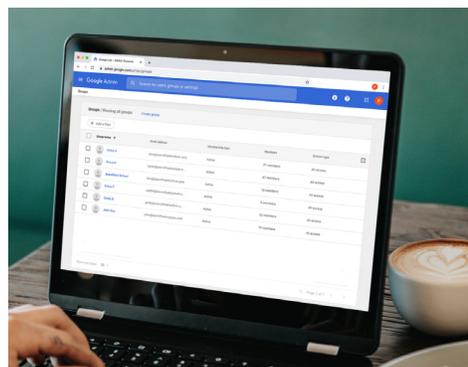




Erste Schritte mit der Integration der Postman API in der Chrome-Verwaltung über die Cloud

Zuletzt aktualisiert: Februar 2022



Die passende Autorisierungsmethode wählen	2
Die gewünschten API-Bereiche (Funktionalität) wählen	2
Das API-Konto in der Admin-Konsole erstellen	3
Ihr Projekt auf console.cloud.google.com erstellen	5
Methode 1: Autorisierung per Zustimmung	6
Methode 2: Autorisierung per Identitätsübertragung (Dienstkonto)	10
Integration der Postman API einrichten	14
Die Verbindung zur Chrome-Verwaltung über die Cloud überprüfen	22

In diesem Dokument erfahren Sie, wie Sie die Integration über die [Postman API-Plattform](#) einrichten. Mit der Nutzung von Postman können Sie das Design, Mocking und Testing Ihrer Skripts beschleunigen, um die Verwendung von APIs für die [Chrome-Verwaltung über die Cloud](#) so einfach wie noch nie zu gestalten. Die Cloud Management APIs ermöglichen Ihnen, Daten in großem Umfang an die Konsole zu senden sowie abzurufen und so die Berichte über Ihre registrierten Browser zu verbessern. In diesem Dokument wird Folgendes vorausgesetzt:

- Vorhandener Zugriff auf die Admin-Konsole
- Ein Super Admin-Konto für die Einrichtung
- Mindestens ein (oder mehrere) Gerät(e), die zum Testen in der Chrome-Verwaltung über die Cloud angemeldet sind

Hier finden Sie nützliche Links:

- [Chrome Enterprise-GitHub](#)
 - [Readme-Datei für die API](#)
 - [Google Cloud Platform Console](#)
 - [Postman API-Plattform](#)
-

Die passende Autorisierungsmethode wählen

Google bietet zwei unterschiedliche Methoden an, um die Verbindung zwischen der Chrome-Verwaltung über die Cloud, der API und Postman zu autorisieren. Je nachdem, wie die API verwendet werden soll, empfiehlt sich jeweils eine dieser Methoden.

[Autorisierung per Zustimmung](#)

Bei jeder Token-Anfrage wird der Administrator dazu aufgefordert, die Anfrage über die API zu autorisieren.

- Postman-Skripts werden mithilfe dieser Autorisierungsmethode entwickelt. Um API-Aufrufe zu prüfen, empfiehlt sich diese Methode für die schrittweise Entwicklung der Integration.

[Autorisierung per Identitätsübertragung oder Dienstkonto](#)

Nach der einmaligen Autorisierung mit dem Dienstkonto finden bei Anfragen keine weiteren Aufforderungen zur Autorisierung statt.

- Unterstützt Interaktionen zwischen Servern, beispielsweise zwischen einer Webanwendung und einem Google-Dienst. Eignet sich optimal für Produktionsinteraktionen zwischen Servern.

Die gewünschten API-Bereiche (Funktionalität) wählen

Die API stellt vier verschiedene APIs bereit, die Sie aktivieren können. Je nach Anfrage oder Aktion, die Sie über die API durchführen möchten, variiert der zu aktivierende Bereich. Sie können die Aktivierung zusätzlich mit Lese- oder Schreibzugriff (oder beidem) vornehmen.

Eine vollständige Beschreibung der jeweiligen Funktionen finden Sie in der [GitHub-Dokumentation](#).

Ein kurzer Überblick über die Bereiche:

Bereich	Beschreibung
Bereiche mit Schreibzugriff	
https://www.googleapis.com/auth/admin-directory.device.chromerowsers	Chrome-Verwaltung über die Cloud Registrierte Browser und Tokens aufrufen und modifizieren

https://www.googleapis.com/auth/admin.directory.orgunit	Organisationseinheiten – Organisationseinheiten aufrufen und modifizieren
https://www.googleapis.com/auth/chrome.management.policy	Chrome-Richtlinien – Chrome-Richtlinien für Geräte und Nutzer aufrufen und modifizieren

