






# General Security tab

## Overview

Use this tab to configure the general, site-wide security settings.







## To Access

From the Security Admin page, click the **General Security** tab.

| Option               | Description   | Default |
|----------------------|---|---------|
| Smarty security      | Enable/Disable Smarty security. If checked, you can then define allowed and disabled modifiers and tags(functions, blocks and filters) that should be or not accesible to the template.<br> <i>You should leave this on unless you know what you are doing.</i>  | Enabled |
| Allowed Smarty tags  | This is a list of allowed tags. It's the list of (registered / autoloaded) function-, block and filter plugins that should be accessible to the template. If empty, no restriction by allowed_tags. This may be needed for custom templates.<br> <i>Use "," to separate values</i><br> <i>There may be security implications. Make sure you know what you are doing.</i>        | None    |
| Disabled Smarty tags | This is a list of disabled tags. It's the list of (registered / autoloaded) function-, block and filter plugins that may not be accessible to the template. If empty, no restriction by disabled_tags. This may be needed for custom templates.<br> <i>Use "," to separate values</i><br> <i>There may be security implications. Make sure you know what you are doing.</i> | None    |


## Related Topics

- [Login](#)
- [General Preferences](#)
- [Security](#)

| Option                    | Description   | Default |
|---------------------------|---|---------|
| Allowed Smarty modifiers  | <p>This is the list of allowed modifier plugins. It's the array of (registered / autoloaded) modifiers that should be accessible to the template. If this array is non-empty, only the herein listed modifiers may be used. This is a whitelist. If empty, no restriction by allowed_modifiers. This may be needed for custom templates.</p> <p> Use ", " to separate values</p> <p> <i>There may be security implications. Make sure you know what you are doing.</i></p>  | None    |
| Disabled Smarty modifiers | <p>This is a list of disabled modifier plugins. It's the list of (registered / autoloaded) modifiers that may not be accessible to the template. If empty, no restriction by disabled_modifiers. This may be needed for custom templates.</p> <p> Use ", " to separate values</p> <p> <i>There may be security implications. Make sure you know what you are doing.</i></p>   | None    |
| Extra Smarty directories  | <p>Make additional directories available as Smarty directories. This may be needed for custom icons (clear temp/cache after changing).</p> <p> <i>There may be security implications. Make sure you know what you are doing.</i></p>   | None    |
| HTML purifier             | <p>HTML Purifier is a standards-compliant HTML filter library written in PHP and integrated in Tiki. HTML Purifier will not only remove all malicious code (better known as XSS) with a thoroughly audited, secure yet permissive whitelist, it will also ensure that your documents are standards-compliant. Keep in mind that HTML Purifier is not HTML5 compatible and may rewrite HTML5 syntax and produce unwanted results.</p> <p> <i>If you use HTML in your wiki page and it gets stripped out or rewritten, make sure your HTML is valid, or de-activate this feature. Keep in mind that HTML Purifier is not HTML5 compatible and may rewrite HTML5 syntax and produce unwanted results.</i></p> | Enabled |

| Option  | Description   | Default  |
|---|---|----------|
| Output should be HTML purified  | <p>This activates HTML Purifier on wiki content and other outputs, to filter out potential security problems like XSS code. Keep in mind that HTML Purifier is not HTML5 compatible and may rewrite HTML5 syntax, producing unwanted results.</p> <p>👉 <i>If you are trying to use HTML in your pages and it gets stripped out, you should make sure your HTML is valid or de-activate this feature.</i> 🛠️</p> | Disabled |
| Protect all sessions with HTTPS                                       | <p>Always redirect to HTTPS to prevent a session hijack through network sniffing.</p> <p>⚠️ <i>Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site</i></p>   | Disabled |
| HTTP Basic Authentication   | <p>Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials.</p> <p>☰ Disable   SSL Only (Recommended)   Always</p>  | Disable  |
| Prevent common passwords  | <p>For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -&gt; Log in -&gt; Password Blacklist.</p>   | Disabled |
| Require admin users to enter their password for some critical actions | <p>User password will be required for critical operations that can compromise the system security or stability, like adding users to the admin group</p>  | Enabled  |
| Allow sending newsletters through external clients                    | <p>Generate mailto links using the recipients as the BCC list.</p> <p>⚠️ <i>This will expose the list if email addresses to all users allowed to send newsletters.</i></p>  | Disabled |
| Validate uploaded file content  | <p>Do not trust user input and open the files to verify their content.</p>  | Enabled  |
| Allow the tiki_p_trust_input permission.                              | <p>Bypass user input filtering.</p> <p>⚠️ <i>Note: all permissions are granted to the Admins group including this one, so if you enable this you may expose your site to XSS (Cross Site Scripting) attacks for admin users.</i></p>  | Disabled |
| Quick permission assignment   | <p>Quickperms are an interface in addition to the normal edit-permissions page, for quick assignment of permissions for a page or other object. 🛠️</p>  | Enabled  |

