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.

Related Topics

- Login General Preferences
- Security

Option	Description	Default
Smarty security	Do not allow PHP code in Smarty templates. ⚠ *You should leave this on unless you know what you are doing.*	Enabled
Extra Smarty functions	Make additional PHP functions available as Smarty functions. This may be needed for custom templates. ⚠ *There may be security implications. Make sure you know what you are doing.*	None
Extra Smarty modifiers	Make additional PHP functions available as Smarty modifiers. This may be needed for custom templates. ⚠ *There may be security implications. Make sure you know what you are doing.*	None
Extra Smarty directories	Make additional directories available as Smarty directories. This may be needed for custom icons (clear temp/cache after changing). ⚠ *There may be security implications. Make sure you know what you are doing.*	None
HTML purifier	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. *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.*	Enabled

Option	Description	Default
Output should be HTML purified	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. *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.*	Disabled
Protect all sessions with HTTPS	Always redirect to HTTPS to prevent a session hijack through network sniffing. *Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site*	Disabled
HTTP Basic Authentication	Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials. Disable | SSL Only (Recommended) | Always	Disable
Prevent common passwords	For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.	Disabled
Require admin users to enter their password for some critical actions	User password will be required for critical operations that can compromise the system security or stability, like adding users to the admin group	Enabled
Allow sending newsletters through external clients	Generate mailto links using the recipients as the BCC list. *This will expose the list if email addresses to all users allowed to send newsletters.*	Disabled
Validate uploaded file content	Do not trust user input and open the files to verify their content.	Enabled
Allow the tiki_p_trust_input permission.	Bypass user input filtering. *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.*	Disabled
Quick permission assignment	Quickperms are an interface in addition to the normal edit-permissions page, for quick assignment of permissions for a page or other object.	Disabled

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) 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. *Only viewable by admins* ⚠ *Not suitable for production use.*	Disabled
Tiki template viewing	⚠ *May not be functional in Tiki 14+*	Disabled
Edit templates	⚠ *May not be functional in Tiki 14+*	Disabled
Edit CSS	Edit CSS files directly in the browser. ⚠ *May not be functional in Tiki 14+*	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. *Enable personal, secure storage of sensitive data such as passwords* ⚠ *This is an experimental feature. Using it may cause loss of the encrypted data.*	Disabled
Password domains	Securely store extra user passwords and other user specific data for other "domains", or just for yourself	Userkey
Use short lived CSRF tokens	CSRF tokens generated will be valid for one use only and will have a limited life span ⚠ *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.*	Disabled

Option	Description	Default
Security timeout	Sets the expiration of CSRF tickets and related forms. The `session_lifetime` preference is used for the default, if set, otherwise the `session.gc_maxlifetime` `php.ini` setting is used, subject to a default maximum of four hours in any case. ⚠ *Minimum value is 30 seconds to avoid blocking everyone from being able to make any changes, including to this setting*	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 <frame>, <iframe> or <object>	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 example.com set this value to `frame-ancestors https://example.com/`	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

Option	Description	Default
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

Option	Description	Default
Smarty security	Do not allow PHP code in Smarty templates. ⚠ *You should leave this on unless you know what you are doing.*	Enabled
Extra Smarty functions	Make additional PHP functions available as Smarty functions. This may be needed for custom templates. ⚠ *There may be security implications. Make sure you know what you are doing.*	None
Extra Smarty modifiers	Make additional PHP functions available as Smarty modifiers. This may be needed for custom templates. ⚠ *There may be security implications. Make sure you know what you are doing.*	None
Extra Smarty directories	Make additional directories available as Smarty directories. This may be needed for custom icons (clear temp/cache after changing). ⚠ *There may be security implications. Make sure you know what you are doing.*	None
HTML purifier	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. *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.*	Enabled

Option	Description	Default
Output should be HTML purified	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. *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.*	Disabled
Protect all sessions with HTTPS	Always redirect to HTTPS to prevent a session hijack through network sniffing. *Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site*	Disabled
HTTP Basic Authentication	Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials. Disable | SSL Only (Recommended) | Always	Disable
Prevent common passwords	For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.	Disabled
Require admin users to enter their password for some critical actions	User password will be required for critical operations that can compromise the system security or stability, like adding users to the admin group	Enabled
Allow sending newsletters through external clients	Generate mailto links using the recipients as the BCC list. *This will expose the list if email addresses to all users allowed to send newsletters.*	Disabled
Validate uploaded file content	Do not trust user input and open the files to verify their content.	Enabled
Allow the tiki_p_trust_input permission.	Bypass user input filtering. *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.*	Disabled
Quick permission assignment	Quickperms are an interface in addition to the normal edit-permissions page, for quick assignment of permissions for a page or other object.	Disabled

