-les respectivement dans le champ "Client ID" (ID client) et "Client Secret" (Code secret du client) dans Postman.
11. Si vous utilisez la version du navigateur de Postman, le champ "Callback URL" (URL de rappel) est prérempli.
Avec la version pour ordinateur, il se peut que vous deviez saisir manuellement l'URL suivante :
<https://www.getpostman.com/oauth2/callback>
12. Cliquez sur le bouton "Get New Access Token" (Obtenir un nouveau jeton d'accès).
13. Lorsque vous cliquez sur ce bouton, vous êtes invité à vous authentifier à l'aide de vos identifiants d'administrateur associés à la gestion cloud du navigateur Chrome.
Assurez-vous que le compte en question dispose des droits d'API nécessaires pour les champs d'application que vous avez ajoutés.

accounts.google.com/o/oauth2/auth/oauthchooseaccount?response_type=code&clie...




Sign in with Google

Choose an account
to continue to [oauth.pstmn.io](#)

oauth.pstmn.io wants to access
your Google Account

 admin@fletcher.bigr.name

This will allow **oauth.pstmn.io** to:

- See and manage Chrome browsers under your organization 
- View and manage organization units on your domain 
- See, edit, create or delete policies applied to Chrome OS and Chrome Browsers managed within your organization 

Make sure you trust oauth.pstmn.io

You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

See [oauth.pstmn.io's Privacy Policy](#) and [Terms of Service](#).


14. Une fois l'authentification réussie, le nouveau jeton que vous utiliserez pour authentifier les requêtes aux API s'affichera.

Cliquez sur le bouton "Use Token" (Utiliser le jeton) et les informations du jeton seront automatiquement remplies dans la collection.

Par défaut, les jetons sont valables une heure.

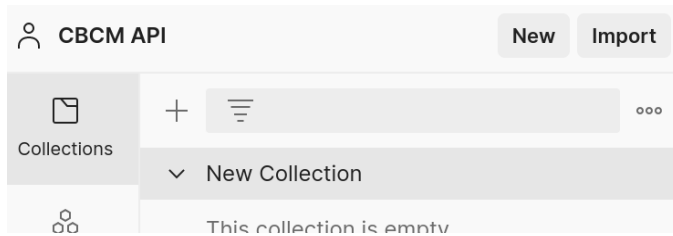
MANAGE ACCESS TOKENS ✕

All Tokens Delete ▼ Token Details Use Token

| Token Name | |
|--------------|--|
| Token Name | Token Name  |
| Access Token | <div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div> |
| Token Type | Bearer |
| expires_in | 3599 |
| scope | https://www.googleapis.com/auth/admin.directory.orgunit https://www.googleapis.com/auth/admin.directory.device.chromebrowsers https://www.googleapis.com/auth/chrome.management.policy |

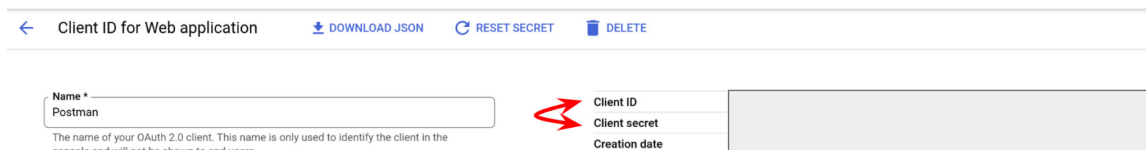
Création d'une collection

1. Dans l'onglet "Collections", cliquez sur le symbole + pour créer une nouvelle collection.



Les étapes suivantes sont nécessaires seulement si la méthode d'autorisation avec consentement a été choisie.

2. Sélectionnez "OAuth2" dans le champ "Type of Authorization" (Type d'autorisation).
3. Pour "Callback URL" (URL de rappel) :
 - a. Si vous utilisez la version du navigateur de Postman, ce champ est prérempli. Sur la version pour ordinateur, saisissez l'URL suivante : <https://www.getpostman.com/oauth2/callback>
4. Pour "Auth URL" (URL d'authentification), saisissez : <https://accounts.google.com/o/oauth2/auth>
5. Pour "Access Token URL" (URL de jeton d'accès), saisissez : <https://oauth2.googleapis.com/token>
6. Récupérez l'ID client et le code secret du client dans la section "API et services" de la console Cloud (<https://console.cloud.google.com/> ou [lien direct](#)) et copiez-les respectivement dans le champ "Client ID" (ID client) et "Client Secret" (Code secret du client) dans Postman.



Nous vous recommandons d'ajouter ces valeurs en tant que variables pour simplifier leur ajout à plusieurs collections à mesure que vous les importez et pour assurer la sécurité des données sensibles.

Pour en savoir plus sur les variables dans Postman, consultez [cette page](#).

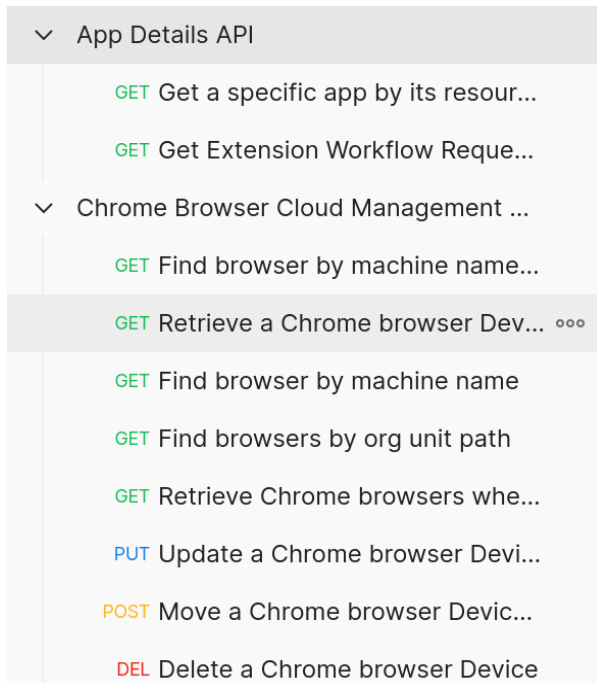
7. Ajoutez le ou les champs d'application spécifiques à l'API Cloud Management souhaités. ([Reportez-vous à cette section pour en savoir plus.](#)) Chaque champ d'application doit être séparé par un espace.
 8. Cliquez sur le bouton "Get New Access Token" (Obtenir un nouveau jeton d'accès).
-

