Score

Option	Description	Default
Score	Score is a game to motivate participants to increase their contribution by comparing to other users.	Disabled
Score expiry		0 days

Option	Description	Default
Score	Score is a game to motivate participants to increase their contribution by comparing to other users.	Disabled
Score expiry		0 days

Option	Description	Default
Score	Score is a game to motivate participants to increase their contribution by comparing to other users.	Disabled
Score expiry		0 days

Option	Description	Default
Score	Score is a game to motivate participants to increase their contribution by comparing to other users.	Disabled
Score expiry		0 days

Option	Description	Default
Score	Score is a game to motivate participants to increase their contribution by comparing to other users.	Disabled
Score expiry		0 days

Search - Federated search

Option	Description	Default
Federated search	Search through alternate site indices. *Elasticsearch or Manticore Search is required*	Disabled
Elasticsearch tribe node URL	URL of the tribe client node accessing multiple clusters.	None
Manticore distributed index prefix	The prefix used when creating distributed index in Manticore. This needs to be the same for all sites participating in the federation.	Tiki_

Option	Description	Default
Federated search	Search through alternate site indices. *Elasticsearch or Manticore Search is required*	Disabled
Elasticsearch tribe node URL	URL of the tribe client node accessing multiple clusters.	None
Manticore distributed index prefix	The prefix used when creating distributed index in Manticore. This needs to be the same for all sites participating in the federation.	Tiki_

Option	Description	Default
Federated search	Search through alternate site indices. *Elasticsearch or Manticore Search is required*	Disabled
Elasticsearch tribe node URL	URL of the tribe client node accessing multiple clusters.	None
Manticore distributed index prefix	The prefix used when creating distributed index in Manticore. This needs to be the same for all sites participating in the federation.	Tiki_

Option	Description	Default
Federated search	Search through alternate site indices. *Elasticsearch is required*	Disabled
Elasticsearch tribe node URL	URL of the tribe client node accessing multiple clusters.	None

Option	Description	Default
Federated search	Search through alternate site indices. *Elasticsearch is required*	Disabled
Elasticsearch tribe node URL	URL of the tribe client node accessing multiple clusters.	None

Search - General settings

Option	Description	Default
Unified search index	Enables searching for content at the site using a Tiki-managed index. It's recommended to set a cron job to periodically rebuild the search index.	Enabled
Search statistics	Enables administrators to collect and view statistics on search activity.	Disabled
Users available in search results	Users available within search results. Content related to the user will be included in the index. None | All | Public	None
Incremental Index Update	Update the index incrementally as the site content is modified. *This may lead to lower performance and accuracy than processing the index on a periodic basis.*	Enabled
Search index rebuild memory limit	Temporarily adjust the memory limit to use during Search index rebuild. Depending on the volume of data, some large operations require more memory. Increasing it locally, per operation, allows to keep a lower memory limit globally. Keep in mind that memory usage is still limited to what is available on the server. *for example: 256M*	None
Search index rebuild time limit	Temporarily adjust the time limit to use during Search index rebuild. Depending on the volume of data, some requests may take longer. Increase the time limit locally to resolve the issue. Use reasonable values. *for example: 30*	None

Option	Description	Default
Unified search engine	Search engine used to index the content of this Tiki site. Some engines are more suitable for larger sites, but require additional software on the server. ☰ MySQL full-text search | Elasticsearch | Manticore Search	MySQL full-text search
Elasticsearch URL	URL of any node in the cluster	http://localhost:9200
Elasticsearch Authentication	When Elasticsearch security module is enabled, user authentication can be set up here. ☰ No Authentication | Basic Authentication	None
Elasticsearch User	HTTP basic authentication user to be sent with each request to Elasticsearch.	None
Elasticsearch Password	HTTP basic authentication password to be sent with each request to Elasticsearch.	None
Elasticsearch index prefix	The prefix that is used for all indexes for this installation in Elasticsearch	Tiki_
Elasticsearch current index	A new index is created upon rebuilding, and the old one is then destroyed. This setting enables seeing the currently active index. *Do not change this value unless you know what you are doing.*	None
Elasticsearch field limit per index	The maximum number of fields per search index in Elasticsearch version 5.x and above	1000 fields
Relation types to index within object.	Comma-separated relation types for which objects should be indexed in their related objects. *Elasticsearch needed*	None
Use MySQL Full-Text Search (fallback)	In case of Elasticsearch is active and unavailable, use MySQL Full-Text Search as fallback	Disabled
MySQL use short field names	Due to frm file constraints, number of search fields that one index can hold is usually limited to about 1500. This can be exceeded if you have numerous tracker fields. Enabling this option will try to shorten the field names internally that should allow you to use 300-500 more fields. Switching this option requires full index rebuild.	Disabled
Restore old MySQL indexes during reindex	If set, after the reindex is performed, old table MySQL indexes will be restored to the reindex related table.	Disabled

Option	Description	Default
Manticore URL	URL of the Manticore search server	http://127.0.0.1
Manticore HTTP(S) Port	Port number for the HTTP(S) interface.	9308
Manticore MySQL Port	Port number for the MySQL interface.	9306
Manticore index prefix	The prefix that is used for all indexes for this installation in Manticore	Tiki_
Manticore current index	A new set of indexes are created upon rebuilding, and the old ones are then destroyed. This setting enables seeing the currently active index prefix. *Do not change this value unless you know what you are doing.*	None
Morphology processing	Advanced morphology preprocessors to apply in the Manticore index, comma-separated. For example libstemmer_en,libstemmer_fr. See Manticore manual for possible values.	None
Manticore indexed full-text fields	Manticore has a hard-limit of 256 full-text indexed fields per index. If your installation has more, some will be indexed as string attributes and perform the slower regex search. You can add a comma-separated list of fields to always index as full-text here.	title,contents
Default Boolean Operator	Use OR or AND as the default search operator. AND | OR	AND
Excluded categories	List of category IDs to exclude from the search index	None
Excluded plugins	List of plugin names to exclude while indexing	None
Additional plugins searchable by default	List of plugin names that are required to additionnaly include while indexing. Example: fancytable,list,trackerlist,trackerfilter	attach, box, code, copyrigh...
Don't index non searchable fields	Indexing will skip adding all tracker fields that are not marked as "searchable". This will free index space but also make it impossible to use those fields in search index queries.	Disabled
Index forum replies together with initial post	Forum replies will be indexed together with the initial post as a single document instead of being indexed separately.	Enabled

Option	Description	Default
Tokenize version numbers	Tokenize version number strings so that major versions are found when sub-versions are mentioned. For example, searching for 2.7 would return documents containing 2.7.4, but not 1.2.7.	Disabled
Tokenize CamelCase words	Consider the components of camel-case words as separate tokens, allowing them to be searched individually. ⚠️ *Conflicts with Tokenize Version Numbers.*	Disabled
Possessive Stemmer	The possessive stemmer removes possessives (trailing "'s") from words before indexing them.	Enabled
Field weights	Allow the field weights to be set that apply when ranking pages in the search results. The weight is applied only when the field is in the query. To nullify the value of a field, use an insignificant amount, but not 0, which may lead to unexpected behaviors such as stripping of results. (Add these fields to the "Default content fields" preference below for it to have an effect in a global "content" search) 👆 *One field per line, field_name**:**5.3*	title:2.5 allowed_groups:0....
Default content fields	All of the content is aggregated in the contents field. For custom weighting to apply, the fields must be included in the query. This option allows other fields to be included in the default content search.	contents, title
Cache per user and query for Tiki built-in search	Time in minutes a user has a same query cached applied to Tiki built-in search interface only.	0 minutes
Cache result-specific formatted results	Formatted search results such as the ones used in the List plugin will be cached to prevent process-intensive reformatting on each page load. The cache is result-specific. ⚠️ *Every different result will generate a separate cache. This could quickly build up a large cache directory. It is recommended to clear Tiki caches often (e.g. once per week) via an automated job if you use this feature.*	Disabled
Cache individual search formatters	List of search formatters whose output will be cached. This is separate to the result-specific formatted results cache.	None

Option	Description	Default
LIST plugin cache default on	If selected, LIST plugins will be cached by default unless turned off at plugin level.	Disabled
LIST plugin cache default expiry	Default number of minutes for LIST plugin cache expiry.	30
Index Tracker Category names	Index the names and paths of category field values 👆 *Requires reindexing*	Enabled
Use unified search in category admin	Use unified search to find objects to add to categories. This limits the types of objects available to those included in the unified index.	Disabled
Automatically trim Elasticsearch results on date-sorted query	Automatically trim Elasticsearch results in unified search if the query is sorted by modification or creation date.	Disabled
Show error on missing field	When using List plugin to specify certain fields, especially tracker fields, this check helps ensure their names were entered correctly.	Enabled
Stop Word List	Words excluded from the search index, because they can be too frequent and produce unwanted results. 👆 *MySQL full-text search has its own list of stop words configured in the server.*	a, an, and, are, as, at, be...
Search index outdated	Number of days to consider the search index outdated	2 days
Automatic indexing of file content	Uses command line tools to extract the information from the files based on their MIME types.	Disabled
Automatic indexing of emails stored as files	Parses message/rfc822 types of files (aka eml files) and stores individual email headers and content in search index.	Disabled
Asynchronous indexing		Enabled
Autocomplete page names	Automatically complete page names as the user starts typing. For example the user types the start of the wiki page name “Sear” and Tiki returns “Search”, “Search General Settings”, etc 🧹	Disabled

Option	Description	Default
Referer search highlighting	When a user lands on a Tiki page from a search engine, Tiki highlights the search words they used. Its similar to using Tiki's search facility.	Enabled
File thumbnail preview	Have a preview of attachments in search results	Disabled
Forum name search	👆 *When listing forums*	Disabled
Forum content search	👆 *When listing forums*	Enabled
Topic content search		Enabled
Unified search for forums and file galleries		Enabled

Option	Description	Default
Unified search index	Enables searching for content at the site using a Tiki-managed index. It's recommended to set a cron job to periodically rebuild the search index.	Enabled
Search statistics	Enables administrators to collect and view statistics on search activity.	Disabled
Users available in search results	Users available within search results. Content related to the user will be included in the index. ☰ None | All | Public	None
Incremental Index Update	Update the index incrementally as the site content is modified. ⚠️ *This may lead to lower performance and accuracy than processing the index on a periodic basis.*	Enabled
Search index rebuild memory limit	Temporarily adjust the memory limit to use during Search index rebuild. Depending on the volume of data, some large operations require more memory. Increasing it locally, per operation, allows to keep a lower memory limit globally. Keep in mind that memory usage is still limited to what is available on the server. 👆 *for example: 256M*	None

