

Allowed HTML

Use this administration tool to control what HTML tags are allowed to be used on your site where users enter text. Note that this applies to any text entered by the user where HTML is allowed, including, if you are using the Storefront Addon, any HTML used on pages within a user's Storefront Manager.

Tags Matching <tag ...> or </tag>

Save Changes

| Tags matching <tag ...> or </tag> | | |
|-----------------------------------|-------------------------------------|--------|
| Tag | Allowed? | Delete |
| a * | <input type="checkbox"/> | |
| applet * | <input type="checkbox"/> | |
| area | <input checked="" type="checkbox"/> | |
| b | <input checked="" type="checkbox"/> | |
| blink * | <input type="checkbox"/> | |
| blockquote | <input checked="" type="checkbox"/> | |
| body | <input checked="" type="checkbox"/> | |

On the list of HTML tags, check the box for **Allowed?** for any HTML tags you wish to allow your users to use when entering text on the site, for example in the "listing details" when placing a listing. If a user attempts to enter a HTML tag that is on this list that is not allowed, it will simply be removed from the text with no replacement. The tags with an asterisk (*) are strongly recommended to **not be allowed**. This is because the potential for a user to enter malicious code exists with the tags we have identified with an asterisk.

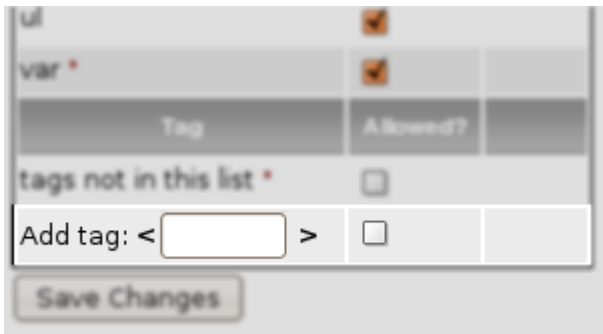
Tags not in this list

| tr * | <input type="checkbox"/> | |
|-----------------------------------|-------------------------------------|--|
| u | <input checked="" type="checkbox"/> | |
| ul | <input checked="" type="checkbox"/> | |
| var * | <input checked="" type="checkbox"/> | |
| Tag | Allowed? | |
| tags not in this list * | <input type="checkbox"/> | |
| Add tag: < <input type="text"/> > | <input type="checkbox"/> | |

Save Changes

Use this setting to allow or not allow a user to enter tags not found on this list at all. We recommend leaving this setting disallowed (by un-checking the box for "Allowed?").

Add Tag



The screenshot shows a form with the following elements:

- A 'Tag' input field with a placeholder text 'Add tag: < >'.
- An 'Allowed?' checkbox.
- A 'Save Changes' button.

When you enter a tag you only need to enter the *first* part of the HTML tag **BETWEEN** the "<" and ">", **without** the attributes. For example, if the "a" (HTML anchor) tag was not one of the default tags defined, and you wanted to add it, you would only need to enter "a" into the tool.

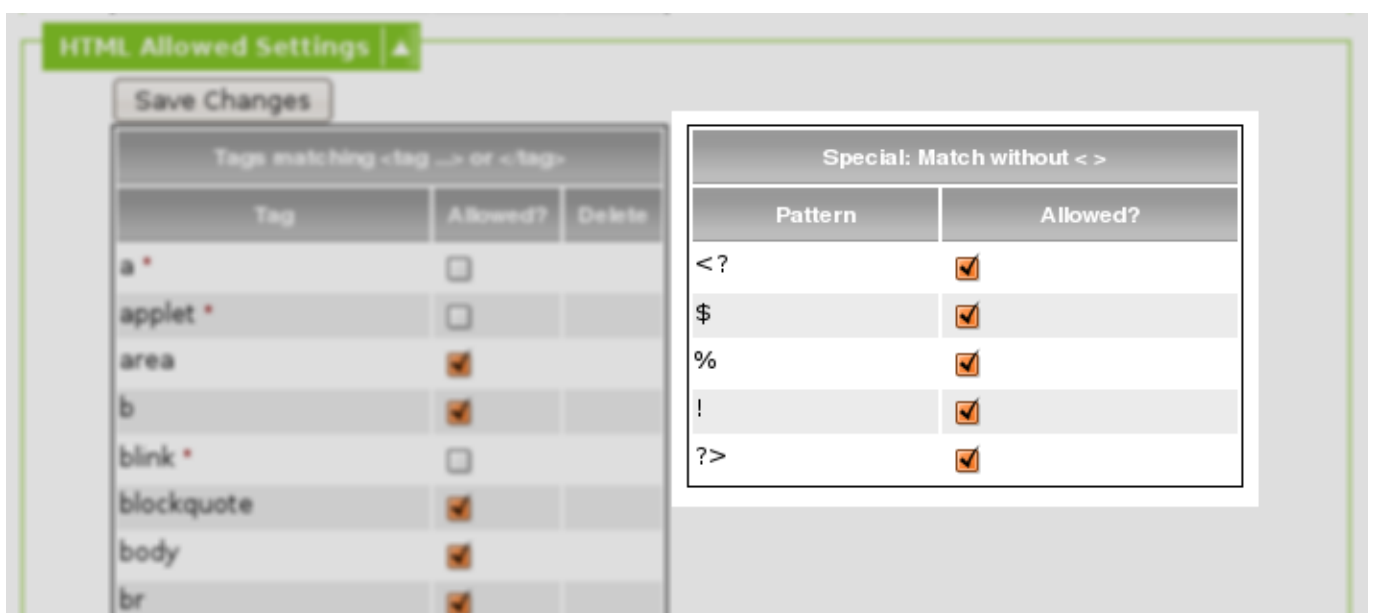
The full HTML tag may look something like:

```
<a href="http://www.geodesicsolutions.com"> go to Geodesic Solutions website</a>
```