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) 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. *Only viewable by admins* ⚠ *Not suitable for production use.*	Disabled
Tiki template viewing	⚠ *May not be functional in Tiki 14+*	Disabled
Edit templates	⚠ *May not be functional in Tiki 14+*	Disabled
Edit CSS	Edit CSS files directly in the browser. ⚠ *May not be functional in Tiki 14+*	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. *Enable personal, secure storage of sensitive data such as passwords* ⚠ *This is an experimental feature. Using it may cause loss of the encrypted data.*	Disabled
Password domains	Securely store extra user passwords and other user specific data for other "domains", or just for yourself	Userkey
Use short lived CSRF tokens	CSRF tokens generated will be valid for one use only and will have a limited life span ⚠ *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.*	Disabled

Option	Description	Default
Security timeout	Sets the expiration of CSRF tickets and related forms. The `session_lifetime` preference is used for the default, if set, otherwise the `session.gc_maxlifetime` `php.ini` setting is used, subject to a default maximum of four hours in any case. ⚠ *Minimum value is 30 seconds to avoid blocking everyone from being able to make any changes, including to this setting*	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 <frame>, <iframe> or <object>	Disabled
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	Disabled
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.	Disabled
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.	Disabled
Header value	For example, to allow your Tiki to appear in an iframe on example.com set this value to `frame-ancestors https://example.com/`	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.	Disabled
Header value		None

Option	Description	Default
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.	Disabled
Header value		None

Option	Description	Default
Smarty security	Do not allow PHP code in Smarty templates. ⚠ *You should leave this on unless you know what you are doing.*	Enabled
Extra Smarty functions	Make additional PHP functions available as Smarty functions. This may be needed for custom templates. ⚠ *There may be security implications. Make sure you know what you are doing.*	None
Extra Smarty modifiers	Make additional PHP functions available as Smarty modifiers. This may be needed for custom templates. ⚠ *There may be security implications. Make sure you know what you are doing.*	None
Extra Smarty directories	Make additional directories available as Smarty directories. This may be needed for custom icons (clear temp/cache after changing). ⚠ *There may be security implications. Make sure you know what you are doing.*	None
HTML purifier	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. *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.*	Enabled

Option	Description	Default
Output should be HTML purified	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. *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.* ⚗	Disabled
Protect all sessions with HTTPS	Always redirect to HTTPS to prevent a session hijack through network sniffing. ⚠ *Warning: activate only if SSL is already configured; otherwise, all users including admin will be locked out of the site*	Disabled
HTTP Basic Authentication	Check credentials from HTTP Basic Authentication, which is useful to allow webservices to use credentials. ☰ Disable | SSL Only (Recommended) | Always	Disable
Prevent common passwords	For improved security, prevent users from creating blacklisted passwords. Use default blacklist or create custom blacklists through Control Panel -> Log in -> Password Blacklist.	Disabled
Allow sending newsletters through external clients	Generate mailto links using the recipients as the BCC list. ⚠ *This will expose the list if email addresses to all users allowed to send newsletters.*	Disabled
Validate uploaded file content	Do not trust user input and open the files to verify their content.	Enabled
Allow the tiki_p_trust_input permission.	Bypass user input filtering. ⚠ *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.*	Disabled
Quick permission assignment	Quickperms are an interface in addition to the normal edit-permissions page, for quick assignment of permissions for a page or other object. ⚗	Disabled
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) ☰ Do not enforce verification | Enforce verification	None

Option	Description	Default
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. *Only viewable by admins* ⚠ *Not suitable for production use.*	Disabled
Tiki template viewing	⚠ *May not be functional in Tiki 14+* ⚗	Disabled
Edit templates	⚠ *May not be functional in Tiki 14+* ⚗	Disabled
Edit CSS	Edit CSS files directly in the browser. ⚠ *May not be functional in Tiki 14+* ⚗	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. *Enable personal, secure storage of sensitive data such as passwords* ⚠ *This is an experimental feature. Using it may cause loss of the encrypted data.* ⚗	Disabled
Password domains	Securely store extra user passwords and other user specific data for other "domains", or just for yourself ⚗	Userkey
Security timeout	Sets the expiration of CSRF tickets and related forms. The `session_lifetime` preference is used for the default, if set, otherwise the `session.gc_maxlifetime` `php.ini` setting is used, subject to a default maximum of four hours in any case. ⚠ *Minimum value is 30 seconds to avoid blocking everyone from being able to make any changes, including to this setting*	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 <frame>, <iframe> or <object>	Disabled

Option	Description	Default
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	Disabled
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.	Disabled
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.	Disabled
Header value	For example, to allow your Tiki to appear in an iframe on example.com set this value to `frame-ancestors https://example.com/`	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.	Disabled
Header value		None
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.	Disabled
Header value		None