

Kentico allows you to protect your website from automated spam bots. You can secure all forms where users enter data, by requiring users to type a security code called [CAPTCHA](#).

You can use CAPTCHA to tell humans and computers apart in the following places:

- Blog comments
- Custom tables
- Page types
- Forms
- Forums
- Message boards
- Other web parts that allow user input

Changing the default CAPTCHA type

You can choose which CAPTCHA type the system uses:



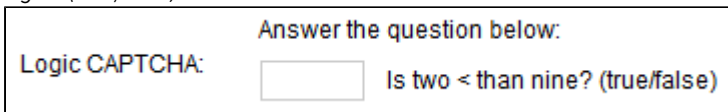
We recommend using **reCAPTCHA**, which is the most secure and user-friendly CAPTCHA type.

- **Simple** – prompts users to retype a sequence of numbers from an image.



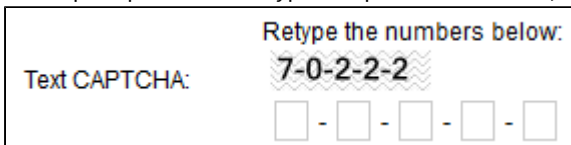
Simple CAPTCHA: Enter security code: 804828

- **Logic** – asks users to solve a simple arithmetic problem or to compare two numbers. Example: "one + four"; "Is six > than eight? (true/false)"



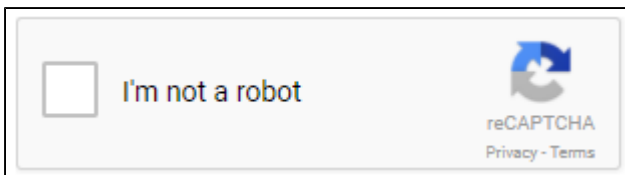
Logic CAPTCHA: Answer the question below: Is two < than nine? (true/false)


- **Text** – prompts users to retype a sequence of numbers, each number into an individual box.



Text CAPTCHA: Retype the numbers below: 7-0-2-2-2
 - - - -

- **reCAPTCHA** – loads the verification element using a web service. Requires users to click a checkbox to prove they are not a bot. The user either passes immediately, or needs to perform an additional image selection test to prove they are human.



I'm not a robot 
reCAPTCHA
Privacy - Terms



To use reCAPTCHA, you need to perform the [required configuration](#).

The default CAPTCHA type is **Simple**. To change the default type:

1. Open the **Settings** application.
2. Navigate to the **Security & Membership** -> **Protection** settings category.
3. Under **CAPTCHA settings**, select a **Control to use**.
4. **Save** the settings.

When you change the CAPTCHA type, all web parts and features that have CAPTCHA enabled use the new type. Also, all fields in custom tables, page types, and forms that use the **Security code form control**, use the new type of CAPTCHA. Fields that use a specific CAPTCHA control do not change.

Configuring reCAPTCHA

reCAPTCHA is an online service which allows your application to tell apart humans and computers. reCAPTCHA requires users to click a checkbox indicating they are not a robot. This either passes the user immediately or challenges them to validate whether or not they are human (using an additional image selection or audio test).

You need to register your site to use the reCAPTCHA API and obtain a pair of API keys:

1. Go to <https://www.google.com/recaptcha/admin> and sign in with your Google account.
2. Select the **reCAPTCHA v2** type (other reCAPTCHA types are not supported by default).
3. Fill in all required details, including the domain where your site is running.
4. Copy your **Site key** and **Secret key**.

Next, enter your site's reCAPTCHA API keys into Kentico:

1. Open the **Settings** application.
2. Navigate to the **Security & Membership** -> **Protection** settings category.
3. Under **CAPTCHA settings**, paste the API keys into the **reCAPTCHA site key** and **reCAPTCHA secret key** settings respectively.
4. **Save** the settings.



Tip: If you run multiple sites in your Kentico instance, you can switch between them using the **Site** selector and enter different API keys for each site.

With the API keys entered into the system, you can select *reCAPTCHA* as the default CAPTCHA type (via the **Control to use** setting).

You can also create verification fields in page types, forms or custom tables using the **reCAPTCHA** form control. In this case, the form control allows you to configure additional settings for the specific field:

- **Control theme** – sets the appearance of the reCAPTCHA element (Light or Dark).
- **Type** – sets the type of challenge used if the initial noCAPTCHA validation fails (Image or Audio).
- **Size** – sets the size of the reCAPTCHA element (Normal or Compact).



Using multiple reCAPTCHAs on the same page

The system does not support the use of multiple reCAPTCHA fields within the same form. You can have multiple different forms with a reCAPTCHA field on the same page, but successful validation for one form also automatically validates the others.

Customizing reCAPTCHA messages

If you wish to change the error messages that reCAPTCHA displays to users, create custom **resource strings** with the appropriate keys and enter the required text content as the translation values for specific cultures.

Use the following resource string keys for error messages related to basic verification:

- **recaptcha.error.missing-input-response** – displayed when a user does not provide the required input, for example when the validation checkbox is not clicked.
- **recaptcha.error.invalid-input-response** – displayed when the user's input is invalid or malformed.

You can also use the following resource string keys for other technical errors:

- **recaptcha.error.serverunavailable** – the reCAPTCHA server is unavailable.
- **recaptcha.error.bad-request** – the validation request is invalid or malformed.
- **recaptcha.error.invalidconfiguration** – the reCAPTCHA site and secret key settings are not configured in Kentico.
- **recaptcha.error.missing-input-secret** – the secret API key is missing.
- **recaptcha.error.invalid-input-secret** – the secret API key is invalid or malformed.
- **recaptcha.error.timeout-or-duplicate** – timeout or the same form contains multiple reCAPTCHA fields.