Option	Description	Default
Search index rebuild time limit	Temporarily adjust the time limit to use during Search index rebuild. Depending on the volume of data, some requests may take longer. Increase the time limit locally to resolve the issue. Use reasonable values. *for example: 30*	None
Unified search engine	Search engine used to index the content of this Tiki site. Some engines are more suitable for larger sites, but require additional software on the server. MySQL full-text search | Elasticsearch | Manticore Search	MySQL full-text search
Elasticsearch URL	URL of any node in the cluster	http://localhost:9200
Elasticsearch Authentication	When Elasticsearch security module is enabled, user authentication can be set up here. No Authentication | Basic Authentication	None
Elasticsearch User	HTTP basic authentication user to be sent with each request to Elasticsearch.	None
Elasticsearch Password	HTTP basic authentication password to be sent with each request to Elasticsearch.	None
Elasticsearch index prefix	The prefix that is used for all indexes for this installation in Elasticsearch	Tiki_
Elasticsearch current index	A new index is created upon rebuilding, and the old one is then destroyed. This setting enables seeing the currently active index. *Do not change this value unless you know what you are doing.*	None
Elasticsearch field limit per index	The maximum number of fields per search index in Elasticsearch version 5.x and above	1000 fields
Relation types to index within object.	Comma-separated relation types for which objects should be indexed in their related objects. *Elasticsearch needed*	None
Use MySQL Full-Text Search (fallback)	In case of Elasticsearch is active and unavailable, use MySQL Full-Text Search as fallback	Disabled

Option	Description	Default
MySQL use short field names	Due to frm file constraints, number of search fields that one index can hold is usually limited to about 1500. This can be exceeded if you have numerous tracker fields. Enabling this option will try to shorten the field names internally that should allow you to use 300-500 more fields. Switching this option requires full index rebuild.	Disabled
Restore old MySQL indexes during reindex	If set, after the reindex is performed, old table MySQL indexes will be restored to the reindex related table. 🧪	Disabled
Manticore URL	URL of the Manticore search server	http://127.0.0.1
Manticore HTTP(S) Port	Port number for the HTTP(S) interface.	9308
Manticore MySQL Port	Port number for the MySQL interface.	9306
Manticore index prefix	The prefix that is used for all indexes for this installation in Manticore	Tiki_
Manticore current index	A new set of indexes are created upon rebuilding, and the old ones are then destroyed. This setting enables seeing the currently active index prefix. 👆 *Do not change this value unless you know what you are doing.*	None
Morphology processing	Advanced morphology preprocessors to apply in the Manticore index, comma-separated. For example libstemmer_en,libstemmer_fr. See Manticore manual for possible values.	None
Manticore indexed full-text fields	Manticore has a hard-limit of 256 full-text indexed fields per index. If your installation has more, some will be indexed as string attributes and perform the slower regex search. You can add a comma-separated list of fields to always index as full-text here.	title,contents
Default Boolean Operator	Use OR or AND as the default search operator. ☰ AND | OR	AND
Excluded categories	List of category IDs to exclude from the search index	None
Excluded plugins	List of plugin names to exclude while indexing	None

Option	Description	Default
Additional plugins searchable by default	List of plugin names that are required to additionnaly include while indexing. Example: fancytable,list,trackerlist,trackerfilter	attach, box, code, copyrigh...
Don't index non searchable fields	Indexing will skip adding all tracker fields that are not marked as "searchable". This will free index space but also make it impossible to use those fields in search index queries.	Disabled
Index forum replies together with initial post	Forum replies will be indexed together with the initial post as a single document instead of being indexed separately.	Enabled
Tokenize version numbers	Tokenize version number strings so that major versions are found when sub-versions are mentioned. For example, searching for 2.7 would return documents containing 2.7.4, but not 1.2.7.	Disabled
Tokenize CamelCase words	Consider the components of camel-case words as separate tokens, allowing them to be searched individually. ⚠️ *Conflicts with Tokenize Version Numbers.*	Disabled
Possessive Stemmer	The possessive stemmer removes possessives (trailing "'s") from words before indexing them.	Enabled
Field weights	Allow the field weights to be set that apply when ranking pages in the search results. The weight is applied only when the field is in the query. To nullify the value of a field, use an insignificant amount, but not 0, which may lead to unexpected behaviors such as stripping of results. (Add these fields to the "Default content fields" preference below for it to have an effect in a global "content" search) 👆 *One field per line, field_name**:**5.3*	title:2.5 allowed_groups:0....
Default content fields	All of the content is aggregated in the contents field. For custom weighting to apply, the fields must be included in the query. This option allows other fields to be included in the default content search.	contents, title
Cache per user and query for Tiki built-in search	Time in minutes a user has a same query cached applied to Tiki built-in search interface only.	0 minutes

Option	Description	Default
Cache result-specific formatted results	Formatted search results such as the ones used in the List plugin will be cached to prevent process-intensive reformatting on each page load. The cache is result-specific. ⚠️ *Every different result will generate a separate cache. This could quickly build up a large cache directory. It is recommended to clear Tiki caches often (e.g. once per week) via an automated job if you use this feature.*	Disabled
Cache individual search formatters	List of search formatters whose output will be cached. This is separate to the result-specific formatted results cache.	None
LIST plugin cache default on	If selected, LIST plugins will be cached by default unless turned off at plugin level.	Disabled
LIST plugin cache default expiry	Default number of minutes for LIST plugin cache expiry.	30
Format to use for tracker field keys	Choose between field IDs and permanent names for the tracker indexing ☰ Permanent name | Field ID (backward compatibility mode with Tiki 7 and 8)	Permanent name
Index Tracker Category names	Index the names and paths of category field values 👆 *Requires reindexing*	Enabled
Use unified search in category admin	Use unified search to find objects to add to categories. This limits the types of objects available to those included in the unified index.	Disabled
Automatically trim Elasticsearch results on date-sorted query	Automatically trim Elasticsearch results in unified search if the query is sorted by modification or creation date.	Disabled
Show error on missing field	When using List plugin to specify certain fields, especially tracker fields, this check helps ensure their names were entered correctly.	Enabled
Stop Word List	Words excluded from the search index, because they can be too frequent and produce unwanted results. 👆 *MySQL full-text search has its own list of stop words configured in the server.*	a, an, and, are, as, at, be...

Option	Description	Default
Search index outdated	Number of days to consider the search index outdated	2 days
Automatic indexing of file content	Uses command line tools to extract the information from the files based on their MIME types.	Disabled
Automatic indexing of emails stored as files	Parses message/rfc822 types of files (aka eml files) and stores individual email headers and content in search index.	Disabled
Asynchronous indexing		Enabled
Autocomplete page names	Automatically complete page names as the user starts typing. For example the user types the start of the wiki page name “Sear” and Tiki returns “Search”, “Search General Settings”, etc 🧹	Disabled
Referer search highlighting	When a user lands on a Tiki page from a search engine, Tiki highlights the search words they used. Its similar to using Tiki’s search facility.	Enabled
File thumbnail preview	Have a preview of attachments in search results	Disabled
Forum name search	👆 *When listing forums*	Disabled
Forum content search	👆 *When listing forums*	Enabled
Topic content search		Enabled
Unified search for forums and file galleries		Enabled

Option	Description	Default
Unified search index	Enables searching for content at the site using a Tiki-managed index. It's recommended to set a cron job to periodically rebuild the search index.	Enabled
Search statistics	Enables administrators to collect and view statistics on search activity.	Disabled

Option	Description	Default
Users available in search results	Users available within search results. Content related to the user will be included in the index. ☰ None | All | Public	None
Incremental Index Update	Update the index incrementally as the site content is modified. ⚠ *This may lead to lower performance and accuracy than processing the index on a periodic basis.*	Enabled
Search index rebuild memory limit	Temporarily adjust the memory limit to use during Search index rebuild. Depending on the volume of data, some large operations require more memory. Increasing it locally, per operation, allows to keep a lower memory limit globally. Keep in mind that memory usage is still limited to what is available on the server. ☝ *for example: 256M*	None
Search index rebuild time limit	Temporarily adjust the time limit to use during Search index rebuild. Depending on the volume of data, some requests may take longer. Increase the time limit locally to resolve the issue. Use reasonable values. ☝ *for example: 30*	None
Unified search engine	Search engine used to index the content of this Tiki site. Some engines are more suitable for larger sites, but require additional software on the server. ☰ MySQL full-text search | Elasticsearch | Manticore Search	MySQL full-text search
Elasticsearch URL	URL of any node in the cluster	http://localhost:9200
Elasticsearch Authentication	When Elasticsearch security module is enabled, user authentication can be set up here. ☰ No Authentication | Basic Authentication	None
Elasticsearch User	HTTP basic authentication user to be sent with each request to Elasticsearch.	None
Elasticsearch Password	HTTP basic authentication password to be sent with each request to Elasticsearch.	None
Elasticsearch index prefix	The prefix that is used for all indexes for this installation in Elasticsearch	Tiki_

Option	Description	Default
Elasticsearch current index	A new index is created upon rebuilding, and the old one is then destroyed. This setting enables seeing the currently active index. 👆 *Do not change this value unless you know what you are doing.*	None
Elasticsearch field limit per index	The maximum number of fields per search index in Elasticsearch version 5.x and above	1000 fields
Relation types to index within object.	Comma-separated relation types for which objects should be indexed in their related objects. 👆 *Elasticsearch needed*	None
Use MySQL Full-Text Search (fallback)	In case of Elasticsearch is active and unavailable, use MySQL Full-Text Search as fallback	Disabled
MySQL use short field names	Due to frm file constraints, number of search fields that one index can hold is usually limited to about 1500. This can be exceeded if you have numerous tracker fields. Enabling this option will try to shorten the field names internally that should allow you to use 300-500 more fields. Switching this option requires full index rebuild.	Disabled
Restore old MySQL indexes during reindex	If set, after the reindex is performed, old table MySQL indexes will be restored to the reindex related table. 🧪	Disabled
Manticore URL	URL of the Manticore search server	http://127.0.0.1
Manticore HTTP(S) Port	Port number for the HTTP(S) interface.	9308
Manticore MySQL Port	Port number for the MySQL interface.	9306
Manticore index prefix	The prefix that is used for all indexes for this installation in Manticore	Tiki_
Manticore current index	A new set of indexes are created upon rebuilding, and the old ones are then destroyed. This setting enables seeing the currently active index prefix. 👆 *Do not change this value unless you know what you are doing.*	None
Morphology processing	Advanced morphology preprocessors to apply in the Manticore index. See Manticore manual for possible values.	None