Schreibgeschützte Bereiche

https://www.googleapis.com/auth/admin.directory.device.chromebrowsers.readonly	Chrome-Verwaltung über die Cloud Detaillierte Informationen zu registrierten Browsern und Tokens erhalten (schreibgeschützt)
https://www.googleapis.com/auth/chrome.management.reports.readonly	Berichte – Chrome-Versionen und installierte Anwendungen (schreibgeschützt)
https://www.googleapis.com/auth/chrome.management.appdetails.readonly	Anwendungsdetails – detaillierte Informationen zu angeforderten oder bestimmten Anwendungen erhalten (schreibgeschützt)
https://www.googleapis.com/auth/chrome.management.policy.readonly	Chrome-Richtlinien – Chrome-Richtlinien für Geräte und Nutzer aufrufen (schreibgeschützt)
https://www.googleapis.com/auth/admin.directory.orgunit.readonly	Organisationseinheiten – Organisationseinheiten aufrufen (schreibgeschützt)
https://www.googleapis.com/auth/admin.reports.audit.readonly	Admin-Konsolen-Berichte – Aktivitäten von Administratoren über die Admin-Konsole und OAuth-Token-Aktivitäten aufrufen (schreibgeschützt)

Das API-Konto in der Admin-Konsole erstellen

Um API-Aufrufe an die Admin-Konsole vorzunehmen, muss ein API-Nutzerkonto erstellt werden. Dieses Konto erfordert alle spezifischen API-Berechtigungen, um Daten von der Admin-Konsole zu senden und abzurufen.

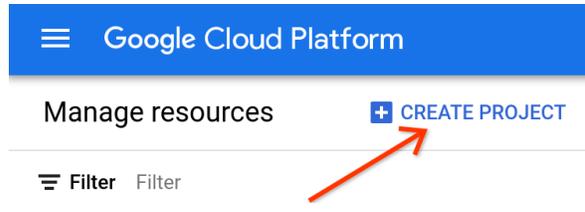
1. Um den API-Zugriff zu aktivieren und ein neues Nutzerkonto (in der Regel ein Super Admin-Konto) zu erstellen, melden Sie sich in der Admin-Konsole mit dem Administratorkonto an, das über die notwendigen Berechtigungen verfügt.
2. Gehen Sie zu „Administratorrollen“ > „Rolle erstellen“.
3. Erstellen Sie einen Namen für Ihre API-Rolle, wählen Sie die gewünschten Berechtigungen unter „Organisationseinheiten“ > „Chrome-Verwaltung“ aus und klicken Sie anschließend auf die Schaltfläche „Rolle erstellen“.
4. Erstellen Sie das Nutzerkonto, dem Sie die API-Rolle zuweisen werden, unter „Verzeichnis“ > „Nutzer“ > „Neuen Nutzer hinzufügen“.
5. Geben Sie dem API-Konto eine Bezeichnung, erstellen Sie eine E-Mail-Adresse und klicken Sie auf die Schaltfläche „Neuen Nutzer hinzufügen“.
6. Klicken Sie auf das im vorherigen Schritt erstellte Nutzerkonto und dann auf „Administratorrollen und -berechtigungen“.
Wählen Sie nun die Rolle aus, die Sie in Schritt 3 erstellt haben.
 - a. Hinweis: Es kann ein paar Minuten dauern, bis die neue Berechtigung übertragen wird.

Ihr Projekt auf console.cloud.google.com erstellen

1. Öffnen Sie console.cloud.google.com.

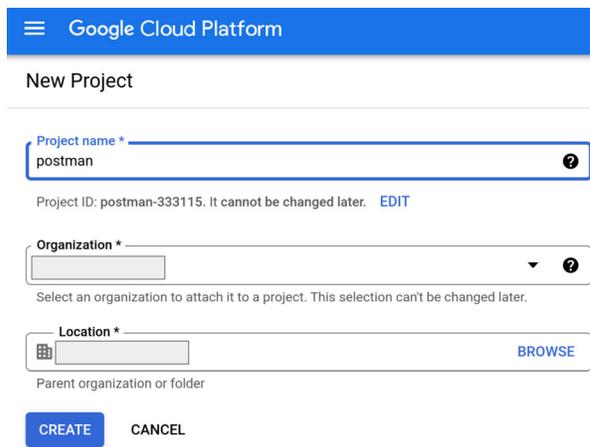
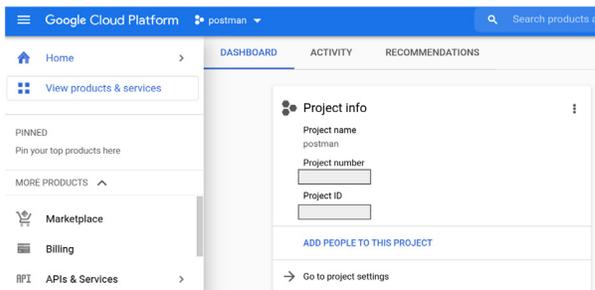
Stellen Sie sicher, dass Sie mit dem Konto, dem Sie die im vorherigen Abschnitt erstellte API-Rolle zugewiesen haben, in der Cloud Console angemeldet sind.

2. Klicken Sie auf die Schaltfläche „Projekt erstellen“.



3. Geben Sie einen Projektnamen ein.

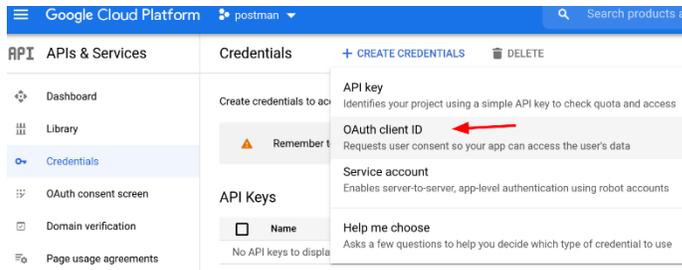
Der Ort sollte mit der Domain Ihrer Admin-Konsole übereinstimmen. Klicken Sie auf „Erstellen“.