You would enter the tag as just **a**, leave off the rest of the tag. Also check the box for **Allowed?** if you wish to allow this new tag that you are adding to the list.

Note that the tags on this list are **case insensitive**, meaning that if a tag is on this list and not allowed, it will be removed from text regardless of if the tag is upper-case or lower-case, or even a combination of both.

Special: Match without < >



The screenshot shows the 'HTML Allowed Settings' interface. It includes a 'Save Changes' button and a table of tags. A 'Special: Match without < >' section is highlighted, showing a table of patterns and their allowed status.

| Tag | Allowed? | Delete |
|------------|-------------------------------------|--------|
| a * | <input type="checkbox"/> | |
| applet * | <input type="checkbox"/> | |
| area | <input checked="" type="checkbox"/> | |
| b | <input checked="" type="checkbox"/> | |
| blink * | <input type="checkbox"/> | |
| blockquote | <input checked="" type="checkbox"/> | |
| body | <input checked="" type="checkbox"/> | |
| br | <input checked="" type="checkbox"/> | |

| Pattern | Allowed? |
|---------|-------------------------------------|
| < ? | <input checked="" type="checkbox"/> |
| \$ | <input checked="" type="checkbox"/> |
| % | <input checked="" type="checkbox"/> |
| ! | <input checked="" type="checkbox"/> |
| ?> | <input checked="" type="checkbox"/> |

This is a list of things you can allow or not allow, that will be matched even if they are not part of a

tag. You cannot add additional things to this list, there is only the pre-defined ones. If you need to filter out anything else that is not a tag, and not on this special list, we recommend using the **Badwords** tool to do so.

If any of the items on this list are not allowed, if it is found anywhere in the text at all, it will be removed. This can result in un-desired side effects, and for this reason we highly recommend you leave all items on this list as "allowed".

See below for an explanation of what each of the patterns on this list does.

| Pattern | Common Use | Recommendation |
|---------|--|---|
| <? | Open PHP tag | Doesn't matter This can be disallowed with little little chance of removing something legitimate. However, allowing it does not pose a security risk ¹⁾ . |
| \$ | Start of a variable in PHP | Allow. Dis-allowing this can cause \$ removed from text, even when it may just be used as the currency symbol |
| % | Not sure why this is here. | Allow. Turning this off can inadvertently break the width of things, if the width of something is set to a % value. |
| ! | Not sure why this one is here, either. | Allow. Your "excited" clients will look like they fail at punctuation if you do not allow this! |
| ?> | Close PHP Tag | Doesn't matter. Allowing it won't be a security problem. Dis-allowing it will most likely not cause any accidental removals, since ?> does not come up in every day conversation (unless discussing PHP) |

Warning: HTML Removed by WYSIWYG

Note there may be **inadvertent** tags disallowed if you use the WYSIWYG within your place a listing process. The WYSIWYG does not have the ability to represent flash or dynamic content within it, among other things. So even if you allowed the <param>, <object>, ...etc tags to display this content within the WYSIWYG the WYSIWYG itself may remove the tags.

The WYSIWYG will also attempt to **auto-correct** HTML according to what it considers is *valid HTML*. If your clients use the *HTML* button in the WYSIWYG editor to manually insert or edit the HTML directly, if that HTML is not *valid* (according to what the WYSIWYG editor considers valid), the editor will try to auto-correct the HTML. Most of the time the effect is fine, as it causes the HTML to be "valid" which search engines (at least Google) seem to prefer. But sometimes, this can cause problems, for instance it may result in un-expected things happening like things being moved around, resized, or removed altogether as a result of the "auto correcting".

In those cases, where the WYSIWYG editor is causing problems with entering the HTML as desired, advise your users to click on **[Add/Remove Editor]** to temporarily turn off the WYSIWYG editor, and they can enter the HTML directly into a normal "textarea".

¹⁾

But the paranoid may choose to block it anyways, just in case.

Last update: 2014/09/25 16:55 admin_menu:site_setup:allowed_html:start http://geodesicsolutions.org/wiki/admin_menu/site_setup/allowed_html/start?rev=1229300107

From: <http://geodesicsolutions.org/wiki/> - **Geodesic Solutions Community Wiki**

Permanent link: http://geodesicsolutions.org/wiki/admin_menu/site_setup/allowed_html/start?rev=1229300107

Last update: **2014/09/25 16:55**