Option	Description	Default
Manticore indexed full-text fields	Manticore has a hard-limit of 256 full-text indexed fields per index. If your installation has more, some will be indexed as string attributes and perform the slower regex search. You can add a comma-separated list of fields to always index as full-text here.	title,contents
Default Boolean Operator	Use OR or AND as the default search operator. ☰ AND | OR	AND
Excluded categories	List of category IDs to exclude from the search index	None
Excluded plugins	List of plugin names to exclude while indexing	None
Additional plugins searchable by default	List of plugin names that are required to additionnaly include while indexing. Example: fancytable,list,trackerlist,trackerfilter	None
Don't index non searchable fields	Indexing will skip adding all tracker fields that are not marked as "searchable". This will free index space but also make it impossible to use those fields in search index queries.	Disabled
Index forum replies together with initial post	Forum replies will be indexed together with the initial post as a single document instead of being indexed separately.	Enabled
Tokenize version numbers	Tokenize version number strings so that major versions are found when sub-versions are mentioned. For example, searching for 2.7 would return documents containing 2.7.4, but not 1.2.7.	Disabled
Tokenize CamelCase words	Consider the components of camel-case words as separate tokens, allowing them to be searched individually. ⚠ *Conflicts with Tokenize Version Numbers.*	Disabled
Possessive Stemmer	The possessive stemmer removes possessives (trailing "'s") from words before indexing them.	Enabled

Option	Description	Default
Field weights	Allow the field weights to be set that apply when ranking pages in the search results. The weight is applied only when the field is in the query. To nullify the value of a field, use an insignificant amount, but not 0, which may lead to unexpected behaviors such as stripping of results. (Add these fields to the "Default content fields" preference below for it to have an effect in a global "content" search) *One field per line, field_name:5.3*	title:2.5 allowed_groups:0....
Default content fields	All of the content is aggregated in the contents field. For custom weighting to apply, the fields must be included in the query. This option allows other fields to be included in the default content search.	contents, title
Cache per user and query for Tiki built-in search	Time in minutes a user has a same query cached applied to Tiki built-in search interface only.	0 minutes
Cache result-specific formatted results	Formatted search results such as the ones used in the List plugin will be cached to prevent process-intensive reformatting on each page load. The cache is result-specific. *Every different result will generate a separate cache. This could quickly build up a large cache directory. It is recommended to clear Tiki caches often (e.g. once per week) via an automated job if you use this feature.*	Disabled
Cache individual search formatters	List of search formatters whose output will be cached. This is separate to the result-specific formatted results cache.	None
LIST plugin cache default on	If selected, LIST plugins will be cached by default unless turned off at plugin level.	Disabled
LIST plugin cache default expiry	Default number of minutes for LIST plugin cache expiry.	30
Format to use for tracker field keys	Choose between field IDs and permanent names for the tracker indexing Permanent name | Field ID (backward compatibility mode with Tiki 7 and 8)	Permanent name
Index Tracker Category names	Index the names and paths of category field values *Requires reindexing*	Disabled

Option	Description	Default
Use unified search in category admin	Use unified search to find objects to add to categories. This limits the types of objects available to those included in the unified index.	Disabled
Automatically trim Elasticsearch results on date-sorted query	Automatically trim Elasticsearch results in unified search if the query is sorted by modification or creation date.	Disabled
Show error on missing field	When using List plugin to specify certain fields, especially tracker fields, this check helps ensure their names were entered correctly.	Enabled
Stop Word List	Words excluded from the search index, because they can be too frequent and produce unwanted results. 👆 *MySQL full-text search has its own list of stop words configured in the server.*	a, an, and, are, as, at, be...
Search index outdated	Number of days to consider the search index outdated	2 days
Automatic indexing of file content	Uses command line tools to extract the information from the files based on their MIME types.	Disabled
Automatic indexing of emails stored as files	Parses message/rfc822 types of files (aka eml files) and stores individual email headers and content in search index.	Disabled
Asynchronous indexing		Enabled
MySQL full-text search	Also known as 'Basic Search'. This search uses the MySQL full-text search feature. The indexation is continuously updated. 🧹	Disabled
Referer search highlighting	When a user lands on a Tiki page from a search engine, Tiki highlights the search words they used. Its similar to using Tiki’s search facility.	Enabled
Ignore individual object permissions	Display items the user may not be entitled to view in search results. ⚠️ *Will improve performance, but may show forbidden results.*	Disabled

Option	Description	Default
Ignore category viewing restrictions	Display items the user may not be entitled to view in search results. ⚠️ *Will improve performance, but may show forbidden results*	Disabled
Autocomplete page names	Automatically complete page names as the user starts typing. For example the user types the start of the wiki page name “Sear” and Tiki returns “Search”, “Search General Settings”, etc 🧹	Disabled
File thumbnail preview	Have a preview of attachments in search results	Disabled
Forum name search	👆 *When listing forums*	Disabled
Forum content search	👆 *When listing forums*	Enabled
Topic content search		Enabled
Unified search for forums and file galleries		Enabled

Option	Description	Default
Unified search index	Enables searching for content at the site using a Tiki-managed index. It's recommended to set a cron job to periodically rebuild the search index.	Enabled
Search statistics	Enables administrators to collect and view statistics on search activity.	Disabled
Users available in search results	Users available within search results. Content related to the user will be included in the index. ☰ None | All | Public	None
Incremental Index Update	Update the index incrementally as the site content is modified. ⚠️ *This may lead to lower performance and accuracy than processing the index on a periodic basis.*	Enabled

Option	Description	Default
Search index rebuild memory limit	Temporarily adjust the memory limit to use during Search index rebuild. Depending on the volume of data, some large operations require more memory. Increasing it locally, per operation, allows to keep a lower memory limit globally. Keep in mind that memory usage is still limited to what is available on the server. *for example: 256M*	None
Search index rebuild time limit	Temporarily adjust the time limit to use during Search index rebuild. Depending on the volume of data, some requests may take longer. Increase the time limit locally to resolve the issue. Use reasonable values. *for example: 30*	None
Unified search engine	Search engine used to index the content of this Tiki site. Some engines are more suitable for larger sites, but require additional software on the server. MySQL full-text search | Elasticsearch	MySQL full-text search
Elasticsearch URL	URL of any node in the cluster	http://localhost:9200
Elasticsearch Authentication	When Elasticsearch security module is enabled, user authentication can be set up here. No Authentication | Basic Authentication	None
Elasticsearch User	HTTP basic authentication user to be sent with each request to Elasticsearch.	None
Elasticsearch Password	HTTP basic authentication password to be sent with each request to Elasticsearch.	None
Elasticsearch index prefix	The prefix that is used for all indexes for this installation in Elasticsearch	Tiki_
Elasticsearch current index	A new index is created upon rebuilding, and the old one is then destroyed. This setting enables seeing the currently active index. *Do not change this value unless you know what you are doing.*	None
Elasticsearch field limit per index	The maximum number of fields per search index in Elasticsearch version 5.x and above	1000 fields
Relation types to index within object.	Comma-separated relation types for which objects should be indexed in their related objects. *Elasticsearch needed*	None

Option	Description	Default
Use MySQL Full-Text Search (fallback)	In case of Elasticsearch is active and unavailable, use MySQL Full-Text Search as fallback	Disabled
MySQL use short field names	Due to frm file constraints, number of search fields that one index can hold is usually limited to about 1500. This can be exceeded if you have numerous tracker fields. Enabling this option will try to shorten the field names internally that should allow you to use 300-500 more fields. Switching this option requires full index rebuild.	Disabled
Restore old MySQL indexes during reindex	If set, after the reindex is performed, old table MySQL indexes will be restored to the reindex related table. 🧪	Disabled
Default Boolean Operator	Use OR or AND as the default search operator. ☰ AND | OR	AND
Excluded categories	List of category IDs to exclude from the search index	None
Excluded plugins	List of plugin names to exclude while indexing	None
Exclude all plugins	Indexing will exclude all plugins.	Enabled
Except included plugins	List of plugin names that are required to be included while indexing, when excluding all. Example: fancytable,list,trackerlist,trackerfilter	None
Don't index non searchable fields	Indexing will skip adding all tracker fields that are not marked as "searchable". This will free index space but also make it impossible to use those fields in search index queries.	Disabled
Index forum replies together with initial post	Forum replies will be indexed together with the initial post as a single document instead of being indexed separately.	Enabled
Tokenize version numbers	Tokenize version number strings so that major versions are found when sub-versions are mentioned. For example, searching for 2.7 would return documents containing 2.7.4, but not 1.2.7.	Disabled
Tokenize CamelCase words	Consider the components of camel-case words as separate tokens, allowing them to be searched individually. ⚠️ *Conflicts with Tokenize Version Numbers.*	Disabled

Option	Description	Default
Possessive Stemmer	The possessive stemmer removes possessives (trailing "'s") from words before indexing them.	Enabled
Field weights	Allow the field weights to be set that apply when ranking pages in the search results. The weight is applied only when the field is in the query. To nullify the value of a field, use an insignificant amount, but not 0, which may lead to unexpected behaviors such as stripping of results. (Add these fields to the "Default content fields" preference below for it to have an effect in a global "content" search) *One field per line, field_name:5.3*	title:2.5 allowed_groups:0....
Default content fields	All of the content is aggregated in the contents field. For custom weighting to apply, the fields must be included in the query. This option allows other fields to be included in the default content search.	contents, title
Cache per user and query for Tiki built-in search	Time in minutes a user has a same query cached applied to Tiki built-in search interface only.	0 minutes
Cache result-specific formatted results	Formatted search results such as the ones used in the List plugin will be cached to prevent process-intensive reformatting on each page load. The cache is result-specific. *Every different result will generate a separate cache. This could quickly build up a large cache directory. It is recommended to clear Tiki caches often (e.g. once per week) via an automated job if you use this feature.*	Disabled
Cache individual search formatters	List of search formatters whose output will be cached. This is separate to the result-specific formatted results cache.	None
LIST plugin cache default on	If selected, LIST plugins will be cached by default unless turned off at plugin level.	Disabled
LIST plugin cache default expiry	Default number of minutes for LIST plugin cache expiry.	30
Format to use for tracker field keys	Choose between field IDs and permanent names for the tracker indexing Permanent name | Field ID (backward compatibility mode with Tiki 7 and 8)	Permanent name

