

# Tab Generelle Sicherheit

## Übersicht

Benutze diesen Tab um die site-weit gültigen Sicherheitseinstellungen zu konfigurieren.

## Zugriff

Unter Sicherheit auf der Verwaltungsseite, klicke auf den Tab **Allgemeine Sicherheit**.

Verwandte Themen

- Generelle Einstellungen Login
- dev:Sicherheit

Security

General Security Spam protection Search results Site Access Tokens Clipperz online password management

Smarty Security

HTML Purifier

*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.*

Output should be HTML Purified

REALLY allow HTML (INSECURE)

*You need to set Allow HTML in menu option names and URLs*

Protect all sessions

Please also see: HTTPS (SSL) and other login preferences

CSRF Security

Use these options to protect against cross-site request forgeries (CSRF).

Require confirmation if possible CSRF detected

Protect against CSRF with a ticket

Apply

Tab Generelle Sicherheit

Feld	Beschreibung	Standardwert
Smarty Sicherheit	Wenn aktiviert <b>ist keine</b> PHP--Kodierung in Smarty TPL Vorlagen erlaubt.	Aktiviert
HTML Reiniger	Wenn aktiviert wird Tiki versuchen, alle erstellten Seiten zu "desinfizieren" um zu den Standardkompatible Seiten zu erstellen.	
Ausgabe soll HTML-gereinigt sein		
Erlaube HTML in Link-Texten...	Wenn aktiviert kannst Du HTML in Menülinks verwenden	Deaktiviert
Bestätigung erforderlich, wenn möglicher CSRF entdeckt wird		

Feld	Beschreibung	Standartwert
Schütze gegen CSRF mit einem Ticket		
<div data-bbox="1097 151 1142 183" style="display: inline-block; border: 1px solid black; padding: 2px;">x</div>		
Tab name		
Feld	Beschreibung	Standartwert
Smarty Sicherheit	Wenn aktiviert <b>ist keine</b> PHP--Kodierung in Smarty TPL Vorlagen erlaubt.	Aktiviert
HTML Reiniger	Wenn aktiviert wird Tiki versuchen, alle erstellten Seiten zu "desinfizieren" um zu den Standarts kompatible Seiten zu erstellen.	
Ausgabe soll HTML-gereinigt sein		
Erlaube HTML in Link-Texten...	Wenn aktiviert kannst Du HTML in Menülinks verwenden	Deaktiviert
Bestätigung erforderlich, wenn möglicher CSRF entdeckt wird		
Schütze gegen CSRF mit einem Ticket		