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 several fields: 'Project name *' with the value 'postman' and a question mark icon; 'Project ID: postman-333115. It cannot be changed later. EDIT'; 'Organization *' with a dropdown menu and a question mark icon; 'Location *' with a dropdown menu and a 'BROWSE' button; and 'Parent organization or folder'. At the bottom of the form are two buttons: 'CREATE' and 'CANCEL'.

4. Stellen Sie anschließend sicher, dass Sie das Projekt ausgewählt haben.

Methode 1: Autorisierung per Zustimmung

1. Öffnen Sie console.cloud.google.com und wählen Sie das im vorherigen Schritt erstellte Projekt aus. Klicken Sie nun auf „APIs und Dienste“ > „Anmeldedaten“ und dann auf die Schaltfläche „Anmeldedaten erstellen“. Wählen Sie „OAuth-Client-ID“ aus.



2. Wählen Sie „Webanwendung“ als Anwendungstyp aus und geben Sie einen Namen ein.
3. Geben Sie bei „Autorisierte Weiterleitungs-URIs“ Folgendes ein:
 - a. <https://www.getpostman.com/oauth2/callback>
 - b. <https://oauth.pstmn.io/v1/browser-callback>
4. Klicken Sie auf „Erstellen“.

← 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. Klicken Sie im Fenster „OAuth-Client erstellt“ auf die Schaltfläche zum Herunterladen von JSON.

6. Klicken Sie zum Konfigurieren auf den OAuth-Zustimmungsbildschirm.

Wenn Sie für die Autorisierung OAuth 2.0 verwenden, fordert Ihre Anwendung Autorisierungen für einen oder mehrere Zugriffsbereiche von einem Google-Konto an. Google zeigt Nutzern einen Zustimmungsbildschirm an, der eine Übersicht Ihres Projekts und dessen Richtlinien sowie die angeforderten Zugriffsbereiche enthält.

Es gibt zwei Arten von Meldungen:

- a. **Interne** Meldungen sind ausschließlich für Nutzer in Ihrer Google Workspace-Domain gedacht. Sie erfordern Google Workspace oder eine Google-Identität.
- b. **Externe** Meldungen sind für alle Testnutzer mit einem Google-Konto verfügbar. Die Anwendung startet im Testmodus und ist nur für Nutzer verfügbar, die Sie in die Liste der Testnutzer aufnehmen. Gegebenenfalls müssen Sie die Anwendung verifizieren, sobald sie in die Produktionsumgebung übernommen werden kann.

7. Geben Sie den Anwendungsnamen und die Support-E-Mail-Adresse (die E-Mail-Adresse Ihres Administratorkontos in der Admin-Konsole) ein. Außerdem können Sie ein benutzerdefiniertes Logo auswählen.

8. Geben Sie unter „Autorisierte Domains“ `getpostman.com` ein.
9. Geben Sie eine E-Mail-Adresse ein, über die Sie von Google über Änderungen in Ihrem Projekt benachrichtigt werden möchten. Klicken Sie anschließend auf „Speichern und fortfahren“.

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. Klicken Sie auf die Schaltfläche „Bereiche hinzufügen oder entfernen“, um bestimmte Bereiche manuell hinzuzufügen. Alle Bereiche finden Sie in der [Liste der Bereiche auf dem Chrome Enterprise-GitHub](#). Klicken Sie auf „Speichern und fortfahren“.

Hinweis: Die Liste beinhaltet sowohl schreibgeschützte Bereiche als auch solche mit vollem Zugriff. Wählen Sie die Bereiche aus, die Sie für Ihren spezifischen Anwendungsfall benötigen.

✕ 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. **Optional:** Fügen Sie einen oder mehrere Nutzer hinzu, die Zugriff haben sollen, während der Veröffentlichungsstatus auf „Tests“ gesetzt ist. Geben Sie das Konto ein, das Sie benutzen haben, um das Projekt zu erstellen, sowie alle anderen, denen Sie Zugriff gewähren möchten. Klicken Sie dazu auf die Schaltfläche „Nutzer hinzufügen“.

12. Klicken Sie auf „Speichern und fortfahren“, prüfen Sie die Seite mit der Zusammenfassung und klicken Sie dann auf „Zurück zum Dashboard“.