Option	Description	Default
Index Tracker Category names	Index the names and paths of category field values 👆 *Requires reindexing*	Disabled
Use unified search in category admin	Use unified search to find objects to add to categories. This limits the types of objects available to those included in the unified index.	Disabled
Automatically trim Elasticsearch results on date-sorted query	Automatically trim Elasticsearch results in unified search if the query is sorted by modification or creation date.	Disabled
Show error on missing field	When using List plugin to specify certain fields, especially tracker fields, this check helps ensure their names were entered correctly.	Enabled
Stop Word List	Words excluded from the search index, because they can be too frequent and produce unwanted results. 👆 *MySQL full-text search has its own list of stop words configured in the server.*	a, an, and, are, as, at, be...
Search index outdated	Number of days to consider the search index outdated	2 days
Automatic indexing of file content	Uses command line tools to extract the information from the files based on their MIME types.	Disabled
Automatic indexing of emails stored as files	Parses message/rfc822 types of files (aka eml files) and stores individual email headers and content in search index.	Disabled
Asynchronous indexing		Enabled
MySQL full-text search	Also known as 'Basic Search'. This search uses the MySQL full-text search feature. The indexation is continuously updated. 🧹	Disabled
Referer search highlighting	When a user lands on a Tiki page from a search engine, Tiki highlights the search words they used. Its similar to using Tiki's search facility.	Enabled
Ignore individual object permissions	Display items the user may not be entitled to view in search results. ⚠️ *Will improve performance, but may show forbidden results.*	Disabled

Option	Description	Default
Ignore category viewing restrictions	Display items the user may not be entitled to view in search results. ⚠️ *Will improve performance, but may show forbidden results*	Disabled
Autocomplete page names	Automatically complete page names as the user starts typing. For example the user types the start of the wiki page name “Sear” and Tiki returns “Search”, “Search General Settings”, etc 🧹	Disabled
File thumbnail preview	Have a preview of attachments in search results	Disabled
Forum name search	👆 *When listing forums*	Disabled
Forum content search	👆 *When listing forums*	Enabled
Topic content search		Enabled
Unified search for forums and file galleries		Enabled

Option	Description	Default
Unified search index	Enables searching for content at the site using a Tiki-managed index. It's recommended to set a cron job to periodically rebuild the search index.	Enabled
Search statistics	Enables administrators to collect and view statistics on search activity.	Disabled
Users available in search results	Users available within search results. Content related to the user will be included in the index. ☰ None | All | Public	None
Incremental Index Update	Update the index incrementally as the site content is modified. ⚠️ *This may lead to lower performance and accuracy than processing the index on a periodic basis.*	Enabled

Option	Description	Default
Search index rebuild memory limit	Temporarily adjust the memory limit to use during Search index rebuild. Depending on the volume of data, some large operations require more memory. Increasing it locally, per operation, allows to keep a lower memory limit globally. Keep in mind that memory usage is still limited to what is available on the server. *for example: 256M*	None
Search index rebuild time limit	Temporarily adjust the time limit to use during Search index rebuild. Depending on the volume of data, some requests may take longer. Increase the time limit locally to resolve the issue. Use reasonable values. *for example: 30*	None
Unified search engine	Search engine used to index the content of this Tiki site. Some engines are more suitable for larger sites, but require additional software on the server. Lucene (PHP implementation) - Deprecated | MySQL full-text search | Elasticsearch	MySQL full-text search
Highlight results snippets	Highlight the result snippet based on the search query to improve user experience. *May impact performance*	Disabled
Lucene index location	Path to the location of the Lucene search index. The index must be on a local filesystem with enough space to contain the volume of the database.	temp/unified-index
Lucene maximum results	Maximum number of results to produce. Results beyond these will need a more refined query to be reached.	200 results
Lucene maximum result-set limit	This is used when calculating result scores and sort order which can lead to "out of memory" errors on large data sets. The default of 1000 is safe with the PHP memory_limit set to 128M *Maximum size of result set to consider.* *0 for unlimited*	1000 result sets
Lucene terms per query limit	Maximum number of terms to be generated. This value may need to be increased in the case of "Terms per query limit is reached" especially with wildcard, range and fuzzy searches.	1024 terms

Option	Description	Default
Lucene maximum number of buffered documents	Number of documents required before the buffered in-memory documents are written into a new segment.	10 documents
Lucene maximum number of merge documents	Largest number of documents merged by addDocument(). Small values (for example, less than 10,000) are best for interactive indexing, as this limits the length of pauses while indexing to a few seconds. Larger values are best for batched indexing and speedier searches. 👆 *Small values (for example, less than 10,000) are best for interactive indexing. Use 0 for the Lucene default, which is practically infinite.*	0 merge documents
Lucene merge factor	How often segment indices are merged by addDocument(). With smaller values, less RAM is used while indexing, and searches on unoptimized indices are faster, but indexing speed is slower. With larger values, more RAM is used during indexing, and while searches on unoptimized indices are slower, indexing is faster. 👆 *Large values (greater than 10) are best for batch index creation, and smaller values (less than 10) for indices that are interactively maintained.*	10
Elasticsearch URL	URL of any node in the cluster	http://localhost:9200
Elasticsearch index prefix	The prefix that is used for all indexes for this installation in Elasticsearch	Tiki_
Elasticsearch current index	A new index is created upon rebuilding, and the old one is then destroyed. This setting enables seeing the currently active index. 👆 *Do not change this value unless you know what you are doing.*	None
Elasticsearch field limit per index	The maximum number of fields per search index in Elasticsearch version 5.x and above	1000 fields
Relation types to index within object.	Comma-separated relation types for which objects should be indexed in their related objects. 👆 *Elasticsearch needed*	None
Use MySQL Full-Text Search (fallback)	In case of Elasticsearch is active and unavailable, use MySQL Full-Text Search as fallback	Disabled

Option	Description	Default
MySQL use short field names	Due to frm file constraints, number of search fields that one index can hold is usually limited to about 1500. This can be exceeded if you have numerous tracker fields. Enabling this option will try to shorten the field names internally that should allow you to use 300-500 more fields. Switching this option requires full index rebuild.	Disabled
Default Boolean Operator	Use OR or AND as the default search operator. ☰ AND | OR	AND
Excluded categories	List of category IDs to exclude from the search index	None
Excluded plugins	List of plugin names to exclude while indexing	None
Exclude all plugins	Indexing will exclude all plugins.	Enabled
Except included plugins	List of plugin names that are required to be included while indexing, when excluding all. Example: fancytable,list,trackerlist,trackerfilter	None
Don't index non searchable fields	Indexing will skip adding all tracker fields that are not marked as "searchable". This will free index space but also make it impossible to use those fields in search index queries.	Disabled
Index forum replies together with initial post	Forum replies will be indexed together with the initial post as a single document instead of being indexed separately.	Enabled
Tokenize version numbers	Tokenize version number strings so that major versions are found when sub-versions are mentioned. For example, searching for 2.7 would return documents containing 2.7.4, but not 1.2.7.	Disabled
Tokenize CamelCase words	Consider the components of camel-case words as separate tokens, allowing them to be searched individually. ⚠ *Conflicts with Tokenize Version Numbers.*	Disabled
Possessive Stemmer	The possessive stemmer removes possessives (trailing "'s") from words before indexing them.	Enabled

Option	Description	Default
Field weights	Allow the field weights to be set that apply when ranking pages in the search results. The weight is applied only when the field is in the query. To nullify the value of a field, use an insignificant amount, but not 0, which may lead to unexpected behaviors such as stripping of results. (Add these fields to the "Default content fields" preference below for it to have an effect in a global "content" search) *One field per line, field_name:5.3*	title:2.5 allowed_groups:0....
Default content fields	All of the content is aggregated in the contents field. For custom weighting to apply, the fields must be included in the query. This option allows other fields to be included in the default content search.	contents, title
Cache per user and query for Tiki built-in search	Time in minutes a user has a same query cached applied to Tiki built-in search interface only.	0 minutes
Cache result-specific formatted results	Formatted search results such as the ones used in the List plugin will be cached to prevent process-intensive reformatting on each page load. The cache is result-specific. *Every different result will generate a separate cache. This could quickly build up a large cache directory. It is recommended to clear Tiki caches often (e.g. once per week) via an automated job if you use this feature.*	Disabled
Cache individual search formatters	List of search formatters whose output will be cached. This is separate to the result-specific formatted results cache.	None
LIST plugin cache default on	If selected, LIST plugins will be cached by default unless turned off at plugin level.	Disabled
LIST plugin cache default expiry	Default number of minutes for LIST plugin cache expiry.	30
Format to use for tracker field keys	Choose between field IDs and permanent names for the tracker indexing Permanent name | Field ID (backward compatibility mode with Tiki 7 and 8)	Permanent name
Index Tracker Category names	Index the names and paths of category field values *Requires reindexing*	Disabled

Option	Description	Default
Use unified search in category admin	Use unified search to find objects to add to categories. This limits the types of objects available to those included in the unified index.	Disabled
Automatically trim Elasticsearch results on date-sorted query	Automatically trim Elasticsearch results in unified search if the query is sorted by modification or creation date.	Disabled
Show error on missing field	When using List plugin to specify certain fields, especially tracker fields, this check helps ensure their names were entered correctly.	Enabled
Stop Word List	Words excluded from the search index, because they can be too frequent and produce unwanted results. 👆 *MySQL full-text search has its own list of stop words configured in the server.*	a, an, and, are, as, at, be...
Search index outdated	Number of days to consider the search index outdated	2 days
Automatic indexing of file content	Uses command line tools to extract the information from the files based on their MIME types.	Disabled
Asynchronous indexing		Enabled
MySQL full-text search	Also known as 'Basic Search'. This search uses the MySQL full-text search feature. The indexation is continuously updated. 🧹	Disabled
Referer search highlighting	When a user lands on a Tiki page from a search engine, Tiki highlights the search words they used. Its similar to using Tiki’s search facility.	Enabled
Ignore individual object permissions	Display items the user may not be entitled to view in search results. ⚠️ *Will improve performance, but may show forbidden results.*	Disabled
Ignore category viewing restrictions	Display items the user may not be entitled to view in search results. ⚠️ *Will improve performance, but may show forbidden results*	Disabled

