General	
Display account lock information message	Indicates if user friendly information about account lock should be displayed.
Enable Autocomplete	If true Autocomplete for user name text box in sign-in form is enabled.

Bad words	
Check bad words	Determines if bad word check should be performed.
Bad word replacement	Default replacement text which will be used during bad word check.
Bad word action	Default action which will be performed during bad words check.

Banned IPs	
Enable banned IPs	Enables or disables banned IPs features.
Redirect banned IPs to URL	If the IP address is banned the user is redirected to this page.

Flood protection	
Enable flood protection	Enables or disables flood protection, which prevents spam on forums and other community services.
Flood protection interval	Value in seconds which represent the minimal interval between user's actions.

CAPTCHA settings	
Control to use	Determines the default CAPTCHA control that should be used for CAPTCHA verification throughout the system – in web parts and for the **Security code** form control. The following four types of controls are available: • Logic CAPTCHA – requires answering a logical question. • Simple CAPTCHA – requires re-typing of a string displayed in an image. • Text CAPTCHA – requires re-typing of a string into multiple fields. • reCAPTCHA – requires the user to click a checkbox to prove they are not a bot. The user either passes immediately, or needs to perform an additional image selection test to prove they are human.
reCAPTCHA site key	⚠ **Important**: To use reCAPTCHA after March 31, 2018, you need to download and apply hotfix 11.0.10 or newer, which updates the system to use reCAPTCHA v2. The site API key for the site where you want to use reCAPTCHA. Obtain the necessary API keys from https://www.google.com/recaptcha/admin.
reCAPTCHA secret key	The secret API key for the site where you want to use reCAPTCHA. Obtain the necessary API keys from https://www.google.com/recaptcha/admin.

Invalid sign-in attempts	

Maximum invalid sign-in attempts	Maximum invalid sign-in attempts before the user account is locked. If set to *0*, invalid sign-in attempts functionality is disabled.
Send unlock account e-mail	Indicates if an account unlock email is sent when a user account is locked due to reaching the maximum invalid sign-in attempts.
Unlock user account path	Path to custom page for unlocking user account (if not set, system page ~/CMSModules/Membership /CMSPages/UnlockUserAccount.aspx will be used).
Screen lock	
Enable screen lock	Enables or disables screen lock feature, which locks the part of the browser with the Kentico administration interface.
Lock interval (minutes)	Time (in minutes) that has to pass before the screen is locked. This value has to be greater than 0 and lower than session timeout.
Warning interval (seconds)	Warning period (in seconds). Warning with countdown is shown for this number of seconds before the screen is locked.