On this tab, you can adjust settings related to Kentico REST service. The following settings can be adjusted:

General	
Service enabled	Enables or disables the Kentico REST service. See Configuring the REST service.
Service enabled for	Choose if the REST service allows access to objects, pages, or both.
Always check page security	If disabled, security is not checked when accessing published versions of pages. If enabled, security is always checked.
Page access is read only	If enabled, the REST service only allows GET requests for pages (pages cannot be modified).
Object access is read only	If enabled, the REST service only allows GET requests for objects (objects cannot be modified).
Allowed page types	Specifies a list of page types that the REST service is allowed to access. Enter the names of page types separated by semicolons. If empty, all page types are allowed.
Allowed object types	Specifies a list of object types that the REST service is allowed to access. Enter object type values separated by semicolons. To find the values for specific object types, open the **System** application in the Kentico administration interface and select the **Object types** tab. If empty, all object types are allowed.
Generate authentication hash for URL	Click the button to generate an authentication hash for specific REST URLs. 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* The system adds the authentication hash parameter to the URL. You can copy the URL and use it to perform the REST request without authentication headers. **Restrictions**: • Only works for GET requests (read only data retrieval) • You cannot use hash parameter authentication for */all* object retrieval requests (*~/rest/<objecttype>/all*).
Default encoding	Sets the character encoding that the REST service uses for requests that do not contain a supported *Accept-Charset* header.
Allow sensitive fields for administrators	If enabled, REST requests authenticated using the credentials of users with the Global administrator privilege level are allowed to work with data fields that contain sensitive information (for example fields related to passwords). Requests authenticated under non-administrator users can NEVER access sensitive fields, regardless of this setting's value.