Option	Description	Default
Autocomplete page names	Automatically complete page names as the user starts typing. For example the user types the start of the wiki page name “Sear” and Tiki returns “Search”, “Search General Settings”, etc 🧹	Disabled
File thumbnail preview	Have a preview of attachments in search results	Disabled
Forum name search	👆 *When listing forums*	Disabled
Forum content search	👆 *When listing forums*	Enabled
Topic content search		Enabled
Tiki-indexed search		Disabled
Use database (full-text) search		Disabled

Search - Stored search

Option	Description	Default
Stored searches	Allow users to store search queries.	Disabled

Option	Description	Default
Stored searches	Allow users to store search queries.	Disabled

Option	Description	Default
Stored searches	Allow users to store search queries.	Disabled

Option	Description	Default
Stored searches	Allow users to store search queries.	Disabled

Option	Description	Default
Stored searches	Allow users to store search queries.	Disabled

Security - General security

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. ⚠ *You should leave this on unless you know what you are doing.*	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. 👆 *Use "," to separate values* ⚠ *There may be security implications. Make sure you know what you are doing.*	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. 👆 *Use "," to separate values* ⚠ *There may be security implications. Make sure you know what you are doing.*	None
Allowed Smarty modifiers	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. 👆 *Use "," to separate values* ⚠ *There may be security implications. Make sure you know what you are doing.*	None

Option	Description	Default
Disabled Smarty modifiers	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. 👆 *Use "," to separate values* ⚠️ *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
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

Option	Description	Default
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. 🧪	Enabled
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

Option	Description	Default
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
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

Option	Description	Default
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
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	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. ⚠️ *You should leave this on unless you know what you are doing.*	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. 👆 *Use "," to separate values* ⚠️ *There may be security implications. Make sure you know what you are doing.*	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. 👆 *Use "," to separate values* ⚠️ *There may be security implications. Make sure you know what you are doing.*	None
Allowed Smarty modifiers	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. 👆 *Use "," to separate values* ⚠️ *There may be security implications. Make sure you know what you are doing.*	None
Disabled Smarty modifiers	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. 👆 *Use "," to separate values* ⚠️ *There may be security implications. Make sure you know what you are doing.*	None

Option	Description	Default
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
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

Option	Description	Default
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. 🧪	Enabled
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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

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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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
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

Option	Description	Default
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

Security - OpenPGP

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠️ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled

Option	Description	Default
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠️ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. 👆 *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠️ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. 👆 *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠️ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. 👆 *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Option	Description	Default
PGP/MIME encrypted email messaging	Use OpenPGP PGP/MIME-compliant encrypted email messaging. All email messaging, notifications, and newsletters are sent as PGP/MIME-encrypted messages, signed with the signer key, and are completely opaque to outsiders. All user accounts need to be properly configured in a gnupg keyring with public keys associated with their tiki-account-related email addresses. ⚠️ *Enable only if gpg, keyring, and tikiaccounts are properly configured for PGP/MIME functionality. NOTE: Requires that all accounts have their public-keys configured into gnupg-keyring, so do not allow non-administred registrations (or e.g. non-configured emails for newsletters etc) to site if this feature turned on.*	Disabled
Path to gnupg keyring	Full directory path to gnupg keyring (default /home/www/.gnupg/). The directory, related subdirectories (e.g., a subdirectory 'signer'), and files must have proper permissions for tiki to access/read the directories/files, and create/delete necessary temporary workfiles there.	/home/www/.gnupg/
Path to gpg executable	Full path to gpg executable.	/usr/bin/gpg
Read signer pass phrase from prefs or from a file	Read GnuPG signer pass phrase from preferences or from a file (default is 'file'). With file option, configure other preference for the full path including the filename of the file containing the GnuPG signer private-key pass phrase. ☰ preferences | file	Preferences
Signer pass phrase	GnuPG signer private-key passphrase. Define pass phrase either here or in a signer pass phrase file. 👆 *leave empty if read from file*	None
Path to signer pass phrase filename	Full path including the filename of the file containing the GnuPG signer private-key pass phrase. The directory and file must have proper permissions for tiki to access/read the signer pass phrase file.	/home/www/.gnupg/signer/sig...

Security - Search results

Option	Description	Default
Ignore category viewing restrictions	Display items the user may not be entitled to view in search results. ⚠ *Will improve performance, but may show forbidden results*	Disabled
Ignore individual object permissions	Display items the user may not be entitled to view in search results. ⚠ *Will improve performance, but may show forbidden results.*	Disabled

Option	Description	Default
Ignore category viewing restrictions	Display items the user may not be entitled to view in search results. ⚠ *Will improve performance, but may show forbidden results*	Disabled
Ignore individual object permissions	Display items the user may not be entitled to view in search results. ⚠ *Will improve performance, but may show forbidden results.*	Disabled

Option	Description	Default
Ignore category viewing restrictions	Display items the user may not be entitled to view in search results. ⚠ *Will improve performance, but may show forbidden results*	Disabled
Ignore individual object permissions	Display items the user may not be entitled to view in search results. ⚠ *Will improve performance, but may show forbidden results.*	Disabled

Security - Site access

Option	Description	Default
Close site	Use this setting to "close" the Tiki site (such as for maintenance). Users attempting to access the site will see only a log-in form. Only users with specific permission will be allowed to log in. Use the Message to display to specify the message that visitors will see when attempting to access your site.	Disabled
Title		Coming soon
Message		Site is closed for maintena...
Close site when server load is above the threshold	Use this option to "close" the Tiki site when the server load exceeds a specific threshold. Only users with specific permission will be allowed to log in. Use "Maximum average server load threshold in the last minute" to define the maximum server load. Use the "Message to display" to specify the message that visitors will see when attempting to access the site.	Disabled
Maximum average server load threshold in the last minute		3
Site Busy Title		Server too busy
Site Busy Message		Server is currently too bus...
Enable intrusion detection system	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.	Disabled
Custom rules file		temp/ids_custom_rules.json
Intrusion detection system mode	Define IDS operation mode, log only, or log and block with impact over a given threshold. Log only | Log and block requests	Log only
Intrusion detection system threshold	Define IDS threshold, when configured in "Log and block requests" more.	0

Option	Description	Default
Log to file		ids.log
Log to database		Disabled

Option	Description	Default
Close site	Use this setting to "close" the Tiki site (such as for maintenance). Users attempting to access the site will see only a log-in form. Only users with specific permission will be allowed to log in. Use the Message to display to specify the message that visitors will see when attempting to access your site.	Disabled
Title		Coming soon
Message		Site is closed for maintena...
Close site when server load is above the threshold	Use this option to "close" the Tiki site when the server load exceeds a specific threshold. Only users with specific permission will be allowed to log in. Use "Maximum average server load threshold in the last minute" to define the maximum server load. Use the "Message to display" to specify the message that visitors will see when attempting to access the site.	Disabled
Maximum average server load threshold in the last minute		3
Site Busy Title		Server too busy
Site Busy Message		Server is currently too bus...
Enable intrusion detection system	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.	Disabled
Custom rules file		temp/ids_custom_rules.json
Intrusion detection system mode	Define IDS operation mode, log only, or log and block with impact over a given threshold. ☰ Log only | Log and block requests	Log only

Option	Description	Default
Intrusion detection system threshold	Define IDS threshold, when configured in "Log and block requests" more.	0
Log to file		ids.log
Log to database		Disabled

Option	Description	Default
Close site	Use this setting to "close" the Tiki site (such as for maintenance). Users attempting to access the site will see only a log-in form. Only users with specific permission will be allowed to log in. Use the Message to display to specify the message that visitors will see when attempting to access your site.	Disabled
Title		Coming soon
Message		Site is closed for maintena...
Close site when server load is above the threshold	Use this option to "close" the Tiki site when the server load exceeds a specific threshold. Only users with specific permission will be allowed to log in. Use "Maximum average server load threshold in the last minute" to define the maximum server load. Use the "Message to display" to specify the message that visitors will see when attempting to access the site.	Disabled
Maximum average server load threshold in the last minute		3
Site Busy Title		Server too busy
Site Busy Message		Server is currently too bus...
Enable intrusion detection system	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.	Disabled
Custom rules file		temp/ids_custom_rules.json

Option	Description	Default
Intrusion detection system mode	Define IDS operation mode, log only, or log and block with impact over a given threshold. ☰ Log only | Log and block requests	Log only
Intrusion detection system threshold	Define IDS threshold, when configured in "Log and block requests" more.	0
Log to file		ids.log
Log to database		Disabled

Option	Description	Default
Close site	Use this setting to \"close\" the Tiki site (such as for maintenance). Users attempting to access the site will see only a log-in form. Only users with specific permission will be allowed to log in. Use the Message to display to specify the message that visitors will see when attempting to access your site.	Disabled
Title		Coming soon
Message		Site is closed for maintena...
Close site when server load is above the threshold	Use this option to "close" the Tiki site when the server load exceeds a specific threshold. Only users with specific permission will be allowed to log in. Use "Maximum average server load threshold in the last minute" to define the maximum server load. Use the "Message to display" to specify the message that visitors will see when attempting to access the site.	Disabled
Maximum average server load threshold in the last minute		3
Site Busy Title		Server too busy
Site Busy Message		Server is currently too bus...

