Optional password security rules

Graham Smith - 2017-06-22 - Security / Privacy

The **standard** setup for a Kahootz site is to require each user's password to be between 6 and 16 characters but to have no other constraints. A password strength meter is shown when users register or change their password to encourage the use of strong passwords, but we find the open approach allows people to use passwords they can remember, rather than needing special ones to match constraints that they then forget. This helps people login from anywhere without having to use 'forgotten password' regularly or writing their password down.

UK Government sites ordered through the G-Cloud at 'OFFICIAL over the Internet' security have a slightly higher set of constraints, based on the old IL2 requirements and CESG guidance. Passwords must be between 8 and 16 characters and contain at least one uppercase letter (A-Z), at least one lowercase letter (a-z) and at least one number (0-9). Kahootz will also lock an account out for 30 minutes after five failed login attempts (ie: correct email address but wrong password).

Kahootz Enterprise clients can specify their own password security rules to satisfy their own requirements. Options include:

- The minimum and maximum length of a password.
- Password format controls, allowing you to require or block characters or words. for example, requiring uppercase letters or numbers, or blocking predictable words like 'password' or your company name or office location. (Technical detail: we can add anything that can be put as in 'regular expression' syntax).
- Optional audit recording of failed logins.
- Lockout - blocking login on an account for a specified amount of time after a specified number of failed logins. Users will be notified by email of the lock, but NOT in the web browser - this is deliberate so that any potential hacker trying to guess passwords will continue guessing on the now locked account without realising they need to try another, thus increasing the protection.
- The ability to force regular password changes (specified number of days).
- If regularly changing passwords, how many old passwords to remember to prevent re-use.
- A minimum password age, to stop people working around the above rule by changing their password several times in a row to get back to their original password.
- Whether to allow users to use the "remember me" cookie, or to require login each time people visit the site.
- The ability to automatically log out users if they aren't active in their browser for a specified amount of time.

Site owners can see the current settings for their site through **Account > Site Admin > Settings**. If you need to make changes to your password policy please contact support.

Related Content

- Additional security measures for Kahootz Enterprise
- How-To Change your Password