bitwarden | Article du Centre d'Aide

CONSOLE ADMIN

API publique de Bitwarden

Afficher dans le centre d'aide:
https://bitwarden.com/help/public-api/

API publique de Bitwarden

L'API publique de Bitwarden fournit aux organisations une suite d'outils pour gérer les membres, les collections, les groupes, les journaux d'événements et les politiques de sécurité.

> **Tip**
>
> Cette API ne permet pas de gérer les éléments individuels du coffre. Si c'est ce que vous devez accomplir, utilisez plutôt l'API de gestion du coffre.

L'API publique est une API RESTful avec des URL orientées ressources prévisibles, accepte les corps de requête encodés en JSON, renvoie des réponses encodées en JSON, et utilise des codes de réponse HTTP standard, l'authentification, et des verbes.

L'API publique est compatible avec la spécification OpenAPI (OAS3) et publie un fichier de définition swagger.json conforme. Explorez la spécification OpenAPI en utilisant l'interface utilisateur Swagger :

- Pour les instances hébergées sur le cloud public : `https://bitwarden.com/help/api/`
- Pour les instances auto-hébergées : `https://votre.domaine.com/api/docs/`

> **Note**
>
> L'accès à l'API publique Bitwarden est disponible pour les clients de toutes les organisations Entreprise et Équipes. Pour plus d'informations, voir À propos des plans Bitwarden.

Points finaux

URL de base

Pour l'hébergement dans le cloud, `https://api.bitwarden.com` ou `https://api.bitwarden.eu`.

Pour auto-hébergé, `https://votre.domaine.com/api`.

Points de terminaison d'authentification

Pour le cloud-hébergé, `https://identity.bitwarden.com/connect/jeton` ou `https://identity.bitwarden.eu/connect/jeton`.

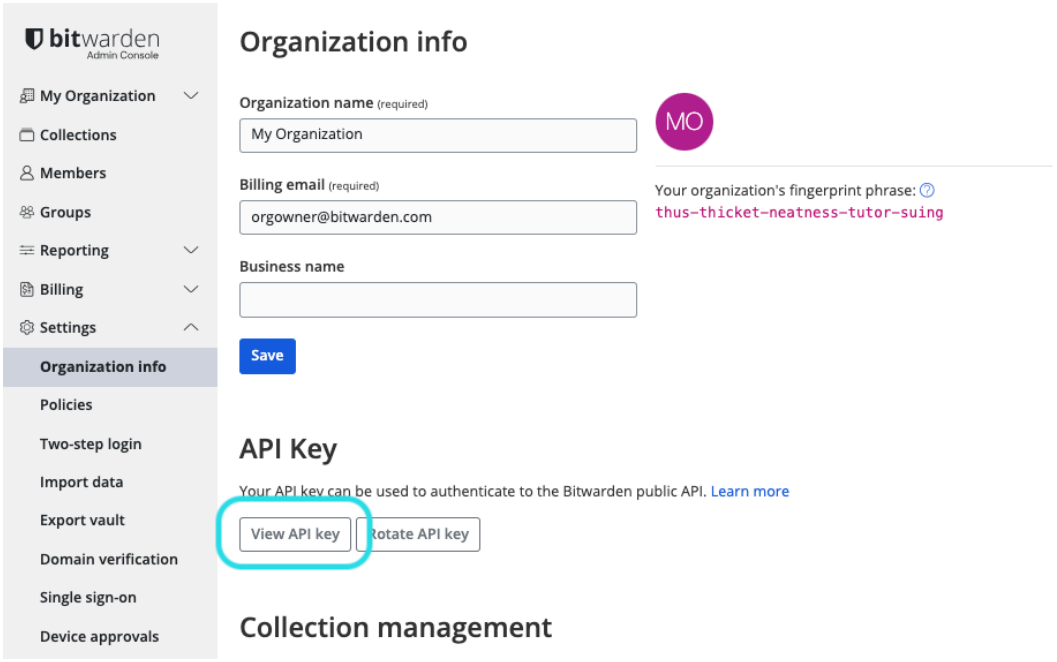
Pour auto-hébergé, `https://votre.domaine.com/identité/connect/jeton`.

Authentification

L'API utilise des jetons d'accès porteurs pour s'authentifier avec des points de terminaison API protégés. Bitwarden utilise un flux de demande d'application OAuth2 Client Credentials pour accorder des jetons d'accès porteurs à partir du point de terminaison. Les demandes d'authentification prennent `client_id` et `client_secret` comme paramètres requis.