Option	Description	Default
Enable intrusion detection system	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.	Disabled
Custom rules file		temp/ids_custom_rules.json
Intrusion detection system mode	Define IDS operation mode, log only, or log and block with impact over a given threshold. ☰ Log only | Log and block requests	Log only
Intrusion detection system threshold	Define IDS threshold, when configured in "Log and block requests" more.	0
Log to file		ids.log
Log to database		Disabled

Option	Description	Default
Close site	Use this setting to \"close\" the Tiki site (such as for maintenance). Users attempting to access the site will see only a log-in form. Only users with specific permission will be allowed to log in. Use the Message to display to specify the message that visitors will see when attempting to access your site.	Disabled
Title		Coming soon
Message		Site is closed for maintena...
Close site when server load is above the threshold	Use this option to "close" the Tiki site when the server load exceeds a specific threshold. Only users with specific permission will be allowed to log in. Use "Maximum average server load threshold in the last minute" to define the maximum server load. Use the "Message to display" to specify the message that visitors will see when attempting to access the site.	Disabled
Maximum average server load threshold in the last minute		3

Option	Description	Default
Site Busy Title		Server too busy
Site Busy Message		Server is currently too bus...
Enable intrusion detection system	An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.	Disabled
Custom rules file		temp/ids_custom_rules.json
Intrusion detection system mode	Define IDS operation mode, log only, or log and block with impact over a given threshold. Log only | Log and block requests	Log only
Intrusion detection system threshold	Define IDS threshold, when configured in "Log and block requests" more.	0
Log to file		ids.log
Log to database		Disabled

Security - Spam protection

Option	Description	Default
Anonymous editors must enter anti-bot code (CAPTCHA)	Use CAPTCHA to ensure that anonymous input is from a person.	Enabled
CAPTCHA image word length	Number of characters the CAPTCHA will display.	6 characters
CAPTCHA image width	Width of the CAPTCHA image in pixels.	180 pixels
CAPTCHA image noise	Level of noise of the CAPTCHA image. *Choose a smaller number for less noise and easier reading.*	100
Use reCAPTCHA	Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA *You will need to register at http://www.google.com/recaptcha*	Disabled

Option	Description	Default
Site key	reCAPTCHA public key obtained after registering.	None
Secret key	reCAPTCHA private key obtained after registering.	None
reCAPTCHA theme	Choose a theme for the reCAPTCHA widget. ☰ Clean | Black Glass | Red | White	Clean
Version	reCAPTCHA version. ☰ 1.0 | 2.0 | 3.0	2.0
CAPTCHA questions	Requires anonymous visitors to enter the answer to a question.	Disabled
CAPTCHA questions and answers	Add some simple questions that only humans should be able to answer, in the format: "Question?: Answer" with one per line 👆 *One question per line with a colon separating the question and answer*	None
Protect email against spam	Protect email against spam submissions. ⚠️ *Protect email against spam currently does not operate in pages edited in WYSIWYG mode (Tiki 6.1)*	Enabled
Add "rel=nofollow" to external links	Nofollow is used to instruct some search engines that the link should not influence the ranking of the link's target in the search engine's index.	Disabled
Banning system	Deny access to specific users based on username, IP, and date/time range.	Disabled
Ban usernames and emails	Banning rules use both email and username to match rules.	Disabled
Attempts number	Number of attempts user is allowed to login incorrectly before banning them from further attempts.	5
Banning system	The duration of the incorrect login attempts ban in minutes.	30
Comments moderation	Enables the admin or other authorized group member to validate comments before they are visible	Disabled
Use Akismet to filter comments	Prevent comment spam by using the Akismet service to determine if the comment is spam. If comment moderation is enabled, Akismet will indicate if the comment is to be moderated or not. If there is no comment moderation, the comment will be rejected if considered to be spam.	Disabled
Akismet API Key	Key required for the Akismet comment spam prevention. 👆 *Obtain this key by registering your site at http://akismet.com*	None

Option	Description	Default
Filter spam for registered users	Activate spam filtering for registered users as well. Useful if your site allows anyone to register without screening.	Disabled
Require passcode to register	Users must enter an alphanumeric code to register. The site administrator must inform users of this code. This is to restrict registration to invited users.	Disabled
Passcode	*Alphanumeric code required to complete the registration*	None
Show passcode on registration form	Displays the required passcode on the registration form. This is helpful for legitimate users who want to register while making it difficult for automated robots because the passcode is unique for each site and because it is displayed in JavaScript.	Disabled
Registration page key	To register, users need to go to, for example: tiki-register.php?key=yourregistrationkeyvalue *Key required to be on included the URL to access the registration page (if not empty).*	None

Option	Description	Default
Anonymous editors must enter anti-bot code (CAPTCHA)	Use CAPTCHA to ensure that anonymous input is from a person.	Enabled
CAPTCHA image word length	Number of characters the CAPTCHA will display.	6 characters
CAPTCHA image width	Width of the CAPTCHA image in pixels.	180 pixels
CAPTCHA image noise	Level of noise of the CAPTCHA image. *Choose a smaller number for less noise and easier reading.*	100
Use reCAPTCHA	Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA *You will need to register at http://www.google.com/recaptcha*	Disabled
Site key	reCAPTCHA public key obtained after registering.	None
Secret key	reCAPTCHA private key obtained after registering.	None
reCAPTCHA theme	Choose a theme for the reCAPTCHA widget. Clean | Black Glass | Red | White	Clean

Option	Description	Default
Version	reCAPTCHA version. ☰ 1.0 | 2.0 | 3.0	2.0
CAPTCHA questions	Requires anonymous visitors to enter the answer to a question.	Disabled
CAPTCHA questions and answers	Add some simple questions that only humans should be able to answer, in the format: "Question?: Answer" with one per line *One question per line with a colon separating the question and answer*	None
Protect email against spam	Protect email against spam submissions. *Protect email against spam currently does not operate in pages edited in WYSIWYG mode (Tiki 6.1)*	Enabled
Add "rel=nofollow" to external links	Nofollow is used to instruct some search engines that the link should not influence the ranking of the link's target in the search engine's index.	Disabled
Banning system	Deny access to specific users based on username, IP, and date/time range.	Disabled
Ban usernames and emails	Banning rules use both email and username to match rules.	Disabled
Attempts number	Number of attempts user is allowed to login incorrectly before banning them from further attempts.	5
Banning system	The duration of the incorrect login attempts ban in minutes.	30
Comments moderation	Enables the admin or other authorized group member to validate comments before they are visible	Disabled
Use Akismet to filter comments	Prevent comment spam by using the Akismet service to determine if the comment is spam. If comment moderation is enabled, Akismet will indicate if the comment is to be moderated or not. If there is no comment moderation, the comment will be rejected if considered to be spam.	Disabled
Akismet API Key	Key required for the Akismet comment spam prevention. *Obtain this key by registering your site at http://akismet.com*	None
Filter spam for registered users	Activate spam filtering for registered users as well. Useful if your site allows anyone to register without screening.	Disabled
Require passcode to register	Users must enter an alphanumeric code to register. The site administrator must inform users of this code. This is to restrict registration to invited users.	Disabled

Option	Description	Default
Passcode	*Alphanumeric code required to complete the registration*	None
Show passcode on registration form	Displays the required passcode on the registration form. This is helpful for legitimate users who want to register while making it difficult for automated robots because the passcode is unique for each site and because it is displayed in JavaScript.	Disabled
Registration page key	To register, users need to go to, for example: tiki-register.php?key=yourregistrationkeyvalue *Key required to be on included the URL to access the registration page (if not empty).*	None

Option	Description	Default
Anonymous editors must enter anti-bot code (CAPTCHA)	Use CAPTCHA to ensure that anonymous input is from a person.	Enabled
CAPTCHA image word length	Number of characters the CAPTCHA will display.	6 characters
CAPTCHA image width	Width of the CAPTCHA image in pixels.	180 pixels
CAPTCHA image noise	Level of noise of the CAPTCHA image. *Choose a smaller number for less noise and easier reading.*	100
Use reCAPTCHA	Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA *You will need to register at http://www.google.com/recaptcha*	Disabled
Site key	reCAPTCHA public key obtained after registering.	None
Secret key	reCAPTCHA private key obtained after registering.	None
reCAPTCHA theme	Choose a theme for the reCAPTCHA widget. Clean | Black Glass | Red | White	Clean
Version	reCAPTCHA version. 1.0 | 2.0 | 3.0	2.0
CAPTCHA questions	Requires anonymous visitors to enter the answer to a question.	Disabled

Option	Description	Default
CAPTCHA questions and answers	Add some simple questions that only humans should be able to answer, in the format: "Question?: Answer" with one per line 👆 *One question per line with a colon separating the question and answer*	None
Protect email against spam	Protect email against spam submissions. ⚠️ *Protect email against spam currently does not operate in pages edited in WYSIWYG mode (Tiki 6.1)*	Enabled
Add "rel=nofollow" to external links	Nofollow is used to instruct some search engines that the link should not influence the ranking of the link's target in the search engine's index.	Disabled
Banning system	Deny access to specific users based on username, IP, and date/time range.	Disabled
Ban usernames and emails	Banning rules use both email and username to match rules.	Disabled
Attempts number	Number of attempts user is allowed to login incorrectly before banning them from further attempts.	5
Banning system	The duration of the incorrect login attempts ban in minutes.	30
Comments moderation	Enables the admin or other authorized group member to validate comments before they are visible	Disabled
Use Akismet to filter comments	Prevent comment spam by using the Akismet service to determine if the comment is spam. If comment moderation is enabled, Akismet will indicate if the comment is to be moderated or not. If there is no comment moderation, the comment will be rejected if considered to be spam.	Disabled
Akismet API Key	Key required for the Akismet comment spam prevention. 👆 *Obtain this key by registering your site at http://akismet.com*	None
Filter spam for registered users	Activate spam filtering for registered users as well. Useful if your site allows anyone to register without screening.	Disabled
Require passcode to register	Users must enter an alphanumeric code to register. The site administrator must inform users of this code. This is to restrict registration to invited users.	Disabled
Passcode	👆 *Alphanumeric code required to complete the registration*	None

Option	Description	Default
Show passcode on registration form	Displays the required passcode on the registration form. This is helpful for legitimate users who want to register while making it difficult for automated robots because the passcode is unique for each site and because it is displayed in JavaScript.	Disabled
Registration page key	To register, users need to go to, for example: tiki-register.php?key=yourregistrationkeyvalue *Key required to be on included the URL to access the registration page (if not empty).*	None