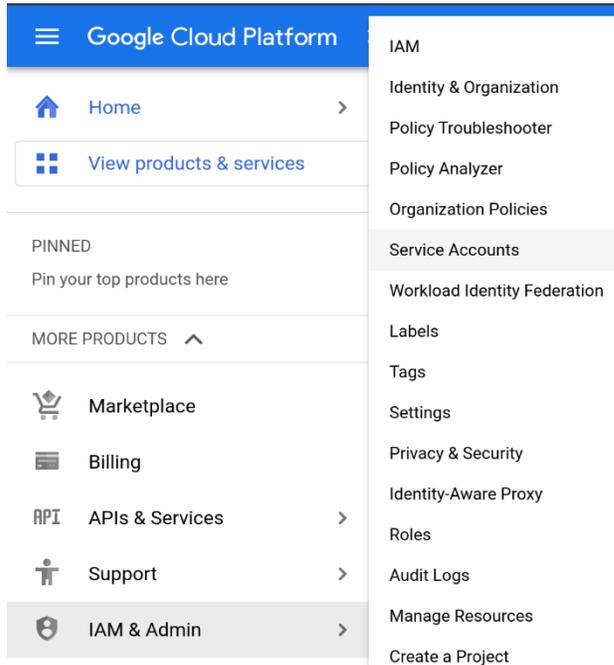
13. Wenn Sie möchten, können Sie jetzt Ihre Anwendung veröffentlichen.

- a. Wenn Sie für die Anwendung den Status „In Produktion“ wählen, steht sie allen Nutzern mit einem Google-Konto zur Verfügung. Abhängig von der Konfiguration des OAuth-Bildschirms müssen Sie die Anwendung ggf. zur Prüfung einreichen.

Methode 2: Autorisierung per Identitätsübertragung (Dienstkonto)

Ein Dienstkonto erstellen (per Identitätsübertragung autorisieren)

1. Öffnen Sie [die Seite mit den Dienstkonten](#) unter „IAM und Verwaltung“. Wenn Sie dazu aufgefordert werden, wählen Sie ein Projekt aus.



2. Klicken Sie auf „Dienstkonto erstellen“ und geben Sie einen Namen und eine Beschreibung für das Dienstkonto ein.



3. Sie können die standardmäßige Dienstkonto-ID verwenden oder eine andere eindeutige ID auswählen. Wenn Sie fertig sind, klicken Sie auf „Erstellen“.

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. Stellen Sie in den Dienstkontoberechtigungen sicher, dass Sie dem Dienstkonto die Rolle des **Dienstkontonutzers** zuweisen. Klicken Sie auf „Weiter“.
5. Auf dem Bildschirm „Nutzern Zugriff auf dieses Dienstkonto erteilen“ können Sie **entsprechende Nutzer hinzufügen**. Klicken Sie anschließend auf die Schaltfläche „Fertig“.

Filter Type to filter

- Roles
- Secret Manager
- Security Center
- Serverless VPC Access
- Service Accounts**
- Service Agents
- Service Consumer

- Create Service Accounts
- Delete Service Accounts
- Service Account Admin
- Service Account Key Admin
- Service Account Token Creator
- Service Account User**
- Workload Identity User

optional)

Service Account User
Run operations as the service account.

6. Wählen Sie das von Ihnen erstellte Dienstkonto auf dem nächsten Bildschirm aus.

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. Gehen Sie auf den Tab „Schlüssel“ am oberen Bildschirmrand und klicken Sie im Drop-down-Menü auf „Neuen Schlüssel erstellen“. Wählen Sie als Schlüsseltyp JSON aus.

The screenshot shows the 'Keys' tab in the Google Cloud IAM console. At the top, there are navigation tabs: DETAILS, PERMISSIONS, KEYS (selected), METRICS, and LOGS. Below the tabs is a warning message: 'Service account keys could pose a security risk if compromised. We [here](#).' Below the warning, there is a text prompt: 'Add a new key pair or upload a public key certificate from an existing key pair.' and a link: 'Block service account key creation using [organization policies](#). [Learn more about setting organization policies for service accounts](#)'. A button labeled 'ADD KEY' is open, showing two options: 'Create new key' and 'Upload existing key'. To the right of the dropdown menu, there is a table with two columns: 'Key creation date' and 'Key expiration date'.

8. Ihr neues öffentliches/privates Schlüsselpaar wird generiert und auf Ihren Computer heruntergeladen. Dies ist die einzige Kopie dieses Schlüssels. Da er den Zugriff auf Ihre Cloud Console ermöglicht, **bewahren Sie ihn sicher auf**.
9. **Klicken Sie auf den Tab „Details“** in Ihrem ausgewählten Dienstkonto und kopieren Sie die E-Mail-Adresse (sie lautet <projektname><id>@<projektname>.iam.gserviceaccount.com).

The screenshot shows the 'Service account details' page in the Google Cloud IAM console. At the top, there are navigation tabs: DETAILS (selected), PERMISSIONS, KEYS, METRICS, and LOGS. Below the tabs is the title 'Service account details'. There are two input fields: 'Name' with the value 'postman' and a 'SAVE' button, and 'Description' with a 'SAVE' button. Below these fields is the 'Email' field with the value 'postman@' followed by a text input box.

10. Gehen Sie in dem Projekt, das Sie zuvor auf der Google Cloud Platform erstellt haben, auf die Seite „APIs und Dienste“. Klicken Sie auf „+ APIs und Dienste aktivieren“

The screenshot shows the 'APIs & Services' page in the Google Cloud Platform console. At the top, there is a blue header with the Google Cloud Platform logo, the text 'Google Cloud Platform', and the project name 'postman' with a dropdown arrow. Below the header, there is a section titled 'APIs & Services' with a '+ ENABLE APIS AND SERVICES' button. Below this section, there is a button labeled 'Enabled APIs & services' with a gear icon.

