Restrict public access to your content

March 28, 2023 • Jan Cerman • 4 min read • JavaScript

Protect your content and assets with secure access. You might want to enable secure access with sensitive content, content hidden behind sign-in walls, or for projects that are not public facing.

Without secure access, your assets and published content items are publicly available by default.

Enable secure access

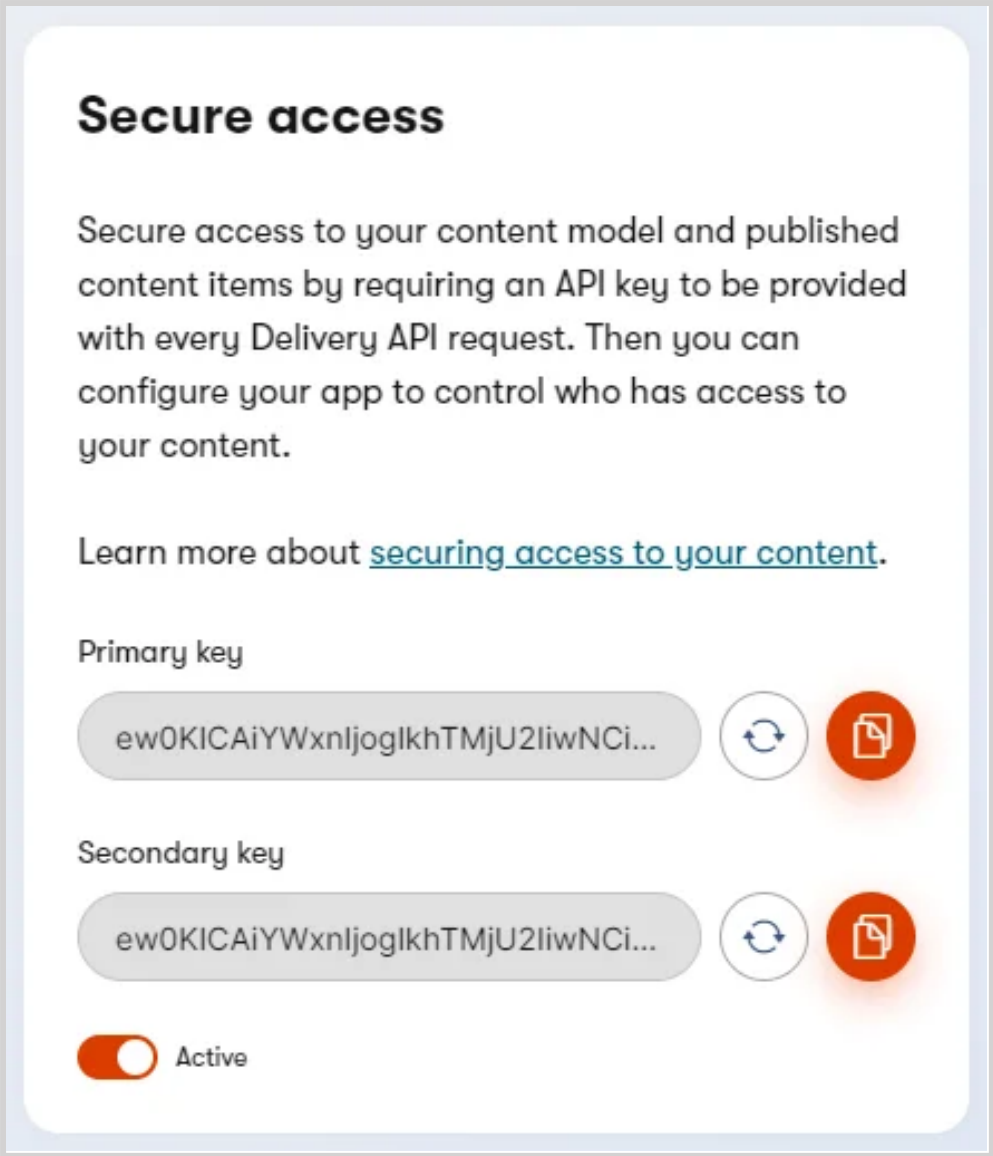
When you activate secure access, Delivery API requires an API key with each API request for content. This applies to both Delivery REST API and Delivery GraphQL API. Kontent.ai generates two API keys for Delivery API – Primary and Secondary keys.

Quick facts about the Primary and Secondary keys

- The scope of the API keys is per environment.
- Their default expiration date is 1 year.
- Use the Primary key for continuous use in your apps.
- Use the Secondary key when revoking the Primary key to prevent downtime.

1. In Kontent.ai, go to **Environment settings** > **API keys**.
2. In **Delivery API** > **Secure access**, click the switch to activate secure access.
3. For one of the keys, click .

Use the new API key to authenticate your API requests.



Retrieve content items securely

Tips for staying safe with secure access

- Retrieve content on the server side and NOT client side to prevent leaking your API keys.
- Store your API Keys outside your source code. For example, store them as environment variables. Make sure they're encrypted too.
- Regenerate only one key at a time to prevent downtime.
- Regenerate your API keys periodically. The older a key is, the higher the probability it could have been compromised.

When getting content items, add an API key on top of your requests. The code below shows how to securely retrieve the content of an article named *My article*.

JavaScript

```
// Tip: Find more about JS/TS SDKs at https://kontent.ai/learn/javascript
const KontentDelivery = require('@kontent-ai/delivery-sdk');

const deliveryClient = KontentDelivery.createDeliveryClient({
  environmentId: '<YOUR_ENVIRONMENT_ID>',
  defaultQueryConfig: {
    useSecuredMode: true, // Queries the Delivery API using secure access.
  },
  secureApiKey: '<YOUR_API_KEY>',
});

const response = await deliveryClient.item('my_article')
  .toPromise();
```

After sending the request, you receive a single content item in the JSON format. You can filter your requests to retrieve only specific elements or items.

Retrieve assets securely

With advanced asset management, you can restrict access to your assets by requiring an API key. This API key differs from the API keys in ⚙ **Environment settings** > **API keys**.

To set up secure access for assets, contact our support and let them know the following:

- Your environment ID
- Whether secure assets should be enabled for the Delivery Preview API, Delivery API, or both

Once you enable secure assets, you need to provide an API key for every asset request. Fetch assets on the server side of your app to prevent exposing the API key.

Revoke API keys

When you suspect unauthorized key usage, you need to revoke one or both of the API keys and generate new ones. For example, when a user with access to the Primary key had left your company. In such cases, we recommend that you switch to the Secondary key and regenerate the Primary key.

Generating a new key will replace and revoke the old key. The revocation process can take up to a couple of minutes. Any requests made with a revoked API key receive the 401 Unauthorized error.

1. In Kontent.ai, go to ⚙ **Environment settings** > **API keys**.
2. In the **Delivery API** card, regenerate the Secondary key.
3. Update your apps to use the newly generated Secondary key.
4. Validate that your apps work correctly with the new key.
5. In the **Delivery API** card, regenerate the Primary key to ensure unauthorized users cannot use it to access your content.

6. (Optional) Switch to using the regenerated Primary key in your apps so that your configuration is the same as you started.