Option	Description	Default
Anonymous editors must enter anti-bot code (CAPTCHA)	Use CAPTCHA to ensure that anonymous input is from a person.	Enabled
CAPTCHA image word length	Number of characters the CAPTCHA will display.	6 characters
CAPTCHA image width	Width of the CAPTCHA image in pixels.	180 pixels
CAPTCHA image noise	Level of noise of the CAPTCHA image. *Choose a smaller number for less noise and easier reading.*	100
Use reCAPTCHA	Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA *You will need to register at http://www.google.com/recaptcha*	Disabled
Site key	reCAPTCHA public key obtained after registering.	None
Secret key	reCAPTCHA private key obtained after registering.	None
reCAPTCHA theme	Choose a theme for the reCAPTCHA widget. Clean | Black Glass | Red | White	Clean
Version	reCAPTCHA version. 1.0 | 2.0 | 3.0	2.0
CAPTCHA questions	Requires anonymous visitors to enter the answer to a question.	Disabled

Option	Description	Default
CAPTCHA questions and answers	Add some simple questions that only humans should be able to answer, in the format: "Question?: Answer" with one per line 👆 *One question per line with a colon separating the question and answer*	None
Protect email against spam	Protect email against spam submissions. ⚠️ *Protect email against spam currently does not operate in pages edited in WYSIWYG mode (Tiki 6.1)*	Enabled
Add "rel=nofollow" to external links	Nofollow is used to instruct some search engines that the link should not influence the ranking of the link's target in the search engine's index.	Disabled
Banning system	Deny access to specific users based on username, IP, and date/time range.	Disabled
Ban usernames and emails	Banning rules use both email and username to match rules.	Disabled
Comments moderation	Enables the admin or other authorized group member to validate comments before they are visible	Disabled
Use Akismet to filter comments	Prevent comment spam by using the Akismet service to determine if the comment is spam. If comment moderation is enabled, Akismet will indicate if the comment is to be moderated or not. If there is no comment moderation, the comment will be rejected if considered to be spam.	Disabled
Akismet API Key	Key required for the Akismet comment spam prevention. 👆 *Obtain this key by registering your site at http://akismet.com*	None
Filter spam for registered users	Activate spam filtering for registered users as well. Useful if your site allows anyone to register without screening.	Disabled
Require passcode to register	Users must enter an alphanumeric code to register. The site administrator must inform users of this code. This is to restrict registration to invited users.	Disabled
Passcode	👆 *Alphanumeric code required to complete the registration*	None
Show passcode on registration form	Displays the required passcode on the registration form. This is helpful for legitimate users who want to register while making it difficult for automated robots because the passcode is unique for each site and because it is displayed in JavaScript.	Disabled

Option	Description	Default
Registration page key	To register, users need to go to, for example: tiki-register.php?key=yourregistrationkeyvalue *Key required to be on included the URL to access the registration page (if not empty).*	None

Option	Description	Default
Anonymous editors must enter anti-bot code (CAPTCHA)	Use CAPTCHA to ensure that anonymous input is from a person.	Enabled
CAPTCHA image word length	Number of characters the CAPTCHA will display.	6 characters
CAPTCHA image width	Width of the CAPTCHA image in pixels.	180 pixels
CAPTCHA image noise	Level of noise of the CAPTCHA image. *Choose a smaller number for less noise and easier reading.*	100
Use reCAPTCHA	Use reCAPTCHA, a specialized captcha service, instead of default CAPTCHA *You will need to register at http://www.google.com/recaptcha*	Disabled
Site key	reCAPTCHA public key obtained after registering.	None
Secret key	reCAPTCHA private key obtained after registering.	None
reCAPTCHA theme	Choose a theme for the reCAPTCHA widget. Clean | Black Glass | Red | White	Clean
Version	reCAPTCHA version. 1.0 | 2.0 | 3.0	2.0
CAPTCHA questions	Requires anonymous visitors to enter the answer to a question.	Disabled
CAPTCHA questions and answers	Add some simple questions that only humans should be able to answer, in the format: "Question?: Answer" with one per line *One question per line with a colon separating the question and answer*	None
Protect email against spam	Protect email against spam submissions. *Protect email against spam currently does not operate in pages edited in WYSIWYG mode (Tiki 6.1)*	Enabled

Option	Description	Default
Add "rel=nofollow" to external links	Nofollow is used to instruct some search engines that the link should not influence the ranking of the link's target in the search engine's index.	Disabled
Banning system	Deny access to specific users based on username, IP, and date/time range.	Disabled
Attempts number	Number of attempts user is allowed to login incorrectly before banning them from further attempts.	5
Banning system	The duration of the incorrect login attempts ban in minutes.	30
Comments moderation	Enables the admin or other authorized group member to validate comments before they are visible	Disabled
Use Akismet to filter comments	Prevent comment spam by using the Akismet service to determine if the comment is spam. If comment moderation is enabled, Akismet will indicate if the comment is to be moderated or not. If there is no comment moderation, the comment will be rejected if considered to be spam.	Disabled
Akismet API Key	Key required for the Akismet comment spam prevention. *Obtain this key by registering your site at http://akismet.com*	None
Filter spam for registered users	Activate spam filtering for registered users as well. Useful if your site allows anyone to register without screening.	Disabled
Require passcode to register	Users must enter an alphanumeric code to register. The site administrator must inform users of this code. This is to restrict registration to invited users.	Disabled
Passcode	*Alphanumeric code required to complete the registration*	None
Show passcode on registration form	Displays the required passcode on the registration form. This is helpful for legitimate users who want to register while making it difficult for automated robots because the passcode is unique for each site and because it is displayed in JavaScript.	Disabled
Registration page key	To register, users need to go to, for example: tiki-register.php?key=yourregistrationkeyvalue *Key required to be on included the URL to access the registration page (if not empty).*	None

Security - Tokens

Option	Description	Default
Token access	With the presentation of a token, allow access to the content with elevated rights. The primary use of this authentication method is to grant temporary access to content to an external service.	Disabled
Token access default timeout	The default duration for which the generated tokens will be valid.	604800 seconds
Token access default maximum hits	The default maximum number of times a token can be used before it expires.	10 hits
Share access rights with friends when using Share	Allow users to share their access rights for the current page with a friend when sending the link by email, Twitter, or Facebook. The lifespan of the link is defined by the site.	Disabled
Do not delete temporary users when token is deleted/expired	Normally temporary users created (see tiki-adminusers.php) are deleted when their access token is deleted/expired. If turned on, this will keep those users around (and can be manually deleted later) but they will have no groups and therefore no perms	Disabled

Option	Description	Default
Token access	With the presentation of a token, allow access to the content with elevated rights. The primary use of this authentication method is to grant temporary access to content to an external service.	Disabled
Token access default timeout	The default duration for which the generated tokens will be valid.	604800 seconds
Token access default maximum hits	The default maximum number of times a token can be used before it expires.	10 hits
Share access rights with friends when using Share	Allow users to share their access rights for the current page with a friend when sending the link by email, Twitter, or Facebook. The lifespan of the link is defined by the site.	Disabled
Do not delete temporary users when token is deleted/expired	Normally temporary users created (see tiki-adminusers.php) are deleted when their access token is deleted/expired. If turned on, this will keep those users around (and can be manually deleted later) but they will have no groups and therefore no perms	Disabled

Option	Description	Default
Token access	With the presentation of a token, allow access to the content with elevated rights. The primary use of this authentication method is to grant temporary access to content to an external service.	Disabled
Token access default timeout	The default duration for which the generated tokens will be valid.	604800 seconds
Token access default maximum hits	The default maximum number of times a token can be used before it expires.	10 hits
Share access rights with friends when using Share	Allow users to share their access rights for the current page with a friend when sending the link by email, Twitter, or Facebook. The lifespan of the link is defined by the site.	Disabled
Do not delete temporary users when token is deleted/expired	Normally temporary users created (see tiki-adminusers.php) are deleted when their access token is deleted/expired. If turned on, this will keep those users around (and can be manually deleted later) but they will have no groups and therefore no perms	Disabled

Option	Description	Default
Token access	With the presentation of a token, allow access to the content with elevated rights. The primary use of this authentication method is to grant temporary access to content to an external service.	Disabled
Token access default timeout	The default duration for which the generated tokens will be valid.	604800 seconds
Token access default maximum hits	The default maximum number of times a token can be used before it expires.	10 hits
Share access rights with friends when using Share	Allow users to share their access rights for the current page with a friend when sending the link by email, Twitter, or Facebook. The lifespan of the link is defined by the site.	Disabled
Do not delete temporary users when token is deleted/expired	Normally temporary users created (see tiki-adminusers.php) are deleted when their access token is deleted/expired. If turned on, this will keep those users around (and can be manually deleted later) but they will have no groups and therefore no perms	Disabled

Option	Description	Default
Token access	With the presentation of a token, allow access to the content with elevated rights. The primary use of this authentication method is to grant temporary access to content to an external service.	Disabled
Token access default timeout	The default duration for which the generated tokens will be valid.	604800 seconds
Token access default maximum hits	The default maximum number of times a token can be used before it expires.	10 hits
Share access rights with friends when using Share	Allow users to share their access rights for the current page with a friend when sending the link by email, Twitter, or Facebook. The lifespan of the link is defined by the site.	Disabled
Do not delete temporary users when token is deleted/expired	Normally temporary users created (see tiki-adminusers.php) are deleted when their access token is deleted/expired. If turned on, this will keep those users around (and can be manually deleted later) but they will have no groups and therefore no perms	Disabled

Security - SEFURL

Option	Description	Default
Search engine friendly URL	If the site is using Apache, you can rename _htaccess as .htaccess to use short URLs. On IIS, rename web_config as web.config	Disabled
Canonical URL tag	Indicates to search engines which URL to use, to prevent duplicate listings	Enabled
HTTPS for user-specific links	When building notification emails, RSS feeds, the canonical URL or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.	Disabled