11. Suchen Sie nach den folgenden APIs, wählen Sie alle nacheinander aus und klicken Sie auf die Schaltfläche „Verwalten“.



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

12. Melden Sie sich noch einmal in der [Admin-Konsole](#) mit Ihrem Super Admin-Konto an.

13. Klicken Sie auf [Konto > Administratorrollen](#) und wählen Sie die Dienstkontenrolle aus, die Sie im [Abschnitt API-Konto erstellen](#) eingerichtet haben.

14. Klicken Sie auf die Karte „Administratoren“ am oberen Bildschirmrand.

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. Klicken Sie auf „Dienstkonten zuweisen“.

CUSTOM ROLE

Service Account User

CBCM service account user

Admins

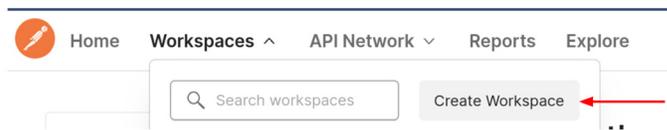
Showing all admins [Assign users](#) [Assign service accounts](#)

16. Geben Sie die E-Mail-Adresse ein, die Sie in Schritt 9 kopiert haben und klicken Sie auf die Schaltfläche „Hinzufügen“.

Postman-Integration einrichten

Konto einrichten

1. Gehen Sie zu [Postman.com](https://postman.com), richten Sie ein neues Konto ein oder verwenden Sie ein bestehendes Konto.
2. Sobald Ihr Konto eingerichtet ist, klicken Sie auf „Workspaces“ > „Create Workspace“ (Arbeitsbereiche > Arbeitsbereich erstellen), geben Sie einen Namen ein, wählen Sie die gewünschte Sicherheitsstufe aus und klicken Sie auf die Schaltfläche „Create Workspace“ (Arbeitsbereich erstellen).



Create workspace

Name

CBCM API

Summary

Add a brief summary about this workspace.

Run API actions to push and pull data from Chrome Browser Cloud Management.

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

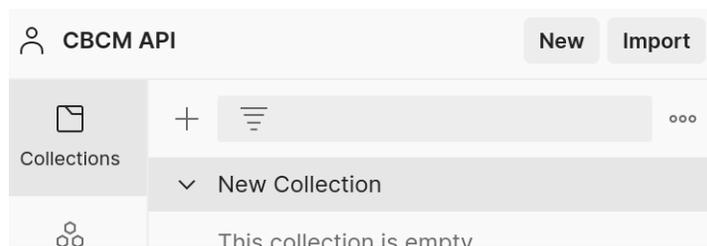
Cancel

Eine Sammlung aus dem Chrome Enterprise-GitHub importieren

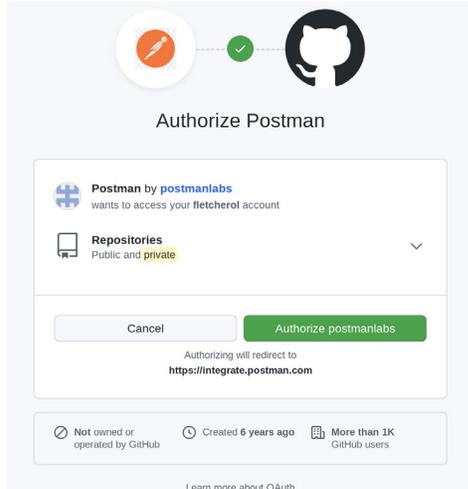
Wir empfehlen, die im [Chrome Enterprise-GitHub](#) bereitgestellten Sammlungen zu importieren. Diese beinhalten Beispielskripts häufiger Anwendungsfälle für Aufrufe an die Chrome-Verwaltung über die Cloud. Sie können sie per Datei-Upload oder per Link in Ihr GitHub-Repository importieren.

Per Code-Repository importieren

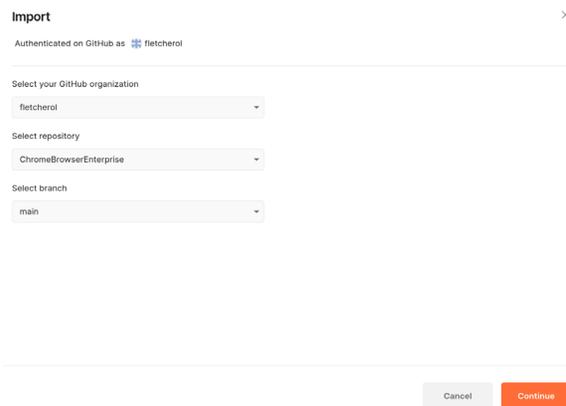
1. Melden Sie sich in Ihrem GitHub-Konto an.
2. Gehen Sie zu <https://github.com/google/Chrome BrowserEnterprise> und klicken Sie auf die Schaltfläche „Fork“, um die Sammlung zu Ihrem Repository hinzuzufügen.
3. Stellen Sie sicher, dass Ihr Arbeitsbereich in Postman ausgewählt ist, und klicken Sie dann auf die Schaltfläche Import (Importieren)