> **Tip**
>
> La clé API utilisée pour l'authentification avec l'API publique n'est **pas la même** que la clé API personnelle. Les clés API de l'organisation auront un `client_id` au format `"organisation.ClientId"`, tandis que les clés API personnelles auront un `client_id` au format `"user.clientId"`.

La clé API `client_id` et `client_secret` peuvent être obtenues par un propriétaire à partir du coffre de la console Admin en naviguant vers **Paramètres** → écran **Informations de l'organisation** et en descendant jusqu'à la section **Clé API** :



Obtenez la clé API de l'organisation

Si, en tant que propriétaire, vous souhaitez partager la clé API avec un admin ou un autre utilisateur, utilisez une méthode de communication sécurisée comme Bitwarden Send.

> **⚠ Warning**
>
> La clé API de votre organisation permet un accès complet à votre organisation. Gardez votre clé API privée. Si vous pensez que votre clé API a été compromise, sélectionnez **Paramètres > Informations sur l'organisation > Régénérer la clé API** bouton sur cet écran. Les mises en œuvre actives de votre clé API actuelle devront être reconfigurées avec la nouvelle clé avant utilisation.

Jeton d'accès porteur

Pour obtenir un jeton d'accès porteur, faites une demande `POST` avec `Content-Type: application/x-www-form-urlencoded` avec votre `client_id` et `client_secret` vers le point de terminaison d'authentification. Lors de l'utilisation de l'API pour la gestion de l'organisation, vous utiliserez toujours `grant_type=client_credentials` et `scope=api.organization`. Par exemple:

```bash
curl -X POST \
  https://identity.bitwarden.com/connect/token \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  -d 'grant_type=client_credentials&scope=api.organization&client_id=<ID>&client_secret=<SECRET>'
```

Cette demande entraînera la réponse suivante:

```Bash
{
  "access_token": "<TOKEN>",
  "expires_in": 3600,
  "token_type": "Bearer"
}
```

Dans cette réponse, `3600` représente la valeur d'expiration (en secondes), ce qui signifie que ce jeton est valide pendant 60 minutes après avoir été émis. Effectuer un appel API avec un jeton expiré renverra un `401 Non autorisé` code de réponse.

Types de contenu

L'API publique de Bitwarden communique avec des requêtes et des réponses `application/json`, avec une exception :

Le point de terminaison d'authentification attend une demande `application/x-www-form-urlencoded`, cependant il répondra avec `application/json`.

Demande d'échantillon

```Bash
curl -X GET \
  https://api.bitwarden.com/public/collections \
  -H 'Authorization: Bearer <TOKEN>'
```

Où est la valeur pour la clé `access_token:` dans le jeton d'accès porteur obtenu.

Cette demande entraînera une réponse :

```Bash
{
  "object": "list",
  "data": [
    {
      "object": "event",
      "type": 1000,
      "itemId": "string",
      "collectionId": "string",
      "groupId": "string",
      "policyId": "string",
      "memberId": "string",
      "actingUserId": "string",
      "date": "2020-11-04T15:01:21.698Z",
      "device": 0,
      "ipAddress": "xxx.xx.xxx.x"
    }
  ],
  "continuationToken": "string"
}
```

Statut

Bitwarden a une page de statut publique, où vous pouvez trouver des informations sur la santé du service et les incidents pour tous les services, y compris l'API publique.

Codes de réponse

L'API publique de Bitwarden utilise des codes de réponse HTTP conventionnels pour indiquer le succès ou l'échec d'une demande d'API :

Code de Statut	Description
200 OK	Tout a fonctionné comme prévu.
400 Mauvaise Demande	La demande était inacceptable, peut-être en raison de paramètre(s) manquant(s) ou mal formé(s).

Code de Statut	Description
`401 Non autorisé`	Le jeton d'accès porteur était manquant, invalide ou expiré.
`404 Non Trouvé`	La ressource demandée n'existe pas.
`429 Trop de demandes`	Trop de demandes ont frappé l'API trop rapidement. Nous recommandons de réduire le nombre de demandes.
`500, 502, 503, 504 Erreur de Serveur`	Quelque chose a mal tourné de la part de Bitwarden. Ceux-ci sont rares, mais contactez-nous s'ils se produisent.

Lecture supplémentaire

Pour plus d'informations sur l'utilisation de l'API publique Bitwarden, consultez les articles suivants :

- Spécification OAS de l'API publique Bitwarden
- Journal des événements