Option	Description	Default
Canonical URL domain	If this is a testing site with duplicate content, you may want to put the real site domain here so search engines don't index the testing site. In complex perspective setups using multiple domains, you may want more control on which canonical domain is advertised.	None
Wiki URL scheme	Alter the SEFURL pattern for page names. 👆 *Use the "View" action to regenerate your URLs after changing this setting.* ☰ Replace spaces with dashes | Replace spaces with underscores | URL Encode (Tiki Classic)	Replace spaces with dashes
Custom Routes	Custom routes allow the definition of URLs by the admin, that can be mapped to existing Tiki objects like pages and trackers. "Add BASE tag in the page HEAD" is required when you have "/" as part of the URL.	Enabled
Short URL	Provides the ability to create a short url, easy to share.	Disabled
Short URL base URL	The base URL that is used when generating short URLs, including the HTTP prefix, example: "http://www.example.com". By default will use the URL of the current website.	None
SEFURL postfilter	⚠️ *Do not enable this feature as most Tiki features output friendly URLs and this feature has high processor overhead.*	Disabled
Max size of title in the search engine friendly URL (Tracker Items and Forum Threads)	Limit the number of characters in the tracker item or forum thread title.	200
Article title in SEFURL	The article title rather than article number can be displayed in the search engine friendly URL.	Enabled
Blog title in SEFURL	The blog title rather than blog number can be displayed in the search engine friendly URL.	Enabled
Display forum thread or forum post title in the search engine friendly URL		Enabled

Option	Description	Default
Tracker title in SEFURL	To display the title, you should disable `Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page`	Enabled
Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page	This redirection uses the wiki prefix alias feature	Disabled
Use Only ASCII in SEFURLs	Do not use accented characters in short (search engine friendly) URLs.	Disabled
URL Frgament format	Provides ability to change anchor format * *Set to "Complete" to change the encoding and allow anchors to contain other characters in addition to ASCII letters and digits.* Strict | Complete	Strict
URL Fragment Guesser	Scroll to the closest anchor when the one indicated in the URL is missing in a page.	Disabled

Option	Description	Default
Search engine friendly URL	If the site is using Apache, you can rename _htaccess as .htaccess to use short URLs. On IIS, rename web_config as web.config	Disabled
Canonical URL tag	Indicates to search engines which URL to use, to prevent duplicate listings	Enabled
HTTPS for user-specific links	When building notification emails, RSS feeds, the canonical URL or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.	Disabled
Canonical URL domain	If this is a testing site with duplicate content, you may want to put the real site domain here so search engines don't index the testing site. In complex perspective setups using multiple domains, you may want more control on which canonical domain is advertised.	None

Option	Description	Default
Wiki URL scheme	Alter the SEFURL pattern for page names. 👆 *Use the "View" action to regenerate your URLs after changing this setting.* ☰ Replace spaces with dashes | Replace spaces with underscores | URL Encode (Tiki Classic)	Replace spaces with dashes
Custom Routes	Custom routes allow the definition of URLs by the admin, that can be mapped to existing Tiki objects like pages and trackers. "Add BASE tag in the page HEAD" is required when you have "/" as part of the URL.	Enabled
Short URL	Provides the ability to create a short url, easy to share.	Disabled
Short URL base URL	The base URL that is used when generating short URLs, including the HTTP prefix, example: "http://www.example.com". By default will use the URL of the current website.	None
SEFURL postfilter	⚠️ *Do not enable this feature as most Tiki features output friendly URLs and this feature has high processor overhead.*	Disabled
Max size of title in the search engine friendly URL (Tracker Items and Forum Threads)	Limit the number of characters in the tracker item or forum thread title.	200
Article title in SEFURL	The article title rather than article number can be displayed in the search engine friendly URL.	Enabled
Blog title in SEFURL	The blog title rather than blog number can be displayed in the search engine friendly URL.	Enabled
Display forum thread or forum post title in the search engine friendly URL		Enabled
Tracker title in SEFURL	To display the title, you should disable `Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page`	Enabled
Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page	This redirection uses the wiki prefix alias feature	Disabled

Option	Description	Default
Use Only ASCII in SEFURLs	Do not use accented characters in short (search engine friendly) URLs.	Disabled
URL Frgament format	Provides ability to change anchor format ✱ *Set to "Complete" to change the encoding and allow anchors to contain other characters in addition to ASCII letters and digits.* ☰ Strict | Complete	Strict
URL Fragment Guesser	Scroll to the closest anchor when the one indicated in the URL is missing in a page.	Disabled

Option	Description	Default
Search engine friendly URL	If the site is using Apache, you can rename _htaccess as .htaccess to use short URLs. On IIS, rename web_config as web.config	Disabled
Canonical URL tag	Indicates to search engines which URL to use, to prevent duplicate listings	Enabled
HTTPS for user-specific links	When building notification emails, RSS feeds, the canonical URL or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.	Disabled
Canonical URL domain	If this is a testing site with duplicate content, you may want to put the real site domain here so search engines don't index the testing site. In complex perspective setups using multiple domains, you may want more control on which canonical domain is advertised.	None
Wiki URL scheme	Alter the SEFURL pattern for page names. ☝ *Use the "View" action to regenerate your URLs after changing this setting.* ☰ Replace spaces with dashes | Replace spaces with underscores | URL Encode (Tiki Classic)	Replace spaces with dashes
Custom Routes	Custom routes allow the definition of URLs by the admin, that can be mapped to existing Tiki objects like pages and trackers. "Add BASE tag in the page HEAD" is required when you have "/" as part of the URL.	Disabled

Option	Description	Default
Short URL	Provides the ability to create a short url, easy to share.	Disabled
Short URL base URL	The base URL that is used when generating short URLs, including the HTTP prefix, example: "http://www.example.com". By default will use the URL of the current website.	None
SEFURL postfilter	⚠ *Do not enable this feature as most Tiki features output friendly URLs and this feature has high processor overhead.*	Disabled
Max size of title in the search engine friendly URL (Tracker Items and Forum Threads)	Limit the number of characters in the tracker item or forum thread title.	200
Article title in SEFURL	The article title rather than article number can be displayed in the search engine friendly URL.	Enabled
Blog title in SEFURL	The blog title rather than blog number can be displayed in the search engine friendly URL.	Enabled
Display forum thread or forum post title in the search engine friendly URL		Enabled
Tracker title in SEFURL	To display the title, you should disable `Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page`	Disabled
Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page	This redirection uses the wiki prefix alias feature	Disabled
Use Only ASCII in SEFURLs	Do not use accented characters in short (search engine friendly) URLs.	Disabled

Option	Description	Default
Search engine friendly URL	If the site is using Apache, you can rename _htaccess as .htaccess to use short URLs. On IIS, rename web_config as web.config	Disabled
Canonical URL tag	Indicates to search engines which URL to use, to prevent duplicate listings	Enabled

Option	Description	Default
HTTPS for user-specific links	When building notification emails, RSS feeds, the canonical URL or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.	Disabled
Canonical URL domain	If this is a testing site with duplicate content, you may want to put the real site domain here so search engines don't index the testing site. In complex perspective setups using multiple domains, you may want more control on which canonical domain is advertised.	None
Wiki URL scheme	Alter the SEFURL pattern for page names. 👆 *Use the "View" action to regenerate your URLs after changing this setting.* ☰ Replace spaces with dashes | Replace spaces with underscores | URL Encode (Tiki Classic)	Replace spaces with dashes
Custom Routes	Custom routes allow the definition of URLs by the admin, that can be mapped to existing Tiki objects like pages and trackers. "Add BASE tag in the page HEAD" is required when you have "/" as part of the URL.	Disabled
Short URL	Provides the ability to create a short url, easy to share.	Disabled
Short URL base URL	The base URL that is used when generating short URLs, including the HTTP prefix, example: "http://www.example.com". By default will use the URL of the current website.	None
SEFURL postfilter	⚠️ *Do not enable this feature as most Tiki features output friendly URLs and this feature has high processor overhead.*	Disabled
Max size of title in the search engine friendly URL (Tracker Items and Forum Threads)	Limit the number of characters in the tracker item or forum thread title.	200
Article title in SEFURL	The article title rather than article number can be displayed in the search engine friendly URL.	Enabled

Option	Description	Default
Blog title in SEFURL	The blog title rather than blog number can be displayed in the search engine friendly URL.	Enabled
Display forum thread or forum post title in the search engine friendly URL		Enabled
Tracker title in SEFURL	To display the title, you should disable `Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page`	Disabled
Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page	This redirection uses the wiki prefix alias feature	Disabled
Use Only ASCII in SEFURLs	Do not use accented characters in short (search engine friendly) URLs.	Disabled

Option	Description	Default
Search engine friendly URL	If the site is using Apache, you can rename _htaccess as .htaccess to use short URLs. On IIS, rename web_config as web.config	Disabled
Canonical URL tag	Indicates to search engines which URL to use, to prevent duplicate listings	Enabled
HTTPS for user-specific links	When building notification emails, RSS feeds, the canonical URL or other externally available links, use HTTPS when the content applies to a specific user. HTTPS must be configured on the server.	Disabled
Canonical URL domain	If this is a testing site with duplicate content, you may want to put the real site domain here so search engines don't index the testing site. In complex perspective setups using multiple domains, you may want more control on which canonical domain is advertised.	None
Wiki URL scheme	Alter the SEFURL pattern for page names. *Use the "View" action to regenerate your URLs after changing this setting.* Replace spaces with dashes | Replace spaces with underscores | URL Encode (Tiki Classic)	Replace spaces with dashes

Option	Description	Default
Custom Routes	Custom routes allow the definition of URLs by the admin, that can be mapped to existing Tiki objects like pages and trackers. "Add BASE tag in the page HEAD" is required when you have "/" as part of the URL.	Disabled
Short URL	Provides the ability to create a short url, easy to share.	Disabled
Short URL base URL	The base URL that is used when generating short URLs, including the HTTP prefix, example: "http://www.example.com". By default will use the URL of the current website.	None
SEFURL postfilter	⚠ *Do not enable this feature as most Tiki features output friendly URLs and this feature has high processor overhead.*	Disabled
Max size of title in the search engine friendly URL (Tracker Items and Forum Threads)	Limit the number of characters in the tracker item or forum thread title.	200
Article title in SEFURL	The article title rather than article number can be displayed in the search engine friendly URL.	Enabled
Blog title in SEFURL	The blog title rather than blog number can be displayed in the search engine friendly URL.	Enabled
Display forum thread or forum post title in the search engine friendly URL		Enabled
Tracker title in SEFURL	To display the title, you should disable `Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page`	Disabled
Rewrite tiki-view_tracker.php?itemId=yyy to Prefixyyy page	This redirection uses the wiki prefix alias feature	Disabled
Use Only ASCII in SEFURLs	Do not use accented characters in short (search engine friendly) URLs.	Disabled