| Option  | Description  | Default  |
|---|--|----------|
| Verify HTTPS certificates of remote servers                         | When set to enforce, the server will fail to connect over HTTPS to a remote server that do not have a SSL certificate that is valid and can be verified against the local list of Certificate Authority (CA)<br>☰ Do not enforce verification   Enforce verification   | None     |
| Use CURL for HTTP connections                                       | Use CURL instead of sockets for server to server HTTP connections, when sockets are not available.   | Disabled |
| Debugger console  | A popup console with a list of all PHP and Smarty variables used to render the current webpage. It can be viewed by clicking 'Quick Administration->Smarty debug window' or by appending ?show_smarty_debug=1 or &show_smarty_debug=1 to the page URL. You may also execute SQL, watch vars and perform a number of other functions.<br>👉 <i>Only viewable by admins</i><br>⚠️ <i>Not suitable for production use.</i> | Disabled |
| Tiki template viewing   | ⚠️ <i>May not be functional in Tiki 14+</i> 🚫  | Disabled |
| Edit templates  | ⚠️ <i>May not be functional in Tiki 14+</i> 🚫  | Disabled |
| Edit CSS  | Edit CSS files directly in the browser.<br>⚠️ <i>May not be functional in Tiki 14+</i> 🚫   | Disabled |
| All new trackers are restricted to wiki page access only by default | Option "Restrict non admins to wiki page access only" is not checked by default.   | Disabled |
| User encryption   | Tiki user encryption enables a personal, secure storage of sensitive data, e.g. password. Only the user can see the data. No decryption passwords are stored.<br>👉 <i>Enable personal, secure storage of sensitive data such as passwords</i><br>⚠️ <i>This is an experimental feature. Using it may cause loss of the encrypted data.</i> 🚫   | Disabled |
| Password domains  | Securely store extra user passwords and other user specific data for other "domains", or just for yourself 🚫   | Userkey  |

| Option   | Description   | Default       |
|--|---|---------------|
| Use short lived CSRF tokens                                      | <p>CSRF tokens generated will be valid for one use only and will have a limited life span</p> <p><b>⚠️</b> <i>Changing the CSRF tokens to be short lived may lead to an increase of errors on submitting information when the users take a long time to finish an operation or the session is lost.</i></p>   | Disabled      |
| Security timeout   | <p>Sets the expiration of CSRF tickets and related forms. The <code>session_lifetime</code> preference is used for the default, if set, otherwise the <code>session.gc_maxlifetime</code> <code>php.ini</code> setting is used, subject to a default maximum of four hours in any case.</p> <p><b>⚠️</b> <i>Minimum value is 30 seconds to avoid blocking everyone from being able to make any changes, including to this setting</i></p> | 14400 seconds |
| Require confirmation of an action if a possible CSRF is detected |    | Disabled      |
| HTTP header x-frame options                                      | The x-frame-options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <code>&lt;frame&gt;</code> , <code>&lt;iframe&gt;</code> or <code>&lt;object&gt;</code> ;   | Enabled       |
| Header value   | ☰ DENY   SAMEORIGIN   | DENY          |
| HTTP header x-xss-protection                                     | The x-xss-protection header is designed to enable the cross-site scripting (XSS) filter built into modern web browsers  | Enabled       |
| Header value   | ☰ 0   1   1;mode=block  | 1;mode=block  |
| HTTP header x-content-type-options                               | The x-content-type-options header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed.  | Enabled       |
| HTTP header content-security-policy                              | The Content-Security-Policy header allows web site administrators to control resources the user agent is allowed to load for a given page.  | Enabled       |
| Header value   | For example, to allow your Tiki to appear in an iframe on <code>example.com</code> set this value to <code>frame-ancestors https://example.com/</code>  | None          |
| HTTP header strict-transport-security                            | The Strict-Transport-Security header (often abbreviated as HSTS) is a security feature that lets a web site tell browsers that it should only be communicated with using HTTPS, instead of using HTTP.  | Enabled       |
| Header value   |   | None          |

| <b>Option</b>               | <b>Description</b>   | <b>Default</b> |
|-----------------------------|--|----------------|
| HTTP header public-key-pins | The public-key-pins header associates a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates. If one or several keys are pinned and none of them are used by the server, the browser will not accept the response as legitimate, and will not display it. | Enabled        |
| Header value                |  | None           |