Vérifier la connexion à la gestion cloud du navigateur Chrome

Toutes les collections rassemblées dans l'interface GitHub du navigateur Chrome pour les entreprises contiennent des exemples de scripts pour vous aider à vous lancer, y compris des exemples concernant les requêtes GET, PUT, POST et DEL. Lorsque vous avez importé une collection, vous pouvez exécuter ces scripts pour vérifier que Postman est en mesure d'envoyer des requêtes à la gestion cloud du navigateur Chrome.

1. Cliquez sur la collection que vous avez importée.

Les étapes suivantes (2 à 6) sont nécessaires seulement si la méthode d'autorisation avec consentement a été choisie.



2. Confirmez que les champs "Auth URL", "Access Token URL", "Client ID" et "Client Secret" (URL d'autorisation, URL de jeton d'accès, ID client et Code secret du client) ainsi que la section concernant les champs d'application sont bien remplis, soit avec les valeurs correspondantes, soit avec une variable.

3. Cliquez sur le bouton "Get New Access Token" (Obtenir un nouveau jeton d'accès).

App Details API

Authorization ● Pre-request Script Tests Variables ●

This authorization method will be used for every request in this collection. You can override this by specifying one in the request.

ya29.A0ARrdaM_ydeit346V0Z...

Header Prefix ⓘ Bearer

Configure New Token

Configuration Options ● Advanced Options

Token Name AppDetailsApiToken

Grant Type Authorization Code

Callback URL ⓘ https://oauth.pstmn.io/v1/browser-call

Auth URL ⓘ {{Auth URL}}

Access Token URL ⓘ {{Access Token URL}}

Client ID ⓘ {{Client ID}}

Client Secret ⓘ {{Client Secret}}

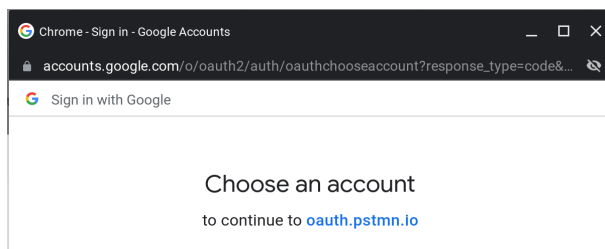
Scope ⓘ https://www.googleapis.com/auth/cl...

State ⓘ State

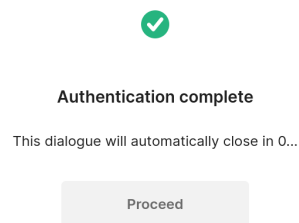
Client Authentication Send as Basic Auth header

Get New Access Token

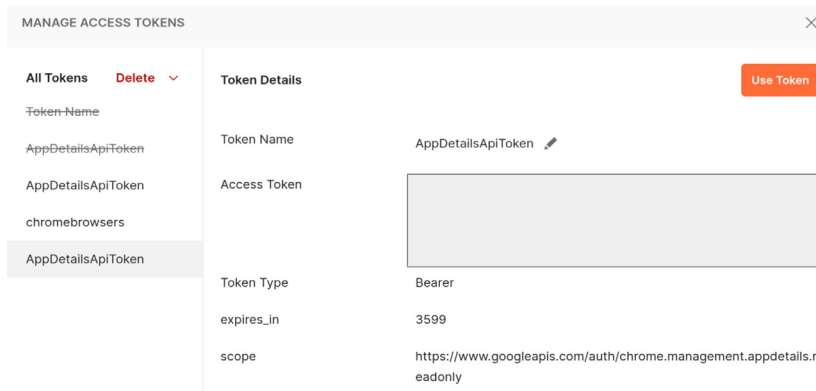
4. Choisissez le compte pour lequel vous souhaitez vous authentifier.



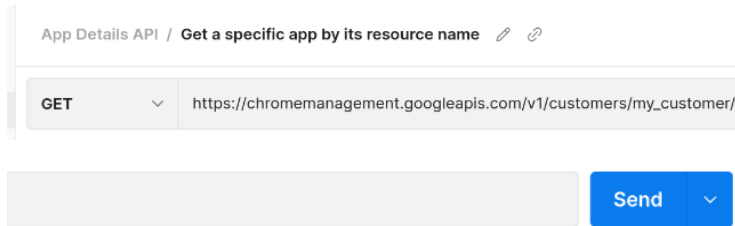
5. Une boîte de dialogue confirmant l'authentification s'affichera si toutes les informations sont correctes.



6. Cliquez sur le bouton "Use Token" (Utiliser le jeton).



7. Sélectionnez la requête que vous souhaitez effectuer et cliquez sur "Send" (Envoyer).



8. La réponse s'affichera en dessous. Si vous le souhaitez, vous pouvez choisir d'autres formats à la place de JSON dans le menu déroulant.