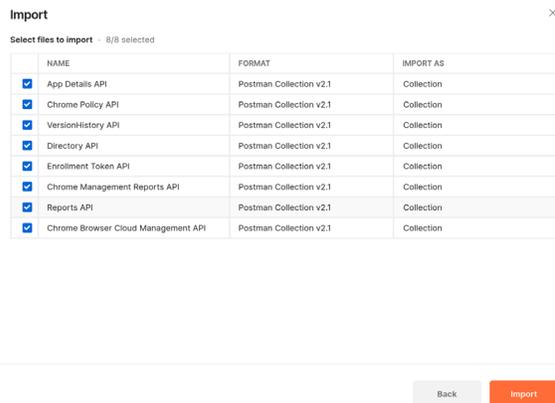
4. Klicken Sie auf „Code repository“ (Code-Repository) > „GitHub“.
5. Melden Sie sich in Ihrem GitHub-Konto an, klicken Sie auf die Schaltfläche „Authorize postmanlabs“ (Postmanlabs autorisieren) und geben Sie zur Bestätigung Ihr Passwort ein.



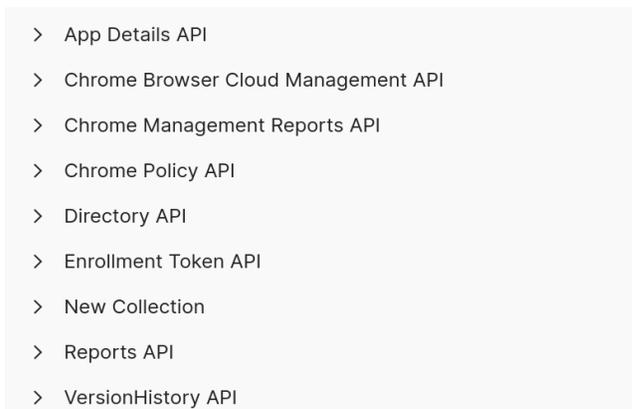
6. Anschließend sollten Sie im Abschnitt „Import“ (Importe) unter „Select repository“ (Repository auswählen) im Drop-down-Menü den Eintrag „ChromeBrowserEnterprise“ sehen. Klicken Sie auf die Schaltfläche „Continue“ (Weiter).



7. Wählen Sie die Sammlungen aus, die Sie importieren möchten, und klicken Sie auf die Schaltfläche „Import“ (Importieren).



8. Nun sollten Sie alle Sammlungen in Ihrem Postman-Arbeitsbereich sehen.



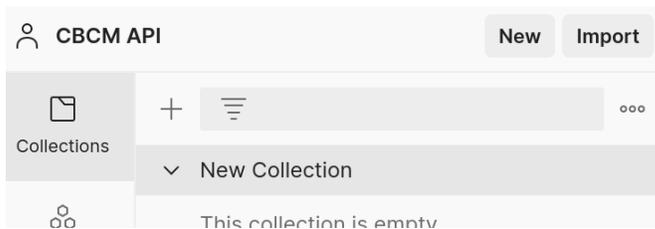
Per Datei-Upload importieren

1. Rufen Sie das [Chrome Enterprise-GitHub](#) auf und wählen Sie die Sammlung aus, die Sie importieren möchten.
2. Klicken Sie auf die Schaltfläche „Raw“.



3. Klicken Sie mit der rechten Maustaste, um die Datei als .json zu speichern.

4. Stellen Sie sicher, dass Ihr Arbeitsbereich in Postman ausgewählt ist, und klicken Sie dann auf die Schaltfläche **Import** (Importieren).



5. **Klicken Sie auf die Schaltfläche „Upload files“ (Dateien hochladen) und wählen Sie die JSON-Datei aus, die Sie im vorherigen Schritt heruntergeladen haben. Klicken Sie anschließend auf die Schaltfläche „Import“ (Importieren).**



Die folgenden Schritte sind nur für die Autorisierung per Zustimmung erforderlich:

6. Sobald die Sammlung angezeigt wird, müssen Sie die rot hervorgehobenen Abschnitte ausfüllen.

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. Geben Sie für die Authentifizierungs-URL Folgendes ein:

<https://accounts.google.com/o/oauth2/auth>

8. Geben Sie für die Zugriffstoken-URL Folgendes ein:

<https://oauth2.googleapis.com/token>

9. Entnehmen Sie die Client-ID und den Clientschlüssel unter <https://console.cloud.google.com/> dem Abschnitt „API und Dienste“ ([Direktlink](#)) und geben Sie sie in Postman ein.

