Bruteforce

In order to prevent brute force attacks on passwords to measures are implemented

- Maximum number of retries for passwords
- Detection of spread attacks across multiple accounts

Maximum login retries

Configuration options for Maximum number of login retries are

After the defined amount of retries have been reached, the user account is suspended.

There is an option for automatic password reset (password is sent to user).

Policy_reference#Security

Brute force detection

Detection of spread attacks are implemented by registering the number of failed login attempts during a defined amount of time.

If a certain threshold is passed, the server will temporarily deny further login attempts, for a defined amount of time.

During this period the server will function normally for already logged in users.

Configuration options for brute force detection are

Policy_reference#Protection

Revision #2
Created 3 April 2025 13:17:46 by Theis Villumsen
Updated 13 October 2025 12:47:29 by Max Gøtske