Every request aimed at the Kentico REST service must be authenticated. Otherwise the service replies with a 403 Forbidden HTTP status code.

You need to specify the username and password through the **Authorization** line in the HTTP header of every REST request. The header line consists of:

- The authentication type (*Basic*)
- The username and password connected by a colon (***username:password***), encoded using the Base64 algorithm

For example, the following header line uses *RestClient:MyPassword* as the authentication credentials:

```
Authorization: Basic UmVzdENsaWVudDpNeVBhc3N3b3Jk
```

The credentials must belong to a standard user created in Kentico. If your website uses Windows Active Directory authentication, you need to manually create a non-AD user for the purposes of REST authentication, with the **Is external user** and **Is domain user** properties disabled.

Once authenticated, the system allows the REST request to perform operations depending on the specified user's privilege level and permissions.

**Note**: The Kentico REST service does not require Basic Authentication to be enabled in IIS. Keep Basic Authentication disabled in IIS as described in Configuring the REST service.

**Security**

- We strongly recommend using SSL to protect the authentication credentials in the request headers. See also: Configuring SSL
- The REST service does not support more advanced authentication standards by default. If you have additional authentication or security requirements, we recommend creating a custom single-purpose Web API endpoint to retrieve the required data and using it instead of the REST service.

**Tip**: When testing REST requests manually in a browser, you do not need to edit the HTTP header. Most browsers provide a dialog where you can type in the authentication credentials.

## Hash parameter authentication

You can authenticate individual REST requests by adding a hash parameter to the URL. The hash parameter allows you to prepare REST requests that can be executed by unauthenticated users. Requests that contain the hash parameter ignore the credentials specified in the authentication header.

**Restrictions**

- Only works for GET requests (read only data retrieval)
- You cannot use hash parameter authentication for */all* object retrieval requests (*~/rest/<object type>/all*). This is an intentional security limitation that protects global data in the system.

**Warning**: Only use hash parameter authentication for loading data that you want to make publicly available. REST requests with hash authentication can be executed by anyone who obtains the URL (for example by intercepting the web request).

To get the authentication hash for REST requests:

1. Prepare the URL of your REST request in advance.

2. Open the **Settings** application.
3. Select the **Integration -> REST** category.
4. Click **Generate authentication hash**.
5. Enter the full absolute URL of the REST request, including the protocol, website domain name, virtual directory, REST path, and query string parameters. For example: *http://mywebsite.com/rest/content/currentsite/en-us/all/news?format=json*
6. Click **Authenticate**.

The system adds the authentication hash parameter to the URL. You can copy the URL and use it to perform the REST request without supplying an authentication header.