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. Hinweis: Es wird empfohlen, diese Werte als Variablen einzugeben, um den Schutz sensibler Daten zu gewährleisten und das Hinzufügen dieser Daten zu mehreren Sammlungen beim Import zu vereinfachen.
- b. Wenn Sie dieselben Variablen in mehreren Sammlungen nutzen möchten, müssen Sie sie als globale Variablen deklarieren.
- Weitere Informationen zu Postman-Variablen [finden Sie hier](#).
10. Entnehmen Sie die Client-ID und den Clientschlüssel unter <https://console.cloud.google.com/> dem Abschnitt „API und Dienste“ ([Direktlink](#)) und geben Sie sie in Postman ein.
11. Wenn Sie die Browserversion von Postman verwenden, ist die Callback-URL vorausgefüllt. In der Desktopversion hingegen müssen Sie Folgendes eingeben:
<https://www.getpostman.com/oauth2/callback>
12. Klicken Sie auf die Schaltfläche „Get New Access Token“ (Neues Zugriffstoken abrufen).
13. Wenn Sie auf diese Schaltfläche klicken, werden Sie aufgefordert, sich mit Ihren Anmeldedaten für die Chrome-Verwaltung über die Cloud zu authentifizieren.
Stellen Sie sicher, dass dieses Konto entsprechende API-Berechtigungen für den von Ihnen hinzugefügten Bereich besitzt.



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. Anschließend wird Ihnen das neue Zugriffstoken angezeigt, das Sie zur Authentifizierung von Anfragen an die API nutzen können.

Klicken Sie auf die Schaltfläche „Use token“ (Token verwenden), damit die Informationen zum Token automatisch in die Sammlung eingetragen werden.

Tokens sind standardmäßig für eine Stunde gültig.

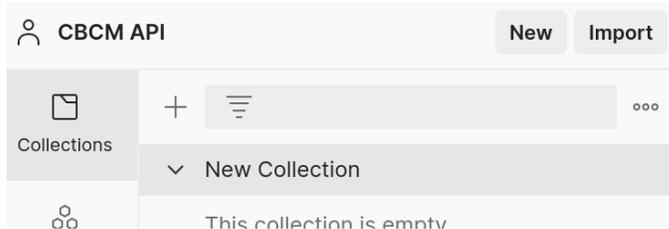
MANAGE ACCESS TOKENS ×

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

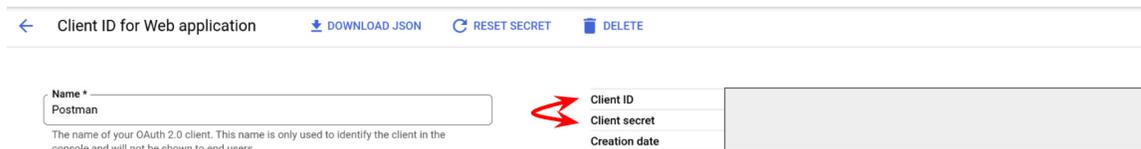
Neue Sammlung erstellen

1. Klicken Sie im Tab „Collections“ (Sammlungen) auf das Pluszeichen, um eine neue Sammlung zu erstellen.



Die folgenden Schritte sind nur für die Autorisierung per Zustimmung erforderlich:

2. Wählen Sie den Autorisierungstyp „OAuth2“ aus.
3. Geben Sie für die Callback-URL Folgendes ein:
 - a. In der Browserversion von Postman ist dies vorausgefüllt. In der Desktopversion hingegen müssen Sie Folgendes eingeben: <https://www.getpostman.com/oauth2/callback>
4. Geben Sie für die Authentifizierungs-URL Folgendes ein: <https://accounts.google.com/o/oauth2/auth>
5. Geben Sie für die Zugriffstoken-URL Folgendes ein: <https://oauth2.googleapis.com/token>
6. Entnehmen Sie die Client-ID und den Clientschlüssel unter <https://console.cloud.google.com/> dem Abschnitt „API und Dienste“ ([Direktlink](#)) und geben Sie sie in Postman ein.



Hinweis: Es wird empfohlen, diese Werte als Variablen einzugeben, um den Schutz sensibler Daten zu gewährleisten und das Hinzufügen dieser Daten zu mehreren Sammlungen beim Import zu vereinfachen.

Weitere Informationen zu Postman-Variablen [finden Sie hier](#).

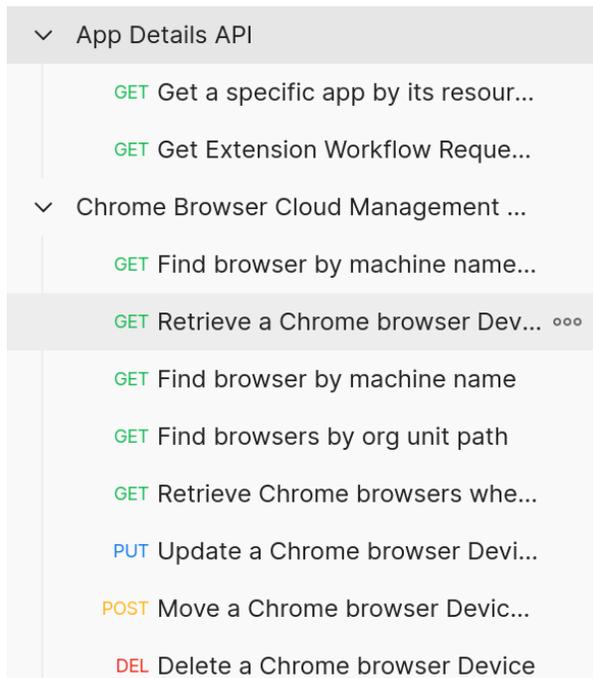
7. Fügen Sie die gewünschten Bereiche der Cloud Management API ein ([in diesem Abschnitt finden Sie weitere Informationen](#)). Jeder Bereich muss dabei mit einem Leerzeichen voneinander getrennt werden.
 8. Klicken Sie auf die Schaltfläche „Get New Access Token“ (Neues Zugriffstoken abrufen).
-

