Security Tokens tab

Overview

Use this tab to configure Tiki to use tokens for site access.

To Access

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

Related Topics

- security admin
- Token Access
- PluginGetAccessToken

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

Option	Description	Default
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

For more details see Token Access.