Die Verbindung zur Chrome-Verwaltung über die Cloud überprüfen

Für jede Sammlung auf dem Chrome Enterprise-GitHub finden Sie einige Beispielskripts, mit denen Sie anfangen können – beispielsweise für Anfragen mit GET, PUT, POST und DEL. Sobald Sie die Sammlung importiert haben, können Sie diese Skripts ausführen, um Postman zu ermöglichen, Anfragen an die Cloud-Verwaltung zu stellen.

1. Klicken Sie auf die importierte Sammlung.

Die folgenden Schritte (2–6) sind nur für die Autorisierung per Zustimmung erforderlich:



2. Prüfen Sie, ob die entsprechenden Werte bzw. Variablen für Auth-URL, Zugriffstoken-URL, Client-ID, Clientschlüssel und die Bereiche ordnungsgemäß eingegeben wurden.

3. Klicken Sie auf die Schaltfläche „Get New Access Token“ (Neues Zugriffstoken abrufen).

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}}

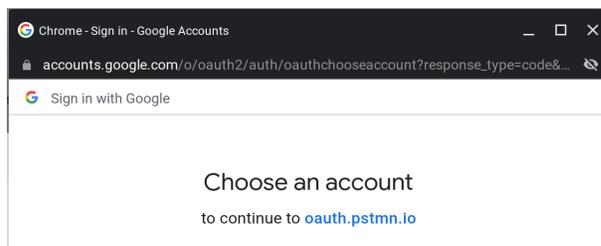
Scope ⓘ https://www.googleapis.com/auth/cl...

State ⓘ State

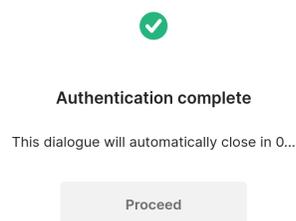
Client Authentication Send as Basic Auth header

Get New Access Token

4. Wählen Sie das Konto für die Autorisierung aus.



5. Wenn alles korrekt ist, wird das Dialogfeld „Authentication complete“ (Authentifizierung abgeschlossen) angezeigt.



6. Klicken Sie auf die Schaltfläche „Use token“ (Token verwenden).

MANAGE ACCESS TOKENS

All Tokens Delete

Token Name: AppDetailsApiToken

Access Token: [Redacted]

Token Type: Bearer

expires_in: 3599

scope: https://www.googleapis.com/auth/chrome.management.appdetails.readonly

Use Token

7. Wählen Sie die gewünschte Anfrage aus und klicken Sie auf die Schaltfläche „Send“ (Senden).

App Details API / Get a specific app by its resource name

GET https://chromemanagement.googleapis.com/v1/customers/my_customer/

Send

8. Die Antwort wird am unteren Bildschirmrand angezeigt. Bei Bedarf können Sie das Format über das Drop-down-Menü ändern.

Body Cookies Headers (13) Test Results Status: 200 OK Time: 934 ms Size: 4.54 KB Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2   "name": "customers/C033fmgff/apps/chrome/nckgahadagoaajjgafhacjanaoiihpd",
3   "displayName": "Google Hangouts",
4   "description": "Use Hangouts to keep in touch. Message friends, start free video or voice calls, and hop on a conversation with one person or a group.\n * Include all your friends with group chats for up to 150 people.\n * Say more with photos, videos, maps, emoji, stickers, and animated GIFs.Turn any conversation into a free group video call with up to 10 friends.\n * Keep in touch with friends across Android, iOS, and the web, and sync chats across all your devices.\n * Message friends anytime, even if they're offline.\n * Snooze your notifications so you can respond later.\n * See what you chatted about in the past, including shared photos and your video call history.\n * Keep a record of any conversation for just a short period of time by turning history off.\n * Connect your Google Voice account to make calls, send and receive SMS, and access your voicemail.\n\nHangouts Chrome extension:\n * Use Hangouts and get notifications as you move from tab to tab in Chrome, or even without a Chrome window open.\n * Position Hangouts anywhere on your screen, even if you have more than one monitor. Keep conversations in a single window or pop out the important ones.\n * View and continue your conversations across devices.\n * Get notifications just once. After you see an alert, it'll be removed on other devices.\n\nNotes:\n * Unlike the Chat for Google app, Hangouts doesn't support "invisible status".\n * Mobile carrier and ISP charges may apply.",
5   "appId": "nckgahadagoaajjgafhacjanaoiihpd",
6   "revisionId": "2020.803.419.1",
7   "type": "CHROME".
```